www.ip-com.com.cn

User Guide

IP-COM ProFi Software Controller

V3.0

IP-COM
World Wide Wireless

Copyright Statement

©2022 IP-COM Networks Co., Ltd. All rights reserved.

IP-COM is the registered trademark of IP-COM Networks Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to IP-COM Networks Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of IP-COM Networks Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM! Please read this user guide before you start. The user guide applies to the ProFi Software Controller and corresponding ProFi devices.

Conventions

The ProFi Software Controller explained in this user guide is based on the software version of V1.0.3.0 (1900). The Controller's functions may vary according to different versions. It is recommended to upgrade your Controller to the latest version.

The screenshots, IP addresses and other information mentioned in this user guide is only for illustration. Please refer to the actual situations.

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	Internet Settings > LAN Setup
Parameter and value	Bold	Set **SSID** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
UI control	Bold	On the **Quick Setup** page, click the **Save** button.

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
	This format is used to add more explanations to certain configuration.

For More Documents

ProFi Software Controller can manage ProFi series APs and switches in a unified manner. For more about this series of APs and switches, refer to user guides of target models.

Search target product models on our official website www.ip-com.com.cn to obtain the latest product documents.

Document	Overview
User Guide	Walks you through detailed functions and configuration of ProFi Software Controller, including all the functions on its web UI.
Quick Configuration Guide	Walks you through installation and quick setup, including ProFi Software Controller installation, network configuration, and so on.

Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.

+86-755-27653089	info@ip-com.com.cn	www.ip-com.com.cn

Revision History

IP-COM is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the ProFi Software Controller was released.

Version	Date	Description
V3.0	2022-07-22	1. Update of web UI 2. Addition of VLAN and guest control examples
V2.0	2021-09-30	1. Addition of content related to manageable switches 2. Other optimization points
V1.0	2021-04-13	Original publication

Contents

Preface ..... **i**

Contents ..... **iii**

1 Quick Setup **1**

1.1 System Requirements 1
1.2 Network Topology 2
1.3 Application Scenario 3
1.4 Install Controller (Example: Windows 10) 5
1.5 Configure Controller 8
Option A: Log in using a ProFi SDN Cloud account 8
Option B: Log in using a local account 12
1.6 Remote Access 17
Scenario A: You have logged in using a ProFi SDN Cloud account 17
Scenario B: You have logged in using a local account 18

2 IP-COM Cloud Network **20**

2.1 Login 20
2.2 Admin 22
2.3 Additional Details 25

3 Use the ProFi Software Controller **28**

3.1 Navigation Bar 29
3.2 Common Interface Options 30
3.2.1 Current Site 30
3.2.2 Username 33
3.2.3 Properties 35
3.2.4 Events 35
3.2.5 Alerts 36
3.2.6 Help Center 37
3.2.7 Settings 38

4 Dashboard **74**

4.1 System Status 74
4.2 ISP Load 75
4.3 Network 75
4.4 Wireless Channel and Client Layout 77
4.5 Operation Status 78
4.5.1 Abnormal Conditions 78
4.5.2 Total WiFi Clients 79

4.5.3 Device Online Status 80
4.5.4 WiFi Clients 80

5 Statistics 81

5.1 System Stats 82
5.1.1 Number of Wireless Clients (Per SSID): Top 5 83
5.1.2 Number of Wireless Clients (Per AP): Top 5 84
5.1.3 Wireless Clients Traffic (Per AP): Top 5 85
5.1.4 Number of Wireless Clients (Per Radio Type) 86
5.1.5 Quick Look 87
5.1.6 Recent Activities 88
5.2 Performance 89
5.2.1 Number of Wireless Clients 90
5.2.2 CPU and Memory Usage 90
5.2.3 Data Traffic 90
5.3 Debugging Metrics 91
5.3.1 Most Active AP 92
5.3.2 Packet Loss Rate 92
5.3.3 Channel Utilization Rate 93
5.3.4 Client Number 94
5.3.5 Client Activity 94
5.3.6 Client Connection Duration 95
5.3.7 Memory Usage Rate 95
5.3.8 CPU Usage Rate 96

6 Map 97

6.1 Add Custom Maps 97
6.2 Edit a Map 100
6.3 Place Devices on the Map 101
6.4 Map Display Options 103
6.5 Additional Options 104

7 Devices 105

8 Switch Details 113

8.1 Details 116
8.1.1 Overview 116
8.1.2 Uplink 117
8.1.3 Downlink 117
8.2 Clients 119
8.3 Ports 120
8.3.1 Overview 120
8.3.2 Port Configuration 121
8.4 Configuration 124

8.4.1 General 124
8.4.2 Service 124
8.4.3 Internet 126
8.4.4 VLAN Configuration 127
8.4.5 Manage Device 131
8.5 Stats 135
9 AP Details 136
9.1 Details 139
9.1.1 Overview 139
9.1.2 Uplink 140
9.1.3 RF 140
9.1.4 WLANs 142
9.1.5 WLAN Downlink 142
9.2 Clients 143
9.3 Configuration 144
9.3.1 General 144
9.3.2 RF 144
9.3.3 Band Steering 147
9.3.4 RF Optimization 147
9.3.5 WLAN 148
9.3.6 SSID Maximum Number of Clients 148
9.3.7 VLAN Configuration 149
9.3.8 Network 150
9.3.9 Manage Device 152
9.4 Stats 156
10 Client Details 157
11 Configuration Examples 171
11.1 Example of VLAN Configuration 171
11.2 Examples of Guest Control Configuration 177
11.2.1 Using Simple Password for Authentication 177
11.2.2 Using Account and Password for Authentication 182
11.2.3 Using SMS for Authentication 188
11.2.4 Using Email for Authentication 193
Appendix 200

1 Quick Setup

1.1 System Requirements

Supported OS:

Windows 11/10/7

Recommended system configurations:

Windows 10 (64-bit) or newer, 8 GB RAM or more, 50 GB or more free space in system partition

Minimum system configurations:

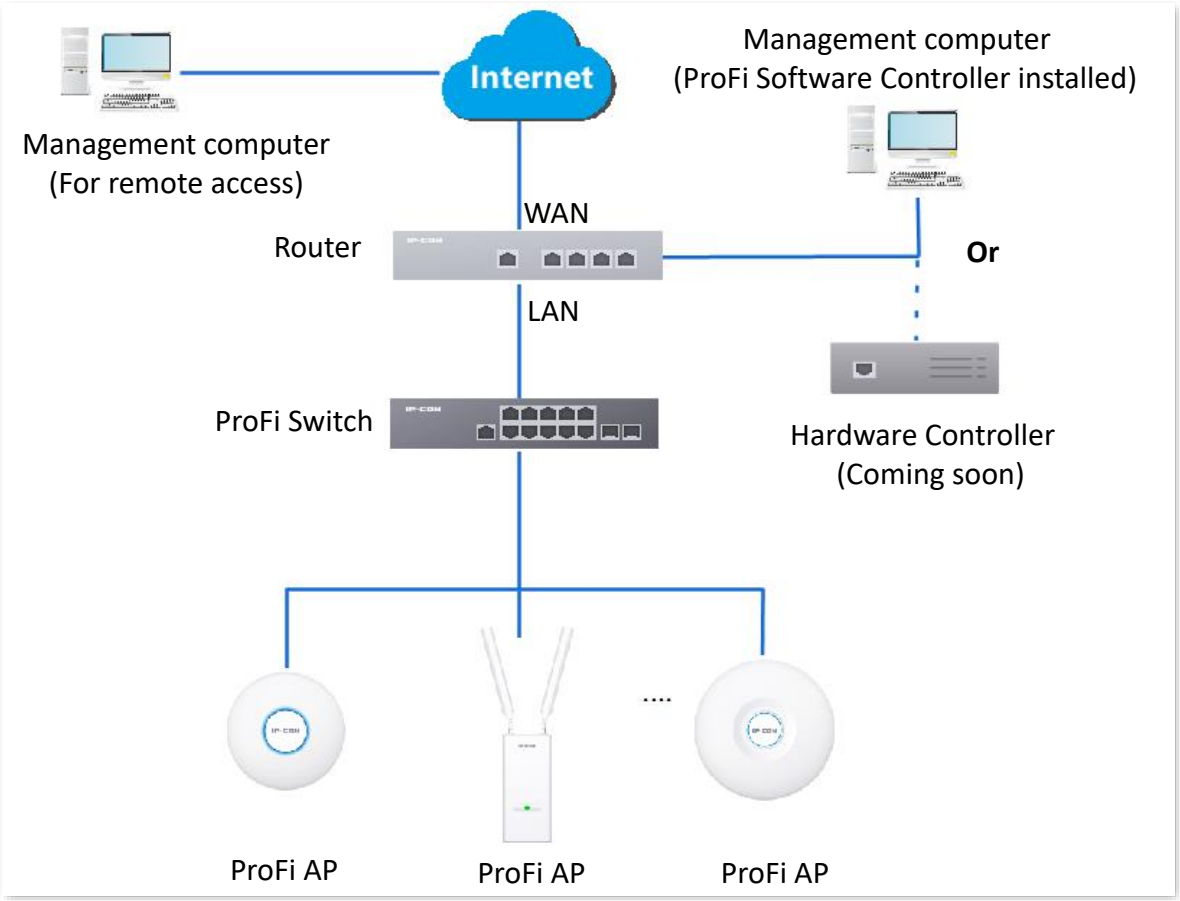
Windows 7 (32-bit), 4 GB RAM or more, 10 GB or more free space in system partition

Compatible web browser:

- Google Chrome: Stable version officially released within last 2 years
- Edge: Stable version officially released within 1 year
- Firefox: Version 60.0 or above
- Opera: Stable version officially released within last 2 years

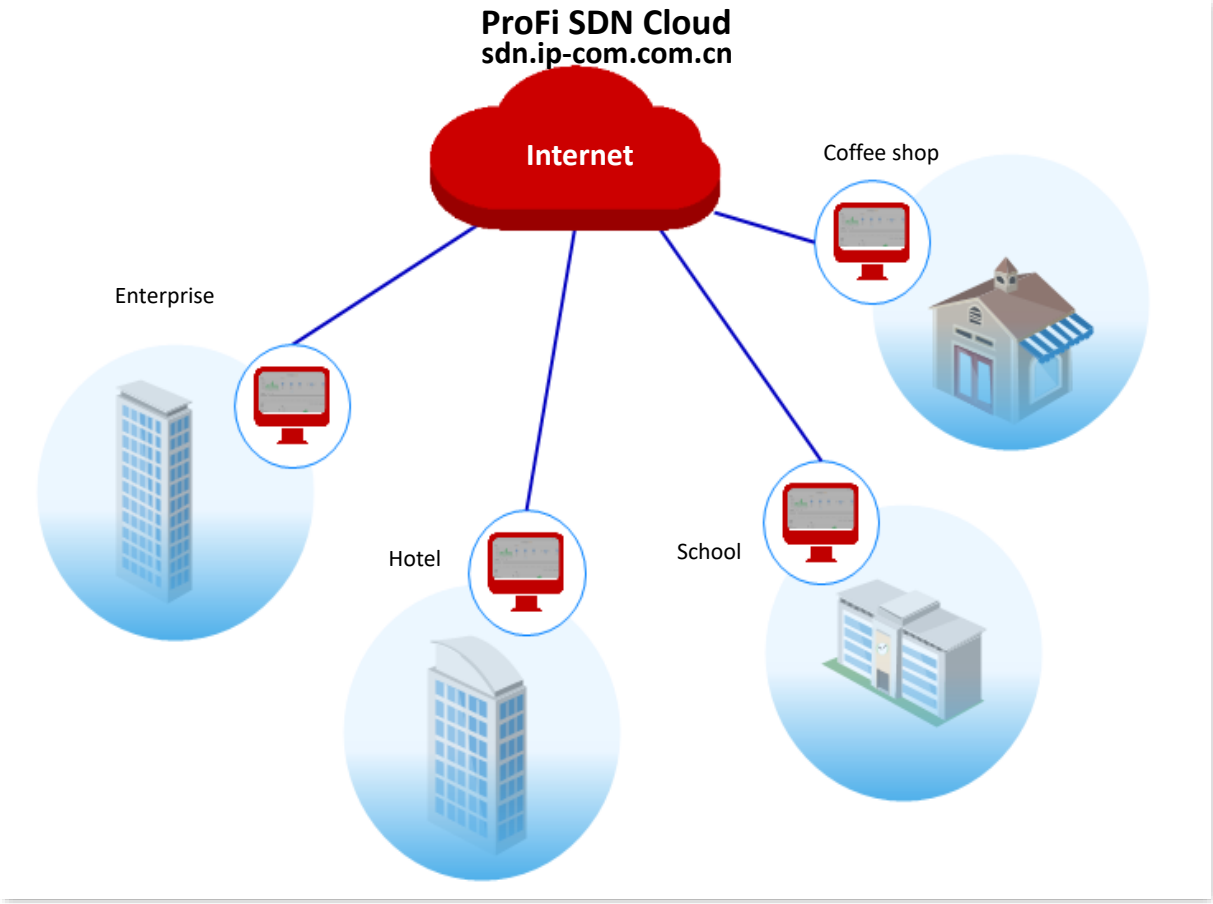
1.2 Network Topology

The ProFi Software Controller allows you to manage locally or remotely your ProFi series APs and switches using a web browser.



1.3 Application Scenario

To achieve ProFi network deployment in real scenarios, ProFi Software Controller can automatically detect all the devices in the LAN supporting ProFi Software Controller management, mark their device information and thus provides centralized management.



As shown above, the enterprise, hotel, school, and coffee shop can all deploy a ProFi Software Controller in their own network, and with this ProFi Software Controller, they can manage and monitor their local networks without having to connect to the internet.

If necessary, you can also enable the remote access function on the local controller. In this way, O&M personnel in charge of multiple locations can remotely access the ProFi Software Controllers deployed in these locations, and manage and maintain the networks, improving O&M efficiency.

- **Local Management**

  Deploy a ProFi Software Controller in a Layer-2 network.

- **Remote Management**

1. Choose **SETTINGS** (⚙) > **Remote Access**, toggle on **Enable Remote Access**, enter the ProFi SDN Cloud account and password, and click **SAVE**.

2. Visit sdn.ip-com.com.cn and log in to ProFi SDN Cloud using your ProFi SDN Cloud account.

----End

After you successfully logged in to the ProFi SDN Cloud, you can remotely manage all the ProFi Software Controllers under this account.

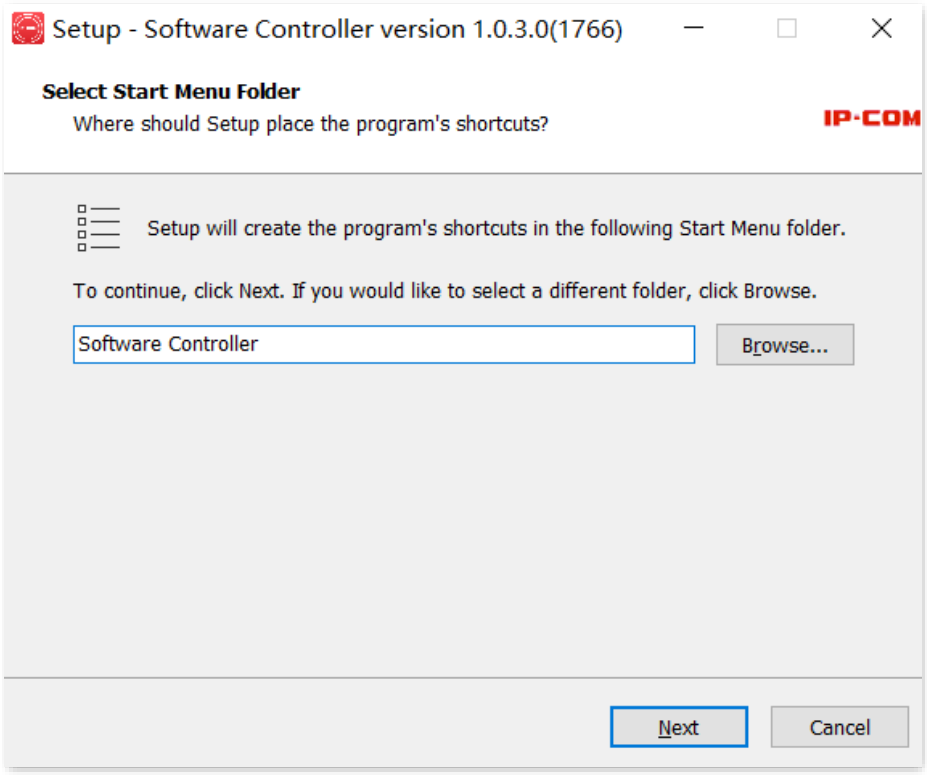
1.4 Install Controller (Example: Windows 10)

Note

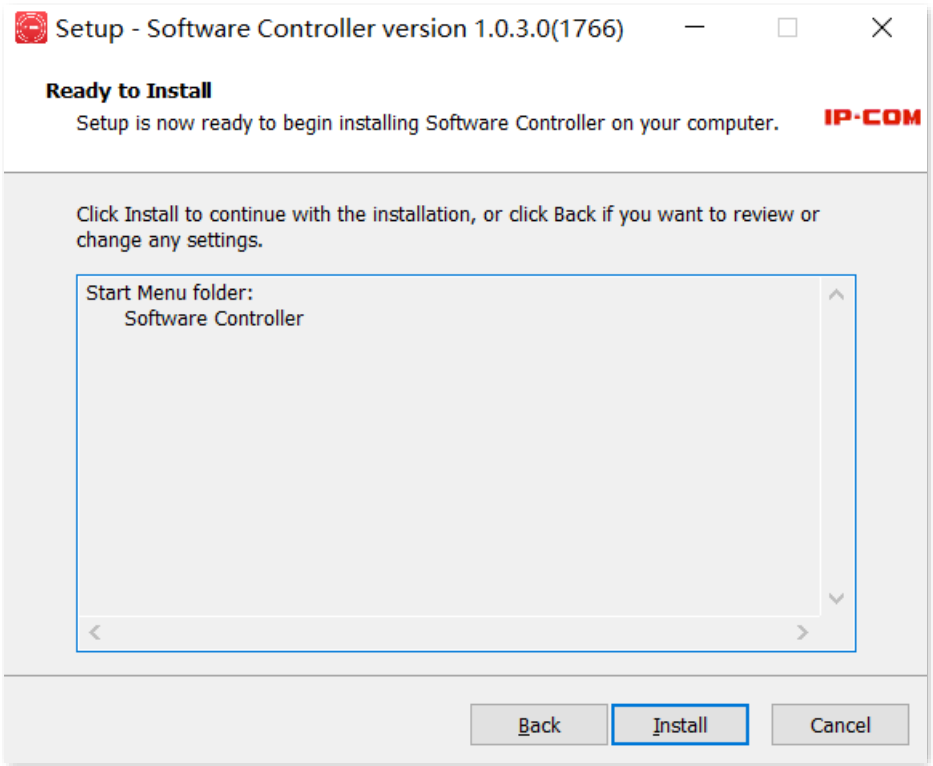
If such antivirus software as Avast Free Antivirus, AVG AntiVirus, ESET Internet Security, Tencent PC Manager, Kingsoft AntiVirus and Kaspersky Free is running, an installation error may occur. In this case, please disable the antivirus software or move the ProFi Software Controller application to whitelist first.

1. Download the installation package of the ProFi Software Controller at www.ip-com.com.cn.
2. Double-click the **Software Controller installer.exe** file.
3. Click **Yes** in the pop-up window.

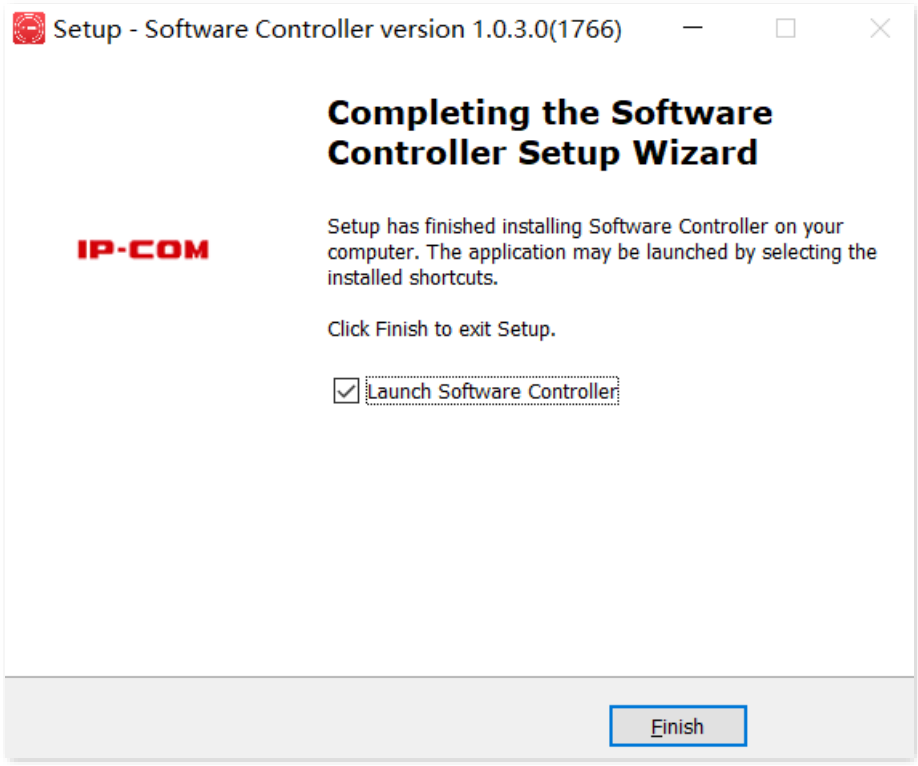
4. Click **Next**, then the Software Controller will be automatically installed on the C drive.



5. Click **Install**.



6. Wait for the installation to complete. Click **Finish**.



----End

1.5 Configure Controller

You can log in to the ProFi Software Controller either using a ProFi SDN Cloud account (for both local access and remote access) or a local account of the ProFi Software Controller (only for local access). Please choose a login type based on your actual scenario.

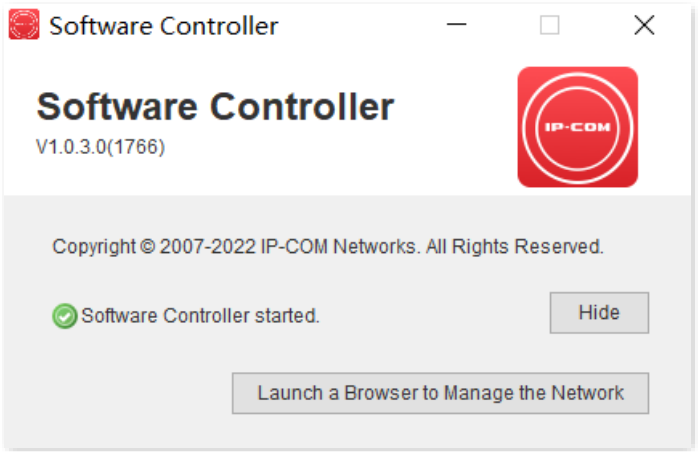
- If the computer installed with the ProFi Software Controller **is connected to the internet**, you can use both accounts, but ProFi SDN Cloud account is recommended.
- If the computer installed with the ProFi Software Controller **is disconnected from the internet**, you can only use a local account.

Tip

The computer's firewall may affect the normal login to the ProFi Software Controller. In such case, disable the firewall before login.

Option A: Log in using a ProFi SDN Cloud account

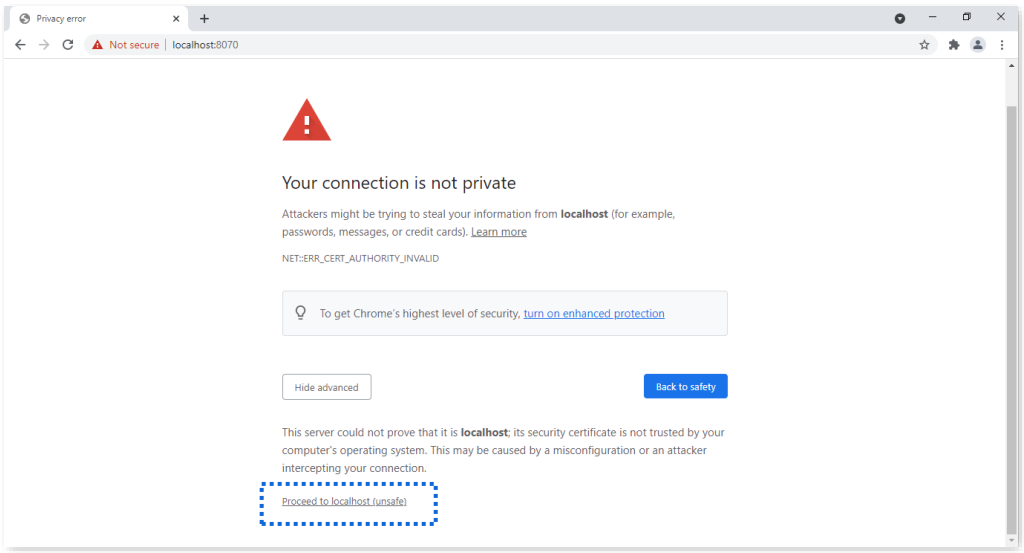
1. Start the ProFi Software Controller and click **Launch a Browser to Manage the Network**.



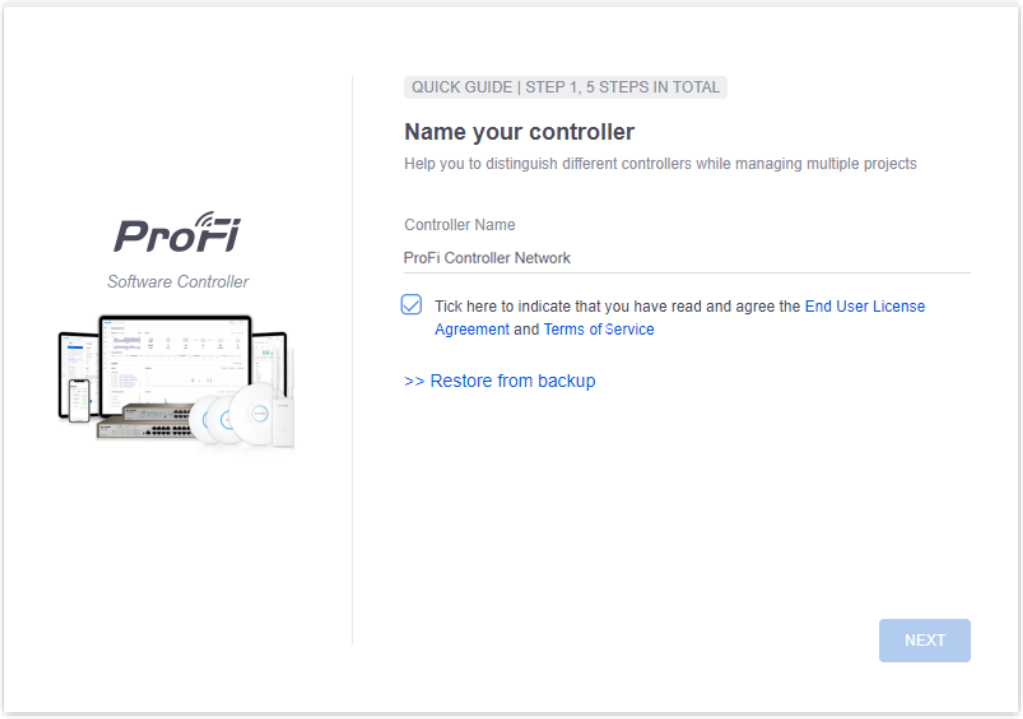
2. Click **Advanced** and **Proceed to localhost (unsafe)** in sequence. Google Chrome is used here as an example.

Tip

ProFi Software Controller supports HTTPS login. When you access its web UI, a prompt message indicating that the web address is not secure, for example, "Your connection is not private", may appear. Ignore the message and go on to visit the webpage.



3. Customize a Controller name as needed, select **Tick here to indicate that you have read and agreed the End User License Agreement and Terms of Service**, and click **NEXT**.



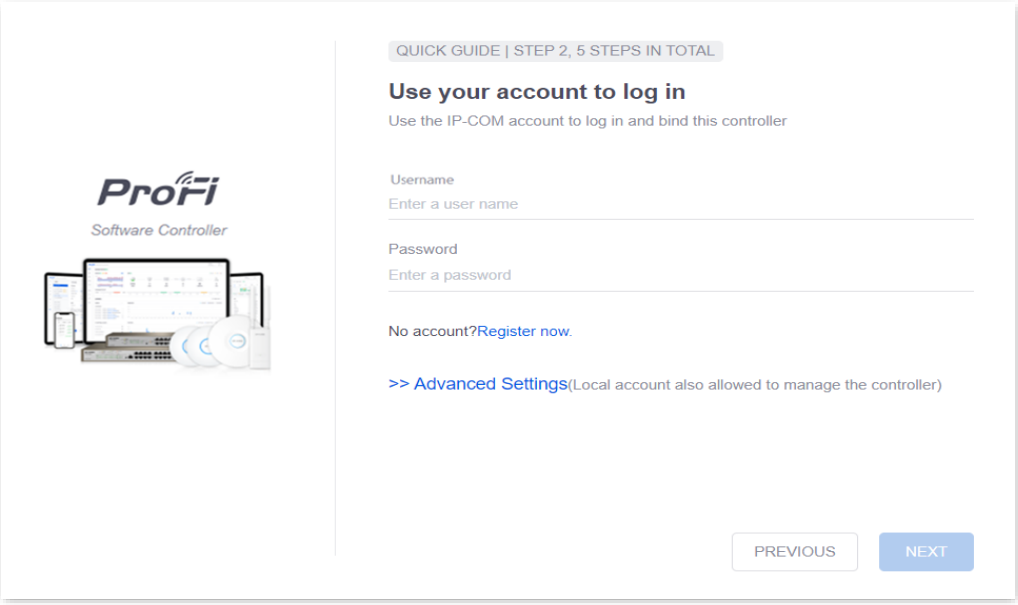
Tip

Alternatively, you can click **Restore from backup** to use a file that contains your previous settings to directly go to the login page of ProFi Software Controller.

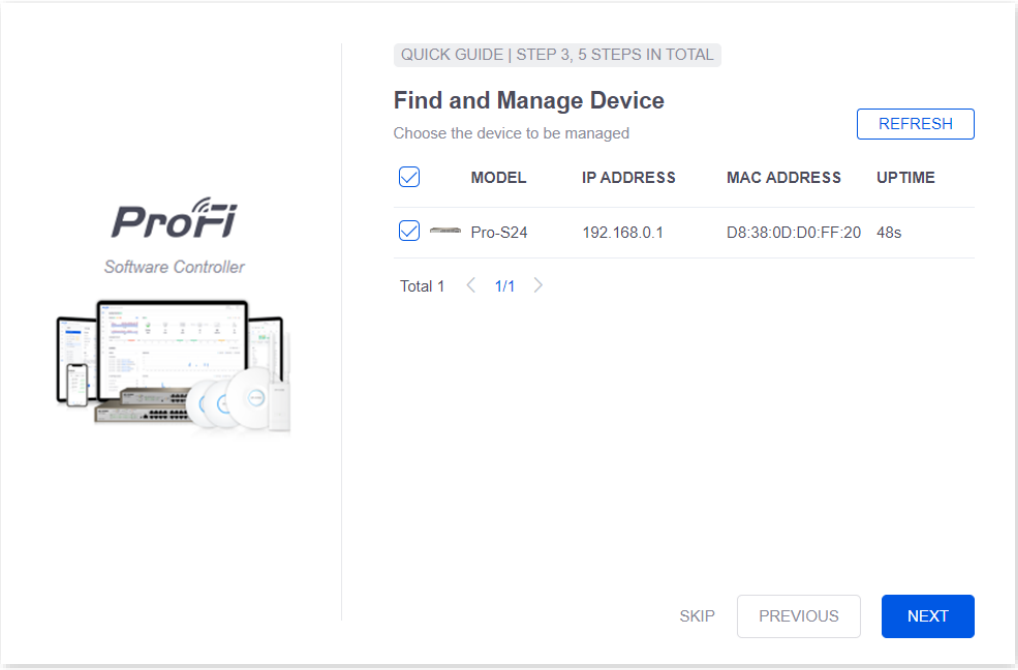
4. Enter your ProFi SDN Cloud username and password and click **NEXT**.

Tip

If you do not have a ProFi SDN Cloud account, register one by following the on-screen instructions. Only through a ProFi SDN Cloud account can you realize remote access.



5. Wait until the ProFi series APs and switches are displayed in the device list, select the APs and switches you wish to adopt and click **NEXT**.

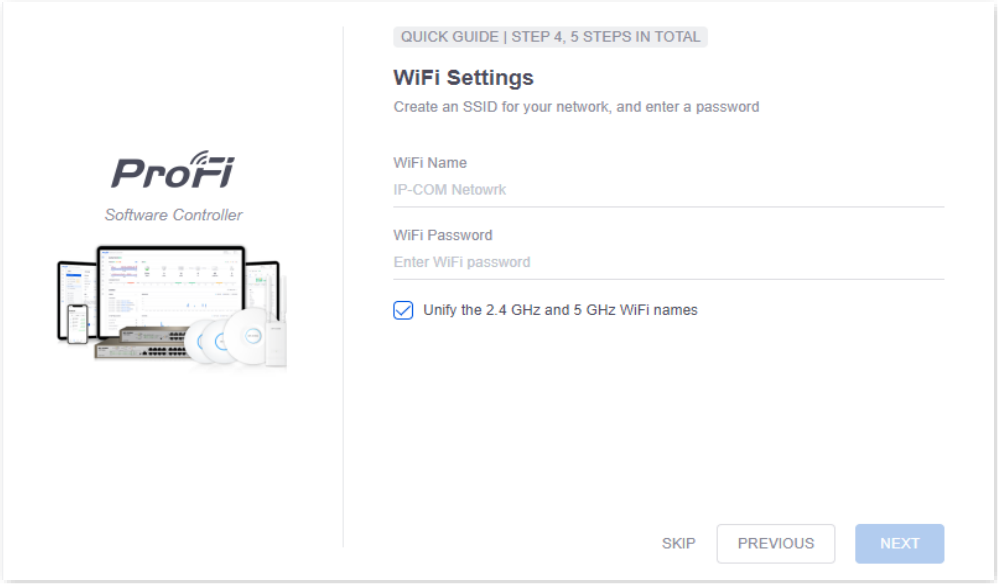


Tip

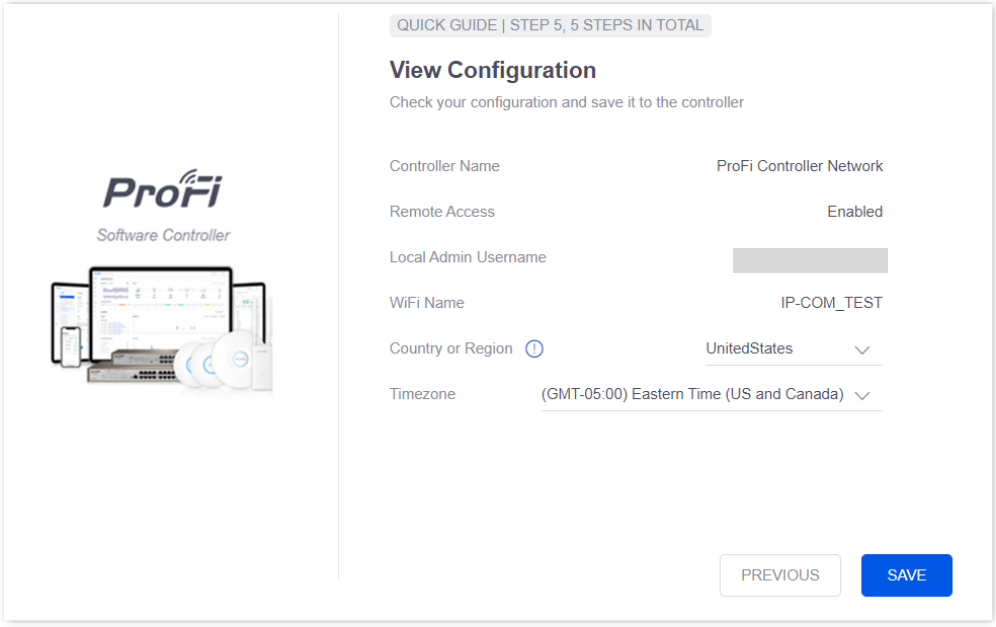
If your devices do not appear in the list, try the following solutions:

- Verify that the IP address of your management computer and IP addresses of your APs and switches are in the same network segment. For example, if the IP address of your AP is **192.168.0.254**, then the IP address of your management computer should be **192.168.0.*X*** (*X* ranges from 2 to 253 and is not occupied).
- Verify that your APs and switches are in factory settings.

6. Set **WiFi Name** and **WiFi Password** for the primary WiFi network of the AP and click **NEXT**.



7. Check your configurations, select **Country or Region** and **Timezone** and click **SAVE**.



----End

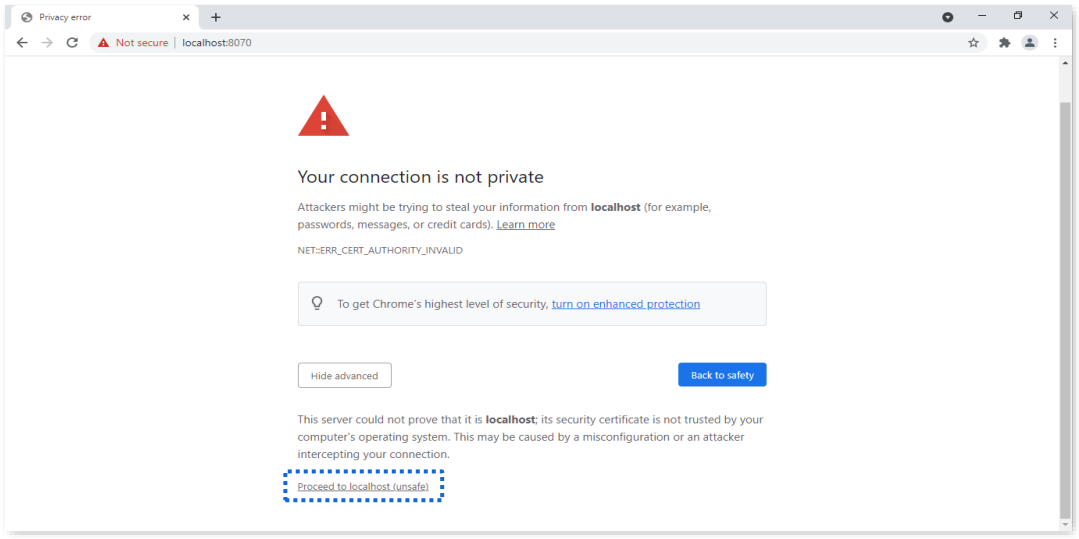
Option B: Log in using a local account

1. Start the ProFi Software Controller and click **Launch a Browser to Manage the Network.**

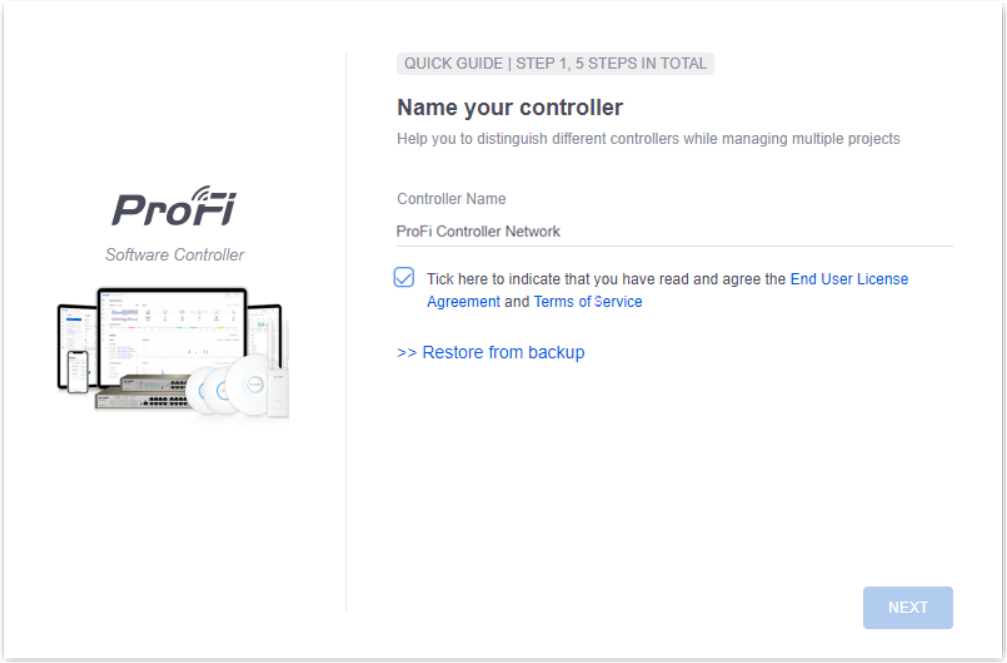
2. Click **Advanced** and **Proceed to localhost (unsafe)** in sequence. Google Chrome is used here as an example.

Tip

ProFi Software Controller supports HTTPS login. When you access its web UI, a prompt message indicating that the web address is not secure, for example, “Your connection is not private”, may appear. Ignore the message and go on to visit the webpage.



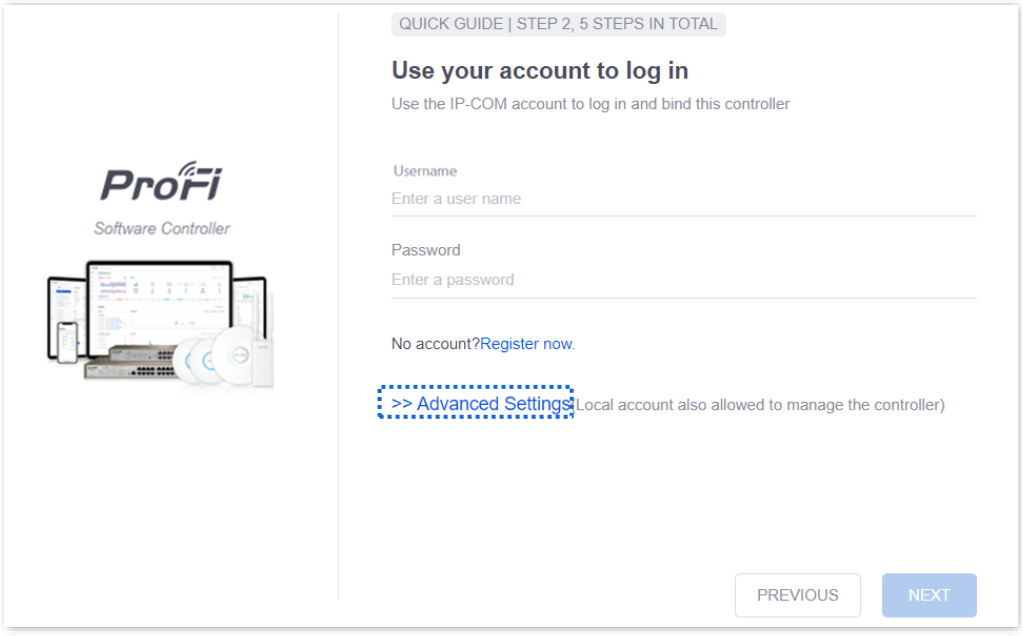
3. Customize a Controller name as needed, select **Tick here to indicate that you have read and agreed the End User License Agreement and Terms of Service**, and click **NEXT**.



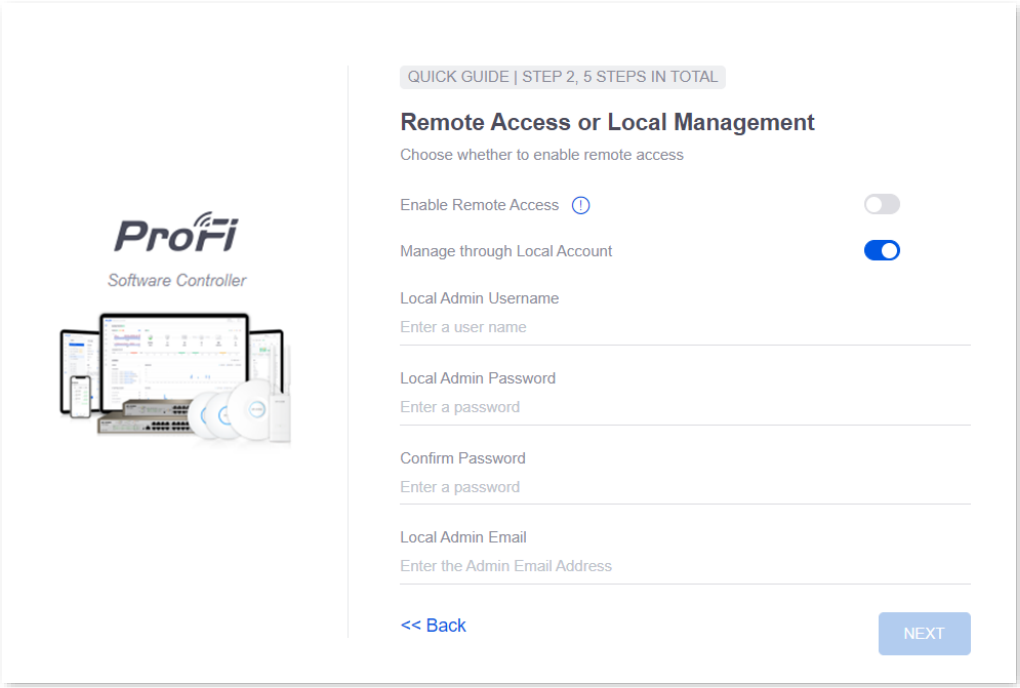
Tip

Alternatively, you can click **Restore from backup** to use a file that contains your previous settings to directly go to the login page of ProFi Software Controller.

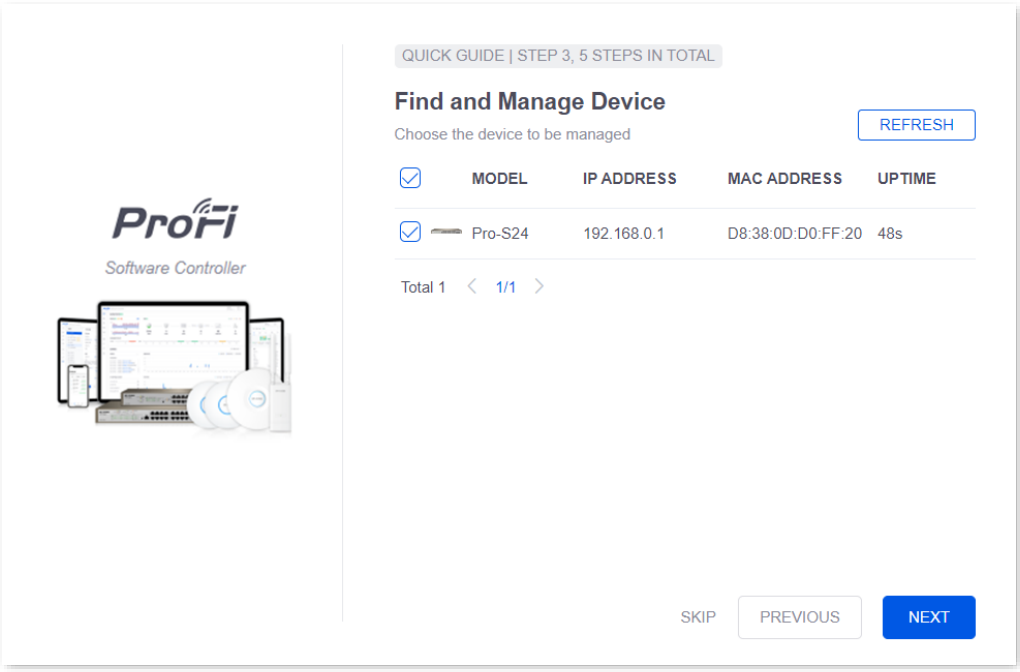
4. Click **Advanced Settings**.



5. Toggle off **Enable Remote Access** and toggle on **Manage through Local Account**, register an account, and click **NEXT**.



6. Wait until the ProFi series APs and switches are displayed in the device list, select the APs and switches you wish to adopt and click **NEXT**.

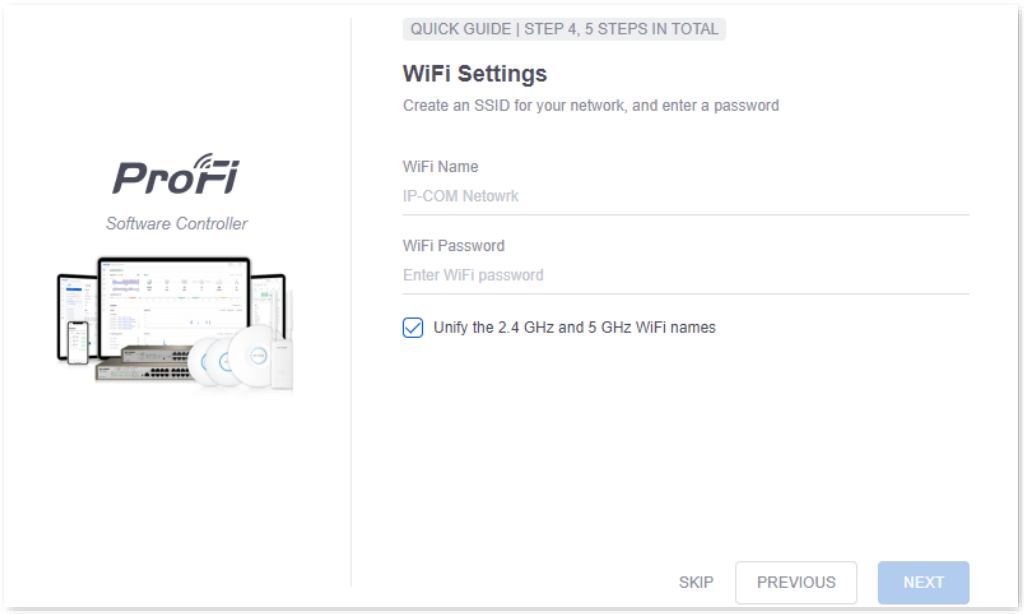


Tip

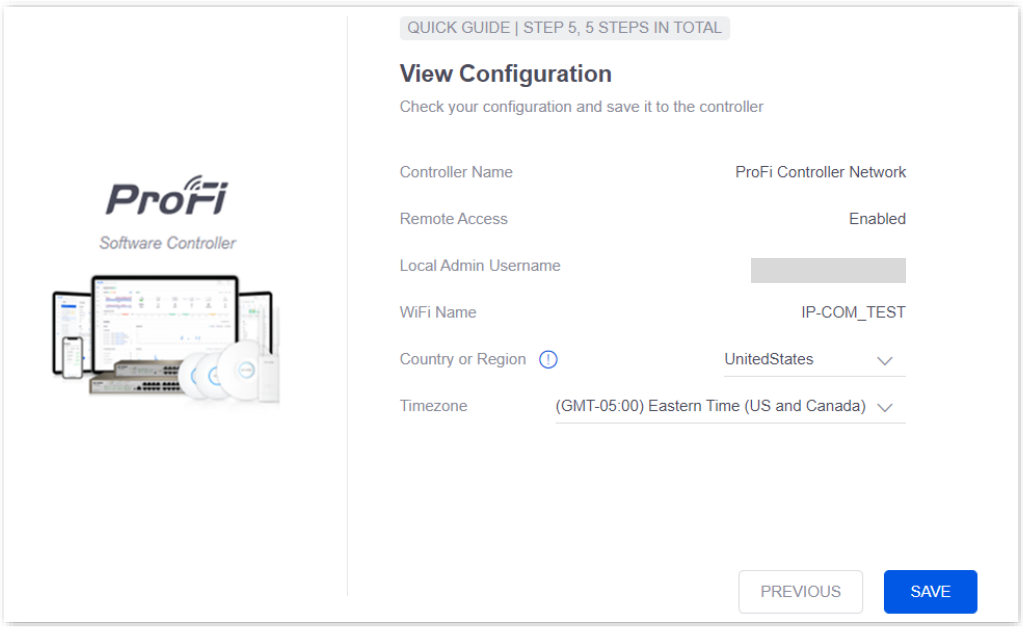
If your devices do not appear in the list, try the following solutions:

- Verify that the IP address of your management computer and IP addresses of your APs and switches are in the same network segment. For example, if the IP address of your AP is **192.168.0.254**, then the IP address of your management computer should be **192.168.0.*X*** (*X* ranges from 2 to 253 and is not occupied).
- Verify that your APs and switches are in factory settings.

7. Set **WiFi Name** and **WiFi Password** for the primary WiFi network of the AP and click **NEXT**.



8. Check your configurations, select **Country or Region** and **Timezone** and click **SAVE**.



----End

If you logged in using a local account for the first time but still want to remotely manage the controller, please refer to **Scenario B: You have logged in using a local account**.

1.6 Remote Access

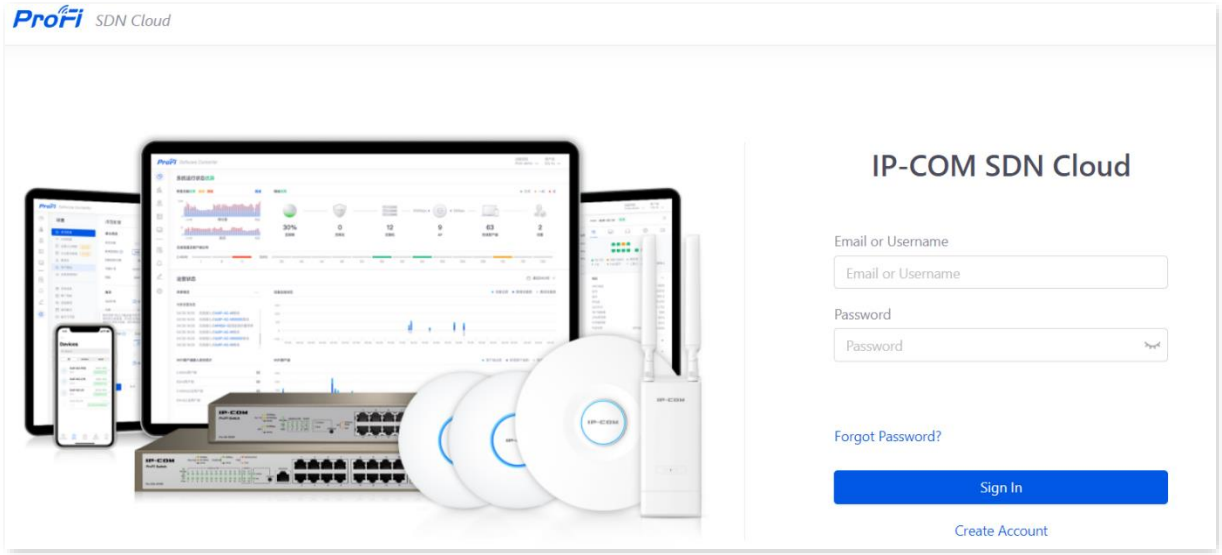
Only through a ProFi SDN Cloud account can you remotely manage your ProFi Software Controllers. If you do not have a cloud account, register one at sdn.ip-com.com.cn

Scenario A: You have logged in using a ProFi SDN Cloud account

To achieve remote access:

On a computer connected to the internet, visit sdn.ip-com.com.cn and log in to ProFi SDN Cloud using your cloud account.

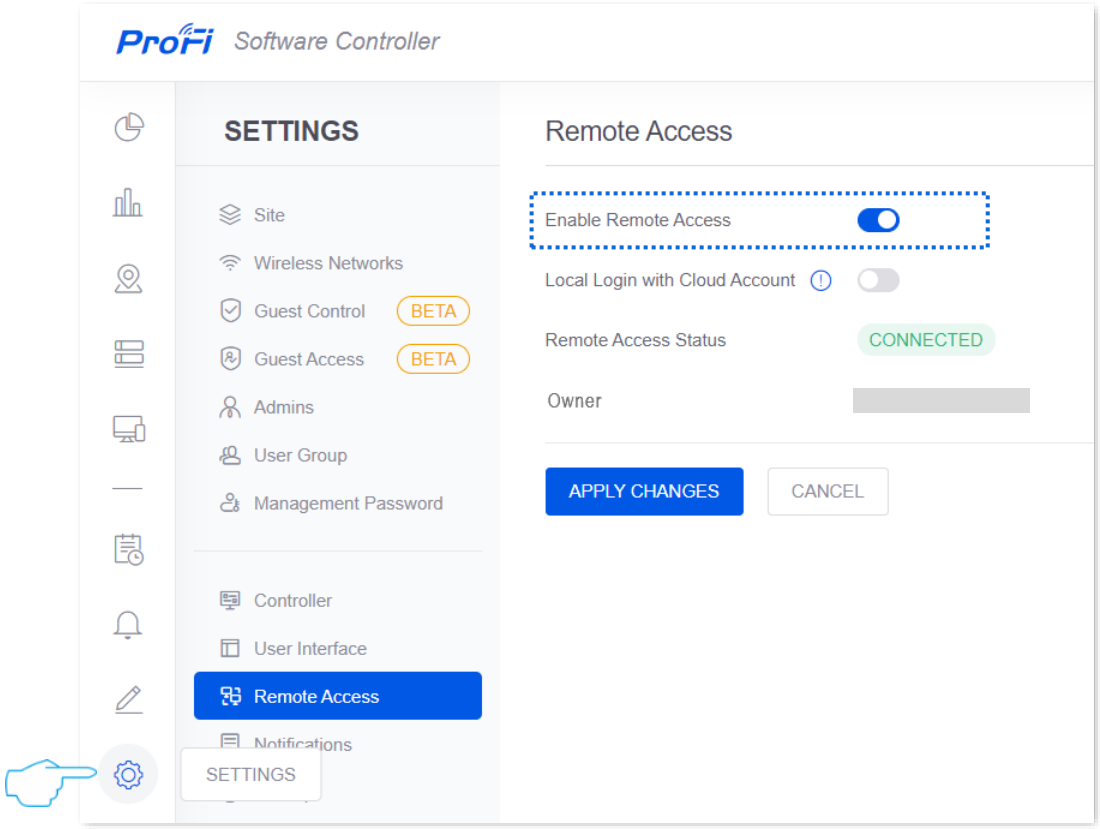
Then, you can remotely manage all the ProFi Software Controllers under this ProFi SDN Cloud account.



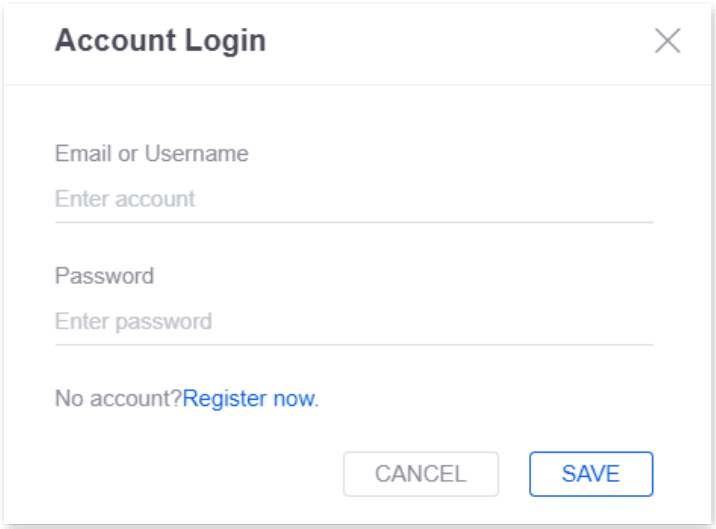
Scenario B: You have logged in using a local account

To achieve remote access:

1. On a computer (with ProFi Software Controller installed and configured for the first login) connected to the internet, go to **SETTINGS** (⚙) > **Remote Access**, and toggle on **Enable Remote Access**.



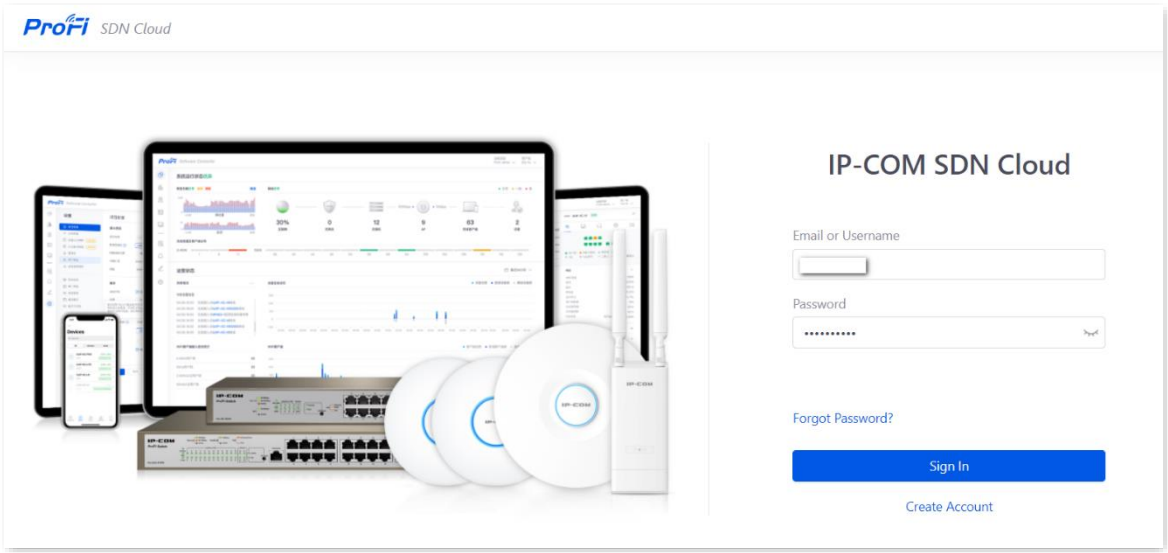
2. Enter the ProFi SDN Cloud account and password, and click **SAVE.**



Tip

- Ensure that the computer installed with the Controller is connected to the internet; otherwise, the **Remote Access** function cannot be enabled successfully.
- When you togged on **Enable Remote Access**, the **Local Login with Cloud Account** will also be automatically enabled to replace the local account with cloud account. The **Local Login with Cloud Account** function takes effect only when the email addresses reserved for the local account and the cloud account are the same.

3. On a computer connected to the internet, visit sdn.ip-com.com.cn and log in to ProFi SDN Cloud using your cloud account.



----End

You can remotely manage all the ProFi Software Controllers under this ProFi SDN Cloud account.

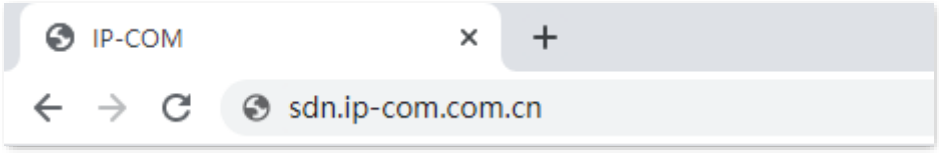
2 IP-COM Cloud Network

After the remote access, you can remotely manage all the software controllers through the ProFi SDN Cloud sdn.ip-com.com.cn.

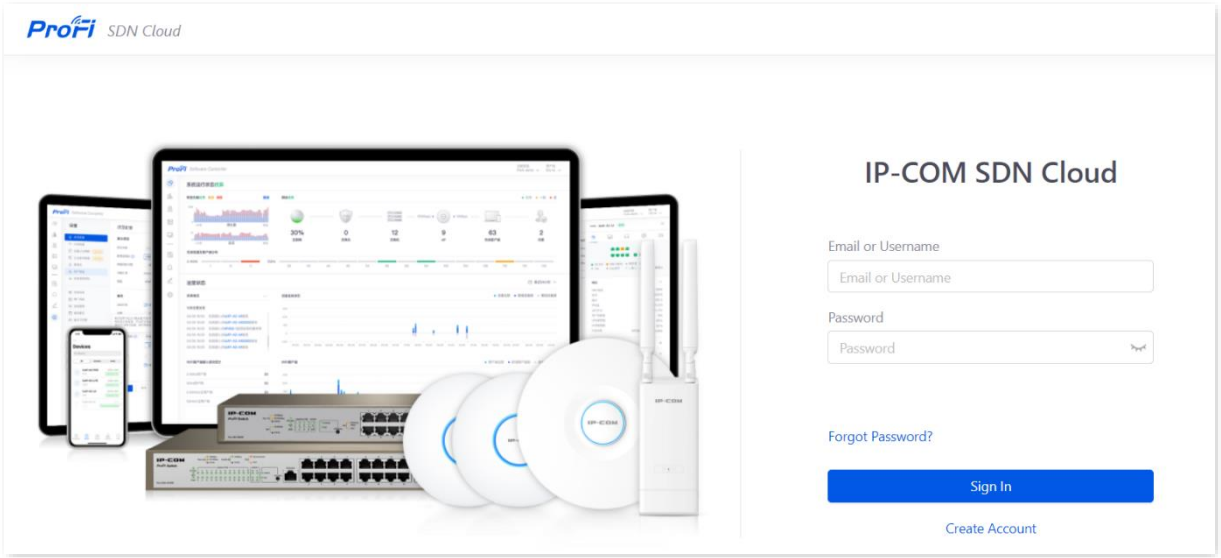
You must be a super administrator for initial cloud management. Once a super administrator enabled cloud access, then other administrators can enable cloud access as well.

2.1 Login

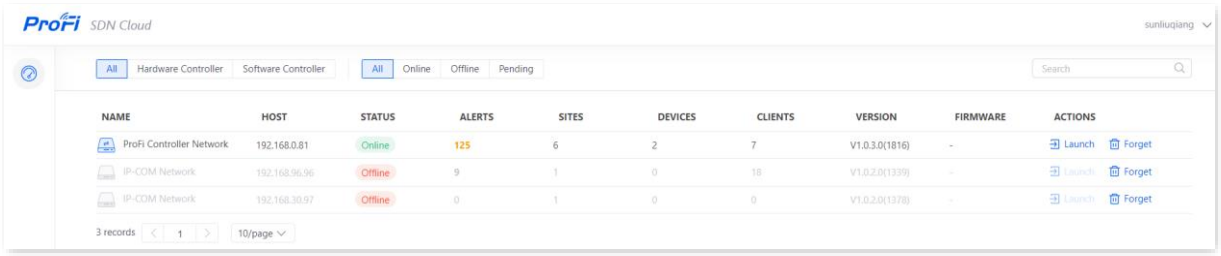
Launch a web browser and visit sdn.ip-com.com.cn



Enter your **Email or Username** and **Password**, and click **Sign In**.



A list of ProFi Software Controllers appears.



You can apply one of the following primary filters:

- **All**: displays all controllers.
- **Hardware Controller**: displays only Hardware Controllers.
- **Software Controller**: displays only ProFi Software Controllers.

You can also apply one of the following secondary filters:

- **All**: displays all controllers.
- **Online**: displays all online controllers.
- **Offline**: displays all offline controllers.
- **Pending**: displays all pending controllers waiting for approval.

Window elements description

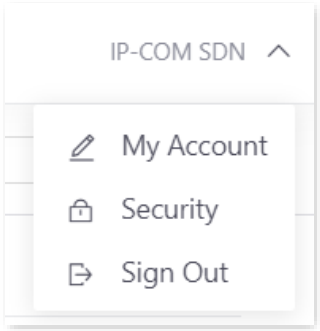
Element	Description
Search	Enter the text you want to search for in the search box and click . You can click any column headers to change the list order.
NAME	It specifies the name of the controller. You can click anywhere on the row where the target controller resides to get its additional details at the right side of the screen.
HOST	It specifies the IP address of the controller.
STATUS	It specifies the status of the controller.
ALERTS	It specifies the number of alerts for the controller.
SITES	It specifies the total number of sites under the controller.
DEVICES	It specifies all ProFi series of devices in the LAN automatically detected by the controller.
CLIENTS	It specifies the total number of online clients under the controller.
VERSION	It specifies the software version number of the ProFi Software Controller.
FIRMWARE	It specifies the firmware version number of the Hardware Controller.
ACTIONS	It specifies the actions you can perform on the controller. – **Launch**: Click it to remotely access the controller. – **Forget**: Click it to remove the controller from your ProFi SDN Cloud account.

2.2 Admin

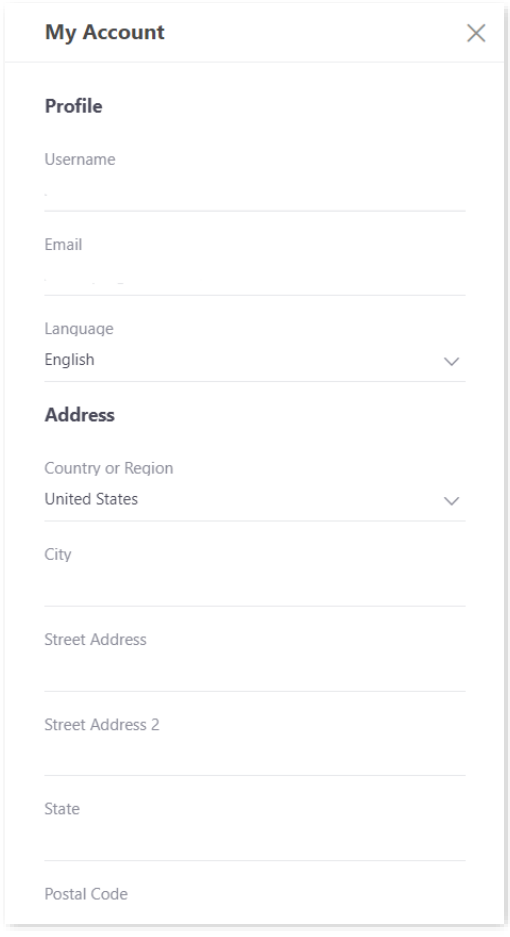
In the top right corner of the screen, click your account to display the options:

- **My Account**
- **Security**
- **Sign Out**

My Account



Click **My Account** to change your profile details such as page language and controller location. See the following figure.

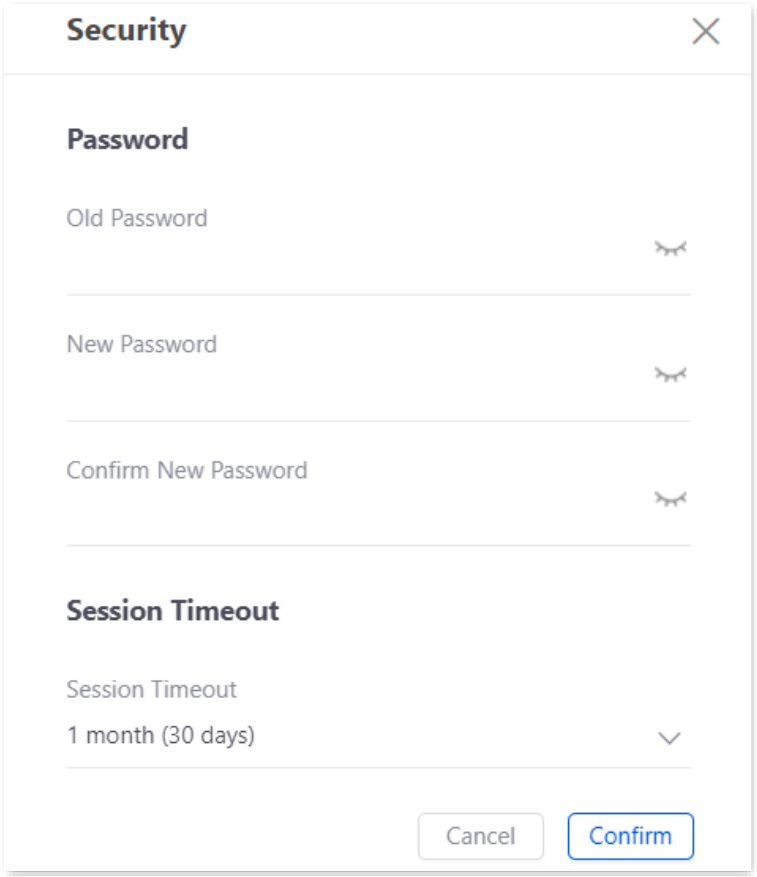


Parameter description

Parameter	Description
Profile	It specifies the basic settings of your account. – **Username**: It specifies your login username. – **Email**: It specifies the email address of your ProFi SDN Cloud account. – **Language**: The default language is English.
Address	It specifies your detailed address information. – **Country or Region**: It specifies the country or region you reside in. – **City**: It specifies the city you reside in. – **Street Address**: It specifies the address of the street you reside on. – **Street Address 2**: It specifies the address of the other street you may reside on. – **State**: It specifies the state you reside in. – **Postal Code**: It specifies the postal code of your region.

Security

Click **Security** to change your account password and change the duration of your session. See the following figure.



Parameter description

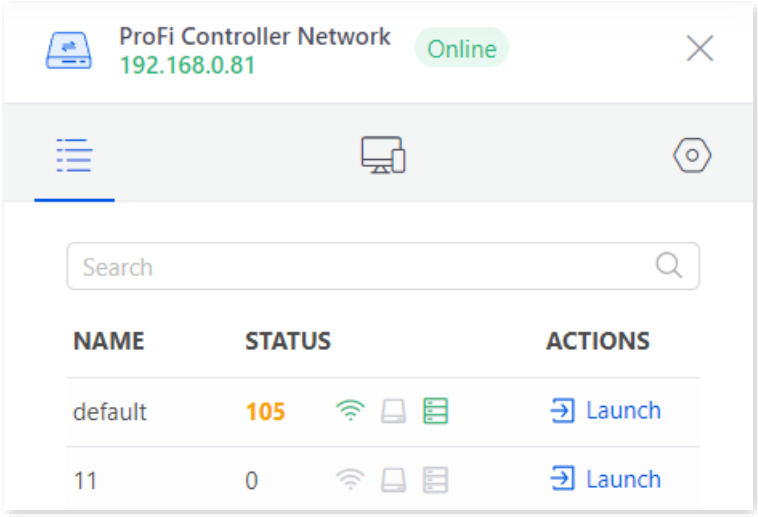
Parameter	Description
Password	It is used to change your account password. – **Old Password**: It specifies the current account password. – **New Password**: It specifies the new account password, which should be 8 to 32 ASCII characters. – **Confirm New Password**: Enter the new account password again.
Session Timeout	It specifies the duration of your ProFi SDN Cloud session. If this duration is exceeded, you will be automatically logged out for security purposes.

Sign Out

Click **Sign Out** to manually sign out of the ProFi SDN Cloud account.

2.3 Additional Details

On the homepage of the ProFi SDN Cloud, click a ProFi Software Controller to display more information on the right side of the screen.

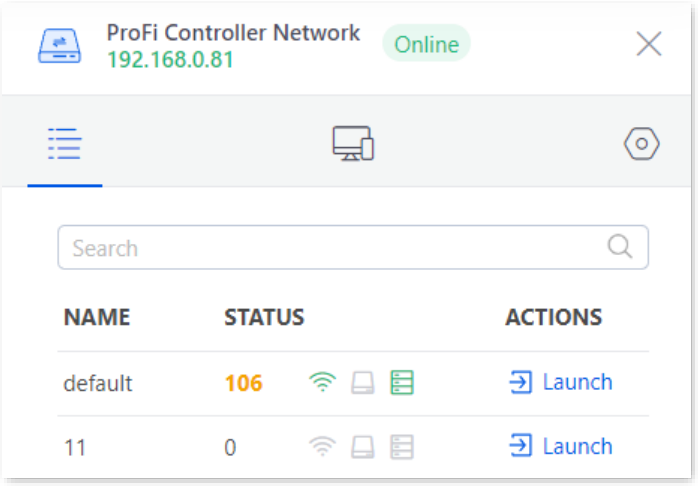


Window elements description

Element	Description
	It specifies the status of the ProFi Software Controller. Blue indicates that the controller is online and gray indicates that the controller is offline. : The ProFi Software Controller is online. : The ProFi Software Controller is offline.
(Controller name)	It specifies the name of the ProFi Software Controller.
(IP address)	It specifies the host IP address of the ProFi Software Controller.

Site Overview

This module displays all the sites under the ProFi Software Controller, and allows you to remotely access the Controller.

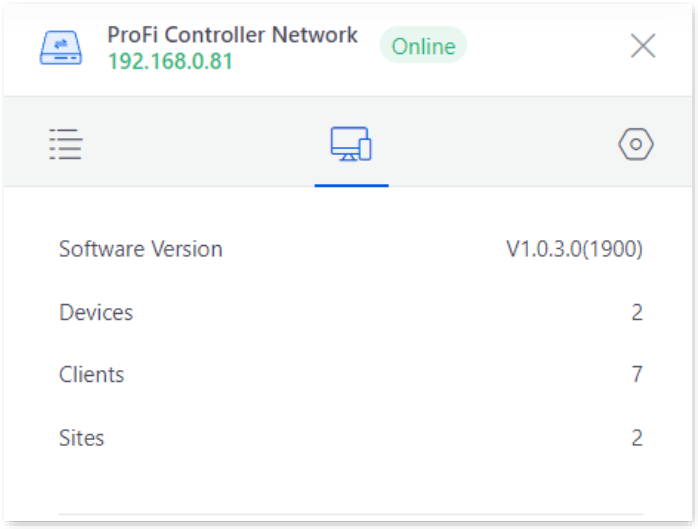


Parameter description

Parameter	Description
Search	Enter the text you want to search for in the search box and click .
NAME	It specifies the names of sites under the controller. Tip You can click the **NAME** column header to change the list order.
STATUS	It specifies the number of unread alerts and the statuses of ProFi series devices. – 106 : It specifies the number of unread alerts. – , , : It specifies the status of each network node, which are AP, gateway, and switch respectively. The status is indicated by color. • Green: indicates all devices in the site are online. • Red: indicates all devices in the site are offline. • Yellow: indicates some devices in the site are offline. • Gray: indicates there are no devices available in the site.
ACTIONS	Click **Launch** to remotely access the ProFi Software Controller.

Details

This module displays some detailed statistics of the ProFi Software Controller.

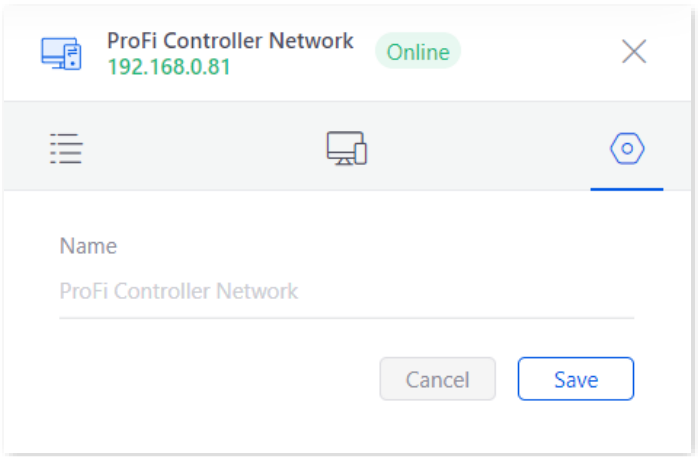


Parameter description

Parameter	Description
Software Version	It specifies the software version number of the ProFi Software Controller.
Devices	It specifies all ProFi series of devices in the LAN automatically detected by the ProFi Software Controller.
Clients	It specifies the total number of online clients under the ProFi Software Controller.
Sites	It specifies the total number of sites under the ProFi Software Controller.

Configuration

This module enables you to modify the name of a ProFi Software Controller, so as to help you quickly locate the controller from multiple controllers.

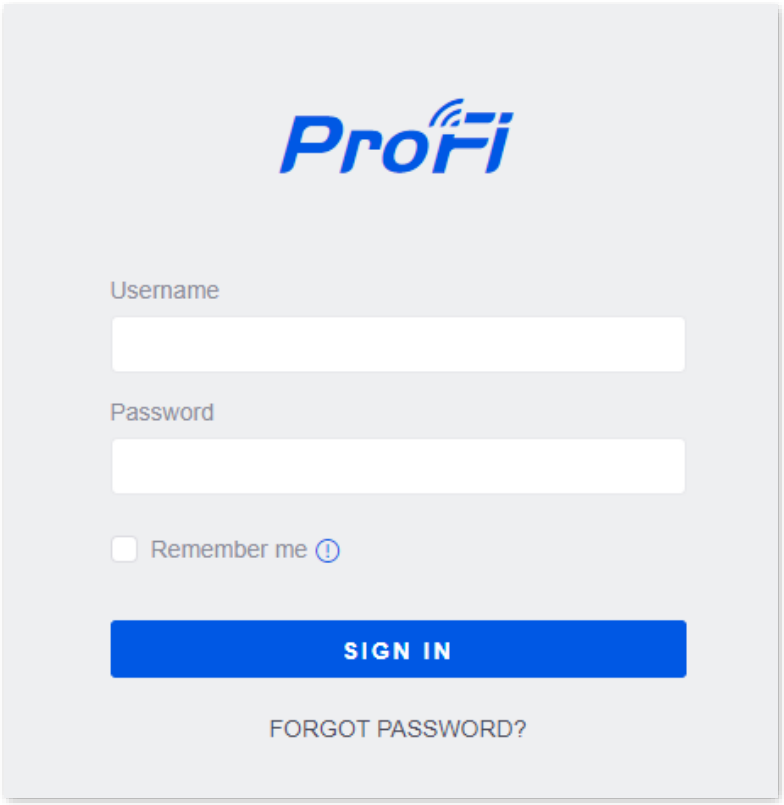


3 Use the ProFi Software Controller

The ProFi Software Controller allows you to manage your ProFi series of devices using a web browser.

To access the page, perform the following steps:

1. Launch the ProFi Software Controller application.
2. Enter the username and password and click **SIGN IN**.



----End

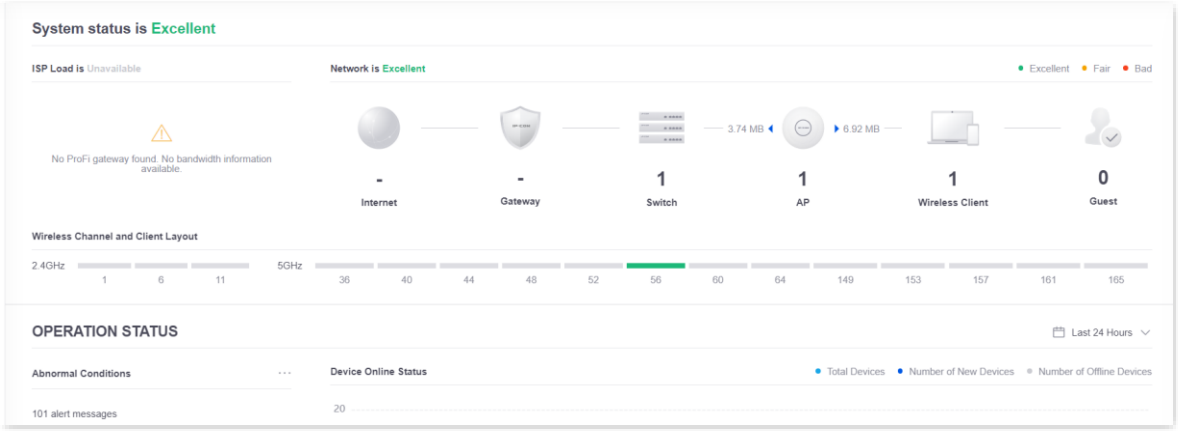
3.1 Navigation Bar

The ProFi Software Controller consists of seven primary themes. This User Guide elaborates on each theme with a chapter. For details on a specific theme, refer to the target chapter:

- 4 Dashboard
- 5 Statistics
- 6 Map
- 7 Devices
- 8 Switch Details
- 9 AP Details
- 10 Client Details

3.2 Common Interface Options

The common interface options are accessible from all tabs in the ProFi Software Controller interface.



3.2.1 Current Site

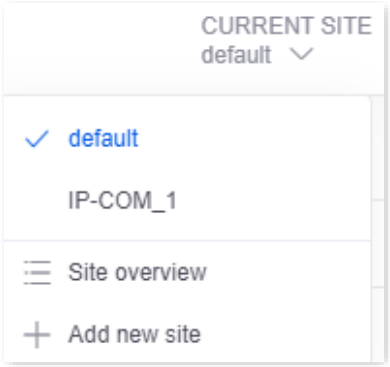
The ProFi Software Controller can manage multiple networks, which are called sites. Each site has its own configurations, maps, statistics, guest portals, and site administrator accounts. These sites are logically separated, and the initial site is called **default**.

Unless you manually switched sites, all the statistics displayed belong to the current site.

To view available sites or create a new site, click **CURRENT SITE** to display the options:

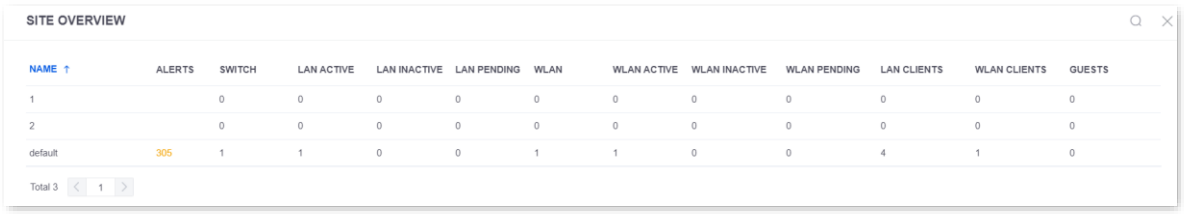
- Site Overview
- Add New Site

See the following figure.



Site Overview

To view the list of available sites, choose **CURRENT SITE** > **Site overview**. See the following figure.

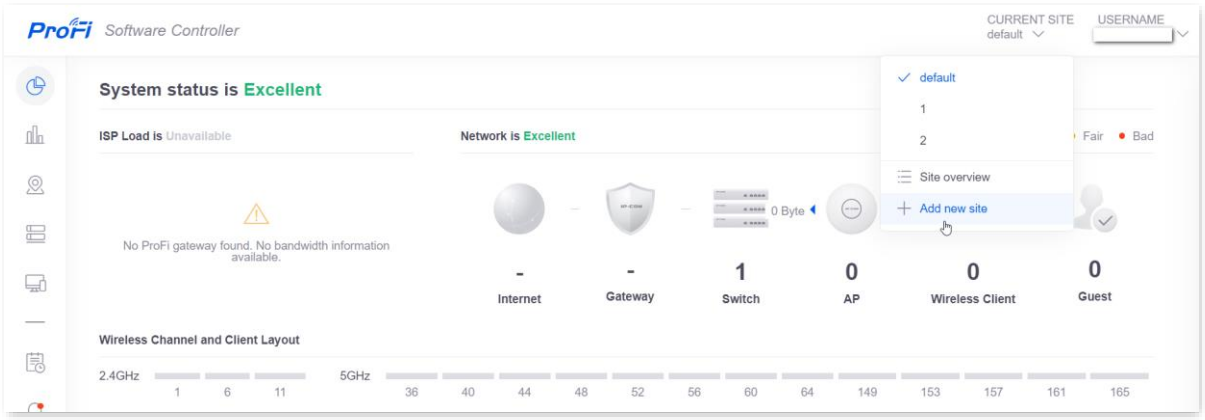


Parameter description

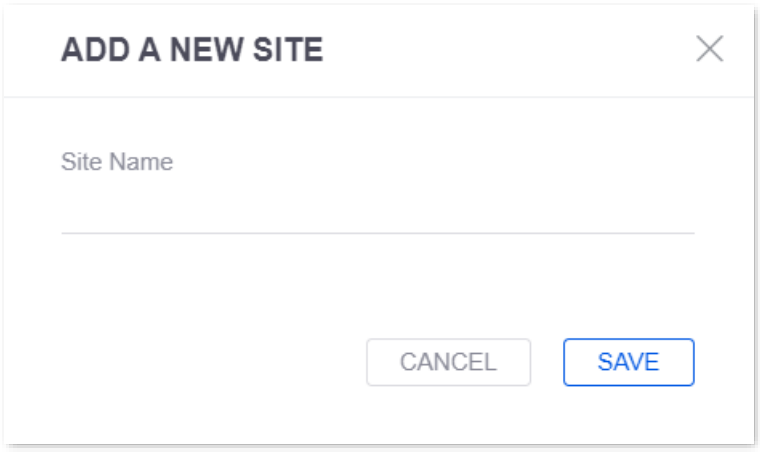
Parameter	Description
	Enter key words to filter the site information you want to view.
NAME	It specifies the name of the site. Click the name of the target site to enter it.
ALERTS	It specifies the number of unread alerts.
SWITCH	It specifies the total number of switches under the site.
LAN ACTIVE	It specifies the number of online switches under the site.
LAN INACTIVE	It specifies the number of offline switches under the site.
LAN PENDING	It specifies the number of switches waiting to be adopted by the site.
WLAN	It specifies the total number of APs under the site.
WLAN ACTIVE	It specifies the number of online APs under the site.
WLAN INACTIVE	It specifies the number of offline APs under the site.
WLAN PENDING	It specifies the number of APs waiting to be adopted by the site.
LAN CLIENTS	It specifies the number of wired clients under the site.
WLAN CLIENTS	It specifies the number of wireless clients (including guest wireless clients) under the site.
GUESTS	It specifies the number of guest wireless clients under the site.

Add New Site

1. Enter the management web UI of the ProFi Software Controller, choose **CURRENT SITE** > **Add new site**.



2. Set a **Site Name**, and click **SAVE**.



----End

After a new site is added, the page will be redirected to the new site.

3.2.2 Username

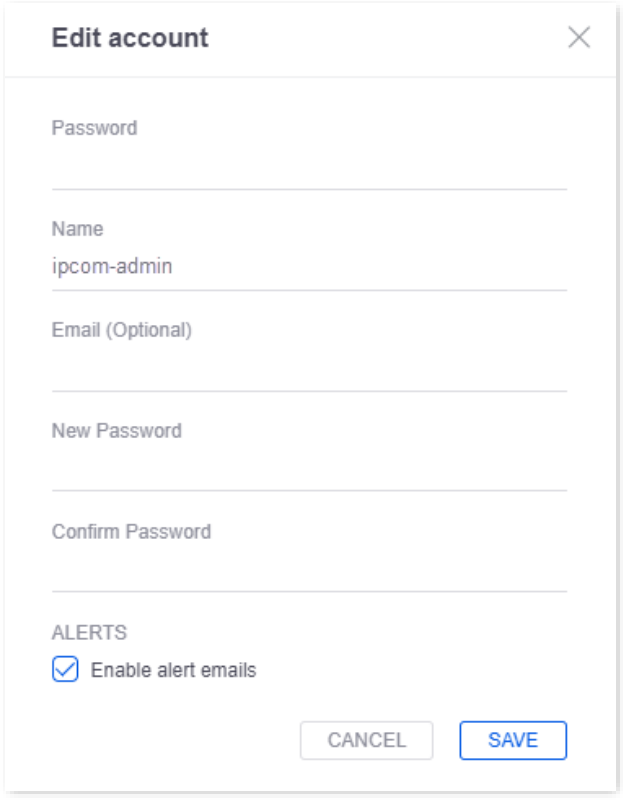
In the upper right corner of the screen, click **USERNAME** to display the options:

- **Edit Account**
- **Logout**

See the following figure.

Edit Account

To change the login username and password, choose **USER NAME** > **Edit account**. See the following figure.



Parameter description

Parameter	Description
Password	Enter the current password of your login account.
Name	It specifies the name of your login account and it cannot be edited.
Email (Optional)	It specifies the email address of the login account. It is optional and you can edit it as required.
New Password	Enter the new password for the login account.
Confirm Password	Enter the new password again.
Enable alert emails	Check it to enable email notifications.
SAVE	Click it to save the made changes.
CANCEL	Click it to discard the made changes.

If you changed any items on this page (parameter **Name** is not editable), you need to use the changed account information to log in to the ProFi Software Controller.

If it is the ProFi SDN Cloud account you changed, you need to disable and enable the **Remote Access** function on the **Remote Access** page to re-apply the function. The detailed procedure is as follows:

1. Log in using the changed account, go to **SETTINGS** ( ) > **Remote Access**, toggle off **Enable Remote Access** and **Local Login with Cloud Account**, and click **APPLY CHANGES**.

Note

If you logged in to the ProFi Software Controller by launching from the ProFi SDN Cloud, start the ProFi Software Controller locally and log in using the changed account. Go to **SETTINGS** ( ) > **Remote Access**.

2. Toggle on **Enable Remote Access** and **Local Login with Cloud Account**, and click **APPLY CHANGES**.

----End

You can log in to the ProFi Software Controller using the changed ProFi SDN Cloud account.

Note

Modifications to the **Enable alert emails** check box will not be overwritten.

Logout

To manually log out of the ProFi Software Controller, choose **USERNAME** > **Logout**.

3.2.3 Properties

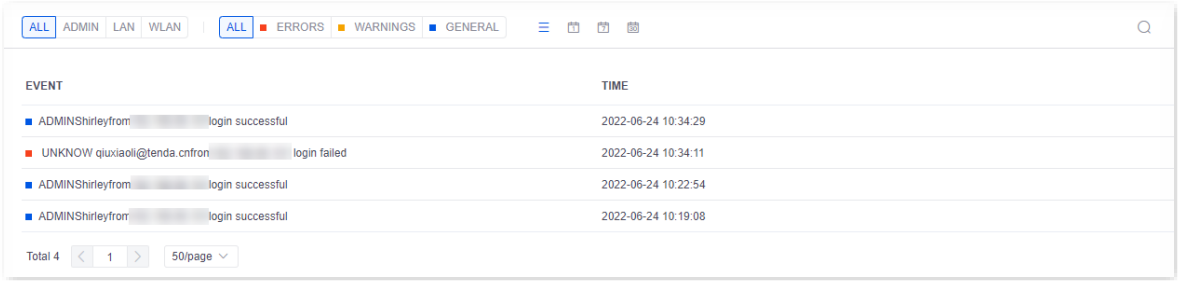
The **Properties** panel is hidden by default. To display it, select a device.

Information about each selected device appears as a popup within the panel. The displayed information varies depending on the device type. For more information, see the target chapter:

- Switch Details
- AP Details
- Client Details

3.2.4 Events

The Events page displays a list of recent events, along with the corresponding MAC addresses, messages, dates and time. See the following figure.



To enter the page, choose **EVENTS** ( ).

Window elements description

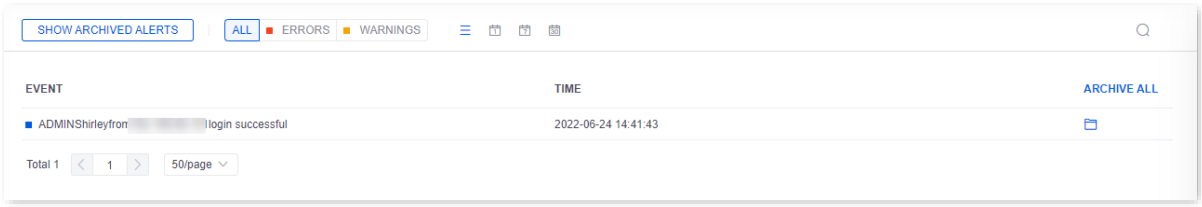
Element	Symbol	Description
Filter by object	ALL	Displays all the events.
	ADMIN	Displays only the events of the administrator.
	LAN	Displays only the events for the wired networks.
	WLAN	Displays only the events for the wireless networks.
Filter by type	ALL	Displays all the events that you select on the Notifications page.
	ERRORS	Displays only the error-level events.
	WARNINGS	Displays only the warning-level events.
	GENERAL	Displays only the general-level events.
Filter by period		Displays events in last 180 days.
		Displays events in last 1 day.

Element	Symbol	Description
		Displays events in last 7 days.
		Displays events in last 30 days.
Search		Click it and enter the text you want to search for in the search box. The searching starts immediately when you enter keywords.

3.2.5 Alerts

When there is a new alert, a red dot appears on the alert icon.

The Alerts page displays a list of important events, along with the corresponding MAC addresses, messages, dates and time. See the following figure.



To enter the page, choose **ALERTS** ( ).

Window elements description

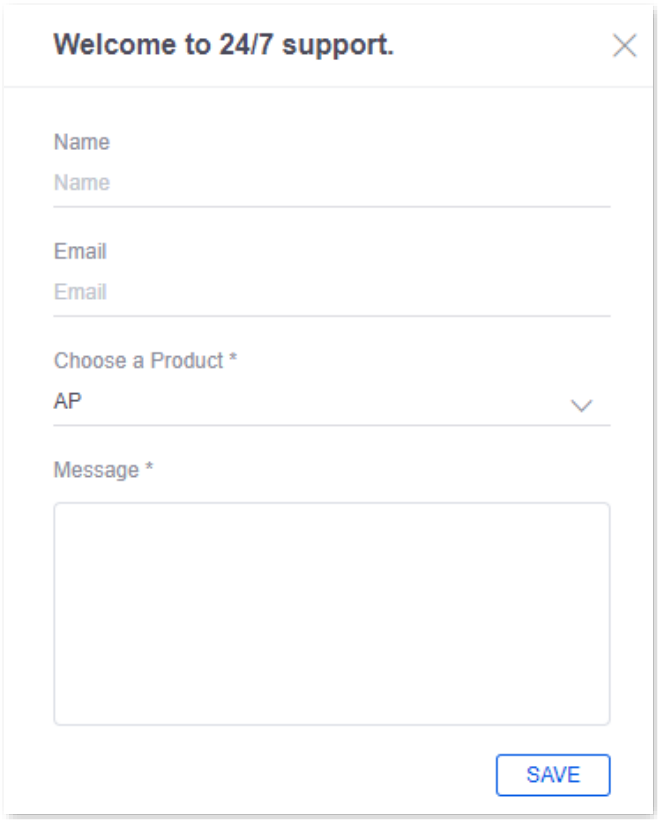
Element	Symbol	Description
Show archived alerts	SHOW ARCHIVED ALERTS	Click it to display only the archived alert messages.
Filter by type	ALL	Displays all the alerts that you select on the Notifications page.
	ERRORS	Displays only the error-level alerts.
	WARNINGS	Displays only the warning-level alerts.
Filter by period		Displays alerts in last 180 days.
		Displays alerts in last 1 day.
		Displays alerts in last 7 days.
		Displays alerts in last 30 days.
Search		Click it and enter the text you want to search for in the search box. The searching starts immediately when you enter keywords.
Archive all	ARCHIVE ALL	Click it to archive all the alert messages to the archived alert list. All the archived alerts are collected under the **Show archived alerts** header and deleted from the current alert list.

Element	Symbol	Description
Archive		Click it to archive a single alert message.

3.2.6 Help Center

This page is used to seek online support. Our support staff will handle your problems within 24 hours.

To enter the page, choose **HELP CENTER** ( ).

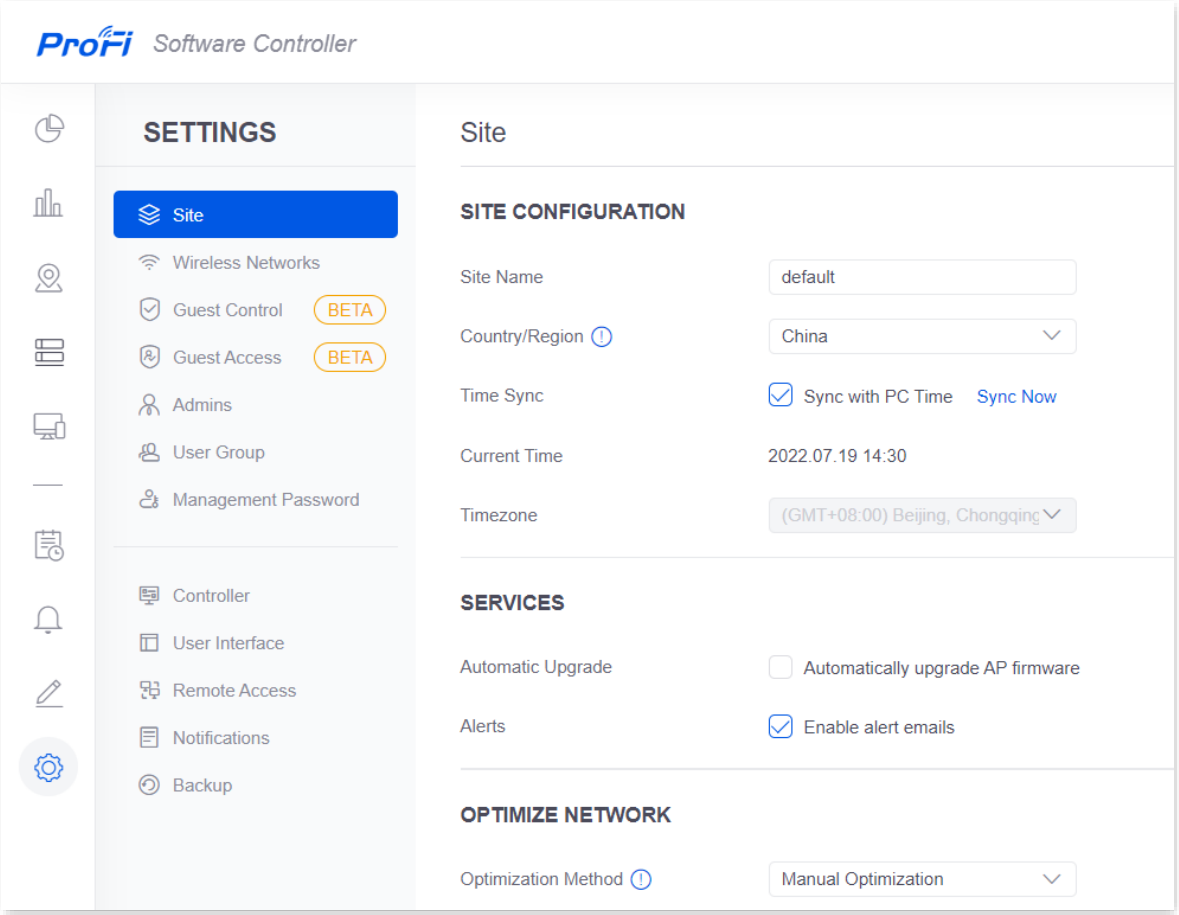


3.2.7 Settings

Site

This page is used to configure the site-specific settings. To switch sites, select a different site from the **CURRENT SITE** drop-down menu in the upper right corner.

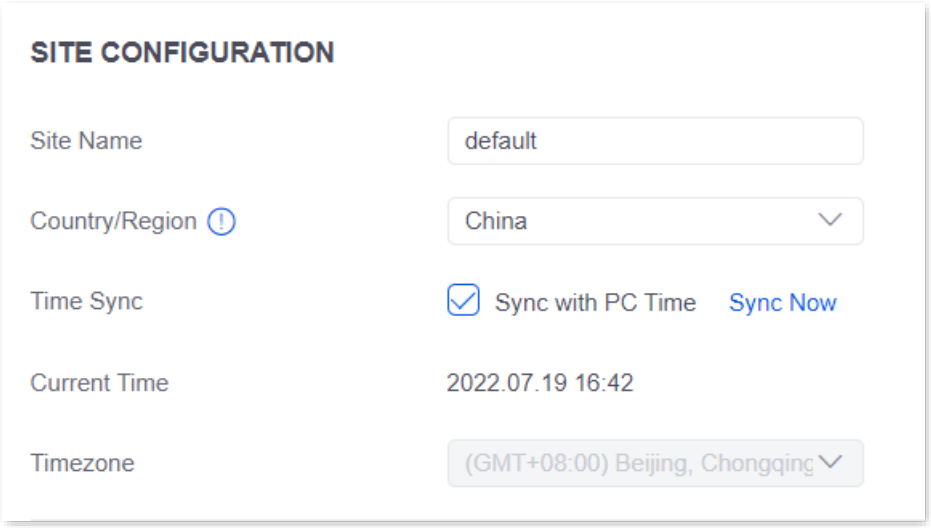
To enter the page, choose **SETTINGS** ( ) > **Site.**



Site Configuration

This module is used to configure some basic settings of the site.

To enter the module, choose **SETTINGS** ( ) > **Site**.



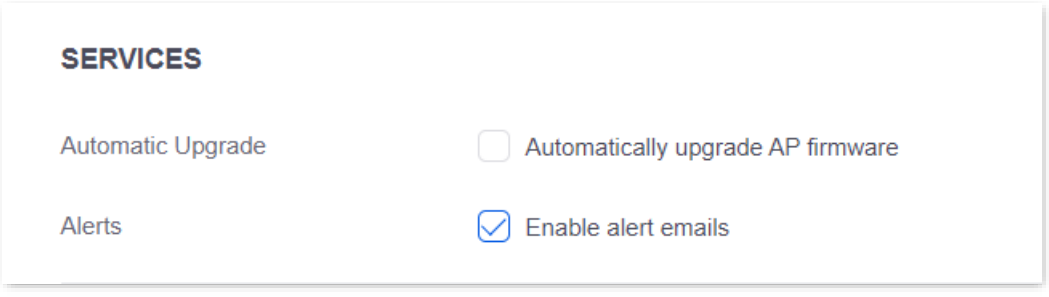
Parameter description

Parameter	Description
Site Name	It specifies the name of the site.
Country/Region	It specifies the country or region. You can select it as required.
Time Sync	It specifies whether the time is synchronized with the time on your PC. When **Sync with PC Time** is selected, **Current Time** and **Timezone** will be synchronized with the time settings on your PC. You can click **Sync Now** to synchronize the time immediately.
Current Time	It specifies the current time corresponding to the country/region or timezone you selected. It cannot be changed.
Timezone	It specifies the time zone and can be changed only when **Sync with PC Time** is deselected.

Services

This module is used to configure the automatic upgrade function and email alert function.

To enter the module, choose **SETTINGS** ( ) > **Site**.



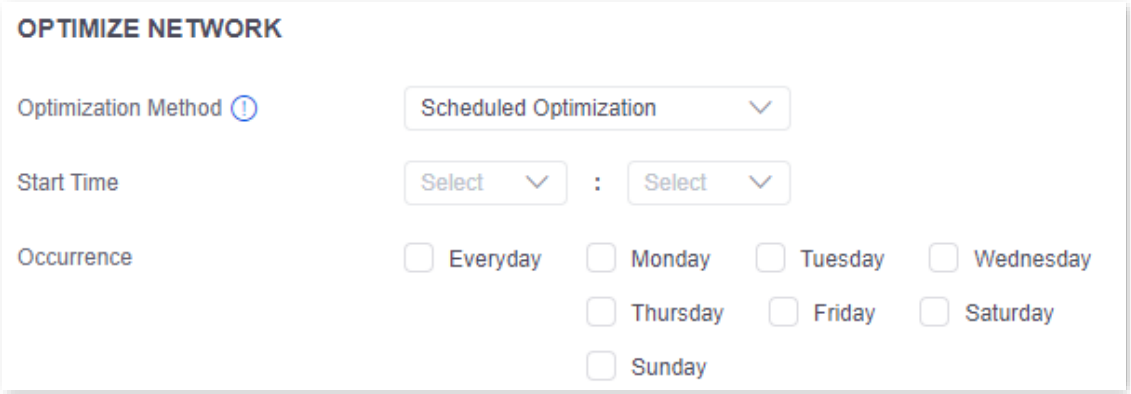
Parameter description

Parameter	Description
Automatic Upgrade	After this function is enabled, the ProFi Software Controller will automatically upgrade the firmware of your APs when a new firmware version is available.
Alerts	After this function is enabled, alert emails will be sent to the email addresses of the administrators.

Optimize Network

This module is used to configure RF optimization settings. Through RF optimization, the system automatically collects and analyzes the occupation status of wireless resources, and automatically adjusts the channel, power and other configurations of wireless devices.

To enter the module, choose **SETTINGS** ( ) > **Site**.



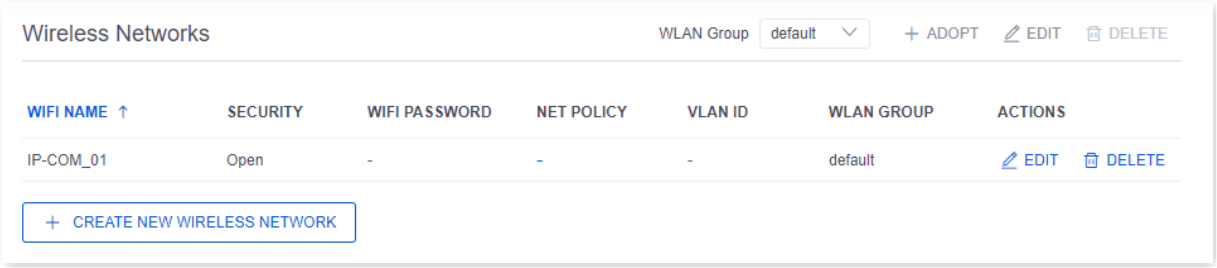
Parameter description

Parameter	Description
Optimization Method	It specifies the whether and how to optimize the network. – **Disabled**: The RF optimization function is disabled. – **Scheduled Optimization**: The ProFi Software Controller will optimize your networks at the **Start Time** and **Occurrence** you specified. – **Manual Optimization**: The system will be optimized after you click **OPTIMIZE**.
Start Time	It specifies the time at which the network is automatically optimized. It is required when **Optimization Method** is set to **Scheduled Optimization**.
Occurrence	It specifies the days on which the network is automatically optimized. It is required when **Optimization Method** is set to **Scheduled Optimization**.
OPTIMIZE	It appears when **Optimization Method** is set to **Manual Optimization**. Click it to optimize the network manually.

Wireless Networks

This page is used to create WLAN groups and add several wireless networks to the WLAN groups.

To enter the page, choose **SETTINGS** ( ) > **Wireless Networks**.



Parameter description

Parameter	Description
WLAN Group	Click the drop-down menu to select the target WLAN group. The **default** WLAN group is created by default. – Click ADOPT to add a new WLAN group. – Click EDIT to edit the current WLAN group. – Click DELETE to delete the current WLAN group. The **default** WLAN group cannot be deleted.
WIFI NAME	It specifies the wireless network name (SSID).
SECURITY	It specifies the encryption type of the wireless network, including Open, WEP, WPA-PSK, WPA2-PSK, WPA3-SAE and WPA3-SAE/WPA2-PSK.
WIFI PASSWORD	It specifies the password of the wireless network. **-** indicates that the wireless network is not encrypted.
NET POLICY	It specifies whether the guest network policy is enabled. ✓: Indicates that the guest network policy is enabled. After the guest network policy is enabled, the wireless users under this wireless network cannot communicate with each other and cannot access the intranet. –: Indicates that the guest network policy is disabled.
VLAN ID	It specifies the VLAN ID of the wireless network. **-** indicates that no VLAN is set for the wireless network.
ACTIONS	It specifies the actions you can perform on the wireless networks. – Click EDIT to edit the wireless network. – Click DELETE to delete the wireless network.
+ CREATE NEW WIRELESS NETWORK	Click it to add a new wireless network. You can add up to eight wireless networks for each WLAN group.

WLAN Group

WLAN groups are a way for the ProFi Software Controller to quickly create a configuration template for several wireless networks. It consists of one or more wireless networks, and each WLAN group has different wireless settings, including the number of wireless networks, names, encryption types, and the adoption of guest network policy or not.

Through the WLAN group, different wireless network policies can be quickly delivered to different ProFi APs.

Security Mode

A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection.

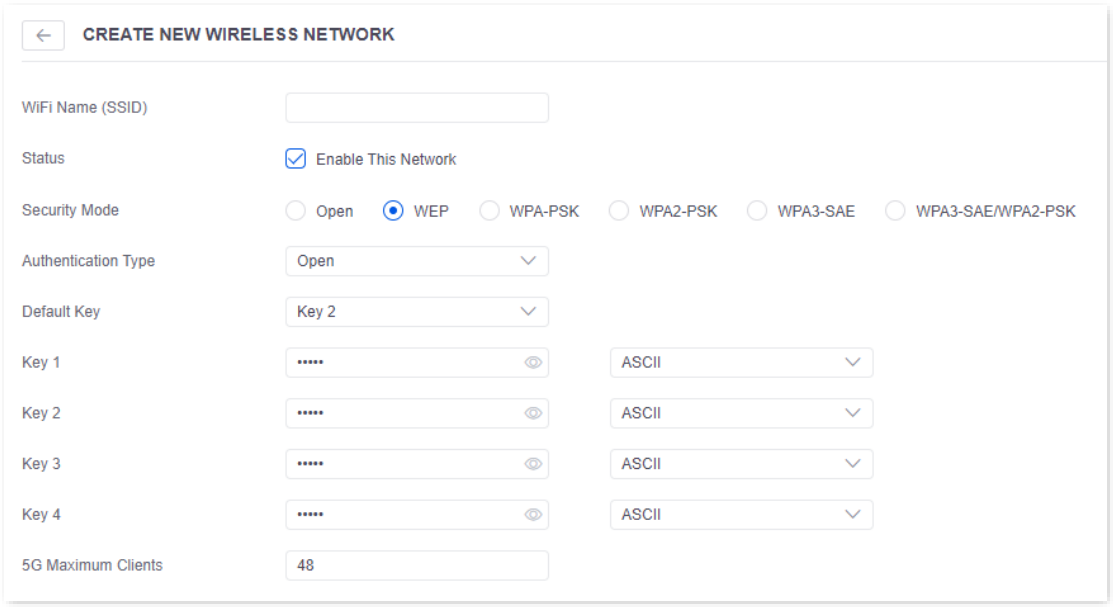
The ProFi Software Controller supports various security modes for network encryption, including **Open**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA3-SAE** and **WPA3-SAE/WPA2-PSK**. Choose a suitable one according to the actual scenario.

- **Open**

  It indicates that any wireless device can connect to the WiFi network. This option is not recommended because it leads to network insecurity.

- **WEP**

  It uses a static key to encrypt all exchanged data, and ensures that a WLAN has the same level of security as a wired LAN. However, data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum WiFi network throughput of only 54 Mbps. Therefore, this security mode is not recommended.

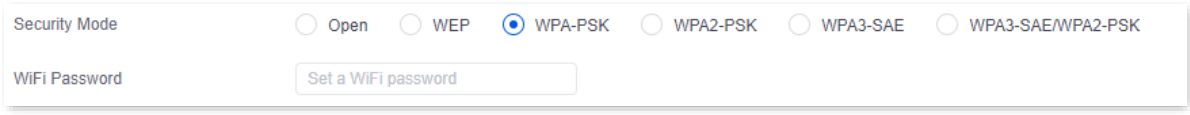


Parameter description

Parameter	Description
Authentication Type	It specifies the authentication type for the WEP security mode. The options include **Open** and **Shared**. The options share the same encryption process. – **Open**: It specifies that authentication is not required and data exchanged is encrypted with WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. – **Shared**: It specifies that a shared key is used for authentication and data exchanged is encrypted with WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	It specifies the WEP key for the current wireless network. For example, if **Default Key** is set to **Key 2**, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by **Key 2**.
Key 1/2/3/4	4 WEP keys are allowed at the same time, but only the one specified by the **Default Key** is valid. The key type includes ASCII and Hexadecimal. – **ASCII**: 5 or 13 ASCII characters are allowed in the key. – **Hex**: 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.

- **WPA-PSK, WPA2-PSK**

Both WPA-PSK and WPA2-PSK adopt a pre-shared key (PSK) for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes WPA-PSK and WPA2-PSK suitable for ensuring security of home wireless networks. Nevertheless, because the initial PSK for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes WPA-PSK and WPA2-PSK not suitable for scenarios where high security is required.

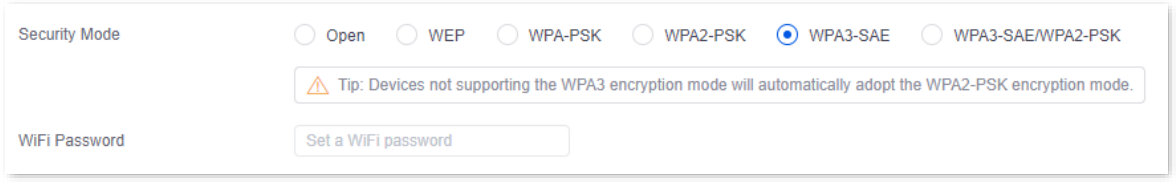


- **WPA3-SAE**

It is an upgraded version of WPA2-PSK. With Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), this security mode provides protection against dictionary attacks and information disclosure, saving you the trouble to set a complicated password.

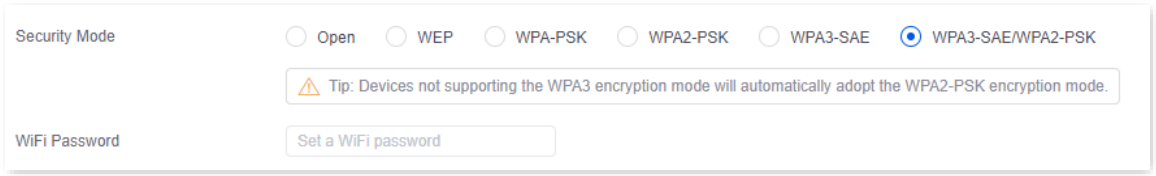
Tip

If your wireless clients do not support WPA3-SAE or the WiFi experience is unsatisfying, you are recommended to set the security mode to WPA2-PSK.



- **WPA3-SAE/WPA2-PSK**

The mixed encryption of WPA2-PSK/AES and WPA3-SAE/AES leads to better security for wireless networks.

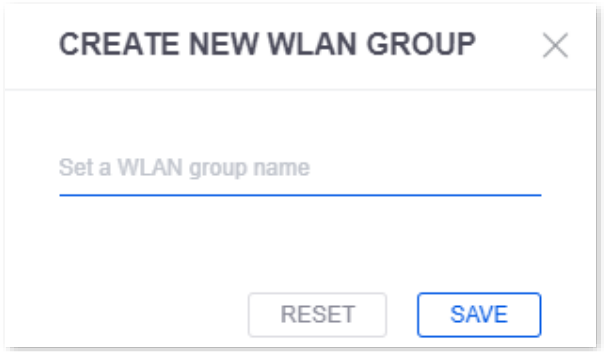


Create a WLAN Group

To create a new WLAN group, click + ADOPT in the upper right corner, set the WLAN group name and click **SAVE**. See the following figure.

Tip

- The WLAN group name should be 1 to 32 bytes in length and composed of uppercase or lowercase letters, digits, or underscores.
- To discard the made changes, click **RESET**.



Edit a WLAN Group

1. Select the WLAN group from the **WLAN Group** drop-down list.
2. Click EDIT in the upper right corner.

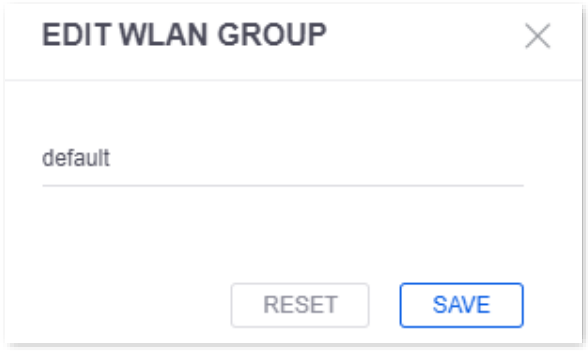
3. Modify the WLAN group name and click **SAVE**.

----End

See the following figure.

Tip

- The WLAN group name should be 1 to 32 bytes in length and composed of uppercase or lowercase letters, digits, or underscores.
- To discard the made changes, click **RESET**.

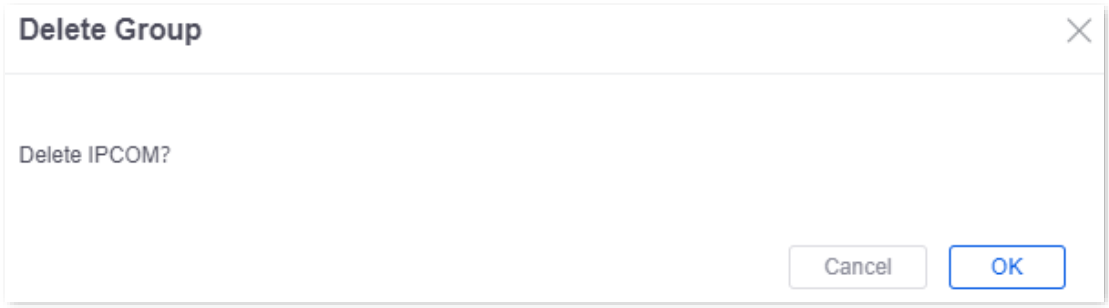


Delete a WLAN Group

1. Select the WLAN group from the **WLAN Group** drop-down list
2. Click DELETE in the upper right corner of the screen.
3. Click **OK** in the pop-up window.

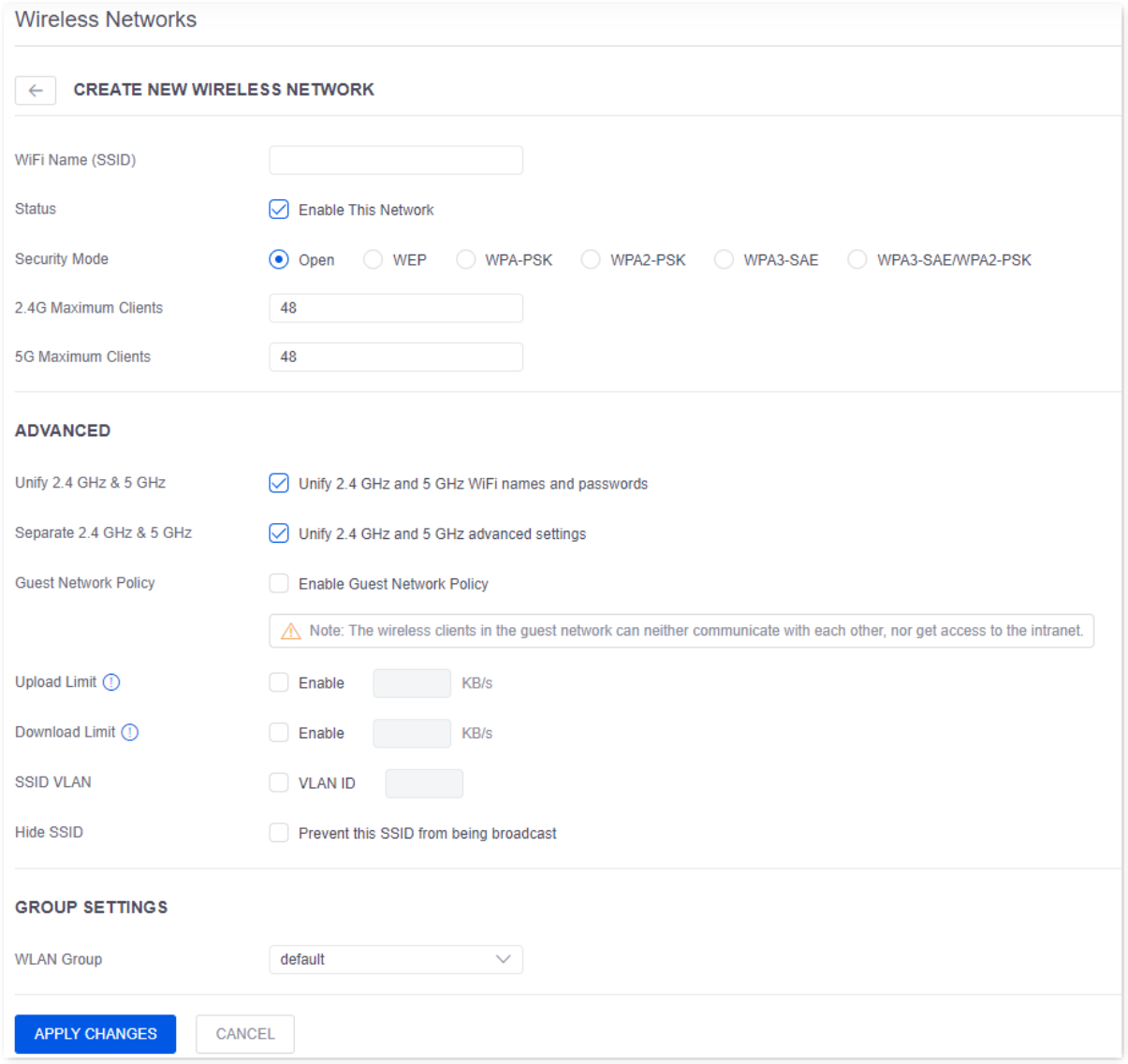
----End

See the following figure.



Create Wireless Network

To add a new wireless network, click **+ CREATE NEW WIRELESS NETWORK**. See the following figure.



Parameter description

Parameter	Description
WiFi Name (SSID)	It specifies the wireless network name (SSID).
Status	It specifies whether the wireless network is enabled. The wireless network is enabled by default, and you can deselect **Enable This Network** to disable it as required.
Security Mode	It specifies the encryption type of the wireless network. The encryption types include Open, WEP, WPA-PSK, WPA2-PSK, WPA3-SAE and WPA3-SAE/WPA2-PSK.
2.4G Maximum Clients	It specifies the maximum number of wireless clients that can be connected to the 2.4 GHz wireless network. Its range is 1 to 128.

Parameter	Description
5G Maximum Clients	It specifies the maximum number of wireless clients that can be connected to the 5 GHz wireless network. Its range is 1 to 128.
Unify 2.4 GHz & 5 GHz	It specifies whether the 2.4 GHz and 5 GHz wireless networks share the same SSID and password. It is enabled by default. When this function is enabled, WiFi-enabled clients connected to wireless network will use the frequency with better connection quality. If you have any wireless client that supports only the 2.4 GHz wireless network, it is recommended that this function be disabled to avoid network connection failure.
2.4G Status	It specifies whether the 2.4 GHz wireless network is enabled. It is enabled by default. It is required when **Unify 2.4 GHz and 5 GHz WiFi names and passwords** is deselected.
2.4G Suffix	It specifies the suffix of the 2.4 GHz wireless network. It is **_2.4G** by default. It is required when **Unify 2.4 GHz and 5 GHz WiFi names and passwords** is deselected.
Separate 2.4 GHz & 5GHz	It specifies whether the advanced settings of the 2.4 GHz and 5 GHz wireless networks are unified. It is enabled by default. When it is enabled, the settings for upload and download limits, VLAN ID, guest network policy and SSID hiding are similar for both 2.4 GHz and 5 GHz wireless networks.
Guest Network Policy	It specifies whether the guest network policy is enabled. It is disabled by default. After it is enabled, the wireless users under this wireless network cannot communicate with each other and cannot access the intranet.

Parameter	Description
Upload Limit Download Limit	They specify whether the upload and download limit functions are enabled. They are disabled by default (no limit on speed). You can enable any of them and set the maximum upload/download speed shared by all wireless clients in the 2.4 GHz and 5 GHz wireless networks. Tip These two parameters are available when **Unify 2.4 GHz and 5 GHz advanced settings** is selected. When **Unify 2.4 GHz and 5 GHz advanced settings** is deselected, **2.4G Upload Limit**, **5G Upload Limit**, **2.4G Download Limit** and 5**G Download Limit** are available and their settings are similar to these two parameters.
SSID VLAN	It specifies whether the VLAN function is enabled. It is disabled by default. After this function is enabled, IEEE 802.1q VLAN is applied. Enter the VLAN ID in the neighboring box. Tip This parameter is available when **Unify 2.4 GHz and 5 GHz advanced settings** is selected. When **Unify 2.4 GHz and 5 GHz advanced settings** is deselected, **2.4G SSID VLAN** and 5**G SSID VLAN** are available and their settings are similar to this parameter.
Hide SSID	It specifies whether the wireless network is hidden. After this function is enabled, this SSID will not be broadcast and will not appear in the available network list on such clients as smartphones, which enhances the security of the wireless network. If you want to connect to a hidden wireless network, manually enter the SSID of the wireless network on your devices.

Guest Control

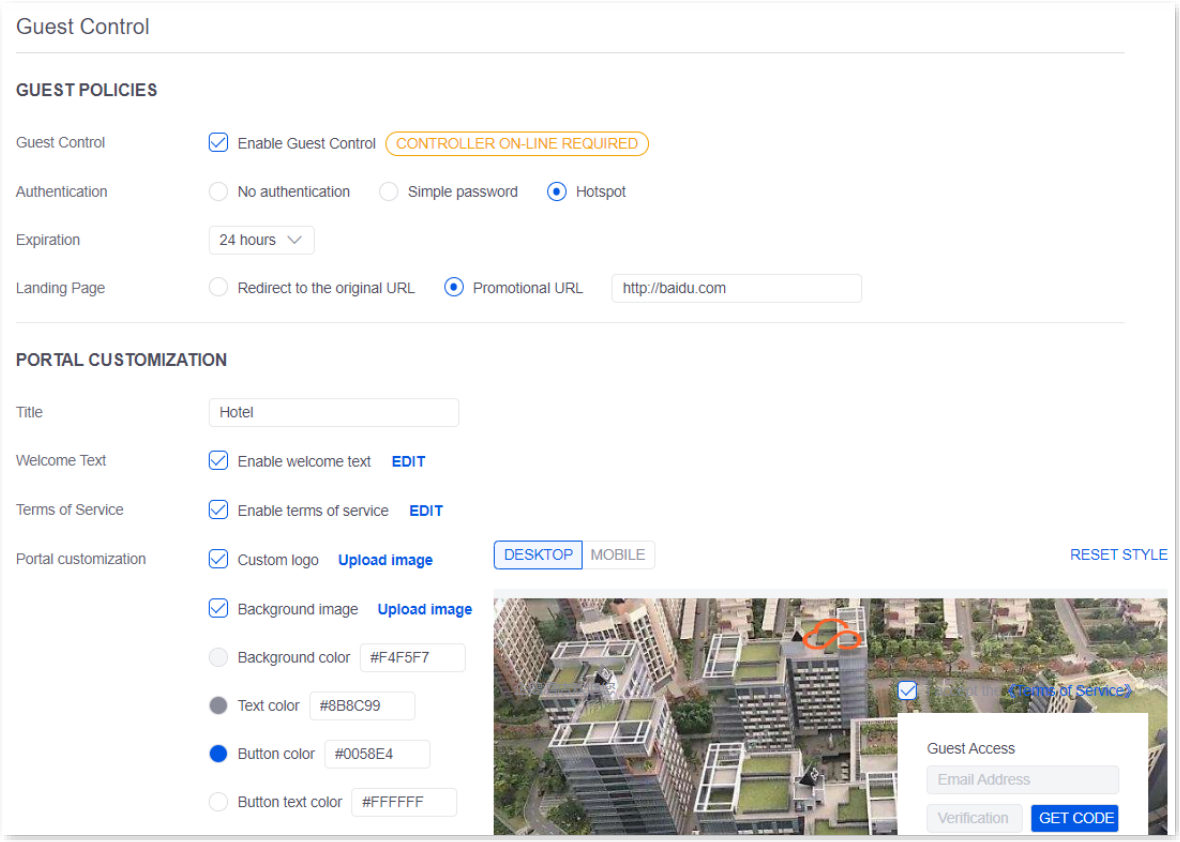
Overview

This page is used to set guest control rules for clients connected to your wireless networks.

With this function enabled, clients need to be authenticated before accessing the internet when connected to a wireless network with guest network policy enabled.

To enter the page, choose **SETTINGS** ( ) > **Guest Control**.

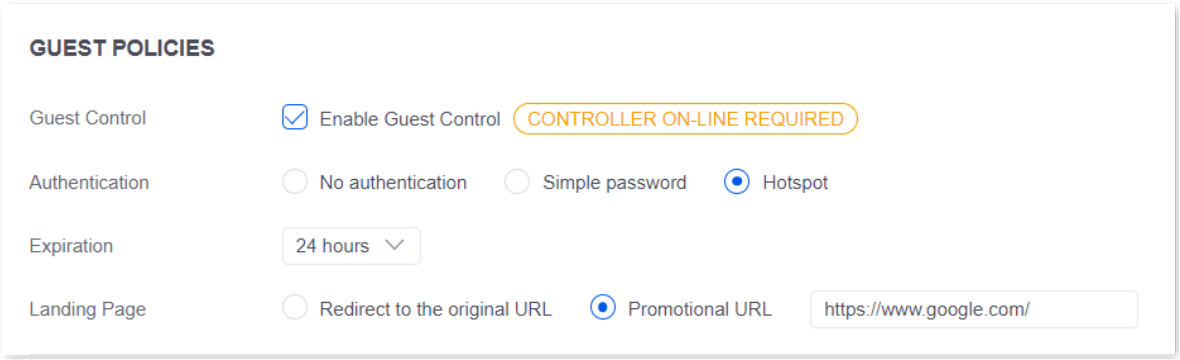
The guest control function is disabled by default. The following figure displays the page when the guest control function is enabled.



Guest Policies

This module is used to select the authentication type and configure the related parameters.

To enter the module, choose **SETTINGS** ( ) > **Guest Control**.



The ProFi Software Controller supports three types of authentication, including No authentication, Simple password and Hotspot. For detailed examples of guess control rule settings, see Examples of Guest Control Configuration.

- **No authentication**

  When a user connects to a wireless network with guest control rules applied and visits a webpage, the browser will automatically redirect to the authentication portal. The user only needs to click **CONNECT** on the authentication portal to gain internet access.

The no authentication type helps increase traffic to your webpage and enhance your publicity.

- **Simple password**

  When a user connects to a wireless network with guest control rules applied and visits a webpage, the browser will automatically redirect to the authentication portal. The user needs to enter the guest password and click **CONNECT** on the authentication portal to gain internet access.

- **Hotspot**

  When a user connects to a wireless network with guest control rules applied and visits a webpage, the browser will automatically redirect to the authentication portal. The user needs to enter the user name and password or obtain a verification code using the SMS/email and click **CONNECT** on the authentication portal to gain internet access.

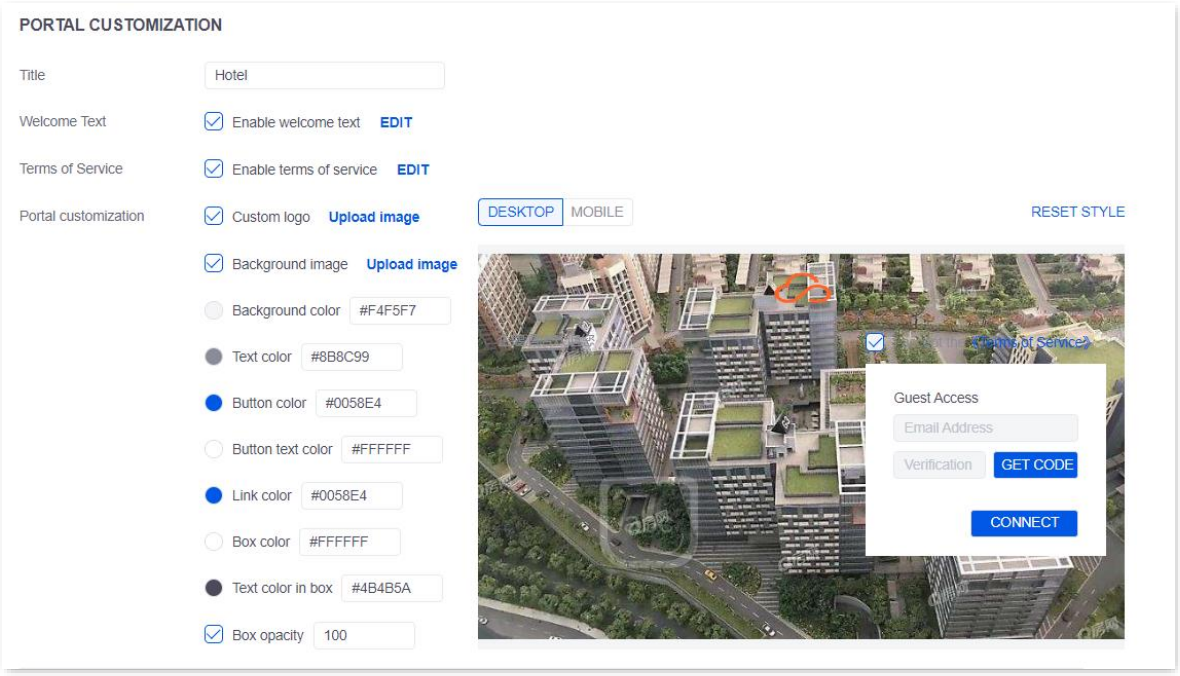
Parameter description

Parameter	Description
Guest Control	It specifies whether the guest control function is enabled.
Authentication	It specifies the authentication mode, including No authentication, Simple password and Hotspot.
Guest Password	This parameter is available only when **Authentication** is set to **Simple password**. It specifies the password users have to enter to gain internet access.
Expiration	It specifies the guest login expiration after a specified period of time. After this period is surpassed, the user will need to re-authenticate to gain internet access.
Landing Page	It specifies the page users are redirected to after passing the authentication. – **Redirect to the original URL**: Users are redirected to the URL they visited before the authentication. – **Promotional URL**: Users are redirected to the URL you specify here.

Portal Customization

This module is used to customize the related authentication portal.

To enter the module, choose **SETTINGS** ( ) > **Guest Control**. The following figure displays the page when the guest control function is enabled.



Parameter description

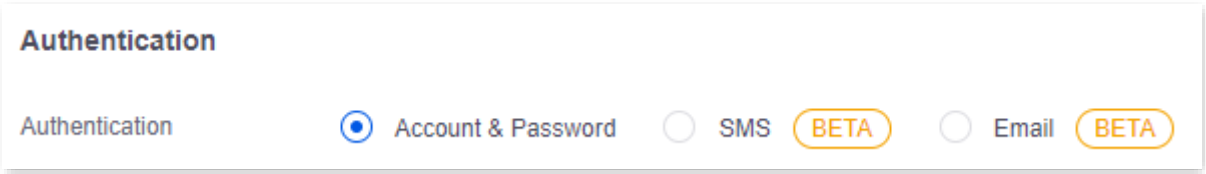
Parameter	Description
Title	It specifies the title of your guest portal.
Welcome Text	It specifies whether a welcome message is displayed on your guest portal. You can check **Enable welcome text** to add a welcome message or click **EDIT** to edit it.
Terms of Service	It specifies whether users are required to accept terms of service on your guest portal. You can check **Enable terms of service** to add terms of service or click **EDIT** to edit it.
Custom logo	It specifies whether a customized logo is displayed on your guest portal. You can check it and click **Upload image** to upload the logo you want to use on the guest portal. It supports the formats of .jpg, jpeg and .png.
Background image	It specifies whether a background image is displayed on your guest portal. You can check it and click **Upload image** to upload the background image you want to use on the guest portal. It supports the formats of .jpg, jpeg and .png.
Background color	Click the circle icon before **Background color** and choose the color you want to display on the background of the guest portal, or you can directly enter a hexadecimal color code in the text box behind **Background color**.
Text color	Click the circle icon before **Text color** and choose the color you want to use on the text on the guest portal, or you can directly enter a hexadecimal color code in the text box behind **Text color**.
Button color	Click the circle icon before **Button color** and choose the color you want to use on the button on the guest portal, or you can directly enter a hexadecimal color code in the text box behind **Button color**.

Parameter	Description
Button text color	Click the circle icon before **Button text color** and choose the color you want to use on the button text on the guest portal, or you can directly enter a hexadecimal color code in the text box behind **Button text color**.
Link color	Click the circle icon before **Link color** and choose the color you want to use on the link on the guest portal, or you can directly enter a hexadecimal color code in the text box behind **Link color**.
Box color	Click the circle icon before **Box color** and choose the color you want to use on the box on the guest portal, or you can directly enter a hexadecimal color code in the text box behind **Box color**.
Text color in box	Click the circle icon before **Text color in box** and choose the color you want to use on the text in box on the guest portal, or you can directly enter a hexadecimal color code in the text box behind **Text color in box**.
Box opacity	It specifies opacity is applied on the box background color. It is selected by default and you can change the opacity of the box background color in the text box behind.
DESKTOP	This preview mode is enabled by default. It displays the portal in the desktop view.
MOBILE	This preview mode displays the portal in the mobile view.
RESET STYLE	Click it to reset portal customization changes to the default settings. It is displayed only when you select the **MOBILE** preview mode.

Authentication

This module is used to choose the nested hotspot authorization, including Account & Password, SMS and Email.

To enter the module, choose **SETTINGS** ( ) > **Guest Control**. The following figure displays the page when the guest control function is enabled and **Authentication** is set to **Hotspot**.

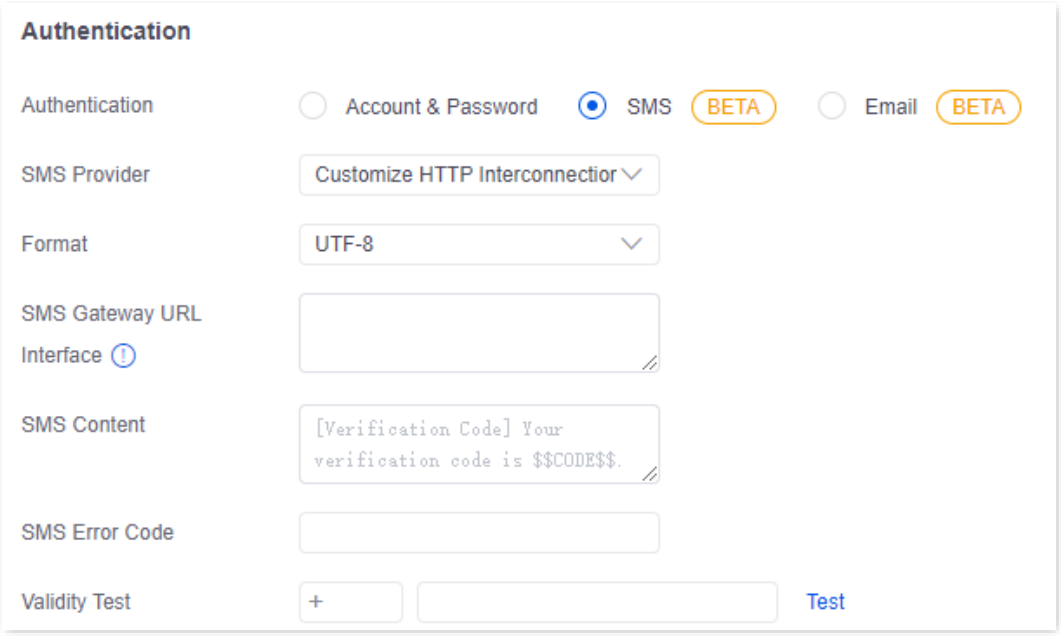


- **Account & Password**

  When this mode is selected, users are required to enter their user names and passwords on the guest portal to log in to the guest network. The user names and passwords can be set on the Guest Access page.

- **SMS**

  When this mode is selected, users are required to enter their mobile numbers and obtain verification codes on the guest portal to log in to the guest network. Currently, the ProFi Software Controller supports the SMS provider **NEXMO**, and you can also select **Customize HTTP Interconnection** to establish a link with other SMS providers.



Tip

You need to subscribe to SMS package services from the corresponding ISP before performing related settings on this page.

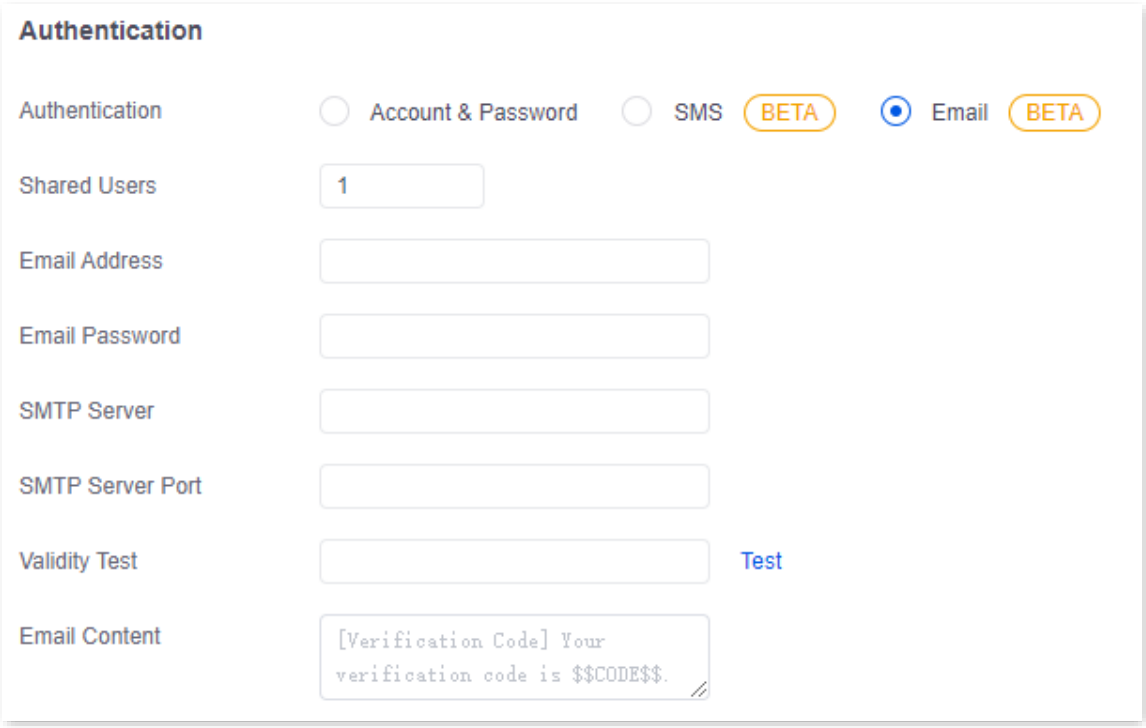
Parameter description

Parameter	Description
Authentication	This parameter is available only when **Authentication** is set to **Hotspot**. It specifies the nested hotspot authorization mode.
SMS Provider	It specifies the ISP that delivers verification codes to mobile numbers. – **NEXMO**: Select this option if you use NEXMO to deliver verification codes. – **Customize HTTP Interconnection**: Select this option if you want to customize the ISP information.
api_key	This parameter is required when **SMS Provider** is set to **NEXMO**. Enter the api_key you applied from NEXMO.
api_secret	This parameter is required when **SMS Provider** is set to **NEXMO**. Enter the api_secret you applied from NEXMO.
Format	This parameter is required when **SMS Provider** is set to **Customize HTTP Interconnection**. It specifies the coding format of the SMS, including **UTF-8** and **GB2312**. Select it according to the ISP you selected.

Parameter	Description
SMS Gateway URL Interface	This parameter is required when **SMS Provider** is set to **Customize HTTP Interconnection**. It specifies the address of the SMS gateway URL interface. Generally, the ISP provides the SMS gateway HTTP interface and you need to complete the address of the SMS gateway URL interface accordingly.
SMS Content	It specifies the content of the SMS delivered to mobile numbers. Tip The verification code must be in the format of **$$CODE$$**.
SMS Error Code	It specifies the error code for SMS sending failure. When the SMS sending fails, a message will be sent to the router and you can consult your ISP based the returned information. For details about the error code, consult your ISP.
Validity Test	It is used to test whether the preceding settings are correct. You can enter your mobile number and click **Test** to check the settings.

- **Email**

When this mode is selected, users are required to enter their email addresses and obtain verification codes on the guest portal to log in to the guest network.



Parameter description

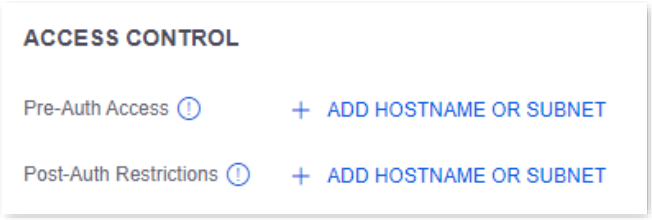
Parameter	Description
Authentication	This parameter is available only when **Authentication** is set to **Hotspot**. It specifies the nested hotspot authorization mode.
Shared Users	It specifies the number of users that are allowed to use a same email address for authentication.
Email Address	It specifies the email address used to send emails.
Email Password	It specifies the password or authorization code of the email address used to send emails.
SMTP Server	It specifies the Simple Mail Transfer Protocol (SMTP) server address. Tip SMTP servers are used to send, receive, and/or relay outgoing mail between email senders and receivers. The SMTP server addresses and ports of different email service providers are different. Please query them accordingly.
SMTP Server Port	It specifies the Simple Mail Transfer Protocol (SMTP) server port. Tip SMTP servers are used to send, receive, and/or relay outgoing mail between email senders and receivers. The SMTP server addresses and ports of different email service providers are different. Please query them accordingly.
Validity Test	It is used to test whether the preceding settings are correct. You can enter your mobile number and click **Test** to check the settings.
Email Content	It specifies the content of emails. Tip The verification code must be in the format of **$$CODE$$**.

Access Control

This module is used to control guest network access before and after user authentication.

Generally, after a user connects to the guest network, the user cannot access any network before authentication and can access the internet only after authentication. If you want to allow your users to access some specified websites before authentication or prohibit them from accessing some specifies websites after authentication, you can perform settings in this module.

To enter the module, choose **SETTINGS** ( ) > **Guest Control**. See the following figure.



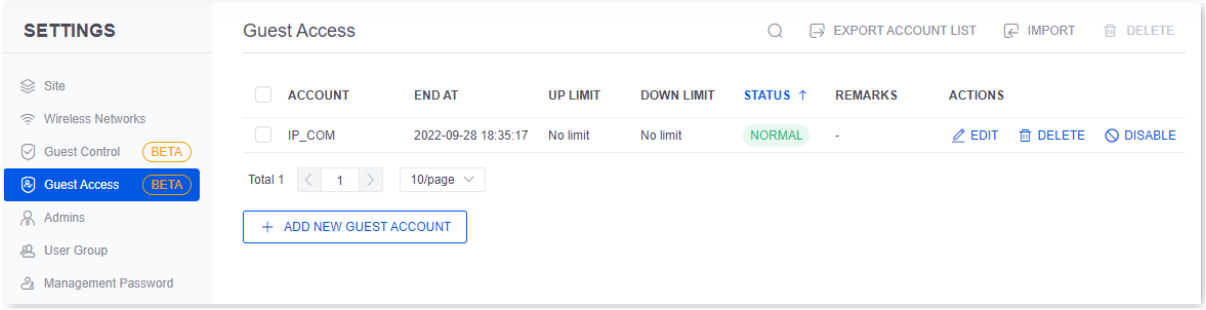
Parameter description

Parameter	Description
Pre-Auth Access	It specifies the host addresses or address segments that users can access before authentication after they connect to the guest network. You can click **+ADD HOSTNAME OR SUBNET** to add multiple host addresses or address segments in the format of ***192.168.0.0/16***. You can click × to delete a host address or address segment.
Post-Auth Restrictions	It specifies the host addresses or address segments that users cannot access after they connect to the guest network and complete authentication. You can click **+ADD HOSTNAME OR SUBNET** to add multiple host addresses or address segments in the format of ***192.168.0.0/16***. You can click × to delete a host address or address segment.

Guest Access

This page is used to set web-based authorization rules, including setting guest access username, password, bandwidth limit, duration, connection limit and number of shared users.

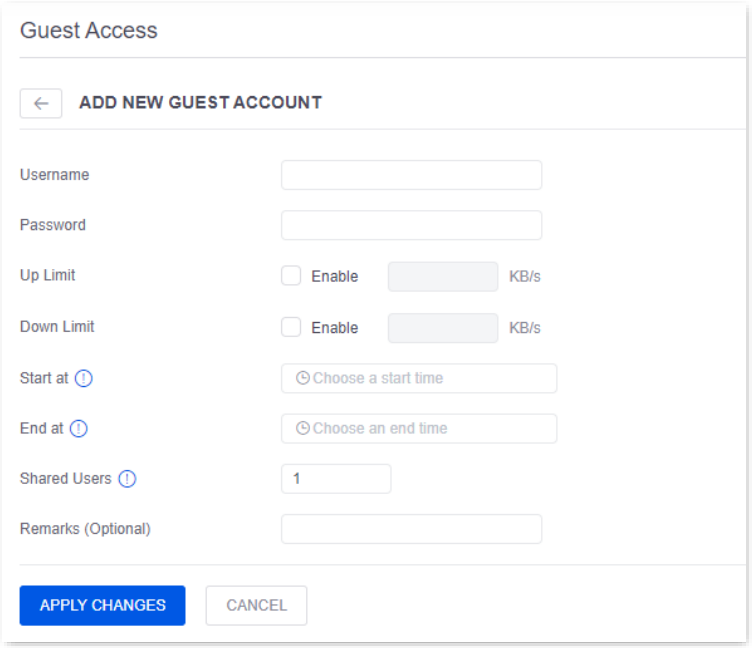
To enter the page, choose **SETTINGS** ( ) > **Guest Access**. The following figure displays the page when a guest access rule is added manually.



Parameter description

Parameter	Description
	Click it and enter the text you want to search for in the search box. The searching starts immediately when you enter keywords.
EXPORT ACCOUNT LIST	Click it to export the configured authentication account data to your local computer.
IMPORT	Click it to import the authentication account data that you exported before to the controller.
DELETE	Click it to delete authentication rules in batches.
ACCOUNT	It specifies the guest access account name.
END AT	It specifies the time point when this guest access account expires.
UP LIMIT	It specifies the maximum upload speed for this account.
DOWN LIMIT	It specifies the maximum download speed for this account.
STATUS	It specifies the status of the account.
REMARKS	It specifies the remarks of the account.
ACTIONS	It specifies the actions you can perform on the guest access rule. – Click EDIT to edit the guest access rule. – Click DELETE to delete the guest access rule. – Click ENABLE /DISABLE to enable or disable the guest access rule.

Click **+ ADD NEW GUEST ACCOUNT** to create a new guest access rule. See the following figure.



Parameter description

Parameter	Description
Username/Password	It specifies the username/password users have to enter to gain internet access when web-based authorization is enabled.
Up Limit	It specifies whether the maximum upload speed for this account is enabled. It is disabled by default. You can enable it and set the upload speed limit in the text box behind.
Down Limit	It specifies whether the maximum download speed for this account is enabled. It is disabled by default. You can enable it and set the download speed limit in the text box behind.
Start at	It specifies the time point when this guest access rule takes effect.
End at	It specifies the time point when this guest access rule expires.
Shared Users	It specifies the number of users that are allowed to gain internet access using this guest account.
Remarks (Optional)	It specifies the remarks you set for this guest access account. This parameter is optional.

Admins

This page is used to create administrator accounts.

As a super administrator, you can create administrators and read only administrators.

To enter the page, choose **SETTINGS** ( ) > **Admins**.

Tip

The **Admins** module appears only for a super administrator and administrators. Only a super administrator can create administrators and read-only administrators. Here takes the super administrator as an example to illustrate more operations.

- **Super Administrator**

  The super administrator account is created during the Quick Setup Wizard. The super administrator account has all the site permissions, including device configuration and management, dashboard editing, system status access, and read-only access to all sites. Besides, the super administrator can add, delete, or modify the information of other non-super administrator accounts.

- **Administrator**

  The administrator account is created by the super administrator. By default, the administrator account has all the site permissions, including device management and configuration dashboard editing and system status access, and these permissions cannot be modified. You can create 8 administrator accounts at most.

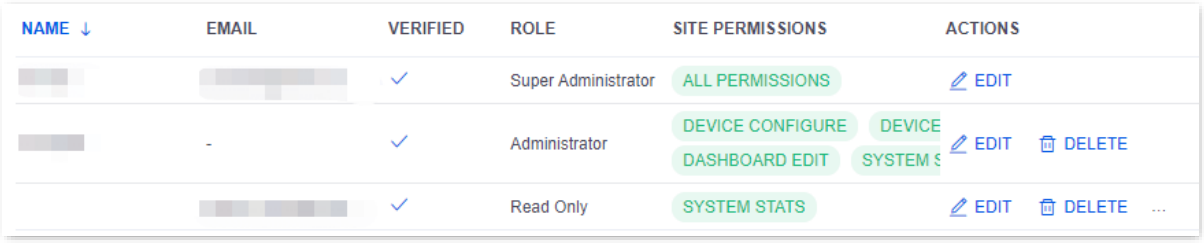
- **Read Only Administrator**

  The read-only administrator account is created by the super administrator. The read-only administrator account has no operating permissions. You can create 16 read-only administrator accounts at most.

Note

Ensure that you save the super administrator account login information for future use.

To enter the page, choose **SETTINGS** ( ) > **Admins**. See the following figure.

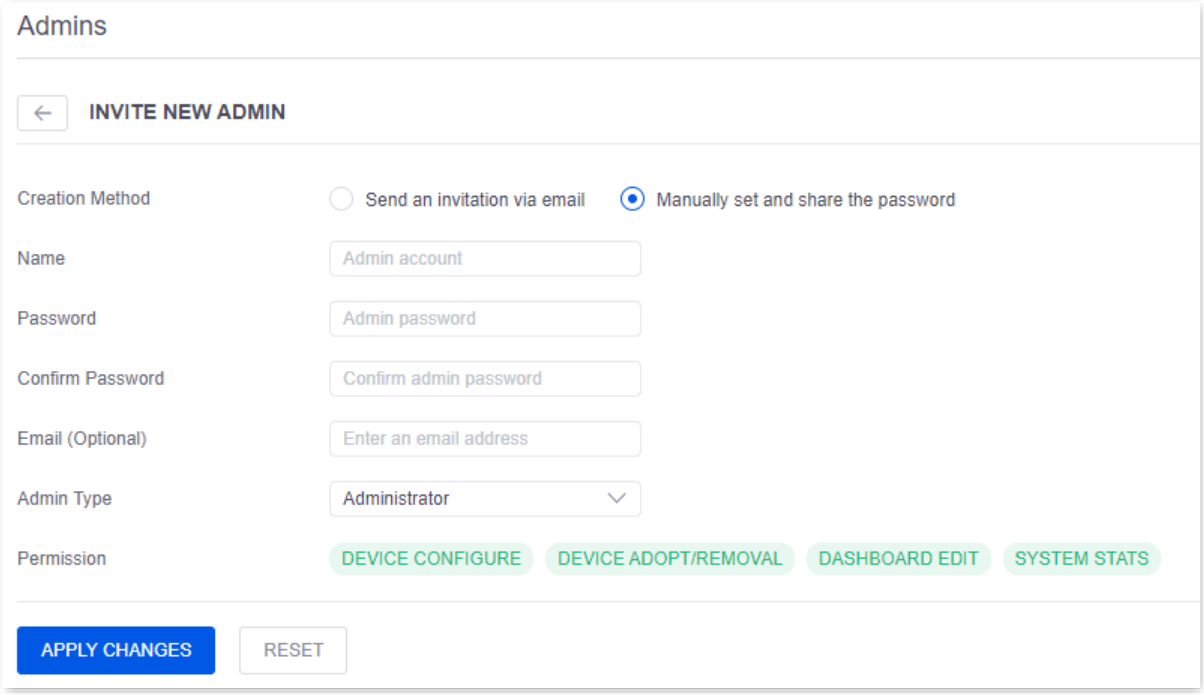


Parameter description

Parameter	Description
	Click it and enter the text you want to search for in the search box.
NAME	It specifies the name of the administrator.
EMAIL	It specifies the email address of the administrator.
VERIFIED	It specifies whether the account is verified. ✓ indicates that the account has been verified.
ROLE	It specifies the permission level of the administrator, including super administrator, administrator, and read only.
SITE PERMISSIONS	It displays the permissions the administrator has over the site. – Read only administrators have only the read-only permissions. – Administrators have the permissions of device configuration and management, dashboards editing, system statistics access, and read-only access to all site. – Super administrators have the permissions of administrators and remote access as well.
ACTIONS	It specifies the actions you can perform on the administrator. – Click EDIT to edit the administrator. – Click DELETE to delete the administrator. The super administrator cannot be deleted.

Add New Admin

Click **+ ADD NEW ADMIN** to create a new administrator. See the following figure.

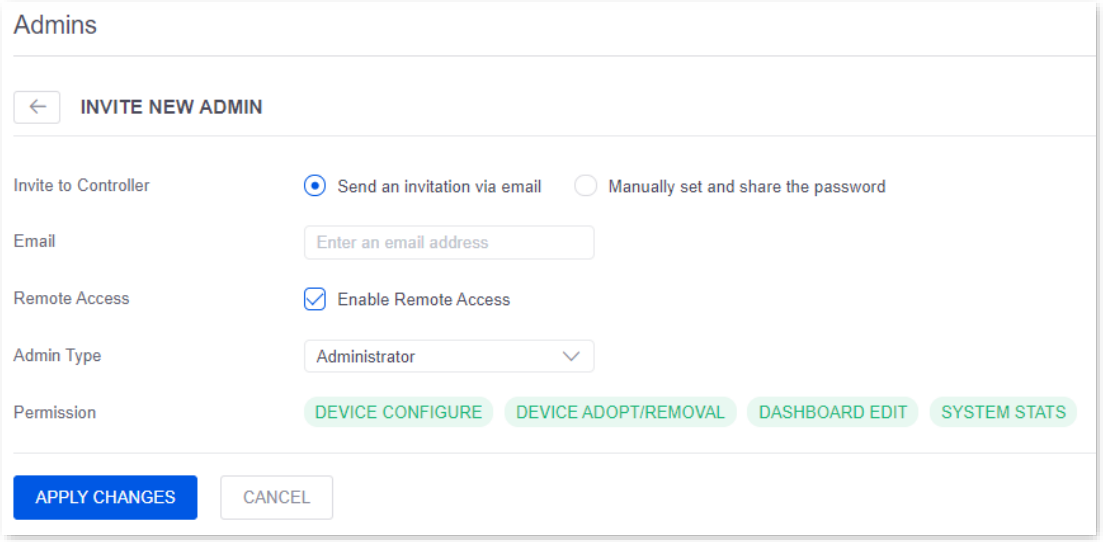


You can create an administrator account by Send an invitation via email or Manually set and share the password.

- **Send an invitation via email**

The administrators authorized by the super administrator through emails can:

- Remotely access the controller through the ProFi Software Controller (sdn.ip-com.com.cn)
- Access the controller through the local computer on which the controller is installed

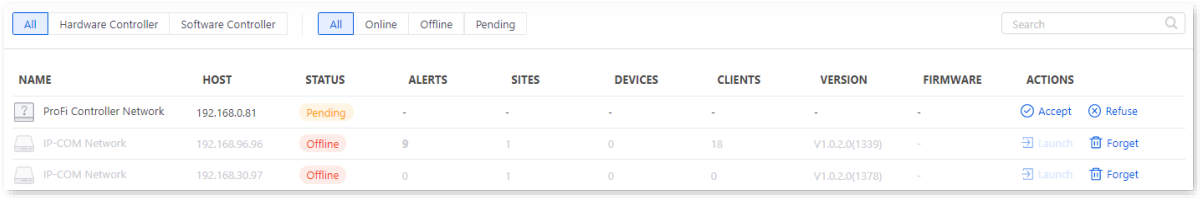


Parameter description

Parameter	Description
Invite to Controller	**Send an invitation via email**: Send an email to invite a user to be the administrator of the current site.
Email	It specifies the email address of the new administrator.
Remote Access	It specifies whether remote access is enabled for the new administrator. Check **Enable Remote Access** to grant the remote access permission to the new administrator.
Admin Type	It specifies the role of the new administrator. – **Administrator**: The administrator has device configuration and management, dashboards editing, system statistics access, and read-only access to all site. – **Read Only**: The administrator has only the read-only permission.
Permission	It specifies the permissions of the account. It changes with the value of **Admin Type** and cannot be modified.

After the configuration completes, the administrator or read-only administrator can remotely access the ProFi Software Controller through the following steps:

1. Log in to the invited email box, open the invitation email, click the invitation link in the email to enter the web UI of ProFi SDN Cloud.
2. Enter the login username and password to log in to ProFi SDN Cloud.
3. Locate the target controller, and click **Accept** behind it.



----End

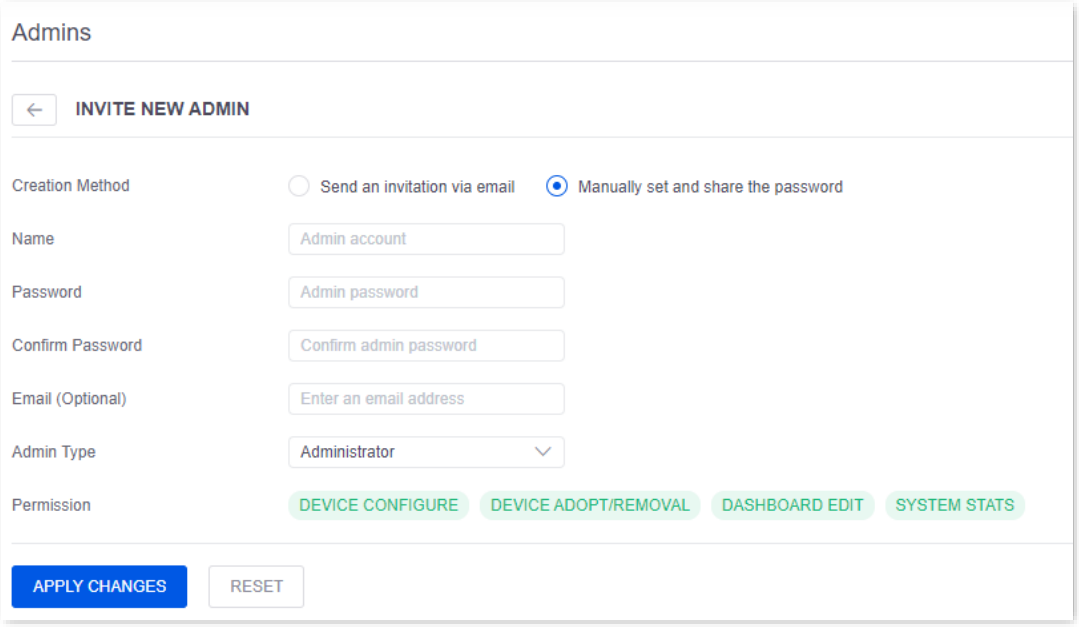
Besides the remote access after accepting the invitation email, the administrator and read-only administrator can also locally access the ProFi Software Controller by starting the local application of ProFi Software Controller at your management computer and using the ProFi SDN cloud account to log in.

Tip

- The email bound to the login account must be consistent with that used for invitation.
- The new administrator who did not register an account before must register an account using the invited email address.

Manually set and share the password

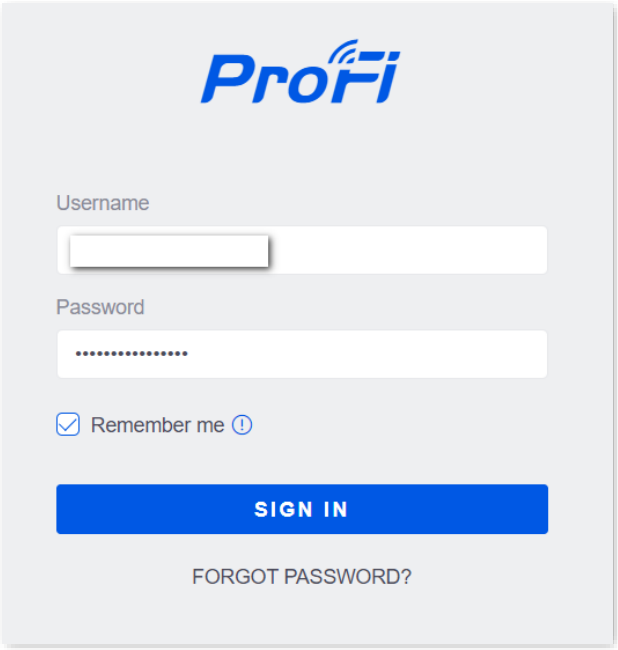
The administrator and read-only administrator manually set by the super administrator can access the controller on the local computer on which the controller is installed.



Parameter description

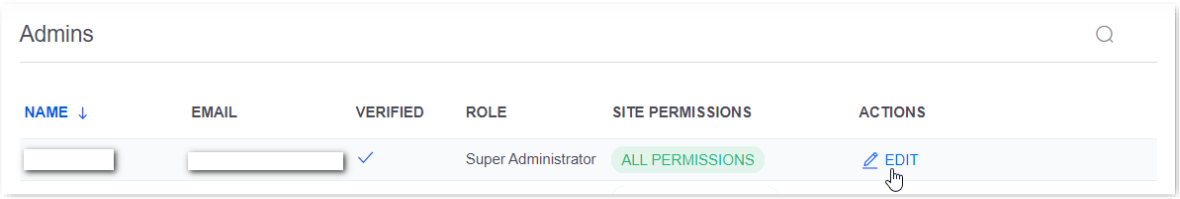
Parameter	Description
Creation Method	**Manually set and share the password**: Manually set the account and password and share the account information to the user.
Name	It specifies the name of the new administrator.
Password	It specifies the password you set for the new administrator.
Confirm Password	Enter the new password again.
Email (Optional)	It specifies the email address of the new administrator. It is optional.
Admin Type	It specifies the role of the new administrator. – **Administrator**: The administrator has device configuration and management, dashboards editing, system statistics access, and read-only access to all site. – **Read Only**: The administrator has only the read-only permission.
Permission	It specifies the permissions of the account. It changes with the value of **Admin Type** and cannot be modified.

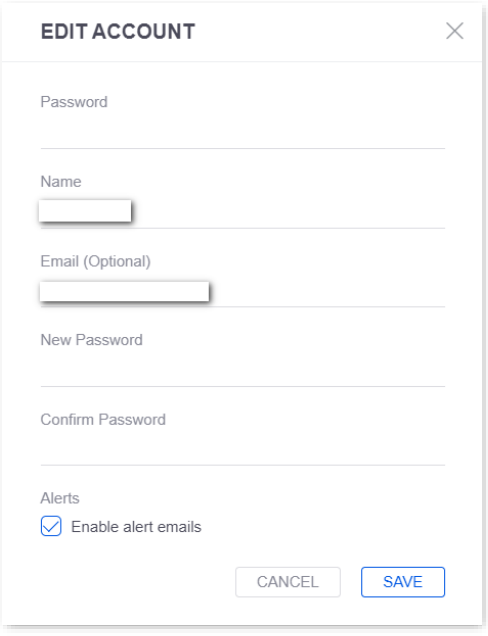
After the configuration completes, the new administrator can log in to the ProFi Software Controller and access the controller with the account and password you set.



Edit Super Administrator Account

Click EDIT behind the Super Administrator column, then you can change the username and password





User Group

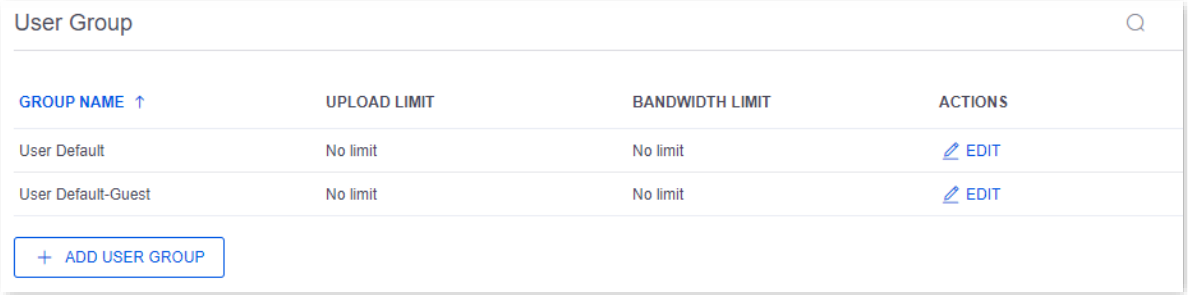
This page is used to create and manage user groups. Through user groups, you can set the upload and download speed limits for clients.

To enter the page, choose **SETTINGS** ( ) > **User Group**.

By default, two user groups are preset in the names of **User Default** and **User Default-Guest**, which can be edited only and cannot be deleted. The authentication users will be automatically added to the **User Default-Guest** group.

You can change the user group to which clients belong by referring to Batch Client Configuration and Single Client Configuration.

Click **+ ADD USER GROUP** to add a user group.



Parameter description

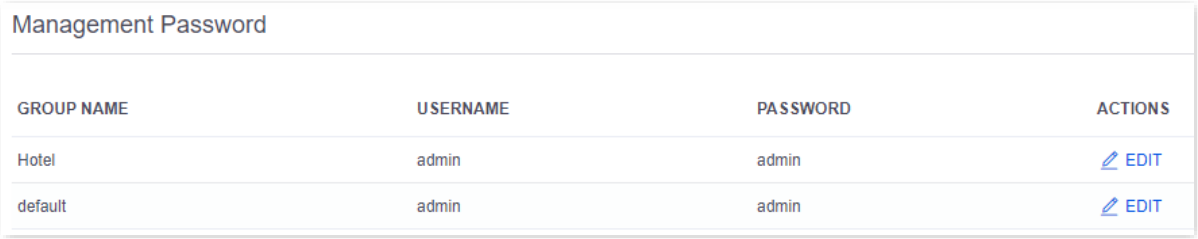
Parameter	Description
	Click it and enter the text you want to search for in the search box. The searching starts immediately when you enter keywords.
GROUP NAME/Name	It specifies the name of the user group.
UPLOAD LIMIT/Upload Limit Per User	They specify the maximum upload and download speeds for each user in the user group.
BANDWIDTH LIMIT/Download Limit Per User	
ACTIONS	It specifies the actions you can perform on the user group. – Click EDIT to edit the user group. – Click DELETE to delete the user group.

Management Password

This page is used to manage the username and password used for logging in to the management web UI of APs in specified WLAN groups which you have created in the page of **Wireless Networks**. By default, it displays such information of the WLAN group **default**.

The default username and password are both **admin** and you can click EDIT to change them.

To enter the page, choose **SETTINGS** ( ) > **Management Password**.



Parameter description

Parameter	Description
GROUP NAME	It specifies the name of the WLAN group.
USERNAME	They specify the user name and password used for logging in to the management page of the AP.
PASSWORD	
ACTIONS	It specifies the actions you can perform on the management password. You can click EDIT to edit the management password.

Controller

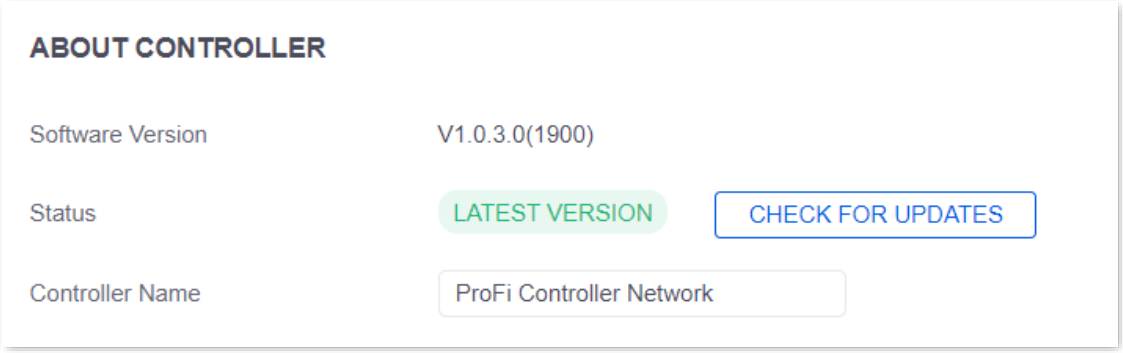
This page is used to manage the controller, including viewing controller and device information and setting web management and fast roaming.

To enter the page, choose **SETTINGS** ( ) > **Controller**.

About Controller

This module is used to display information of the controller and upgrade the controller.

To enter the module, choose **SETTINGS** ( ) > **Controller**.



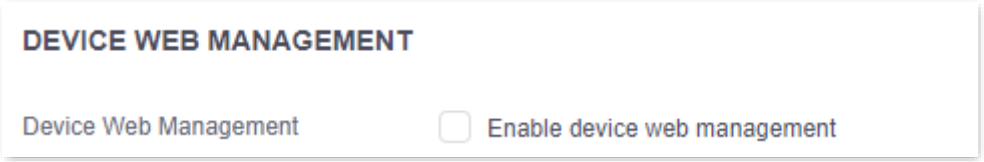
Parameter description

Parameter	Description
Software Version	They specify the software version and status of the controller.
Status	You can click **CHECK FOR UPDATES** to find a new version and upgrade the controller.
Controller Name	It specifies the name of the controller. You can change it here.

Device Web Management

This module is used to enable or disable web management of all ProFi series of devices under the controller. This function is disabled by default and you can enable it as required.

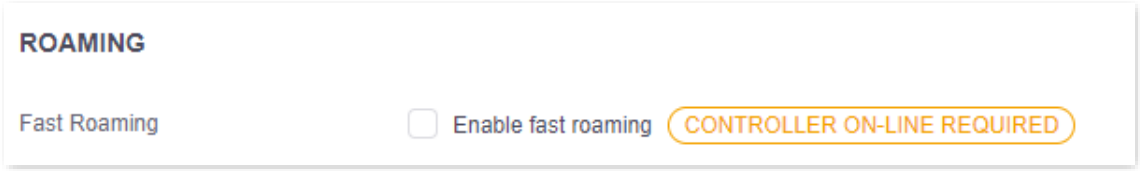
To enter the module, choose **SETTINGS** ( ) > **Controller**.



Roaming

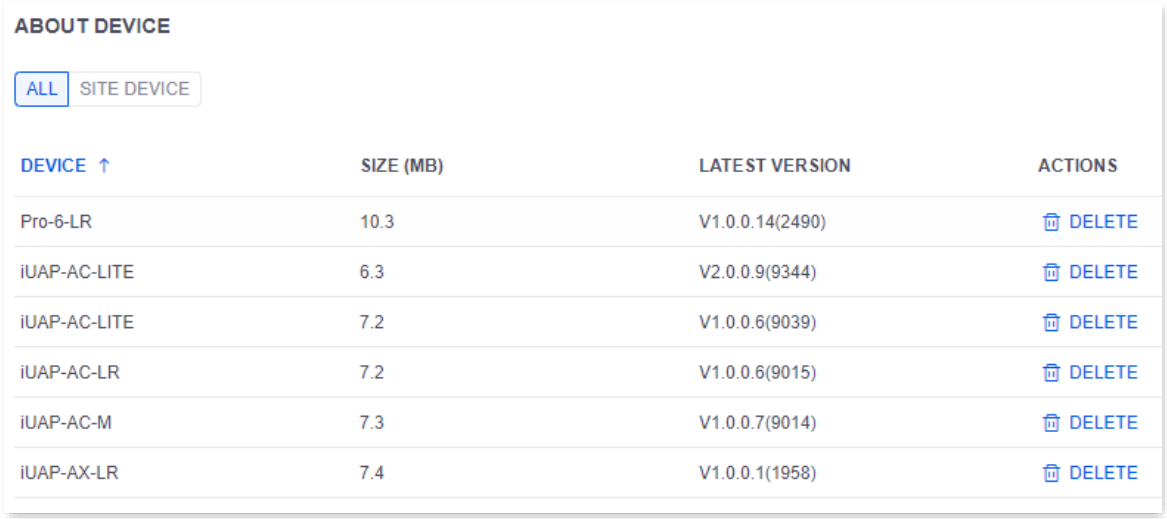
This module is used to enable or disable the fast roaming function of all ProFi APs under the controller. This function is disabled by default and you can enable it as required.

To enter the module, choose **SETTINGS** ( ) > **Controller**.



About Device

Click the **ALL** tab, then you can view information of all ProFi series of devices which can be managed and upgraded online by the controller, including device models and firmware versions.

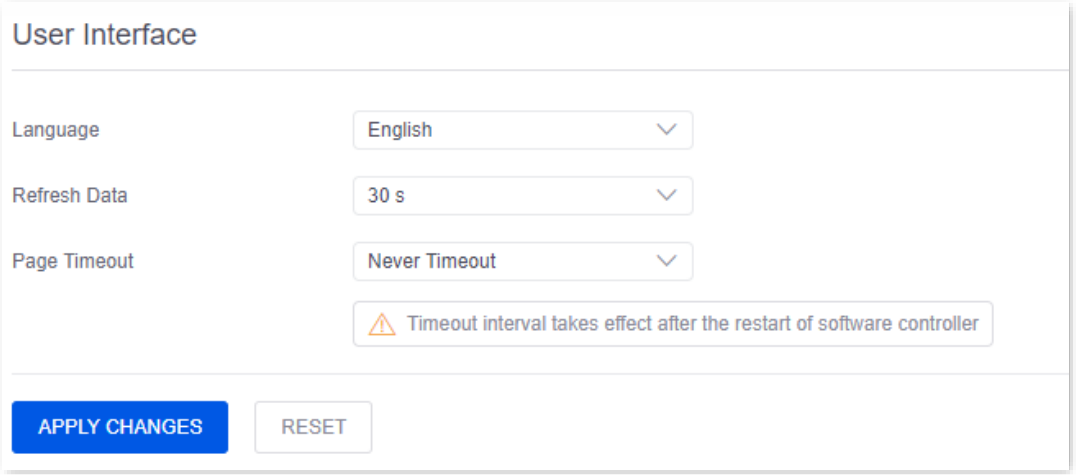


Click the **SITE DEVICE** tab, then you can view the information of ProFi series of devices supporting online upgrade under the current site, including the device models and firmware versions.

User Interface

This page is used to set language, refresh interval and page timeout for the web UI of your ProFi Software Controller.

To enter the page, choose **SETTINGS** ( ) > **User Interface**. See the following figure.



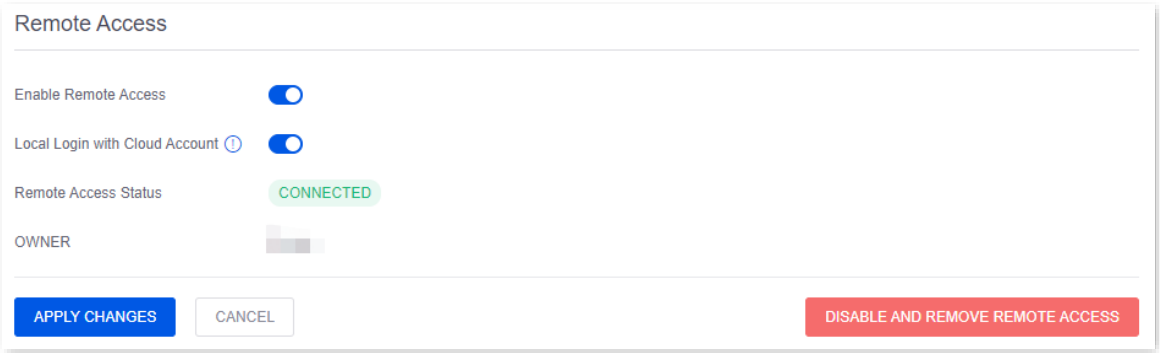
Parameter description

Parameter	Description
Language	It specifies the language displayed on the web UI of your ProFi Software Controller.
Refresh Data	It specifies the interval at which the web UI of the ProFi Software Controller refreshes data. If you do not want the web UI of the ProFi Software Controller to refresh automatically, select **Never Refresh**. If you want to manually refresh the web UI of the ProFi Software Controller, select **Manual Refresh**.
Page Timeout	It specifies the timeout time of the web UI of the ProFi Software Controller if no operation is performed. If you want to keep the web UI of the ProFi Software Controller valid, select **Never Timeout**.

Remote Access

Through the Remote Access function, you can remotey manage the ProFi Software Controllers through ProFi SDN Cloud.

To enter the page, choose **SETTINGS** ( ) > **Remote Access**. See the following figure.



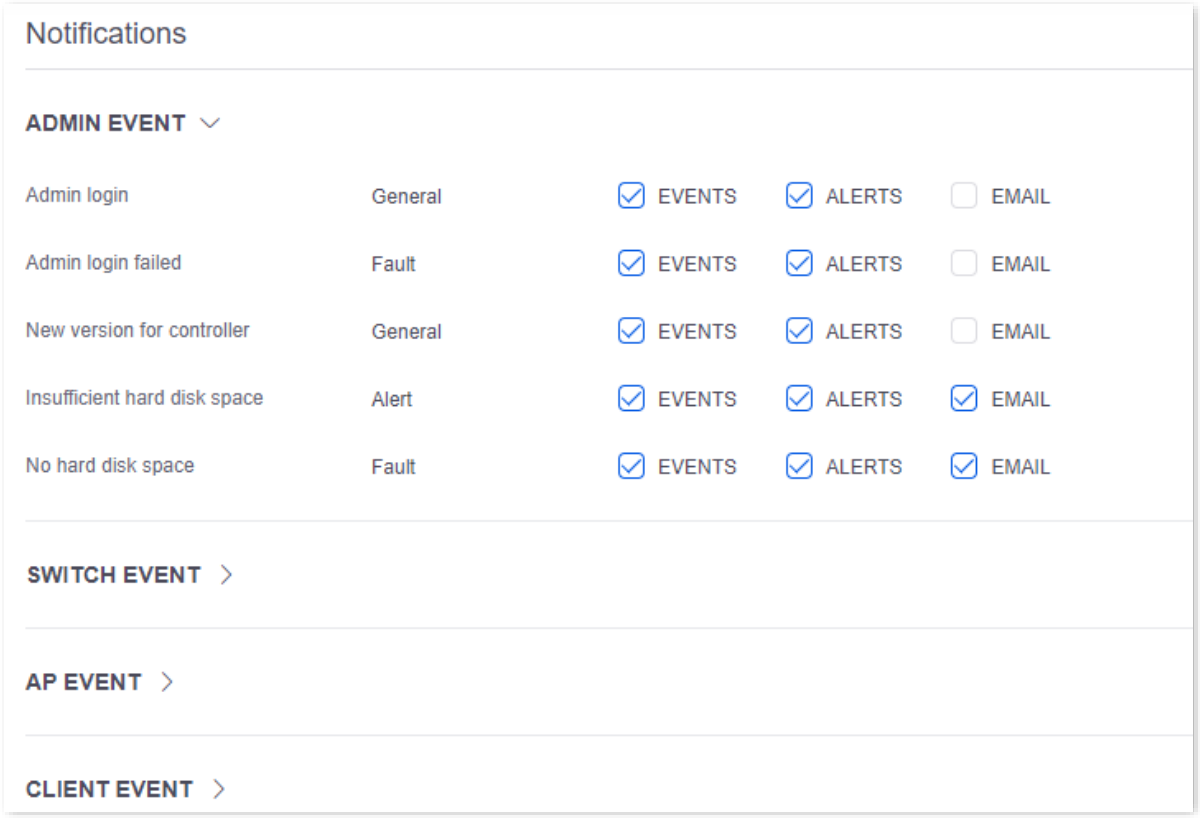
Parameter description

Parameter	Description
Enable Remote Access	It specifies whether the remote access function is enabled. If you logged in using a local account, to enable remote access, you need to enter the ProFi SDN Cloud email/username and password to bind the controller to the cloud. After the remote access function is enabled, **Local Login with Cloud Account** will also be enabled automatically.
Local Login with Cloud Account	It specifies whether to locally log in with a ProFi SDN Cloud account. After this function is enabled, the username, email, and password of the current local account will be replaced with those of the ProFi SDN Cloud account. Tip This function takes effect only when the email bound to the local account is consistent with that of the cloud account.
Remote Access Status	It specifies the remote access status of the ProFi Software Controller.
OWNER	It specifies the cloud account of the ProFi Software Controller.
DISABLE AND REMOVE REMOTE ACCESS	Once disabled and removed, **Remote Access** and **Local Login with Cloud Account** are both cut off. Thus, you need to locally log in to the controller, and restart the remote access function for remote management.

Notifications

This page is used to customize the types of notifications you receive from the ProFi Software Controller for a variety of events.

To enter the page, choose **SETTINGS** ( ) > **Notifications**. See the following figure.



The ProFi Software Controller supports admin events, switch events, AP events and client events. You can click each event category to check the detailed events, and choose how you want a specific event to be notified, be it on the **Events** page, on the **Alerts** page, or through a notification **Email** sent to the email address of the super administrator.

Parameter description

Element	Description
ADMIN EVENT	Click to access administrator events notifications.
SWITCH EVENT	Click to access switch events notifications.
AP EVENT	Click to access AP events notifications.
CLIENT EVENT	Click to access client events notifications.

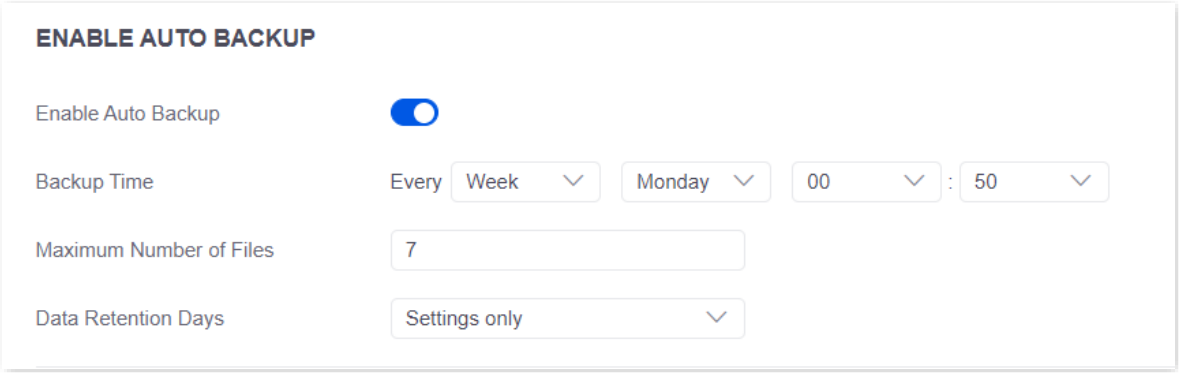
Backup

This page is used to configure automatic backup settings for the ProFi Software Controller, download backup files to your local computer and restore configurations from backup files, and check available backups of the ProFi Software Controller.

Enable Auto Backup

This module is used to configure the auto backup function and its related parameters.

To enter the module, choose **SETTINGS** ( ) > **Backup**. See the following figure.



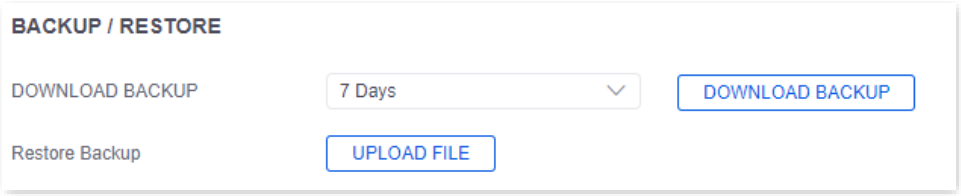
Parameter description

Parameter	Description
Enable Auto Backup	It specifies whether the automatic backup function is enabled.
Backup Time	It specifies how often the ProFi Software Controller performs auto backup. You can set auto backup to every **Day, Week** and **Month**. Then, configure the appropriate time, day, and/or month based on your choice.
Maximum Number of Files	It specifies the maximum number of backup files to be saved. If this number is surpassed, the oldest backup file is deleted. The default value is **7**.
Data Retention Days	Set the auto backup content such as the controller's settings, events and alerts, and length of time in days that data is retained. – **Settings Only**: Back up only the settings excluding logs and alerts. – **7 Days, 30 Days, 60 Days, 90 Days, 180 Days, 365 Days**: Back up the configurations, events and alerts in last 7 days, 30 Days, 60 Days, 90 Days, 180 Days and 365 Days. – **No Limit**: Back up the configurations and all events and alerts.

Backup/Restore

This module is used to download backup files for the ProFi Software Controller and restore the backup files.

To enter the module, choose **SETTINGS** ( ) > **Backup**. See the following figure.



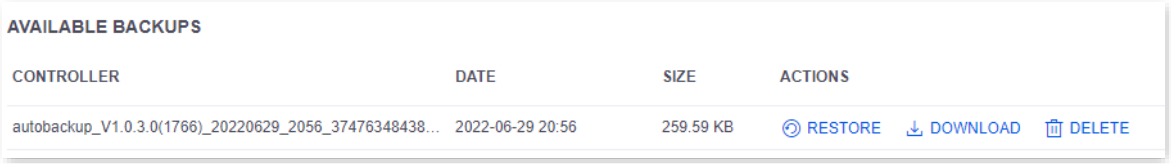
Parameter description

Parameter	Description
DOWNLOAD BACKUP	Set the auto backup content such as the controller's configurations, events and alerts, and length of time in days that data is retained. – **Settings Only**: Back up only the configurations excluding logs and alerts. – **7 Days, 30 Days, 60 Days, 90 Days, 180 Days, 365 Days**: Back up the configurations, events and alerts in last 7 days, 30 Days, 60 Days, 90 Days, 180 Days and 365 Days. – **No Limit**: Back up the configurations and all events and alerts.
Restore Backup	Click **UPLOAD FILE** to upload your backup files to restore the configurations of the ProFi Software Controller to those you uploaded.

Available Backups

This module enables you to view, restore, download and delete the available auto backups for the ProFi Software Controller.

To enter the module, choose **SETTINGS** ( ) > **Backup**. See the following figure.



Parameter description

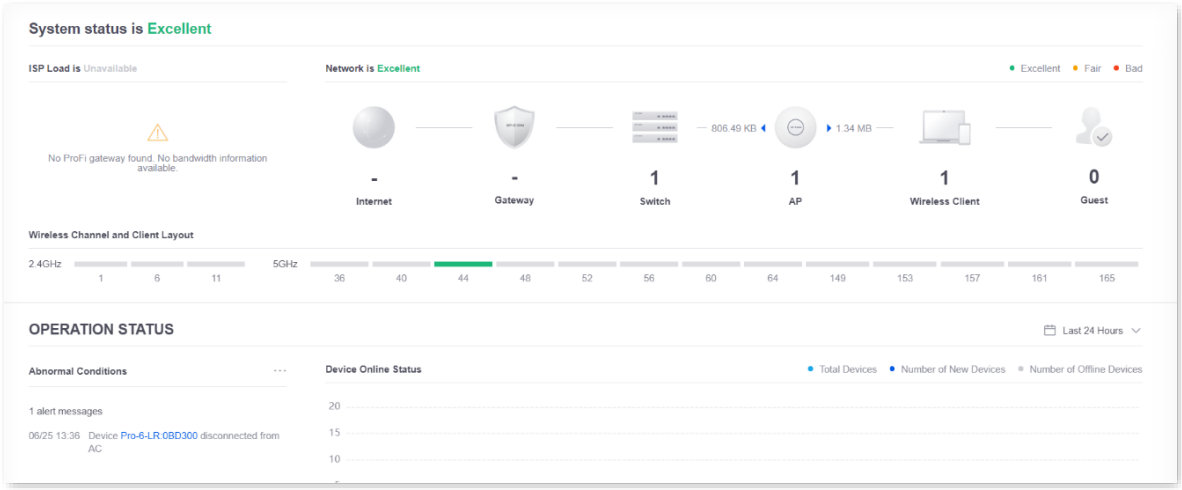
Parameter	Description
CONTROLLER	It specifies the name of the ProFi Software Controller.
DATE	It specifies the date on which the backup file is generated.
SIZE	It specifies the size of the backup file.
ACTIONS	It specifies the actions you can perform on the backup file. – Click RESTORE to restore the ProFi Software Controller from the backup file. – Click DOWNLOAD to download the backup file. – Click DELETE to delete the backup file.

4 Dashboard

This page provides a visual representation for your network.

To enter the page, choose **DASHBOARD** ( ). See the following figure.

Here, you can check the system status and gateway ISP load and bandwidth information, view the number of ProFi devices, wireless channels and corresponding client layout, and examine the operation status of ProFi devices including abnormal conditions, online device status, overall and real-time statistics of WiFi clients.



4.1 System Status

The overall system statuses are divided into three kinds:

- **System status is Excellent**: No ProFi devices of the site are offline or there are no ProFi devices in the site.
- **There are Faults in network**: Some ProFi devices of the site are offline.
- **You network is Malfunctioning**: All ProFi devices of the site are offline.

4.2 ISP Load

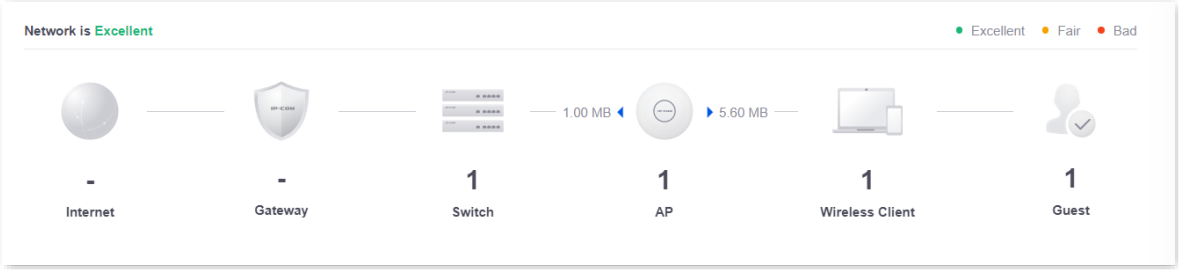
This module displays the ISP load, related throughput and delay statistics, and allows you to conduct speed test. This module is not supported yet in this version.

4.3 Network

This module displays the number of ProFi devices, clients and guests in the network and corresponding statistics. See the follow figure.

Tip

Network is **Excellent**, **Fair** and **Bad** corresponds to **System status is Excellent**, **There are Faults in network,** and **Your network is malfunctioning**.



The head title indicates the level of internet quality evaluated based on data uploading and downloading rate, bandwidth, and latency. The network statuses include:

- **Network is Excellent**: The internet quality is excellent.
- **Network is Fair:** The internet quality is just at an ordinary level.
- **Network is Bad**: The internet quality is unsatisfactory.

Parameter description

Parameter	Description
Internet	It displays the internet bandwidth utilization rate. This parameter is not supported in this version.
Gateway	It displays the CPU utilization of the gateway. This parameter is not supported in this version.
Switch	It displays the number of switches in this network. If you place the mouse over the switch icon, you will see: – **Wired Clients**: specifies the total number of clients connected to switches. – **All Ports**: specifies the total number of switch ports. – **Available Ports:** specifies the number of available switch ports. – **PoE Power (W):** specifies the total PoE power supplied by the switches.

Parameter	Description
AP	It displays the number of APs in this network. If you place the mouse over the AP icon, you will see: – **Wireless Clients**: specifies the total number of wireless clients connected to the APs. – **Wireless Client Groups:** specifies the number of wireless client groups. The blue left triangular ◀ representing total upload traffic of the AP while the blue right triangular ▶ representing total download traffic of the AP.
Wireless Client	It displays the number of clients in this network. If you place the mouse over the client icon, you will see: – **2.4G Clients**: specifies the total number of 2.4G clients connected to the APs. – **5G Clients:** specifies the total number of 5G clients connected to the APs.
Guest	It displays the number of guests connected to the wireless network.

4.4 Wireless Channel and Client Layout

This module displays the channels of 2.4 GHz and 5 GHz, and if you place the mouse over a channel, you can view the number of APs and clients of that channel. See the following figure.

The system identifies the number of wireless clients by different colors.

Band	Color	Description
2.4 GHz	Gray	No wireless clients connected in the channel range.
	Red	Over 100 wireless clients connected in the channel range.
	Orange	50 to 100 wireless clients connected in the channel range.
	Green	Less than 50 wireless clients connected in the channel range.
5 GHz	Gray	No wireless clients connected in the channel range.
	Red	Over 150 wireless clients connected in the channel range.
	Orange	80 to 150 wireless clients connected in the channel range.
	Green	Less than 80 wireless clients connected in the channel range.

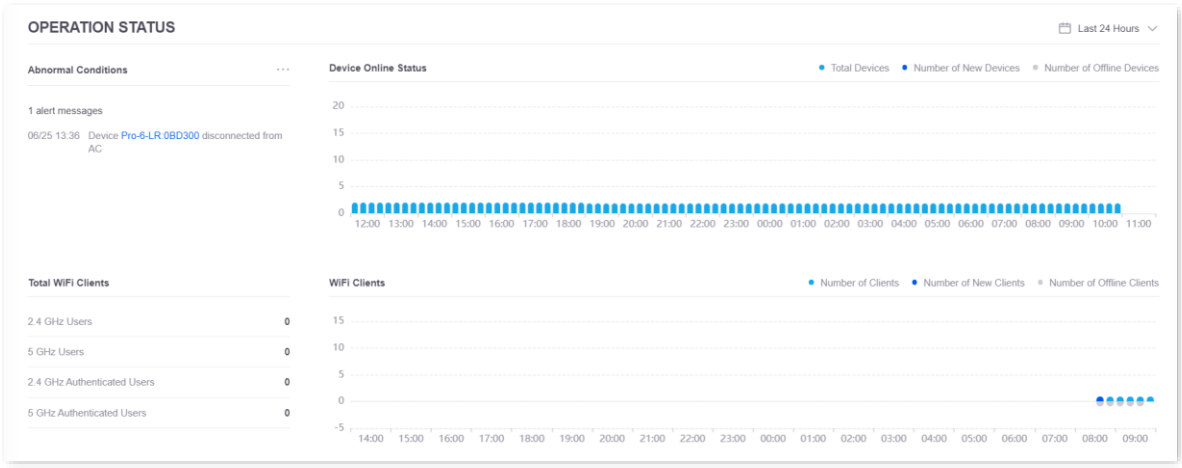
4.5 Operation Status

This part displays modules of abnormal conditions, device online status, overall and real-time statistics of WiFi clients. See the following figure.

The displayed date in the upper right corner is used to filter the statistics in a specific period. You can choose the preset time period such as **Today**, **Yesterday**, **Last 1 Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 14 Days**, **Last 30 Days** and **Last 12 Months**, or you can customize a start date and end date by clicking the dates on the calendar.

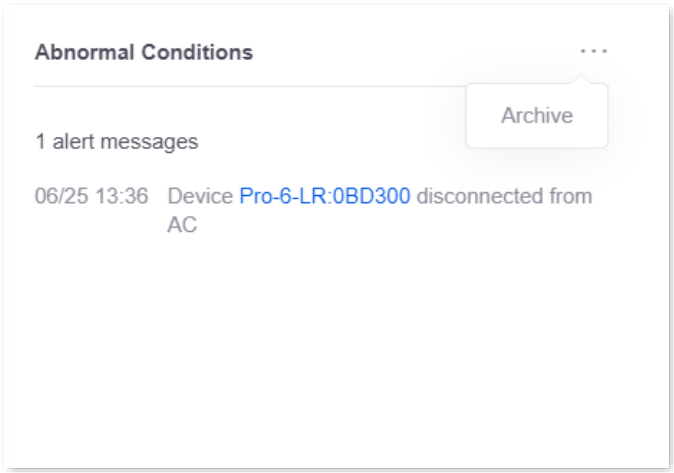
When you place your mouse over the charts, by rolling the mouse wheel up, you can zoom in to get a detailed view. By rolling the mouse wheel down, you can zoom out to get a general view.

If you want to check the statistical details of a specific bar at a specific time point, place your mouse over that bar, and the statistical details will be displayed.

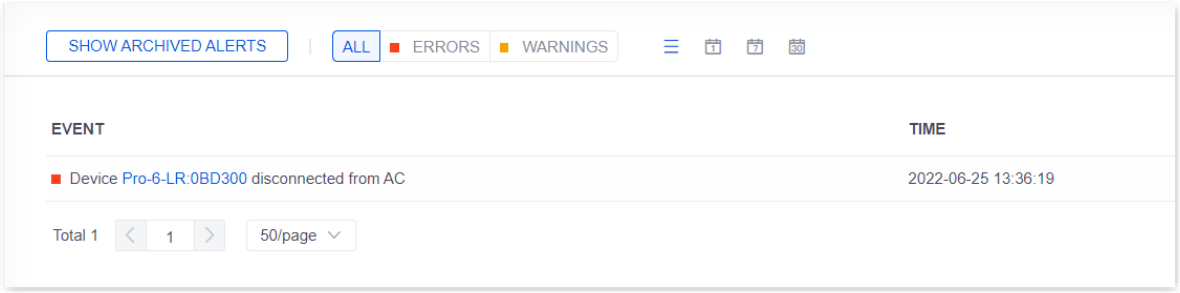


4.5.1 Abnormal Conditions

This module provides an overview of abnormal events of the network. You can check how many alert messages are generated and archive them for maintenance purpose.

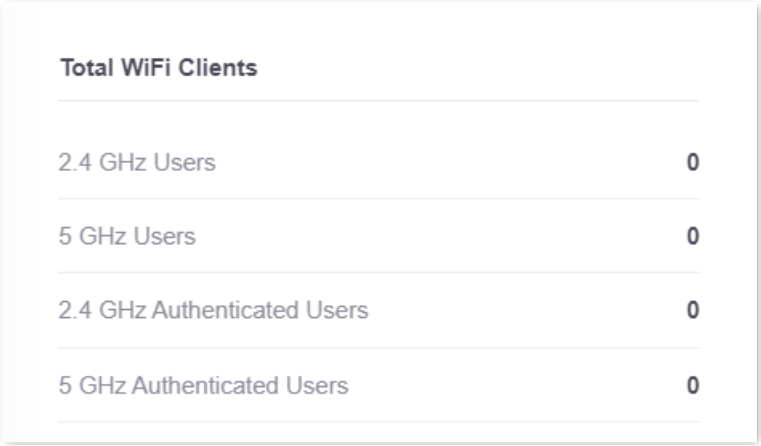


The archived alert messages will be deleted from here, yet you can still view them in the **ALERTS** module. See the following figure.



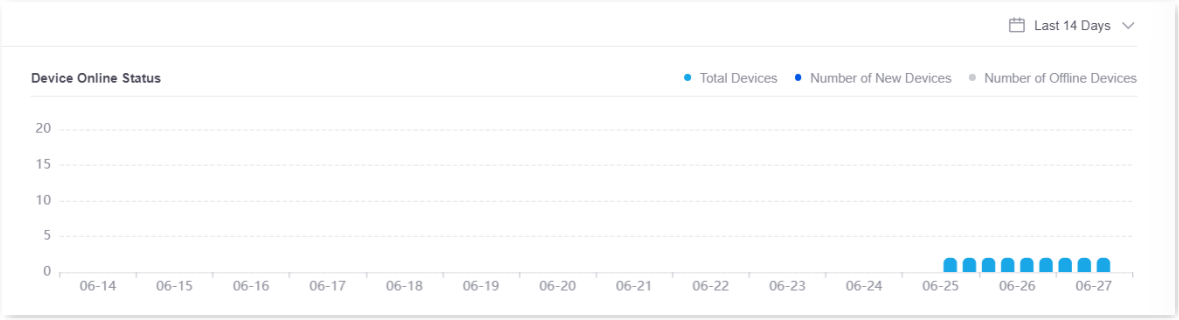
4.5.2 Total WiFi Clients

This module displays the 2.4 GHz and 5 GHz users (non-authenticated) and 2.4 GHz and 5 GHz authenticated users.



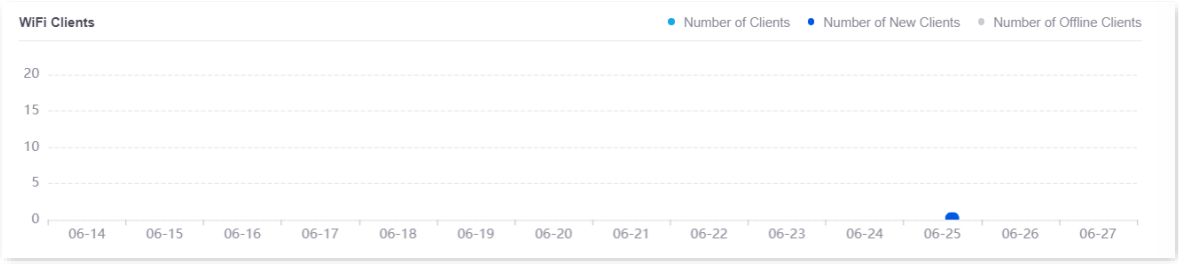
4.5.3 Device Online Status

This module displays the dynamic change of total ProFi devices, new ProFi devices and offline ProFi devices along with time.



4.5.4 WiFi Clients

This module displays the dynamic change of total clients, new clients and offline clients along with time.



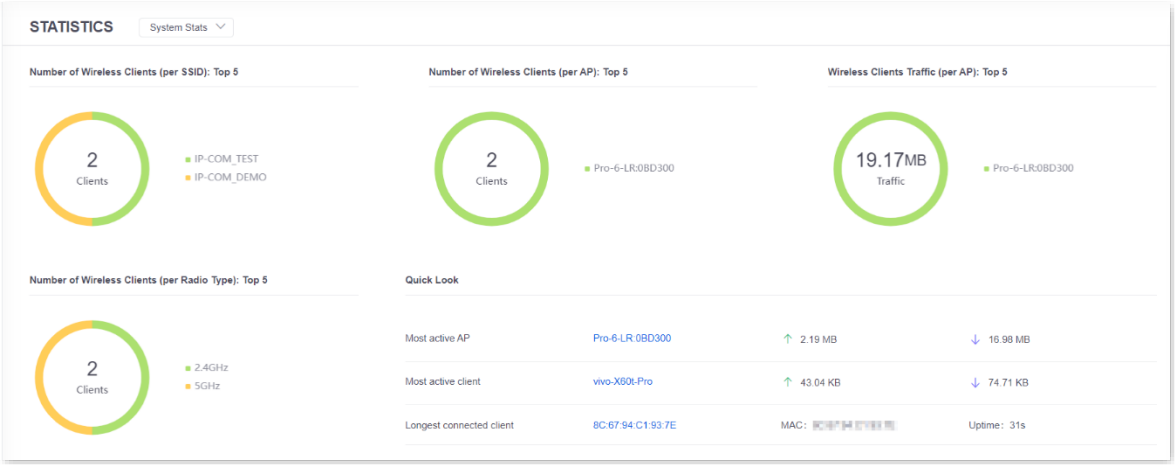
5 Statistics

This page provides a visual representation for **System Stats**, **Performance**, and **Debugging Metrics**. You can select the target item to check its statistics.

To enter the page, choose **Statistics** ( ). See the following figure.

Tip

You can create or edit the wireless networks in the module of **SETTINGS ( )** > **Wireless Networks** or configure the relevant functions corresponding to the specified **AP Details**, then the statistics displayed here will be automatically changed.



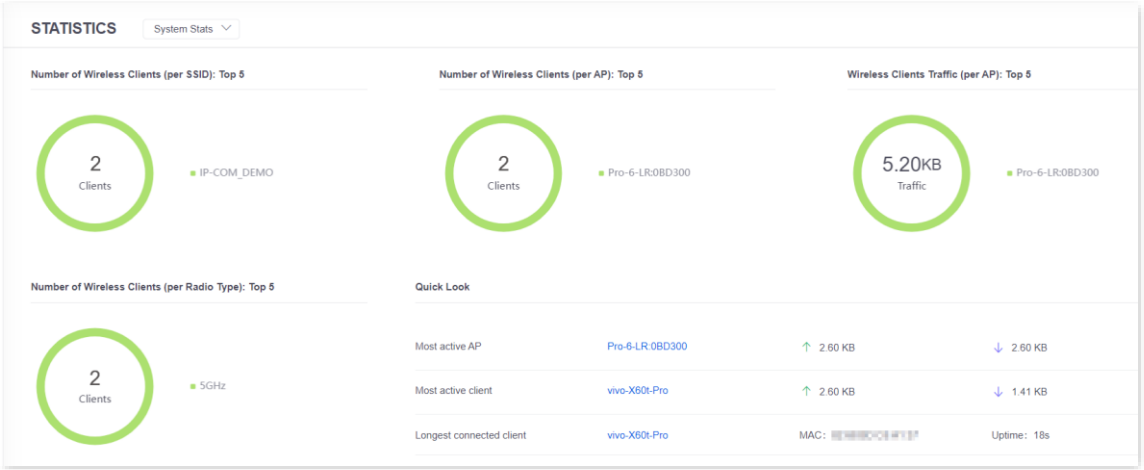
5.1 System Stats

This page displays the general usage statistics of clients and APs with the pie charts, including:

- Number of Wireless Clients (Per SSID): Top 5
- Number of Wireless Clients (Per AP): Top 5
- Wireless Clients Traffic (Per AP): Top 5
- Number of Wireless Clients (Per Radio Type)

For detailed information, you can get a Quick Look of the specified device statistics or examine the Recent Activities of clients.

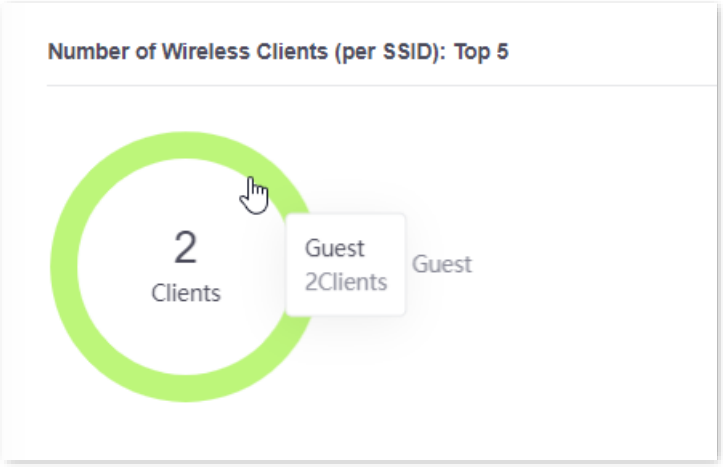
To enter the page, choose **STATISTICS ( )** > **System Stats**. See the following figure.



5.1.1 Number of Wireless Clients (Per SSID): Top 5

This module displays the statistics of the top 5 SSIDs with the largest number of wireless clients up to now.

You can see the total number of wireless clients connected to the top 5 SSIDs. Alternatively, you can place your mouse over the target area to check the corresponding SSID and the number of wireless clients connected to it.

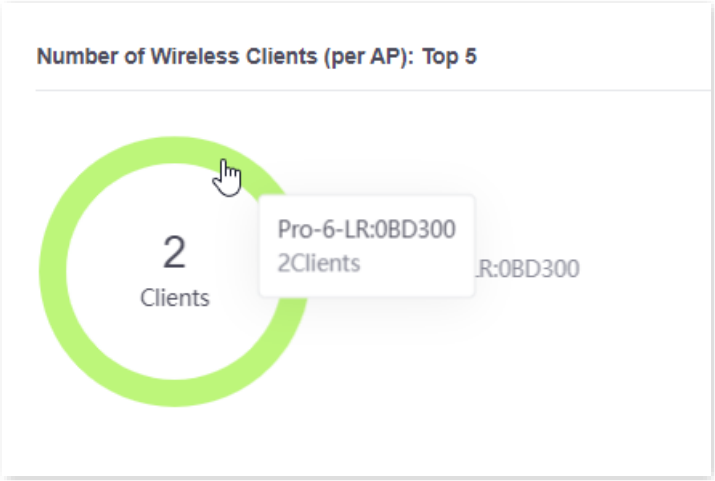


Click the SSID next to the chart, then you can cancel the statistics of the SSID. Click it again, the statistics will be activated again.

5.1.2 Number of Wireless Clients (Per AP): Top 5

This module displays the statistics of the top 5 APs with most connected wireless clients up to now.

You can see the total number of wireless clients connected to the top 5 APs. Alternatively, you can place your mouse over the target AP area to check the corresponding AP name and the number of wireless clients connected to it up to now.

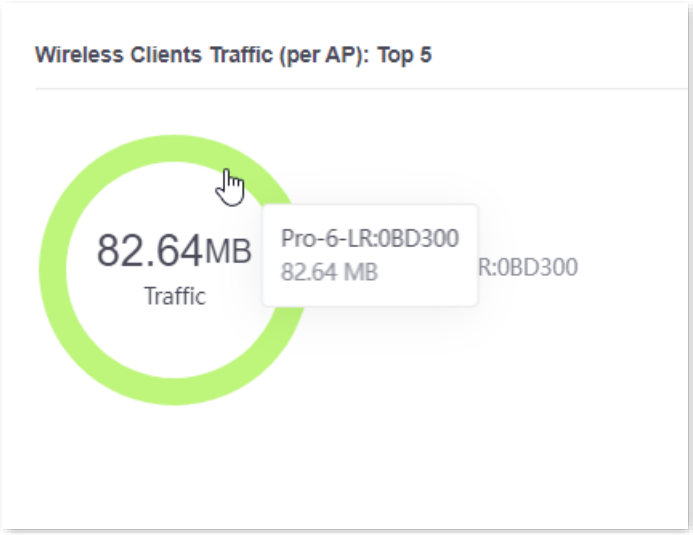


Click the AP next to the chart, then you can cancel the statistics of the AP. Click it again, the statistics will be activated again.

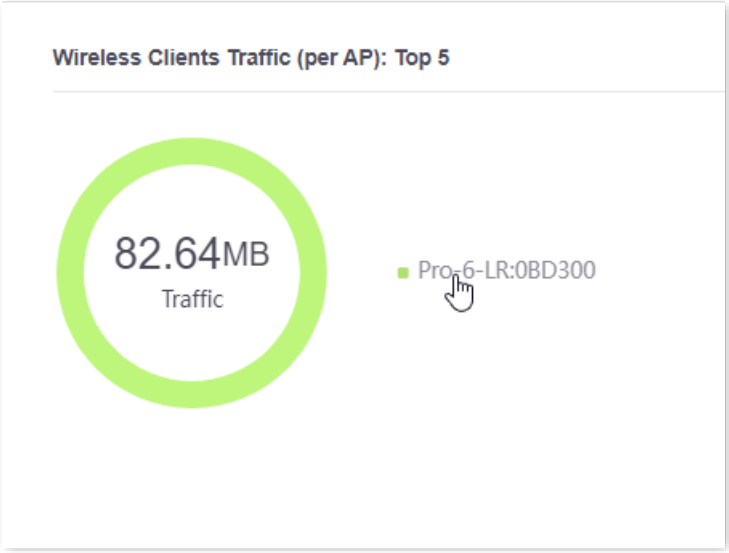
5.1.3 Wireless Clients Traffic (Per AP): Top 5

This module displays the statistics of the top 5 APs with the highest throughput up to now.

You can see the total throughput of the top 5 APs. Alternatively, you can place your mouse over the target AP area to check the corresponding AP name and the throughput it generated up to now.



Click the AP next to the chart, then you can cancel the statistics of the AP. Click it again, the statistics will be activated again.

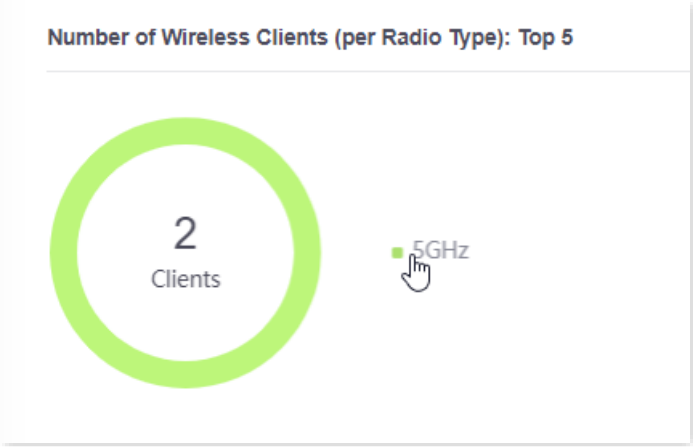


5.1.4 Number of Wireless Clients (Per Radio Type)

This module displays the number of wireless clients connected to each radio type.

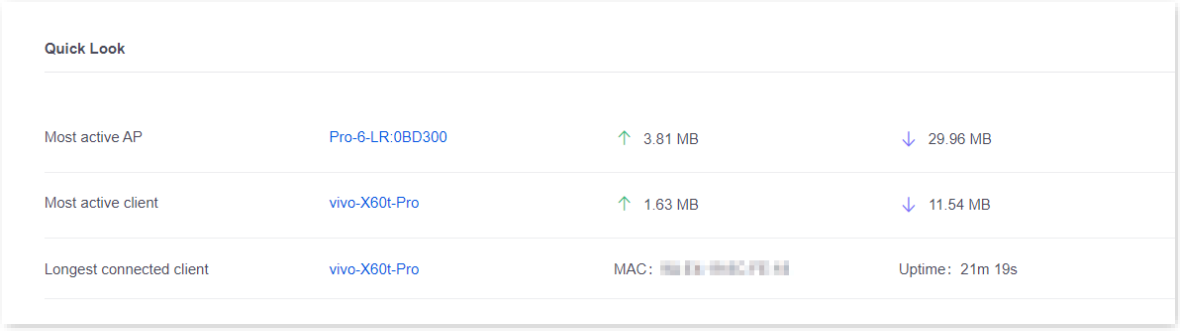
You can see the total number of wireless clients. Alternatively, you can place your mouse over the target area to check the corresponding radio type and the number of wireless clients connected to it.

Click the band next to the chart, then you can cancel the statistics of the band. Click it again, the statistics will be activated again.



5.1.5 Quick Look

This module displays the details of the most active AP, most active client, and the client with the longest connection duration. See the following figure.



- **Most active AP**

  This module displays the name of the AP which generates the highest up and down bytes up to now.

  Click the AP name to expand the details property panel and make more configuration.

- **Most active client**

  This module displays the name of the client which generates the highest up and down bytes up to now. If you never change the client name, its MAC address is displayed by default.

  Click the name or MAC address to expand the details panel and make more configuration.

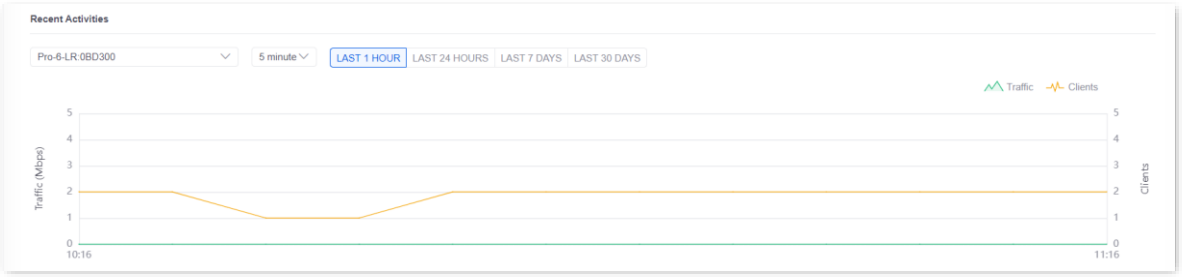
- **Longest connected client**

  - **(Name or MAC address)**: specifies the name or MAC address of the client with the longest connection duration.
  - **MAC**: specifies the MAC address of the client with the longest connection duration.
  - **Uptime**: specifies the duration the client has been connected.

  Click the name or MAC address to expand the details panel and make more configuration.

5.1.6 Recent Activities

This module displays the statistics of the connected client number and throughput of a single AP over time. See the following figure.



Window elements description

Element	Description
(AP name: MAC address)	It specifies the name and last six digits of MAC address of the AP. You can click the drop-down menu to select the AP whose statistics you want to check.
(Interval)	It specifies the duration interval of the X-axis. You can choose **5 minutes**, **Hourly**, and **Daily**. The default interval is **5 minutes**.
(Duration)	It specifies the total time duration of the X-axis. You can choose **LAST 1 HOUR**, **LAST 24 HOURS**, **LAST 7 DAYS**, and **LAST 30 DAYS**.
Traffic	It specifies the network traffic during the selected time period. Place the mouse over a specific time point to view its traffic value.
Clients	It specifies the number of connected clients during the selected time period. Place the mouse over a specific time point to view the number of clients.

5.2 Performance

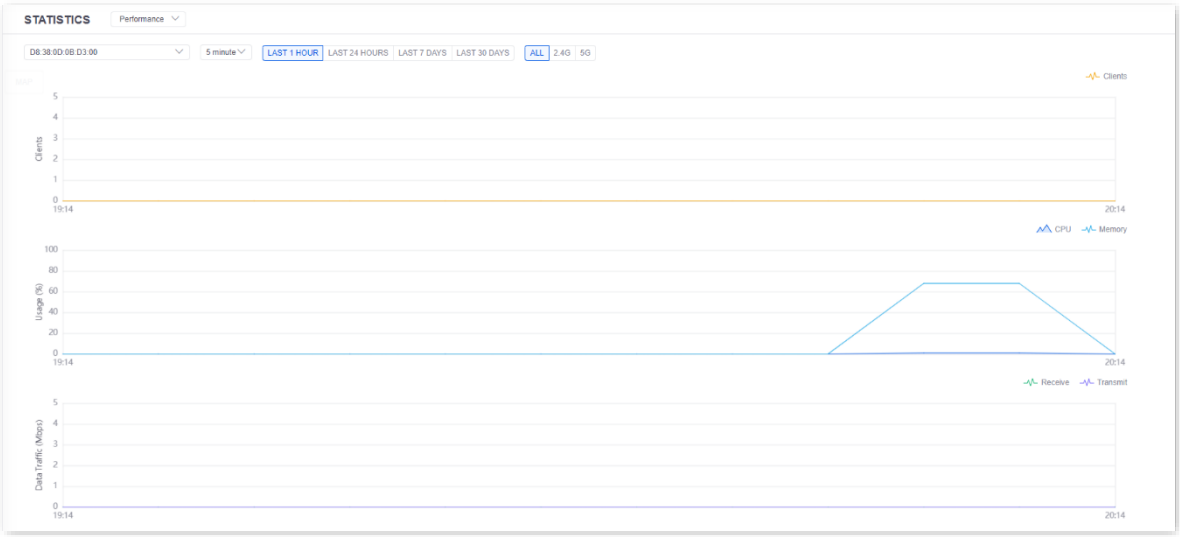
This page displays the statistics related to AP performance including the number of wireless clients, CPU and memory usage, and data traffic.

Here, you can apply the following headers to view specified information:

- (MAC address): It specifies the MAC address of the AP. You can click the drop-down menu to select the AP whose statistics you want to check.
- (Interval): It specifies the interval of the X-axis. You can choose **5 minutes**, **Hourly**, and **Daily**. The default interval is **5 minutes**.
- (Duration): It specifies the total time duration of the X-axis. You can choose **LAST 1 HOUR**, **LAST 24 HOURS**, **LAST 7 DAYS**, and **LAST 30 DAYS**.
- ALL/2.4G/2.5G: It specifies the radio band of the AP. You can choose **2.4G**, **5G** or **ALL** bands.

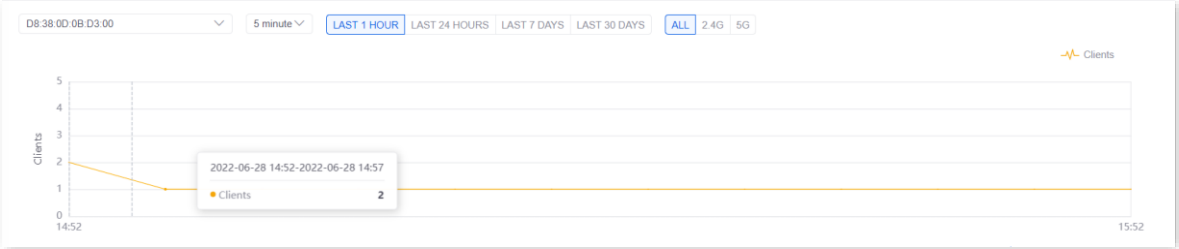
If you want to check the statistical details of a specific bar at a specific time point, place your mouse over that bar, and the statistical details will be displayed.

To enter the page, choose **STATISTICS (** **)** > **Performance**. See the following figure.



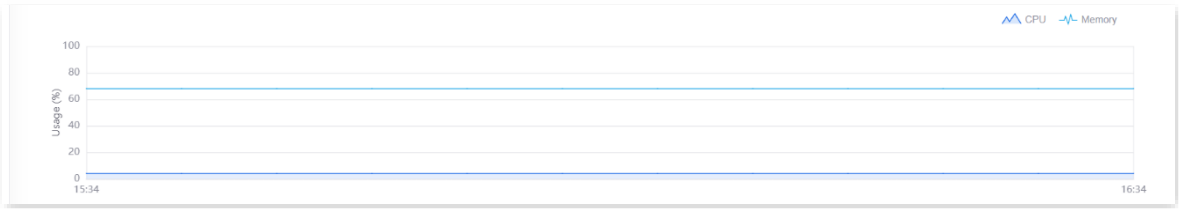
5.2.1 Number of Wireless Clients

This module displays the number of wireless clients connected to the selected AP over time. See the following figure.



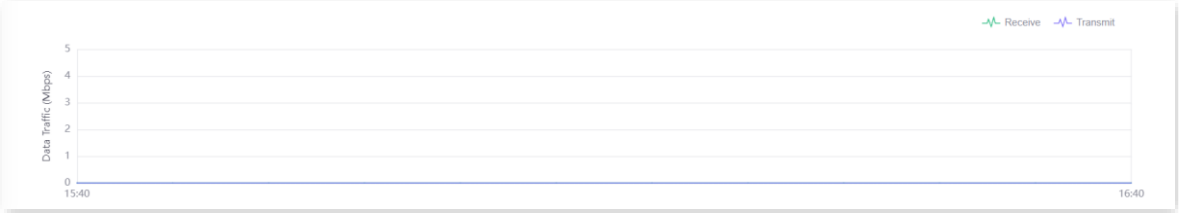
5.2.2 CPU and Memory Usage

This module displays the CPU and memory usage rate of the selected AP over time. See the following figure.



5.2.3 Data Traffic

This module displays the received and transmitted data traffic of the selected AP over time. See the following figure.

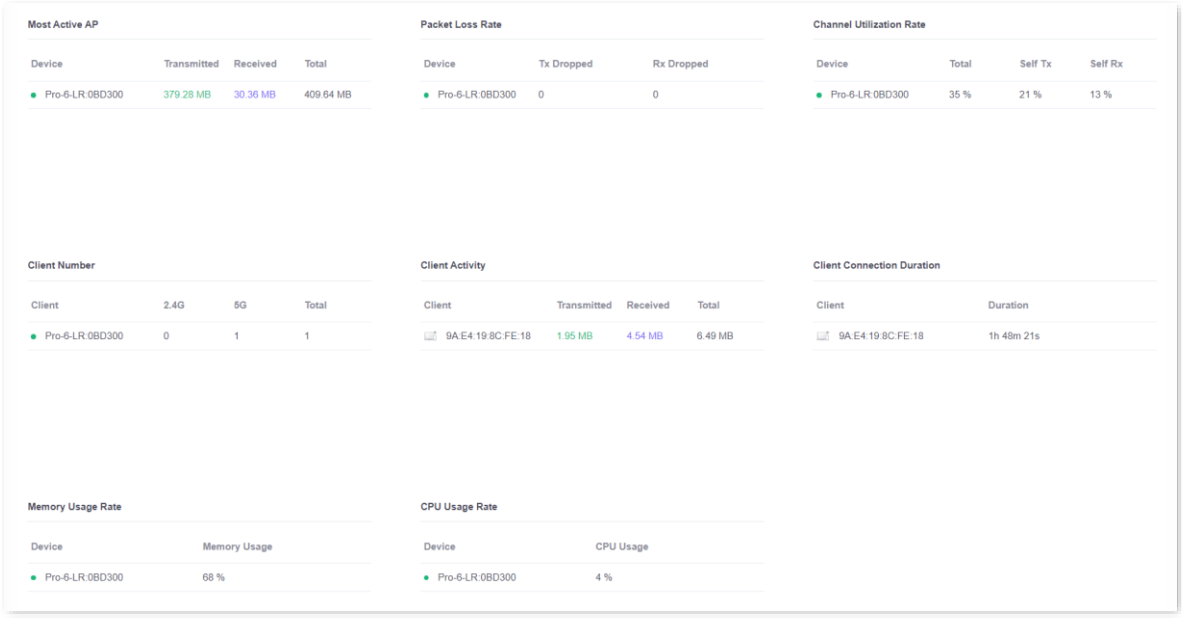


5.3 Debugging Metrics

This page displays the following statistics related to network commissioning:

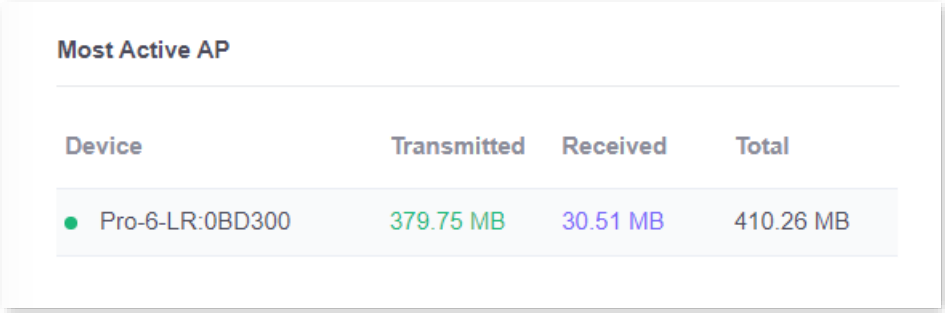
- Most Active AP
- Packet Loss Rate
- Channel Utilization Rate
- Client Number
- Client Activity
- Client Connection Duration
- Memory Usage Rate
- CPU Usage Rate

To enter the page, choose **STATISTICS ( )** > **Debugging Metrics**. See the following figure.



5.3.1 Most Active AP

This module displays the top 5 APs with the largest throughput. See the following figure.

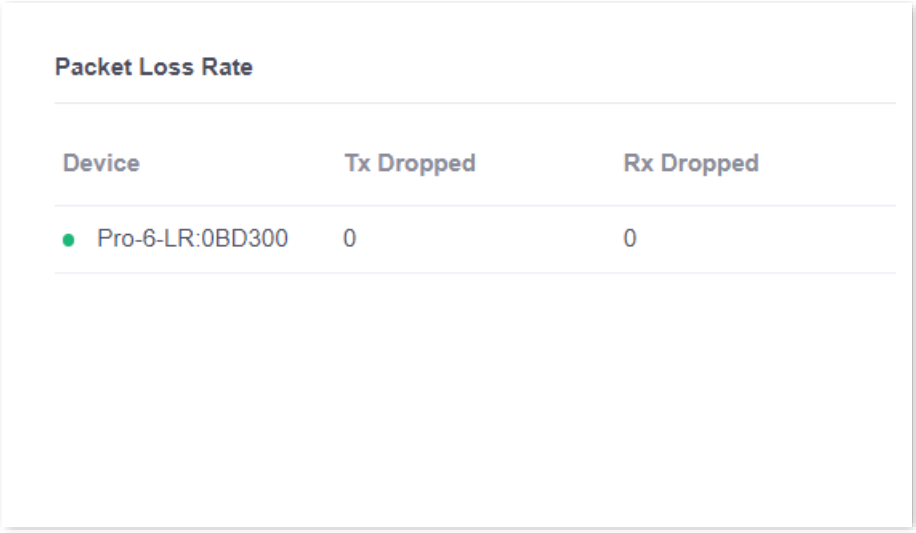


Parameter description

Parameter	Description
Device	It specifies the name and last six digits of the MAC address of the AP. You can specify it at AP Details.
Transmitted	It specifies the amount of data transmitted using the selected radio band.
Received	It specifies the amount of data received using the selected radio band.
Total	It specifies the amount of data transmitted and received using the selected radio band.

5.3.2 Packet Loss Rate

This module displays the top 5 APs with the largest packet loss rate. See the following figure.

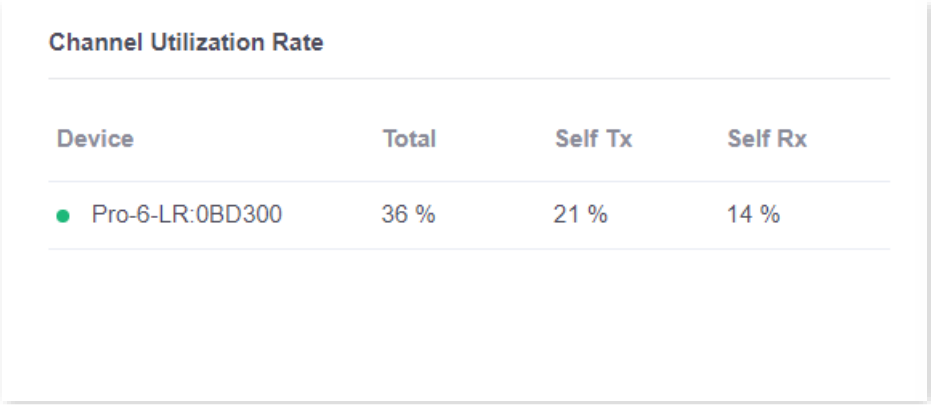


Parameter description

Parameter	Description
Device	It specifies the name and last six digits of the MAC address of the AP. You can specify it at AP Details.
Tx Dropped	It specifies the current transmission packet loss rate of the AP.
Rx Dropped	It specifies the current receiving packet loss rate of the AP.

5.3.3 Channel Utilization Rate

This module displays the top 5 APs with the largest channel utilization rate. See the following figure.

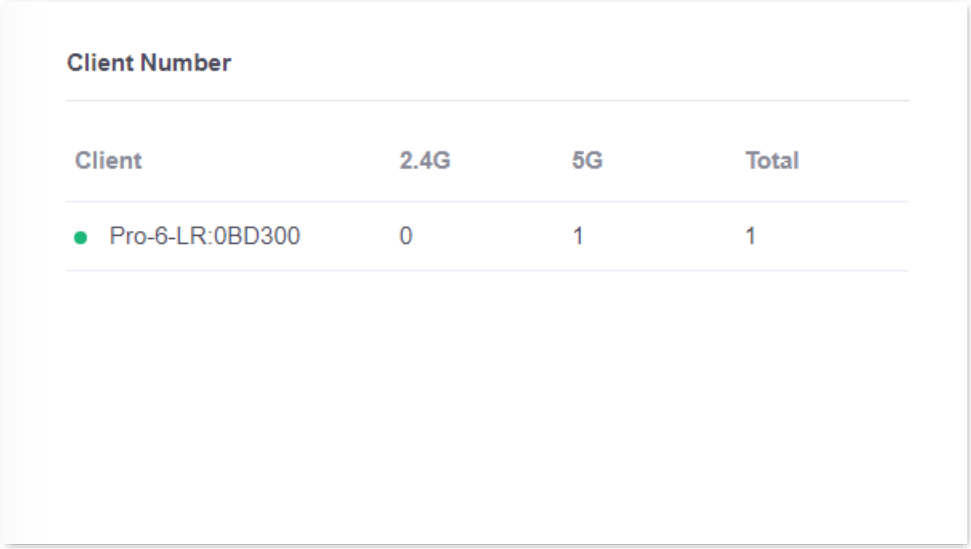


Parameter description

Parameter	Description
Device	It specifies the name and last six digits of the MAC address of the AP. You can specify it at AP Details.
Total	It specifies the total current channel utilization rate of the AP.
Self Tx	It specifies the current channel utilization rate of the AP at the transmitting direction.
Self Rx	It specifies the current channel utilization rate of the AP at the receiving direction.

5.3.4 Client Number

This module displays the top 5 APs with the largest number of clients, which are divided into 2.4G and 5G.

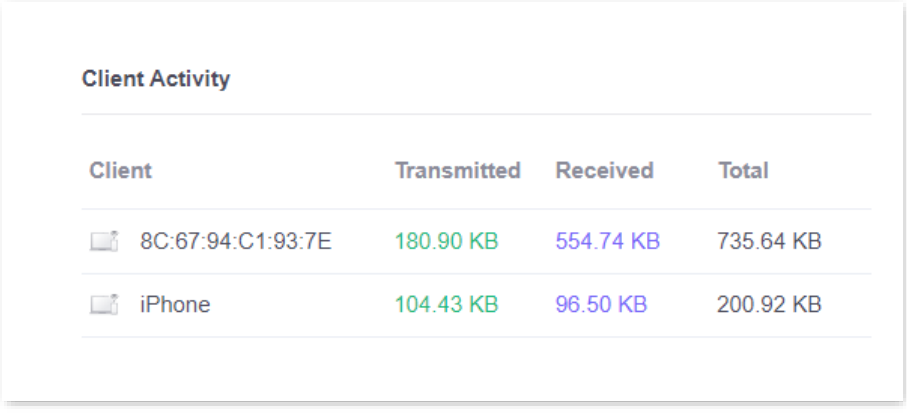


Parameter description

Parameter	Description
Client	It specifies the name and last six digits of the MAC address of the AP. You can specify it at AP Details.
2.4G	It specifies the number of clients currently connected to the 2.4G band of the AP.
5G	It specifies the number of clients currently connected to the 5G band of the AP.
Total	It specifies the total number of clients currently connected to both 2.4G and 5G bands of the AP.

5.3.5 Client Activity

This module displays the top 5 wireless clients with the highest traffic in total for transmission and reception. See the following figure.

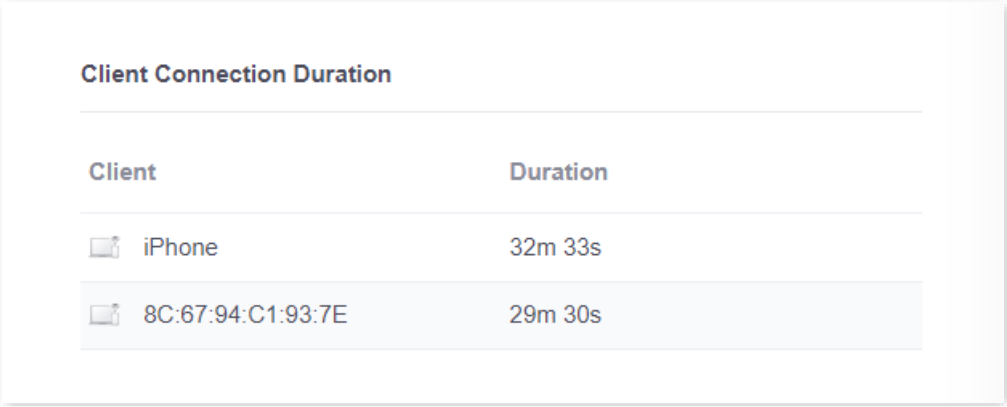


Parameter description

Parameter	Description
Client	It specifies the name of the client.
Transmitted	It specifies the data traffic transmitted by the client.
Received	It specifies the data traffic received by the client.
Total	It specifies the total data traffic transmitted and received by the client.

5.3.6 Client Connection Duration

This module displays the top 5 wireless clients with the longest connection duration. See the following figure.

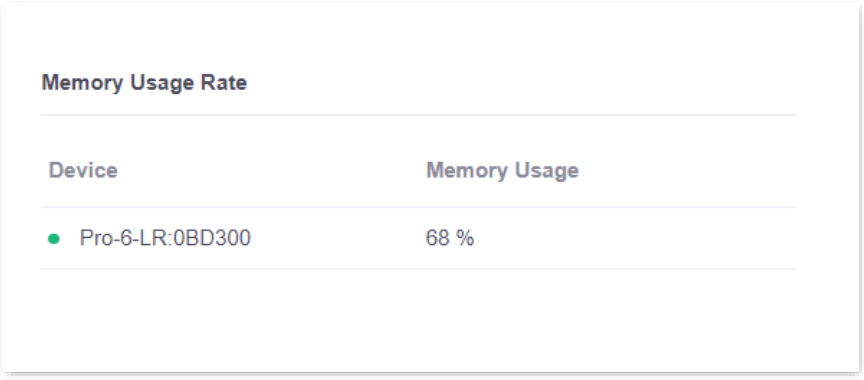


Parameter description

Parameter	Description
Client	It specifies the name of the client.
Duration	It specifies the duration of time since the client has been connected to the AP.

5.3.7 Memory Usage Rate

This module displays the top 5 APs with the highest percentage of memory usage.

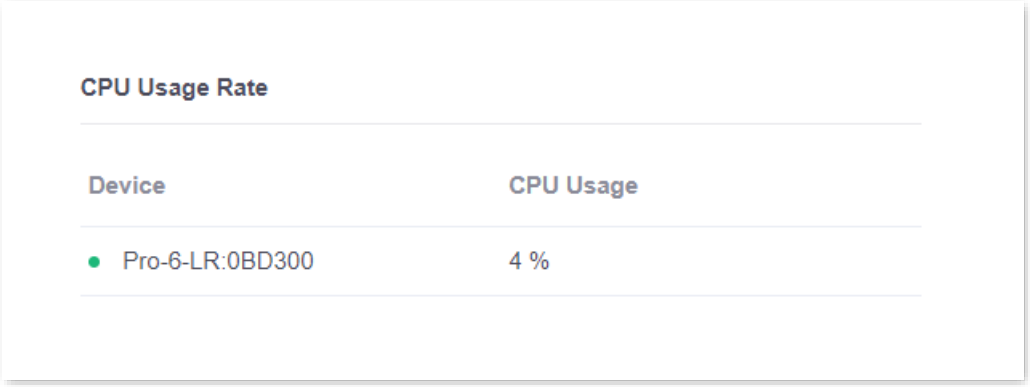


Parameter description

Parameter	Description
Device	It specifies the name of the AP.
Memory Usage	It specifies the memory usage rate of the AP.

5.3.8 CPU Usage Rate

This module displays the top 5 APs with the highest percentage of CPU usage. See the following figure.



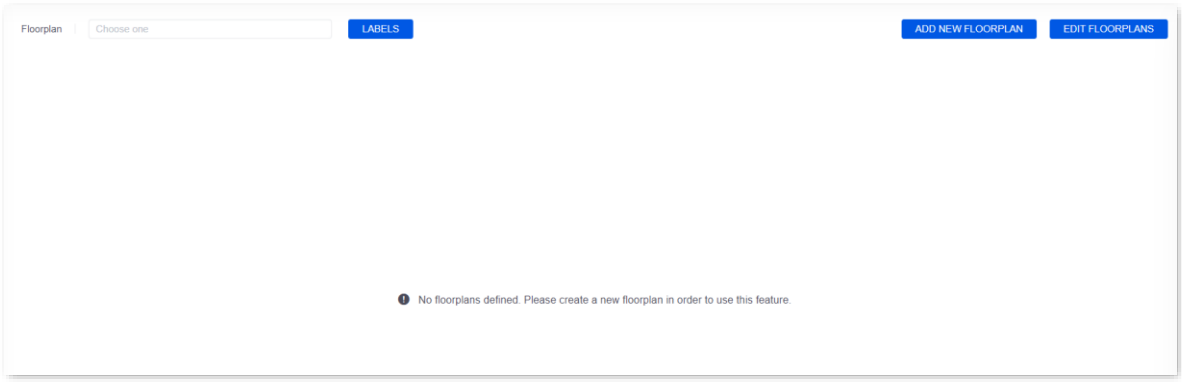
Parameter description

Parameter	Description
Device	It specifies the name of the AP.
CPU Usage	It specifies the CPU usage rate of the AP.

6 Map

This page provides a visual representation for the networks of your sites. You can upload custom map images of your site locations and drag the adopted ProFi devices to the target spots on your maps.

To enter the page, choose **MAP** ( ). See the following figure.

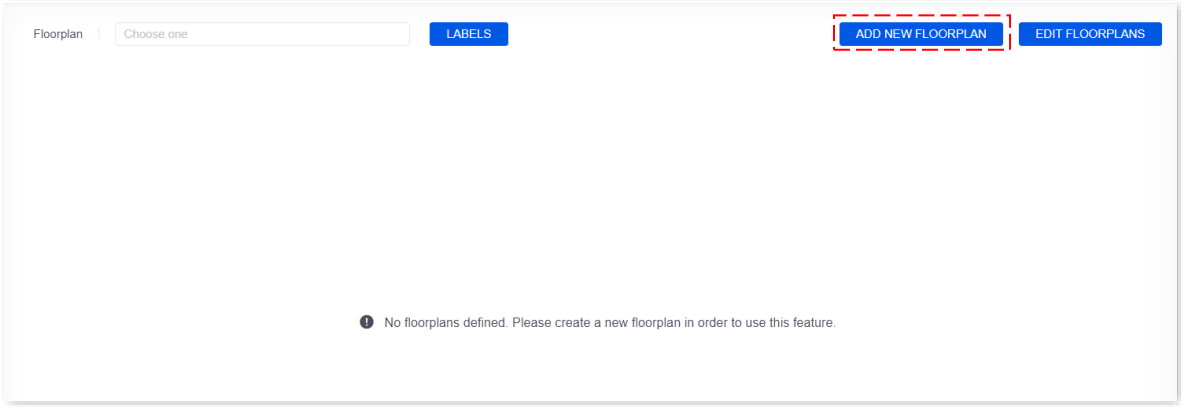


6.1 Add Custom Maps

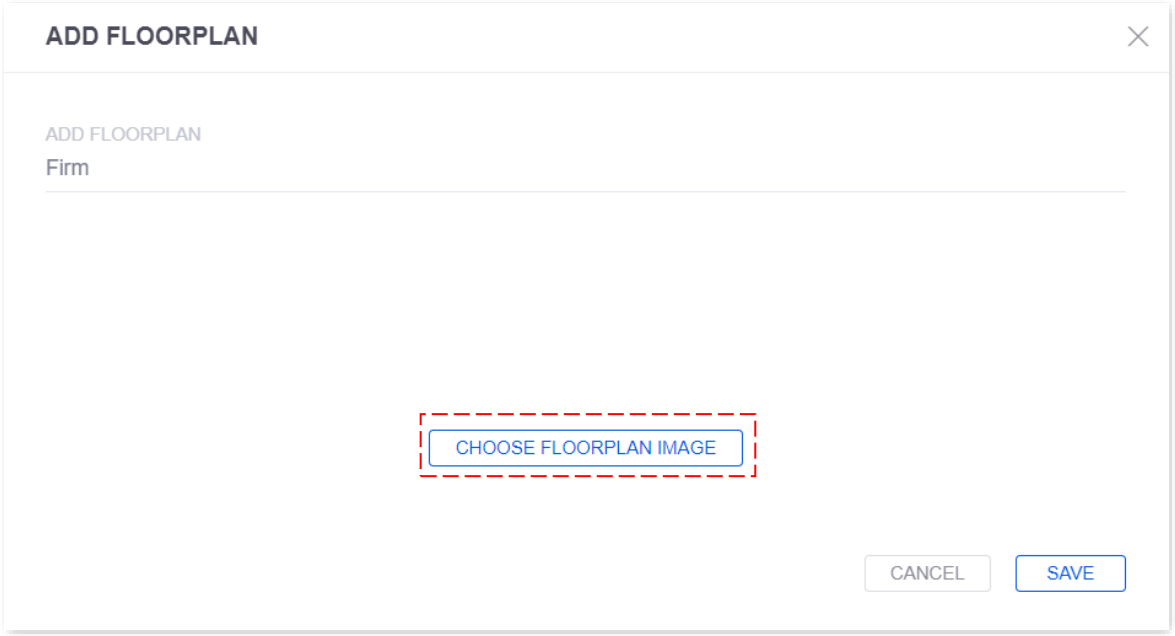
To add a custom map, you need to first create an image in .png, .jpg, or .jpeg format.

After you have created the map, you can upload it to the ProFi Software Controller. Refer to the following procedures.

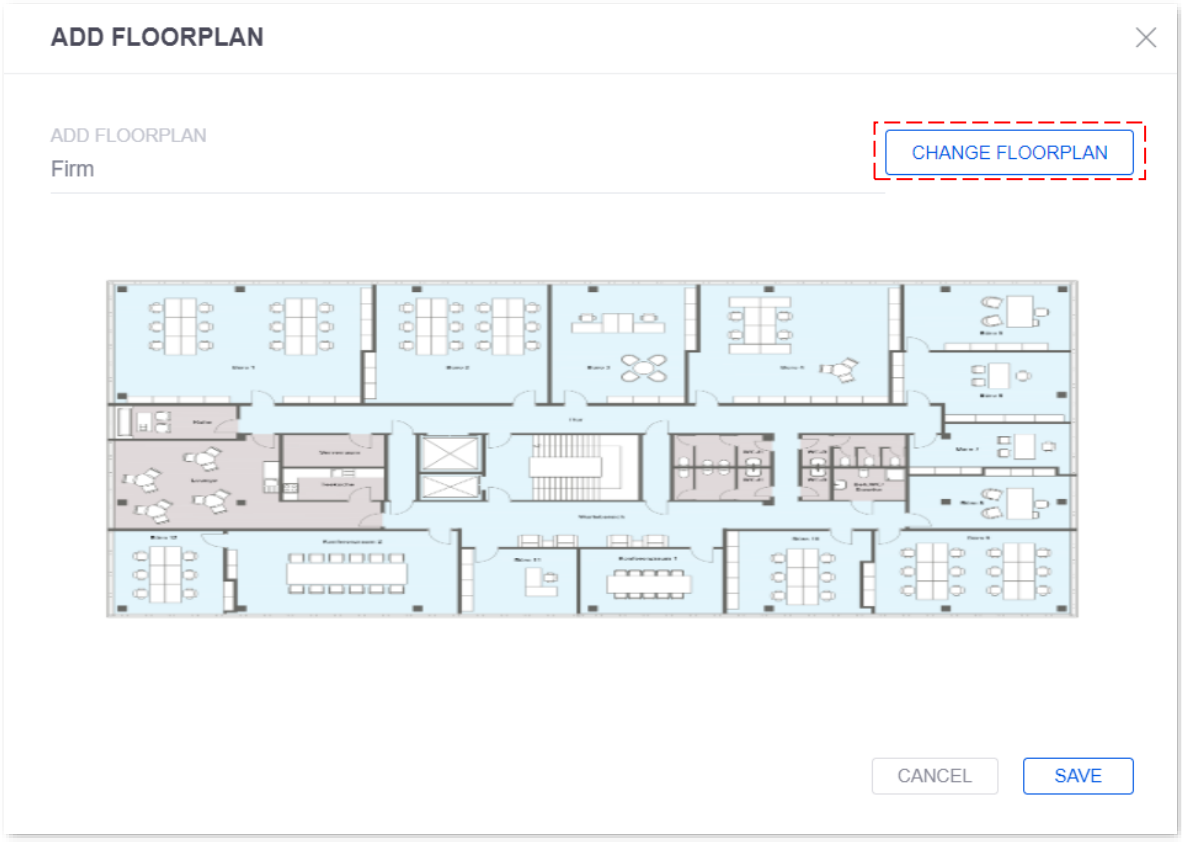
1. Click **ADD NEW FLOORPLAN**.



2. Set a floorplan name in the **Add Floorplan** field, which is **Firm** in this example.
3. Click **CHOOSE FLOORPLAN IMAGE** and choose the map image you created.



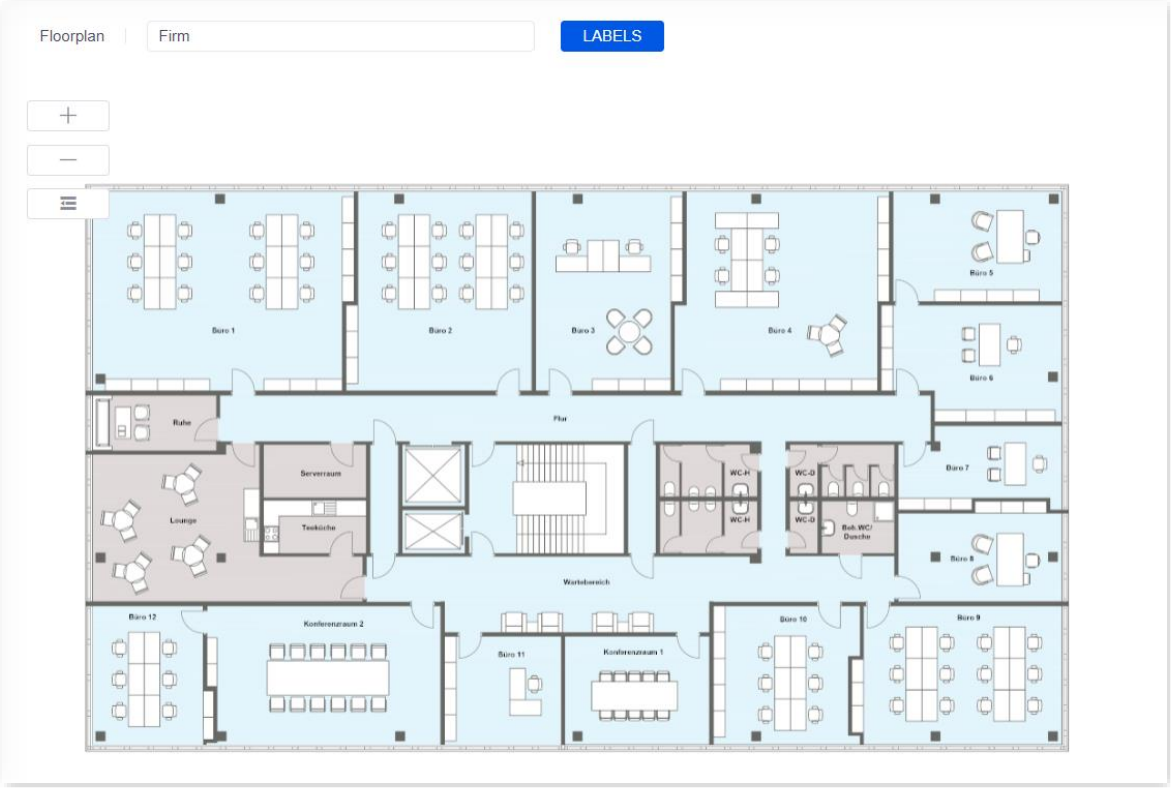
4. (Optional) If you want to change to another floorplan, click **CHANGE FLOORPLAN** and choose the map image you want.



5. Click **SAVE**.

----End

The custom map image is added successfully. See the following figure.

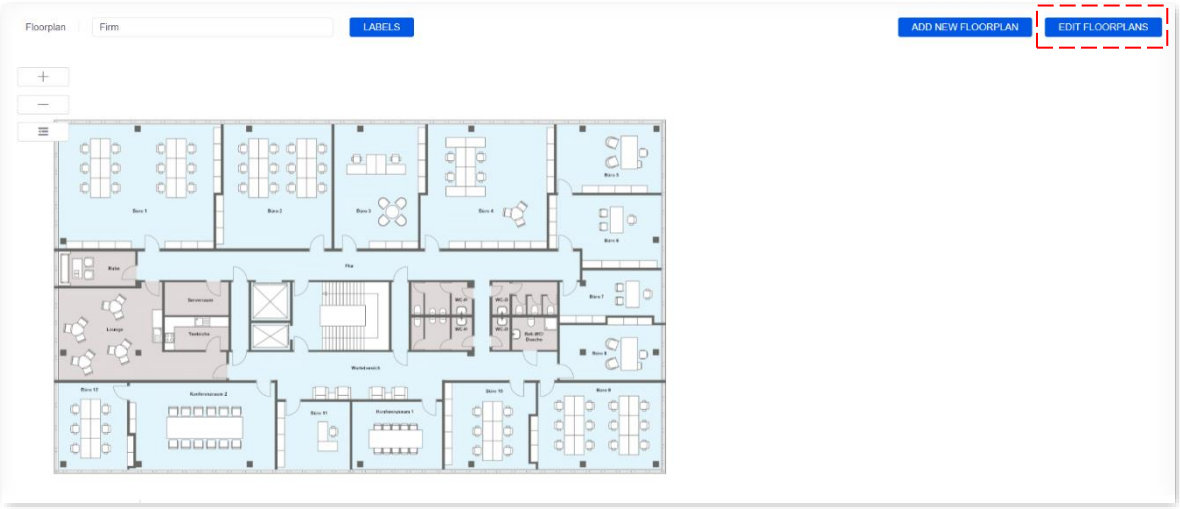


6.2 Edit a Map

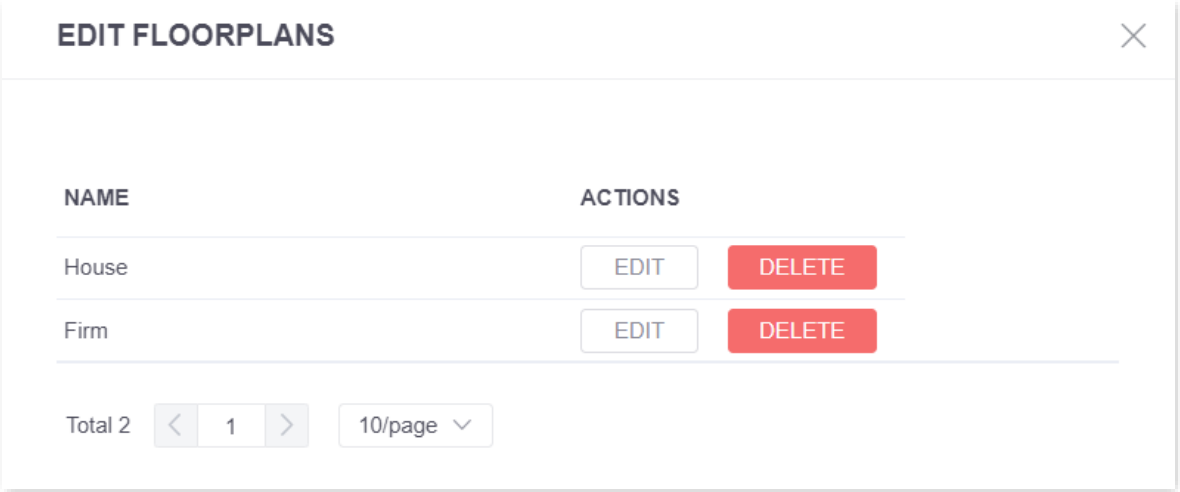
You can edit or delete a map.

Refer to the following procedures.

1. Click **EDIT FLOORPLANS**.



2. Perform the actions you want to do on the target floorplans.
   - Click **EDIT** to make changes.
   - Click **DELETE** to remove the floorplan.



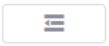
----End

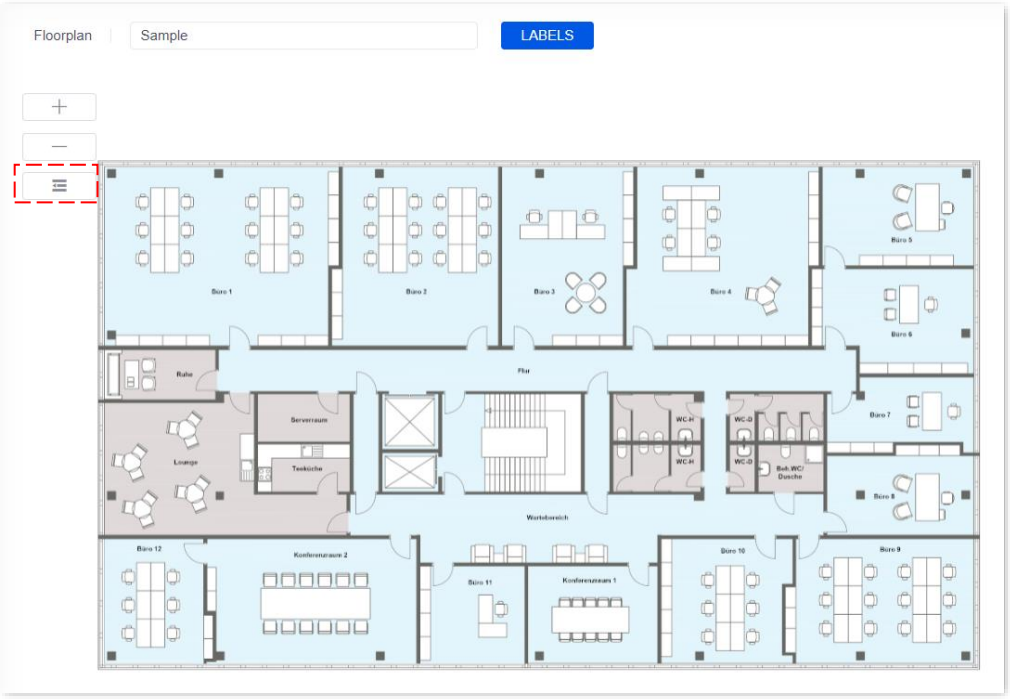
6.3 Place Devices on the Map

You can drag adopted ProFi devices onto the map you designated.

Refer to the following procedures.

1. Click the drop-down menu beside **Floorplan** to select the target floorplan.

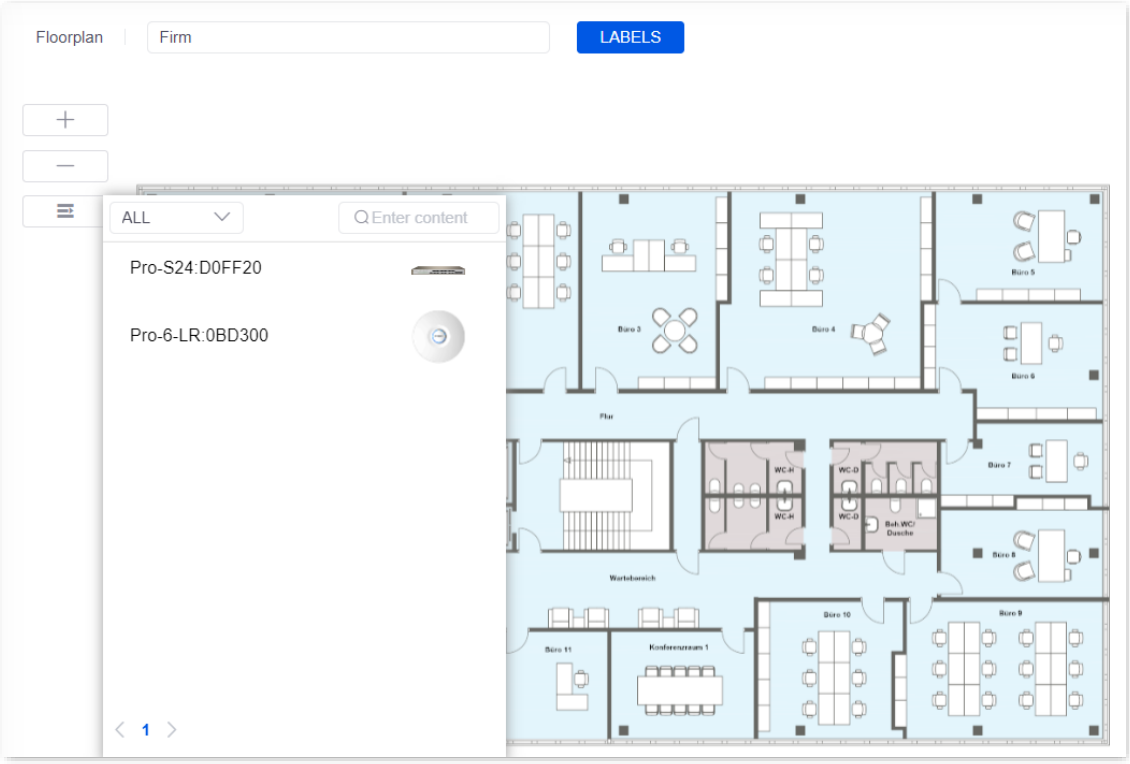
2. Click  at the middle left on the page.



3. Drag each ProFi device from the appeared list to the appropriate location on the map. In addition, you can search for the target device in the search box or select the target type of devices from the **ALL** drop-down menu for quick device locate.

Note

If you cannot drag and drop a device, ensure that you are logging in as a super administrator or an administrator.

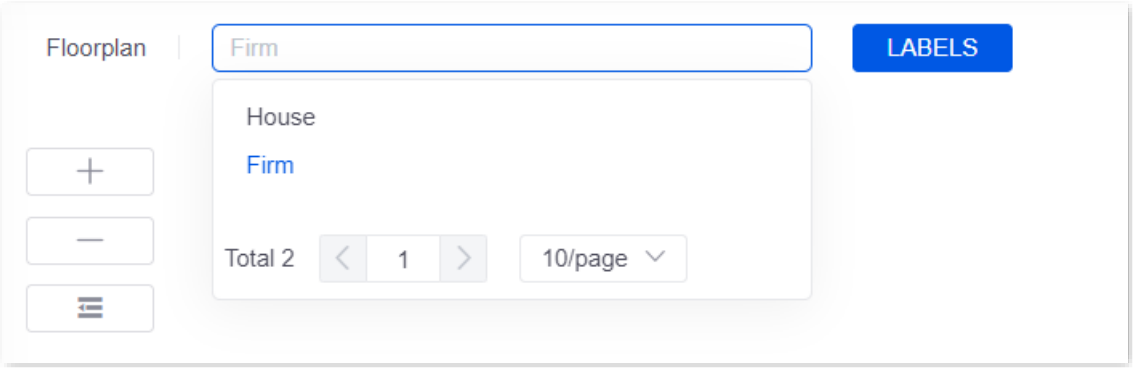


----End

Each device appears on the spot where you dropped it.

6.4 Map Display Options

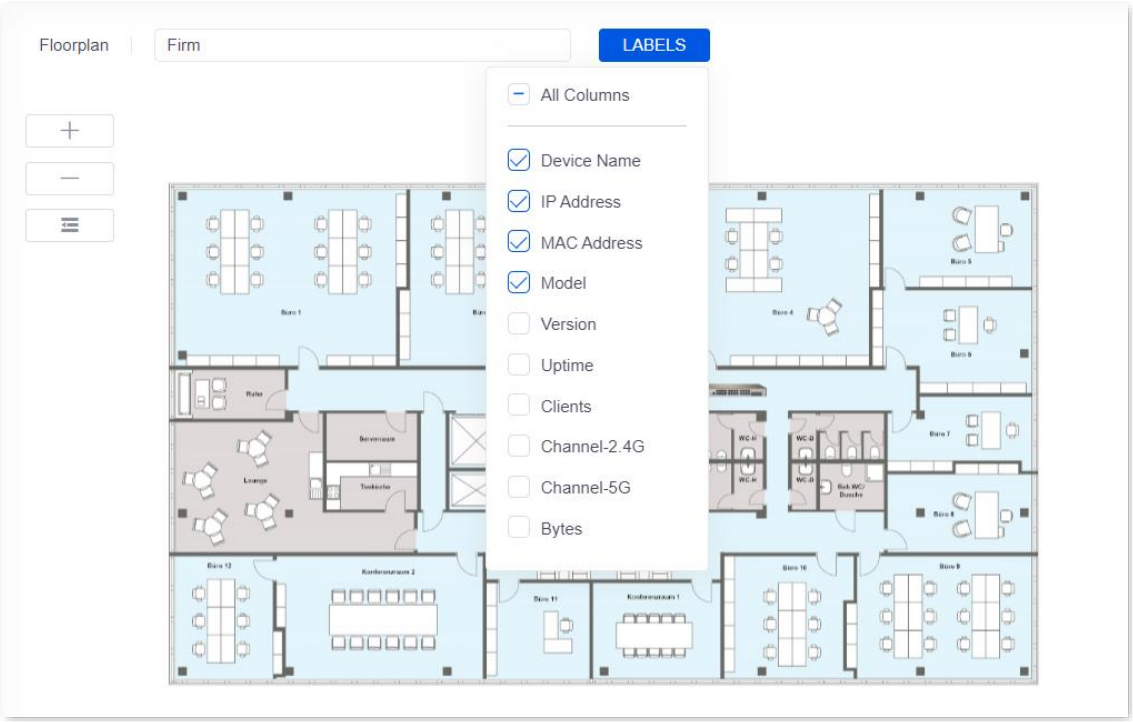
If you uploaded multiple map images, you can select which map is to be displayed from the drop-down menu or search for keywords in the search box.



Each ProFi device is displayed with its device name, IP address, MAC address and model by default. Other labels you can choose include version, uptime, clients, channel-2.4G, channel-5G, and bytes. You can also check **All Columns** to select or deselect all labels.

Tip

After dragging a ProFi device to the floorplan, you can place the mouse over the device icon to view the labels mentioned above.



6.5 Additional Options

The left side of the map page offers the following options.

Zoom Slider: Used to zoom the map detail in and out.

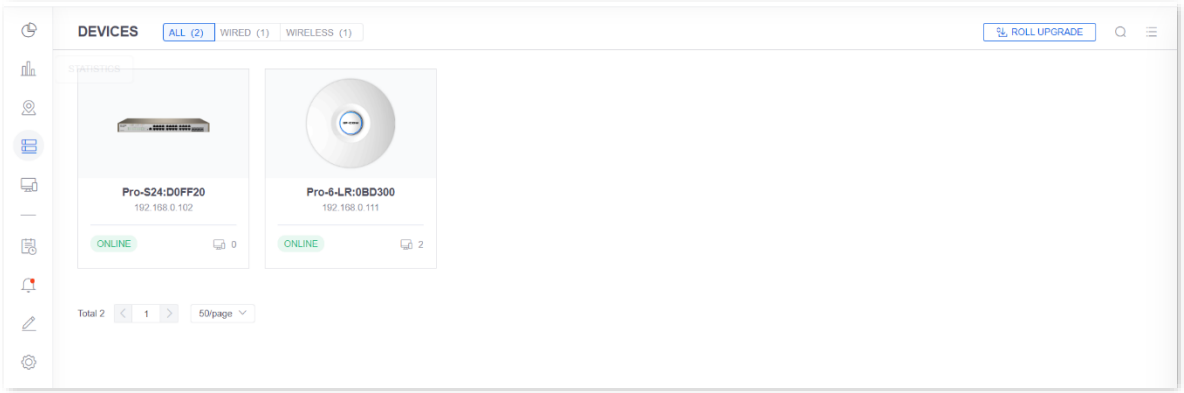
Unplaced Devices: Drag each unplaced device icon from the list to the target spot on the map. (This action requires super administrator or administrator access)

7 Devices

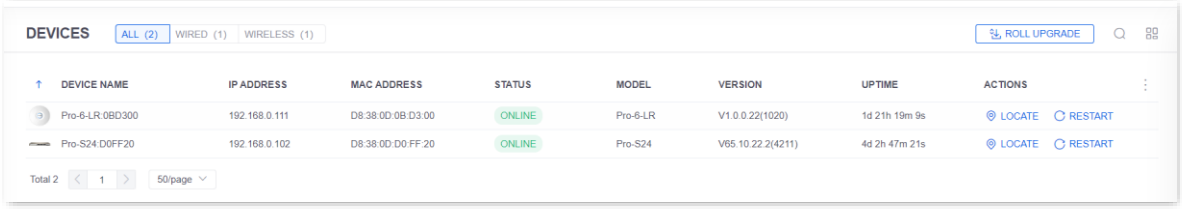
This page displays all the ProFi devices detected by the ProFi Software Controller.

The Controller only supports ProFi APs and switches by now.

To enter the page, choose **DEVICES** ( ). See the following figure.



By default, devices are displayed in a spread-out form ( ) as shown above. Click in the upper right corner to display the devices in a list as shown below.



Filter Target Device Type

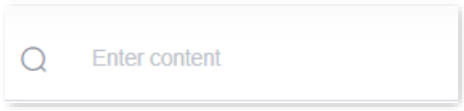
- **ALL**: displays all the ProFi devices.
- **WIRED**: displays all the ProFi switches.
- **WIRELESS**: displays all the ProFi APs.

Device Display Options

Click it to display ProFi devices in a list.

Click it to display ProFi devices in a spread-out form.

Search Devices



Enter keywords to easily search for and filter out target contents.

Sort Devices

Click any column header to sort the devices in an ascending or descending order displayed as ↑ or ↓.

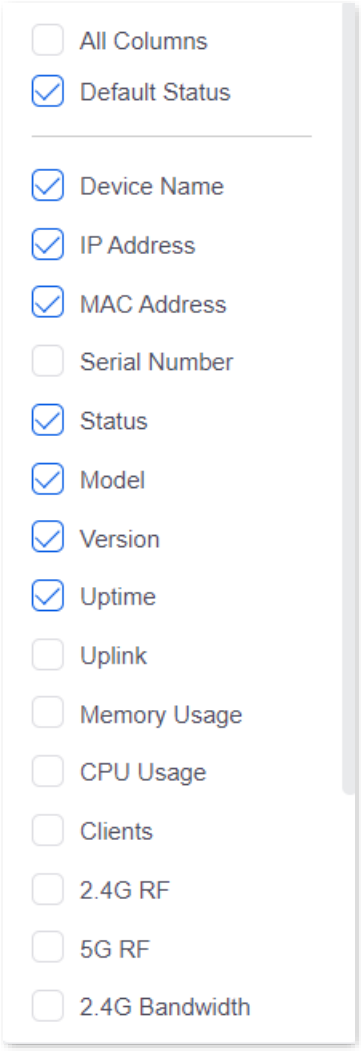
Customize Columns

Click ⋮ in the farthest right of the column header to customize columns.

The following figure displays columns customizable for ProFi APs and switches.

Tip

If a device does not support certain column, - will be shown in the list.



Column description

Parameter	Description
Default Status	Select it to display the ProFi devices in default columns.
Device Name	It specifies the icon and name of the ProFi device.
IP Address	It specifies the IP address of the ProFi device.
MAC Address	It specifies the physical address of the LAN port of the ProFi device.
Serial Number	It specifies the production serial number of the ProFi device.

Parameter	Description
Status	It specifies the status of ProFi devices. Possible statuses include: – **ONLINE:** The ProFi device is managed by the ProFi Software Controller and connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. – **OFFLINE:** The ProFi device is managed by the ProFi Software Controller but not connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. – **CONNECTED (DISABLED):** The ProFi device is managed by the ProFi Software Controller and connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site, but is disabled now. This status is only for ProFi APs. – **OFFLINE (DISABLED)**: The ProFi device is managed by the ProFi Software Controller but not connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site, but is disabled now. This status is only for ProFi APs. – **ONLINE (WIRELESS)**: It specifies the ProFi device connecting to the ProFi Software Controller through bridging. Such ProFi device is managed by the ProFi Software Controller and connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. This status is only ProFi APs. – **PENDING ADOPTION:** The ProFi device is waiting to be managed by the ProFi Software Controller and the site to which it belongs is not determined. – **ADOPTING:** The ProFi device management is under way. – **PROVISIONING:** The ProFi device is synchronizing its configurations with those delivered by the ProFi Software Controller. – **MANAGED BY OTHER:** The ProFi device is managed by another ProFi Software Controller. – **RESTARTING:** The ProFi device is restarting. – **UPGRADING:** The ProFi device is upgrading.
Model	It specifies the device model of the ProFi device.
Version	It specifies the software version of the ProFi device.
Uptime	It specifies the duration the ProFi device has been running.
Uplink	It specifies the name of the uplink device of the ProFi device.
Memory Usage	It specifies the real time memory usage of the ProFi device.
CPU Usage	It specifies the real time CPU usage of the ProFi device.
Clients	It specifies the total number of the clients connected to the ProFi device.
2.4G RF	It specifies the channel and the transmitted power ProFi AP utilizes in the 2.4 GHz radio band.
5G RF	It specifies the channel and the transmitted power ProFi AP utilizes in the 5 GHz radio band.

Parameter	Description
2.4G Channel Bandwidth	It specifies the channel bandwidth ProFi AP utilizes in the 2.4 GHz radio band.
5G Channel Bandwidth	It specifies the channel bandwidth ProFi AP utilizes in the 5 GHz radio band.
2.4G Clients	It specifies the number of the clients connected to the 2.4 GHz wireless networks of the ProFi AP.
5G Clients	It specifies the number of the clients connected to the 5 GHz wireless networks of the ProFi AP.
WLAN-2.4G	It specifies the wireless networks in the 2.4 GHz radio band of the ProFi AP.
WLAN-5G	It specifies the wireless networks in the 5 GHz radio band of the ProFi AP.

Device Adoption

The ProFi Software Controller can automatically detect all ProFi devices in the LAN. You can add detected ProFi devices to the default project upon first login. Or, after the first login, add newly detected ProFi devices to certain project in the device list.

In the device list,

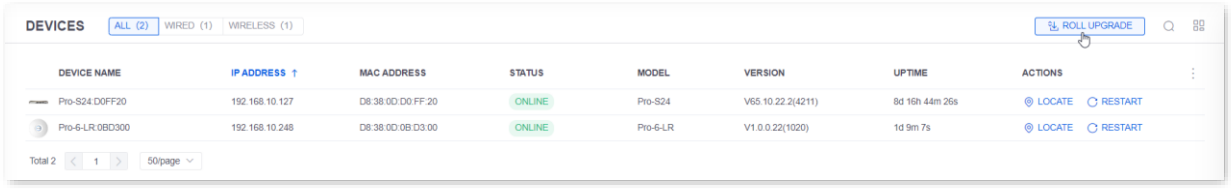
- The status of **Pending Adoption** means the device is waiting to be managed by the controller and the site to which it belongs is not determined. You can click **Manage** to add the device to a specific site under the controller.
- The status of **MANAGED BY OTHER** means the device is managed by another controller. You can click **Manage** and enter such controller's username and password to add the device to a specific site under the controller.

Statuses other than **PENDING ADOPTION** and **MANAGED BY OTHER** mean the device is already managed, being managed or cannot be managed by a controller now.

Batch Online Upgrade

Click **ROLL UPGRADE** in the upper right corner to upgrade the devices in batches.

Through the roll upgrade, the device can be upgraded in sequence, improving your use experience by more functions.



Tip

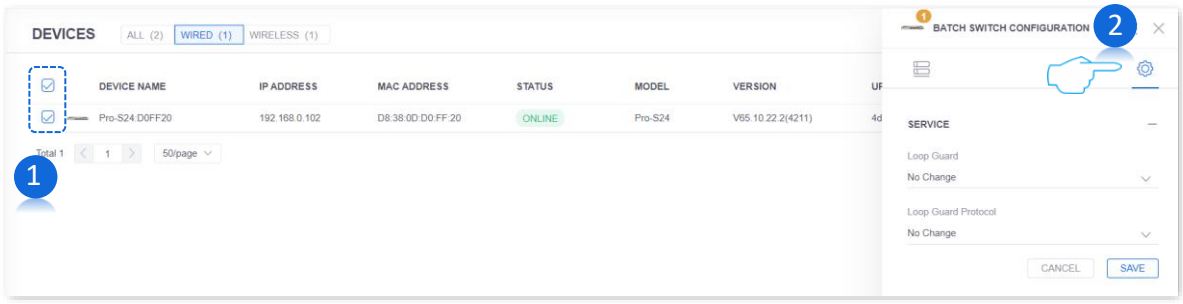
- To avoid damage, ensure that the device is powered on properly during the upgrade.
- The upgrade is available only when there is a new software version.
- If you want to upgrade a single device, refer to local upgrade of AP and local upgrade of switch.

Batch Configuration

Tip

Batch configuration is not supported in the **ALL** list. You need to move to **WIRED** or **WIRELESS**.

In the **WIRED** and **WIRELESS** lists, you can select devices of the same type, then click **CONFIGURATION** ( ) in the pop-up window to do batch configuration. Here takes batch switch configuration as an example.



For the configuration of relevant functions, refer to Switch Details and AP Details.

Locate Devices

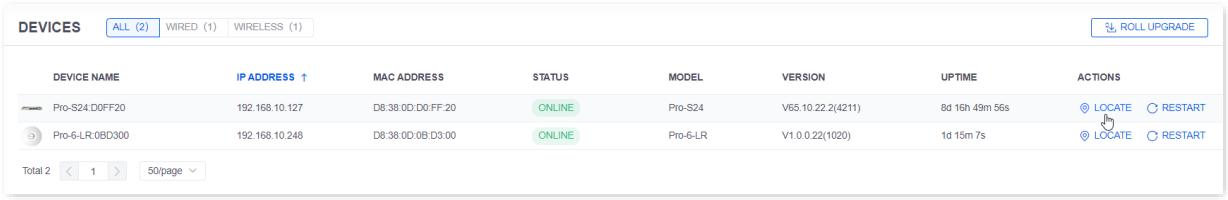
Tip

If there is no LOCATE button in the row where a device resides, the device does not support the locate function.

Enable the locate function

If you want to quickly locate a device in a network, click LOCATE in the row where the target device resides to enable the locate function.

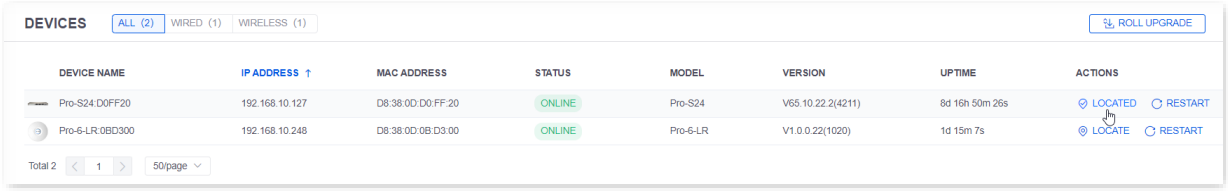
After the function is enabled, the LOCATE button turns to LOCATED and the LED indicator of the located device keeps blinking fast. You can locate the target device by following the clue.



Disable the locate function

If you want to disable the locate function of a device, click LOCATED.

After the locate function is disabled, the LED indicator of the device is restored to the status before the location function is enabled.

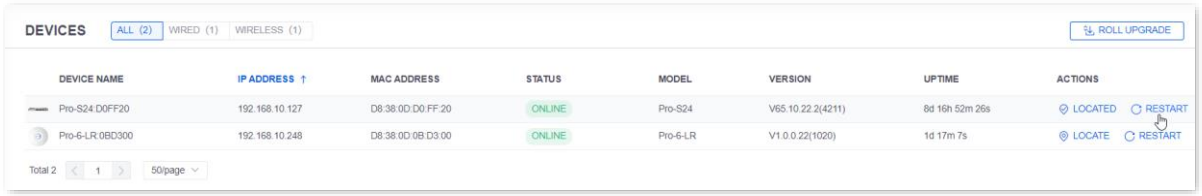


Tip

If the **LOCATED** button is displayed gray, the locating status cannot be cancelled for the device. You can move the mouse over the button to check the reason.

Restart Devices

When some parameters you configured do not take effect, you can click RESTART to restart the target device.



Configure Devices

Click anywhere on the row where the target device resides to check the device details and set the configuration for the device.

For switch devices, refer to Switch Details.

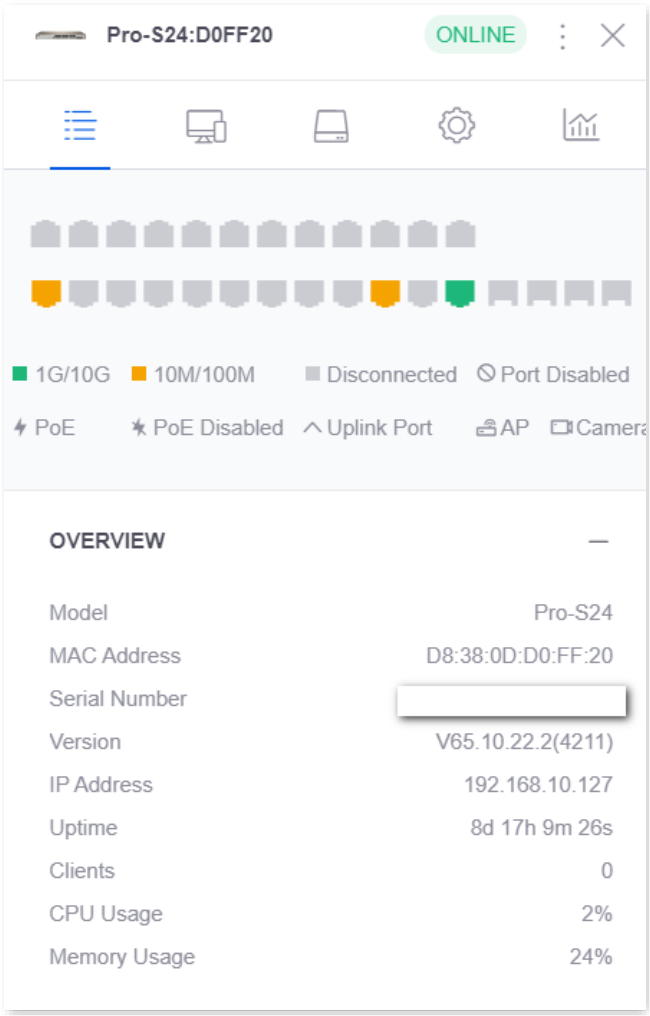
For AP devices, refer to AP Details.

8 Switch Details

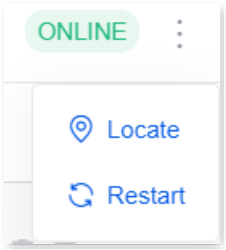
This page displays switch details, including the general information, clients, ports, configuration, and statistics of a switch.

To enter the page, choose **DEVICES** ( ).

Here, you can click a switch, then the details page of the switch pops up from the right side of the screen; or, you can select multiple switches in the **WIRED** tab, then the batch switch configuration page pops up from the right side. Here takes a single switch for illustration. See the following figure.



Window elements description

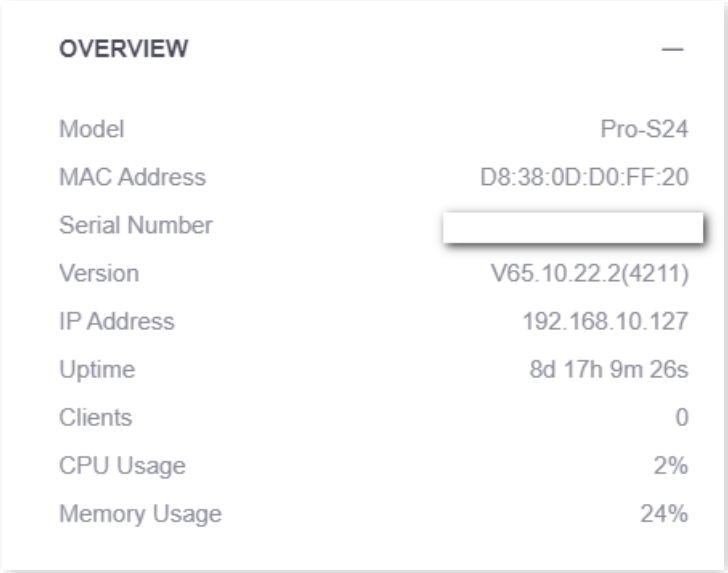
Element	Description
(Status)	It specifies the status of the ProFi switch. – **ONLINE:** The switch is managed by the ProFi Software Controller and connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. – **OFFLINE:** The switch is managed by the ProFi Software Controller but not currently connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. – **PENDING ADOPTION:** The switch is waiting to be managed by the ProFi Software Controller and the site to which it belongs is not determined. – **ADOPTING:** Switch management is under way. – **PROVISIONING:** The switch is synchronizing its configurations with those delivered by the ProFi Software Controller. – **MANAGED BY OTHER:** The switch is managed by another ProFi Software Controller. – **RESTARTING:** The switch is restarting. – **UPGRADING:** The switch is upgrading.
(More actions)	It specifies other actions you can perform on the switch, including locate and restart. This function is valid only for online switches.  Tip – Located indicates that the administrator located the switch on the ProFi Software Controller and has not disabled the locate function. Click Located to disable the locate function. – If a button is missing, that action is not allowed under the current status.
(DETAILS)	Click it to check the general information of the switch such as its port rate, connection status, PoE status, and port identifier.
(CLIENTS)	Click it to check the details of the clients connected to the switch.
(PORTS)	Click it to modify port configurations.

Element	Description
(CONFIGURATION)	Click it to modify switch configurations, including modifying switch name, enabling/disabling loop guard (STP), configuring IP obtaining method and so on.
(STATS)	Click it to check the CPU usage and memory usage.
(ADOPT SWITCH)	Click it to adopt switch to the current site. This function is valid only for switch in the pending adoption status.
1G/10G	It specifies a 1/10 Gbps connection.
10M/100M	It specifies a 10/100 Mbps connection.
Disconnected	It specifies the port is disconnected.
Port Disabled	It specifies the port is disabled.
PoE	It specifies a connection with PoE.
PoE Disabled	It specifies a connection with PoE disabled.
Uplink port/AP/Camera	It specifies the identifier marking the port.

8.1 Details

8.1.1 Overview

This module displays the specifications, IP address, uptime, CPU usage, memory usage, and client statistics of a switch. See the following figure.

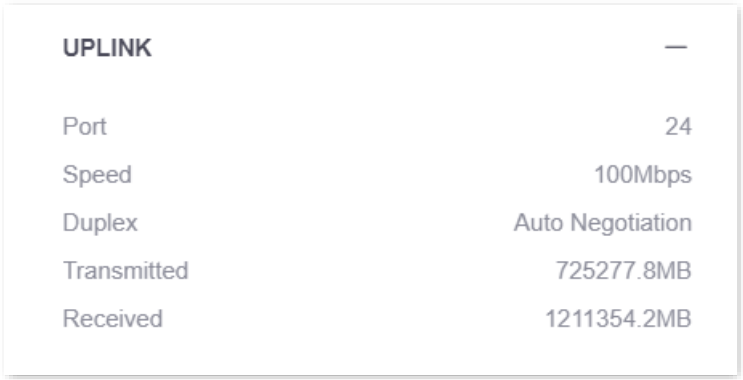


Parameter description

Parameter	Description
Model	It specifies the model of the switch.
MAC Address	It specifies the physical address of the switch.
Serial Number	It specifies the serial number of the switch.
Version	It specifies the current software version of the switch.
IP Address	It specifies the IP address of the switch.
Uptime	It specifies the duration the switch has been running.
Clients	It specifies the number of clients connected to the switch.
CPU Usage	It specifies the CPU usage of the switch.
Memory Usage	It specifies the memory usage of the switch.
PoE Power	It specifies the PoE power of the switch (the power used and the power left).

8.1.2 Uplink

This module displays the details of the uplink of the switch.

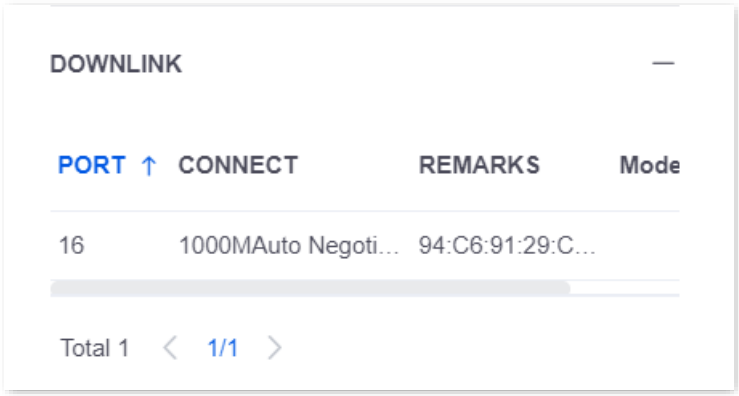


Parameter description

Parameter	Description
Port	It specifies the switch's port number connected to the uplink device.
Speed	It specifies the real-time speed at which the switch negotiates with its uplink device.
Duplex	It specifies the duplex mode of the switch port connected to the uplink device.
Transmitted	It specifies the amount of data transmitted by the switch.
Received	It specifies the amount of data received by the switch.

8.1.3 Downlink

This module displays the details of the downlink of the switch.



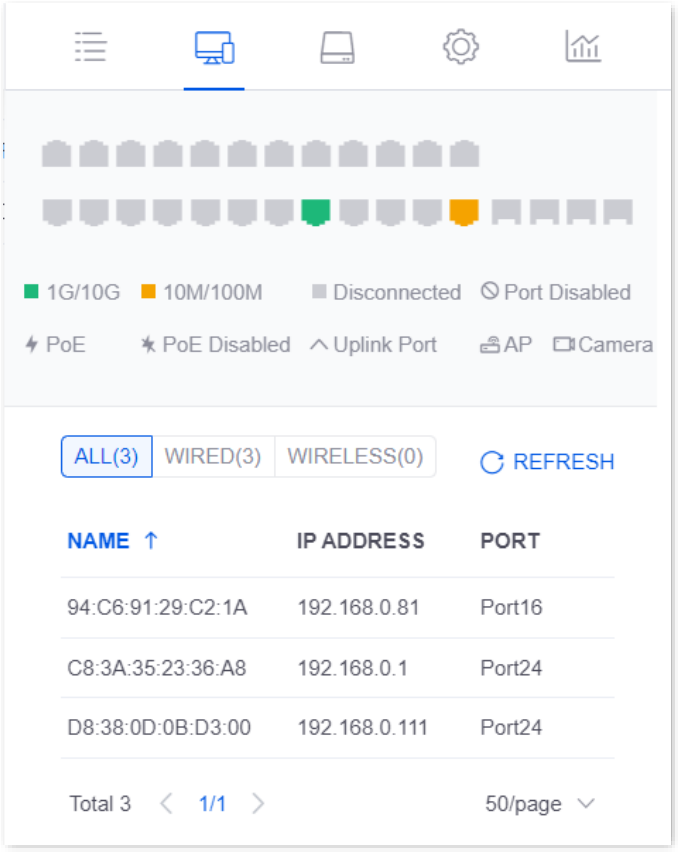
Parameter description

Parameter	Description
(Sort)	Click it beside any column to sort the displayed list. The selected column can display ↑ or ↓ to indicate an ascending or descending order.

Parameter	Description
PORT	It specifies the switch's port number connected to the downlink device.
CONNECT	It specifies the maximum speed at which the switch negotiates with its downlink device and the duplex mode of the switch port connected to the uplink device.
REMARKS	It specifies the description of the downlink device.
MODEL	It specifies the model of the downlink device.

8.2 Clients

This page displays the details of the clients connected to the switch.



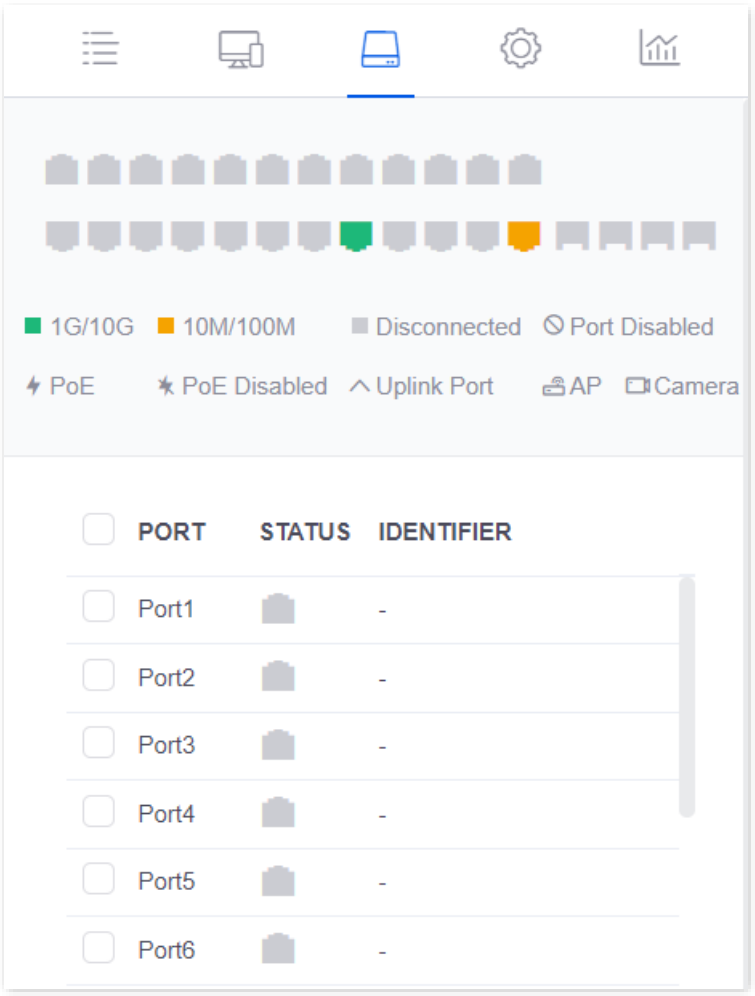
Parameter description

Parameter	Description
(Header)	Click a header to filter out the target types of clients.
(Refresh)	Click it to refresh the client list.
(Sort)	Click it beside any column to sort the displayed list. The selected column can display ↑ or ↓ to indicate an ascending or descending order.
NAME	It specifies the name of the client.
IP ADDRESS	It specifies the IP address of the client.
PORT	It specifies the port to which clients connect.

8.3 Ports

8.3.1 Overview

This page displays the details of all the ports of the switch and is used to set port remarks, enable or disable the port, modify the port speed, set port identifiers, and enable or disable the PoE power supply of PoE port.



Parameter description

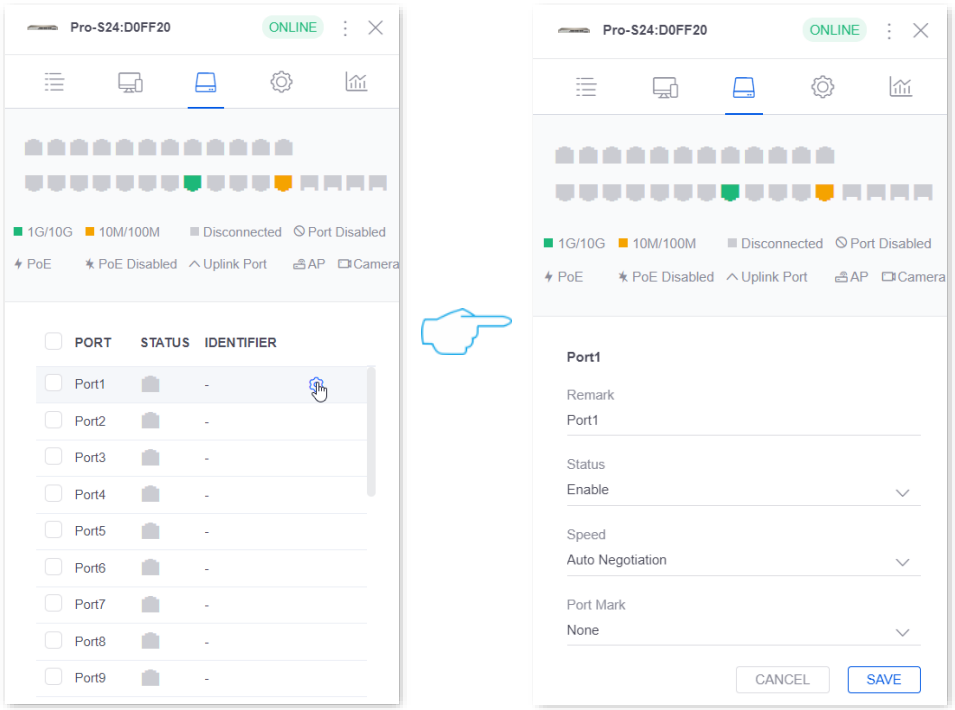
Parameter	Description
PORT	It specifies the port number of the switch.
STATUS	It specifies the status of the port. – : A device is connected to the port, and the negotiation speed is 1G/10G. – : A device is connected to the port, and the negotiation speed is 10M/100M. – : The port is not connected to any device. – : The port is disabled.

Parameter	Description
IDENTIFIER	It specifies the identifier to mark the port. – **None**: It specifies no identifier is set for the port. – **AP**: You are recommended to select this identifier if this port is connected to an AP. – **Camera**: You are recommended to select this identifier if this port is connected to a camera. – **Uplink port**: You are recommended to select this identifier if this port is connected to an uplink port.
PoE(W)	It specifies the PoE output power of the PoE port.
(Actions)	– Click to set port remarks, enable or disable the port, modify the port speed, set port identifiers, and enable or disable the PoE power supply of PoE port. – Click to reboot the PoE power supply of the PoE port. Note The (reboot PoE button) appears only when the port is a PoE port.

8.3.2 Port Configuration

Single Port Configuration

Click to enter the single port configuration page.



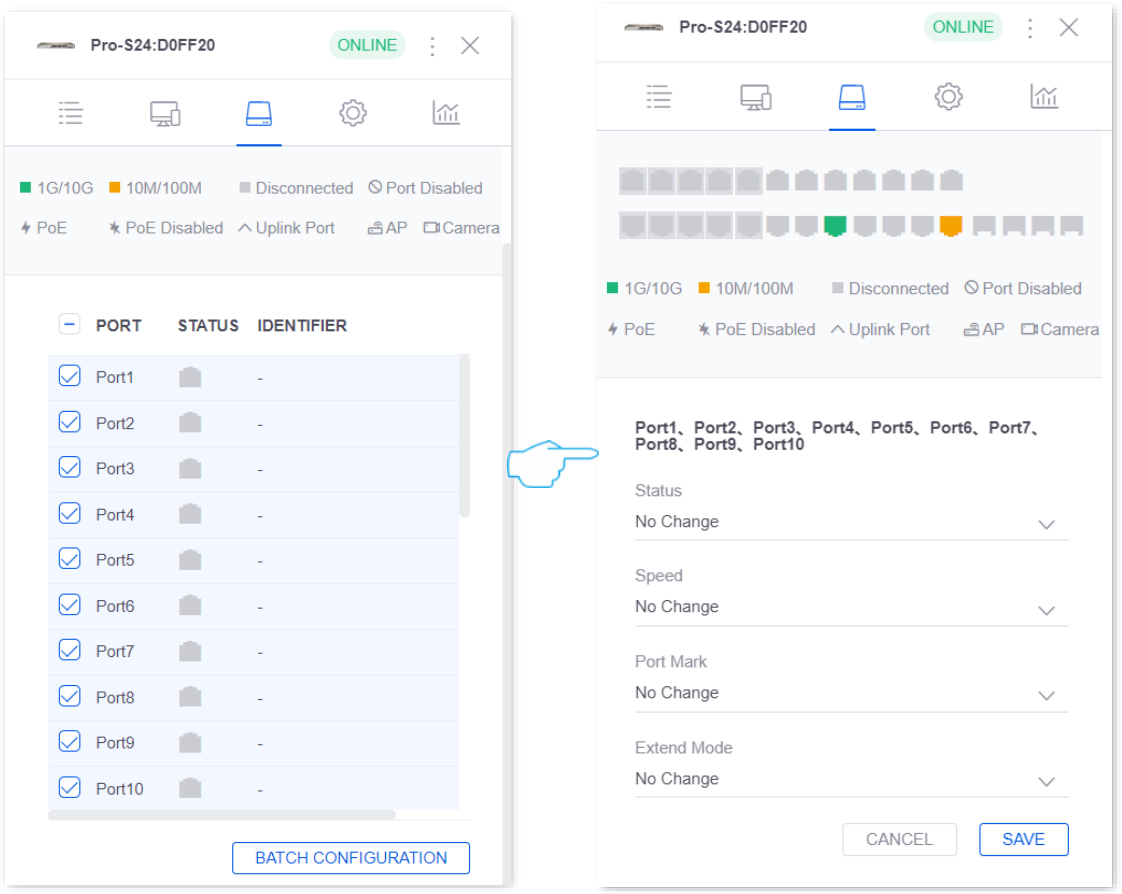
Parameter description

Parameter	Description
Remark	It specifies the remark information of the port.
Status	It specifies the status of the port. – **Enable**: It specifies the port is enabled, which means the port is available. – **Disable**: It specifies the port is disabled, which means the port is unavailable.
Speed	It specifies the negotiation speed of the port. – **Auto Negotiation**: It specifies the port, depending on the speed and duplex mode of the other end, automatically adjusts its speed to the highest level to achieve the fastest speed and duplex mode for both ends. – **1000MFull Duplex**: It specifies the negotiation speed of the port is 1000 Mbps, and the port can receive and transmit data packets at the same time. – **100MFull Duplex**: It specifies the negotiation speed of the port is 100 Mbps, and the port can receive and transmit data packets at the same time. – **100MHalf Duplex**: It specifies the negotiation speed of the port is 100 Mbps, and the port cannot receive and transmit data packets at the same time. – **10MFull Duplex**: It specifies the negotiation speed of the port is 10 Mbps, and the port can receive and transmit data packets at the same time. – **10MHalf Duplex**: It specifies the negotiation speed of the port is 10 Mbps, and the port cannot receive and transmit data packets at the same time.
Port Mark	It specifies the identifier to mark the port.
PoE Power Supply	It specifies whether the PoE power supply function of the PoE port is enabled. – **Enable**: It specifies the PoE power supply function of the PoE port is enabled. – **Disable**: It specifies the PoE power supply function of the PoE port is disabled. This configuration appears only for PoE ports.

Batch Port Configuration

You can check the box before ports, and click **BATCH CONFIGURATION** to configure multiple ports in batches.

No Change means the current configuration of the ports remains unchanged.



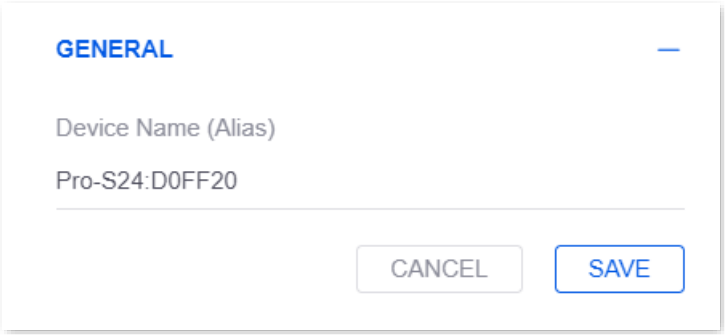
Parameter description

Parameter	Description
Extend Mode	It is used to enable or disable the network extension mode of ports (Available only when the switch supports such function). This function will extend the data transmission and PoE power supply distance of PoE ports, bringing convenience to network deployment. After it is enabled, the selected ports decrease to 10 Mbps in negotiation rate, but transmit up to 250 m in distance. It is recommended to use CAT5e or better Ethernet cables for better network extension. It is recommended to enable this function when the switch is over 100 m away from the downlink devices. Besides, you need to set the speed and duplex mode of the ports of the peer devices to **Auto Negotiation**. It the peer device is an IP camera, set its bit rate below 8 Mbps for timeliness of video transmission.

8.4 Configuration

8.4.1 General

This module is used to modify switch remarks (or alias).

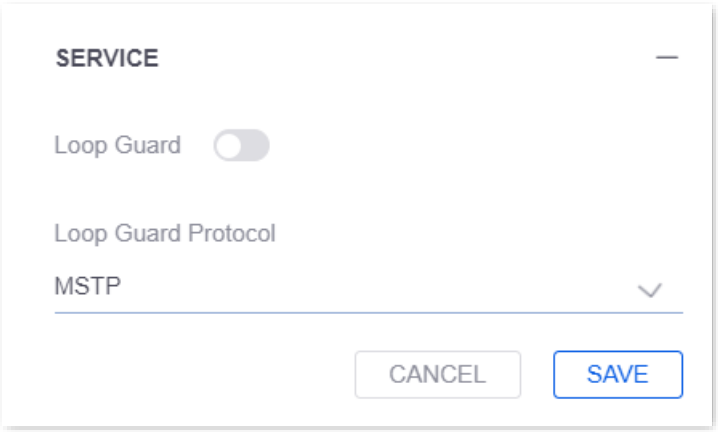


Parameter description

Parameter	Description
Device Name (Alias)	It specifies the device name of the switch. By default, the switch model and the last six digits of switch MAC address are displayed. You can modify it to distinguish switches.

8.4.2 Service

This module is used to enable or disable the loop guard protocol (spanning tree). Enable **Loop Guard**, choose a **Loop Guard Protocol**, and click **Save**.



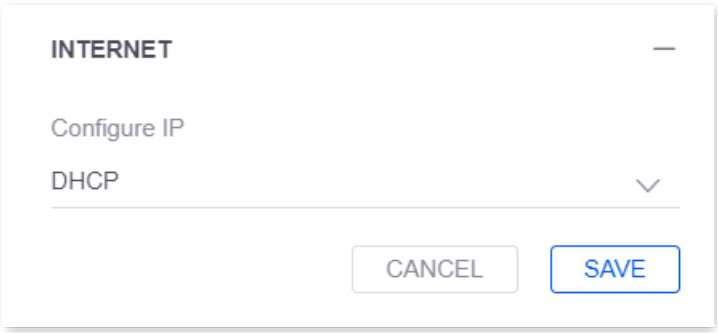
Parameter description

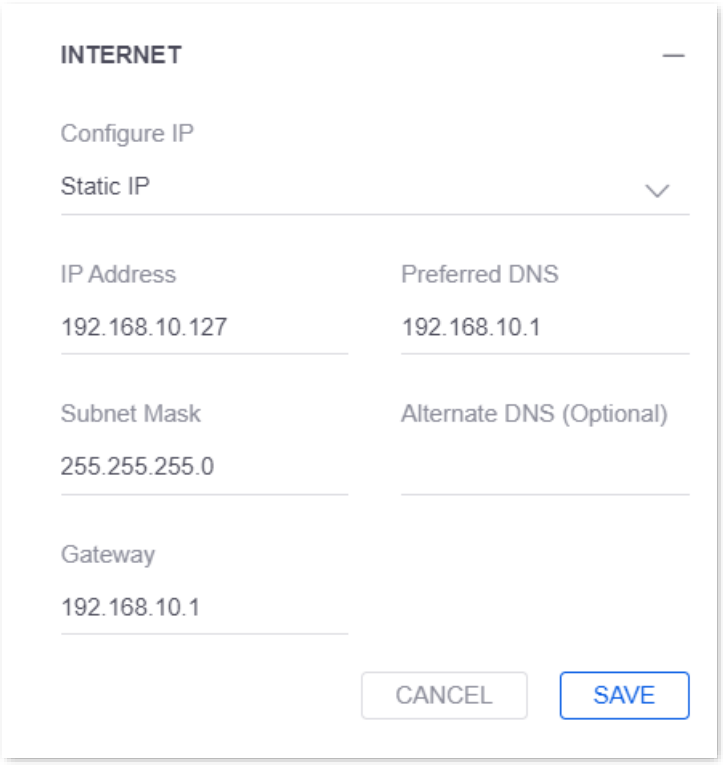
Parameter	Description
Loop Guard	It specifies whether to enable loop guard through the spanning tree. This function helps avoid loops in the network to protect the network from broadcast storms, and provide link redundancy backup.

Parameter	Description
Loop Guard Protocol	It specifies the spanning tree protocol options to achieve loop guard. – **STP**: Spanning Tree Protocol. It is a network protocol based on IEEE 802.1d. It ensures a loop-free topology in local area network and provides backup redundant links. The devices under this protocol discover the loops in the network by communicating with each other, and selectively block some ports, and eventually establish a spanning tree structure without loops to prevent the decline of message processing capacity caused by continuous proliferation and endless circulation of messages in the loop network. – **RSTP**: Rapid Spanning Tree Protocol. It is defined by the IEEE 802.1w standard and downward compatible with IEEE 802.1d STP. In addition to a loop-free network and redundant links, it features with fast convergence. If all bridges in a LAN support RSTP, it enables a rapid topology tree generation when the network topology changes (traditional STP topology tree: 50 seconds, RSTP topology tree: 1 second). – **MSTP:** Multi Spanning Tree Protocol. It is defined by the IEEE 802.1s standard and compatible with STP and RSTP. It not only features fast convergence, but also allows data flows of different VLANs to be forwarded along the paths respectively. These functions lead to better load sharing mechanism for redundant links, and compensate for the limitations of STP and RSTP.

8.4.3 Internet

This module is used to modify the network configuration.





Parameter description

Parameter	Description
Configure IP	It specifies the IP address obtaining mode of the switch. – **DHCP**: the default mode. Under this mode, the switch automatically obtains its IP address, subnet mask, gateway address, and DNS server address from the DHCP server in the network. This mode is applicable to the scenarios where a large number of switches are deployed. – **Static IP**: Under this mode, the IP address, subnet mask, gateway address, and DNS server address of the switch are specified manually. This mode is applicable to the scenarios where only one or several switches are deployed.

Parameter	Description
IP Address	It specifies the IP address of the switch, and is also the management IP address of the switch. LAN users can visit this IP address to log in to the web UI of the switch.
Subnet Mask	It specifies the subnet mask of the switch, which is used to define the IP address range of the network segment.
Gateway	It specifies the IP address of the default gateway. If you want to connect the switch to the internet, set this parameter to the IP address of the LAN port of the router connected to the internet.
Preferred DNS	It specifies the preferred DNS server address. If the router connected to the internet has the DNS proxy function, you can enter the IP address of its LAN port. Otherwise, enter the correct IP address of the DNS server.
Alternate DNS (Optional)	It specifies the alternate DNS server address. This parameter is optional. If you have two DNS server IP addresses, you can enter the other one here.

8.4.4 VLAN Configuration

VLAN (Virtual Local Area Network) is a technology that divides devices in LAN into different logical, instead of physical, network segments to realize virtual working groups. VLANs allow a network station constituted by switches to be logically segmented into different domains for broadcast separation. All members in a VLAN are treated as in the same broadcast domain and communicate as if they were on the same network segment, regardless of their physical locations. Different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer-3 devices that are able to perform Layer-3 forwarding.

Switches supporting 802.1Q VLAN can communicate with devices that support 802.1Q VLAN in VLAN as well.

802.1Q VLAN is defined by IEEE 802.1q protocol. With 802.1Q VLAN, the switch can process messages by identifying the tags in messages.

Generally, switches support three 802.1Q VLAN port types:

- Access: An access port belongs to only 1 VLAN, generally used for connecting the computer.
- Trunk: A trunk port can receive and send messages belonging to multiple VLANs. Usually, a trunk port is used for switches connection.
- Hybrid: A hybrid port can receive and send messages belonging to multiple VLANs. Usually, a hybrid port is used for switches connection, and can be connected to a computer.

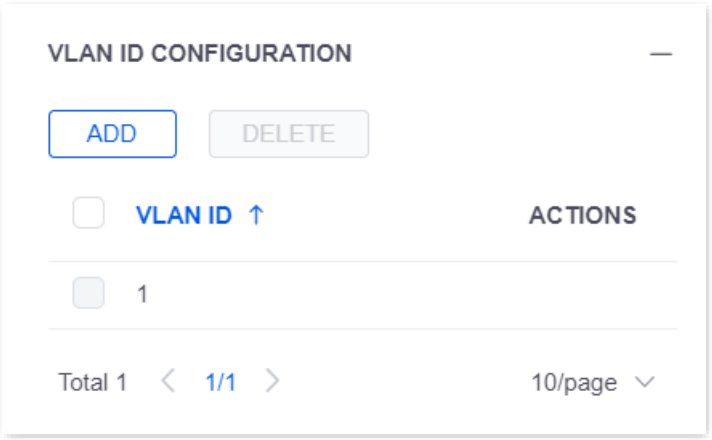
Configuration Procedure

Step	Description
1	Add VLAN ID
2	Configure Port VLAN

Add VLAN ID

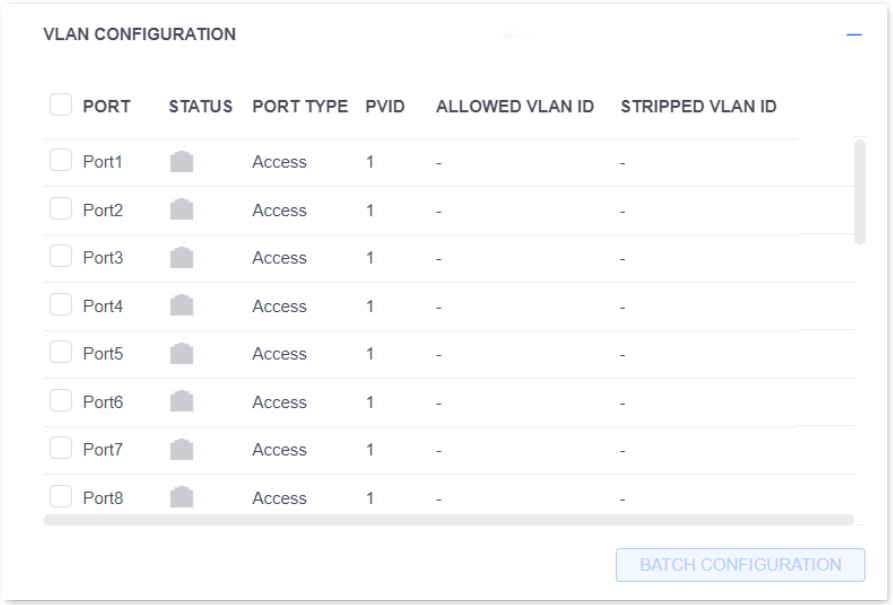
In this module, you can add new VLAN IDs.

By default, VLAN 1 is created and cannot be deleted.



Configure Port VLAN

This module is used to configure VLAN for target ports. Through the port type, PVID and tag treatment policies of switch ports, VLAN isolation can be achieved.

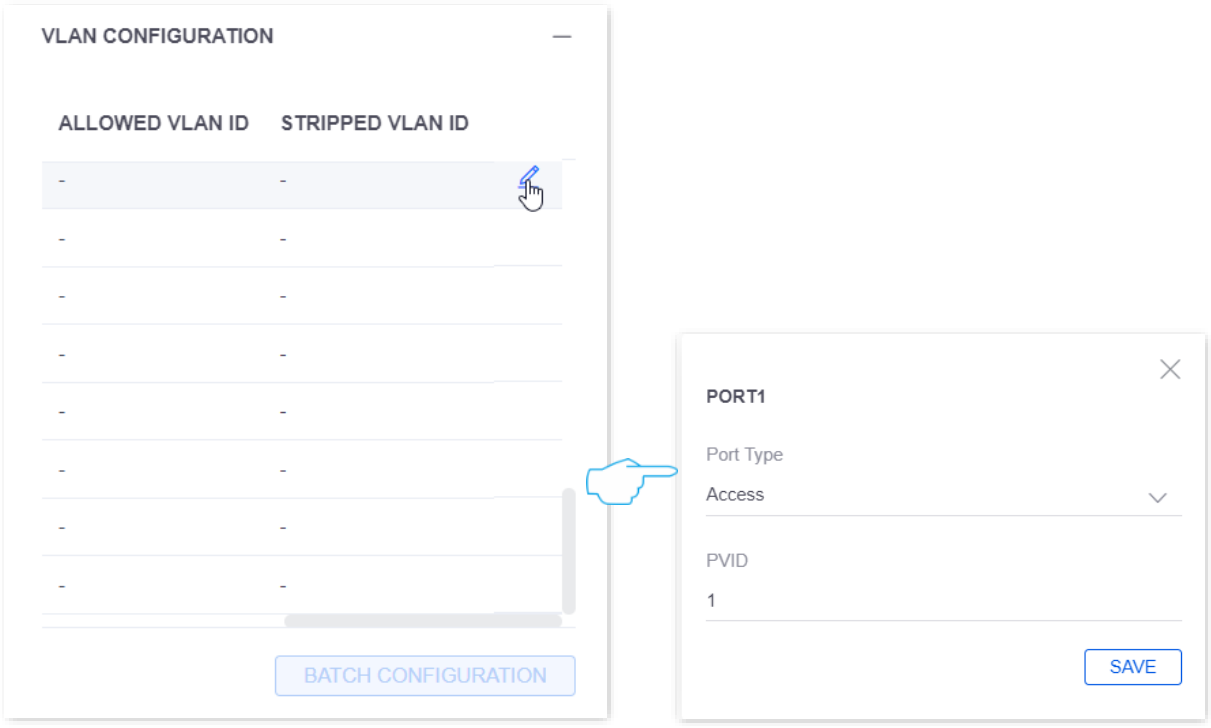


Parameter description

Parameter	Description
PORT	It specifies the port number.
STATUS	It specifies the status of the port.
PORT TYPE	It specifies the type of the port.
PVID	Port VLAN ID. It specifies the default VLAN ID to which the port belongs. When receiving untagged packets, the port forwards them to the corresponding VLAN based on the PVID of the port itself.
ALLOWED VLAN ID	If the VID of the tagged packets received by the port is same as the allowed VLAN ID, the port retains the tags of the packets and transmit them.
STRIPPED VLAN ID	If the VID of the tagged packets received by the port is same as the stripped VLAN ID, the port removes the tags of the packets and transmit them.
	Click to modify the port type and PVID of the port.
BATCH CONFIGURATION	Click it to configure properties of multiple ports of the switch.

Single Port Configuration

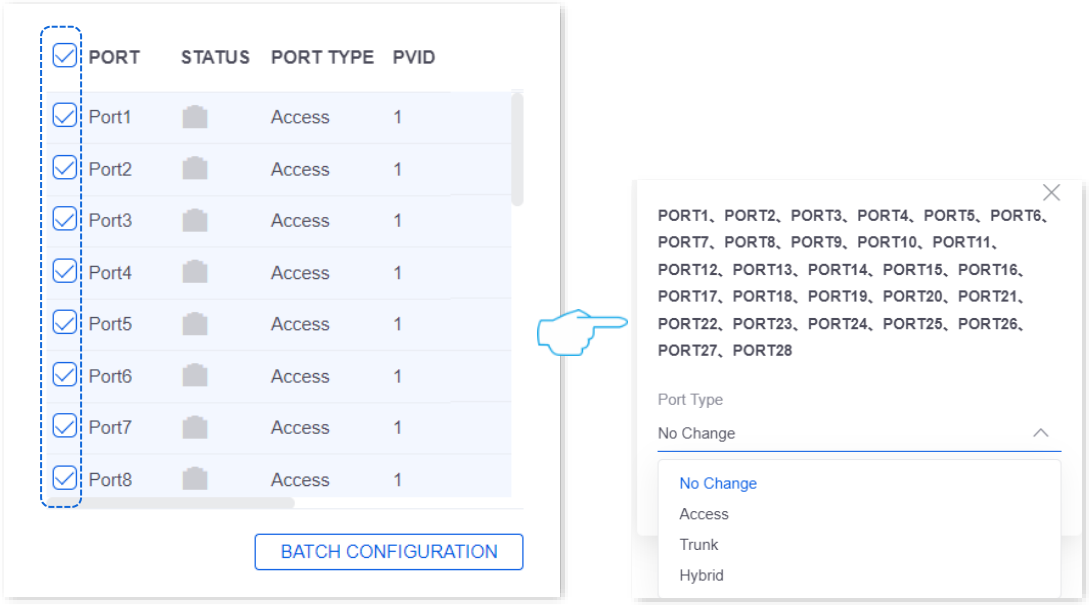
Click at the row of each port, then you can configure the port type and PVID of each port.



Batch Port Configuration

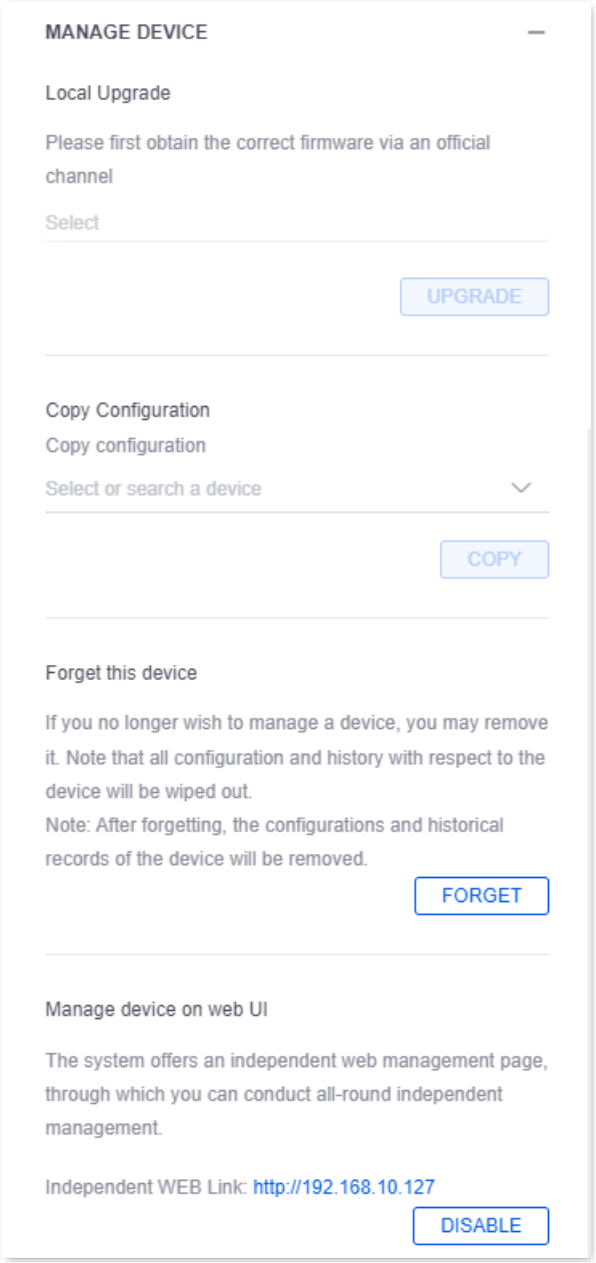
You can select multiple ports and click **BATCH CONFIGURATION** to configure port types in batches.

No Change means that the current port type of the port remains unchanged.



8.4.5 Manage Device

This module is used to upgrade the switch, copy the configuration of another switch, and forget the switch.



Local Upgrade

This module is used to upgrade the switch by uploading the upgrade firmware stored in a local computer.

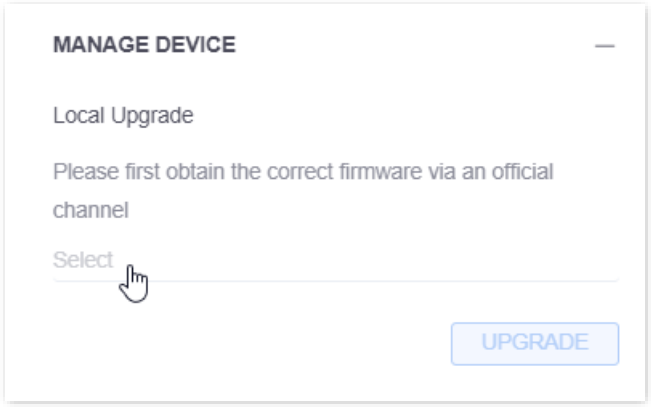
Note

To ensure correct upgrade and avoid device damage,

- Ensure the upgrade file is suitable for the current device.
- Ensure the device is powered on properly during upgrade.

Configuration Procedure

1. Visit the official website of IP-COM www.ip-com.com.cn, download the upgrade firmware of the corresponding switch to your local computer and unzip it. Generally, the suffix of the firmware is generally **.bin**.
2. Log in to the ProFi Software Controller, select your site and choose **DEVICES** ( ).
3. Click a switch, and click at the details panel, then click **MANAGE DEVICE**.
4. Locate **Local Upgrade**, Click **Select** in the text box.



5. Select and upload the upgrade firmware from your computer.

----End

After the upgrade is done, you can view the upgraded firmware version at the **DEVICES** ( ) page, and check whether the version is same as what you just uploaded.

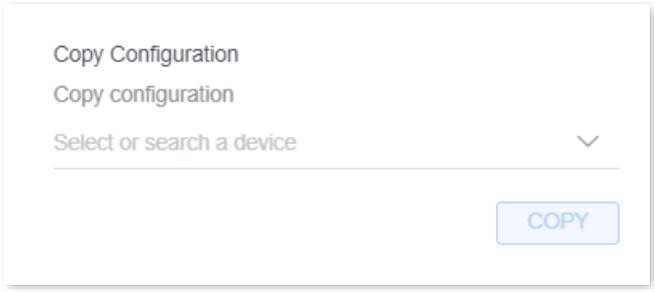
Tip

To improve the stability of switch and experience more functions of the upgraded version, after the finish of upgrade, it is recommended to restore the switch to factory settings and reconfigure the switch.

Copy Configuration

This module enables you to copy the configuration of another switch in the site to this switch.

Click the drop-down menu to select the device whose configuration you want to apply to this switch.

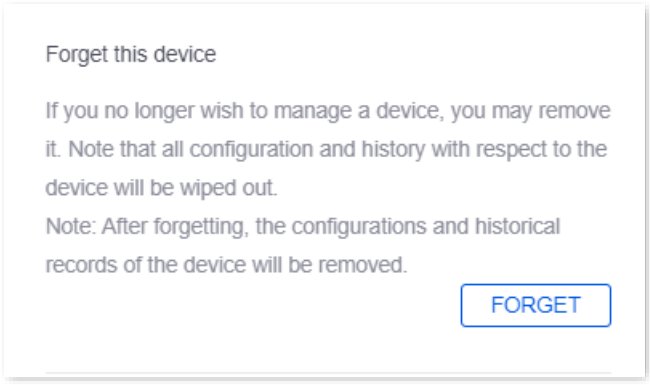


Forget This Device

If you no longer want to manage a switch, you can forget this switch here.

Note

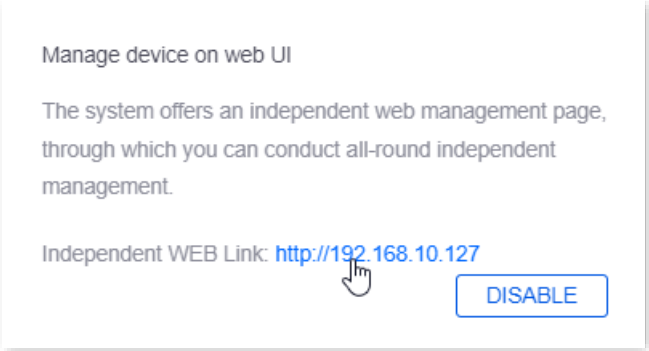
After you forgot the switch, the switch will be restored to factory settings, and all configurations and history of this switch will be cleared.



Manage Device on Web UI

This module is used to enable or disable the independent web UI management function of the switch.

After it is enabled, if the management computer is deployed locally (in the LAN where the switch is deployed), you can click the **Independent WEB Link** to redirect to the web UI of the switch.

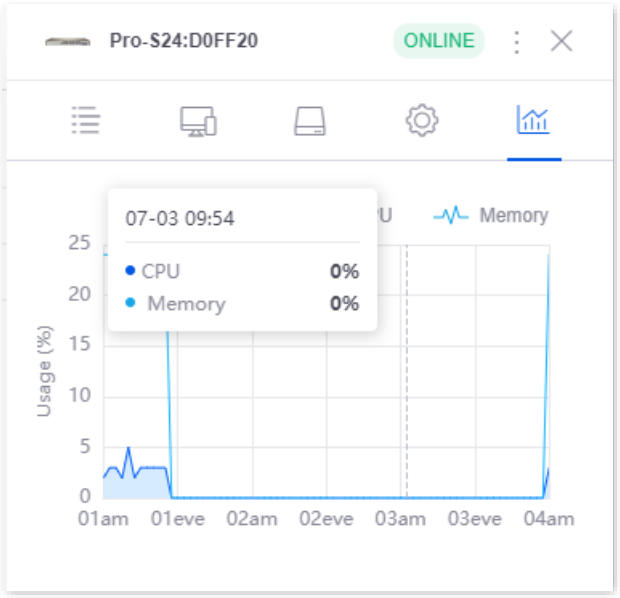


8.5 Stats

This page is used to check the CPU usage and memory usage during the last 72 hours.

Tip

The stats function is valid only when the ProFi Software Controller is running properly. In other words, the statistics during the period when the ProFi Software Controller is closed will not be counted.

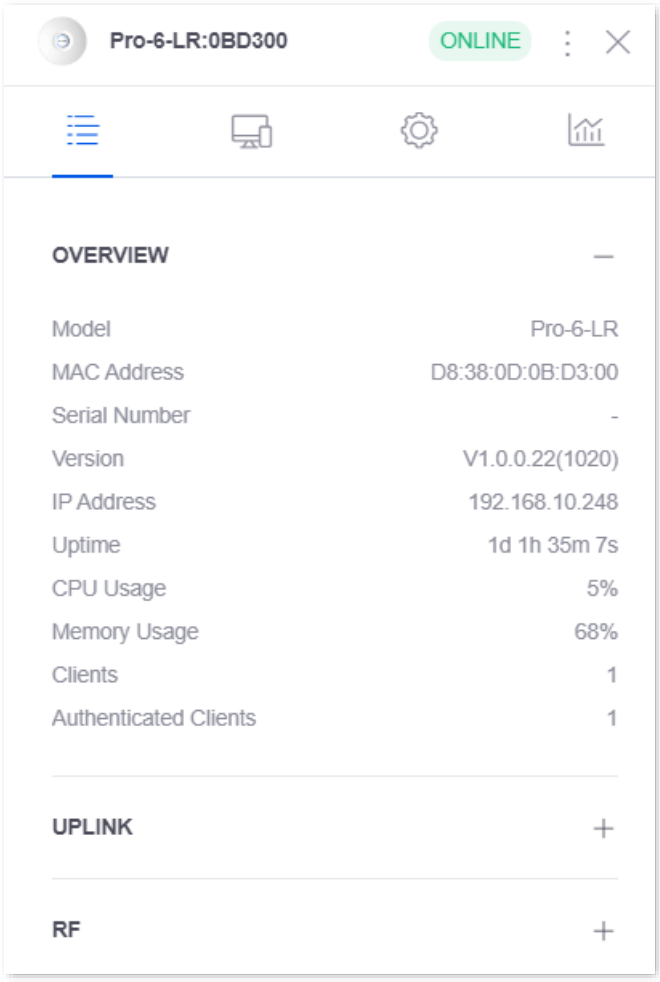


9 AP Details

This page displays AP details, including the general information, clients, configuration and statistics of an AP.

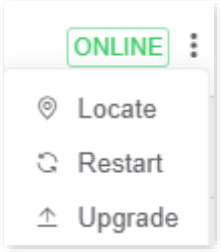
To enter the page, choose **DEVICES** ( ).

Here, you can click an AP, then the details page of the AP pops up from the right side of the screen; or, you can select multiple APs in the **WIRELESS** tab, then the batch AP configuration page pops up from the right side. Here takes a single AP for illustration. See the following figure.



Window elements description

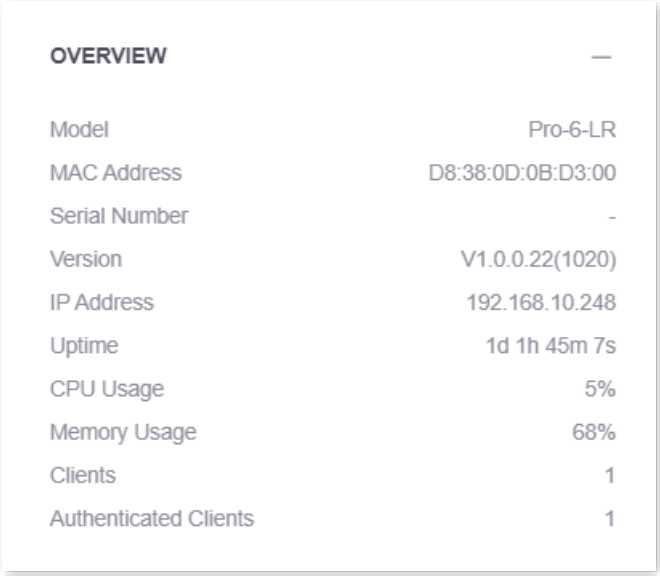
Element	Description
(Status)	It specifies the status of the ProFi AP. – **ONLINE:** The AP is managed by the ProFi Software Controller and connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. – **OFFLINE:** The AP is managed by the ProFi Software Controller but not connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. – **CONNECTED (DISABLED):** The ProFi device is managed by the ProFi Software Controller and connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. In this case, the AP is disabled. – **OFFLINE (DISABLED)**: The ProFi device is managed by the ProFi Software Controller but not connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. In this case, the AP is disabled. – **ONLINE (WIRELESS)**: It specifies the ProFi device connecting to the ProFi Software Controller through bridging. Such ProFi device is managed by the ProFi Software Controller and connected to the network in which the ProFi Software Controller is deployed. It belongs to the current site. – **PENDING ADOPTION:** The AP is waiting to be managed by the ProFi Software Controller and the site to which it belongs is not determined. – **ADOPTING:** The AP management is under way. – **PROVISIONING:** The AP is synchronizing its configurations with those delivered by the ProFi Software Controller. – **MANAGED BY OTHER:** The AP is managed by another ProFi Software Controller. – **RESTARTING:** The AP is restarting. – **UPGRADING:** The AP is upgrading.

Element	Description
(More actions)	It specifies other actions you can perform on the AP, including locate, restart, and upgrade. This function is valid only for online APs.  Tip – Located indicates that the administrator located the AP on the ProFi Software Controller and has not disabled the locate function. Click Located to disable the locate function. – If a button is missing, that action is not allowed under the current status.
(DETAILS)	Click it to check the general information of the AP, including its uplink, RF, WLANs and so on.
(CLIENTS)	Click it to check the details of the clients connected to the AP.
(CONFIGURATION)	Click it to modify the AP configurations, including modifying device name, LED indicator control, band steering, WLAN, VLAN and so on.
(STATS)	Click it to check the CPU usage, memory usage, and the number of connected clients of the AP.
(Adopt AP)	Click it to adopt AP to the current site. This function is valid only for AP in the pending adoption status.

9.1 Details

9.1.1 Overview

This module displays the specifications, IP address, uptime, CPU usage, memory usage, client statistics, and last disconnected time of an AP. See the following figure.

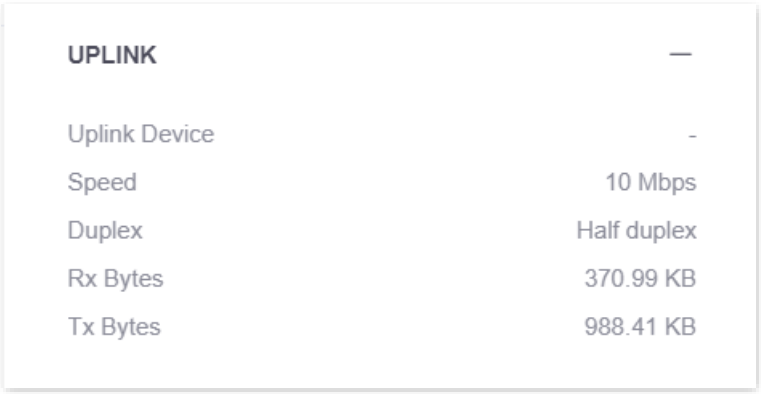


Parameter description

Parameter	Description
Model	It specifies the model of the AP.
MAC Address	It specifies the physical address of the LAN port of the AP.
Serial Number	It specifies the serial number of the AP.
Version	It specifies the software version of the AP.
IP Address	It specifies the IP address of the AP.
Uptime	It specifies the duration the AP has been running.
CPU Usage	It specifies the CPU usage of the AP.
Memory Usage	It specifies the memory usage of the AP.
Clients	It specifies the number of clients connected to the wireless networks of the AP.
Authenticated Clients	It specifies the number of authenticated clients connected to the wireless networks of the AP.
Last Seen	It specifies the time when the AP is disconnected last time.

9.1.2 Uplink

This module displays the details of the uplink of the AP.



Parameter description

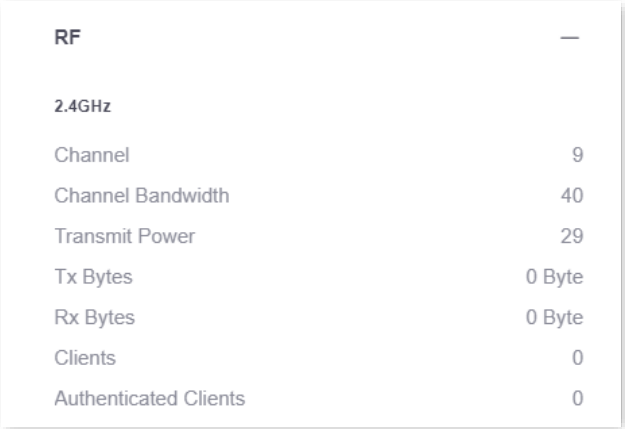
Parameter	Description
Uplink Device	It specifies the name of the uplink device to the AP.
Speed	It specifies the real-time speed at which the AP negotiates with its uplink device.
Duplex	It specifies the duplex mode of the AP port connected to the uplink device.
Rx Bytes	It specifies the total bytes received by the AP.
Tx Bytes	It specifies the total bytes transmitted by the AP.

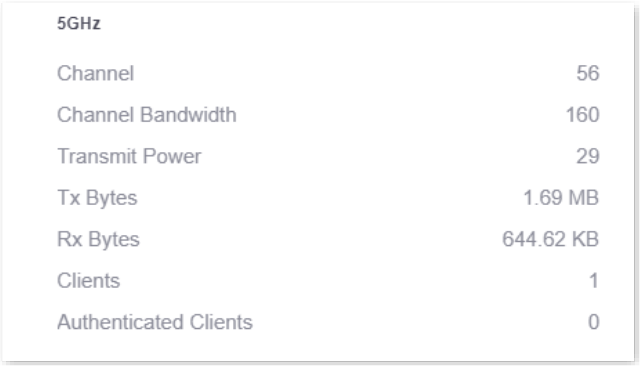
9.1.3 RF

This module displays the RF parameters corresponding to the AP bands.

Tip

If the AP is a single-band AP, only the statistics of that band is displayed.



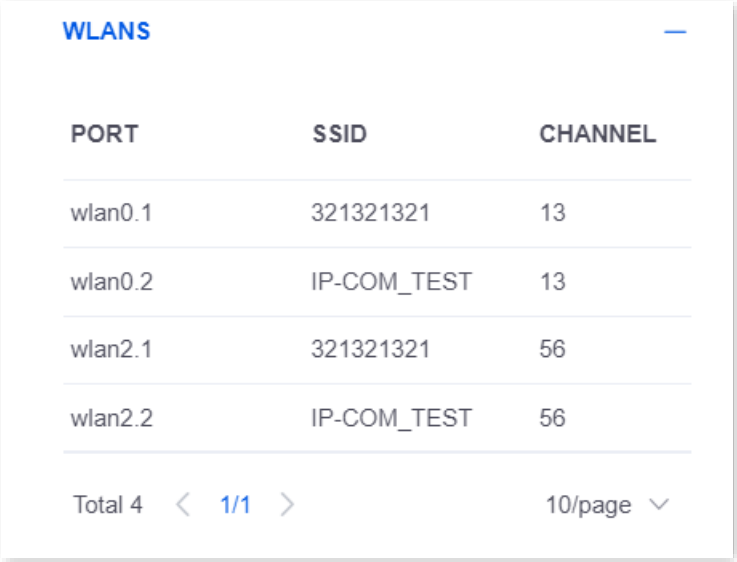


Parameter description

Parameter	Description
Channel	It specifies the channel AP utilizes to transmit and receive the wireless data in the radio band. **0** indicates that the wireless function is not enabled.
Channel Bandwidth	It specifies the frequency range of the wireless channel AP utilizes in the radio band. **0** indicates that the wireless function is not enabled.
Transmit Power	It specifies the transmit power of the radio band.
Tx Bytes	It specifies the total bytes AP transmitted and received.
Rx Bytes	
Clients	It specifies the number of clients connected to the radio band of the AP.
Authenticated Clients	It specifies the number of authenticated clients connected to the radio band of the AP.

9.1.4 WLANs

This module displays the details of the enabled wireless network groups.

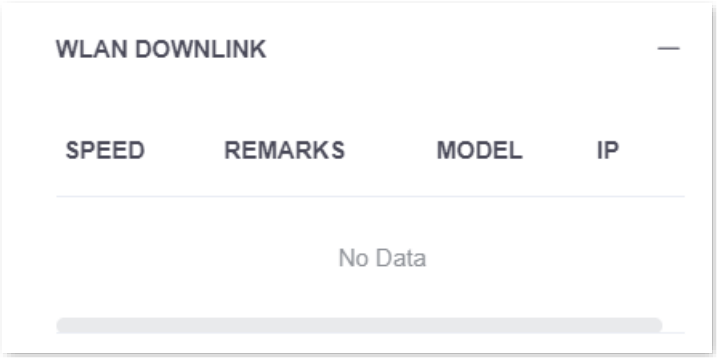


Parameter description

Parameter	Description
PORT	It specifies the wireless network interface.
SSID	It specifies the wireless network name.
CHANNEL	It specifies the channel in which the wireless network operates.

9.1.5 WLAN Downlink

This module displays the downlink information of the AP.



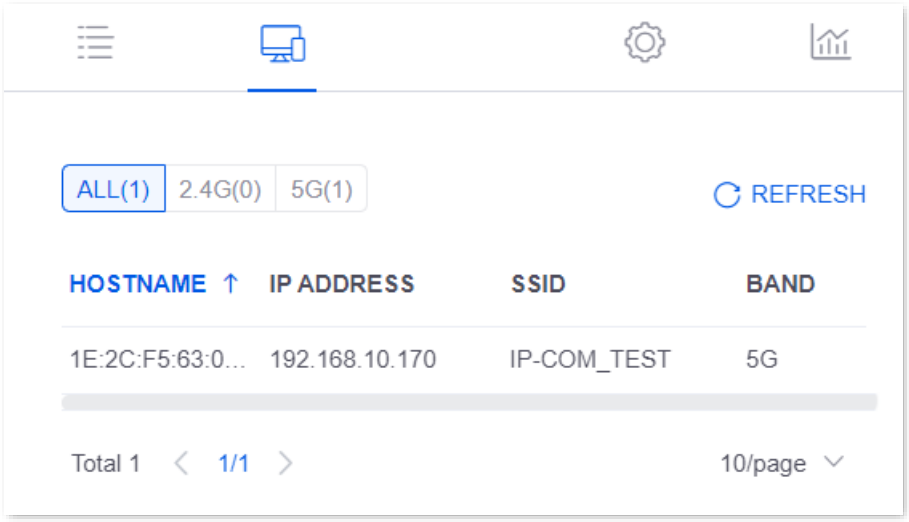
Parameter description

Parameter	Description
SPEED	It specifies the real-time negotiation speed between the AP and client.

Parameter	Description
REMARKS	It specifies the remarks of the client.
MODEL	It specifies the model of the client.
IP	It specifies the IP address of the client.

9.2 Clients

This page displays the details of clients connected to the AP.



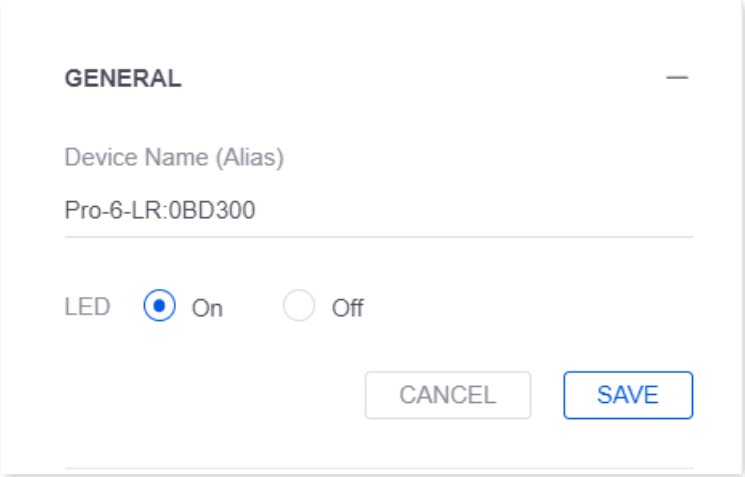
Parameter description

Parameter	Description
HOSTNAME	It specifies the name of the client.
IP ADDRESS	It specifies the IP address of the client.
SSID	It specifies the wireless network the client connects to.
BAND	It specifies the wireless band the client connects to.

9.3 Configuration

9.3.1 General

This module is used to modify AP name, and enable or disable its LED indicator.



Parameter description

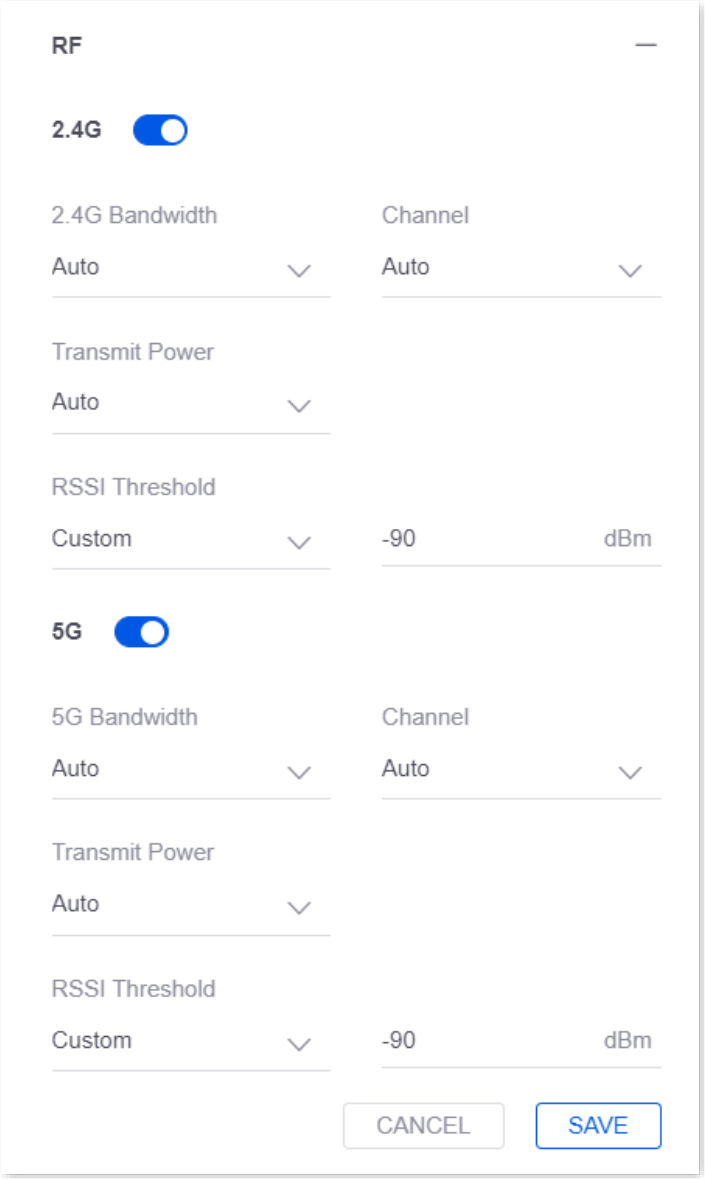
Parameter	Description
Device Name (Alias)	It specifies the name of the AP. By default, the AP model and the last six digits of its MAC address are displayed. It is recommended to change it to the actual installation location of the AP, so that you can quickly locate multiple APs even they are the same modol.
LED	Choose to enable or disable the LED indicator. If the LED indicator is enabled, you can judge the operating status of the AP by the indicator. By default, the LED indicator is enabled (**On**).

9.3.2 RF

This module is used to modify channel parameters, transmit power and RSSI threshold of the AP.

Tip

If the AP is a single-band AP, only the statistics of that band is displayed.



Parameter description

Parameter	Description
2.4G/5G Channel Bandwidth	It specifies the frequency range of the wireless channel AP utilizes in the radio band. The higher the channel bandwidth is, the higher the transmit and receive rates are, but the penetration performance is reduced, and data can be transmitted and received at a short distance. – **Auto**: The AP switches the channel bandwidth based on its surroundings. – **20MHz**: The AP utilizes a channel bandwidth of 20 MHz. – **40MHz**: The AP utilizes a channel bandwidth of 40 MHz. – **80MHz**: The AP utilizes a channel bandwidth of 80 MHz. This option is supported only for the 5 GHz network. – **160MHz**: The AP utilizes a channel bandwidth of 160 MHz. This option is supported only for the 5 GHz network.

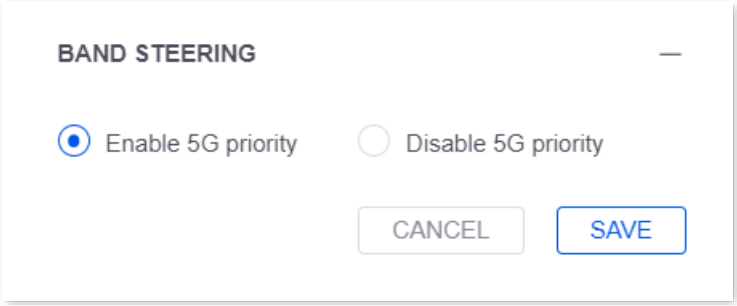
Parameter	Description
Channel	It specifies the channel AP utilizes to transmit and receive the wireless data in the radio band. Its options are determined by your country/region and radio band. By default, **Auto** is selected. **Auto**: The AP automatically detects the channel utilization of each channel and chooses a proper channel accordingly. If disconnection or slow internet connection occurs from time to time, try changing to another channel. You can use such software tools as WiFi analyzer to check channels which are less occupied and have little interference.
Transmit Power	It specifies the transmit power of the radio band of the AP. By default, **Auto** is selected. The higher the transmit power, the wider the wireless coverage will be. However, a proper reduction of the transmit power can help improve the performance and enhance the security of the wireless network. – **Auto**: The AP automatically adjusts its transmit power to the maximum value. You can view the maximum transmit power of the AP by visiting **Wireless** > **RF Settings** on the AP's own management web UI. – **Custom**: Set a transmit power manually.
RSSI Threshold	It specifies the minimum strength of received signals acceptable to the AP. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to the AP. A proper value facilitates wireless devices to connect to the AP with stronger signal in case of multiple APs exist.

9.3.3 Band Steering

This module is used to enable or disable 5G priority. With 5G priority enabled, if the 5 GHz signal strength transmitted by a client is stronger than the **Prioritize 5 GHz Threshold**, then the AP will let the dual-band client take priority to connect to 5 GHz band.

Tip

- You can view the **Prioritize 5 GHz Threshold** by visiting **Wireless** > **RF Settings** on the AP's own management web UI.
- The conditions for 5G priority to take effect are: 2.4 GHz and 5 GHz of the AP are both enabled; the SSIDs configured at 2.4 GHz and 5 GHz are the same; and the corresponding wireless authentication and password are the same.

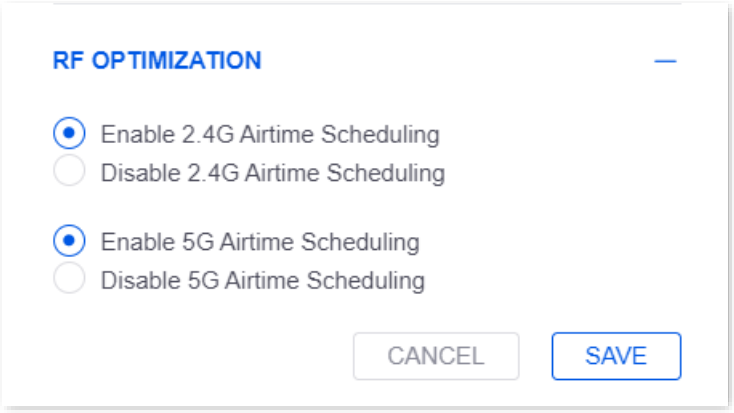


9.3.4 RF Optimization

This module is used to enable or disable 2.4G/5G airtime scheduling. This function assigns equal airtime to clients of different rates, thus improving experience of high rate clients.

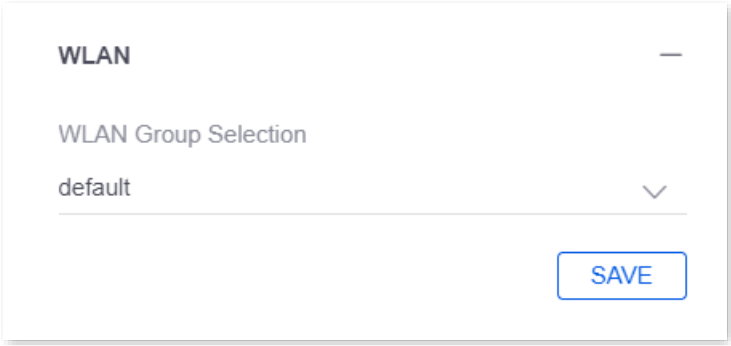
Traditional packet distribution is performed in FIFO mode. In the environment that involves various wireless data rates, high-speed clients have high transmission capability and high frequency use efficiency but has less time to access the air interface. On the contrary, low-speed clients has low transmission capability and low frequency use efficiency but has more time to access the air interface. This reduces the overall throughput of each AP, resulting in lower system efficiency.

Air interface scheduling assigns the same length of time for high-speed clients and low-speed clients to access the air interface, enabling the high-speed clients to transmit more data. This increases the overall throughput and number of connected users of an AP. The airtime scheduling function allocates downlink transmission time to clients so that clients with high transmission rate could transmit more data, improving the throughput of each AP and quantity of clients allowed to be connected.



9.3.5 WLAN

This module enables you to change the WLAN group of an AP. The WLAN group should be configured in advance in **SETTINGS** ( ) > **Wireless Networks**. By default, the AP is under the WLAN group **default**.



9.3.6 SSID Maximum Number of Clients

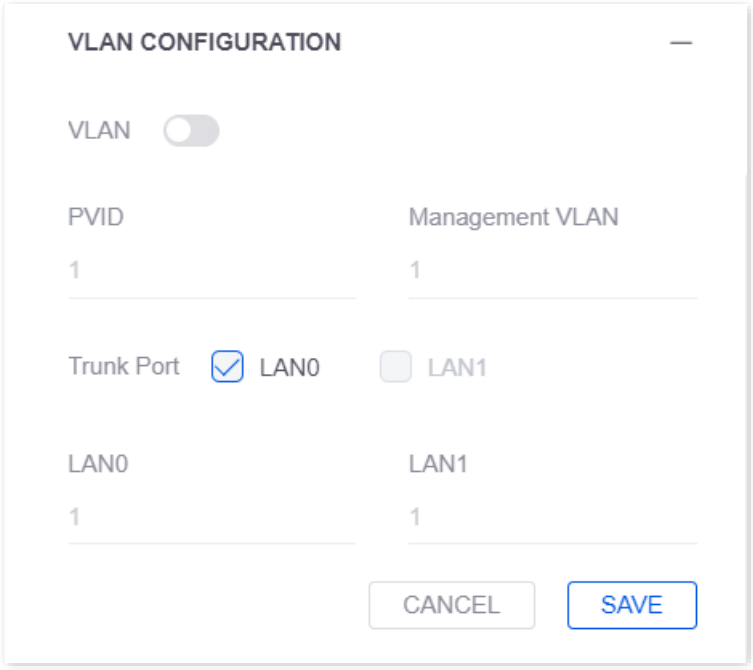
This module is used to modify the maximum number of wireless clients allowed to connect to each SSID of its radio band.

Parameter description

Parameter	Description
PORT	It specifies the radio band of the AP network.
SSID	It specifies the wireless network name of the AP.
NUMBER OF CLIENTS	It specifies the maximum number of wireless clients allowed to connect to each SSID of its radio band.

9.3.7 VLAN Configuration

This module is used to set the VLAN function of the AP.



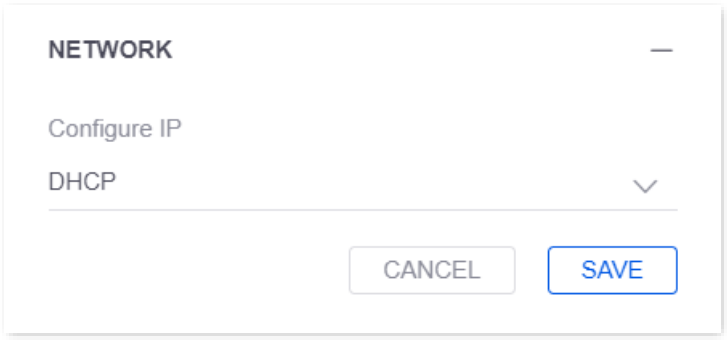
Parameter description

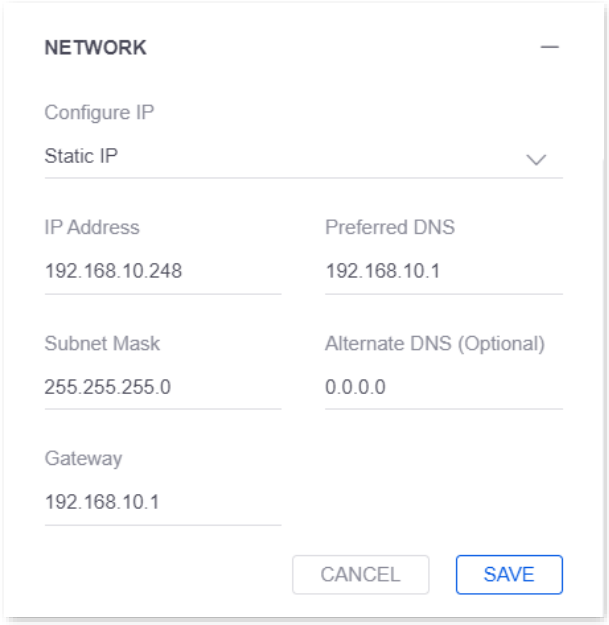
Parameter	Description
VLAN	It is used to enable or disable the VLAN function of the AP.
PVID	Port VLAN ID. It specifies the default VLAN ID to which the AP' trunk port belongs. Only available when the AP' VLAN is enabled.
Management VLAN	It specifies the VLAN ID of the management VLAN. Only available when the AP' VLAN is enabled. After the management VLAN is changed, the Controller must be reconnected to the new management VLAN to manage the AP.

Parameter	Description
Trunk Port	It is used to set the selected Ethernet port (wired LAN0) as the trunk port. By default, it is **LAN0**. The trunk port allows all VLANs to pass. Tip After enabling 802.1Q VLAN, you need to select at least one LAN port as the trunk port. If the AP has only one Ethernet port, then that port will be set as the trunk port by default.
LAN	The Ethernet ports of AP and corresponding VLAN IDs. Tip The Ethernet port not set as a trunk port will be deemed as an access port. You need to set a VLAN ID for the port.

9.3.8 Network

This module is used to modify the LAN IP obtaining mode of the AP.



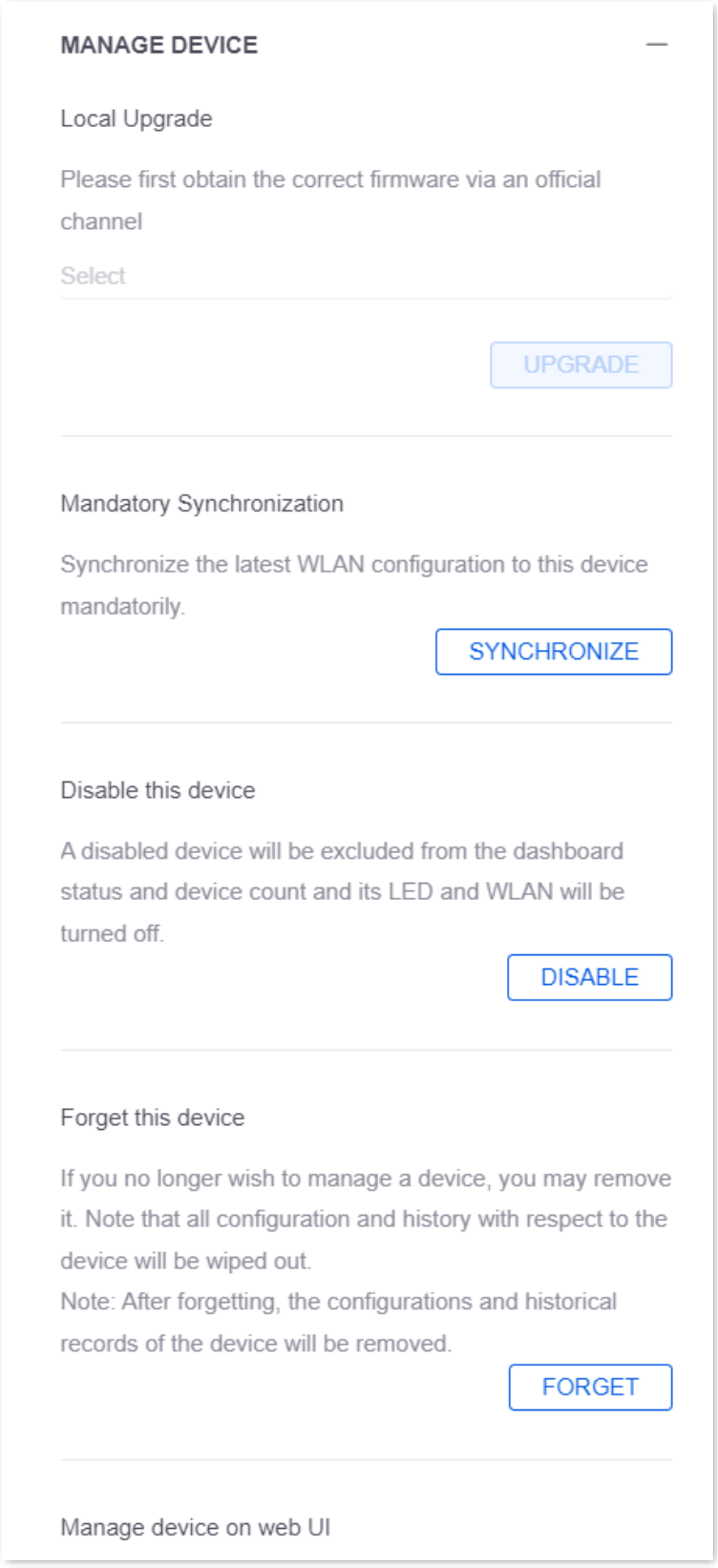


Parameter description

Parameter	Description
Configure IP	It specifies the IP address obtaining mode of the AP. – **DHCP**: the default mode. Under this mode, the AP automatically obtains its IP address, subnet mask, gateway address, and DNS server address from the DHCP server in the network. This mode is applicable to the scenarios where a large number of APs are deployed. – **Static IP**: Under this mode, the IP address, subnet mask, gateway address, and DNS server address of the AP are specified manually. This mode is applicable to the scenarios where only one or several APs are deployed.
IP Address	It specifies the IP address of the AP, and is also the management IP address of the AP. LAN users can visit this IP address to log in to the web UI of the AP.
Subnet Mask	It specifies the subnet mask of the AP, which is used to define the IP address range of the network segment.
Gateway	It specifies the IP address of the default gateway. If you want to connect the AP to the internet, set this parameter to the IP address of the LAN port of the router connected to the internet.
Preferred DNS	It specifies the preferred DNS server address. If the router connected to the internet has the DNS proxy function, you can enter the IP address of its LAN port. Otherwise, enter the correct IP address of the DNS server.
Alternate DNS (Optional)	It specifies the alternate DNS server address. This parameter is optional. If you have two DNS server IP addresses, you can enter the other one here.

9.3.9 Manage Device

This module is used to copy the upgrade the AP locally, mandatorily synchronizing WLAN configuration to the AP, disable and forget the AP, or access the web UI of the AP.



Local Upgrade

This module is used to upgrade the AP by uploading the upgrade firmware stored in a local computer.

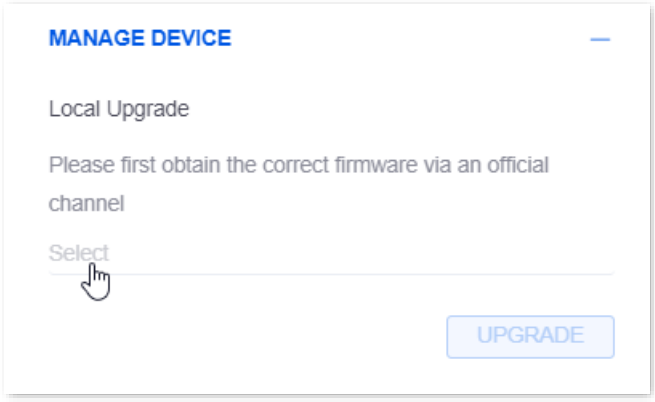
Note

To ensure correct upgrade and avoid device damage,

- Ensure the upgrade file is suitable for the current device.
- Ensure the device is powered on properly during upgrade.

Configuration Procedure

1. Visit the official website of IP-COM www.ip-com.com.cn, download the upgrade firmware of the corresponding AP to your local computer and unzip it. Generally, the suffix of the firmware is generally **.bin**.
2. Log in to the ProFi Software Controller, select your site and choose **DEVICES** ( ).
3. Click an AP, and click at the details panel, then click **MANAGE DEVICE**.
4. Locate **Local Upgrade**, Click **Select** in the text box.



5. Select and upload the upgrade firmware from your computer.

----End

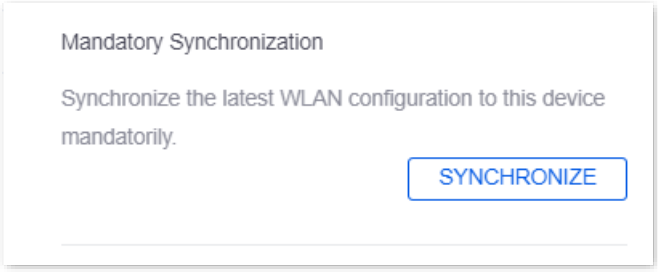
After the upgrade is done, you can view the upgraded firmware version at the **DEVICES** ( ) page, and check whether the version is same as what you just uploaded.

Tip

To improve the stability of AP and experience more functions of the upgraded version, after the finish of upgrade, it is recommended to restore the AP to factory settings and reconfigure the AP.

Mandatory Synchronization

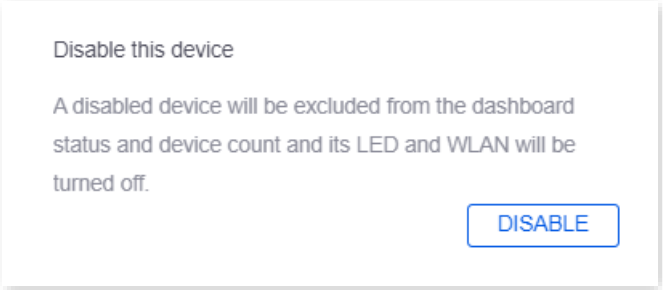
This module enables you to synchronize the latest WLAN configuration created by the site to this AP. For the creation of WLAN configuration, refer to **SETTINGS ( ) > Wireless Networks**.



Disable This Device

Click DISABLE to disable the AP.

After the AP is disabled, its status will be displayed as CONNECTED (DISABLED). Under such circumstances, all functions of the AP cannot be used and its LED indicator and WiFi are both disabled.

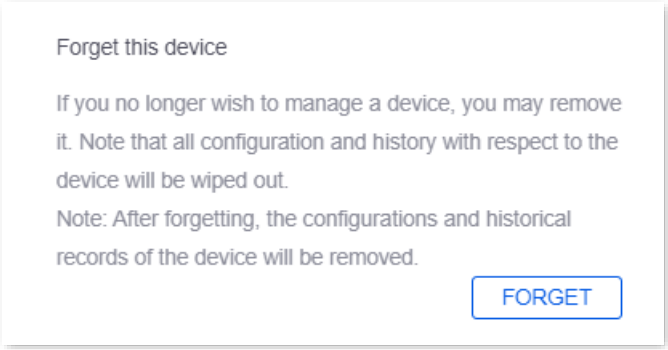


Forget This Device

If you no longer want to manage an AP, you can forget this AP here.

Note

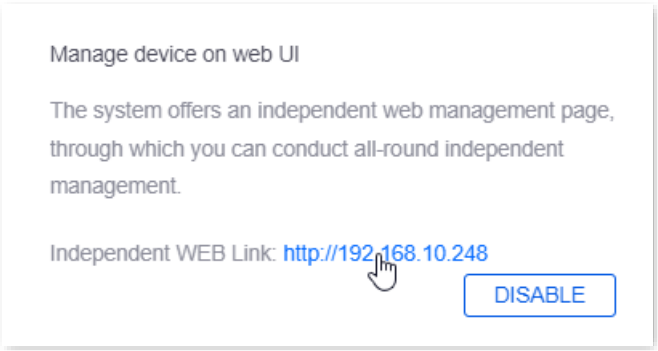
After you forgot the AP, the AP will be restored to factory settings, and all configurations and history of this AP will be cleared. However, the configuration on the **SETTINGS** ( ) page will not be cleared.



Manage Device on Web UI

This module is used to enable or disable the independent web UI management function of the AP.

After it is enabled, if the management computer is deployed locally (in the LAN where the AP is deployed), you can click the **Independent WEB Link** to redirect to the web UI of the AP.

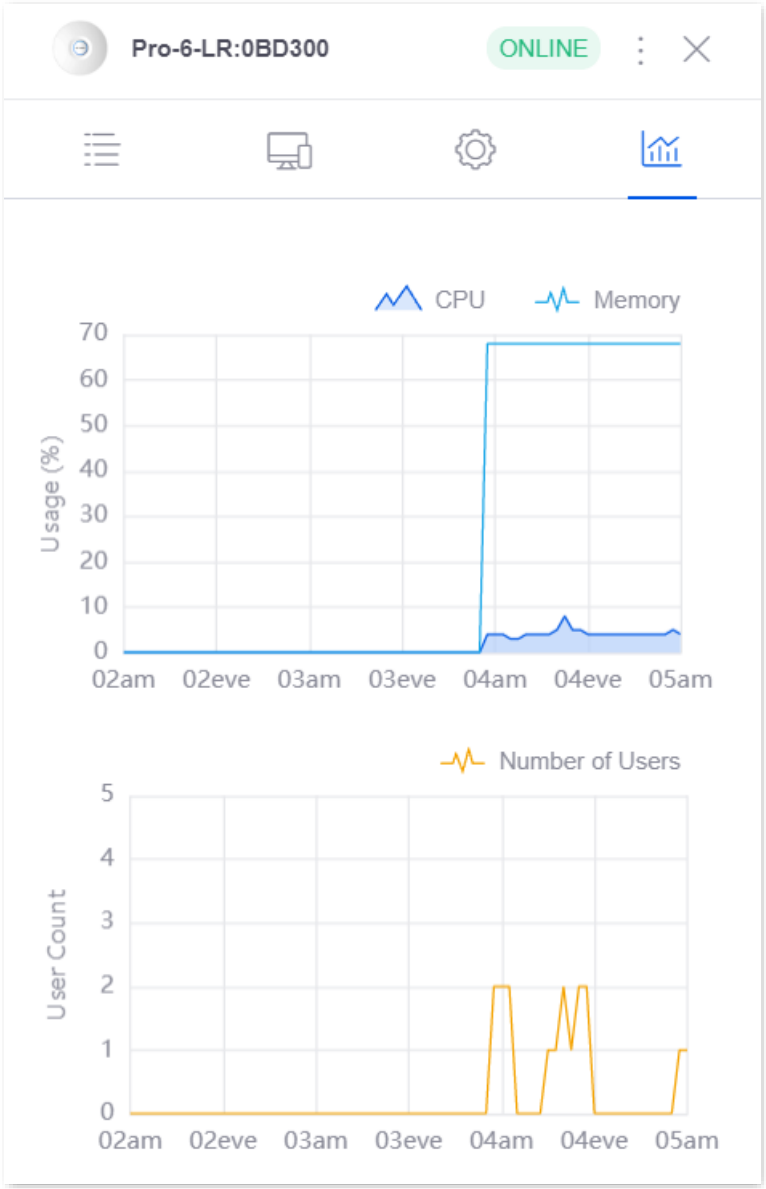


9.4 Stats

This page is used to check the CPU usage, memory usage, and client statistics during the last 72 hours.

Tip

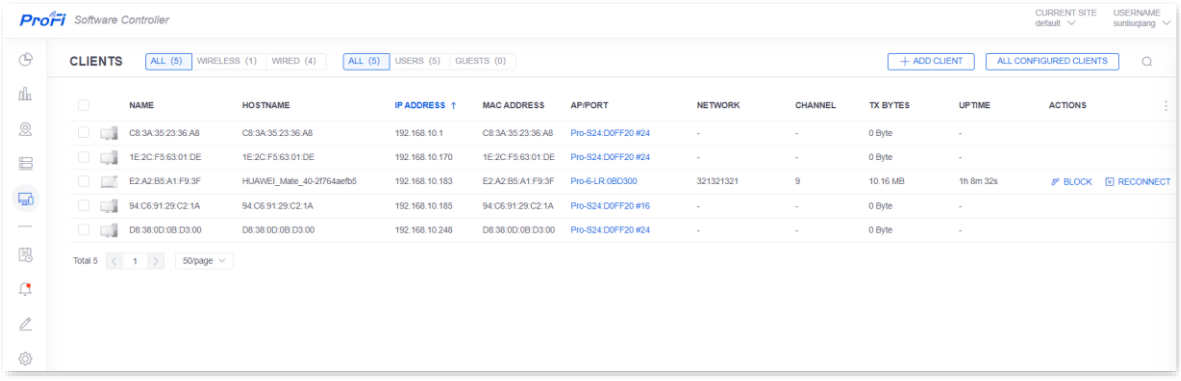
The stats function is valid only when the ProFi Software Controller is running properly. In other words, the statistics during the period when the ProFi Software Controller is closed will not be counted.



10 Client Details

This page is used to check the details of all the clients in the networks under the site.

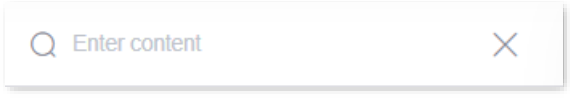
To enter the page, choose **CLIENTS (** **)**. See the following figure.



Filter Target Client Type

- **ALL**: displays all the clients.
- **WIRELESS**: displays all the wireless clients.
- **Wired**: displays all the wired clients.
- **USERS**: displays all the non-authenticated wired and wireless clients.
- **GUESTS**: displays all the authenticated wireless clients.

Search Clients



Enter keywords to easily search for and filter out target contents.

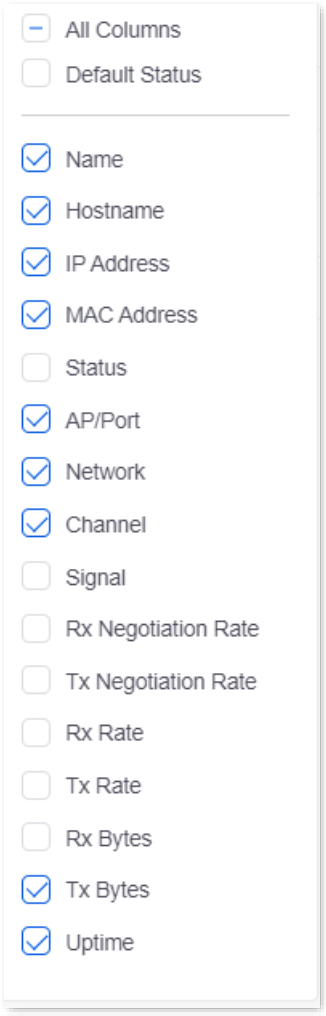
Sort Clients

Click any column header to sort the clients in an ascending or descending order displayed as ↑ or ↓.

Customize Columns

Click ⋮ in the farthest right of the column header to customize columns.

The following figure displays columns customizable for clients.



Column description

Parameter	Description
Name	It specifies the icon and name of the client.
Hostname	It specifies the hostname of the client.
IP Address	It specifies the IP address of the client.
MAC Address	It specifies the physical address of the client.

Parameter	Description
Status	It specifies the authorization status of the client. – **Waiting**: The client is connected to the wireless network with guest network policy enabled, but not authenticated yet (authentication function already enabled). – **Authorized**: – The client is connected to a wireless network with guest network policy enabled and is already authenticated. – The client is connected to a wireless network with guest network policy enabled and does not need to be authenticated (authentication function disabled). – The client is connected to a wireless network with guest network policy disabled. – The client is connected to a wireless network with guest network policy enabled and is already authorized manually.
AP/Port	It specifies the uplink device of the client. Click it to view the details of the uplink device.
Network	It specifies the wireless network to which the wireless client connects.
Channel	It specifies the wireless channel the wireless client utilizes.
Signal	It specifies the signal strength of the wireless client received by the AP.
Rx Negotiation Rate	It specifies the maximum receiving rate at which the client negotiates with the AP.
Tx Negotiation Rate	It specifies the maximum transmitting rate at which the client negotiates with the AP.
Rx Rate	It specifies the real-time receiving rate of the client.
Tx Rate	It specifies the real-time transmitting rate of the client.
Rx Bytes	It specifies the total bytes received by the client.
Tx Bytes	It specifies the total bytes transmitted by the client.
Uptime	It specifies the duration the client has been connected.

Block Wireless Clients

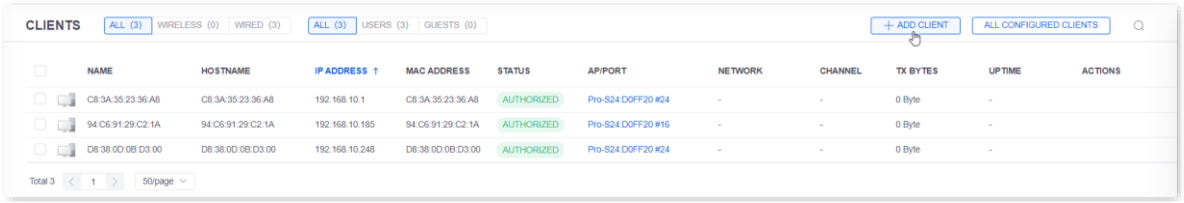
The blocked wireless clients cannot get network access when connecting to the networks managed by the Controller.

Option A: Block Wireless Clients Not Connected to Networks of the Controller

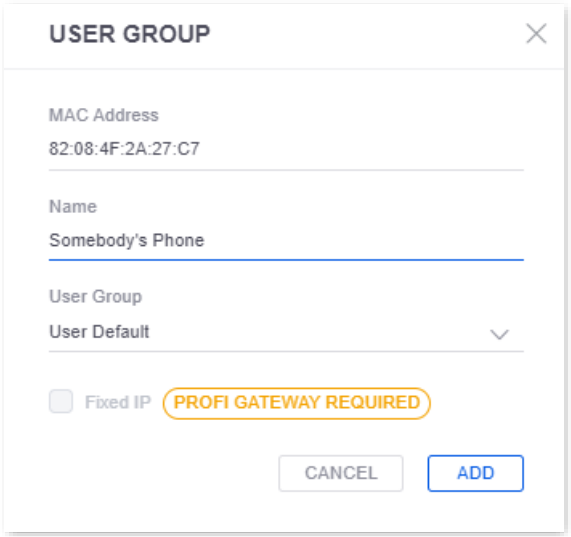
If you want to block a wireless client which is not connected to the network managed by the Controller, you can manually add the client and add the client to the blacklist.

Configuration Procedure:

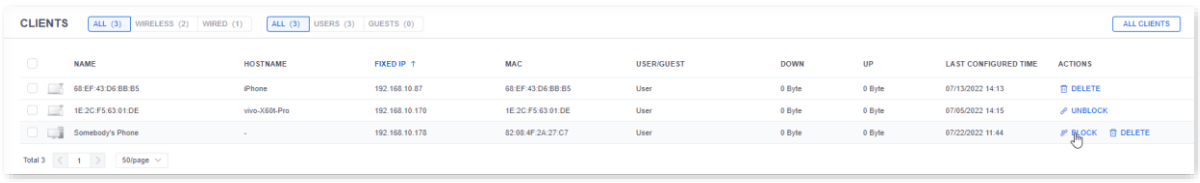
1. Log in to the ProFi Software Controller, select your site and choose **CLIENTS (** **)**.
2. Click ADD CLIENT to add a client manually.



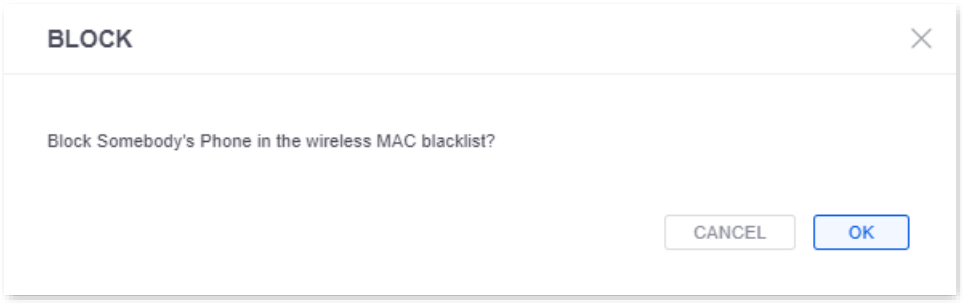
3. In the **USER GROUP** window, configure parameters of the wireless client to be blocked, and click ADD.



4. Click **ALL CONFIGURED CLIENTS**, locate the added wireless client, and click **BLOCK**.



5. Check the message, and click **OK**.



----End

You can also unblock the wireless client to grant network access.

Parameter description

Parameter	Description
MAC Address	It specifies the physical address of the client.
Name	It specifies the name of the client.
User Group	It specifies the user group set for the client.
Fixed IP	It is used to assign a fixed IP address to the client. You can check the box as required. This function is valid only when a ProFi gateway is deployed.
IP Address	It specifies the fixed IP address assigned to the client here. Tip After you saved the configuration, the client will be assigned with this IP address the next time it sends an IP address request.

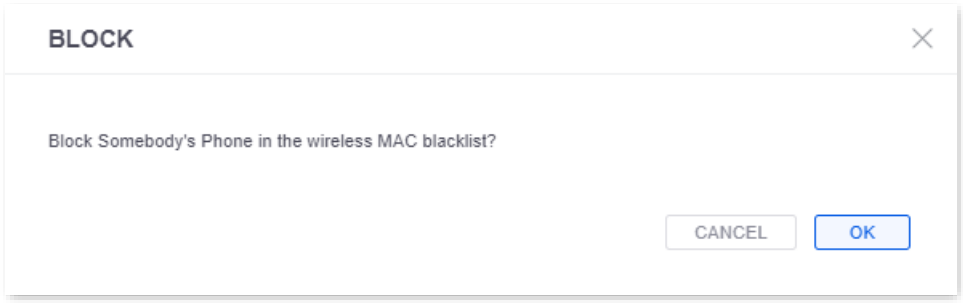
Option B: Block Wireless Clients Connected to Networks of the Controller

If a wireless client is already connected to the network managed by the Controller, you can just click **BLOCK** along the row to block the client from network access.

Configuration Procedure:

1. Log in to the ProFi Software Controller, select your site and choose **CLIENTS (** **)**.
2. Locate the wireless client you want to block, and click **BLOCK**.

3. Check the message, and click **OK**.



----End

You can also unblock the wireless client to grant network access.

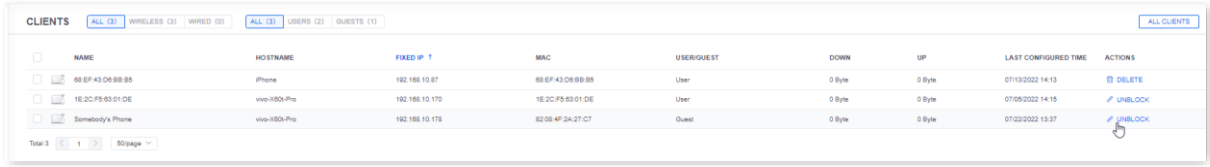
Unblock Wireless Clients

Unblocked wireless clients can obtain the access to the networks managed by the Controller.

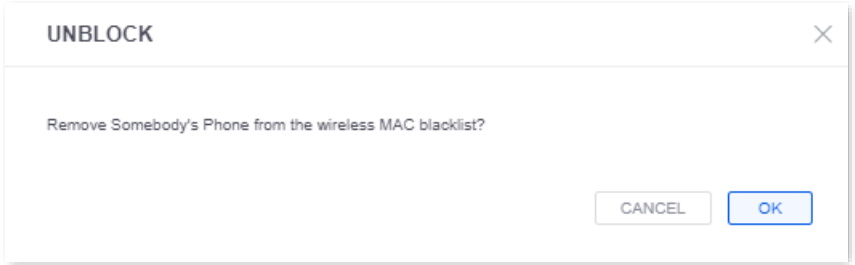
Configuration Procedure:

1. Log in to the ProFi Software Controller, select your site and choose **CLIENTS (** **)**.
2. Click **ALL CONFIGURED CLIENTS**.

3. Locate the wireless client the be unblocked, and click **UNBLOCK**.



4. Check the message, and click **OK**.

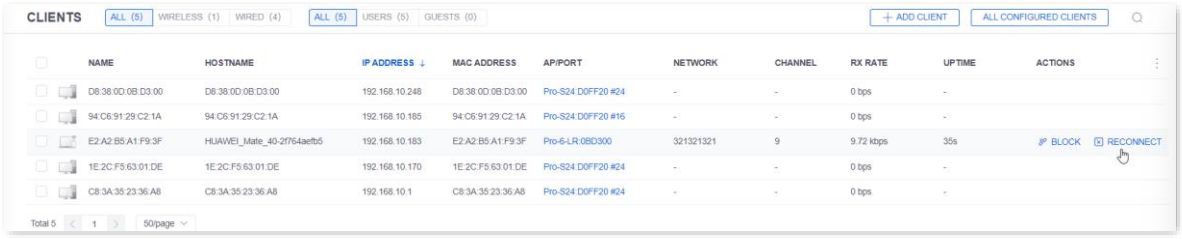


----End

Reconnect Clients

Log in to the ProFi Software Controller, select your site and choose **CLIENTS (** **)**.

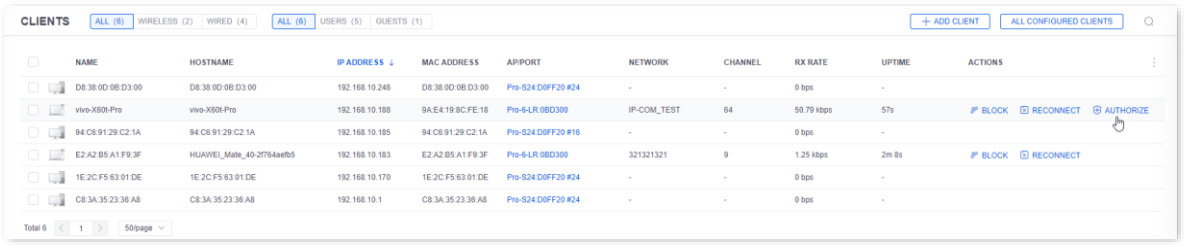
Click RECONNECT to cut off the client connection with the wireless network. If required, the wireless client still can connect to the wireless network again.



Authorize Clients

Log in to the ProFi Software Controller, select your site and choose **CLIENTS (** **)**.

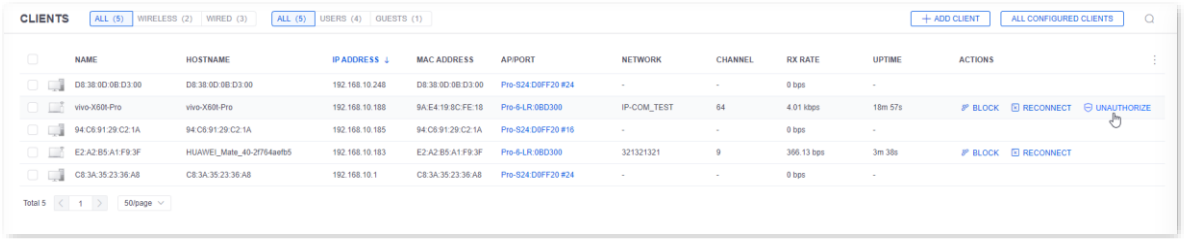
Locate the wireless client, Click AUTHORIZE, then the corresponding client are allowed to connect to the network without authentication.



After you click AUTHORIZE, the button will be changed to UNAUTHORIZE.

Unauthorize Clients

Click UNAUTHORIZE, you can unauthorize certain client for network connection. Then, the client needs authentication before connecting to the guest network.



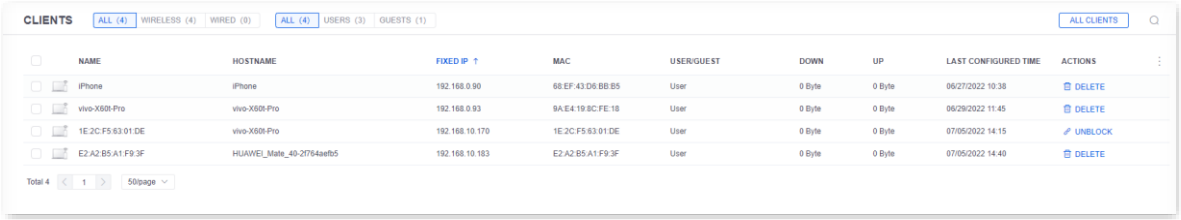
After you click UNAUTHORIZE, the button will be changed to AUTHORIZE.

Check Blacklist of Blocked Clients

Log in to the ProFi Software Controller, select your site, choose **CLIENTS (** **)**, and click ALL CONFIGURED CLIENTS .

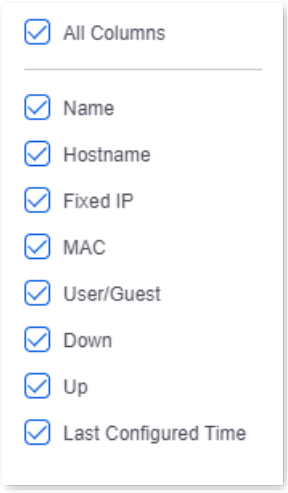
Here, you can:

- View the detailed information of blocked clients;
- Customize the displayed columns of blocked clients;
- Remove the clients from the blacklist;
- Delete records of blocking configuration.



Customize Columns

Click ⋮ in the farthest right of **ALL CONFIGURED CLIENTS** list to customize columns.



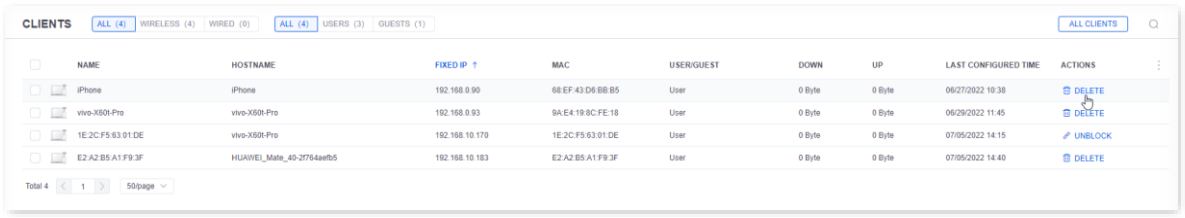
Column description

Parameter	Description
Name	It specifies the icon and name of the client.
Hostname	It specifies the hostname of the client.
Fixed IP	It specifies the IP address of the client.
MAC	It specifies the physical address of the client.

Parameter	Description
User/Guest	It specifies the identity status of the client. – User: It means that the clients do not need to authenticate. – Guest: It means that the clients need to authenticate, including authenticated and unauthenticated clients.
Down	It specifies the total bytes received by the client.
Up	It specifies the total bytes transmitted by the client.
Last Configured Time	It specifies the last configured time on the AP.

Delete Records of Blocking Configuration

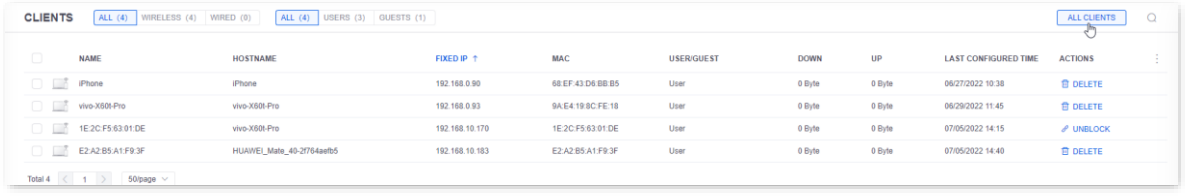
1. Log in to the ProFi Software Controller, select your site, choose **CLIENTS (** **)**, and click **ALL CONFIGURED CLIENTS**.
2. Click **DELETE** to delete the configuration record of the corresponding client.



----End

Check All Clients

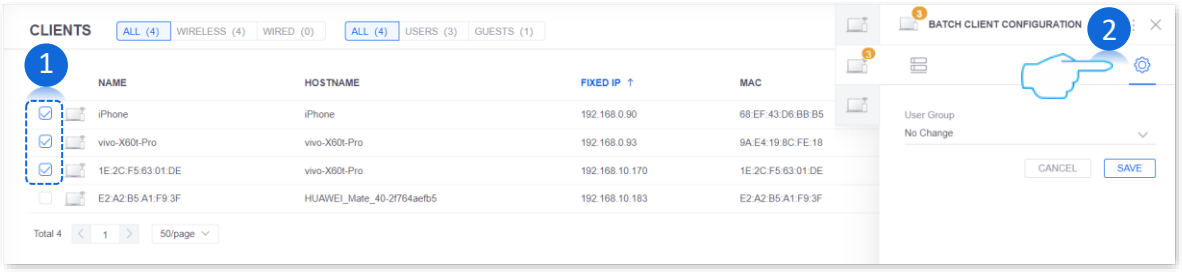
On the ALL CONFIGURED CLIENTS page, click **ALL CLIENTS** to return to the page on which all the clients are displayed.



Batch Client Configuration

Log in to the ProFi Software Controller, select your site, and choose **CLIENTS (** **)**.

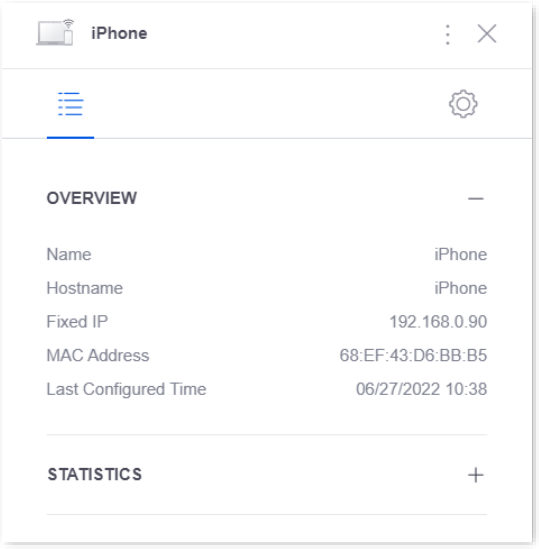
Here, you can select multiple clients, then click **CONFIGURATION** ( ) in the pop-up window to configure the user group of clients in batches.



Single Client Configuration

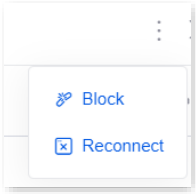
Log in to the ProFi Software Controller, select your site, and choose **CLIENTS (** **)**.

On the **CLIENTS (** **)** page or the **ALL CONFIGURED CLIENTS** page, click a client, then you can view or configure more information of the client on the pop-up window.



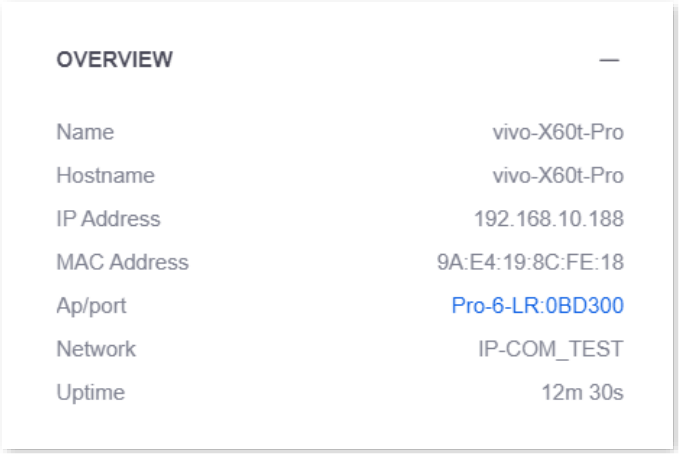
Window elements description

Parameter	Description
Name	It specifies the icon and name of the client. If the remarks of the client are not changed manually, the hostname, MAC address or the host model of the client is displayed here.

Parameter	Description
(More Actions)	Click it to block or reconnect the client from the network. 
(Details)	Click it to view the overview and statistics information of the client.
(Configuration)	Click it to modify the configuration of the client.

Overview

This module enables you to view the name, hostname, IP address and other information of the client.

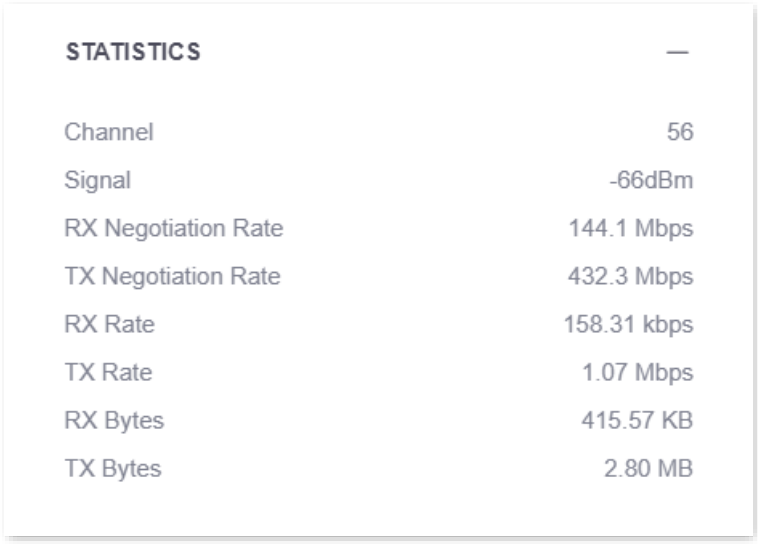


Parameter description

Parameter	Description
Name	It specifies the name of the client.
Hostname	It specifies the hostname of the client.
IP Address	It specifies the IP address of the client.
MAC Address	It specifies the physical address of the client.
AP/Port	It specifies the uplink device of the client.
Network	It specifies the wireless network to which the client connects. Only available for wireless clients.
Uptime	It specifies the duration the client has been connected.

Statistics

This module is used to display the channel utilized by the client, signal strength, rate and other information.



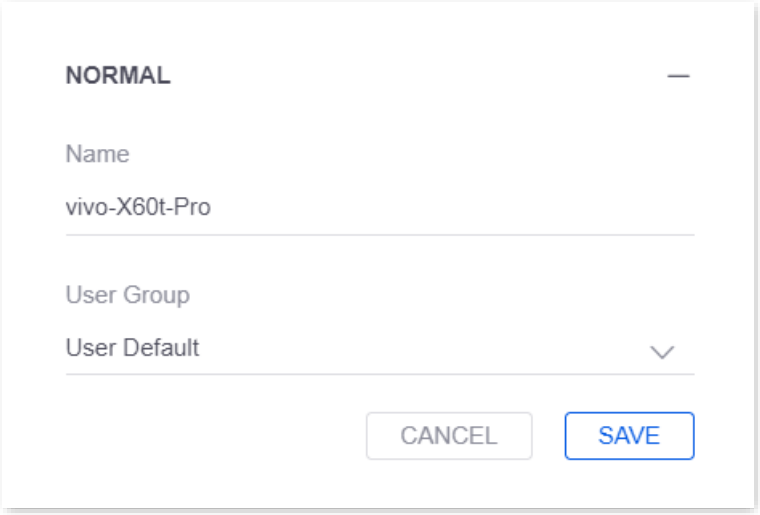
Parameter description

Parameter	Description
Channel	It specifies the wireless channel the client utilizes. Only available for wireless clients.
Signal	It specifies the signal strength of the AP received by the client. Only available for wireless clients.
RX Negotiation Rate	It specifies the maximum receiving/transmitting rate at which the client negotiates with the AP.
TX Negotiation Rate	
RX Rate	It specifies the real-time receiving/transmitting rate of the client.
TX Rate	
RX Bytes	It specifies the total bytes received/transmitted by the client.
TX Bytes	

Configuration

Normal

This module enables you to modify the name and user group of the client.

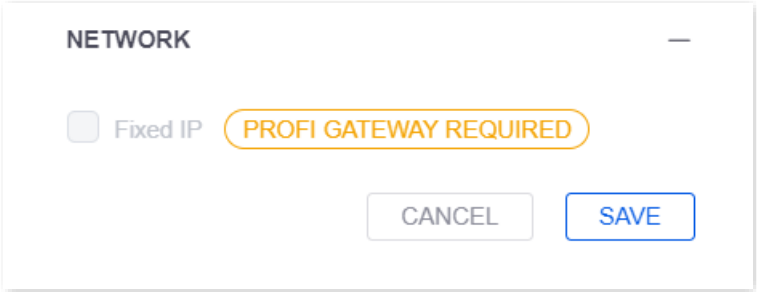


Parameter description

Parameter	Description
Name	It specifies the remarks of the client.
User Group	Select a user group to which the client belongs.

Network

This module is used to assign a fixed IP address to the client.



Parameter description

Parameter	Description
Fixed IP	It is used to assign a fixed IP address to the client. You can check the box as required. This function is valid only when a ProFi gateway is deployed.

Parameter	Description
IP Address	It specifies the fixed IP address assigned to the client here. After you saved the configuration, the client will be assigned with this IP address the next time it sends an IP address request.

11 Configuration Examples

11.1 Example of VLAN Configuration

Networking Requirements

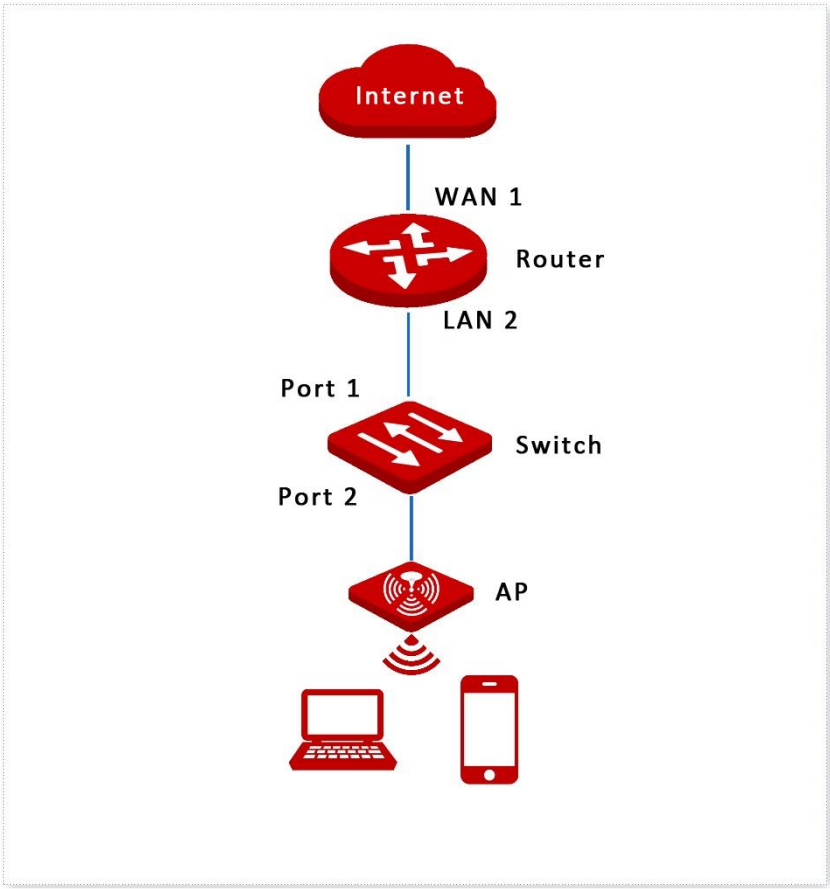
A company uses the IP-COM enterprise router, ProFi switch Pro-S24 and ProFi AP (Pro-6-LR) for network deployment. The switches and APs have been connected to the IP-COM ProFi Software Controller. Now you need to set different network access permissions for staff, managers, and guests.

Solution

Using the wireless policy and VLAN, you can build isolated wireless networks and thus assign different access permissions to staff, managers and guests.

Assume that:

- The wireless network name for staff is **Staff**, and the wireless password is **WMua7848**, belonging to **VLAN10**.
- The wireless network name for managers is **VIP**, and the wireless password is **Vnwa3429**, belonging to **VLAN20**.
- The wireless network name for guests is **Internet**, and no password is set, belonging to **VLAN30**.



Configuration Procedure

I. Configure the router.

Enter the management web UI of the router, set VLANs for LAN2, and configure DHCP servers. Assume that the VLANs, corresponding IP addresses and DHCP servers are list as follows:

User	VLAN ID	IP Address	Address Pool of DHCP Server	Router Port
Staff	10	192.168.10.1/24	192.168.10.2 - 192.168.10.100	LAN2
Manager	20	192.168.20.1/24	192.168.20.2 – 192.168.20.100	LAN2
Guest	30	192.168.30.1/24	192.168.30.2 – 192.168.30.100	LAN2

For the specific configuration, please refer to the user guide of the corresponding router by visiting www.ip-com.com.cn.

II. Configure the AP.

Enable the VLAN function of the AP, and deliver wireless networks to the AP.

The AP enables both 2.4 GHz and 5 GHz wireless networks and separate different user groups through VLAN. See the following table:

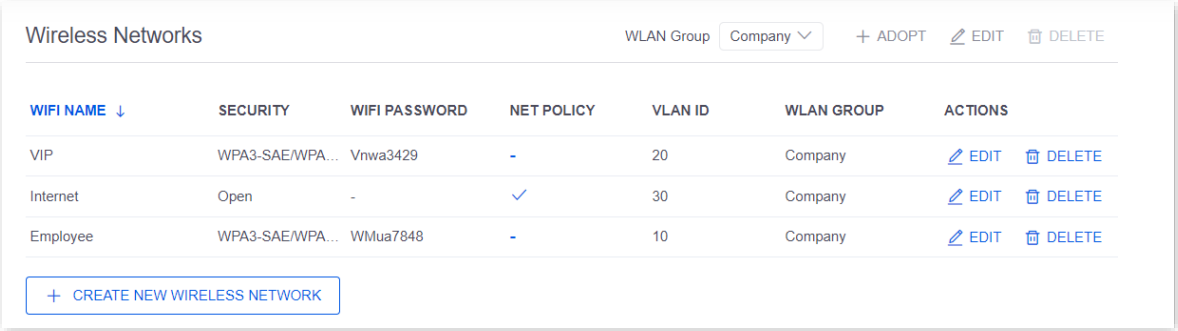
User	SSID	Security Mode	WiFi Password	Guest Network Policy	VLAN ID	WLAN Group
Staff	Staff	WPA3-SAE/ WPA2-PSK	WMua7848	Disabled	10	Company
Manager	VIP	WPA3-SAE/ WPA2-PSK	Vnwa3429	Disabled	20	Company
Guest	Internet	/	/	Enabled	30	Company

1. Configure the wireless networks.

(1) Log in to the ProFi Software Controller, select your site and choose **SETTINGS** ( ) > **Wireless Networks**.

(2) Click **+ ADOPT** to add a WLAN group named **Company**.

(3) Select **Company** from **WLAN Group**, Click **+ CREATE NEW WIRELESS NETWORK** to add the following three wireless policies.



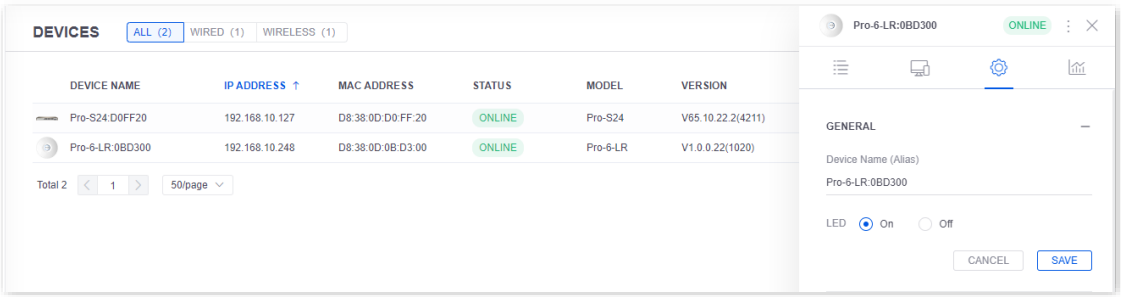
Tip

Generally, a maximum of 128 2.4G/5G clients can be connected to an IP-COM AP. Therefore, check that the total number of **2.4G Maximum Clients/5G Maximum Clients** under all SSIDs in a WLAN group is not greater than 128.

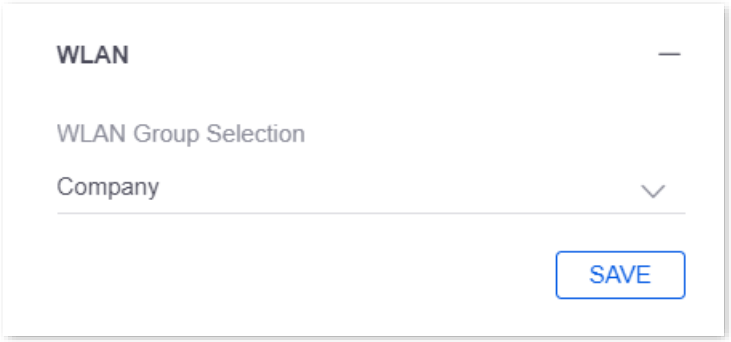
2. Deliver the wireless policies to the AP, and enable the VLAN function of the AP.

(1) Log in to the ProFi Software Controller, select your project and choose **DEVICES** ( ).

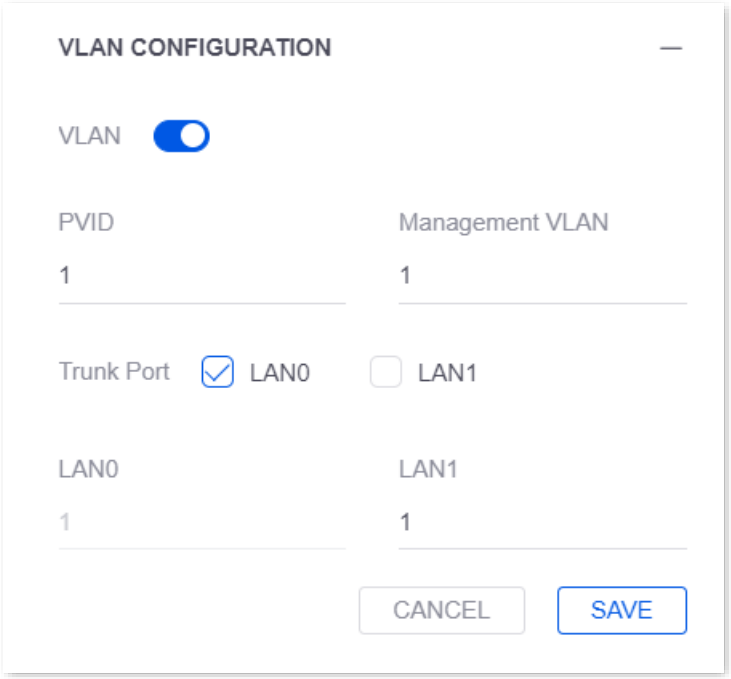
(2) Select your AP and click **CONFIGURATION** ( ) in the panel displayed at the right to access the settings page.



(3) Click **WLAN**, select **Company** from the drop-down list and click **SAVE**.



(4) Click **VLAN CONFIGURATION**, enable **VLAN**, and click **Save**.



III. Configure the switch.

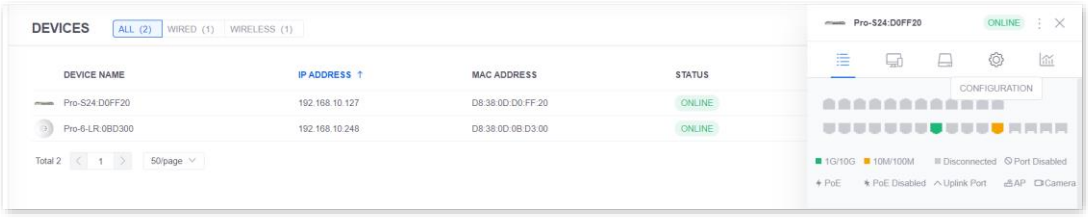
Divide IEEE 802.1q VLAN of the switch as shown below:

Port	VLAN ID (Allowed VLAN ID)	Port Type	PVID
Port 1 (connected to an uplink router)	10, 20, 30	Trunk	1
Port 2 (connect to a downlink AP)	10, 20, 30	Trunk	1

1. Enter the settings page of the switch.

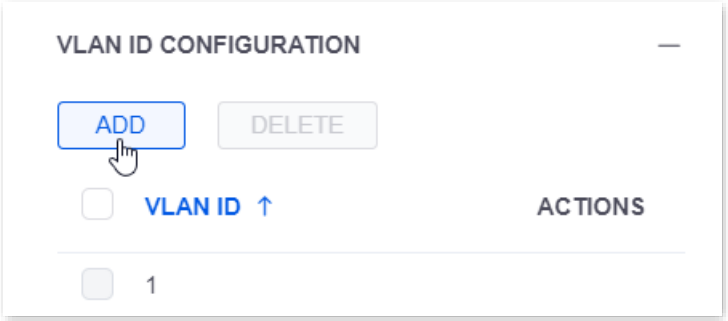
(1) Log in to the ProFi Software Controller, select your project and choose DEVICES ( ).

(2) Select your switch and click **CONFIGURATION** ( ) in the panel displayed on the right.

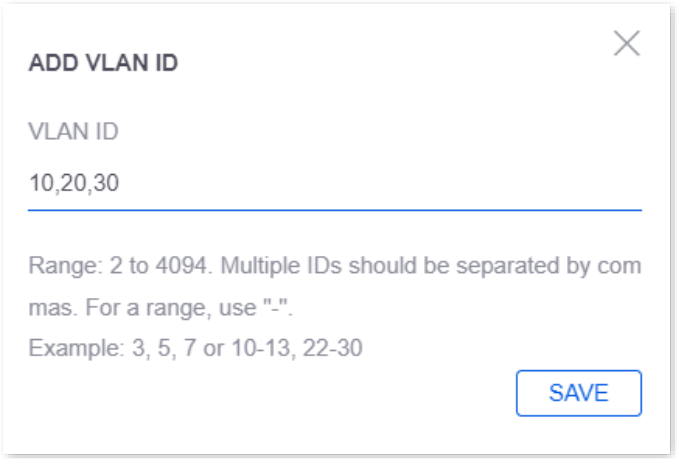


2. Configure the VLAN IDs of the switch.

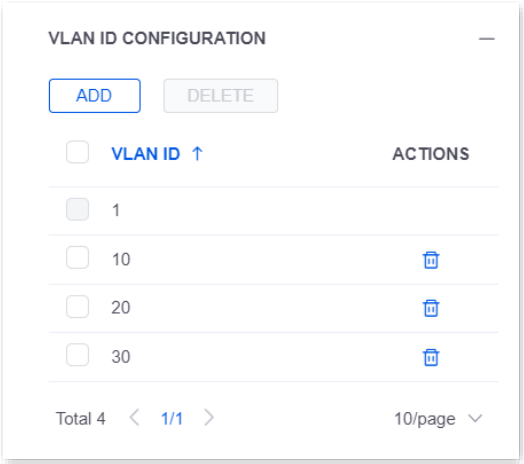
(1) Click **VLAN ID CONFIGURATION**, and click **ADD**.



(2) Set **VLAN ID** to **10, 20, 30**, and click **SAVE**.



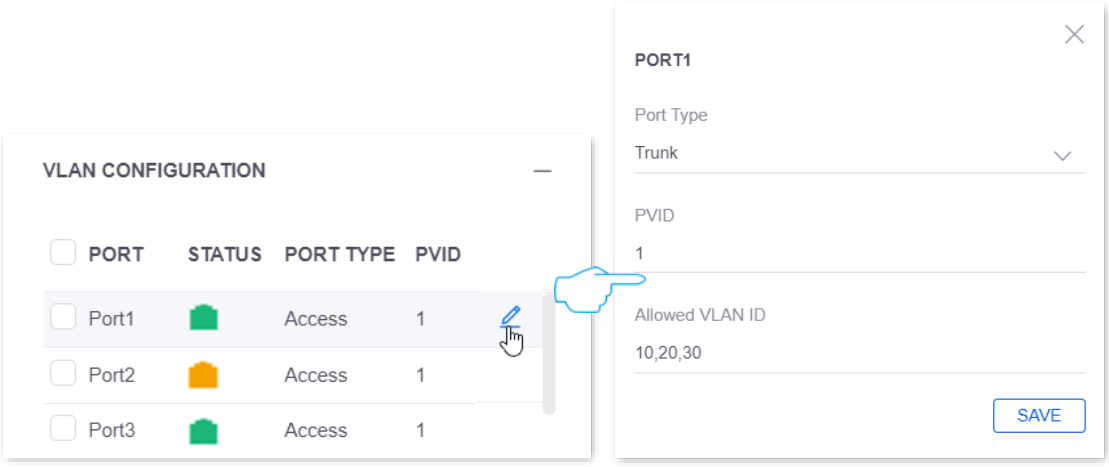
The VLAN is added successfully. See the following figure.



3. Configure the VLAN properties of switch ports

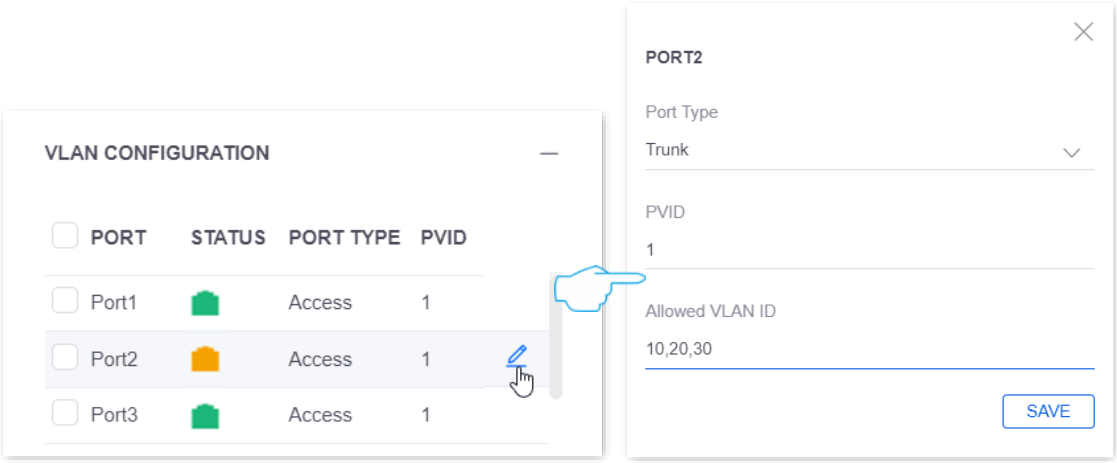
(1) Configure the VLAN property of port 1 (connected to an uplink router).

Click **VLAN CONFIGURATION**, click ✎ at the farthest right of port 1, then set **Port Type** to **Trunk**, set **PVID** to **1**, set **Allowed VLAN ID** to **10,20,30**, and click **SAVE**.



(2) Configure the VLAN property of port 2 (connected to a downstream AP).

Click **VLAN CONFIGURATION**, click ✎ at the farthest right of port 2, then set **Port Type** to **Trunk**, set **PVID** to **1**, set **Allowed VLAN ID** to **10,20,30**, and click **SAVE**.



----End

Verification

- Staff are connected to the wireless network **Staff**, and get the network access by entering the wireless password **WMua7848**.
- Managers are connected to the wireless network **VIP**, and get the network access by entering the wireless password **Vnwa3429**.
- Guests are connected to the wireless network **Internet**, and get the network access without password.

11.2 Examples of Guest Control Configuration

11.2.1 Using Simple Password for Authentication

Networking Requirements

A hotel uses the ProFi AP (Pro-6-LR) for networking and has the following requirements:

- Authentication is not required for staff to access the internet after they connect to the wireless network.
- Authentication is required for guests to access the internet after they connect to the wireless network.

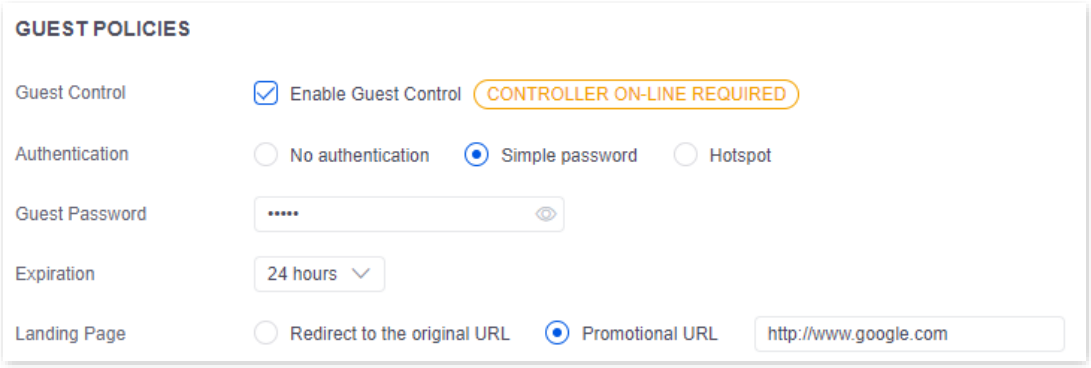
Solution

You can set the authentication mode to Simple Password on the ProFi Software Controller to realize the preceding goals.

Configuration Procedure

I. Set the authentication mode to simple password.

1. Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Guest Control**.
2. Set the authentication policy in the **GUEST POLICIES** module.
   (1) Select **Enable Guest Control**.
   (2) Set **Authentication** to **Simple password** and set your password in **Guest Password**.
   (3) Set **Expiration** as required. **24 hours** is used as an example.
   (4) Set **Landing Page** as required. In this example, Landing Page is set to **Promotional URL (http://www.google.com)**.



3. Customize the guest portal as required in the **PORTAL CUSTOMIZATION**.

The following settings are used as an example.

(1) Set **Title** to **Standard**.

(2) Select **Enable welcome text**, enter welcome texts (**Welcome to IP-COM**) in the displayed dialog box and click **SAVE**.

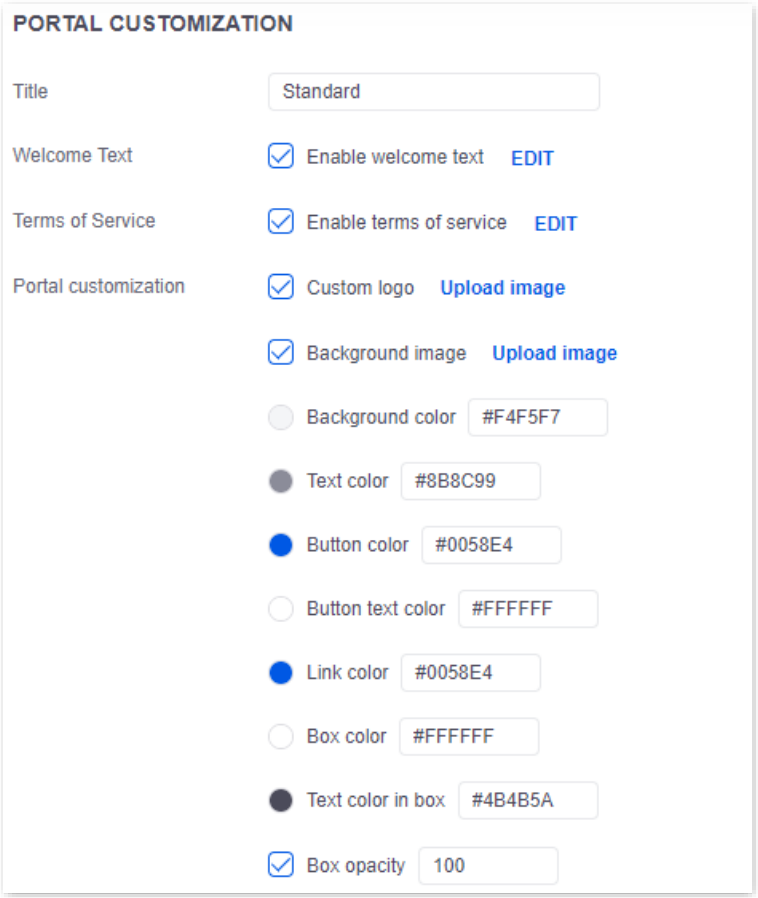
(3) Select **Enable terms of service** and edit the preset terms as required.

(4) Select **Custom logo** and click **Upload image** to upload the logo you want to display on the guest portal.

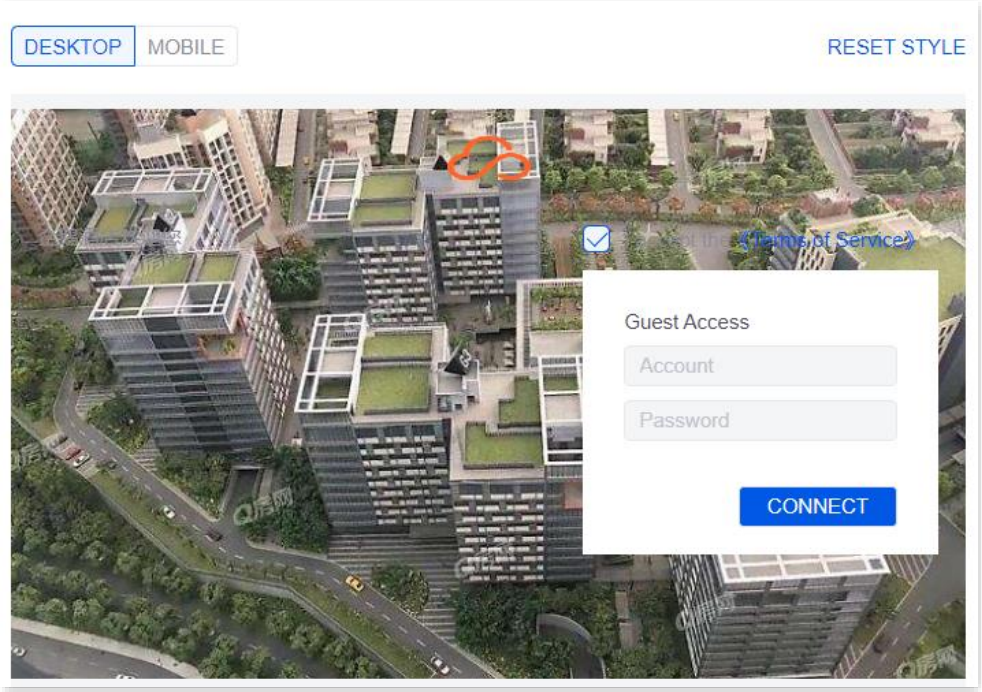
(5) Select **Background image** and click **Upload image** to upload the image that you want to use as the background of the guest portal.

(6) Click the circle icon before **Background color**/**Text color**/**Button color**/**Button text color**/**Link color**/**Box color**/**Text color in box** and choose the color, or directly enter a hexadecimal color code in the text box behind.

(7) Select **Box opacity** and enter the opacity value **100** in the text box behind.



You can preview the customized portal by clicking **DESKTOP** or **MOBILE**.



4. Click **APPLY CHANGES**.

II. Configure the AP.

Deliver wireless networks to the AP as follows:

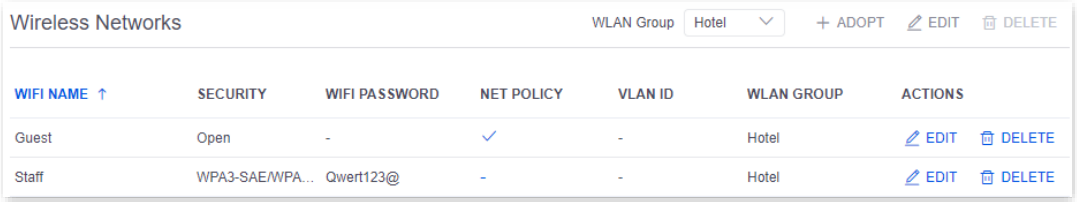
User	SSID	Security Mode	Password	Guest Network Policy	WLAN Group
Guest	Guest	/	/	Enabled	Hotel
Staff	Staff	WPA3-SAE/WPA2-PSK	Qwert123@	Disabled	Hotel

1. Configure the wireless networks.

(1) Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Wireless Networks**.

(2) Click + ADOPT to add a WLAN group named **Hotel**.

(3) Click **+ CREATE NEW WIRELESS NETWORK** to add the following two wireless policies.



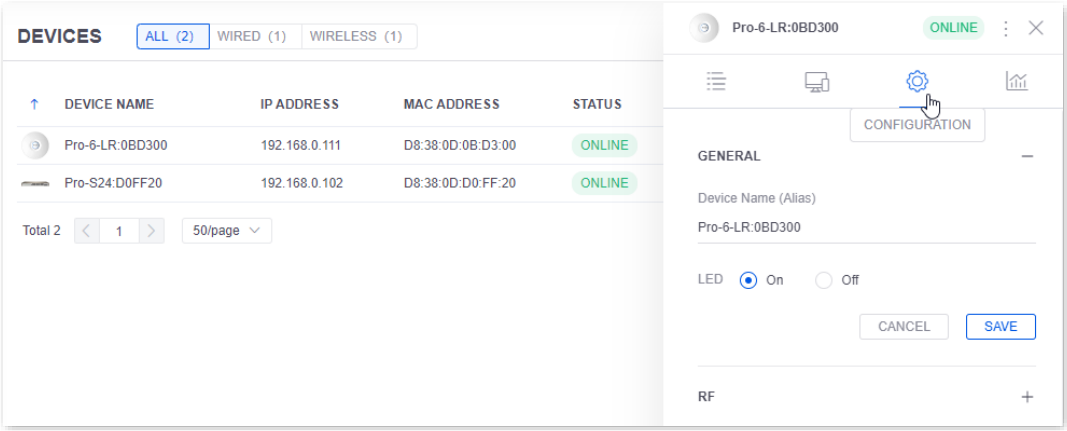
Tip

Generally, a maximum of 128 2.4G/5G clients can be connected to an IP-COM AP. Therefore, check that the total number of **2.4G Maximum Clients** and **5G Maximum Clients** under all SSIDs in the **Hotel** WLAN group is not greater than 128.

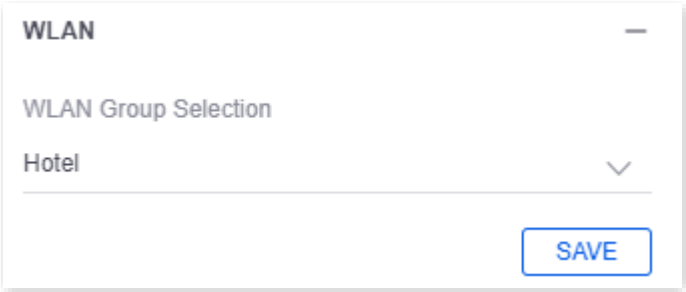
2. Deliver the wireless networks to the AP.

(1) Log in to the ProFi Software Controller, select your project and choose **DEVICES** ( ).

(2) Select your AP and click **CONFIGURATION** ( ) in the panel displayed on the right to access the settings page.



(3) Click **WLAN**, select **Hotel** from the drop-down list and click **SAVE**.



----End

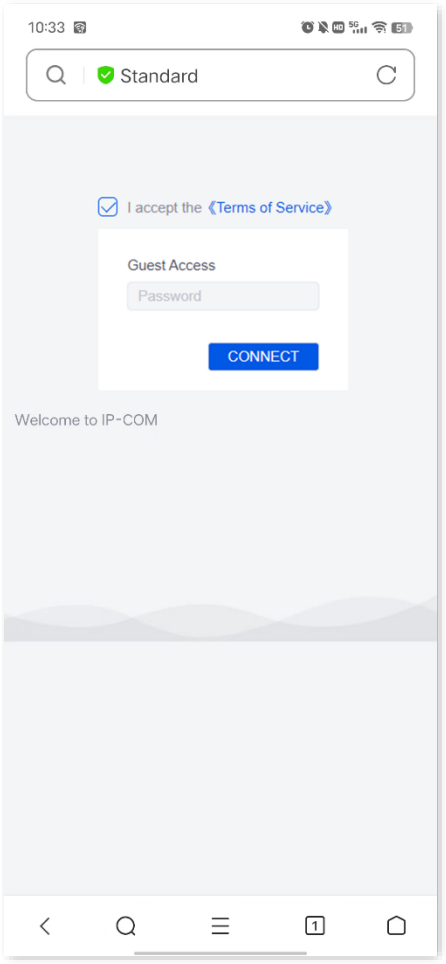
Verification

Authentication is not required when users are connected to the **Staff** wireless network.

Authentication is required when users are connected to the **Guest** wireless network. The verification procedure is as follows:

1. When a wireless client such as mobile phone is connected to the **Guest** wireless network, it will be redirected to the authentication page automatically. If not, open a browser and visit any website to access the page.

2. Select **I accept the <<Terms of Service>>**, enter the password and click **CONNECT.**



After the authentication completes successfully, the page will be redirected to **www.google.com**.

11.2.2 Using Account and Password for Authentication

Networking Requirements

A hotel uses the ProFi AP (Pro-6-LR) for networking and has the following requirements:

- Authentication is not required for staff to access the internet after they connect to the wireless network.
- Authentication is required for guests to access the internet after they connect to the wireless network.

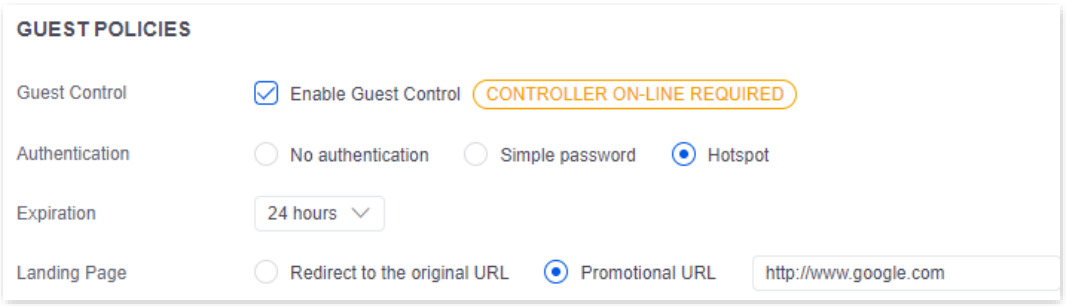
Solution

You can set the authentication mode to Account & Password on the ProFi Software Controller to realize the preceding goals.

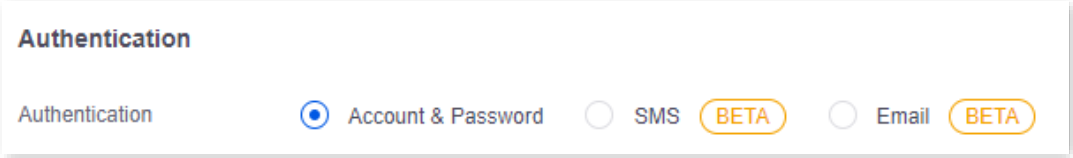
Procedure

I. Set the authentication mode to Account & Password.

1. Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Guest Control**.
2. Set the authentication policy in the **GUEST POLICIES** module.
   (1) Select **Enable Guest Control**.
   (2) Set **Authentication** to **Hotspot**.
   (3) Set **Expiration** as required. **24 hours** is used as an example.
   (4) Set **Landing Page** as required. In this example, **Landing Page** is set to **Promotional URL (http://www.google.com)**.



3. In the **Authentication** module, select **Account & Password**.



4. Customize the guest portal as required in the **PORTAL CUSTOMIZATION**.

The following settings are used as an example.

(1) Set **Title** to **Standard**.

(2) Select **Enable welcome text**, enter welcome texts (**Welcome to IP-COM**) in the displayed dialog box and click **SAVE**.

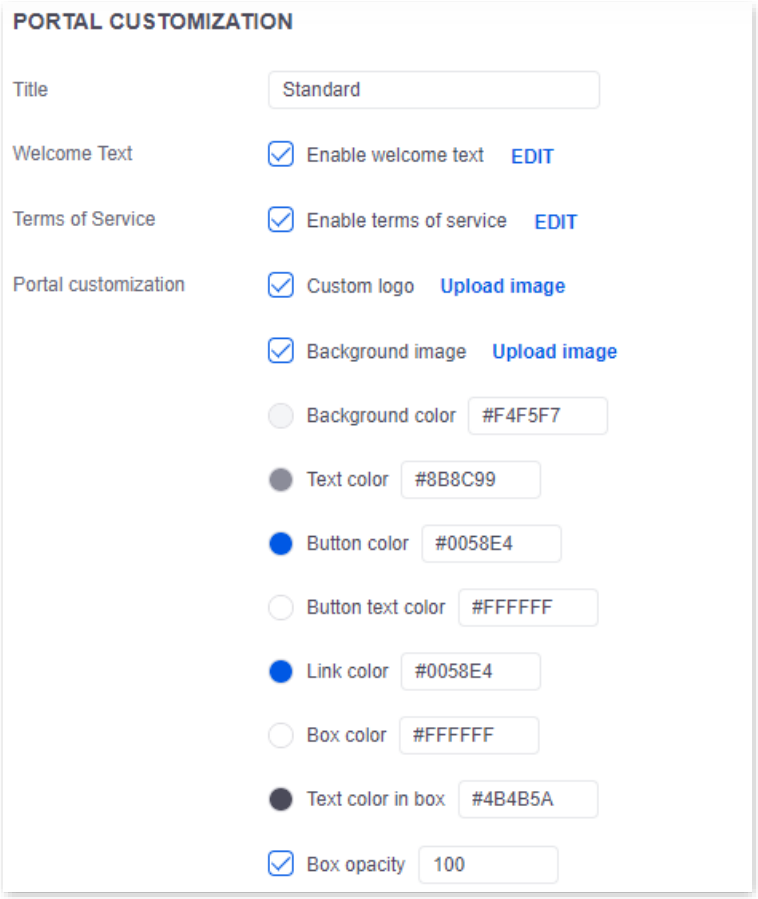
(3) Select **Enable terms of service** and edit the preset terms as required.

(4) Select **Custom logo** and click **Upload image** to upload the logo you want to display on the guest portal.

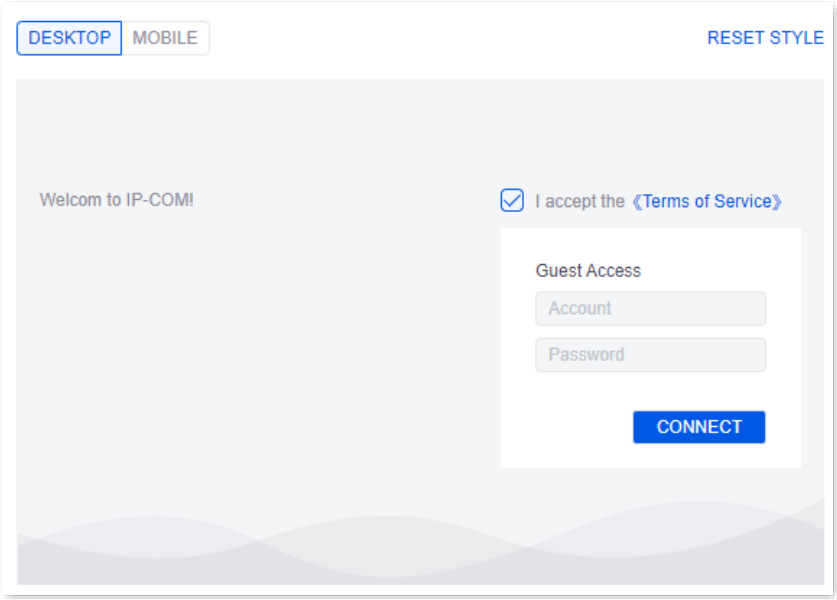
(5) Select **Background image** and click **Upload image** to upload the image that you want to use as the background of the guest portal.

(6) Click the circle icon before **Background color**/**Text color**/**Button color**/**Button text color**/**Link color**/**Box color**/**Text color in box** and choose the color, or directly enter a hexadecimal color code in the text box behind.

(7) Select **Box opacity** and enter the opacity value **100** in the text box behind.



You can preview the customized portal by clicking **DESKTOP** or **MOBILE**.

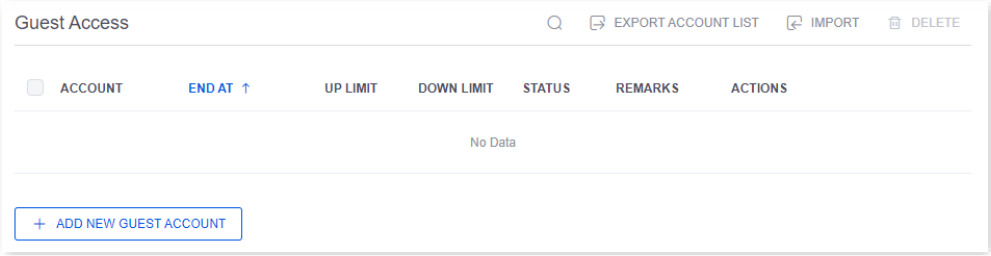


5. Click **APPLY CHANGES**.

II. Add an authentication account.

1. Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Guest Access**.

2. Click **+ ADD NEW GUEST ACCOUNT**.



3. Set the following parameters on the **ADD NEW GUEST ACCOUNT** page.

   The following information is used as an example.

   (1) Set both **Username** and **Password** to **IP_COM**.

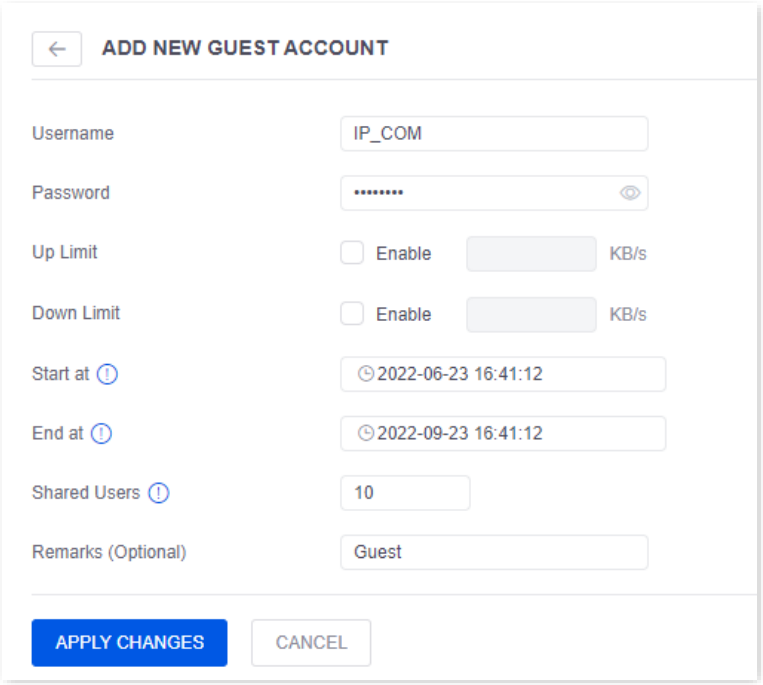
   (2) Keep default settings of **Up Limit** and **Down Limit**.

   (3) Set **Start at** to the time when the account starts to take effect. Here it is set to the current time.

   (4) Set **End at** to the time when the account expires. Here it is set to **2022-09-23 16:41:12**.

   (5) Set **Shared Users** to the number of users that are allowed to use the account for authentication at the same time. Here it is set to **10**.

   (6) Enter account description in **Remarks (Optional)**. Here **Guest** is input.



4. Click **APPLY CHANGES**.

III. Configure the AP.

Deliver wireless networks to the AP as follows:

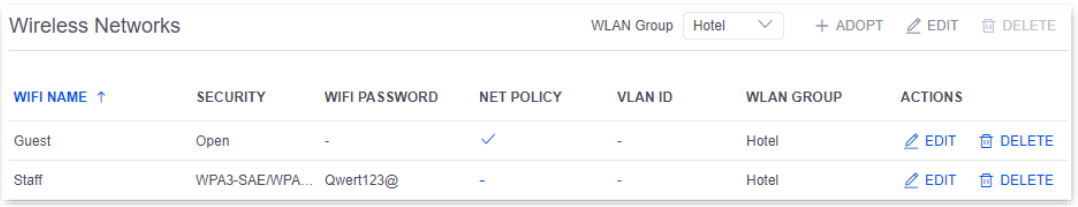
User	SSID	Security Mode	Password	Guest Network Policy	WLAN Group
Guest	Guest	/	/	Enabled	Hotel
Staff	Staff	WPA3-SAE/WPA2-PSK	Qwert123@	Disabled	Hotel

1. Configure the wireless networks.

(1) Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Wireless Networks**.

(2) Click + ADOPT to add a WLAN group named **Hotel**.

(3) Click **+ CREATE NEW WIRELESS NETWORK** to add the following two wireless policies.



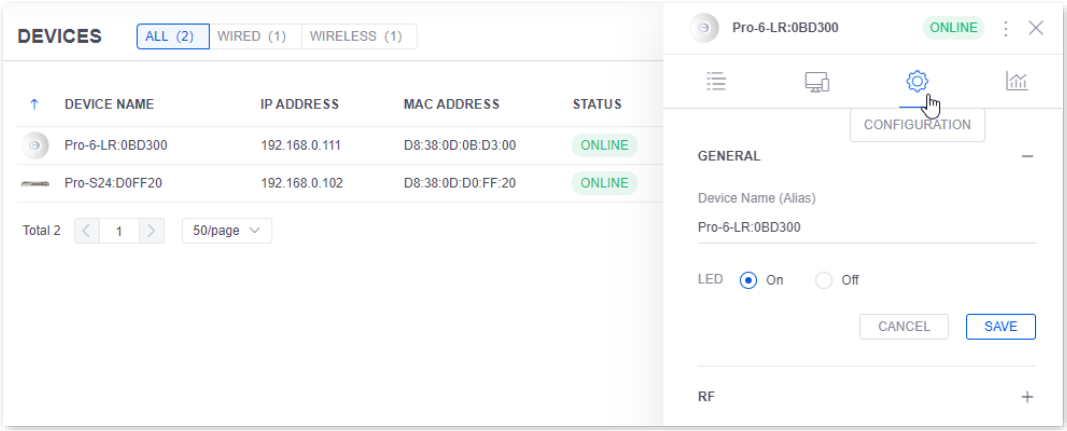
Tip

Generally, a maximum of 128 2.4G/5G clients can be connected to an IP-COM AP. Therefore, check that the total number of **2.4G Maximum Clients** and **5G Maximum Clients** under all SSIDs in the **Hotel** WLAN group is not greater than 128.

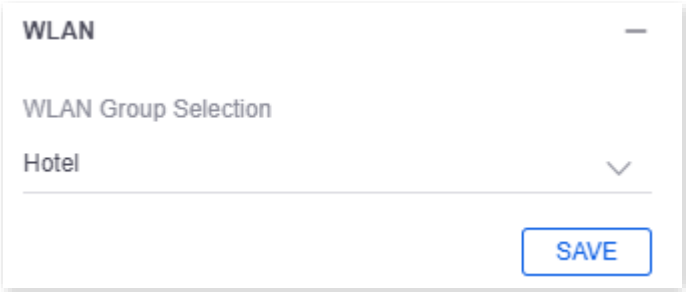
2. Deliver the wireless networks to the AP.

(1) Log in to the ProFi Software Controller, select your project and choose **DEVICES** ( ).

(2) Select your AP and click **CONFIGURATION** ( ) in the panel displayed on the right to access the settings page.



(3) Click **WLAN**, select **Hotel** from the drop-down list and click **SAVE**.



----End

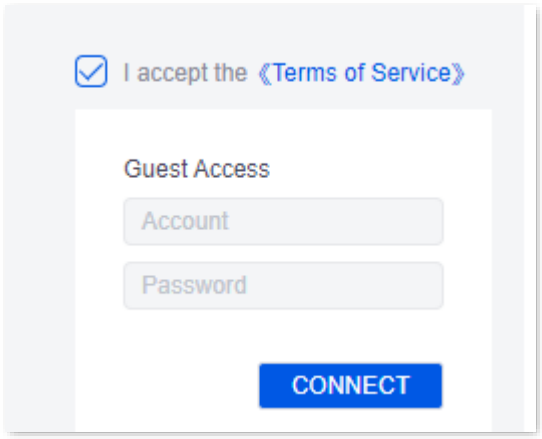
Verification

Authentication is not required when users are connected to the **Staff** wireless network.

Authentication is required when users are connected to the **Guest** wireless network. The verification procedure is as follows:

1. When a wireless client such as mobile phone is connected to the **Guest** wireless network, it will be redirected to the authentication page automatically. If not, open a browser and visit any website to access the page.

2. Select **I accept the <<Terms of Service>>**, enter the authentication account and password and click **CONNECT**.



After the authentication completes successfully, the page will be redirected to **www.google.com**.

11.2.3 Using SMS for Authentication

Networking Requirements

A hotel uses the ProFi AP (Pro-6-LR) for networking and has the following requirements:

- Authentication is not required for staff to access the internet after they connect to the wireless network.
- Authentication is required for guests to access the internet after they connect to the wireless network.

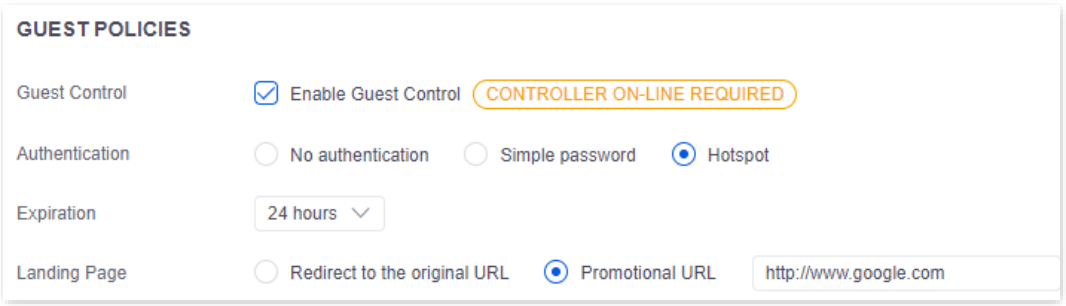
Solution

You can set the authentication mode to SMS on the ProFi Software Controller to realize the preceding goals.

Procedure

I. Set the authentication mode to SMS.

1. Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Guest Control**.
2. Set the authentication policy in the **GUEST POLICIES** module.
   (1) Select **Enable Guest Control**.
   (2) Set **Authentication** to **Hotspot**.
   (3) Set **Expiration** as required. **24 hours** is used as an example.
   (4) Set **Landing Page** as required. In this example, **Landing Page** is set to **Promotional URL (http://www.google.com).**



3. In the **Authentication** module, select **SMS** and set the following parameters.

   The following information is used as an example.

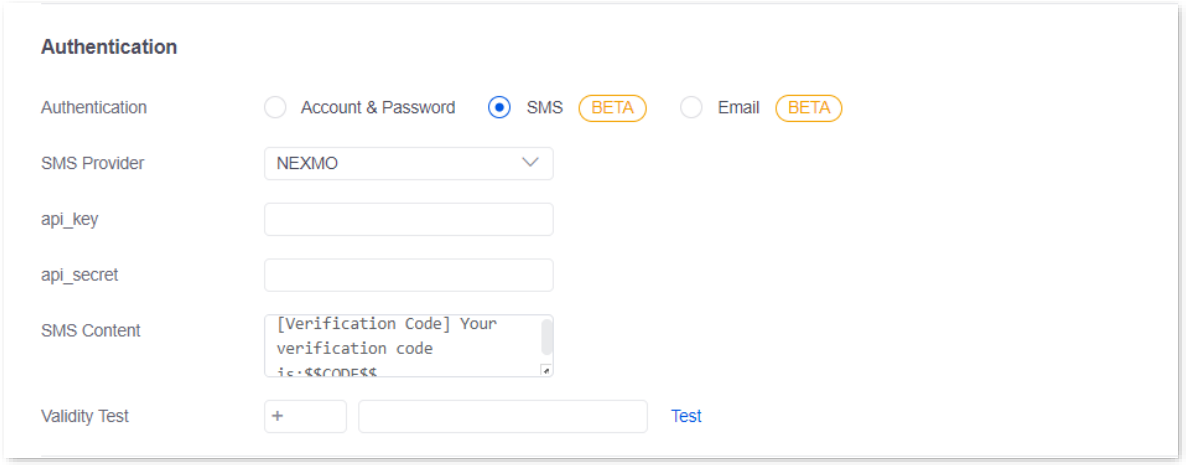
   (1) Set **SMS Provider** to **NEXMO**, which is the SMS service provider.

(2) Enter the **api_key** and **api_secret** applied from NEXMO.

(3) Edit **SMS Content**

(4) Enter a mobile number in **Validity Test** and click **Test**.

If a message indicating that the verification passed is displayed on the page and the mobile number receives the SMS, the configuration is correct.



4. Customize the guest portal as required in the **PORTAL CUSTOMIZATION**.

The following settings are used as an example.

(1) Set **Title** to **Standard**.

(2) Select **Enable welcome text**, enter welcome texts (**Welcome to IP-COM**) in the displayed dialog box and click **SAVE**.

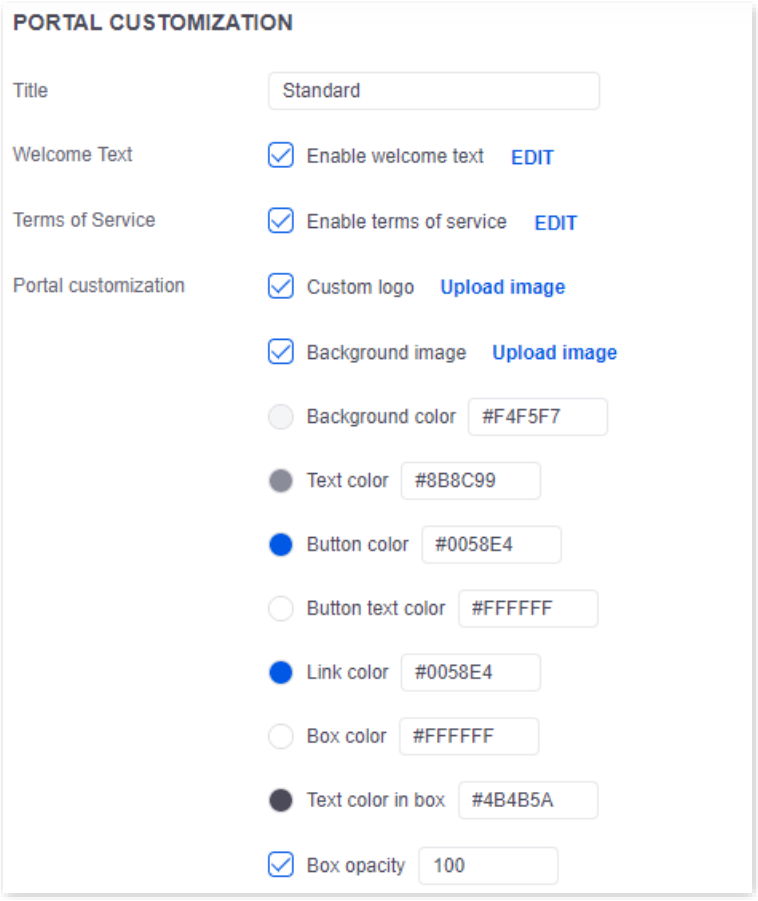
(3) Select **Enable terms of service** and edit the preset terms as required.

(4) Select **Custom logo** and click **Upload image** to upload the logo you want to display on the guest portal.

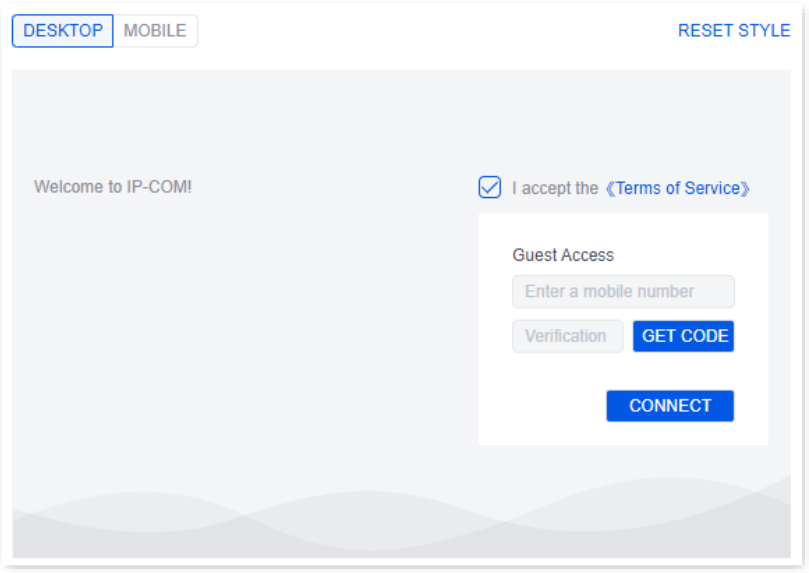
(5) Select **Background image** and click **Upload image** to upload the image that you want to use as the background of the guest portal.

(6) Click the circle icon before **Background color**/**Text color**/**Button color**/**Button text color**/**Link color**/**Box color**/**Text color in box** and choose the color, or directly enter a hexadecimal color code in the text box behind.

(7) Select **Box opacity** and enter the opacity value **100** in the text box behind.



You can preview the customized portal by clicking **DESKTOP** or **MOBILE**.



5. Click **APPLY CHANGES**.

II. Configure the AP.

Deliver wireless networks to the AP as follows:

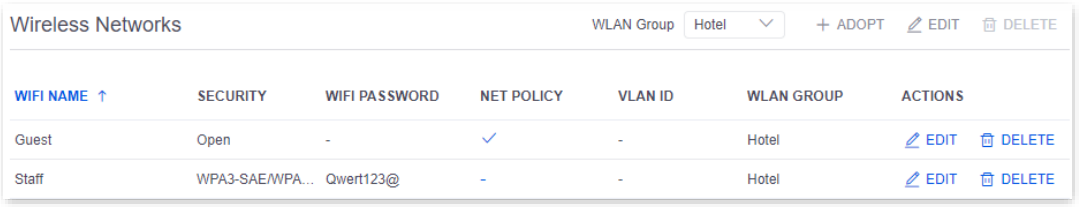
User	SSID	Security Mode	Password	Guest Network Policy	WLAN Group
Guest	Guest	/	/	Enabled	Hotel
Staff	Staff	WPA3-SAE/WPA2-PSK	Qwert123@	Disabled	Hotel

1. Configure the wireless networks.

   (1) Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Wireless Networks**.

   (2) Click + ADOPT to add a WLAN group named **Hotel**.

   (3) Click **+ CREATE NEW WIRELESS NETWORK** to add the following two wireless policies.



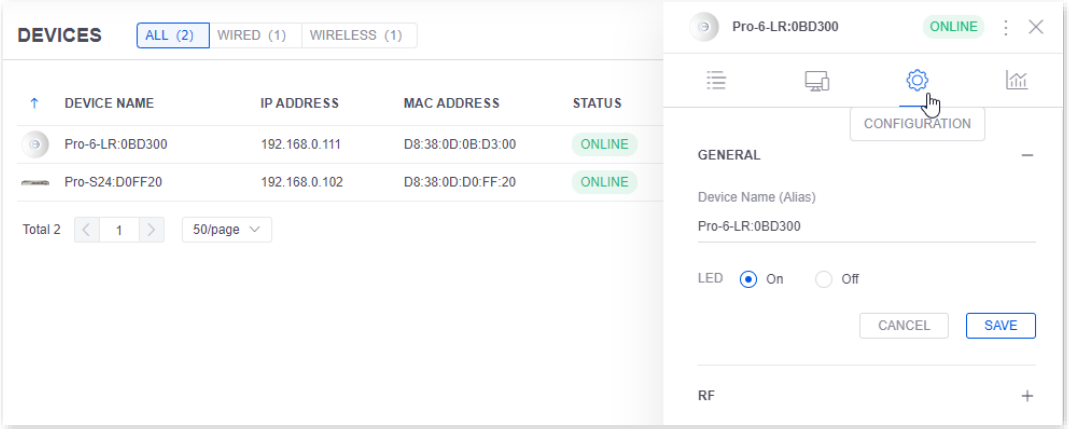
Tip

Generally, a maximum of 128 2.4G/5G clients can be connected to an IP-COM AP. Therefore, check that the total number of **2.4G Maximum Clients** and **5G Maximum Clients** under all SSIDs in the **Hotel** WLAN group is not greater than 128.

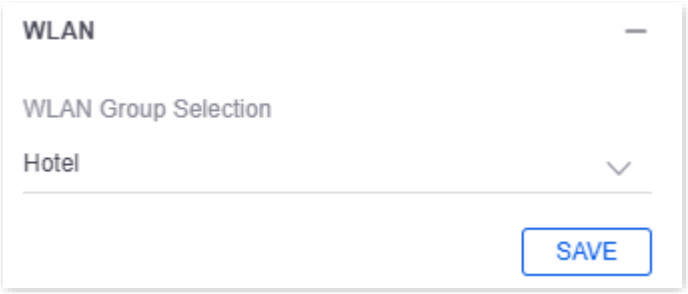
2. Deliver the wireless networks to the AP.

   (1) Log in to the ProFi Software Controller, select your project and choose **DEVICES** ( ).

   (2) Select your AP and click **CONFIGURATION** ( ) in the panel displayed on the right to access the settings page.



   (3) Click **WLAN**, select **Hotel** from the drop-down list and click **SAVE**.



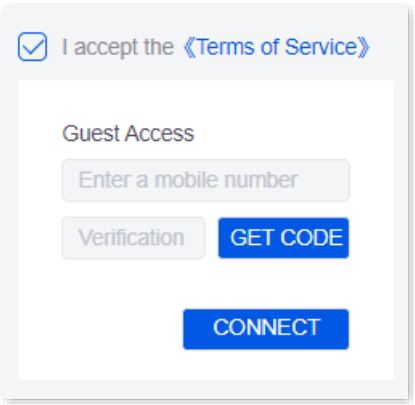
----End

Verification

Authentication is not required when users are connected to the **Staff** wireless network.

Authentication is required when users are connected to the **Guest** wireless network. The verification procedure is as follows:

1. When a wireless client such as mobile phone is connected to the **Guest** wireless network, it will be redirected to the authentication page automatically. If not, open a browser and visit any website to access the page.
2. Select **I accept the <<Terms of Service>>**, enter your mobile number and click **GET CODE**.
3. Enter the received verification code and click **CONNECT**.



After the authentication completes successfully, the page will be redirected to **www.google.com**.

11.2.4 Using Email for Authentication

Networking Requirements

A hotel uses the ProFi AP (Pro-6-LR) for networking and has the following requirements:

- Authentication is not required for staff to access the internet after they connect to the wireless network.
- Authentication is required for guests to access the internet after they connect to the wireless network.

Solution

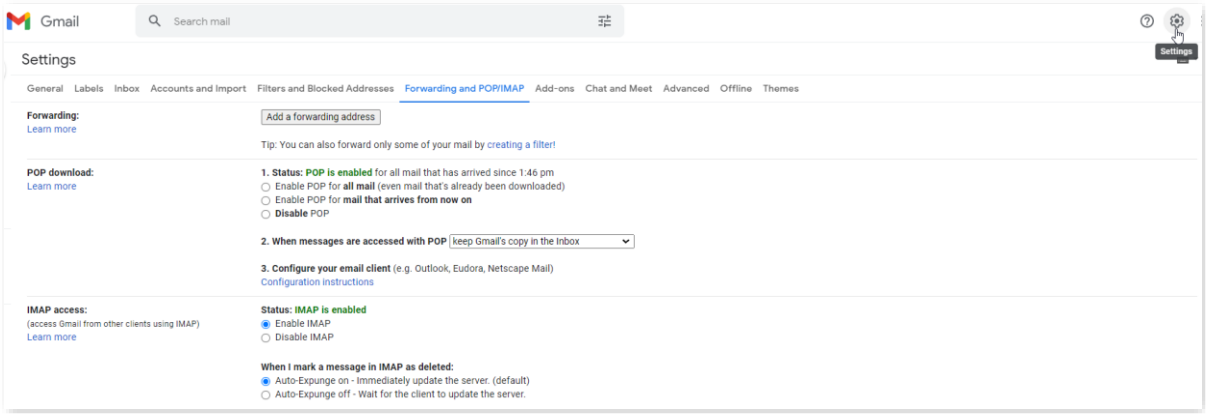
You can set the authentication mode to Email on the ProFi Software Controller to realize the preceding goals. Assume that the email configuration parameters are as follows:

- SMTP Server Address: smtp.gmail.com
- SMTP Server Port: 465
- Email of Sender: Tom78463@gmail.com
- Email of Receiver: Tst78463@gmail.com

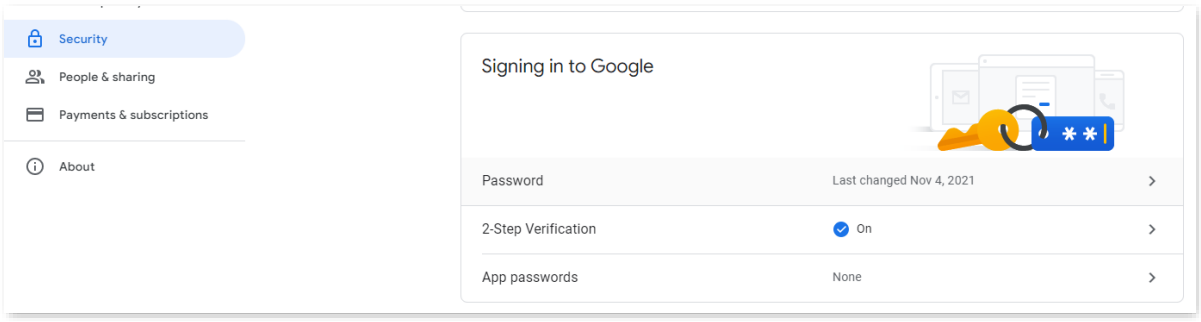
Procedure

I. Enable the SMTP service of email settings and get the email password for the SMTP settings (Gmail as an example).

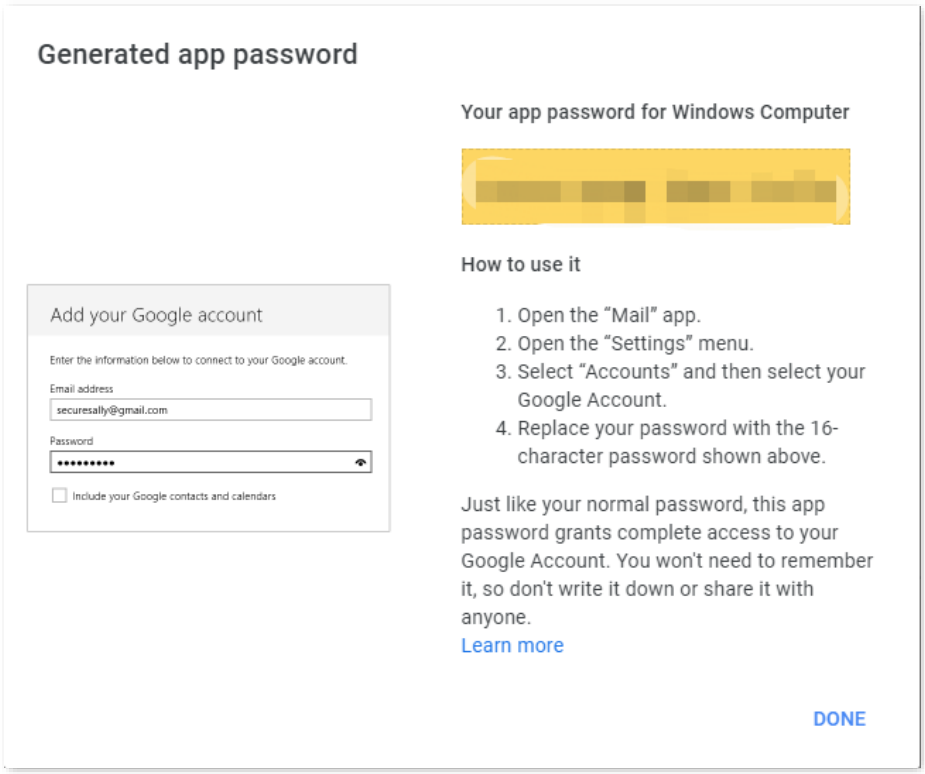
1. Launch a browser, and log in to your Gmail. Click **Settings** > **Forwarding and POP/IMAP**, and enable **POP and IMAP** (When IMAP is enabled, STMP is enabled automatically)**.**



2. Visit https://myaccount.google.com/, and click **Security** > **2-Step Verification**. After you turned on the verification, the **App passwords** appears below it.



3. Click **App passwords**, select **Mail** and **Windows Computer** as the App and device, click **GENERATE**, then the password for the email SMTP settings is generated. Assume that the password is **xmpq ticq vhbm ycpg**.



II. Set the authentication mode to email.

1. Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Guest Control**.

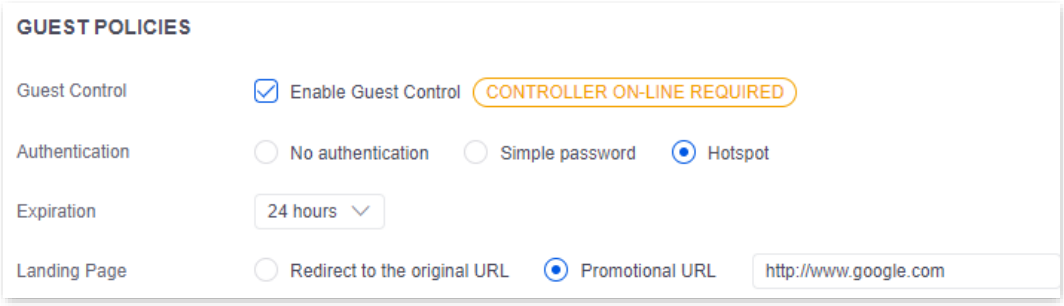
2. Set the authentication policy in the **GUEST POLICIES** module.

   (1) Select **Enable Guest Control**.

   (2) Set **Authentication** to **Hotspot**.

   (3) Set **Expiration** as required. **24 hours** is used as an example.

   (4) Set **Landing Page** as required. In this example, **Landing Page** is set to **Promotional URL (http://www.google.com).**



3. In the **Authentication** module, select **Email** and set the following parameters.

   The following information is used as an example.

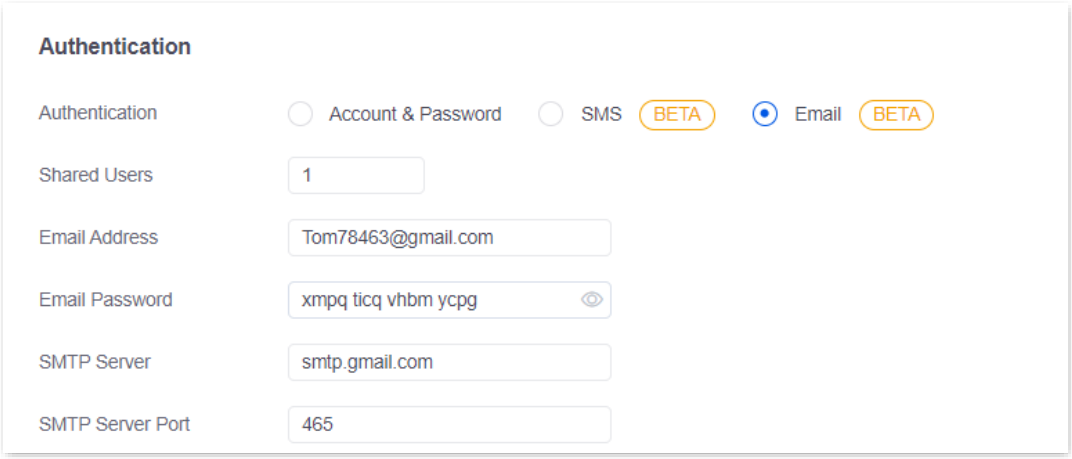
   (1) Set **Shared Users** to the number of users that are allowed to use the account for authentication at the same time. Here it is set to **1**.

   (2) Set **Email Address** to the email address used for sending emails. Here it is set to **Tom78463@gmail.com**.

   (3) Set **Email Password** to the App password above authorizing the SMTP settings. Here it is set to **xmpq ticq vhbm ycpg**.

   (4) Enter the SMTP server address in **SMTP Server**. Here it is set to **smtp.gmail.com**.

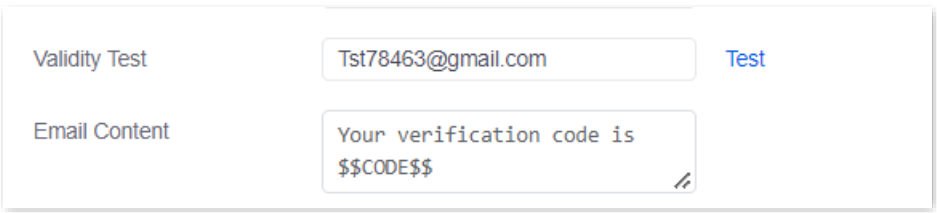
   (5) Set **SMTP Server Port**. Here it is set to **465**.



4. Check whether the email configuration is correct.

   (1) Enter the **Email Content** ($$CODE$$ is the format for email verification and cannot be modified).

   (2) Enter an email address in **Validity Test** for receiving emails, which is **Tst78463@gmail.com** in this example, and click **Test**.



If a message indicating that the verification passed is displayed on the page and the email is received, the configuration is correct.

Tip

If the test fails, try the following solution:

- Check that the SMTP service has been enabled for the email address.
- Check that the email address used for test is valid.
- Edit the email content.

5. Customize the guest portal as required in the **PORTAL CUSTOMIZATION**.

The following settings are used as an example.

(1) Set **Title** to **Standard**.

(2) Select **Enable welcome text**, enter welcome texts (**Welcome to IP-COM**) in the displayed dialog box and click **SAVE**.

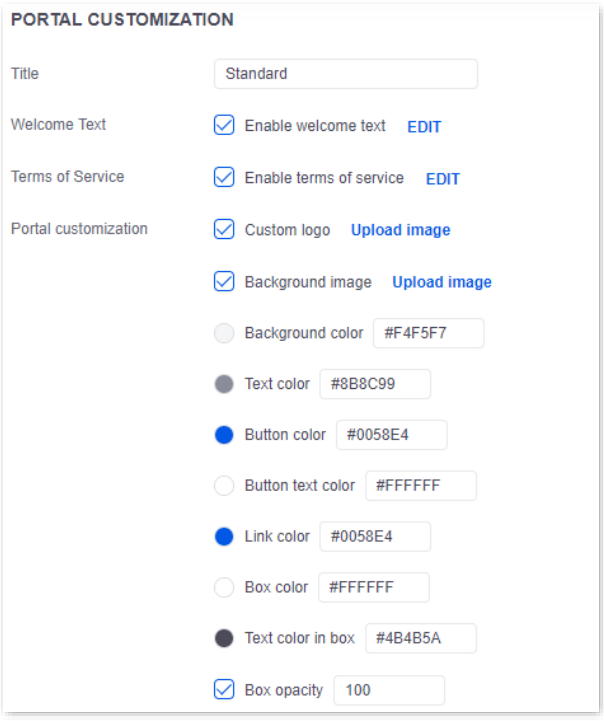
(3) Select **Enable terms of service** and edit the preset terms as required.

(4) Select **Custom logo** and click **Upload image** to upload the logo you want to display on the guest portal.

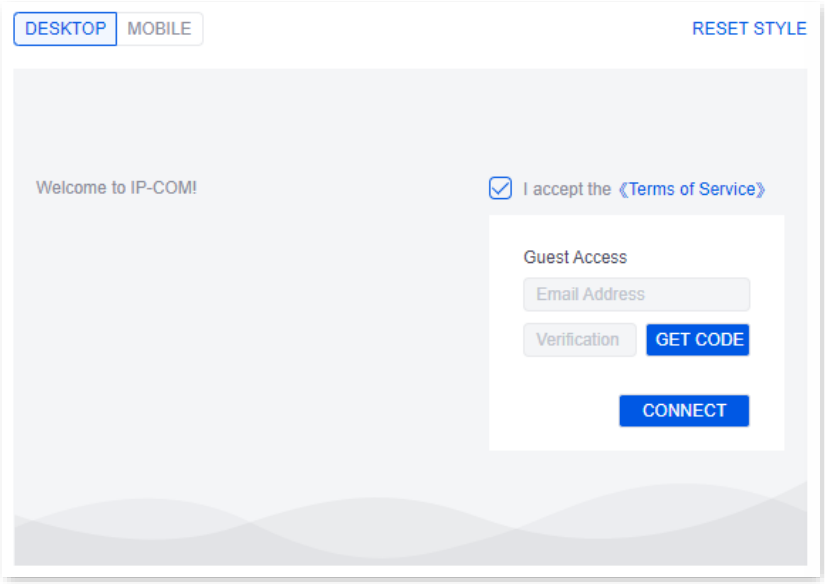
(5) Select **Background image** and click **Upload image** to upload the image that you want to use as the background of the guest portal.

(6) Click the circle icon before **Background color**/**Text color**/**Button color**/**Button text color**/**Link color**/**Box color**/**Text color in box** and choose the color, or directly enter a hexadecimal color code in the text box behind.

(7) Select **Box opacity** and enter the opacity value **100** in the text box behind.



You can preview the customized portal by clicking **DESKTOP** or **MOBILE**.



6. Click **APPLY CHANGES**.

III. Configure the AP.

Deliver wireless networks to the AP as follows:

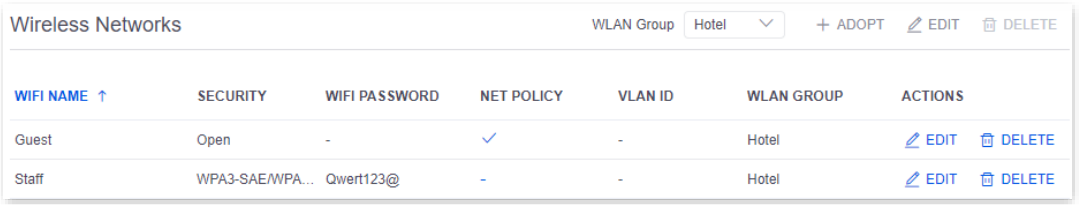
User	SSID	Security Mode	Password	Guest Network Policy	WLAN Group
Guest	Guest	/	/	Enabled	Hotel
Staff	Staff	WPA3-SAE/WPA2-PSK	Qwert123@	Disabled	Hotel

1. Configure the wireless networks.

(1) Log in to the ProFi Software Controller, select your project and choose **SETTINGS** ( ) > **Wireless Networks**.

(2) Click + ADOPT to add a WLAN group named **Hotel**.

(3) Click **+ CREATE NEW WIRELESS NETWORK** to add the following two wireless policies.



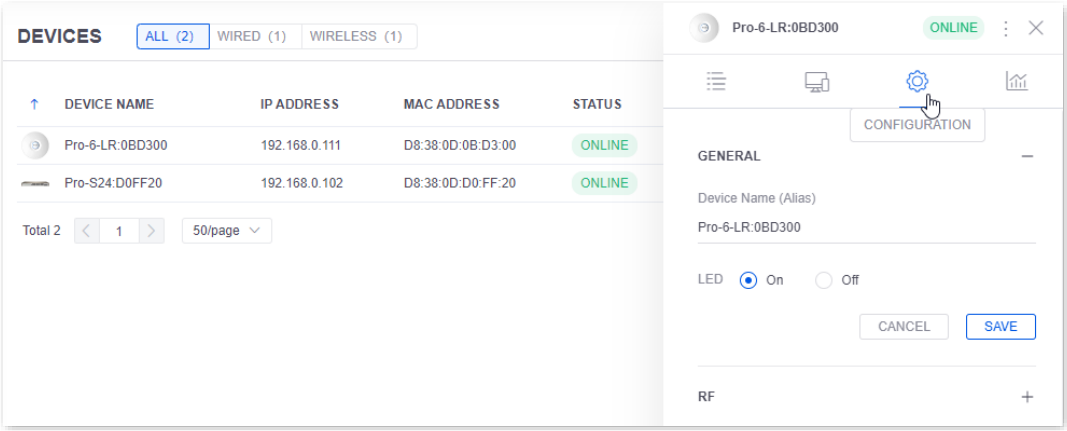
Tip

Generally, a maximum of 128 2.4G/5G clients can be connected to an IP-COM AP. Therefore, check that the total number of **2.4G Maximum Clients** and **5G Maximum Clients** under all SSIDs in the **Hotel** WLAN group is not greater than 128.

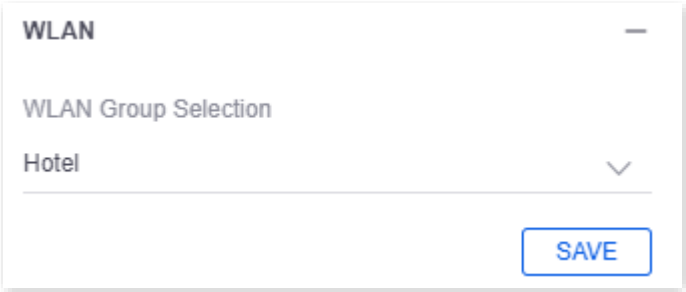
2. Deliver the wireless networks to the AP.

(1) Log in to the ProFi Software Controller, select your project and choose **DEVICES** ( ).

(2) Select your switch and click **CONFIGURATION** ( ) in the panel displayed on the right to access the settings page.



(3) Click **WLAN**, select **Hotel** from the drop-down list and click **SAVE**.



----End

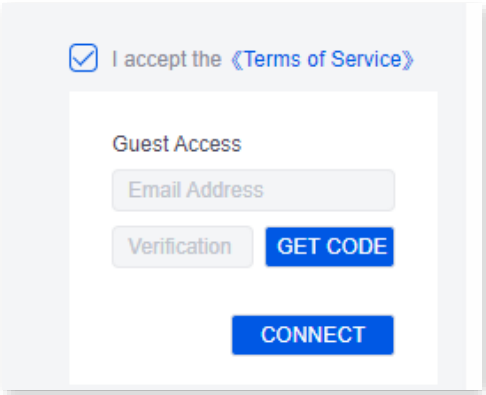
Verification

Authentication is not required when users are connected to the **Staff** wireless network.

Authentication is required when users are connected to the **Guest** wireless network. The verification procedure is as follows:

1. When a wireless client such as mobile phone is connected to the **Guest** wireless network, it will be redirected to the authentication page automatically. If not, open a browser and visit any website to access the page.

2. Select **I accept the <<Terms of Service>>**, enter your email address and click **GET CODE**.
3. Enter the received verification code and click **CONNECT**.



After the authentication completes successfully, the page will be redirected to **www.google.com**.

Appendix

Acronyms & Abbreviations

Acronyms & Abbreviations	Full Name
AC	Access Category
AC	Access Point Controller
ASCII	American Standard Code for Information Interchange
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CPU	Central Processing Unit
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DTIM	Delivery Traffic Indication Map
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
ESSID	Extended Service Set Identifier
FIFO	First-in First-out
FQDN	Fully Qualified Domain Name
GB	Gigabyte
GTK	Group Temporal Key
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
MAC	Media Access Control

Acronyms & Abbreviations	Full Name
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NMS	Network Management System
OS	Operating System
PoE	Power over Ethernet
PSK	Pre-shared Key
PVID	Port-based VLAN ID
RAM	Random Access Memory
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTS	Request to Send
SAE	Simultaneous Authentication of Equals
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
STP	Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
UI	User Interface
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMF	Wireless Multicast Forwarding
WMM	WiFi Multimedia
WPA	Wi-Fi Protected Access