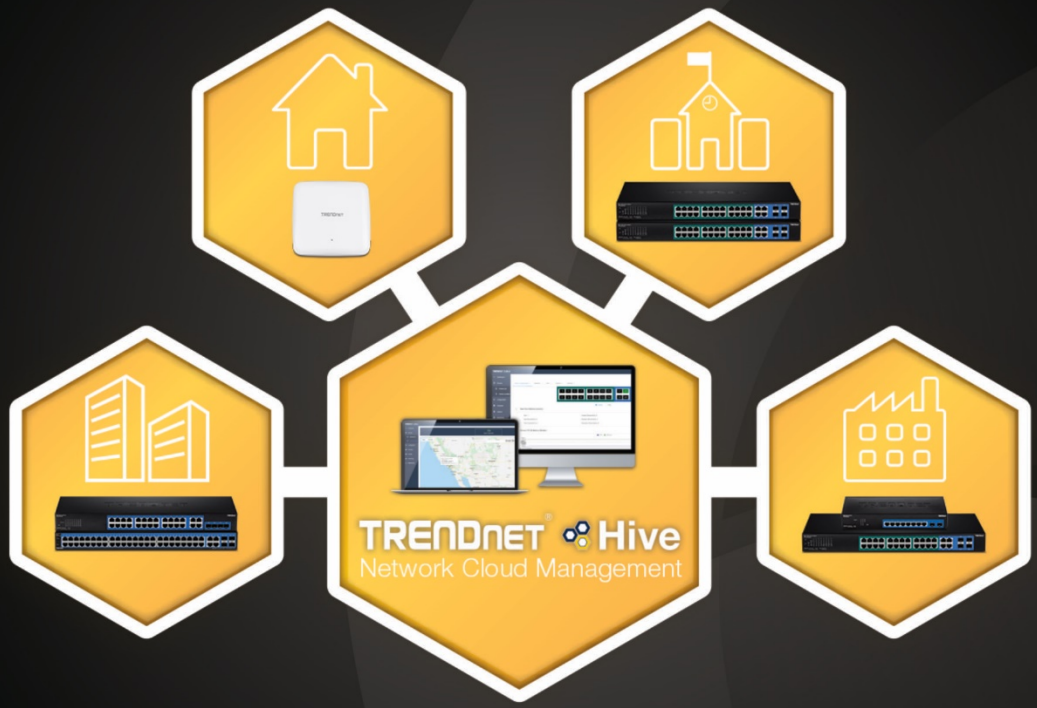
User's Guide

TRENDnet®



TRENDnet® Hive

Contents

TRENDnet Hive Overview

What is TRENDnet Hive?

TRENDnet Hive is a cloud management platform that provides a centralized cloud-based management solution for TRENDnet network devices. TRENDnet network devices can be connected to the Hive cloud management platform. The TRENDnet Hive cloud networking solution offers better overall visibility of your network devices from a single intuitive and easy-to-use cloud interface.

Advanced features supported with cloud networking include event and device hardware monitoring, traffic statistics, notification alerts, and troubleshooting tools. Network device provisioning can be accomplished through scheduled or immediate deployment of batch firmware and configuration updates. Reduce the time, complexity, and management costs of your network with TRENDnet Hive.

Features

Cloud-Based Management

TRENDnet Hive network cloud manager provides better overall visibility of your network devices from a single intuitive and easy-to-use cloud interface

Hassle-Free Remote Monitoring

Remote network management support allows you to monitor your network devices from the cloud with device uptime, detailed logging, traffic statistics, event snapshots, and device health (processor/memory hardware and PoE budget utilization)

Intuitive Alerts and Notifications

Choose customized alerts and notifications to be sent based on exceeded thresholds (CPU/memory) or events (port link status, device offline, switch loop)

Ease of Provisioning

Schedule batch firmware upgrades and configuration updates for deployment from the cloud for your network devices. Create and customize configuration files in the cloud and review records of when firmware and configuration update tasks were carried out

Reduce time and management costs

Reduce maintenance time and costs by moving network device access to the cloud

Minimal Downtime

Service-Level Agreement (SLA) guaranteed 99.9 percent uptime and service availability

Hive Account Features

Features	Hive Premium (for end users)	Hive Pro (for integrators/partners)
Multiple Device Management	Yes	Yes
Multiple Site Management	Yes	Yes
Supports all selected TRENDnet devices	Yes	Yes
Supports unlimited number of devices	Yes	Yes
Device Configuration & Monitoring	Yes	Yes
Batch Firmware and Configuration Deployment	Yes	Yes
Mobile App (iOS® and Android™)	Yes	Yes
Notification Alerts	Yes	Yes
Multiple Tenant Management	No	Yes
Multiple User Accounts	No	Yes
Role-based User Privileges	No	Yes
Google Maps™ mapping service	No	Yes

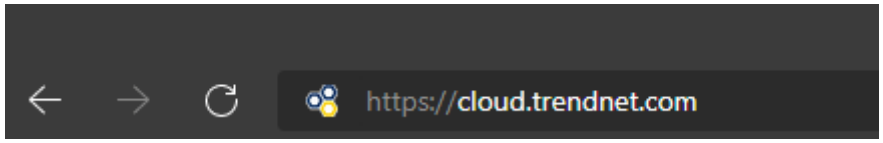
Disclaimer: Features and specifications are subject to change without notice. Please note that Hive Premium accounts cannot be upgraded to Hive Pro accounts. It is strongly recommended to review the Hive subscription options in advance to determine the appropriate option for your application.

Sign up for a Hive Account

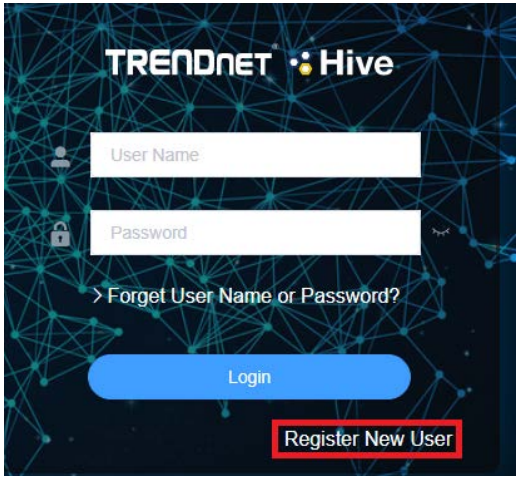
Note: *Sign up for a Hive Premium account at https://cloud.trendnet.com. For Hive Pro accounts, contact your authorized TRENDnet reseller, distributor, or TRENDnet sales. Please note that Hive Premium accounts cannot be upgraded to Hive Pro accounts. It is strongly recommended to review the Hive subscription options in advance to determine the appropriate option for your application.*

Hive Premium Account Sign Up

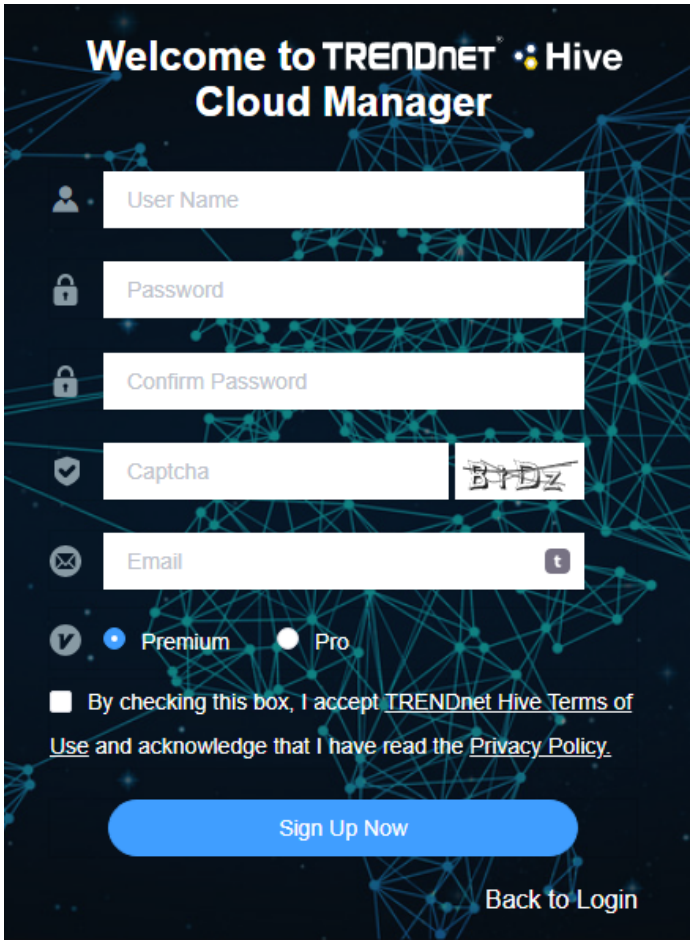
1. In your web browser, go to https://cloud.trendnet.com



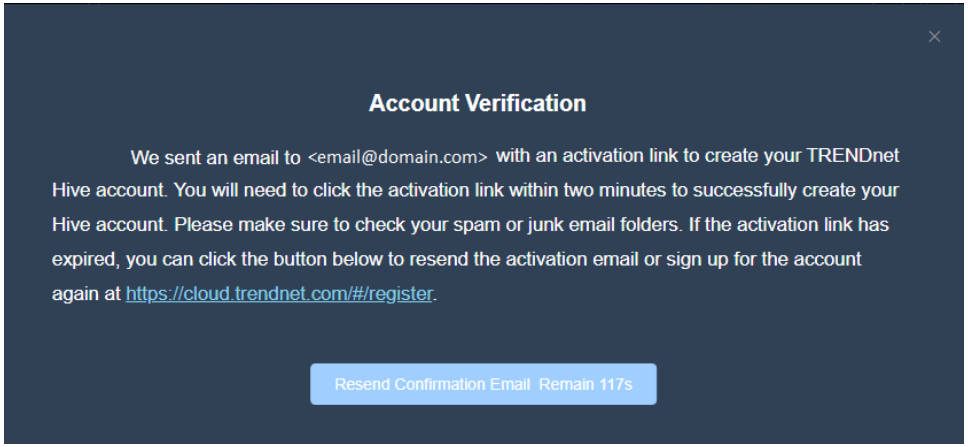
2. Click on **Register New User**.



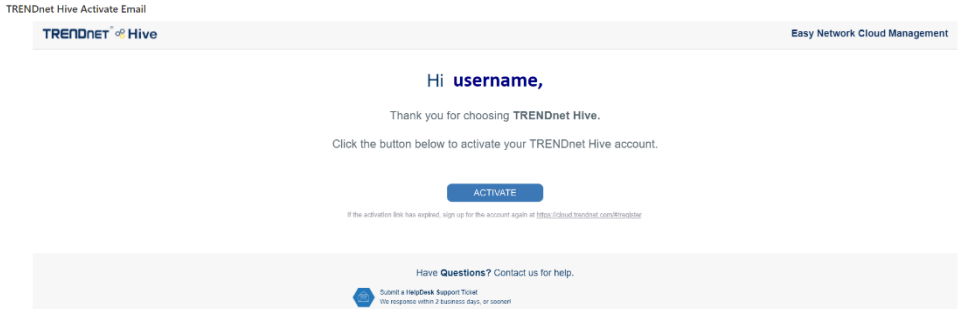
3. In the user account information in the fields provided. After you have completed entering the account information, make sure **Premium** is selected and check the box to confirm the terms of use and privacy policy. You can review the terms and privacy policy by clicking the links provided.
Click **Sign Up Now.**



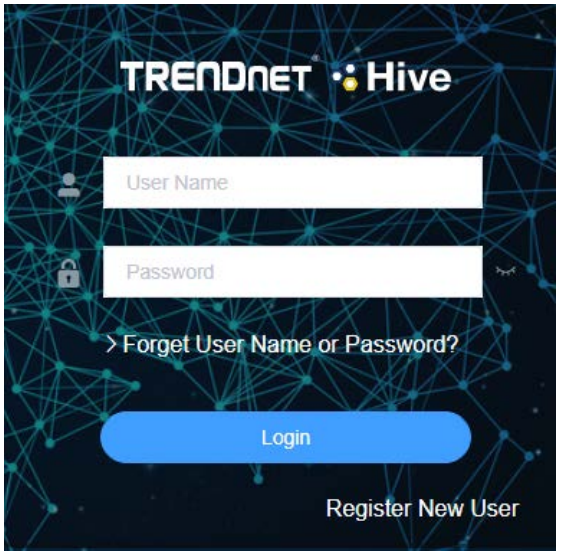
4. You will receive an account verification prompt notifying you of the verification email sent to the email address you entered with the activation link to confirm your Hive account.
   Note: *Please note that the activation link will expire in two minutes. If the activation link expires and this prompt is still open, you can click the button to resend the verification email.*



5. In the activation email, click the **Activate** button to confirm your account.



6. After you have confirmed your account, enter your Hive account credentials and click **Login.**



Adding devices to Hive

Hive compatible devices

The device models listed below are currently compatible with TRENDnet Hive. You may need to upgrade the device firmware to enable TRENDnet Hive. You can find the latest list of Hive compatible devices on the TRENDnet Hive website.
https://www.trendnet.com/hive/#devices

Web Smart Switches		
Model	**Hardware Version (H/W)**	**Hive Firmware Version**
TEG-082WS	**v2.xR**	**3.01.xxx or above**
TEG-204WS	**v1.xR**	
TEG-284WS	**v1.xR**	
TEG-524WS	**v1.xR**	
TEG-30284	**v2.xR**	

PoE Web Smart Switches		
Model	**Hardware Version (H/W)**	
TPE-082WS	**v1.xR**	**3.01.xxx or above**
TPE-1021WS	**v1.xR**	
TPE-1620WS	**v2.xR**	
TPE-1620WSF	**v1.xR**	
TPE-204US	**v1.xR**	
TPE-2840WS	**v2.xR**	
TPE-30284	**v1.xR**	
TPE-5028WS	**v1.xR**	
TPE-5048WS	**v1.xR**	
TPE-5240WS	**v1.xR**	

PoE Wireless Access Points		
Model	**Hardware Version (H/W)**	**Hive Firmware Version**
TEW-821DAP	**v2.xR**	**3.00 or above**
TEW-825DAP	**v1.xR**	**2.00 or above**
TEW-826DAP	**v1.xR**	**2.00 or above**
TEW-921DAP	**v1.xR**	**2.10 or above**

Important Note: *Please make sure you have updated TRENDnet Hive compatible devices to the latest firmware to enable TRENDnet Hive capability and feature compatibility.*

*** Devices registered under a Hive Premium or Hive Pro account cannot interchange with another.*

Disclaimer: Supported models are subject to change without notice.

Using the device setup wizard

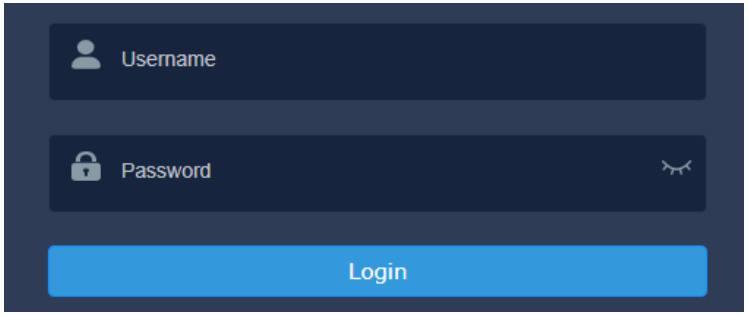
Before connecting TRENDnet devices to the Hive management system, the devices must be configured with the proper IP address, subnet mask, default gateway address, DNS server settings, and connected to a network for Internet access before devices can connect to the Hive management system and registered with your Hive account. Devices must always remain connected to the Internet to ensure they can be managed and monitored from your Hive account. The device setup wizard provides a simplied way to configure your device for Internet access and register/connect your device to your Hive cloud account for management.

Web Smart Switches

Note: *The following example will provide the steps for configuring the TRENDnet web smart switch IP address, subnet mask, default gateway address, and DNS settings.*

1. Login to the web smart switch management page.

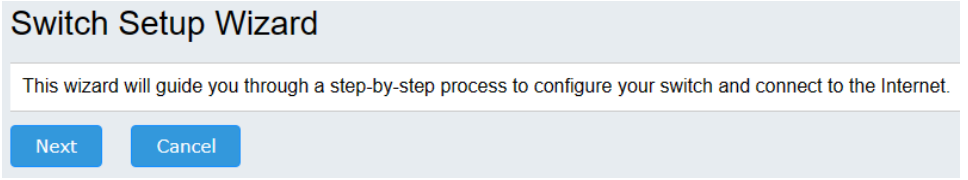
Note: *The TRENDnet web smart switch default IP address and subnet mask is 192.168.10.200 / 255.255.255.0. The TRENDnet web smart switch default user name and password is admin / admin.*



2 Click the Setup Wizard icon at the top right. 

Note: *If this is the first time configuring the switch or the switch has been reset to factory default, the setup wizard will be displayed automatically.*

3. Click **Next** to start the setup wizard.

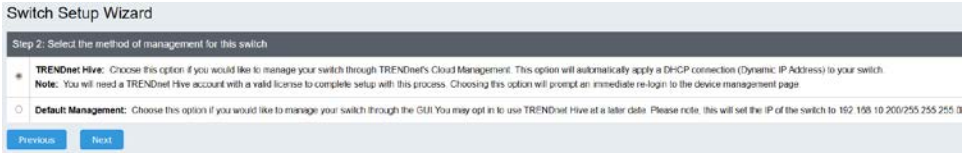


4. Change your administrator password using the fields provided and click **Next**.

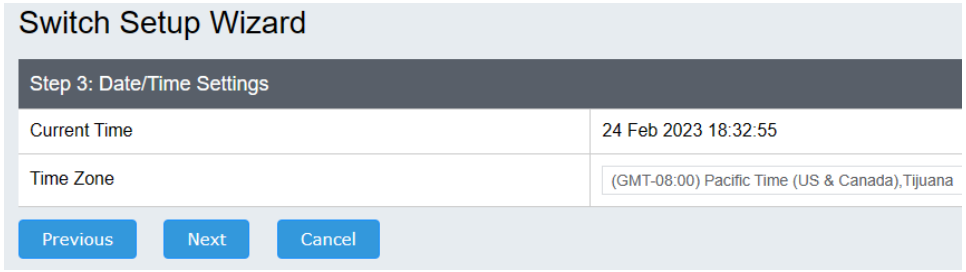
Note: *It is strongly recommended to change the default administrator password.*

5. At the prompt, select **TRENDnet Hive** to configure the switch IP address and DNS settings for Internet access by automatically obtaining these settings through a DHCP server on your network. This is the recommended option for connecting the switch to TRENDnet Hive.

Note: *You can choose the Default Management option to configure your IP address and DNS settings manually and afterwards connect to Hive manually in the switch management page.*

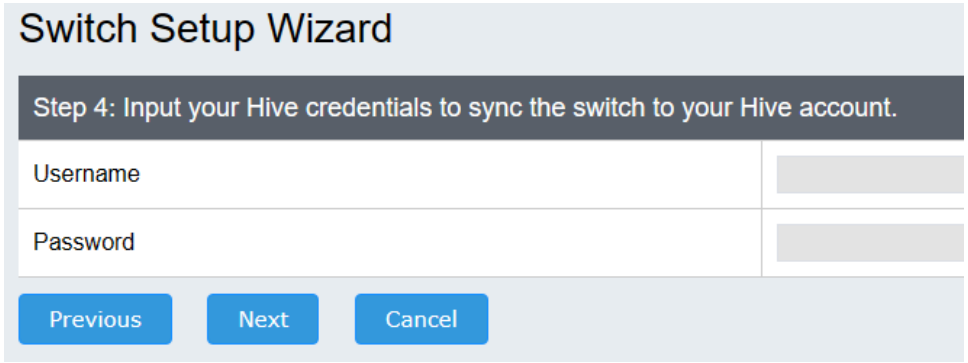


6. Select your **Time Zone** from the drop-down list and click **Next**.

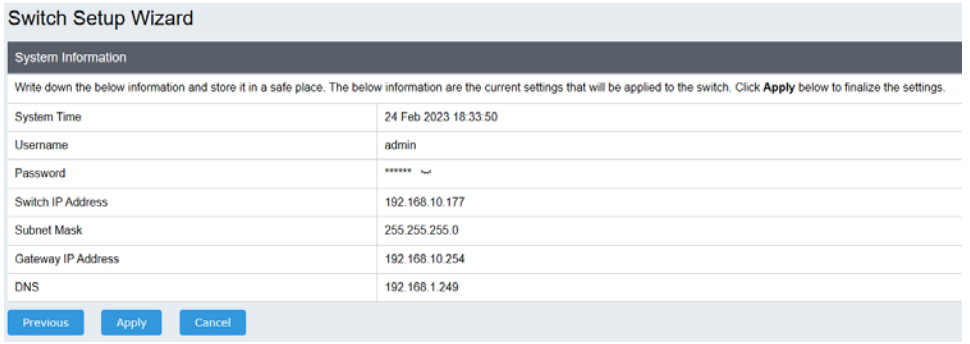


7. Enter your Hive account credentials to register and connect the switch to your Hive account and click **Next**.

Note: *The switch IP address and DNS settings will be modified by settings by your network DHCP server and you will automatically be redirected to the switch management page setup wizard. If this step does not appear, the switch may not have successfully obtained IP address settings by your network DHCP server.*



8. A summary of the all the configuration settings will be displayed. Please take note important settings such as the password and IP address for reference and click **Apply** to complete the setup wizard.



9. The TRENDnet Hive button  at the top right of the management page will be displayed as green to indicate the device has successfully connected to your Hive cloud account.

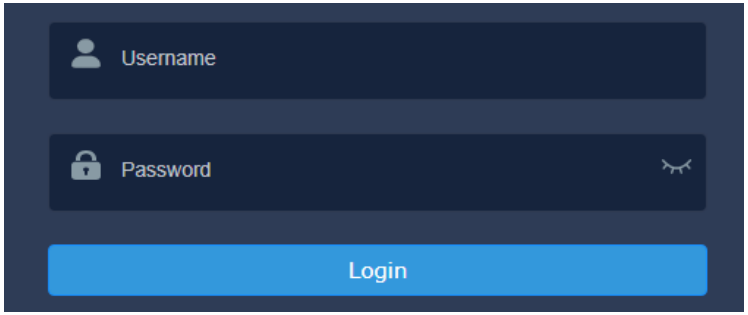
Note: *A yellow Hive button indicates that Hive has been disabled on the device. A red Hive button indicates that there was error/issue connecting the device to the Hive account.*

Manually configure the switch IP address and DNS settings

To manually configure the switch IP address/DNS settings and connect to Hive, follow the steps below.

1. Login to the web smart switch management page.

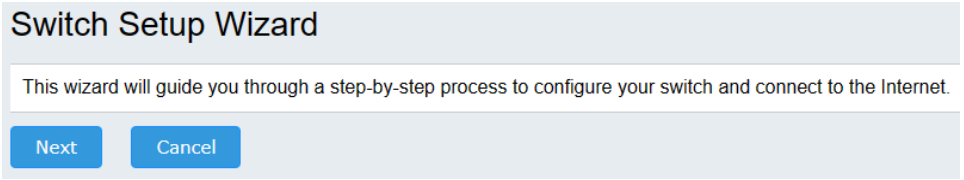
Note: *The TRENDnet web smart switch default IP address and subnet mask is 192.168.10.200 / 255.255.255.0. The TRENDnet web smart switch default user name and password is admin / admin.*



2 Click the Setup Wizard icon at the top right. 

Note: *If this is the first time configuring the switch or the switch has been reset to factory default, the setup wizard will be displayed automatically.*

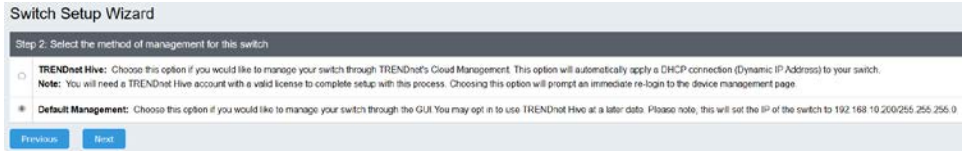
3. Click **Next** to start the setup wizard.



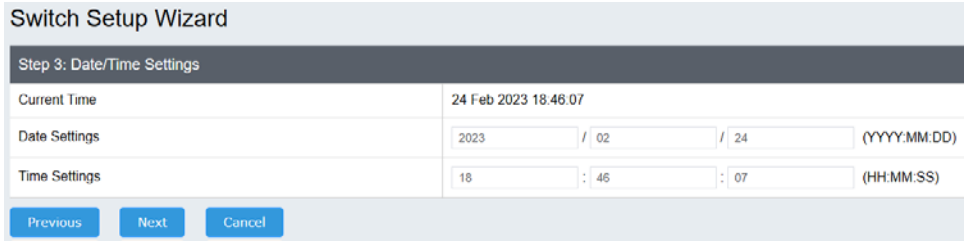
4. Change your administrator password using the fields provided and click **Next**.

Note: *It is strongly recommended to change the default administrator password.*

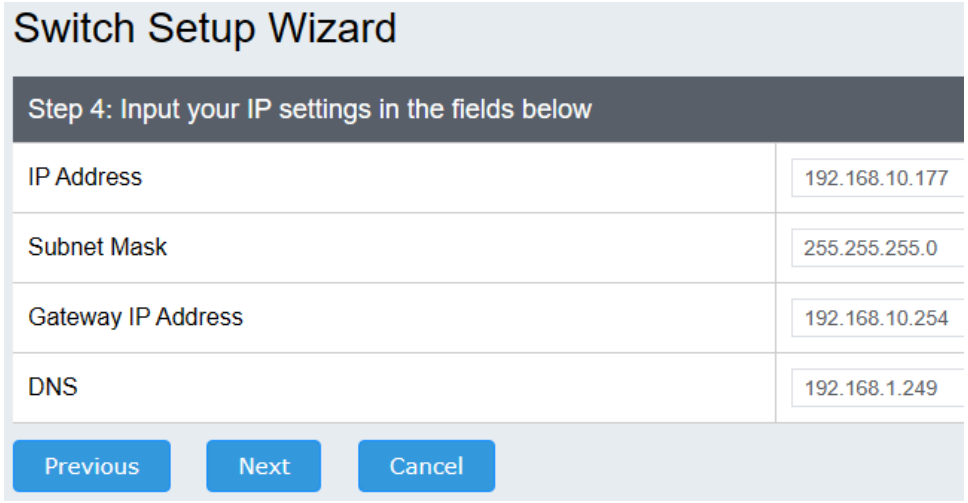
5. At the prompt, select **Default Management** to configure the switch IP address and DNS settings for Internet access manually for Internet access.



6. Manually enter the **Date** and **Time** settings in the fields provided and click **Next**.

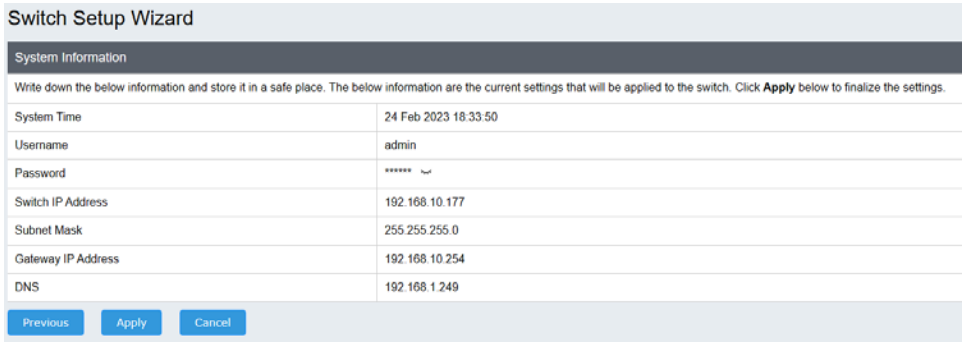


7. Manually enter the **IP Address**, **Subnet Mask**, **Gateway IP Address**, and **DNS** server IP address settings in the fields provided and click **Next**.

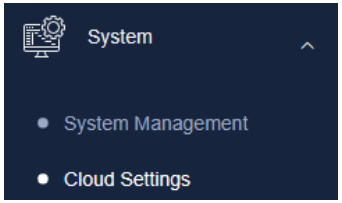


8. A summary of the all the configuration settings will be displayed. Please take note important settings such as the password and IP address for reference and click **Apply** to complete the setup wizard.

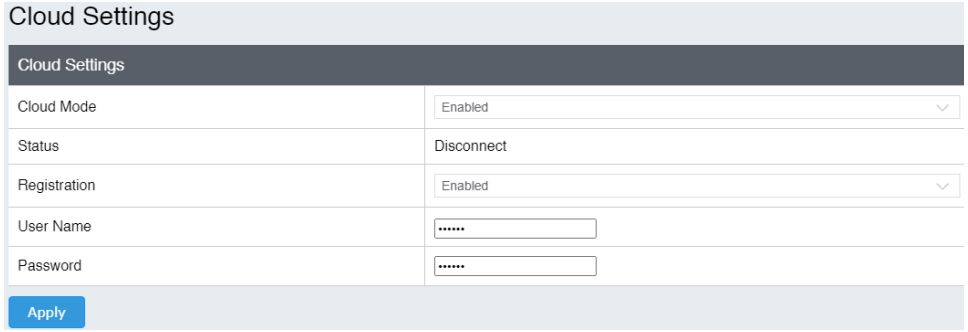
Note: *You may need to login to the switch management page again using the new IP address settings.*



9. In the left navigation menu, click on **System** and **Cloud Settings**.



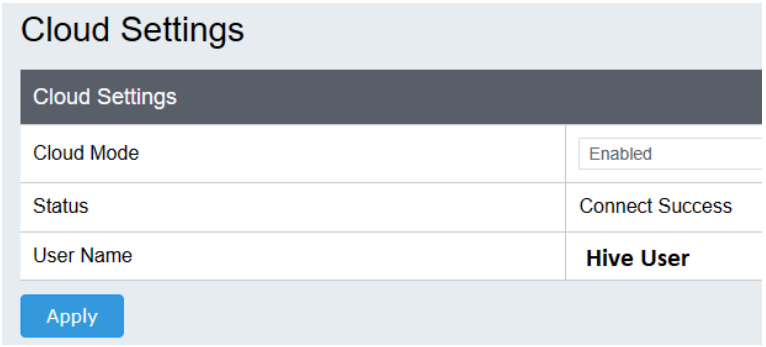
10. Click the **Cloud Mode** drop-down and select **Enabled**. Click the **Registration** drop-down and select **Enabled**, enter your Hive account credentials in the **User Name** and **Password** fields and click **Apply**.



11. The status will display a message indicating that the device has successfully connected to your Hive cloud account with the Hive account user name listed.

Additionally, the TRENDnet Hive button  at the top right of the management page will be displayed as green to indicate the device has successfully connected to your Hive cloud account.

Note: *A yellow Hive button indicates that Hive has been disabled on the device. A red Hive button indicates that there was error/issue connecting the device to the Hive account.*



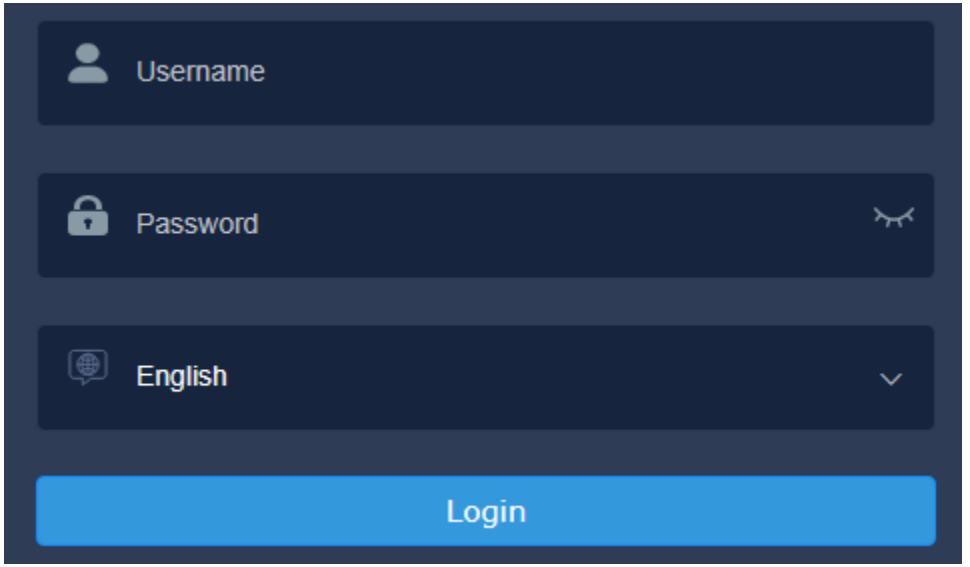
12. Click the save button  at the top right of the device management page to ensure the configuration settings are saved.

Wireless Access Points

Note: *The following example will provide the steps for configuring the TRENDnet wireless access point IP address, subnet mask, default gateway address, and DNS settings.*

1. Select your language from the drop-down list and login to the access point management page.

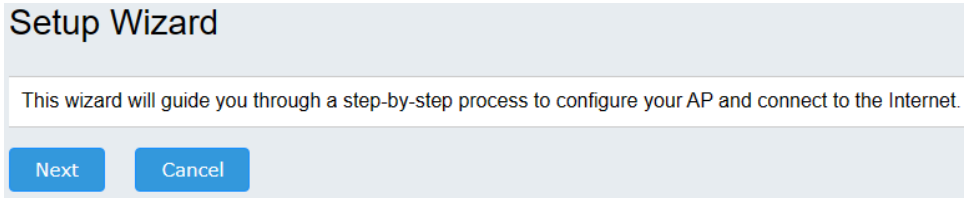
Note: *By default, the access point is configured to obtain IP address and DNS settings automatically from an existing DHCP server on your network. The access point can be access using the URL http://<ap_model_number> (ex: http://tew-921dap). If there is no DHCP server available or if the access point cannot obtain settings through DHCP, the access point will use the default IP address and subnet mask 192.168.10.100 / 255.255.255.0. The TRENDnet access point default user name and password is admin / admin.*



2 Click the Setup Wizard icon at the top right. 

Note: *If this is the first time configuring the access point or the access point has been reset to factory default, the setup wizard will be displayed automatically.*

3. Click **Next** to start the setup wizard.



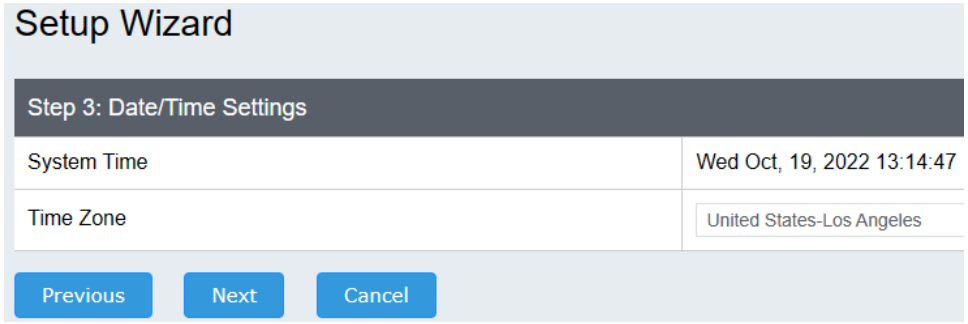
4. Change your administrator password using the fields provided and click **Next**.

Note: *It is strongly recommended to change the default administrator password.*

5. At the prompt, select **TRENDnet Hive** to configure the access point IP address and DNS settings for Internet access by automatically obtaining these settings through a DHCP server on your network. This is the recommended option for connecting the access point to TRENDnet Hive.

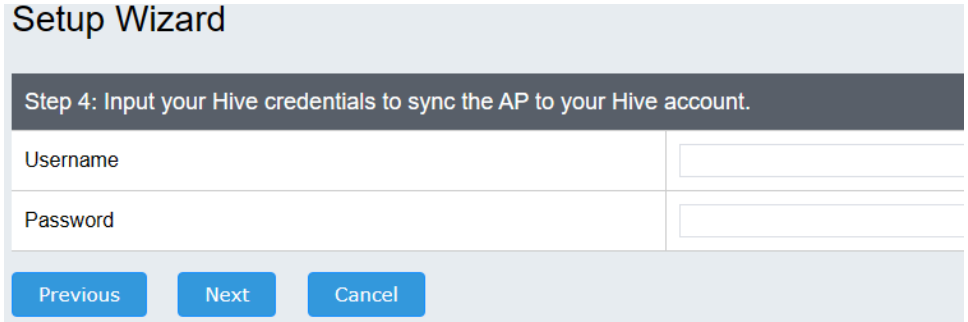
Note: *You can choose the Default Management option to configure your IP address and DNS settings manually and afterwards connect to Hive manually in the access point management page.*

6. Select your **Time Zone** from the drop-down list and click **Next**.

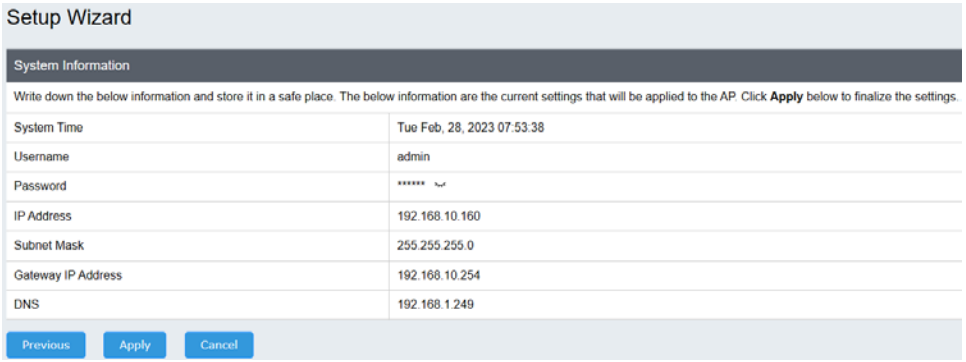


7. Enter your Hive account credentials to register and connect the access point to your Hive account and click **Next**.

Note: *The access point IP address and DNS settings will be modified by settings by your network DHCP server and you will automatically be redirected to the access point management page setup wizard. If this step does not appear, the access point may not have successfully obtained IP address settings by your network DHCP server.*



8. A summary of the all the configuration settings will be displayed. Please take note important settings such as the password and IP address for reference and click **Apply** to complete the setup wizard.



9. The TRENDnet Hive button  at the top right of the management page will be displayed as green to indicate the device has successfully connected to your Hive cloud account.

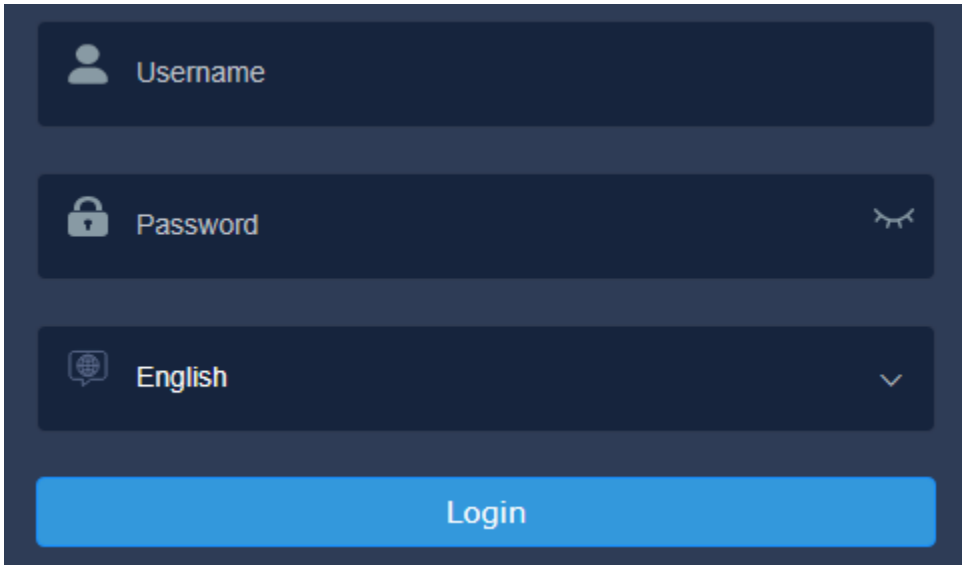
Note: *A yellow Hive button indicates that Hive has been disabled on the device. A red Hive button indicates that there was error/issue connecting the device to the Hive account.*

Manually configure the access point IP address and DNS settings

To manually configure the access point IP address/DNS settings and connect to Hive, follow the steps below.

1. Select your language from the drop-down list and login to the access point management page.

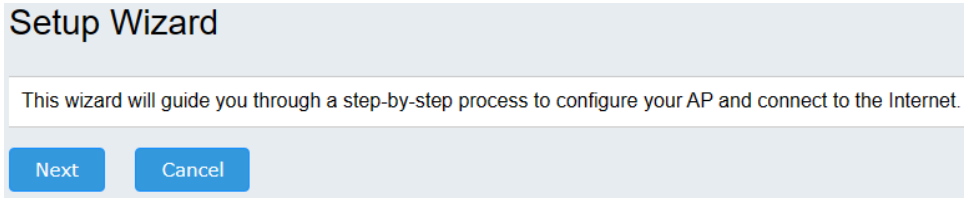
Note: *By default, the access point is configured to obtain IP address and DNS settings automatically from an existing DHCP server on your network. The access point can be access using the URL http://<ap_model_number> (ex: http://tew-921dap). If there is no DHCP server available or if the access point cannot obtain settings through DHCP, the access point will use the default IP address and subnet mask 192.168.10.100 / 255.255.255.0. The TRENDnet access point default user name and password is admin / admin.*



2 Click the Setup Wizard icon at the top right. 

Note: *If this is the first time configuring the access point or the access point has been reset to factory default, the setup wizard will be displayed automatically.*

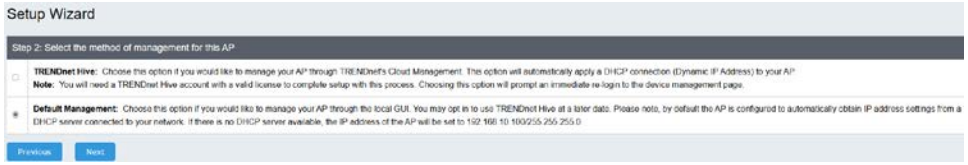
3. Click **Next** to start the setup wizard.



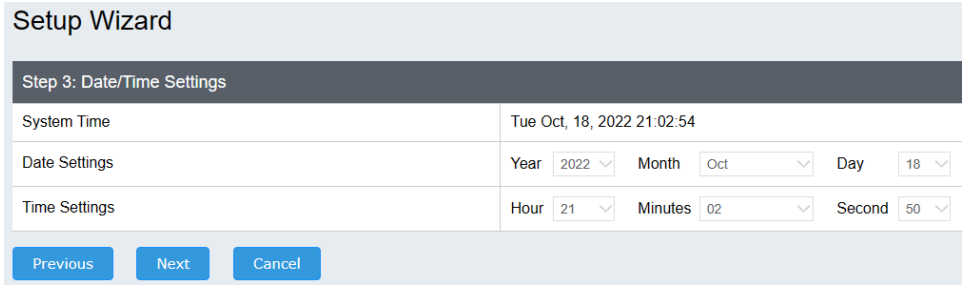
4. Change your administrator password using the fields provided and click **Next**.

Note: *It is strongly recommended to change the default administrator password.*

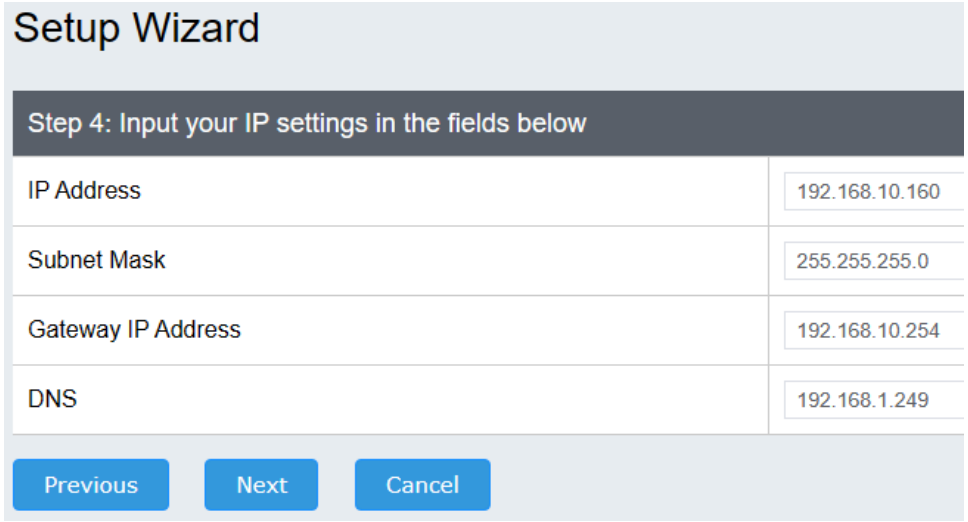
5. At the prompt, select **Default Management** to configure the switch IP address and DNS settings for Internet access manually for Internet access.



6. Manually enter the **Date** and **Time** settings in the fields provided and click **Next**.

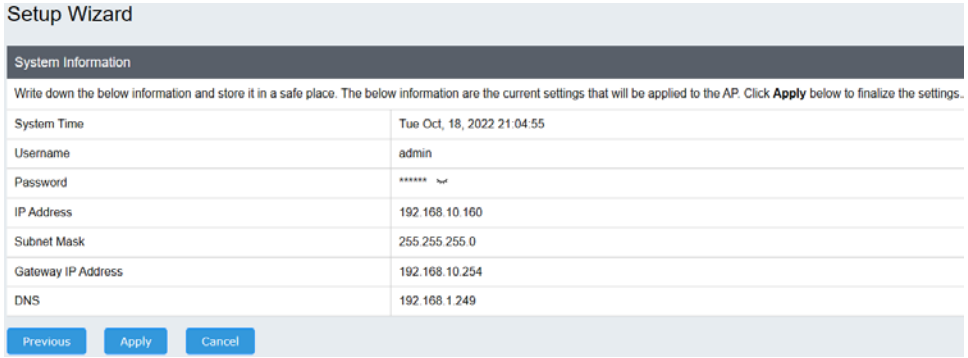


7. Manually enter the **IP Address**, **Subnet Mask**, **Gateway IP Address**, and **DNS** server IP address settings in the fields provided and click **Next**.

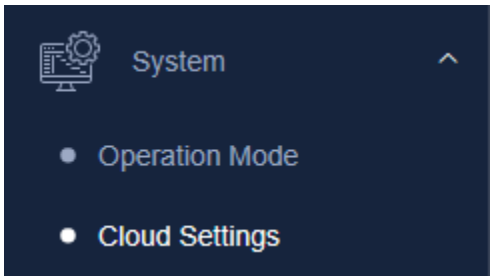


8. A summary of the all the configuration settings will be displayed. Please take note important settings such as the password and IP address for reference and click **Apply** to complete the setup wizard.

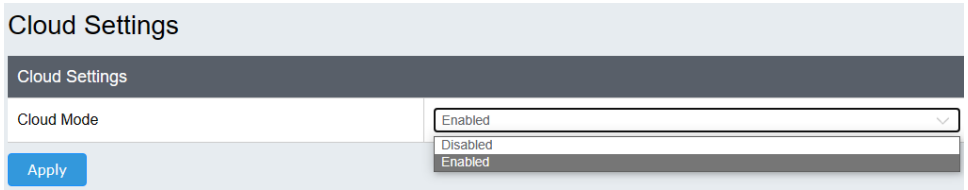
Note: *You may need to login to the acess point management page again using the new IP address settings.*



9. In the left navigation menu, click on **System** and **Cloud Settings**.

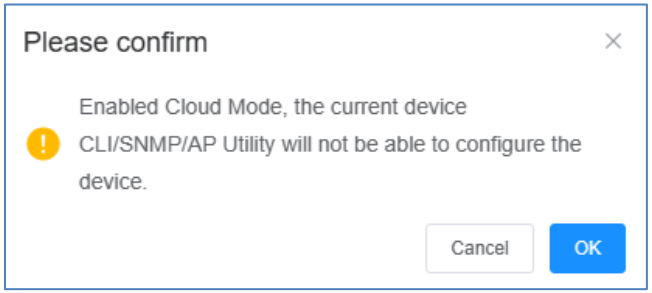


10. Click the **Cloud Mode** drop-down, select **Enabled** and click **Apply**. enter your Hive account credentials in the **User Name** and **Password** fields and click **Apply**.

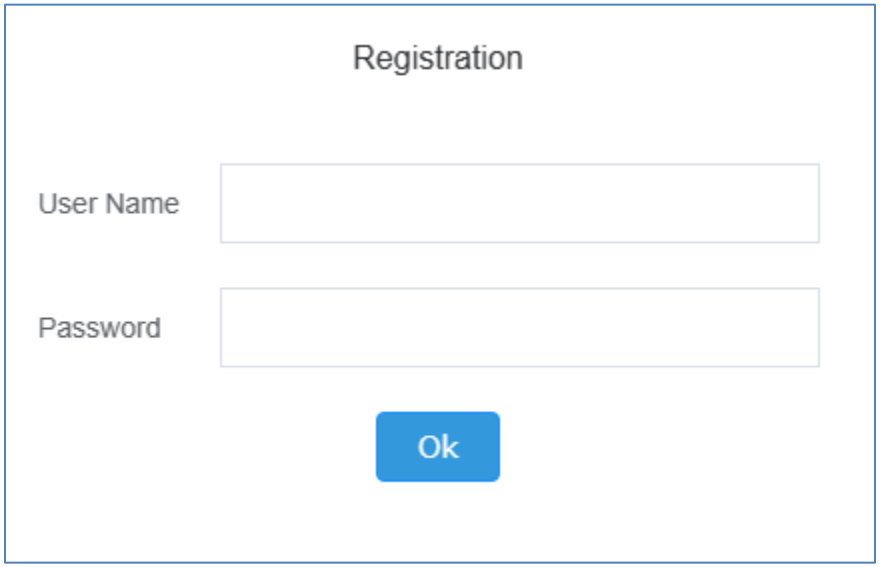


11. Click **OK** at the prompt.

Important Note: Connecting the wireless access point to your Hive account will disable functionality usage with the TRENDnet TEW-WLC100 / TEW-WLC100P wireless controllers and Access Point (AP) software utility.



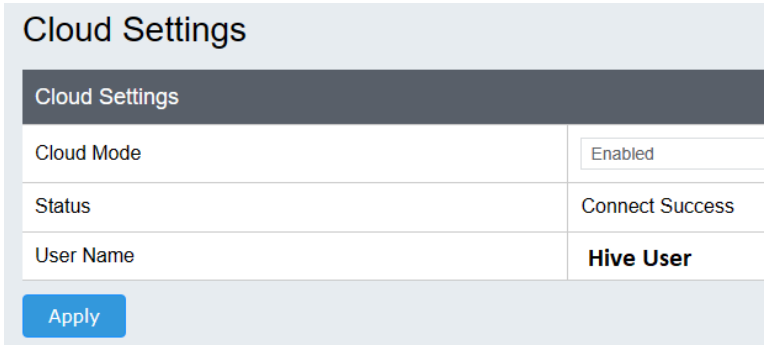
12. At the prompted, enter your Hive account credentials in the **User Name** and **Password** fields and click **OK**.



11. The status will display a message indicating that the device has successfully connected to your Hive cloud account with the Hive account user name listed.

Additionally, the TRENDnet Hive button  at the top right of the device management page will be displayed as green to indicate the device has successfully connected to your Hive cloud account.

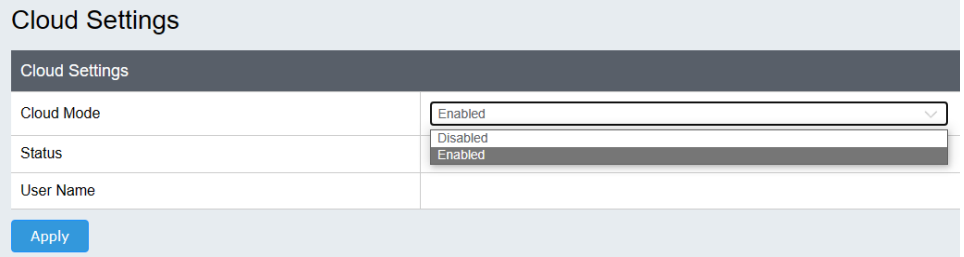
Note: *A yellow Hive button indicates that Hive has been disabled on the device. A red Hive button indicates that there was error/issue connecting the device to the Hive account.*



12. Click the save button  at the top right of the device management page to ensure the configuration settings are saved.

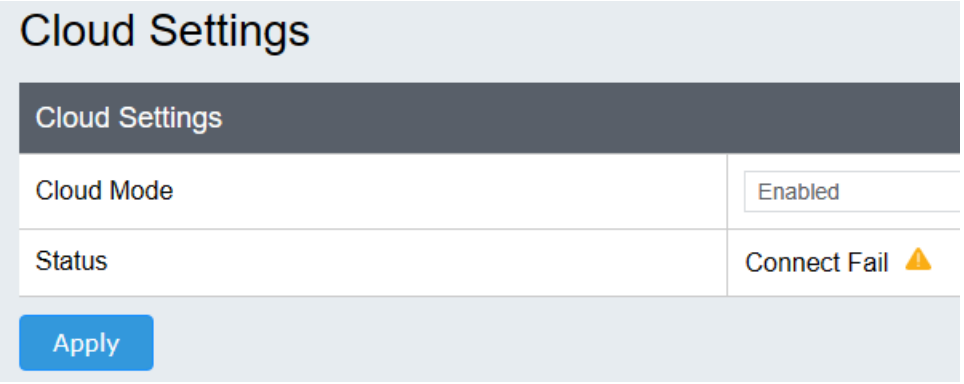
Enable or disable Hive management on your device

After your TRENDnet device has been properly configured and and connected for Internet access (through the setup wizard or manually), you enable or disable Hive device management with your Hive account by logging into your device management page and under **System** and **Cloud Settings**, select Enabled or Disabled and click **Apply**.



Troubleshooting the device connection to Hive

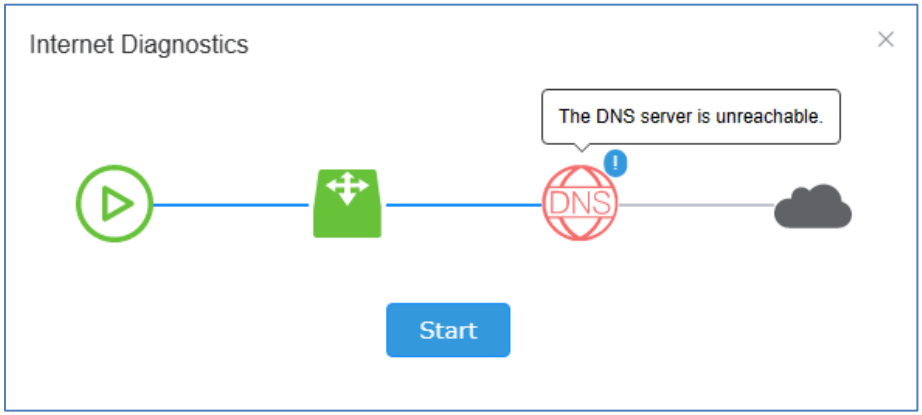
Note: If you encounter any issues registering or connecting your device to your Hive account, mouse over the ⚠ icon and the error message will be displayed indicating the cause of the connection issue.



You can also click the ⚠ button to run a connection diagnostic to further troubleshoot the connection issue.

Click **Start** to run the diagnostic test.

- The first test check both the physical and IP connectivity of the device to your network.
  Note: *If this test fails, please check all physical connections between your device to your network and also reconfirm your device IP address settings. To prevent conflicting configuration settings between Hive and local device management, some device configuration settings may be hidden such IP and DNS. You may need to disable Cloud Mode first under System > Cloud Settings to access and reconfigure these settings locally, then re-enable Cloud Mode afterwards.*
- The second test will check if the device can successfully resolve DNS (domain name resolution).
  Note: *If this test fails, please reconfirm your DNS server IP address settings and also the DNS server(s) used are working directly from your computer. To prevent conflicting configuration settings between Hive and local device management, some device configuration settings may be hidden such IP and DNS. You may need to disable Cloud Mode first under System > Cloud Settings to access and reconfigure these settings locally, then re-enable Cloud Mode afterwards.*
- The third and final test will check if the device can reach the Hive cloud management system.
  Note: *If this test fails, please contact TRENDnet technical support if there is connection issue to the Hive management system.*



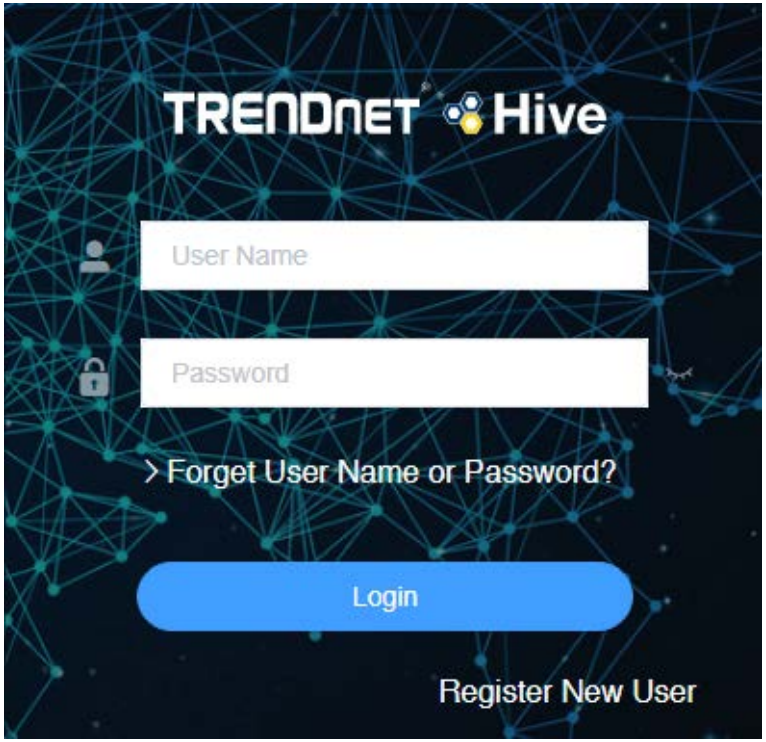
Hive Management Portal

This section will explain how to navigate, functionality and usage of the Hive management portal .

Login to your Hive account

Using a web browser, login to your Hive account at https://cloud.trendnet.com. Enter your user name and password account credentials and click **Login.**

Note: *If you forgot your Hive User Name or Password, you can click the link Forget User Name or Password?, enter the email address you used to create your Hive account and click Get Code to verify email address. Enter the code received via email and follow the instructions to reset your Hive User Name or Password.*



Hive Dashboard

The Hive dashboard displays the total number of tenants (multiple tenants available in Hive Pro only), devices (online/total) and the number of alarm notifications. The dashboard provides an overview of all tenants and snapshot information of the wireless access point information.

You can also create new tenants, remove tenants, check tenant location, check the alarm notifications and online/total number of devices for each tenant from this page.

Note: *Devices must be assigned to tenant in order the devices to be managed from Hive.*

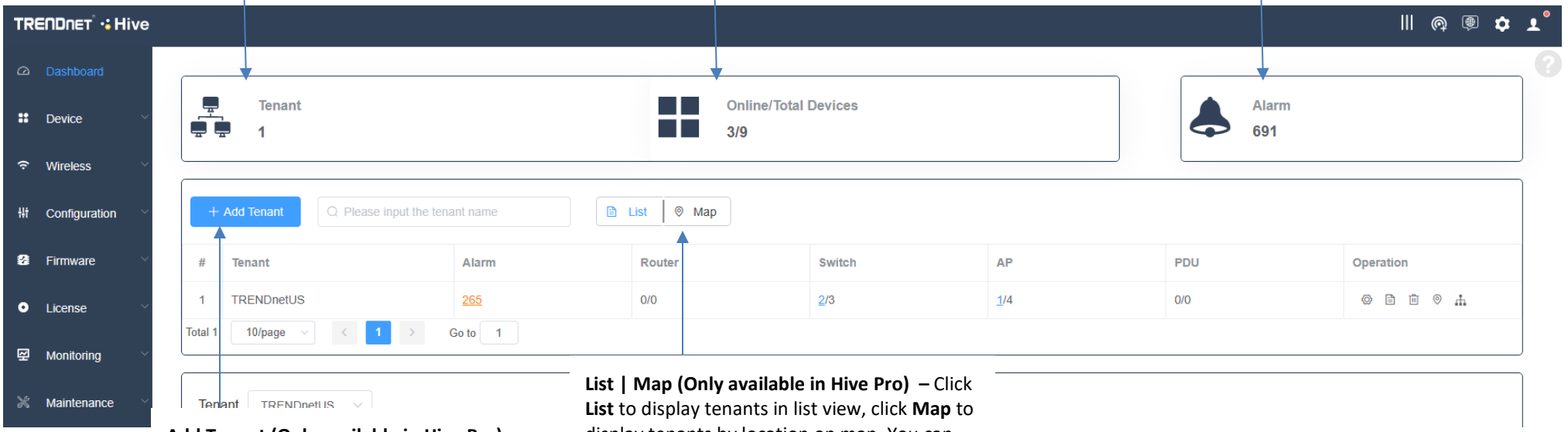
What is a tenant in the Hive Management System?

A tenant is a group in the Hive Management System for easier manageability of network locations, customers, or organizations where TRENDnet Hive compatible devices will be installed, monitored and managed. Tenant management will allow for better organization, maintenance, monitoring of each network location, customer, or organization individually. Additional users can be created for Hive access and restricted only to a specific tenant and restricted only to specific management sections for the specified tenant for access control purposes.

Tenant – Displays total number of tenants.

Online/Total Devices – Displays the total number of devices online/total number of devices for all tenants. Click to view devices (Devices > Device List)

Alarm – Displays the total number of alert notifications for all tenants. Click to view alerts (Account & Logging > System Log)



Add Tenant (Only available in Hive Pro) – Click to add a new tenant.

List | Map (Only available in Hive Pro) – Click **List** to display tenants in list view, click **Map** to display tenants by location on map. You can also view device location by entering the device MAC address.

Collapse/Expand Left Navigation

Create New Tenant (Available in Hive Pro only)

Language Selection

Alert Settings – Configure alert/email notification settings

Account & Logging – Configure your account settings such as password, email, and address. View system/device logging and messages. The red indicator will appear if a new system message is available. (System > Message List)

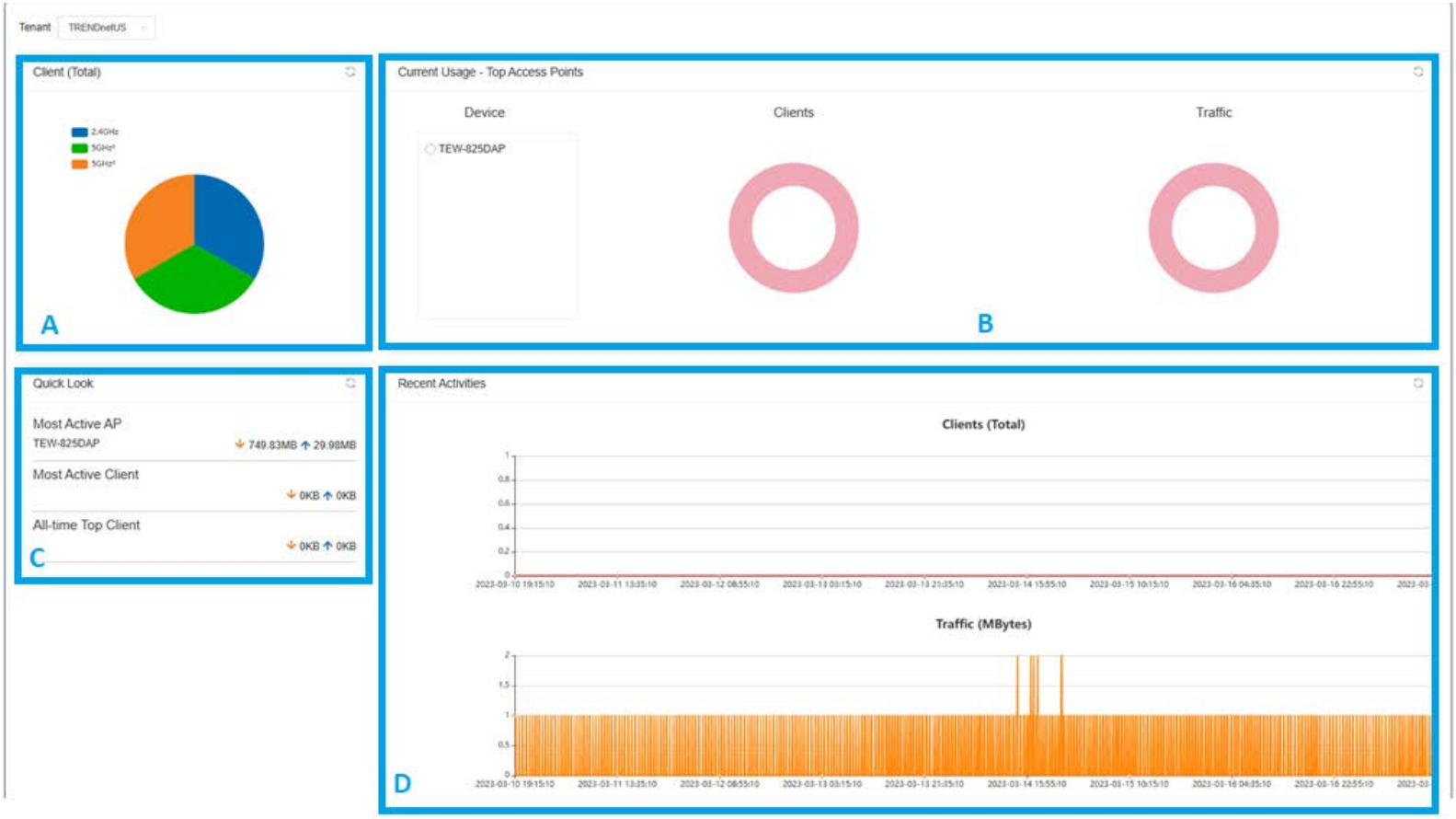
- User Management (Available in Hive Pro only) – Create users and assign access privileges to tenant settings and configuration.

Wireless Dashboard

The wireless dashboard displays an overview of the most recent activity for wireless access points, clients, and data usage over time for each tenant.

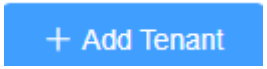
At the top left, you can click the **Tenant** drop-down list to display the wireless access point information for each tenant.

A. Clients (Total) – This section will display a list top 5 wireless profile SSIDs with highest amount of data usage/activity. When hovering over with your cursor, the SSID name and total number of data transmitted/received will be displayed.
B. Current Usage (Top Access Points) – This section will display the top 5 access points with the highest amount of data usage/activity. When hovering over with your cursor, the AP MAC address and total number of packets transmitted/received will be displayed.
C. Quick Look – This section will display the AP with the most recent activity, clients with the most recent activity, and client with the highest amount of data usage.
D. Recent Activities – This section displays a chart of the most recent activity. The Clients (Total) chart displays the total number of clients over the most recent time interval. The Traffic (Mbytes) chart displays the total number of packets transmitted on all APs over the most recent time interval.

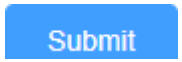


Create a new tenant (Applies to Hive Pro Only)

Important Note: *If you are using a Hive Premium account, only 1 tenant will be available, default name "MyTenant". Only Hive Pro accounts have the capability to create mulitiple tenants. Additionally, location services are only available in Hive Pro.*

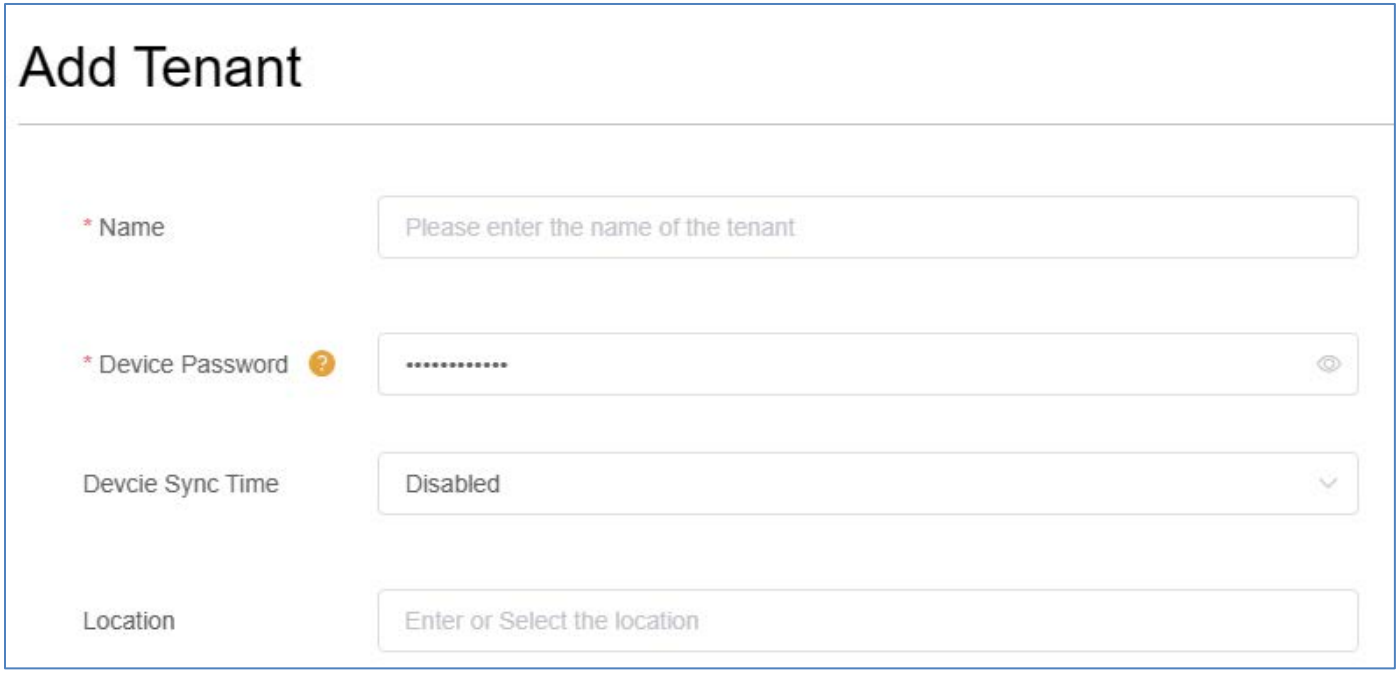
Click 

or in the top right menu, click  to create a new tenant. (Only available in Hive Pro)

In the Add Tenant window, enter the **Name** of the new tenant. Then click 

to create the new tenant.

- **Name:** Enter the name of the tenant (ex: TRENDnetUS, company or customer name and location)
- **Device Password:** The device password will automatically configure the admin password of devices connected to Hive and assigned to this tenant. This means that the default (typically "admin") or currently assigned password configured on devices will be changed automatically to the the device password configured here.
  Note: *It is strongly recommended to configure the device password in the case that administration GUI access is required on site locally.*
- **Device Sync Time:** The sync time function will automatically sync all devices time configuration with the Hive cloud time and date settings.
- **Location (Only available in Hive Pro):** Enter the address of the tenant and you can select the address information automatically listed according to Google® Maps.



The new tenant will be displayed in the tenant list.

- **Tenant –** Displays the tenant name.
- **Alarm –** Displays the current number of alerts for this tenant.
- **Router/Switch/PDU –** Displays the current number of Router/Switch/PDU devices online / total number of switch devices for this tenant.
- **Operation**
  - o Edit tenant name and location. (location only available in Hive Pro)
  - o View available devices and assign devices to the tenant. (available only in Hive Pro)
  - o Delete or remove the tenant. (available only in Hive Pro)
  - o View tenant location on map. (available only in Hive Pro)
  - o View tenant device topology.

Assigning and renewing device licenses

Note: *Devices require an active license subscription in order to be managed with the Hive Management System.*

Purchasing Hive License Key Subscriptions

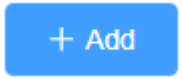
- **Hive Premium Accounts –** When logged into your Hive Management Portal online, click the 

button at the top of the page. Check the license subscription option and enter the quanity to purchase. Review and accept the payment terms and click **Purchase**, then follow the steps to enter your required information for payment.
Note: *Hive Premium license subscriptions can only be purchases through the Hive Management Portal via web browser.*

  After you have purchased your license subscription, the license key(s) will automatically be added to your account **License List** listed under **License > Add License.**

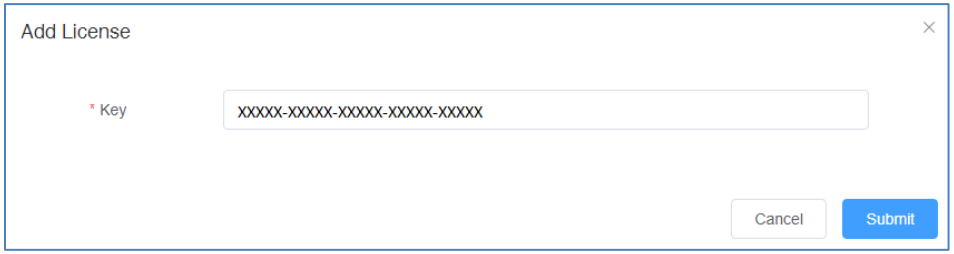
#	Key	Type	Available Model	Remaining Days	Status	Class	Device	Start Time	End Time	Create Time
1	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	-	-	365 Day(s)	Unused	Purchase	-	-	-	2023-02-28 12
2	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	-	-	365 Day(s)	Unused	Purchase	-	-	-	2023-02-28 12
3	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	-	-	365 Day(s)	Unused	Purchase	-	-	-	2023-02-28 12

- **Hive Pro Accounts –** Hive Pro accounts and license Pro subscriptions can only be purchased through an authorized TRENDnet distributor or partner. Please contact your authorized TRENDnet distributor or TRENDnet sales for more information. Hive Pro account activation is included along with Hive Pro license subscription purchases.
After you have purchased and received your license key, add the new license key to your account, in the Hive Management portal, click on **License** and **Add License** in the left navigation menu.

  Click 

button at the top right to add a new license key.

In the Add License window, enter your license key in the Key field provided and click **Submit**.

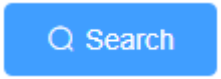


After you have entered in your license key, the new device licenses will appear in the **License List** (depending on the license susbscription purchased).

#	Key	Type	Available Model	Remaining Days	Status	Class	Device	Start Time	End Time	Create Time
1	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	-	-	365 Day(s)	Unused	Purchase	-	-	-	2023-02-28 12
2	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	-	-	365 Day(s)	Unused	Purchase	-	-	-	2023-02-28 12
3	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	-	-	365 Day(s)	Unused	Purchase	-	-	-	2023-02-28 12

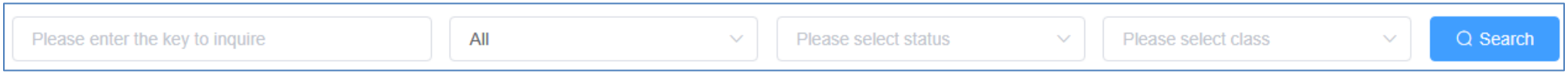
License List Table

- **Key –** Displays the device license key.
- **Type –** Displays the device type the license was assigned. (ex: Switch, AP, Router, PDU, etc.)
- **Available Model –** Displays the device model(s) that the device license key is limited to be used with, if any.
- **Remaining Days –** Displays the remaining days left on the license. You will be notified by email automatically 30 days prior to license expiration.
- **Status –** Displays current status of the license.
  - **Unused –** License is available and has not yet been assigned a device.
  - **Used –** License is not available and has already been assigned a device.
  - **Expired –** License has already been assigned to device and has expired.
  - **Abandoned –** This status may be displayed under rare circumstances such as product return where the license has been manually cancelled or terminated.
- **Class –** Displays the license class whether it was purchased, promotional, or free trial license.
- **Device** - If the device license is already assigned to a device, displays the alias name of the device. (By default, the alias/name assigned is the device serial number)
- **Start Time –** Displays the time and date the device license was activated and assigned to a device.
- **End Time –** Displays the time and date the device license will expire after being assigned to a device.
- **Create Time –** Displays the date and time the license was added to Hive account.



Note: *In the license list, you can search licenses by entering the key manually, device type, license status, and license class filter fields at top of the page. Click* ***Search*** *after you have selected to filters. Please note that the license code received with the subscription purchased will be different from the device license keys when adding the code to your Hive account.*

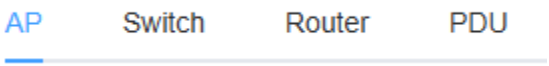
After receiving the license key, the key must be added to your Hive account to assign device licenses.



To assign an available device subscription license to a device, in the left navigation menu, click on **Devices** and click on **Device List.**

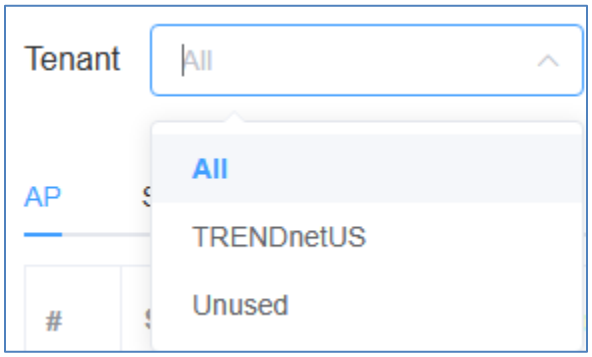
At the top of the of the device list, click the device category.

- **AP –** Wireless access points
- **Switch –** Network switches
- **Router –** Network routers or gateways
- **PDU –** Power distribution units or smart power switches



In the Tenant drop-down list at the top left of the page, select **All** to view a list of all devices for the device category that have been registered to your Hive account.

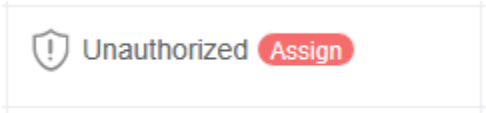
Note: *The drop-down list will also allow you to select and view tenants which will display a list of devices assigned only to the selected tenant. If you already assigned the device to a tenant, click the drop-down list and select the tenant the unlicensed device was assigned. The Unused option will list devices that are not currently assigned to tenants.*



In the list of devices under **Authorize Status,** unlicensed devices with an **Assign** button are new devices that have not been assigned a license. Click on the **Assign** button to assign a new device license to the device.

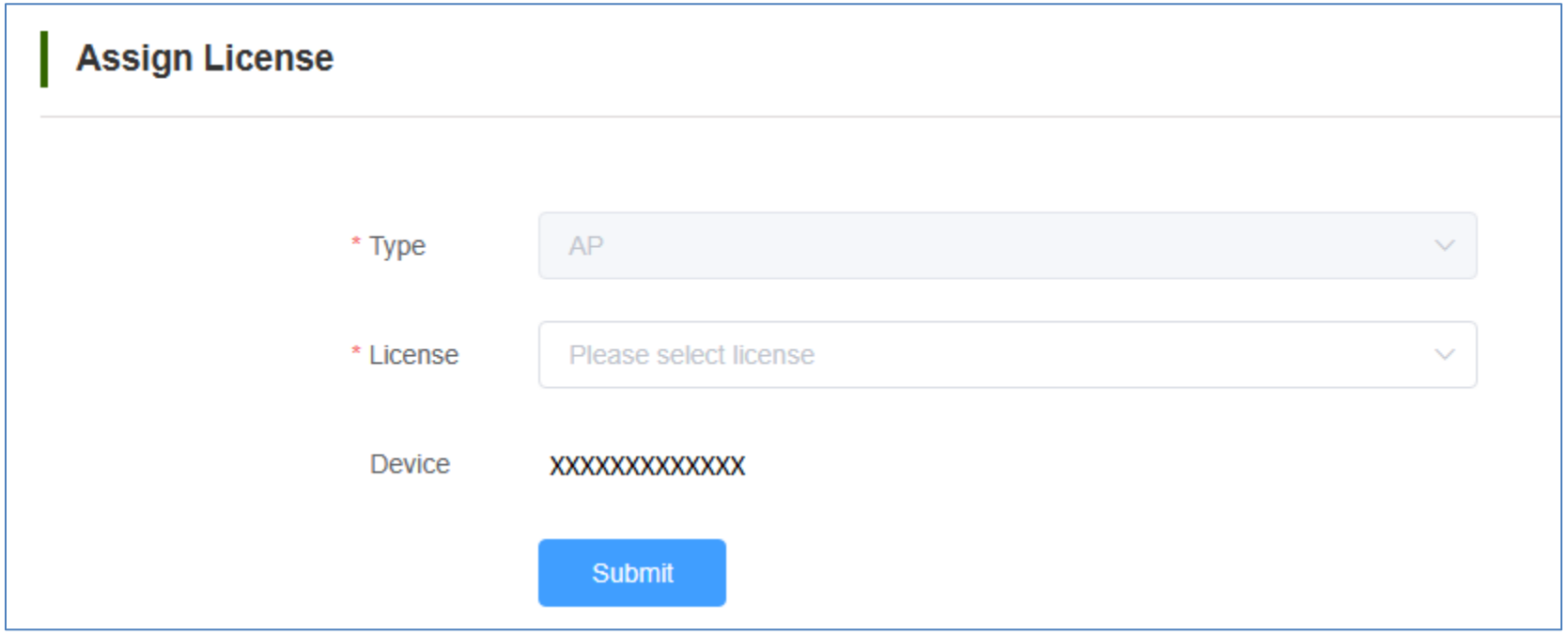
#	Status	Authorize Status	Model	MAC	SN	Alias	Tenant	FW Version	Operation
1		Authorized Renew	TEW-825DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	TEW-825DAP	TRENDnetUS	2.01b03	
2		Unauthorized Assign	TEW-921DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	921AAAAAP		2.10B09	Selelc
3		Expired Assign	TEW-821DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX	TRENDnetUS	3.00b03	
4		Expired Assign	TEW-821DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX	TRENDnetUS	3.00b05	
5		Unauthorized Assign	TEW-921DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX	TRENDnetUS	2.10B08	
6		Unauthorized Assign	TEW-826DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX		2.00b06	Selelc

Total 6 10/page 1 Go to 1

- **Authorize Status**
  - 

    This indicates that the device does not have an active license subscription assigned. Click **Assign** to assign a valid license key to activate the device subscription.
    Note: *Devices require an active license subscription in order to use with the Hive Management System.*

    Click the **License** drop-down list and select an available license to assign to the device and click **Submit.**
    Note: *If there are no licenses available, you must purchase a new license for the device.*



  - 

    This indicates that the device has a valid active license subscription assigned and is authorized for use with your Hive account.

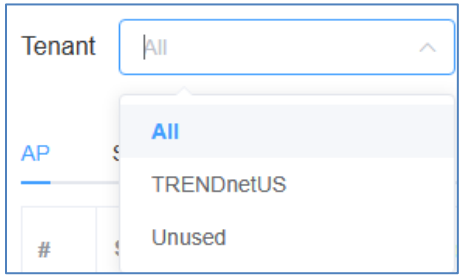
Manage devices in your Hive account

After you have registered your device with your Hive account, the device will be available in your Hive account management portal.

To view newly registered devices in your Hive management portal, in the left navigation menu, click on **Devices** and click on **Device List.**

In the Tenant drop-down list at the top left of the page, select **All** to view a list of all devices for the device category that have been registered to your Hive account.

Note: *The drop-down list will also allow you to select and view tenants which will display a list of devices assigned only to the selected tenant. If you already assigned the device to a tenant, click the drop-down list and select the tenant the unlicensed device was assigned. The Unused option will list devices that are not currently assigned to tenants.*



#	Status	Authorize Status	Model	MAC	SN	Alias	Tenant	FW Version	Operation
1		Authorized Renew	TEW-825DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	TEW-825DAP	TRENDnetUS	2.01b03	
2		Unauthorized Assign	TEW-921DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	921AAAAAP		2.10B09	Selelc
3		Expired Assign	TEW-821DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX	TRENDnetUS	3.00b03	
4		Expired Assign	TEW-821DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX	TRENDnetUS	3.00b05	
5		Unauthorized Assign	TEW-921DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX	TRENDnetUS	2.10B08	
6		Unauthorized Assign	TEW-826DAP	XX-XX-XX-XX-XX-XX	XXXXXXXXXXXX	XXXXXXXXXXXX		2.00b06	Selelc

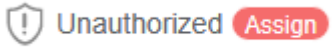
Total 6 10/page 1 Go to 1

Under the **Operation** section, if a drop-down field is available instead of button, this means that the device has not yet been assigned to a Tenant. Click the drop-down list to assigne the device to a Tenant.

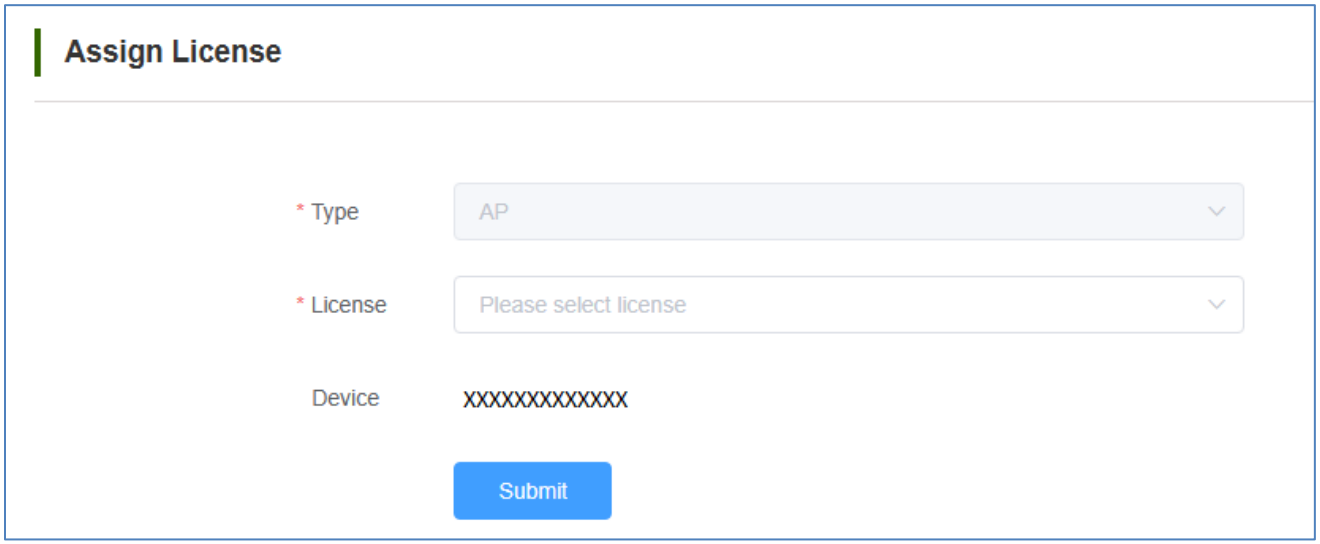
- **Status**
  - 
    This icon will indicate that the device is registered to the Hive account but is currently offline.
    Note: *Devices that are offline can be assigned to a tenant but cannot be managed, monitoring, or configured. Please ensure that the device has the correct IP address, gateway, DNS configuration, and there are no issues preventing the device from reaching the Internet at the installed location. Additionally, you have configured the cloud settings in the device management page and registering your device with your Hive user credentials.*

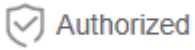
  - 
    This icon will indicate that the device is registered to the Hive account and is currently online.

- **Authorize Status**



  - **Unauthorized**
    This indicates that the device does not have an active license subscription assigned and is typically a new device registered to your Hive account that has never had a license assigned to it. Click **Assign** to assign a valid license key to activate the device subscription.
    Note: *Devices require an active license subscription in order to use with the Hive Management System.*

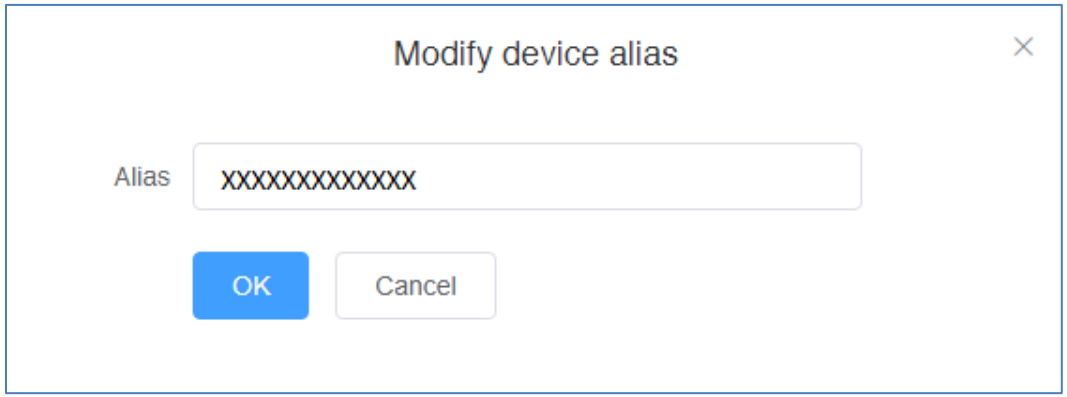




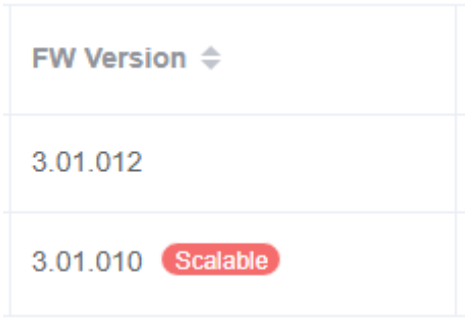
- **Authorized**
  This indicates that the device has a valid active license subscription assigned and is authorized for use with your Hive account.

- **Expired**
  The authorize status will be displayed as Expired if the device has been assigned a device key previously from an inactive/expired device license subscription trial or purchase. Click **Assign** to assign a new license key to renew the device subscription.

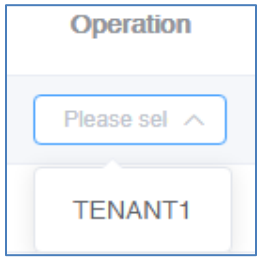
- **Model –** Displays the device model number.
- **MAC –** Displays the device MAC address.
- **SN –** Displays the device serial number.
- **Alias –** Displays the device name or label and is customizable. By default, the serial number (SN) is assigned to all devices as the Alias. Click the entry to modify the device alias, then click **OK**.
  Note: *It is recommended to change the device alias so that the device is easily identifiable in the Hive management system. (ex: TRENDnetHQ-EdgeSW1)*



- **Tenant –** Displays the tenant the device is currently assigned. If there is no tenant listed, the device is not currently assigned to a tenant.
- ***Note:*** *The device must be assigned to tenant in order to be managed, configured, and monitoring. If using a Hive Premium account, there is only one tenant available, default name "MyTenant" and devices are automatically assigned to this tenant when registering devices with a Hive Premium account.*
- **FW Version –** Displays the device firmware version.
  Note: *If Scalable is displayed in the FW version section, this indicates that there is a firmware upgrade available for the device. The device must be assigned to tenant and assigned a valid license first before the firmware can be upgraded. After the device is assigned to a tenant, click on Scalable to upgrade the device firmware.*



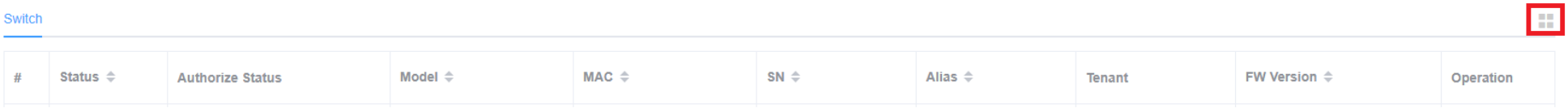
- **Operation –** Click the drop-down list to select which tenant you would like to assign the device.

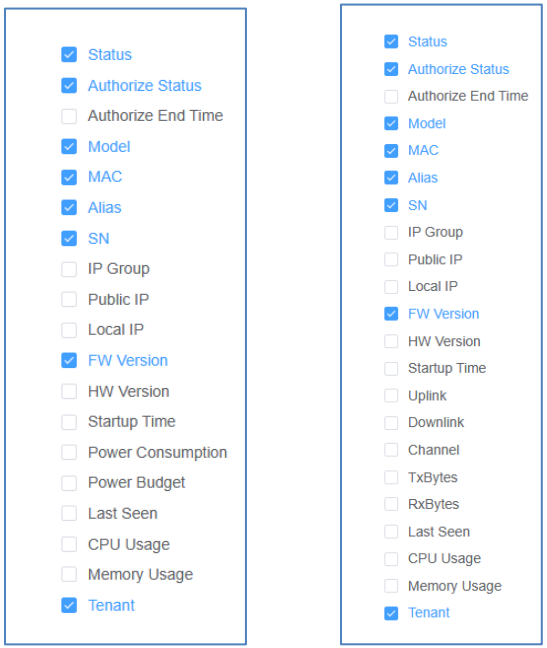


Note: *You can also assign a device to tenant under Dashboard and under Operation, click the edit button* to select which devices to assign to the tenant.

Additional Device Display Information

At the right side of the table, click the Filter Table button to select additional information to display.



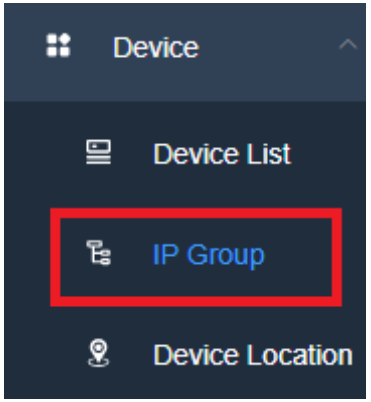


- **Authorize End Time –** Displays the time and date when the device license subscription will expire.
- **IP Group –** Displays the IP group the device is assigned. IP groups are different IP address ranges that can be listed for organization under a single tenant.
- **Public IP –** Displays the public or Internet IP address of the device network location or installation site.
- **Local IP –** Displays the local or private IP address the device is currently assigned in its network location or installation site.
- **HW Version –** Displays the hardware version of the device.
- **Startup Time –** Displays the device status uptime running continuously without reboot.
- **Power Consumption (Applies to Switch devices only)** – Displays the power consumption of the device.
- **Power Budget (Applies to Switch devices only) –** Displays the maximum PoE power budget available on the device.
- **Uplink (Applies to AP devices only) –** Displays a snapshot of the current upload speed from the device.
- **Downlink (Applies to AP devices only) –** Displays a snapshot of the current download speed to the device.
- **TxBytes (Applies to AP devices only) –** Displays a snapshot of the total data transmitted from the device.
- **RxBytes (Applies to AP devices only) –** Displays a snapshot of the total data received by the device.
- **Last Seen –** If the device is currently powered on and connected to Hive, **Online** will be displayed. If the device is currently offline, this field will display the most recent date and time the device was connected to Hive and online.
- **CPU Usage –** Displays the device's current CPU resource utilization by percentage (max. 100%)
- **Memory Usage –** Displays the device's current memory (RAM) utilization by percentage (max. 100%)

Create IP Groups

IP groups can be created under each tenant by IPv4 address range or subnet. This can better organize and simplify device provisioning if a tenant, company, or organization has multiple locations with different IP subnet or a single location with multiple IP subnets or VLANs. This allows you to provision more specified groups with firmware upgrades or configuration.

1. In the left navigation menu, click **Device** and click **IP Group.**



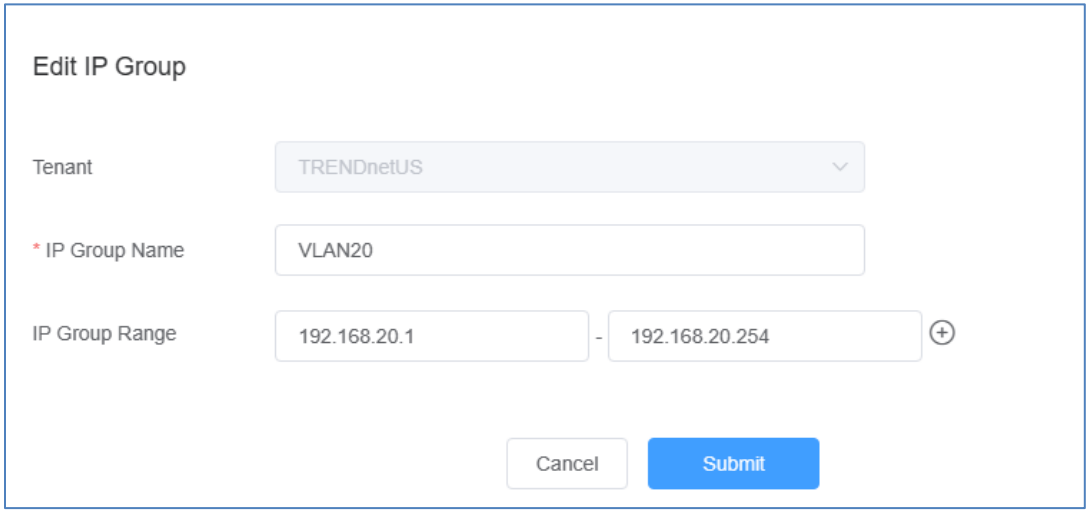
2. At the top, click **Add IP Group**.

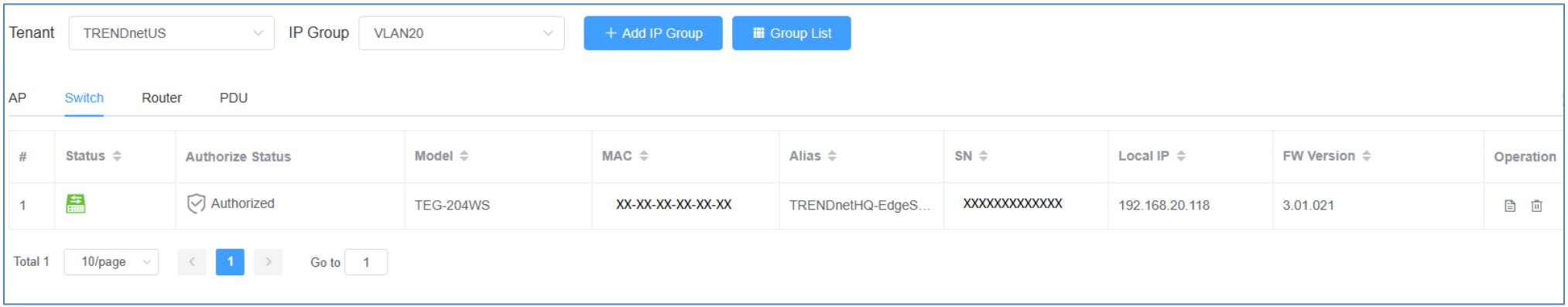
3. In the Add IP Group page, review the settings below to create the IP group and click **Submit** when completed.

- **Tenant –** Click the drop-down list to select which Tenant to create the IP group.
- **IP Group Name –** Enter the name of the IP group. (Example: VLAN20)
- **IP Group Range –** Enter the IPv4 address range for the group. (Example: 192.168.20.1 – 192.168.20.254)
- **Location (Only available with Hive Pro) –** Enter the address of the new IP Group location.

Note: *You can clck the* ⊕ *add button to add additional IPv4 address ranges to the IP group. Please note each IP group must use a different IPv4 subnet. The actual device IPv4 addressing will be dependent on your network device IP configuration. The IP Group will automatically detect the local IPv4 address of devices and categorize into the IP group created.*

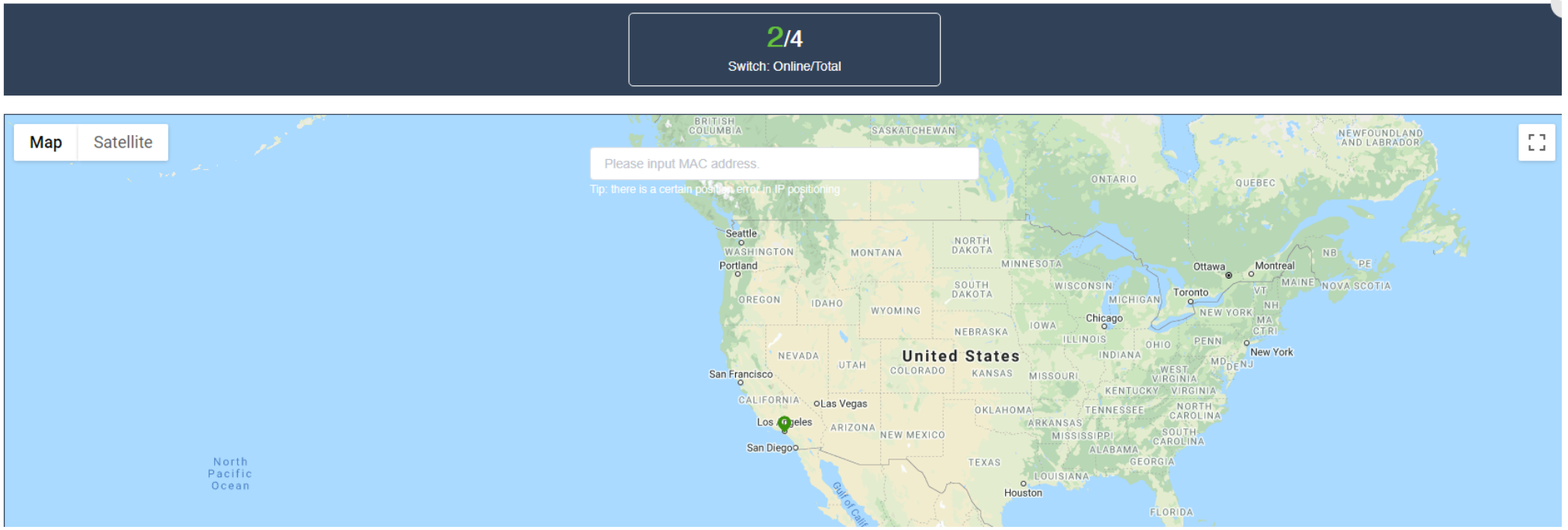
Example: If adding a new VLAN with different IP subnet to a tenant location, create an IP Group with an easily identifiable name such as VLAN20. Enter the IP range of the VLAN IP subnet (ex: 192.168.20.1 – 192.168.20.254). After creating the IP Group with the correct IP address/subnet range, when re-configuring Hive network devices with the matching IP address/subnet range, the device local IP addresses will automatically be detected and categories by Hive to be displayed and listed within the IP group. At the top of the page, click the **IP Group** drop-down list and select the IP group to display under the selected tenant. To modify or remove an existing IP Group, at the top right, click **Group List** to modify or remove an existing IP group.





View Device Location (Available only in Hive Pro)

To view the locations of registered devices in your Hive management portal, in the left navigation menu, click on **Devices** and click on **Device Location.** You can also view the location of specific device by entering the device MAC address. (Format: XX-XX-XX-XX-XX-XX or XX:XX:XX:XX:XX:XX)



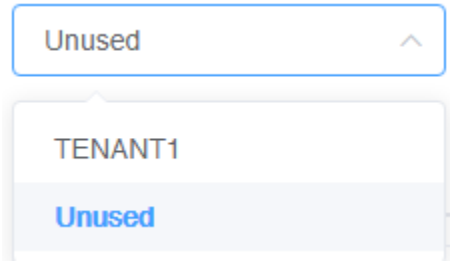
Configure devices in your Hive account

Note: *Devices must be assigned to tenant before they can be configured through Hive management.*

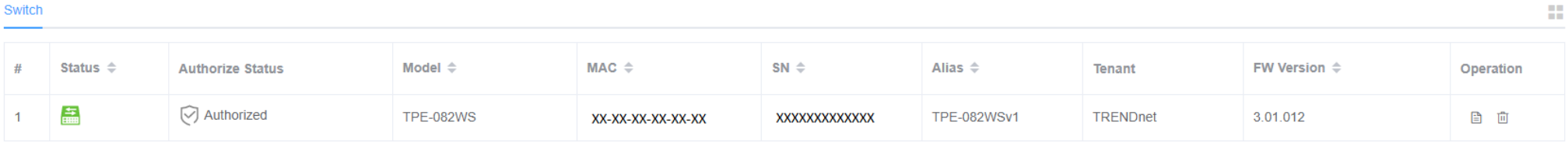
After you have assigned your devices to a tenant, you can apply configuration settings to your devices in your Hive management portal in the left navigation menu, click on **Devices** and click on **Device List.**

In the top left drop-down list and select the tenant to display the list of assigned devices.

In the example below, TENANT1 has been created and will be selected for this example.



Under TENANT1, the assigned device (TRENDnet Web Smart Switch Model TEG-082WS) will be displayed with the device information.



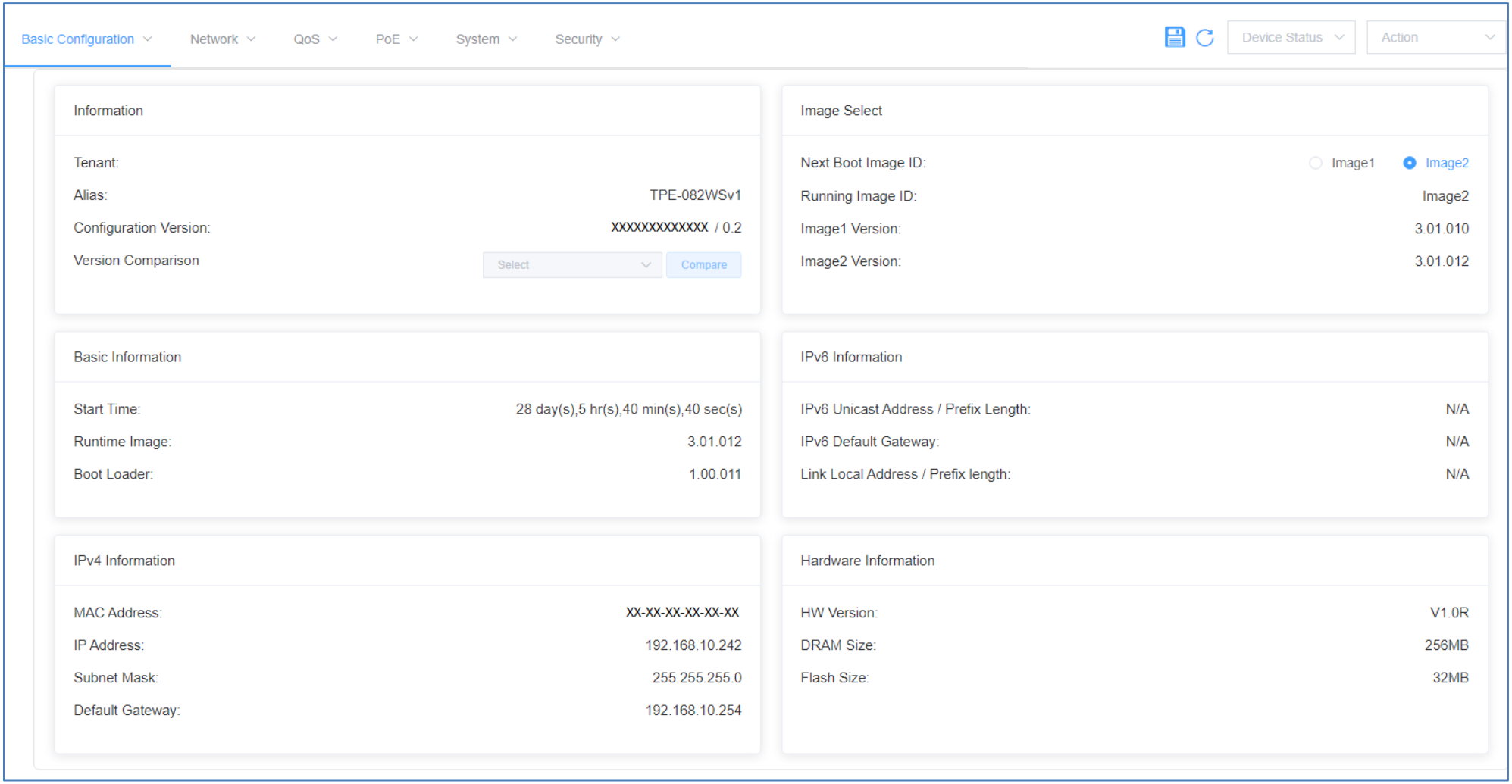
To apply configuration settings to the device (TPE-082WS), under the **Operation** section, click the edit button 

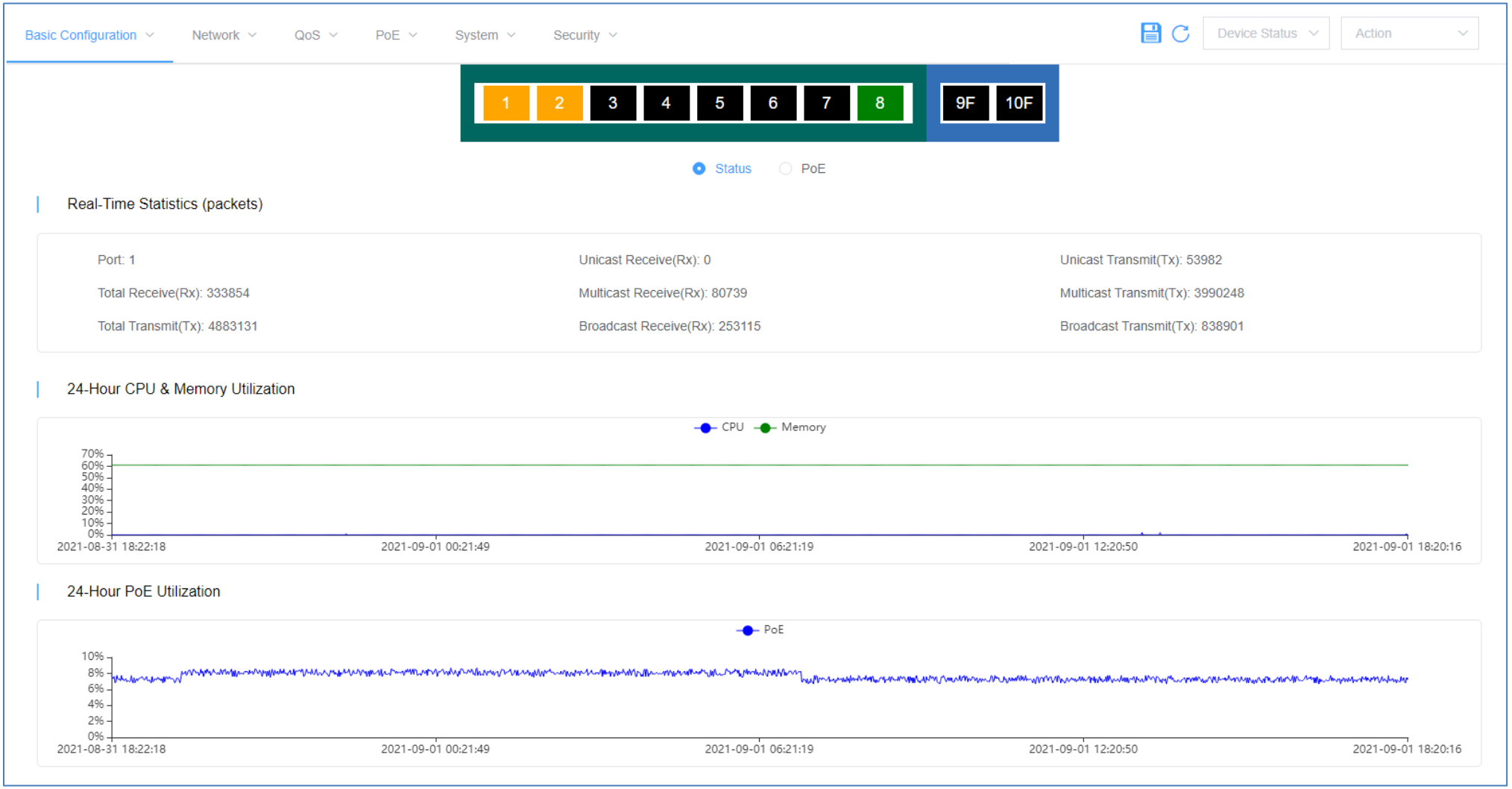
Note: *To remove the assigned device from the tenant, click the trash button*  .

The available device configuration settings will be displayed.

Note: *Please refer to the device User Guide for additional information on the device configuration settings.*

- Displayed below are example configuration pages from TRENDnet Web Smart Switch Model TPE-082WS
- To apply configuration changes for Hive supported Web Smart Switches, modify the device configuration settings and click **Submit.**
- The Version Comparison function for Hive supported Web Smart Switches, will allow you to compare the current switch configuration with new configuration file created in the Hive management system for provisioning.



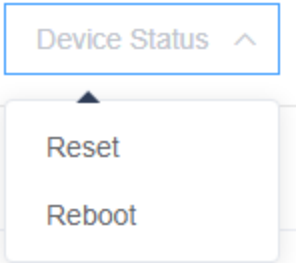


To view newly registered devices in your Hive management portal, in the left navigation menu, click on **Devices** and click on **Device List.**

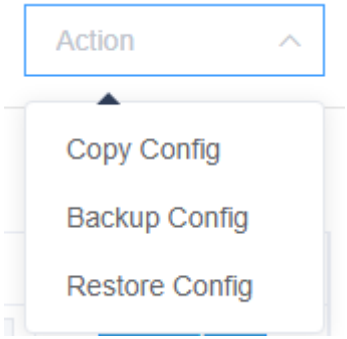
In the top right section of the device configuration page, please reference the functions below.

-  - Permanently commits and saves configuration to device.
-  - Refreshes the device configuration page.

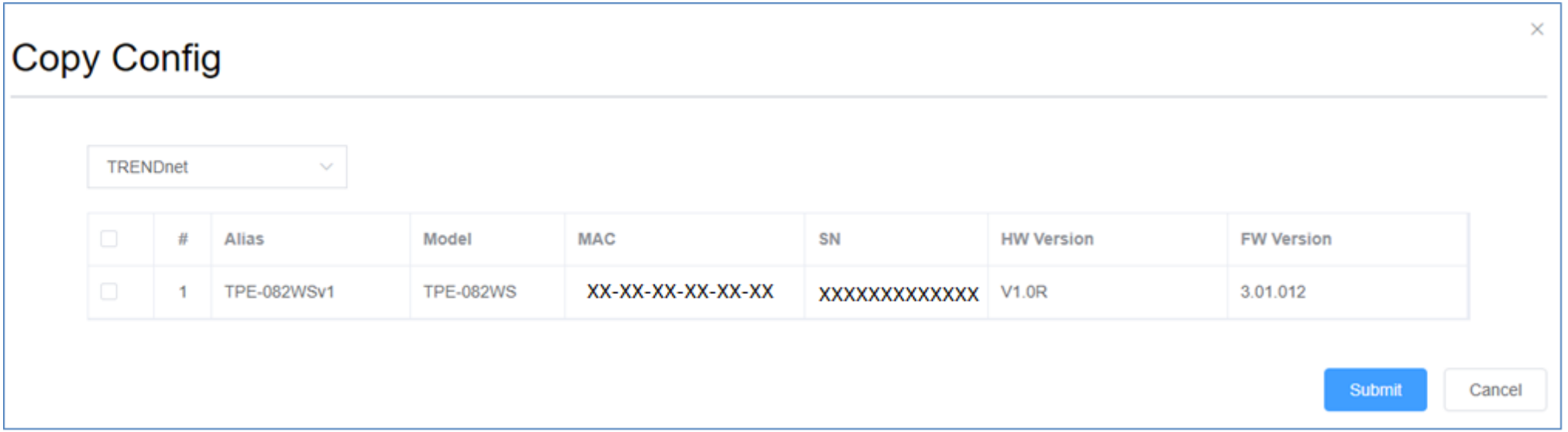
- **Device Status**
  - Reset - Resets the device to factory settings default except for IP address, default gateway, DNS, and cloud registration settings.
  - Reboot – Reboots / power cycles the device.



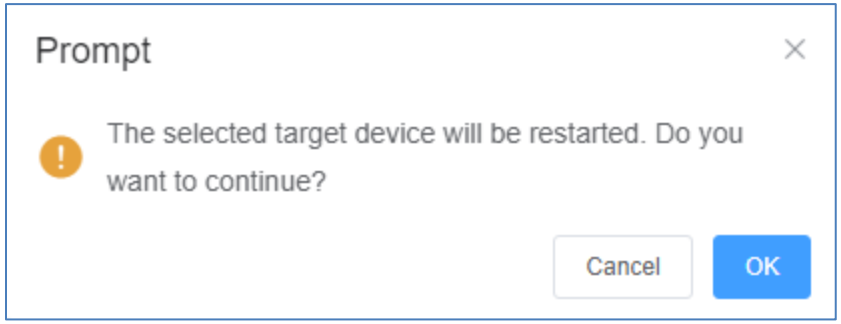
- **Action**
  Note: *The configuration backed up or copied from a device can only restored to the same model device. Configuration files that are backed up from devices to Hive cloud cannot be edited. Customizable configuration files must be created under the Configuration > Create section.*



  - **Copy Config** – Backup configuration file from the device to Hive cloud and copies configuration to target device.
    To copy configuration from a device and restored another device of the same model, click **Action** and then click **Copy Config**.
    In the Copy Config window, click the drop-down to select the Tenant of the destination device you would like to copy over the configuration.
    Check the device to copy over the configuration and click **Submit.**

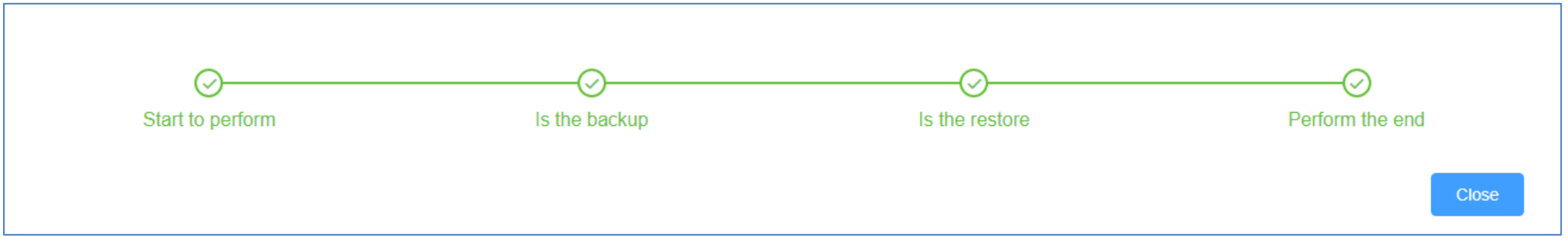


Click **OK** at the prompt to message indicating that the target device will be restarted or rebooted to restore configuration.



After the operation is completed, click **Close.**

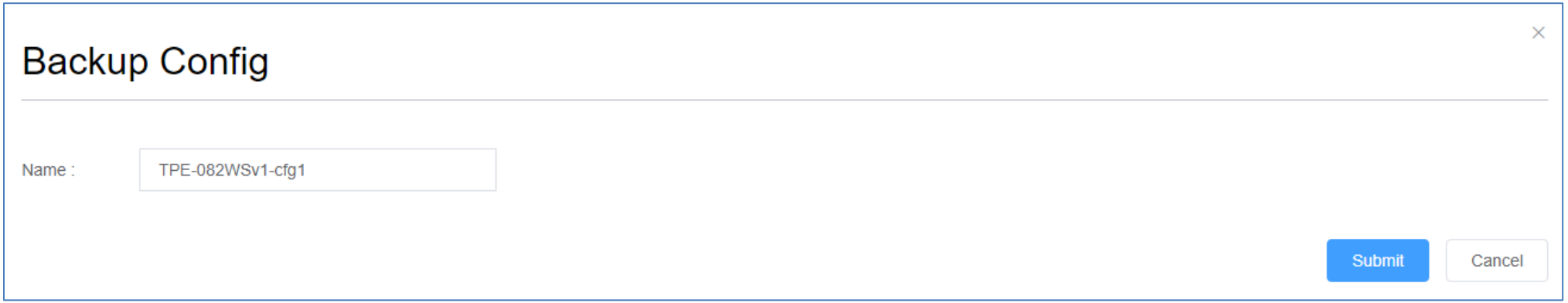
Note: *Please wait for the operation waiting to complete before navigating to another section, otherwise, the operation may fail.*



You can verify that the device configuration was backed up to the Hive cloud under **Configuration > Backup**.

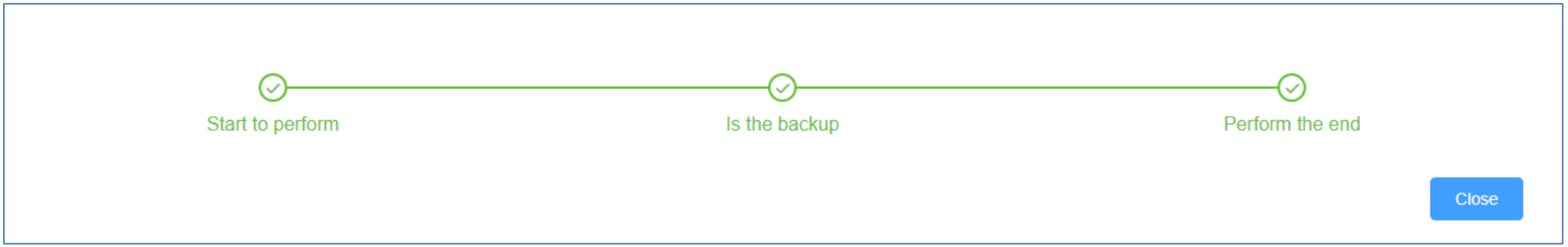
	Name	Operator	Tenant	Model	Create Time
☐	TPE-082WSv1-cfg1	XXXXXXXXXX	TRENDnet	TPE-082WS	2021-09-02 18:12:15
☐	SNXXXXXXXXXX #0851	XXXXXXXXXX	TRENDnet	TPE-082WS	2021-09-02 18:01:16

- **Backup Config** – Backup configuration file from the device to Hive cloud.
  To backup configuration from a device and save to Hive cloud to be restored later, click **Action** and then click **Backup Config**.
  In the Backup Config window, enter a name for the configuration file and click **Submit.**



After the operation is completed, click **Close.**

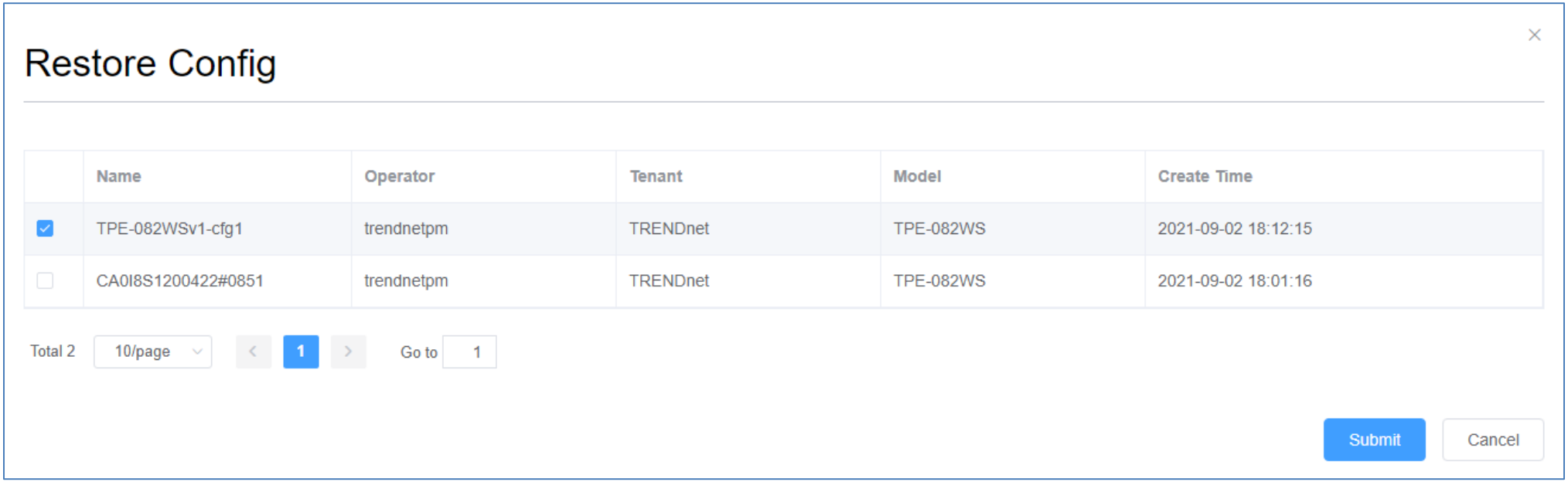
Note: *Please wait for the operation waiting to complete before navigating to another section, otherwise, the operation may fail.*



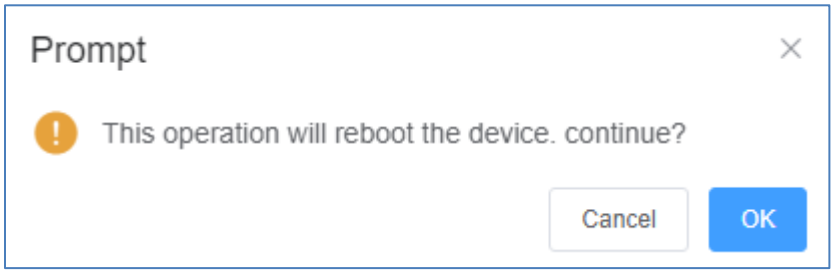
You can verify that the device configuration was backed up to the Hive cloud under **Configuration > Backup**.

	Name	Operator	Tenant	Model	Create Time
☐	TPE-082WSv1-cfg1	XXXXXXXXXX	TRENDnet	TPE-082WS	2021-09-02 18:12:15
☐	SNXXXXXXXXXX#0851	XXXXXXXXXX	TRENDnet	TPE-082WS	2021-09-02 18:01:16

- **Restore Config** – Restores configuration to target device from a previously backed up configuration on the Hive Cloud.
  To restore configuration to a target device, click **Action** and then click **Restore Config**.
  In the Restore Config window, check the previously backed up configuration file to restore and click **Submit.**

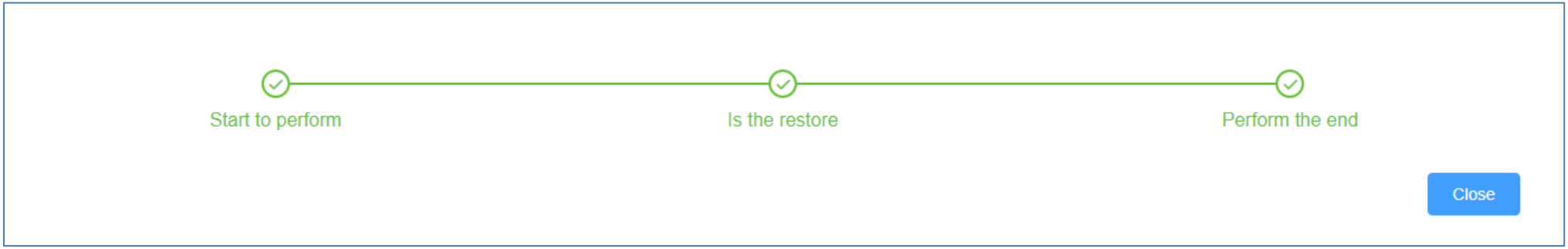


Click **OK** at the prompt to message indicating that the target device will be restarted or rebooted to restore configuration.



After the operation is completed, click **Close.**

Note: *Please wait for the operation waiting to complete before navigating to another section, otherwise, the operation may fail.*

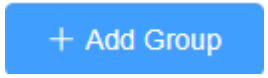


Configuring wireless access point groups

The wireless section allows you to assign multiple wireless access points into wireless groups for simplified and centralized management of onsite WiFi. Easily add a new WiFi network or create a captive portal/wall garden, deploy new access point with configuration and firmware upgrade provisioning with wireless groups. Additionally, assigning wireless access points to wireless groups enables seamless client roaming protocols such as 802.11r fast BSS transition/fast roaming or Opportunistic Key Caching (OKC).

Note: *Wireless access points must be registered to your Hive account along with license subscription before they can be assigned and managed using wireless groups.*

Create and assign wireless access points to a WiFi Group

1. To add a wireless group, click on **Wireless** and click **WiFi Groups.** At the top of the page, click the 

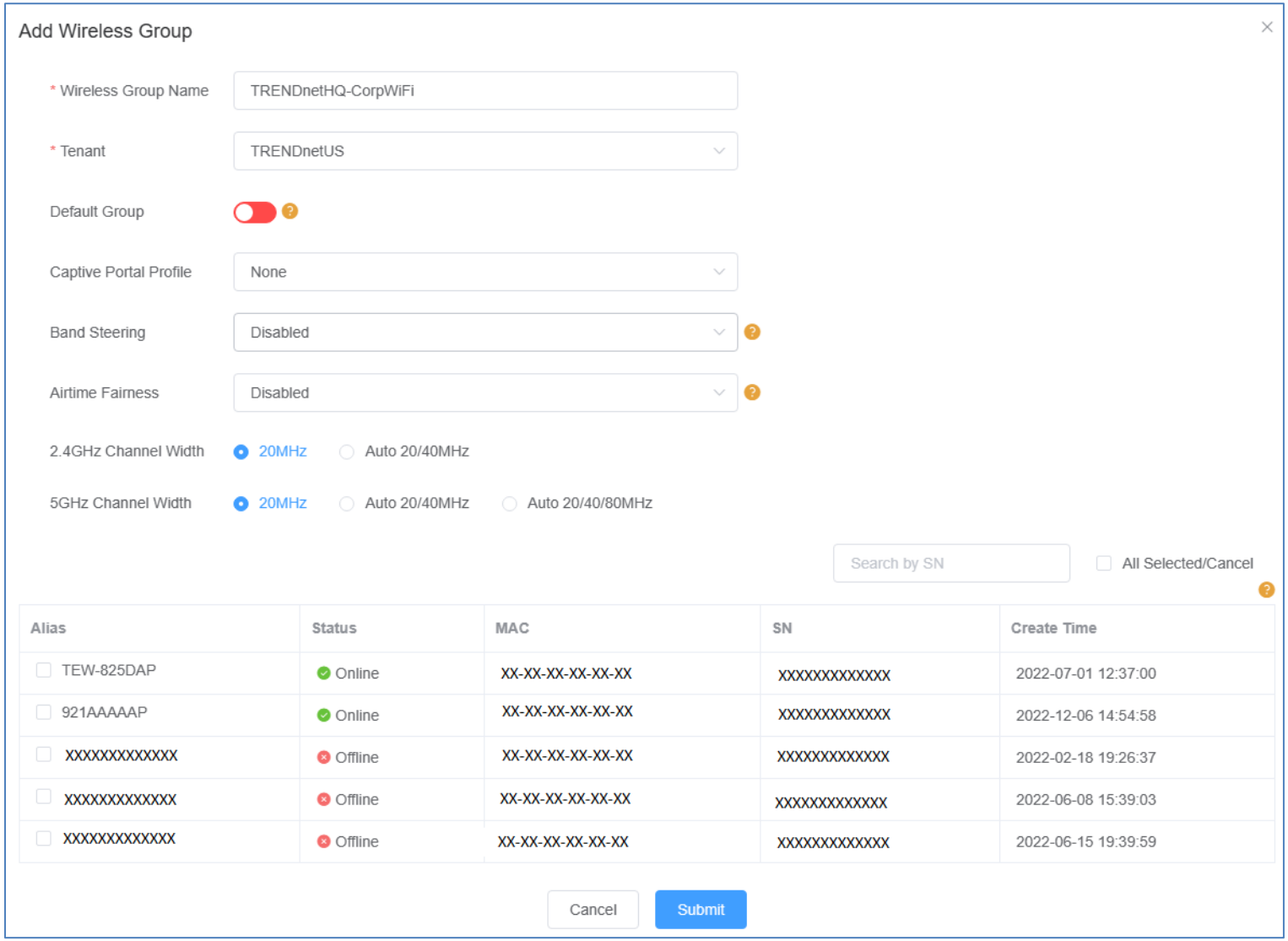
button.

2. Review the configuration settings below.

- **Wireless Group Name:** Enter an easily identifiable name for the wireless group.(ex: TRENDnetHQ-CorpWiFi)
  Note: *This is not wireless network name or SSID. This is the name of the wireless group to be identified in the Hive management system.*
- **Tenant:** Click the drop-down and select the Tenant that the wireless group will be assigned. After the tenant is selected, the wireless access points assigned to the tenant will appear in the table at the bottom of the window.
  Note: *Multiple tenants is only available in Hive Pro.*
- **Default Group:** If this setting is enabled, any wireless access points added to the assigned tenant will automatically be assigned this group along with the group's wireless configuration settings, SSIDs, security, roaming, etc. If this setting is not checked, wireless access points must be manually added to the WiFi group to adopt all of the wireless configuration settings. By default, this setting is disabled.
- **Captive Portal Profile:** If you would like to assign a captive portal profile to be used with specific WiFi networks in the wireless group, click the drop-down and select the captive portal profile. Captive portal profiles must be created in the Wireless and Captive Portal section first before they become available in the WiFi group configuration.
  Note: *Only one captive portal can be assigned to WiFi group at a time. This setting does not apply captive portal authentication for all WiFi networks created under this WiFi group, only WiFi networks with the captive portal authentication setting enabled.*
- **Band Steering:** Enable or disable band steering globally for all access points assigned to this WiFi group.
- **Airtime Fairness:** Enable or disable airtime fairness globally for all access points assigned to this WiFi group.
- **2.4GHz Channel Width:** Configure the 2.4GHz channel width setting globally for all access points assigned to this WiFi group.
  Note: *The recommended setting is 20MHz. The highest channel width setting may not be supported by all wireless access point models. If your wireless access point model does not support the max. channel width setting, the wireless access point will be configured with the highest supported channel width.*
- **5GHz Channel Width:** Enable or disable airtime fairness globally for all access points assigned to this WiFi group.
  Note: *The recommended setting is Auto 20/40/80MHz. The highest channel width setting may not be supported by all wireless access point models. If your wireless access point model does not support the max. channel width setting, the wireless access point will be configured with the highest supported channel width.*

In the tenant wireless access point table at the bottom of the window, check the access points you would like to add to the WiFi group and click **Submit** to create the WiFi group.

Note: *All previous access point configuration settings will be reset to default and will be overwritten with the wireless group configuration settings. If wireless access points are removed WiFi groups, the access points will automatically be reset to factory default configuration.*



#	Group Name	Operator	Create Time	Operation
1	TRENDnetHQ-CorpWiFi		2023-03-22 18:26:14	

After the WiFi group is created, under the **Operation** section, review the options below.

- Modify the WiFi group configuration settings.

- Add a WiFi network configuration profile to the WiFi group.

- Delete the WiFi group.

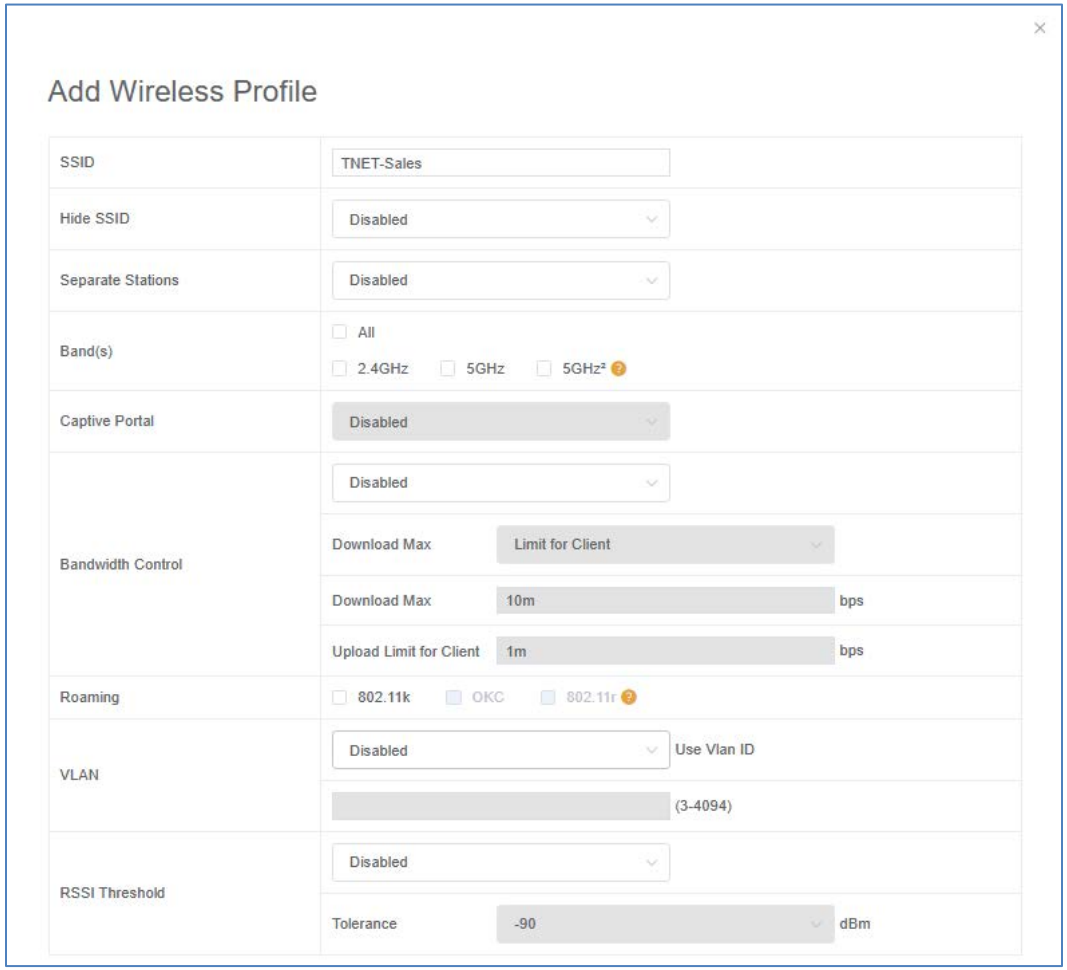
Adding a WiFi network to the WiFi group

Note: *You can create up to 8 WiFi networks max. for each WiFi group.*

1. For the WiFi group, under the Operation section, click to add a new WiFi network to the wireless group.

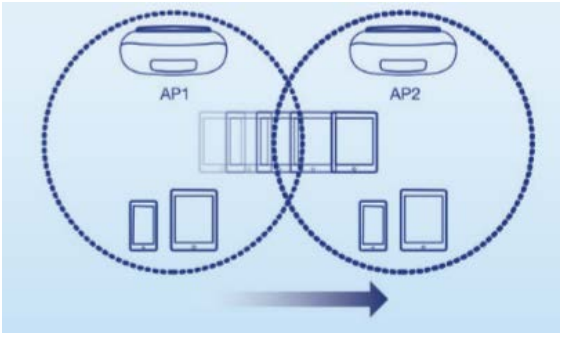
2. At the top right of the window, click the + Add Wireless button to create a new WiFi network profile.

3. Review the WiFi network configuration settings below.



- **SSID:** Enter the wireless network name or SSID for the wireless network. (ex: TNET-Sales)
  Note: *This will be the WiFi name discovered by your wireless clients to connect.*
- **Hide SSID:** Enabling the option to hide the wireless network name from being broadcasted and discovered.
- **Separate Stations:** Enabling this option to enable wireless client isolation to restrict wireless client communication between other wireless clients for this WiFi network.
- **Band(s):** Check the wireless band the WiFi network should operate.
  Note: *The second 5GHz² band may not be available on all wireless access point models. Please refer to your wireless access point specifications. If the All option is checked and 5GHz² band is not supported, only the 5GHz band will be configured the access point.*

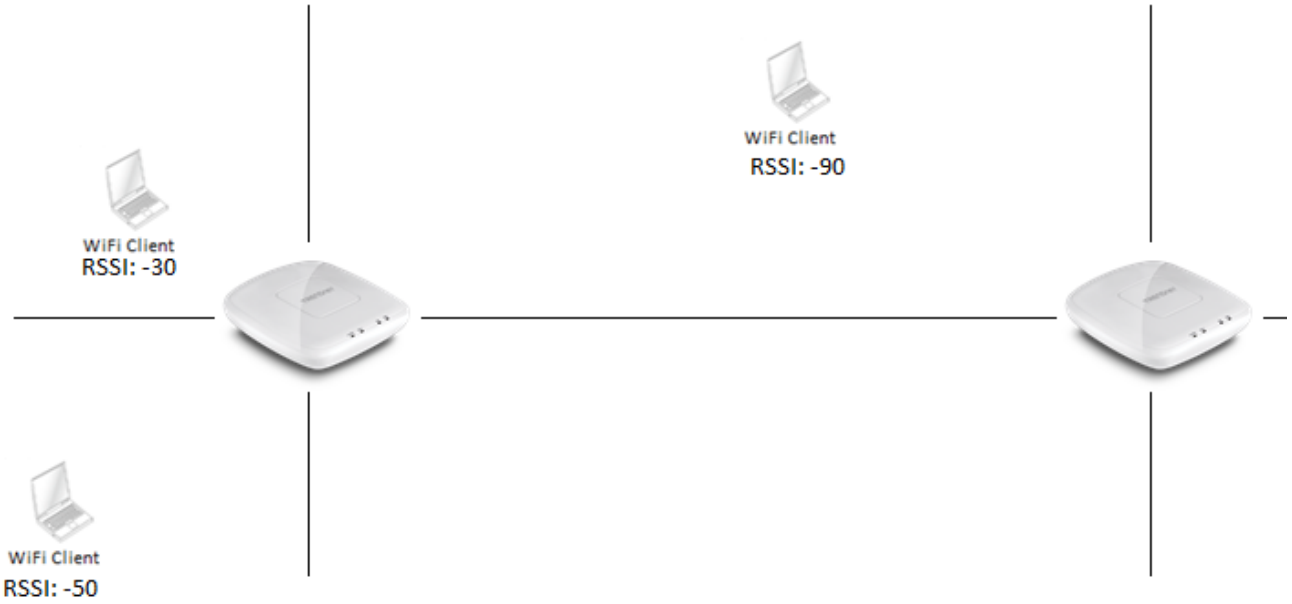
- Captive Portal: Enabling this option will enable captive portal authentication on this WiFi network. The captive portal configuration settings will use the captive portal profile set in the WiFi Group settings under Wireless > WiFi Groups. *The Captive Portal profiles can be created under Wireless > Captive Portal.*
  Note: *If enabling captive portal on the WiFi network, typically, the security settings under the Authentication Method section (Disabled) are not used since captive portal will be used for authentication to connect to this WiFi network. If both captive portal is enabled and a security mode is selected, WiFi clients will need to authenticate with both methods in order to connect to this WiFi network.*
- Bandwidth Control: Check the option to enable bandwidth control. This option allows you to specify the maximum download bandwidth limit for either the SSID or each client device, upload can only be specified each client device. The unit is specified in bits. Lowercase "m" can be used to specify Megabits (e.g. 1m) and lowercase "k" can used to specify kilobits (e.g. 10k
- Roaming: Check the wireless roaming protocols for this WiFi network.
  - **802.11k** – This protocol enables the exchange of messages between APs and client devices which includes utilization and signal strength information of neighboring APs in the same wireless network. This protocol can assist supported client devices in better roaming decisions when transitioning between multiple APs in the same wireless network. Client devices must support 802.11k in order to use this feature but it can be safely enabled and functioning whether or not client devices support this standard.
    Note: *This is a recommended roaming setting to enable along with 802.11r or OKC.*
  - **802.11r –** This protocol allows client devices to pre-authenticate with neighboring APs to significantly reduce the transition time or eliminate the need for re-authentication during transition from one AP to another. Client devices must support 802.11r in order to use this feature and should not be enabled unless client devices support this standard.
    Note: *This is the recommended roaming setting. 802.11r is only available when using WPA/WPA2/WPA3-Personal wireless security. Under Authentication Method at the bottom, click the* ***Security Mode*** *drop-down list and select one of the support security modes to make this roaming option available.*
  - **OKC (Opportunistic Key Caching) –** This protocol functions as a non-standard version of 802.11r in allowing client devices to pre-authenticate with neighboring APs. This protocol operates independently on the controller and APs and does require client devices to support any specific pre-authentication roaming standards. This setting is recommended for the highest compatibility in order for all client devices to benefit fast roaming transition across your wireless network.
    Note: *OKC is only available when using WPA/WPA2/WPA3-Enterprise wireless security. Under Authentication Method at the bottom, click the* ***Security Mode*** *drop-down list and select one of the supported security modes to make this roaming option available.*

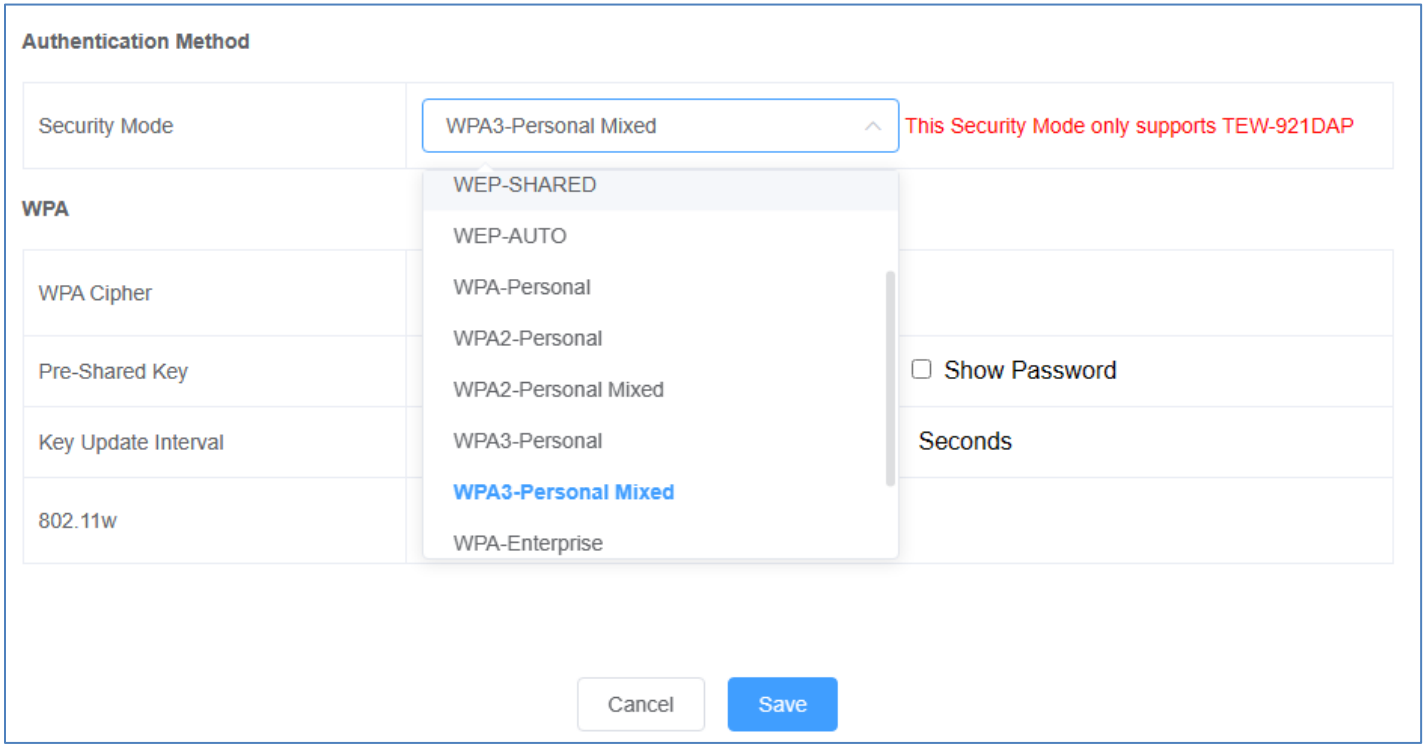


- VLAN: Enable this option to assign a specific 802.1q VLAN tag or ID to the SSID or wireless profile. By assigning a specific VLAN tag or ID, client devices that connect to the profile, will be placed in the specified VLAN.
  Note: *802.1q VLAN should be configured on your switch/router and network infrastructure to support use this feature.*

- **RSSI Threshold:** Enable this option set a signal strength limit on wireless client devices when the AP will force the client to disconnect.
  In a wireless roaming network with multiple access points, this feature can assist by forcing the disconnection of the wireless client device before signal strength and connectivity to the AP are too low to sustain enough bandwidth for Internet streaming applications. This will force the wireless client device to connect to another AP with a stronger signal and connection rate relative to it's new location. It is the nature of wireless client devices to maintain connectivity to the currently connected AP as long as the signal can still be discovered.

In the example diagram, you can see that the further away the client device is from the AP, the lower signal strength. (-30 RSSI is a higher strength value relative to the AP compared to -90 RSSI). The client device at -90 RSSI is closer to the next AP but without the forced disconnection from the AP on the left, without the RSSI threshold function, the client device would remain connected to the much further AP on the left than stronger signal AP on the right. Forcing a disconnect from the originally connected AP on the right would force the client to connect to the much higher signal strength AP on the right providing better connectivity during the transition between physical locations.





Authentication Method

- Select the authentication method used for the WiFi network. Review the configuration settings below and click **Save** at the bottom to save the configuration.
  - **None** – Does not require client devices to authentication or enter in any security parameters to connect to the wireless network. Not recommended for typical usage. Only recommended if using captive portal authentication.
  - **WEP** – Requires client devices to enter an unencrypted key to connect to the wireless network. Only Key Index 1 is supported. Not recommended since key is unencrypted and does not support 802.11n and 802.11ac/11ax link rates.
    Note: *Some wireless access point models may no longer support this security option.*

WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,C,?,*, /,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

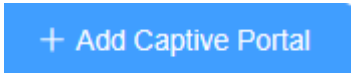
- **WPA/WPA2/WPA3-Personal & Personal Mixed** – Requires client devices to enter an encrypted key/passphrase to connect to the wireless network. The mixed setting allows for client compatibility with the previous security protocol.
  Note: *WPA3-Personal Mixed is the recommended setting to support the latest security protocol and also provide client compatibility allowing connections using WPA2. This is also the recommeneded setting for use with wireless client roaming for compatibility with older wireless access points. Please note that some wireless access point models may not support the WPA3 security standard.*
  Passphrase Format:8-63 alphanumeric characters (a,b,C,?,, /,1,2, etc.)*
- **WPA/WPA2/WPA3-Enterprise & Enterprise Mixed –** Requires the configuration use of an external RAIDIUS server for authentication through EAP (Extensible Authentication Protocol). Depending on the EAP protocol configured on the external RADIUS server, client devices will need to be configured with the same authentication and credentials in order to connect to the wireless network.
  Note: *WPA2-Enterprise is the recommended setting if using RADIUS based authentication to an external authentication server.*
  - **IP Address:** Enter the IP address of the RADIUS server. (e.g. *192.168.10.250)*
  - **Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.
  - ***Note:*** *It is recommended to use port 1812 which is the default RADIUS port.*
  - **Shared Secret:** Enter the shared secret used to authorize your APs with your RADIUS server.
- **OWE (Opportunistic Wireless Encryption) –** This is a newer wireless security standard that was released as part of the WPA3 standard. This type of security allows wireless clients to connect without the need to enter any authentication information such as a key or passphrase.
  Note: *WPA3-Personal Mixed is the recommended setting to support the latest security protocol and also provide client compatibility allowing connections using WPA2. This is also the recommeneded setting for use with wireless client roaming for compatibility with older wireless access points. Please note that some wireless access point models may not support the WPA3 security and OWE standards.*

Using Captive Portal Authentication

The captive portal feature allows you to provide customized authentication typically for public WiFi users and guest user authentication. Captive Portal authentication is typically used in areas such as hotel lobbies, airports, coffee shops and other WiFi hot spots. The access points support both captive portal authentication through the built-in user account database which includes basic portal customization or CoovaChlli which is an open-source implementation of captive portal (UAM) function and 802.1X RADIUS (please note CoovaChilli requires an external CoovaChilli server which must be preconfigured to work and authenticate requests through the access point). The access points also support URL/web page redirect without authentication for advertisement purposes. The captive portal functionality of the access points can be managed through the wireless controller and applied to select wireless profiles as desired. It is recommended to disable standard WiFi security methods such as WEP/WPA/WPA2 in order to use the captive portal authentication method instead on selected wireless profiles. Before applying captive portal functionality to select wireless profiles, the captive portal type must be configured first along with all required parameters.

First, create a captive portal profile so that it can be assigned to a WiFi group.

1. Click on **Wireless** and click on **Captive Portal.**

2. At to the top of the page, click the 

button.

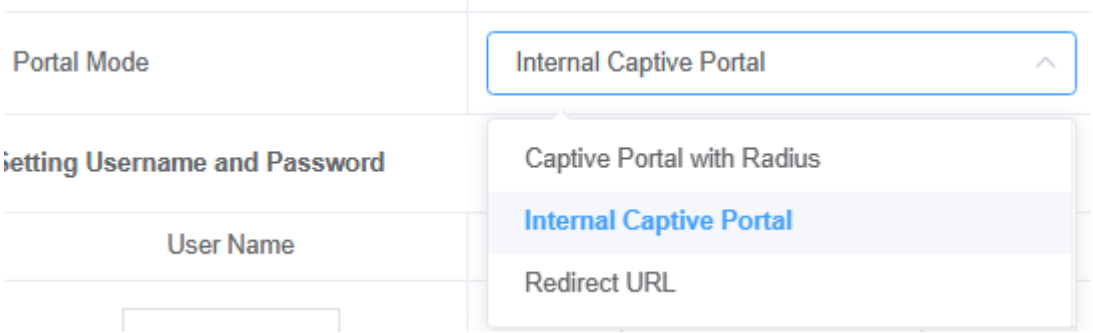
3. Review the configuration settings below.

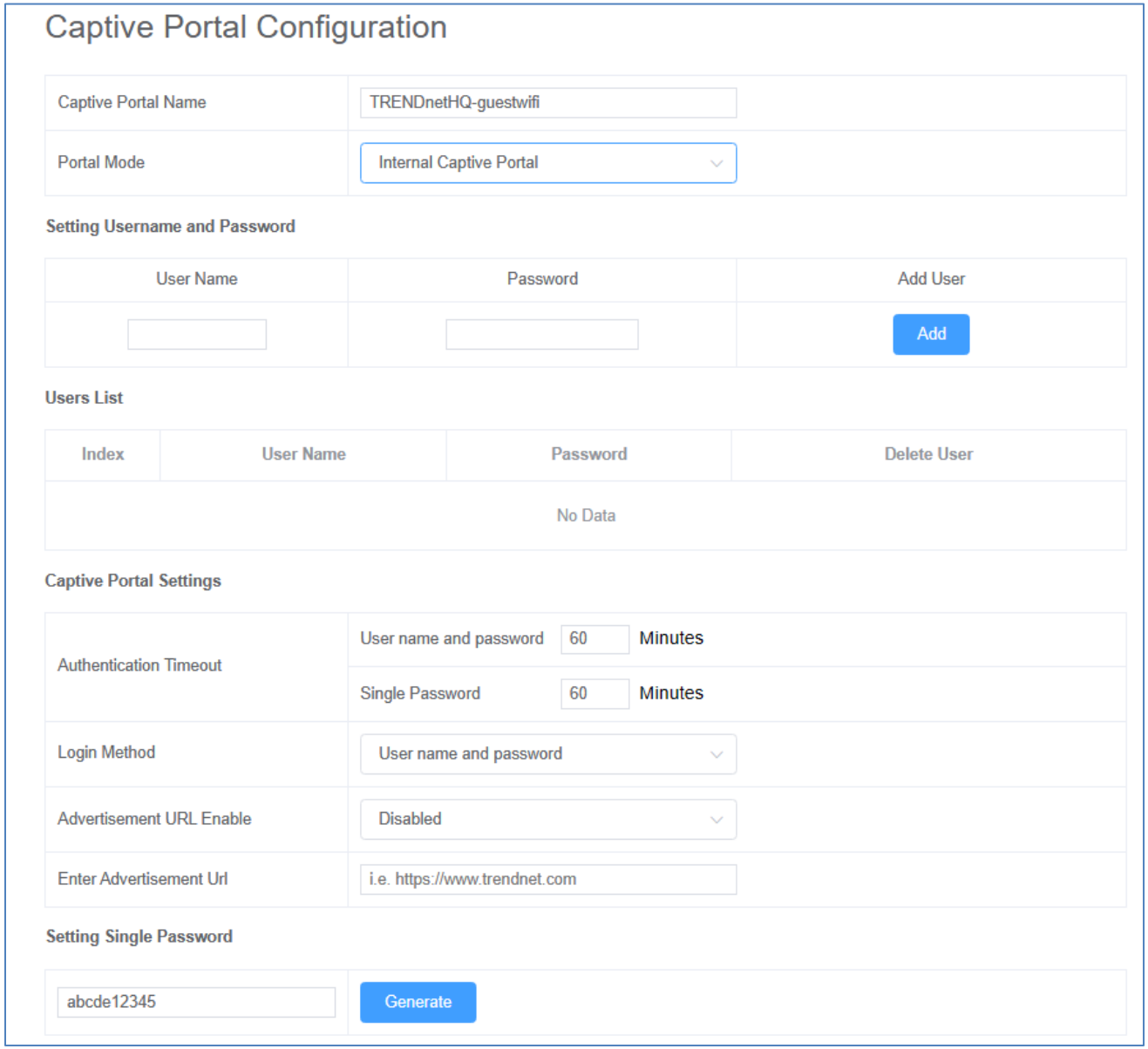
- **Captive Portal Name:** Enter a name for the captive portal profile. (ex: TRENDnetHQ-guestwifi)
- **Portal Model**

Select the **Portal Mode**:

Note: *Only one mode can be used, multiple modes cannot be used at the same time.*

A. **Internal Captive Portal** – This mode allows you to authenticate requests through the built-in user account database and apply basic customization to the captive port user login page. This option is recommended and does not require an external authentication server.
   Note: *This is the recommended mode for easier setup since this authentication database can be configured locally and no external authentication server is required.*
B. **Redirect URL** – This mode requires no authentication and allows redirection of users to a specific website/URL only.
C. **Captive Portal with RADIUS** – This mode requires an external UAM (universal access method) server to be configured to provide the captive portal user login page and authenticate request through the access point.



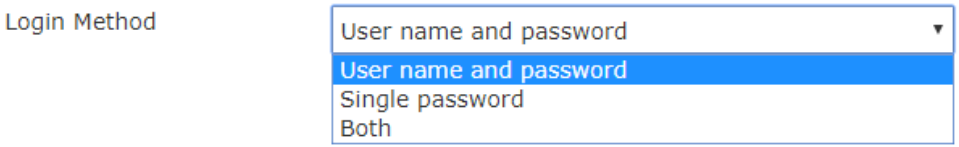


A. To Internal Captive Portal

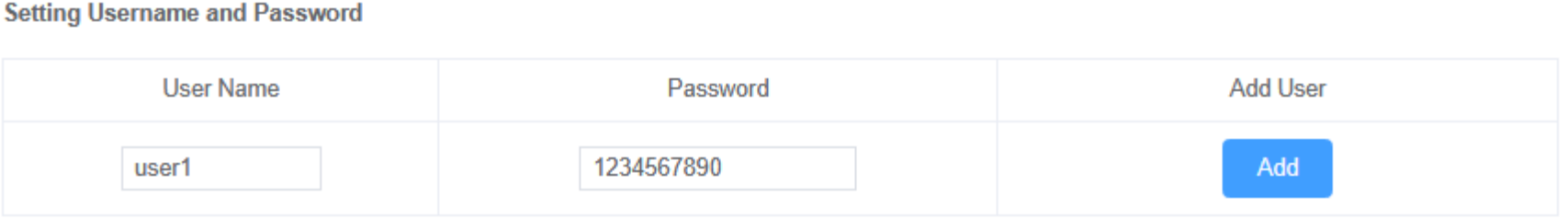
Wireless > Captive Portal

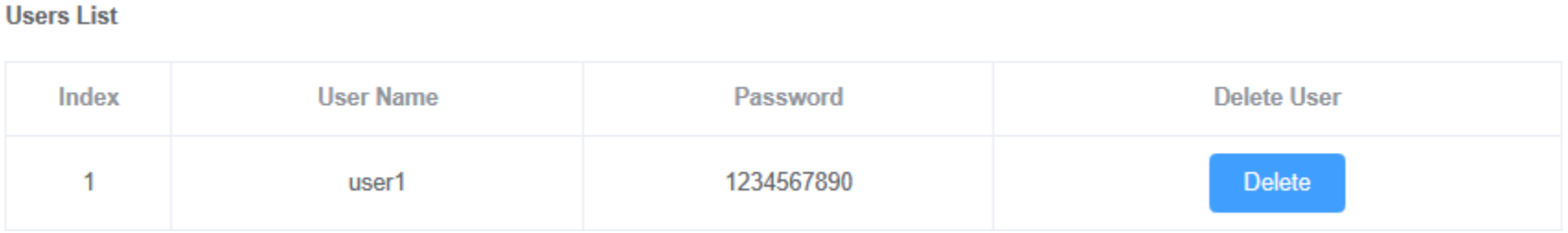
Choose the Portal Mode **Internal Captive Portal**.

a. First, select the login authentication method for connecting your captive portal WiFi network. At the **Login Method** drop-down list, select one of the following.



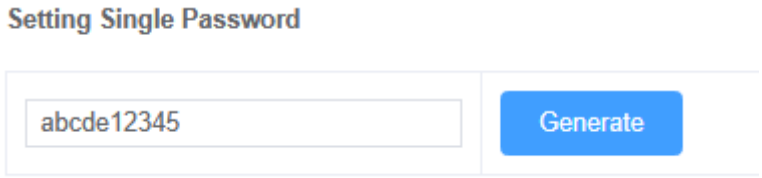
- **User name and password –** Requires users to enter a user name and password for authentication to connect to your captive portal WiFi network which must be defined in the **User List**.





  - To create a new user account, next to **Setting Username and Password**, enter the user name and password for the new user account and click **Add.** Repeat to add more user accounts.

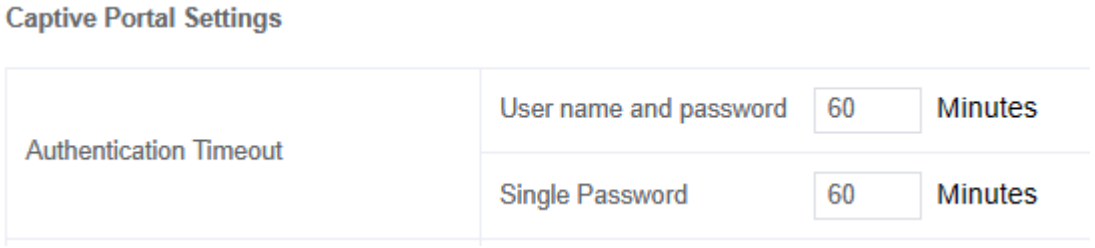
- **Single password** – Requires users to enter a single password to connect your captive portal WiFi network which must be defined in the **Setting Single Password** settings.



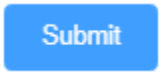
- To specify a single password, next to **Setting Single Password**, enter the new password or click **Generate** to randomly generate a new password.

- **Both** – Users can enter either a user name and password or single password to connect to your captive portal WiFi network. Both prompts will be displayed on the captive portal page and user can select either method to authenticate.

b. Next, specify the **Authentication Timeout** settings. This is the session time period (minutes) which users are allowed to be logged in to your wireless network. Once the time expires, users will automatically logged and will need to log back in through the captive portal page again in order to reconnect to your wireless network. It is recommended to set a value to ensure authentication sessions are closed after a certain time period. Setting the value to 0 minutes allows users to be authenticated and connected to your captive portal WiFi network without any time restrictions.



c. Click **Submit** at the bottom of the page to save the initial captive portal profile.



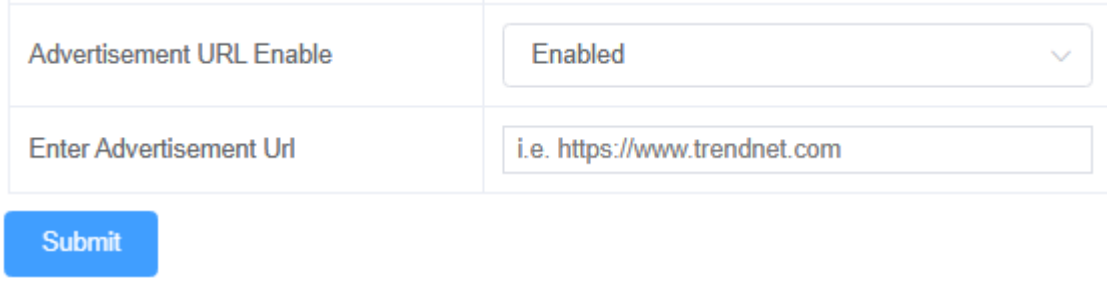
Add a redirect URL/address/website

After your users authenticate and connect to your captive portal WiFi network, you may want to redirect your users to a specific URL, address, or website for advertisement purposes.

In the Captive Portal profile list, for the profile you would like to modify under the Operation column, click the button to modify the profile.

Click the **Advertisement URL Enable** drop-down option and select **Enabled**. Then enter the URL/address/website in the **Enter Advertisement URL** field. Click **Submit** at the bottom of the page to save the settings.

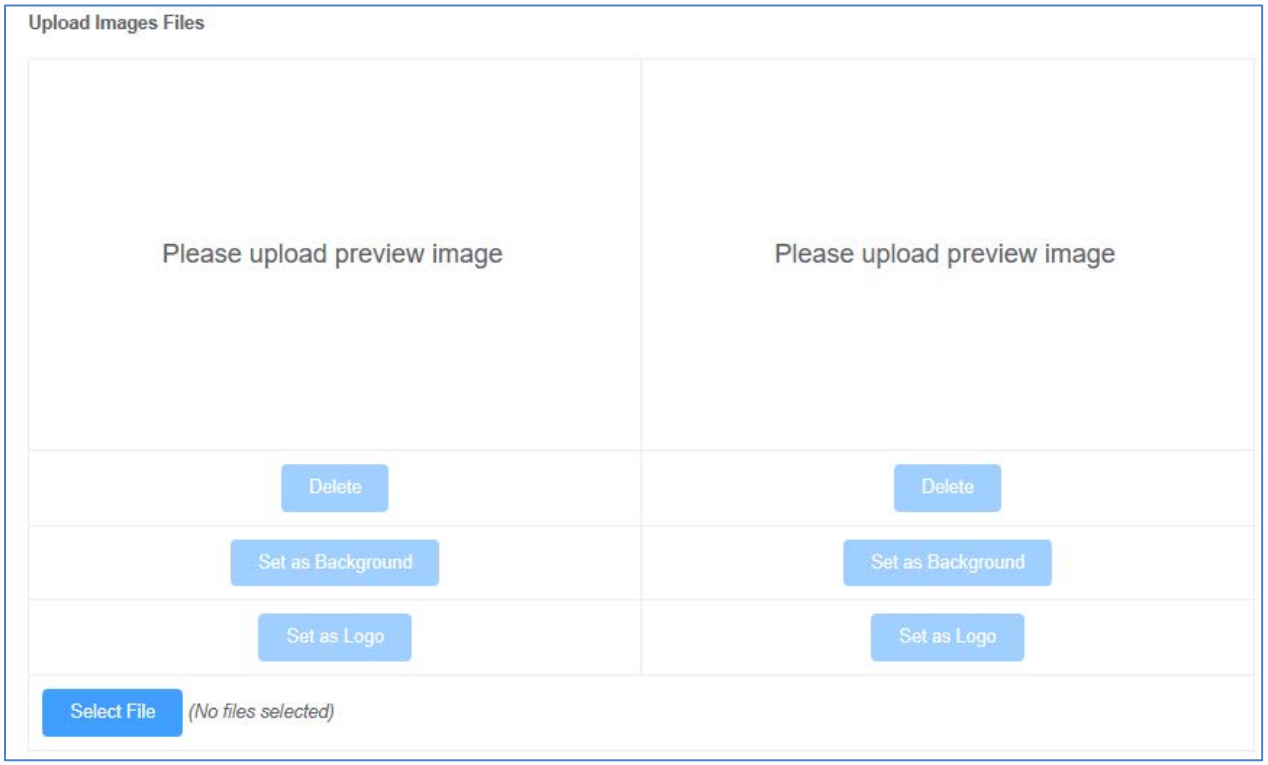
Note: *The prefix http:// or https:// must be included when entering URLs/addresses/websites (ex. https://www.trendnet.com)*



Customize your internal captive portal page
After you have defined the initial parameters, you can apply basic portal page customization.

In the Captive Portal profile list, for the profile you would like to modify under the Operation column, click the button to modify the profile.

Under Upload Image File, click **Select File**, and navigate to the directory where the selected image is located and select the image. Once you have selected the image, click **Upload**.



Once you have uploaded the image, an image preview will appear and you can assign the image **Set as background** or **Set as logo**. If you would like to delete the image and upload a different image, you can also click **Delete** to delete the image.

Note: *Only 2 images can be uploaded for portal page customization (Only one image can be set for the portal page background and another image can be set for the company/organization logo). Images are automatically scaled when uploaded. The recommended image formats are JPG, PNG, GIF. Maximum file size for images is 250KB.*

After you have uploaded your images, you can add a welcome or greeting message to display to your guest users on the captive portal page. A preview of the page and text will also be displayed. After you have finished entering your message, click **Submit**.

Note: *Aside from text, you can enter HTML tags for text formatting and styles.*

Below is an example of a greeting message formatted in html.

*

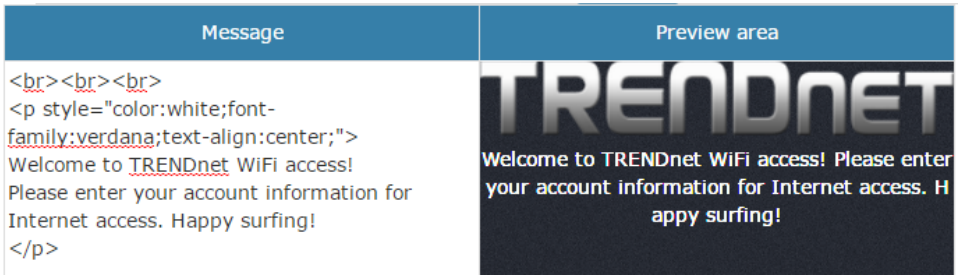
*

* *

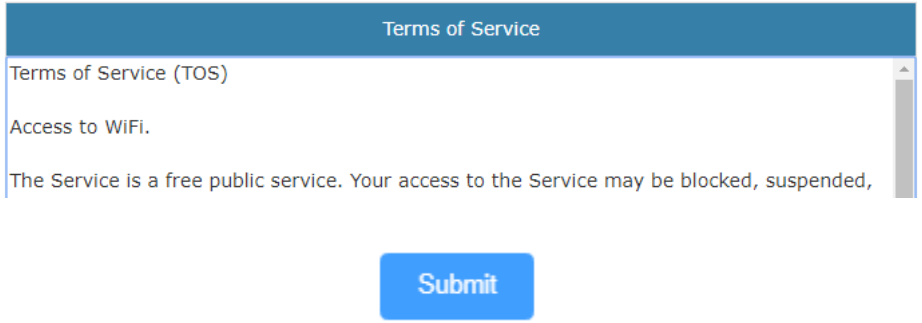
Welcome to TRENDnet WiFi access!

Please enter your account information for Internet access. Happy surfing!

* *



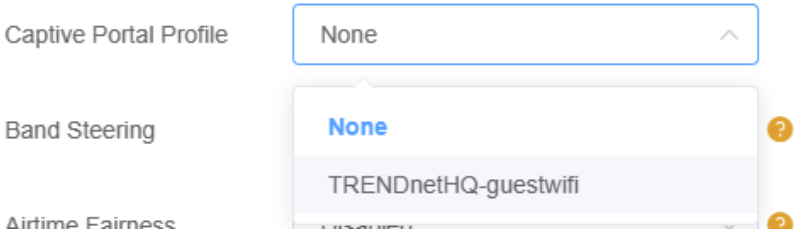
Additionally, you can modify the text displayed to your users for your terms of service. By default, a generic terms of service statement is provided for reference.



To apply the captive portal profile, click on **Wireless** and click on **WiFi Groups.**

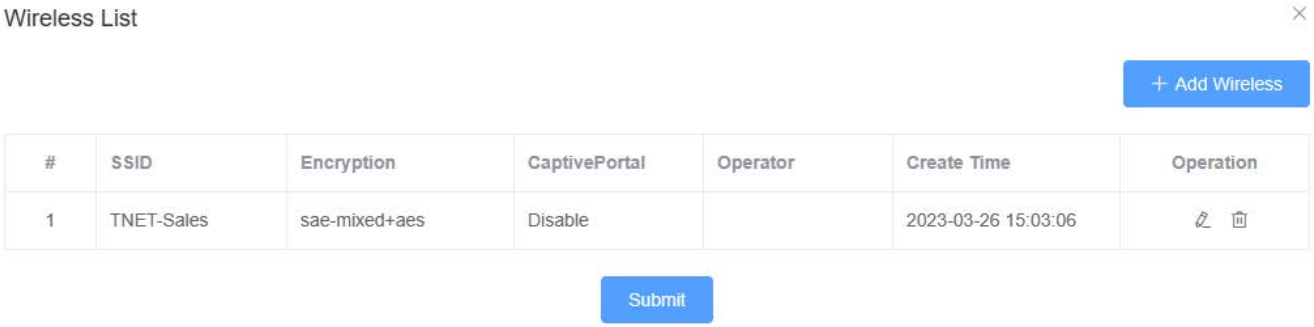
In the WiFi Group list, under **Operation**, click on the button for the WiFi group to apply the captive portal profile.

In the WiFi Group configuration settings, click on the **Captive Portal Profile** drop-down list and select the captive portal profile to apply, then click **Submit** at the bottom of the page.

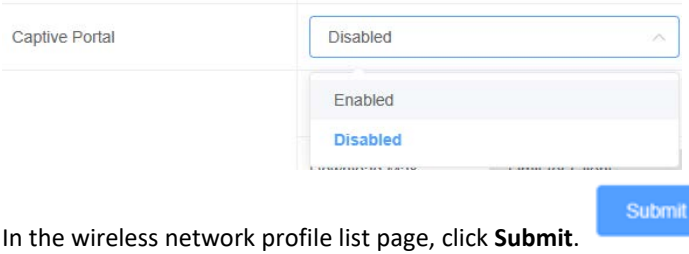


Next, enable captive portal authentication on the wireless network profiles you created on under the wireless group.

In the WiFi Group list, under **Operation**, click the button for the WiFi group to configure the wireless network profiles. Click the to edit the wireless network profile.



In the wireless network profile configuration settings, click the **Captive Portal** drop-down list and select **Enabled**, then click **Save** at the bottom of the page.



In the wireless network profile list page, click **Submit**.

Note: *If there are pending configuration changes that have not yet been applied to wireless access points in the WiFi group, an exclaimation point symbol "!" will be displayed on the Submit button.*

B. Redirect URL

Wireless > Captive Portal

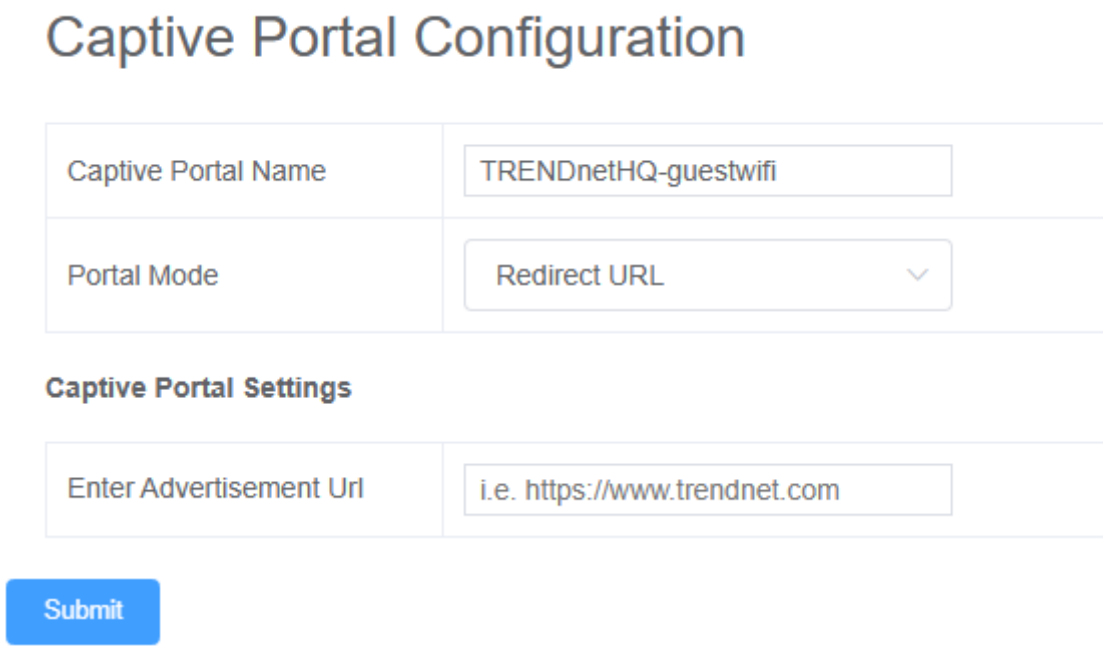
Choose the option **Redirect URL**.

First, enter the authentication timeout value and the advertisement URL and click **Submit** to save the settings.

- **Enter Advertisement URL** – This is the website or URL guest users will be automatically redirected after connecting to your wireless network through your captive portal page.
  Note: *The prefix http:// or https:// must be included when entering URLs/addresses/websites (ex. https://www.trendnet.com)*

Click the **Advertisement URL Enable** drop-down option and select **Enabled**. Then enter the URL/address/website in the **Enter Advertisement URL** field. Click **Submit** at the bottom of the page to save the settings.

Note: *The prefix http:// or https:// must be included when entering URLs/addresses/websites (ex. https://www.trendnet.com)*



After you have defined the initial parameters, you can apply portal page customization.

Under Upload Image File, click **Browse** or **Choose File** depending on your browser, and navigate to the directory where the selected image is located and select the image. Once you have selected the image, click **Upload**.

Once you have uploaded the image, an image preview will appear and you can assign the image **Set as background** or **Set as logo**. If you would like to delete the image and upload a different image, you can also click **Delete** to delete the image.

Note: *Only 2 images can be uploaded for portal page customization (Only one image can be set for the portal page background and another image can be set for the company/organization logo). Images are automatically scaled when uploaded. The recommended image formats are JPEG, PNG, GIF. Maximum file size for images is 250KB.*

After you have uploaded your images, you can add a welcome or greeting message to display to your guest users on the captive portal page. A preview of the page and text will also be displayed. After you have finished entering your message, click **Apply**.

Note: *Aside from text, you can enter HTML tags for text formatting and styles.*

Below is an example of a greeting message formatted in html.

*

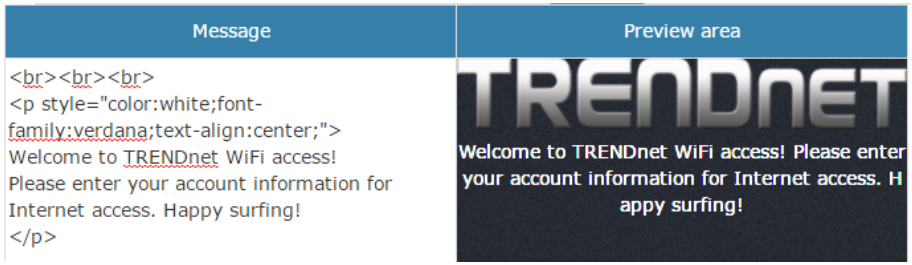
*

* *

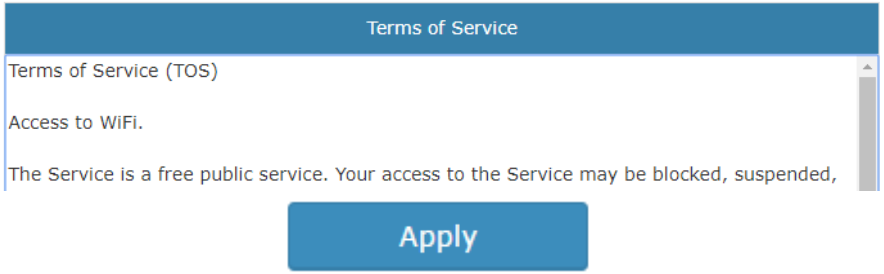
Welcome to TRENDnet WiFi access!

Please enter your account information for Internet access. Happy surfing!

* *



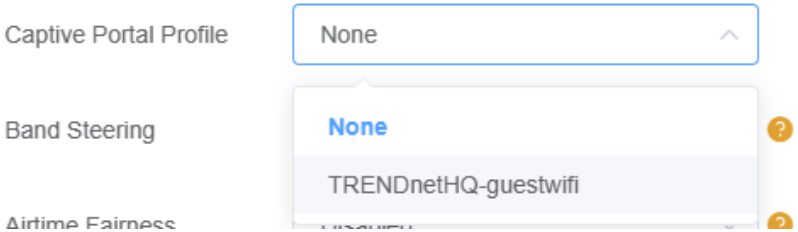
Additionally, you can modify the text displayed to your users for your terms of service. By default, a generic terms of service statement is provided for reference.



To apply the captive portal profile, click on **Wireless** and click on **WiFi Groups.**

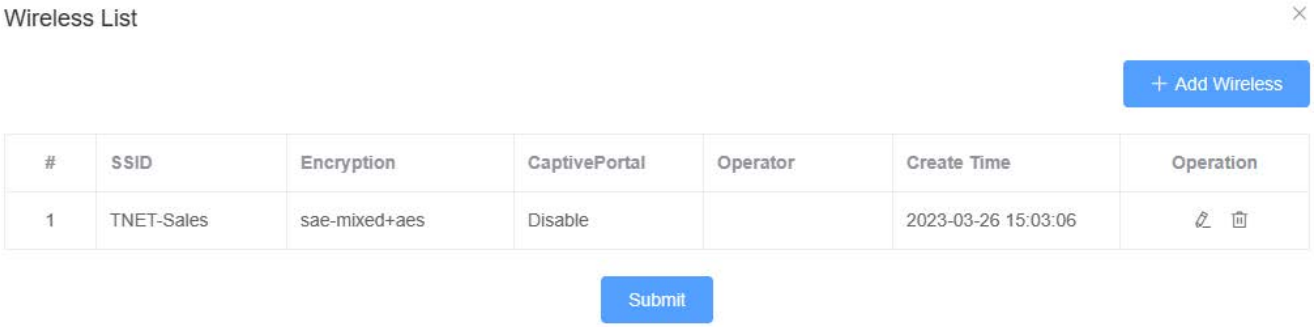
In the WiFi Group list, under **Operation**, click on the button for the WiFi group to apply the captive portal profile.

In the WiFi Group configuration settings, click on the **Captive Portal Profile** drop-down list and select the captive portal profile to apply, then click **Submit** at the bottom of the page.

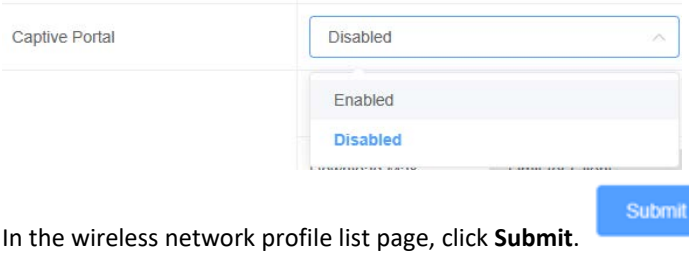


Next, enable captive portal authentication on the wireless network profiles you created on under the wireless group.

In the WiFi Group list, under **Operation**, click the button for the WiFi group to configure the wireless network profiles. Click the to edit the wireless network profile.



In the wireless network profile configuration settings, click the **Captive Portal** drop-down list and select **Enabled**, then click **Save** at the bottom of the page.



In the wireless network profile list page, click **Submit**.

Note: *If there are pending configuration changes that have not yet been applied to wireless access points in the WiFi group, an exclaimation point symbol "!" will be displayed on the Submit button.*

C. Captive Portal with RADIUS (CoovaChilli)

Wireless > Captive Portal

Choose the option **Captive Portal with RADIUS**.

Note: *Since the option requires the use of an external RADIUS/CoovaChilli server for authentication, please make sure it is set up, configured and available on your network accessible by your controller and APs.*

Enter the CoovaChilli server settings. Click **OK.**

- **Primary RADIUS Server** – Enter the IP address of the external CoovaChilli authentication server.

D. **Secondary RADIUS Server** – If you have secondary or backup CoovaChilli authentication server, enter the IP address.

E. **RADIUS Auth Port** – Enter the port number used by the Coovachilli server for authenticating RADIUS requests. The default port number used for RADIUS authentication is 1812.

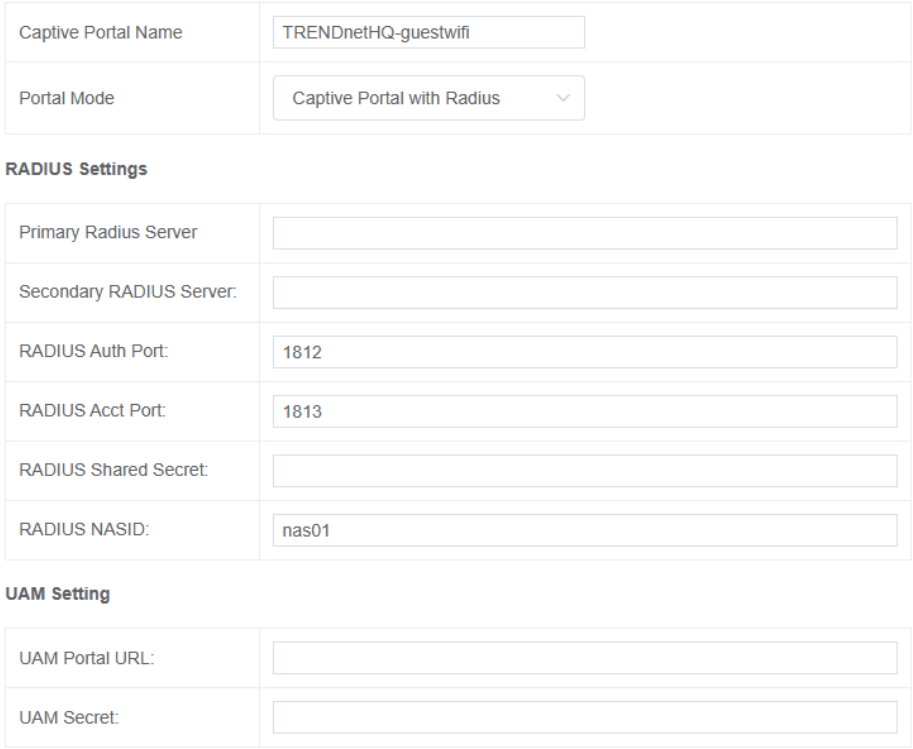
F. **RADIUS Acct Port** – Enter the port number used by the Coovachilli server for accounting on the server. The default port number for RAIDUS accounting is 1813.

G. **RADIUS Shared Secret** – Enter the shared secret used to allow the CoovaChilli server to allow the access point to authentication RADIUS authentication requests.

H. **RADIUS NAS ID**: Enter the NAS ID required by the CoovaChilli server to allow the access point to authentication RADIUS authentication requests.

I. **UAM Portal URL** – Enter the UAM portal web URL address of the login authentication page provided by the CoovaChilli server.

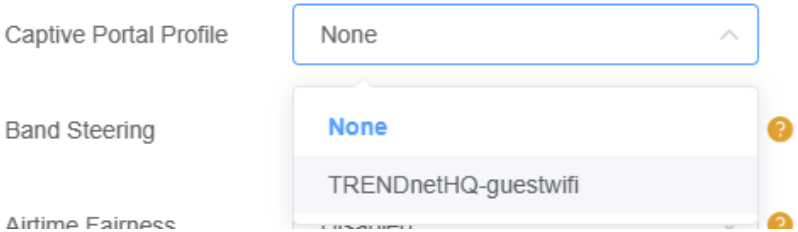
J. **UAM Secret** – Enter the UAM secret required to allow access to this portal page.



To apply the captive portal profile, click on **Wireless** and click on **WiFi Groups.**

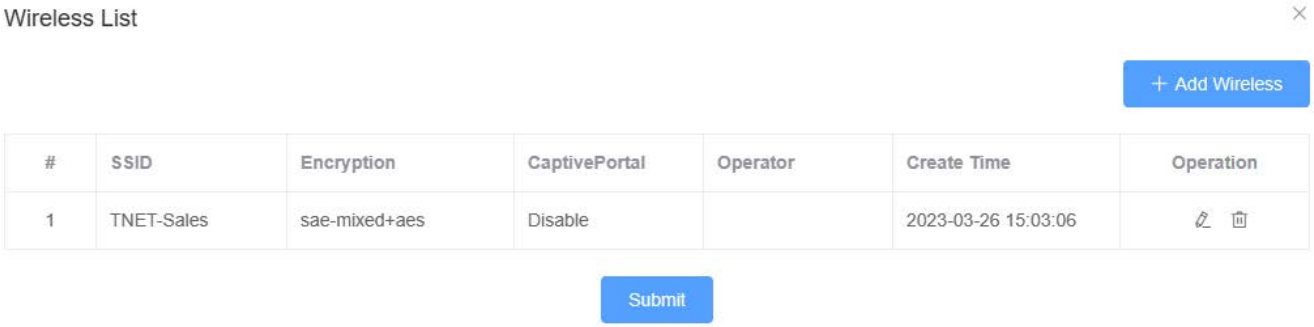
In the WiFi Group list, under **Operation**, click on the button for the WiFi group to apply the captive portal profile.

In the WiFi Group configuration settings, click on the **Captive Portal Profile** drop-down list and select the captive portal profile to apply, then click **Submit** at the bottom of the page.

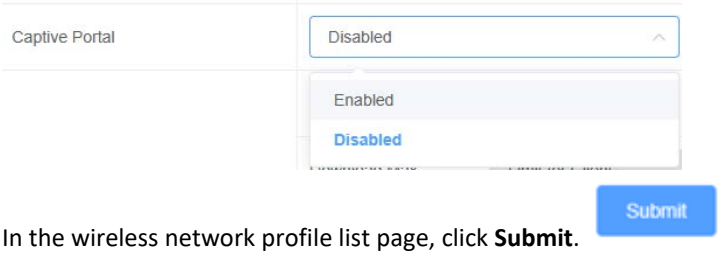


Next, enable captive portal authentication on the wireless network profiles you created on under the wireless group.

In the WiFi Group list, under **Operation**, click the button for the WiFi group to configure the wireless network profiles. Click the to edit the wireless network profile.



In the wireless network profile configuration settings, click the **Captive Portal** drop-down list and select **Enabled**, then click **Save** at the bottom of the page.



In the wireless network profile list page, click **Submit**.

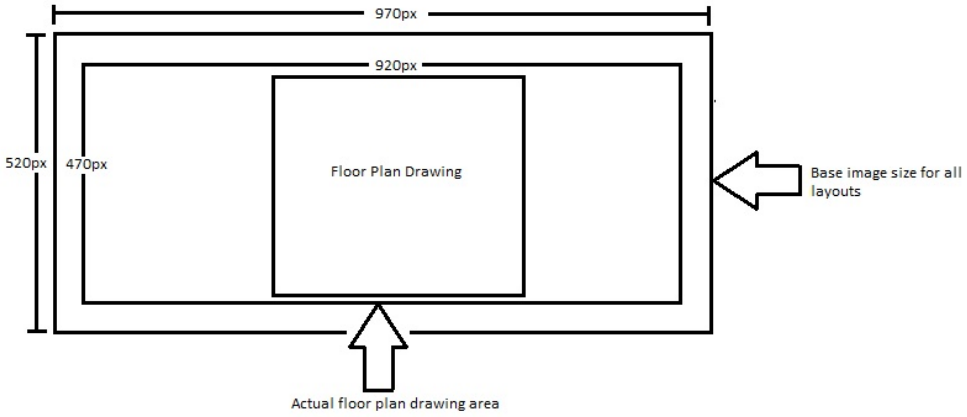
Note: *If there are pending configuration changes that have not yet been applied to wireless access points in the WiFi group, an exclaimation point symbol "!" will be displayed on the Submit button.*

WAP Maps™

The WAP (wireless access point) maps feature allows you to upload a floor plan (JPEG or PNG) to the wireless controller and place your APs on your floor plan for AP location planning and reference.

Note: *For optimal viewing, it is recommended to use a base image size of 970px x 520px (max.) for all uploaded floor plans and the actual layout drawings within 920 x 470px (max.) and the file cannot exceed 2MB in file size.*

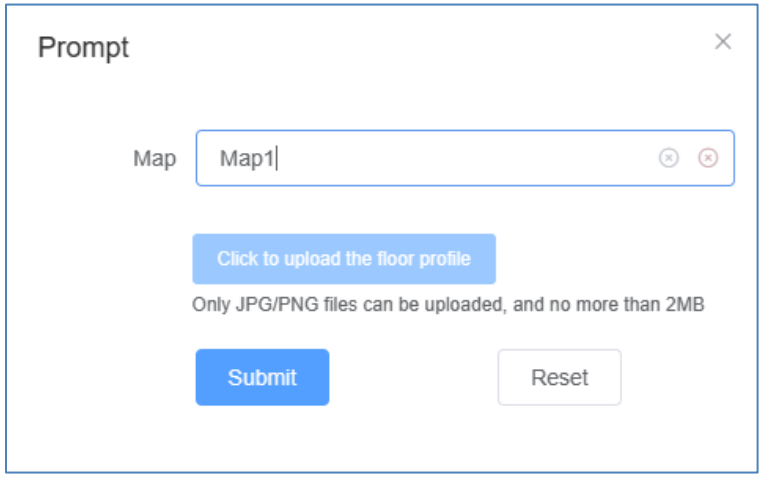
Floor plan image size reference



Upload floor plans

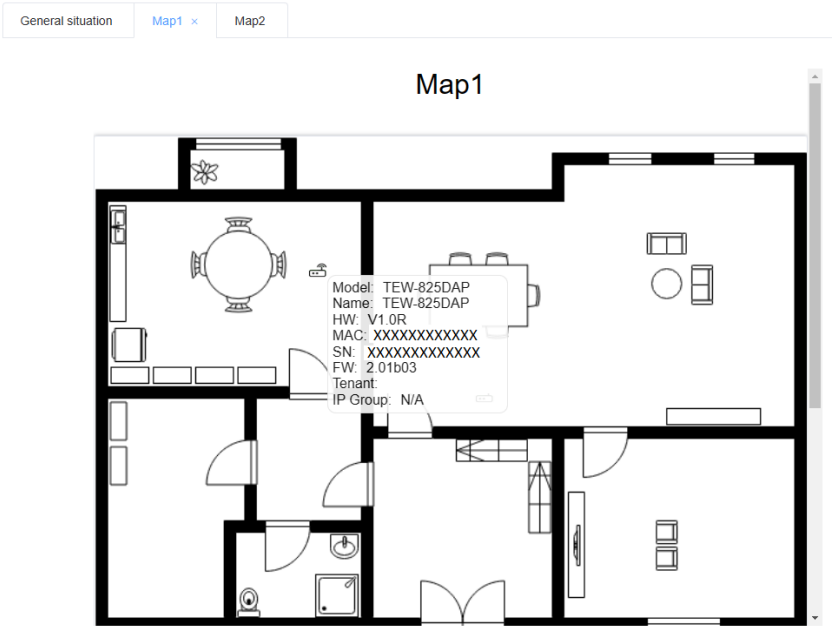
Wireless > WAP Maps™

1. Click on **Wireless** and click **WAP Maps™.**
2. The list of available wireless devices will be displayed on the left side.
3. The **General Situation** tab will display general information about which wireless devices are assigned to which map (by Alias) after wireless devices have been placed on the map.
4. To upload a new map image, click the ⊞ button at the top right.
5. At the prompt, enter a descriptive name for the map, click **Click to upload the floor profile** and select the map image file that meets the format and size requirements, then click **Submit** to upload the map image.



6. Once the floor plan is uploaded, you can drag and drop the available APs located on the left side to the area where the APs will be located on your floor plan.

Note: *Access points will flash in green on the floor plan.*

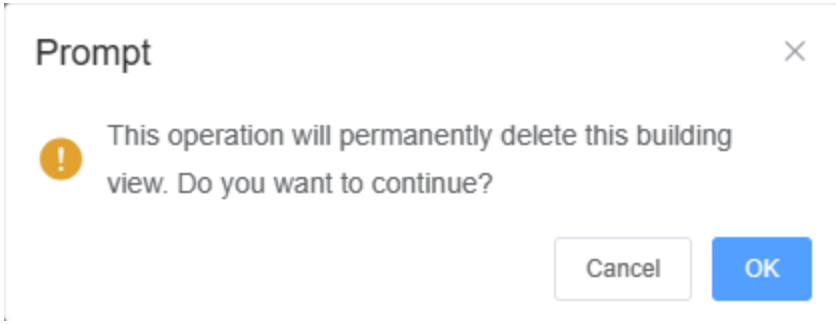


Removing wireless access points and deleting floor plans

To remove wireless access points from floor plans, click and drag the access point back into the list of wireless devices on the left side.

To delete a map, click the X button in the tab section of the floor plan you would like to delete.

At the prompt to delete the floor plan, click **OK**.



View client connections and blacklist clients

Wireless > Client Info

This section allows you to monitor all of the currently connected client devices. Additionally, the client blacklist feature allows you to permanently block specific client devices that are currently connected to your wireless network or manually disconnect clients from your wireless network. The client blacklist prevents/restricts any specified client devices from accessing your wireless network in the future unless they are removed from the blacklist.

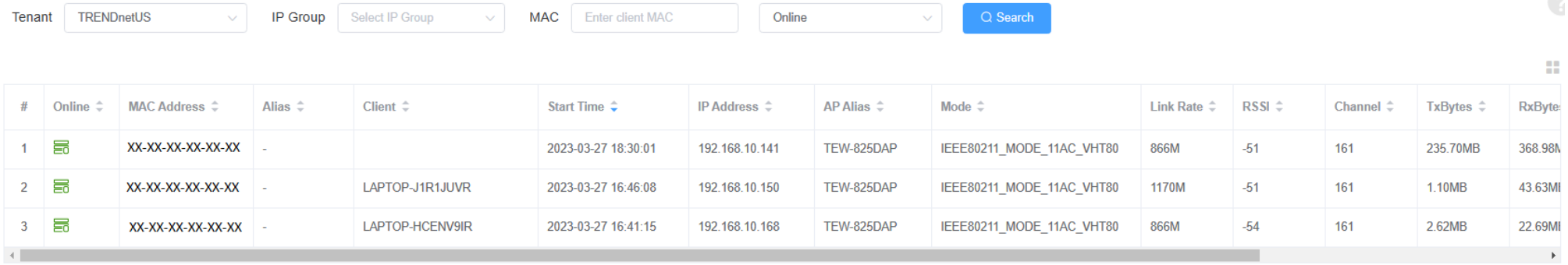
1. Click on **Wireless** and click **Client Info.**

2. In the Client List, the currently connected client devices will be listed along with some additional information.

- **Online:** Indicates if the wireless client is currently connected (online) or offline.
- **MAC Address:** Displays the MAC address of the wireless client.
- **Alias:** Displays the Alias of the wireless. To manually enter an wireless client, double click the Alias field and enter a name for the client.

- **Client:** If discovered, displays the network host name of the client device. The wireless access point may not be able to discover your device(s) host name.
- **Start Time:** Displays the time and date the client device connected to your wireless network.
- **IP Address:** Displays the IP address assigned to the client device.
- **AP Alias:** Displays AP device by Alias that the client is currently connected. The device alias must be modified under Device > Device List.
- **Mode:** Displays the current wireless mode (802.11a/b/g/n/ac/ax + channel width) the client device is currently using to connect to your wireless network.
- **Link Rate:** Displays the current link rate in Mbps (noted by "M") the client device is connected. (ex: 866M is 866Mbps)
- **RSSI:** Displays the client device current signal strength connected to your network from the device's current physical location to the wireless access point.
- **RSSI Threshold:** Enable this option set a signal strength limit on wireless client devices when the AP will force the client to disconnect.
  (Lower negative number indicates a higher signal strength. Ex: -30 RSSI is a higher strength value compared to a value of -90 RSSI)
- **Channel:** Displays the current wireless channel the client device is using to connect to your wireless network.
- **TxBytes:** Displays a snapshot of the total amount of data transmitted or uploaded by the client device.
- **RxBytes:** Displays a snapshot of the total amount of data received or downloaded by the client device.
- **Link Type:** Displays the link type of the client device, wired or wireless.
- **Startup Time:** Displays the total amount of time the client device has been connected to your wireless network.
- **Operation**

- **Blacklist** – Clicking this option will add the client device to the Client Blacklist. To view the client blacklist, click on Wireless > Client Blacklist. Clients that are added to the client blacklist will be permanently blocked from any APs managed by the wireless controller until they are removed the client blacklist.
- **Kick** – Clicking this option will force the AP to immediately disconnect the client device from the wireless network.



Provision devices in your Hive account

Devices in Hive can be provisioned through configuration and firmware upgrades.

Configuration Provisioning

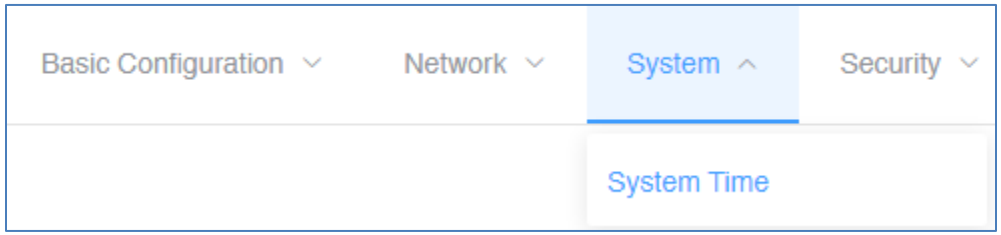
- To provision device configuration, configuration files must first be created in the Hive Management System. Batch configuration provisioning tasks can only be deployed for single TRENDnet device model. (Example: Multiple TRENDnet TEG-082WS or multiple TPE-082WS switches but not both models for a single provisioning task.)

To create a new configuration file, in the left navigation menu, click on **Configuration** and click on **Create**.

In the top left, click the drop-down list to select the type of device to create a new configuration file and click **Add**.

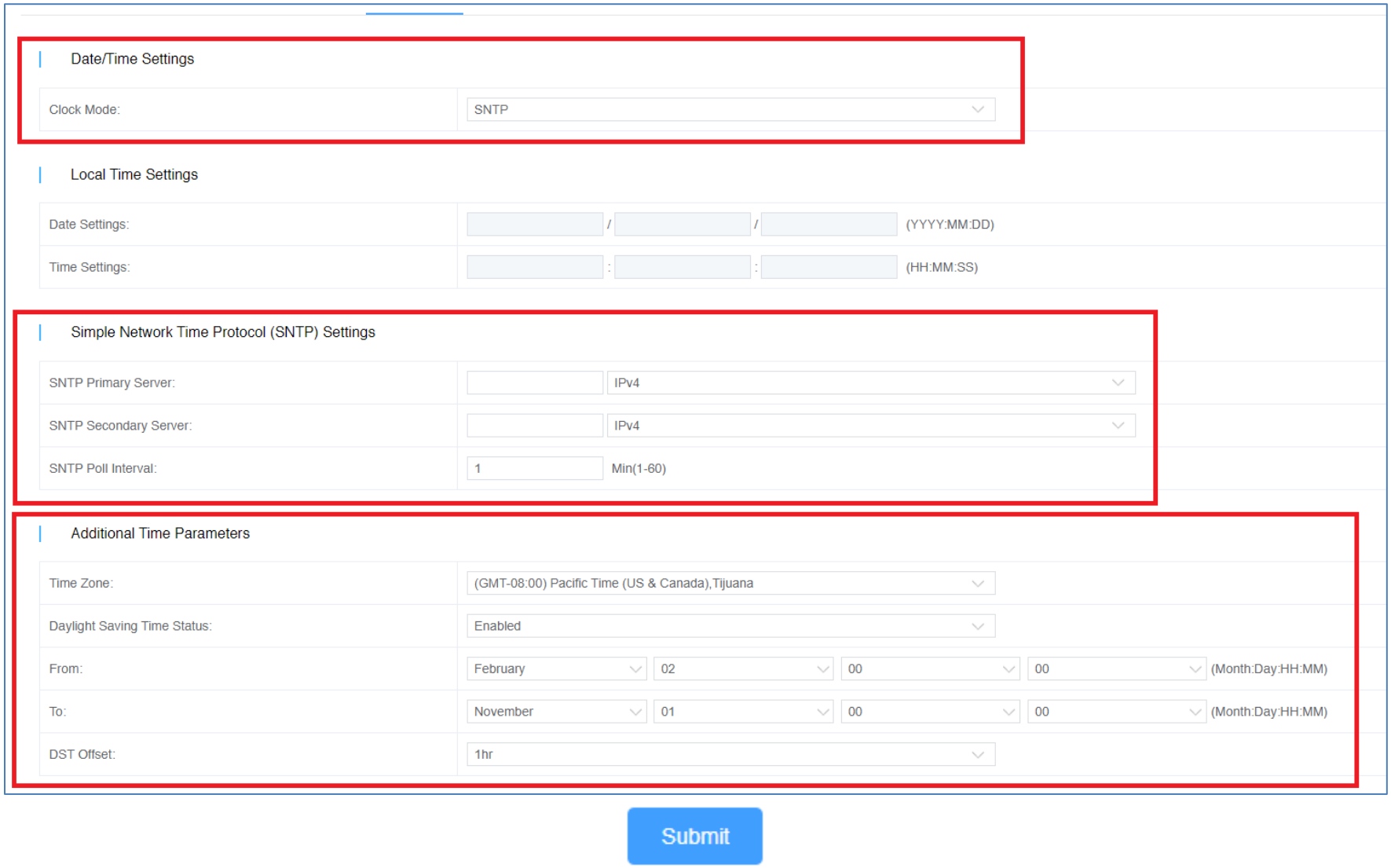
In the example below, we will create a new configuration file for the TEG-082WS.

For the new configuration file, first configure the SNTP/Time Settings under **System > System Time**.



If configuring SNTP, under **Date/Time Settings**, click the **Clock Mode** drop-down list and select **SNTP.**

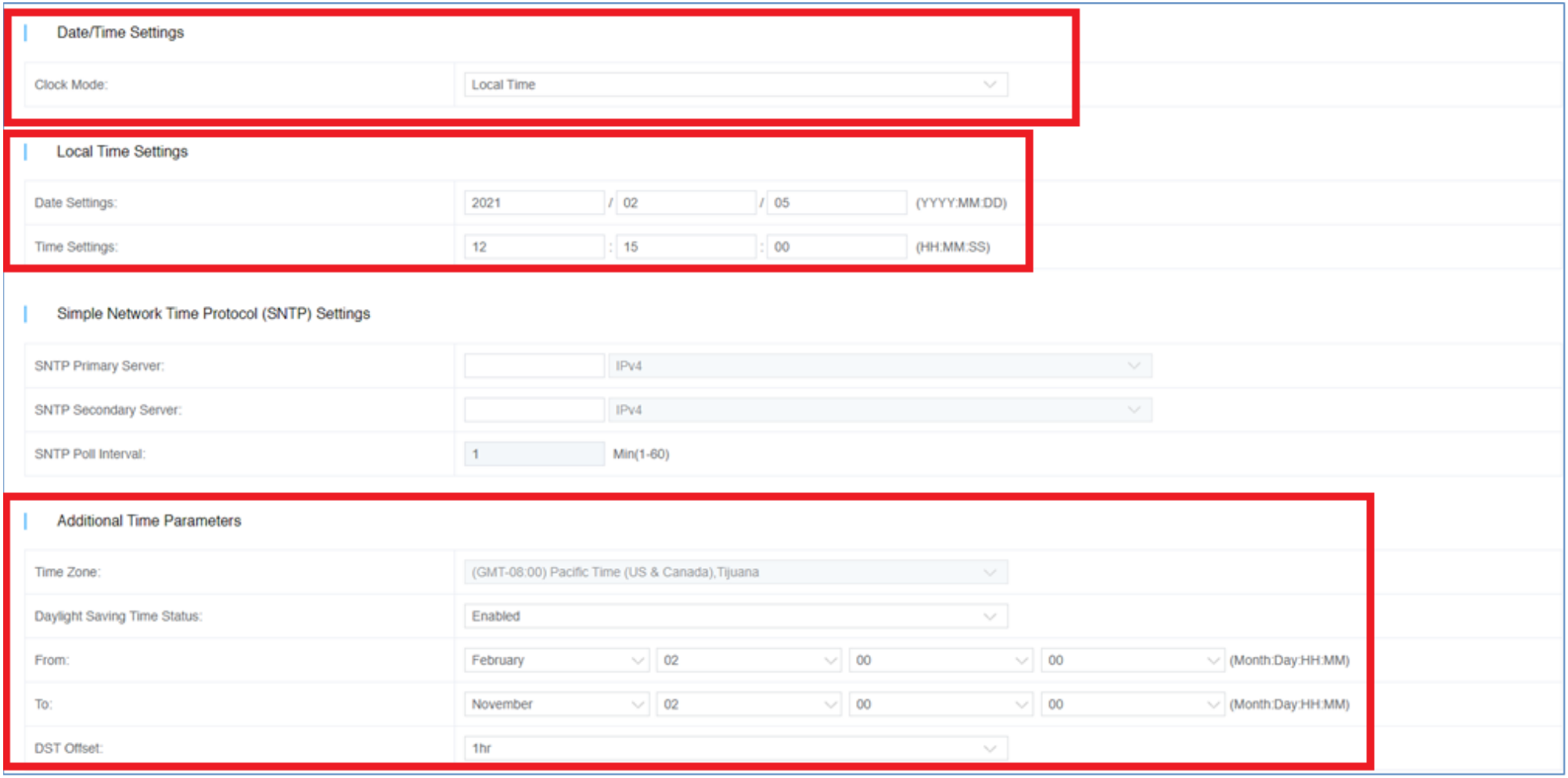
In the **Simple Network Time Protocol (SNTP) Settings**, enter the **SNTP Primary Server, SNTP Secondary Server** as an IPv4 address, IPv6 address, or Domain Name and in top right. In the **Additional Time Parameters** section, click the **Time Zone** drop-down list and select the correct Time Zone and enable and configure your daylight savings time, if any, then click **Submit**.



If configuring Local Time Settings, under **Date/Time Settings**, click the **Clock Mode** drop-down list and select **Local Time.**

In the **Local Time Settings**, enter the **Date Settings** and **Time Settings.** click **Submit**.

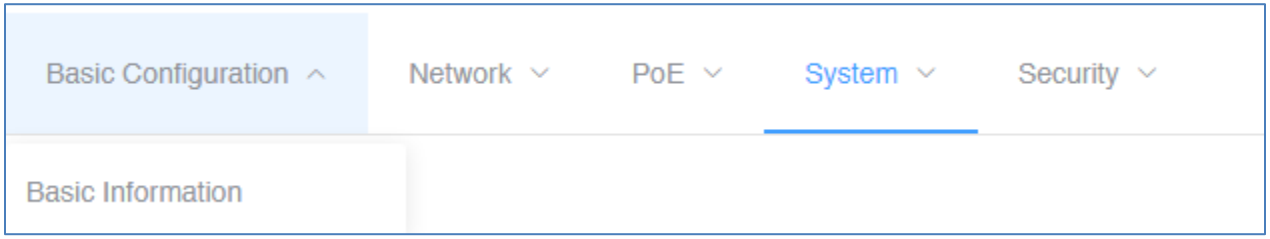
In the **Additional Time Parameters** section, click the **Time Zone** drop-down list and select the correct Time Zone and enable and configure your daylight savings time, if any, then click **Submit**.



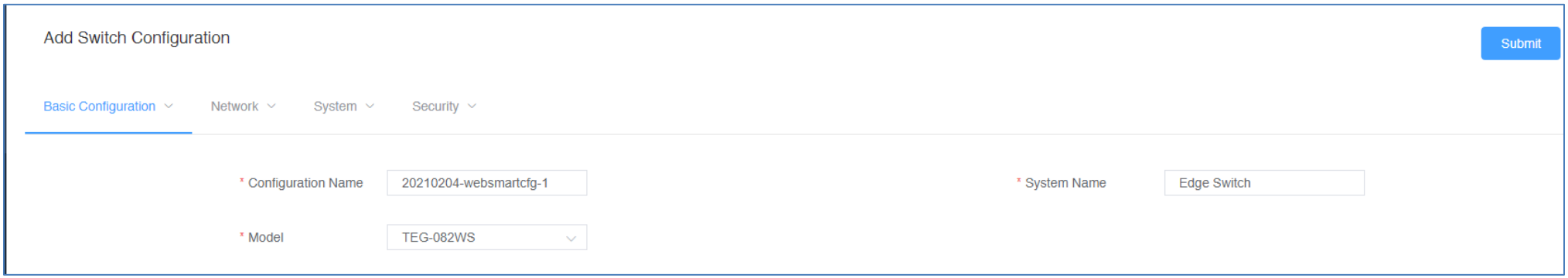
After you have configured and saved the time and date settings for the configuration file, you can more configuration changes to the configuration file.

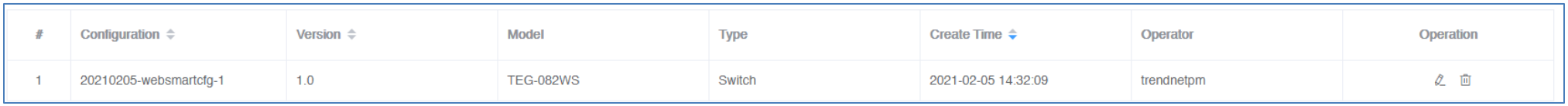
After applying all configuration changes for the new configuration file, in the **Basic Configuration** tab, select **Basic Information.**

Note: *For each configuration change, please make sure to click* ***Submit*** *in the top right after configuration settings have been modified.*



Enter a **Configuration Name**, a **System Name**, and click the **Model** drop-down list to select the TRENDnet device model. In the top right, click **Submit** to save the new configuration file..



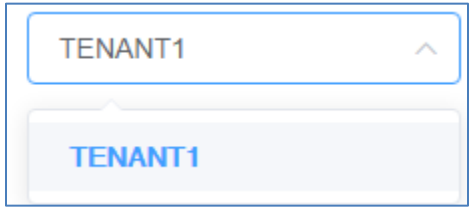


#	Configuration	Version	Model	Type	Create Time	Operator	Operation
1	20210205-websmartcfg-1	1.0	TEG-082WS	Switch	2021-02-05 14:32:09	trendnetpm	

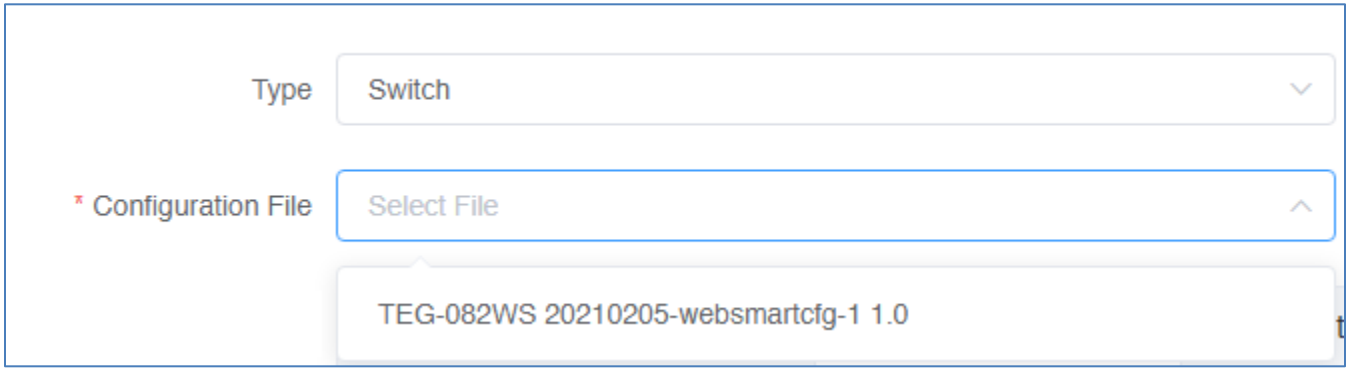
Clicking the edit button will allow you to modify the configuration file.

Clicking the delete button will delete the configuration file.

To provision devices with a new configuration file, click on **Configuration** and click on **Provision**.
In the top left drop-down list, select the tenant.

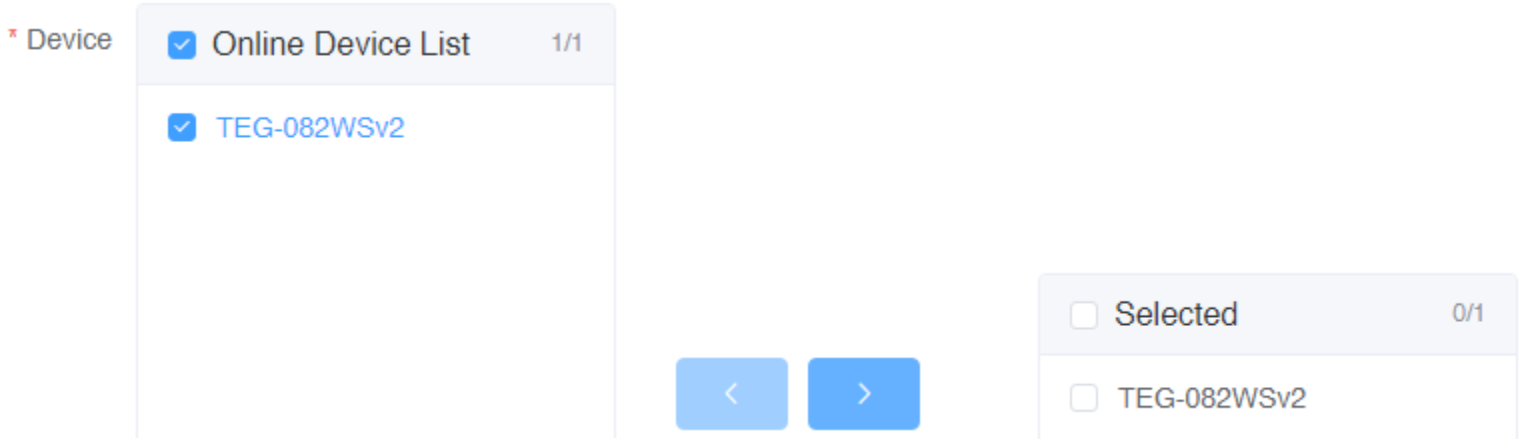


Click the **Type** drop-down list and select the device type. The click the **Configuration File** drop-down list to select the configuration file.



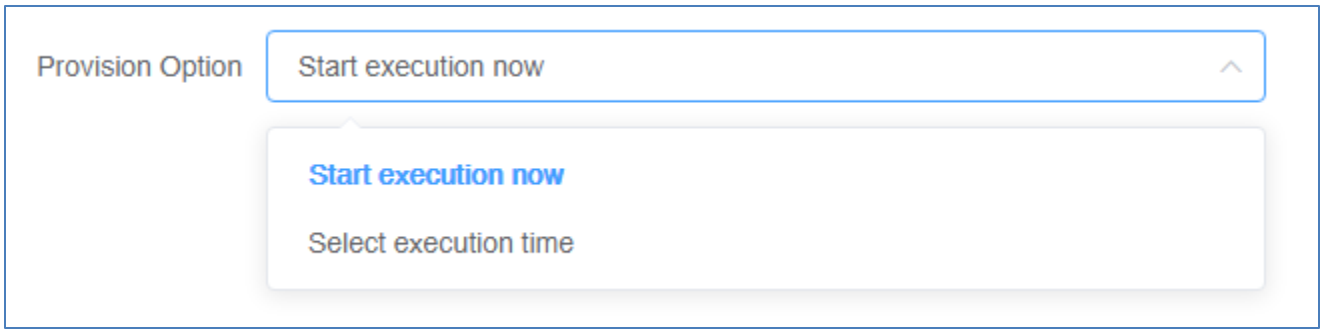
After the configuration file is selected, the applicable online devices for the selected configuration file will appear in the **Device/Online Device List**.

Check the devices you would like to provision, and click  to move the devices to the selected list.

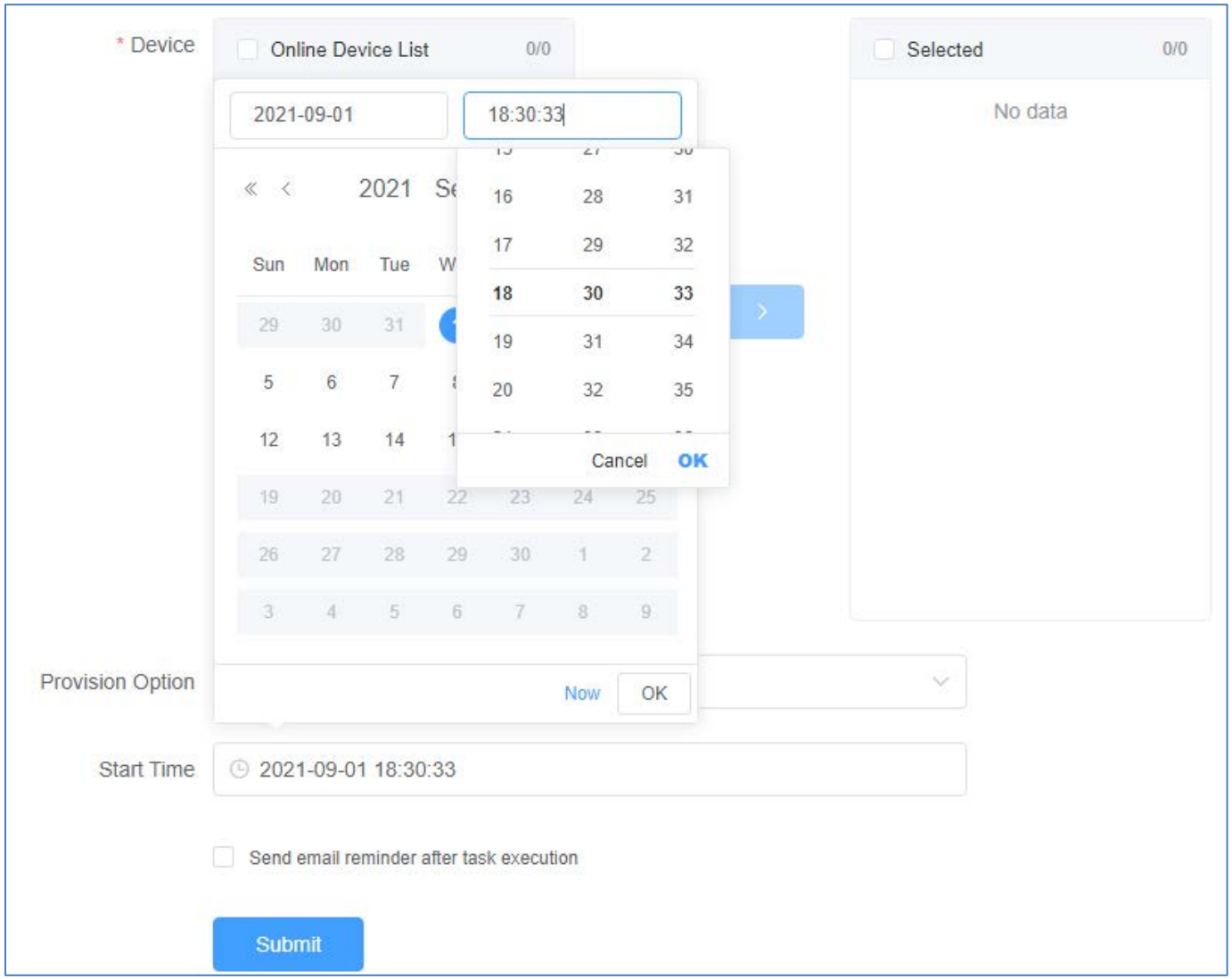


Click the **Provision Option** drop-down list to select when to provision selected devices with the configuration file. After you have selected this desired option, click **Submit.**

- **Start execution now –** Selecting this option will execute the task immediately.



- **Select execution time –** Selecting this option will allow you to schedule a future date and time when to execute this task. Configure the date and time schedule when to execute this task and click **OK**.
  Note: *If scheduling this task, checking the option to Send email reminder after task execution will send an email notification.*



After creating a scheduled configuration task, the task will be listed under **Configuration** > **Schedule** from the left navigation menu.

#	Configuration	Operator	Version	Create Time	Execution Time	Task Status	Operation
1	20210205-websmartcfg-1	XXXXXXXX	1.0	2021-02-05 14:49:58	2021-02-05 15:00:00	Waiting	

- **Configuration** – Displays the configuration file name.
- **Operator** – Displays the user that created the task.
- **Version -** Displays the configuration file version.
  Note: *If the original configuration file is modified under Configuration > Create section, a new version of the configuration file is created and the system will automatically update the version number. (Example: 1.0, 2.0, 3.0, etc)*
- **Create Time –** Displays the date and time the scheduled task was created.
- **Execution Time** - Displays the date and time the task is scheduled to be executed.
- **Task Status** – Displays the current task status.
  - **Waiting –** Indicates that the scheduled task is pending to be carried out until the scheduled/Execution time is reached.
  - **Execution –** Indicates that the scheduled task has already been completed.
- **Operation**

  See task detail.

  Cancel the task.

  After a task is cancelled before the schedule date and time, you can restore or restart the task.

  After tasks are executed, click this button to view more detail.

After configuration tasks have been executed, you can check the status details under **Configuration > Record** and in the **Details** column, click to view more information.

Status List

#	Alias	MAC	Update Time	Status
1	TEG-082WSv2	XX-XX-XX-XX-XX-XX	2021-02-05 17:30:19	Configuration Upgrade Success

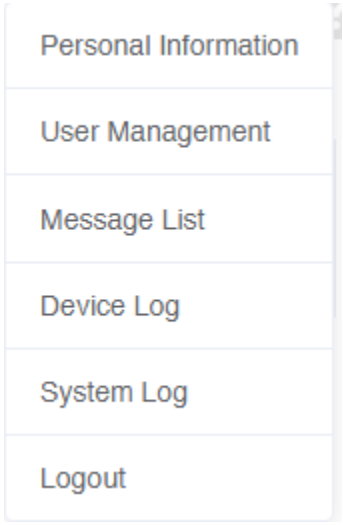
Firmware Provisioning

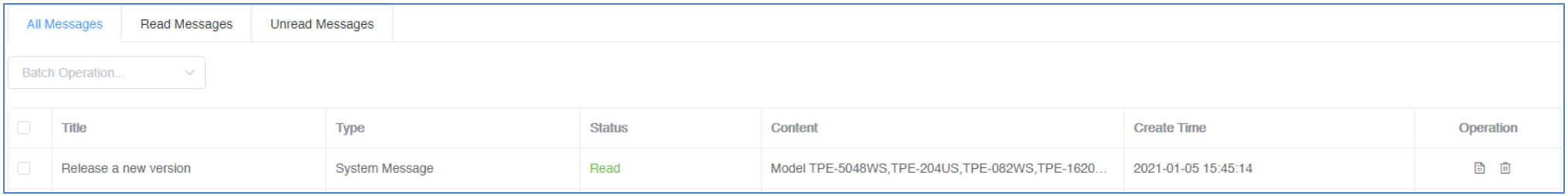
- Standard device firmware will be released by TRENDnet periodically and be available within the Hive Management System for provisioning and can be found under the **Firmware > Information** section from the left navigation menu. You can check the current firmware version of devices under **Devices > Devices List**.

Note: *Only Hive compatible device firmware releases will be available on the Hive Management System. For previous firmware releases, please download from our website https://trendnet.com/support*

- A system message will be sent out to your Hive account when a new firmware is released. An indicator will appear in the top right menu above the Account/Logging button.

Mouse over the Account/Logging button to view the sub menu and click Message List to view system messages.





To view the available device firmware releases, in the left navigation click on **Firmware** and click on **Information.**

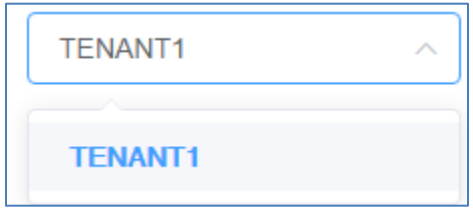
#	Model	Operator	FW Version	Check Sum	MD5	Create Time
1	TPE-5048WS , TPE-204US , TPE-082WS , TPE-1620W...	xxxxxxxxxx	3.01.007	582B7577	00a43e727de27280c8367f2f...	2021-01-05 15:45:14

Total 1 10/page 1 Go to 1

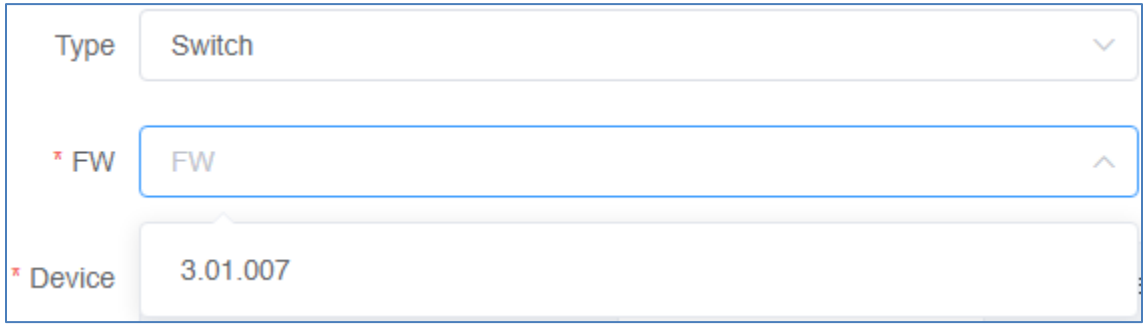
- **Model –** Displays the device model(s) the firmware release applies.
- **Operator –** Displays the user account that created the firmware release.
- **FW Version –** Displays the firmware version number.
- **Check Sum –** Displays the firmware file checksum.
- **MD5 –** Displays the firmware file MD5 checksum.
- **Create Time –** Displays the date and time the firmware release was created.

To provision devices with a new firmware image file, click on **Firmware** and click on **Provision**.

In the top left drop-down list, select the tenant.

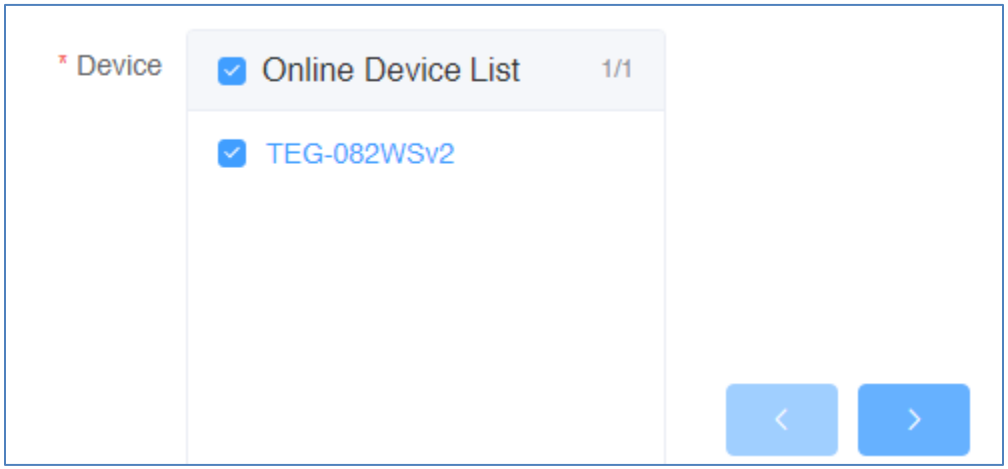


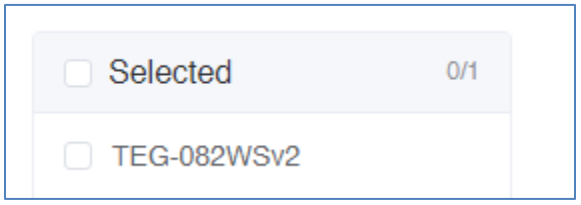
Click the **Type** drop-down list and select the device type. The click the **FW** drop-down list to select the firmware image file.



After you have selected the Type and FW (firmware image file), the applicable online devices for the selected firmware file will appear in the **Device/Online Device List.**

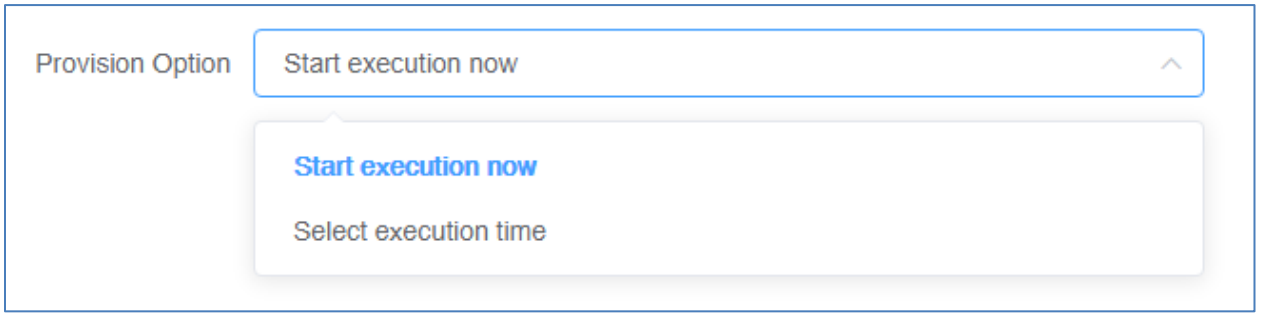
Check the devices you would like to provision, and click  to move the devices to the selected list.



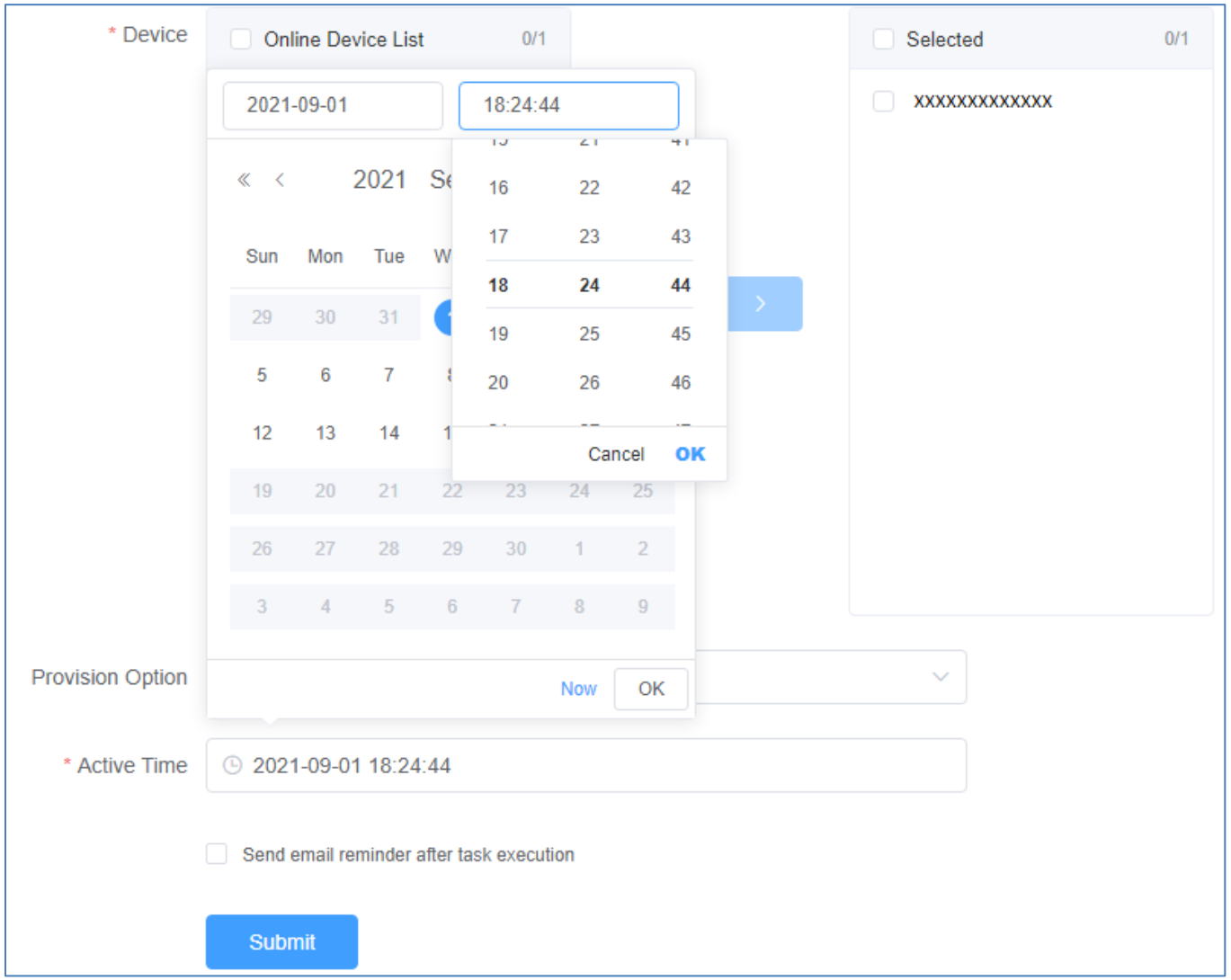


Click the **Provision Option** drop-down list to select when to provision selected devices with the firmware image file. After you have selected this desired option, click **Submit.**

- **Start execution now –** Selecting this option will execute the task immediately.



- **Select execution time –** Selecting this option will allow you to schedule a future date and time when to execute this task. Configure the date and time schedule when to execute this task and click **OK**.
  Note: *If scheduling this task, checking the option to Send email reminder after task execution will send an email notification.*



After creating a scheduled configuration task, the task will be listed under **Firmware** > **Schedule** from the left navigation menu.

#	FW Version	Operator	Create Time	Execution Time	Task Status	Operation
1	3.01.007	XXXXXXXXXXXXXX	2021-02-08 16:04:59	2021-02-08 16:07:00	Waiting	

- **FW Version** – Displays the firmware version number that will be used to provision devices.
- **Operator** – Displays the user that created the task.
- **Create Time –** Displays the date and time the scheduled task was created.
- **Execution Time** - Displays the date and time the task is scheduled to be executed.
- **Task Status** – Displays the current task status.
  - **Waiting –** Indicates that the scheduled task is pending to be carried out until the scheduled/Execution time is reached.
  - **Execution –** Indicates that the scheduled task has already been completed.
- **Operation**

  See task detail.

  Cancel the task.

  After a task is cancelled before the schedule date and time, you can restore or restart the task.

  After tasks are executed, click this button to view more detail.

After firmware tasks have been executed, you can check the status details under **Firmware > Record** and in the **Details** column, click to view more information.

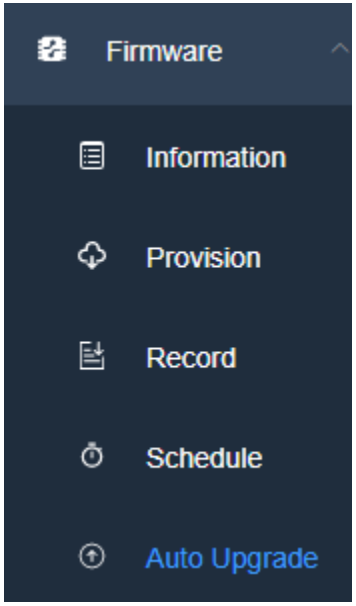
Status List

#	Model	Alias	MAC	Update Time	Status
1	TEG-082WS	TEG-082WSv2	XX-XX-XX-XX-XX-XX	2021-02-08 16:10:36	Upgrade Success

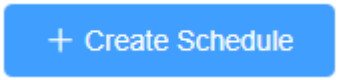
- Firmware Auto Upgrade

Firmware upgrades can be completed automatically by schedule and frequency through the Auto Upgrade function.

To configure firmware auto upgrade, in the left navigation menu, click **Firmware** and click **Auto Upgrade.**

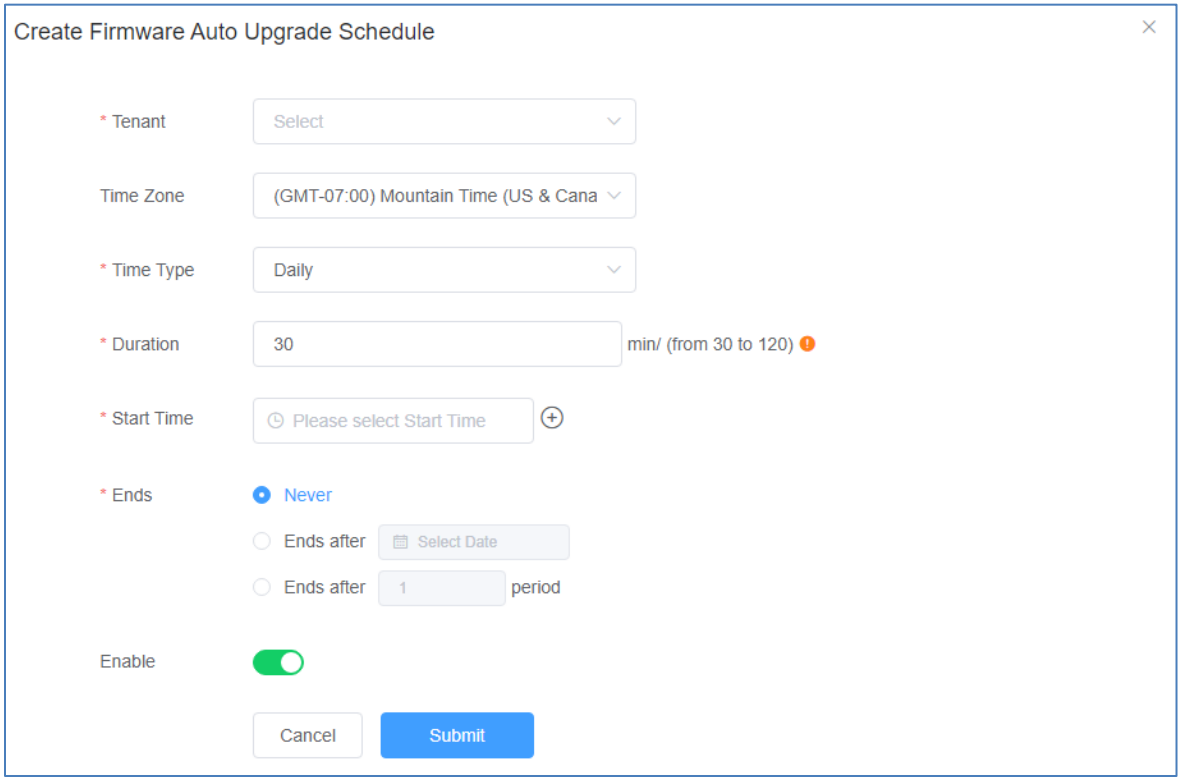


At the top of the page, click **Create Schedule.**



Review the settings below to configuration the automatic upgrade schedule. After you have completed the configuration, click **Submit**.

- **Tenant –** Click the drop-down list and select the tenant to apply the firmware auto upgrade schedule.
- **Time Zone –** Click the drop-down list and select the Time Zone.
- **Time Type –** Select the frequency of the automatic firmware upgrade, daily, weekly, or monthly and select the day or date accordingly.
- **Duration –** This is maximum allowable time for automatic firmware upgrades to complete including device reboot to consider down time. More devices may require more time. Default time is set to minimum of 30 minutes. It is recommended to increase the time if there several devices assigned to the tenant. Edge devices will upgraded first such as WiFi access points, then distribution devices such as switches, and final core devices such as routers or gateways will be upgraded last.
- **Start Time –** Click the field to set the time the automatic upgrade will start daily, selected day or date.
- **Ends**
  - **Never –** The automatic upgrade schedule will always be active on the set time, day, or date.
  - **End after –** Selecting this option will stop automatic firmware upgrades after the selected date.
  - **Ends after –** Selecting this option and specifying a period wil set a limited number of times to automatically upgrade firmware based on the Time Type or frequency set.
- **Enable –** Enable this option to enable the automatic firmware upgrade function.



Monitoring devices

Event Monitoring

To monitor device events, in the left navigation menu, click on **Monitoring** and click on **Events**.

The **Top 10 Device Events** tab displays an event snapshot of the top 10 devices that generated the most events in the last 24 hours.

Click the top left drop-down list to select a specific tenant or select All to view devices from all tenants.

Click the drop-down list next to the tenant selection to select the type of event.

The devices will be listed on the left and the bars will display the number of occurrences the event took place.

To view more detail on device events, in the left navigation menu, click on the **Device Event Analysis** tab.

Click the top left drop-down list to select a specific tenant or select All to view devices from all tenants.

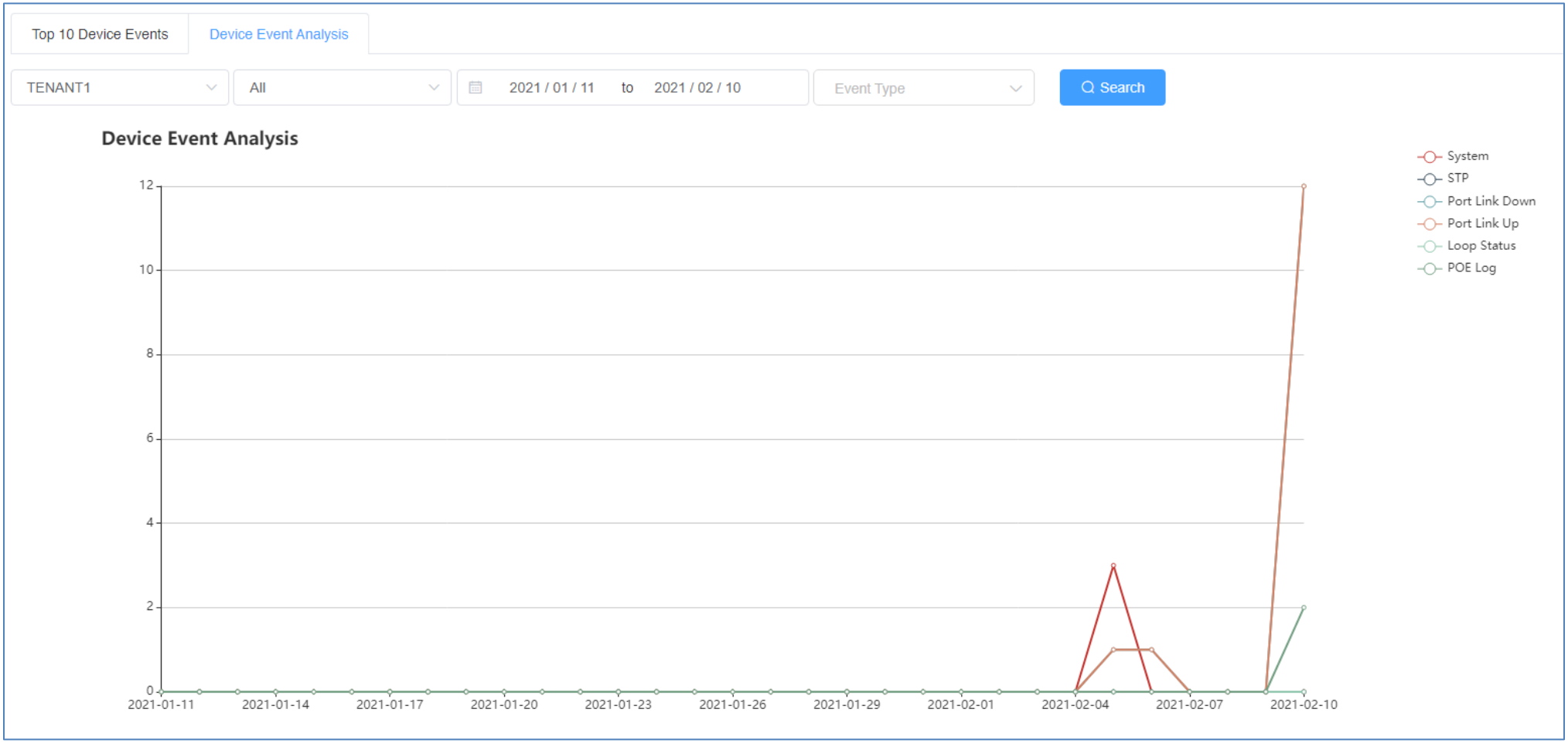
Click the drop-down list next to the tenant selection to select a specific device or select All to view all devices.

Click the drop-down list next to the device selection and select the range of dates to view.

Note: *Event data is limited to only to 30 days prior to the current date.*

Click on **Event Type** drop-down list to select a specific event or select All to view all events. If none is select, by default, the chart will display all events.

Mouse over the chart to view the specific number of occurrences the events took place on the specific date.

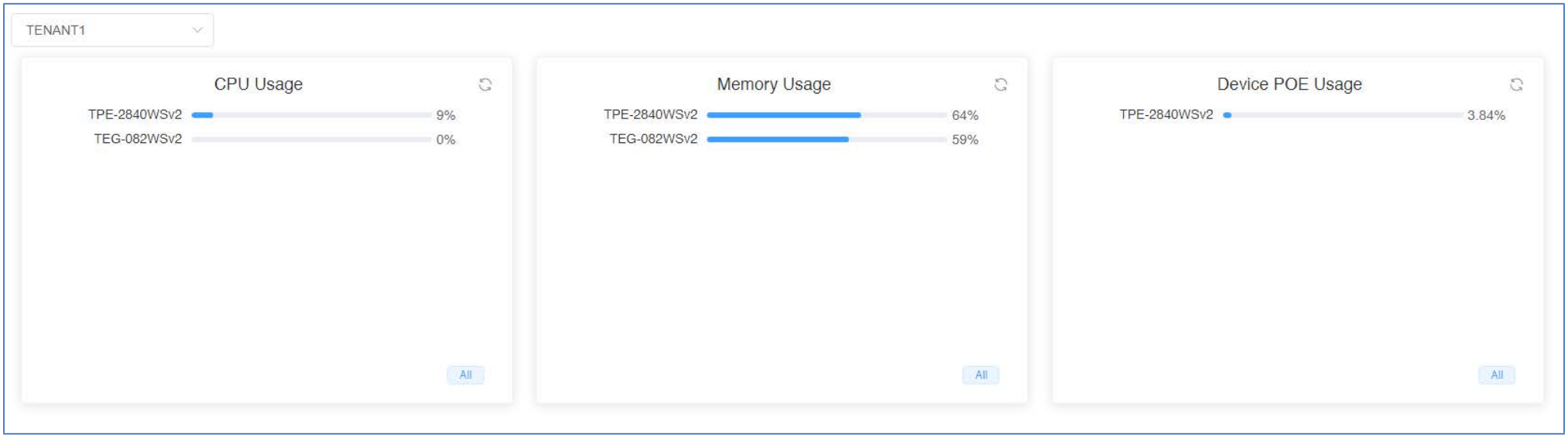


Device Utilization

To view device CPU, memory, and PoE utilization (if applicable), click on **Monitoring** and click on **Utilization**.

Click the top left drop-down list to select a specific tenant or select All to view devices from all tenants.

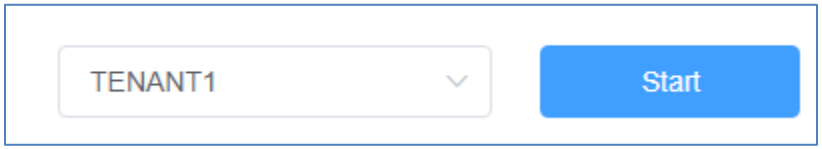
The current CPU, memory, and PoE budget utilization will be displayed for the devices.



Diagnostic Tools

To access the diagnostic tools, in the left navigation menu, click on **Maintenance** and click on **Diagnostic.**

At the top, click the drop-down list to select the tenant to run the diagnostic and click on **Start**.

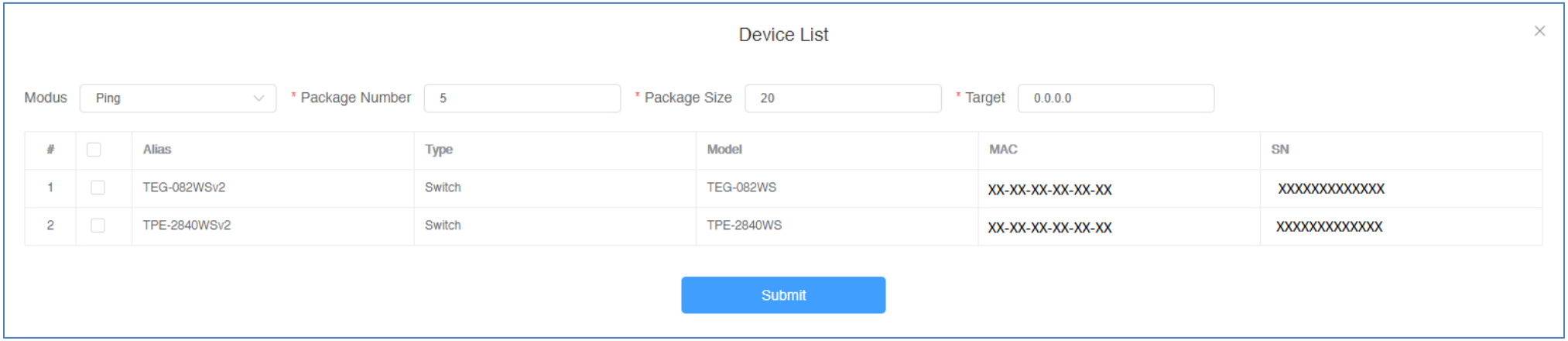


Ping IPv4 Host

To run a ping test to check for network connectivity from a device to an IPv4 host, click the **Modus** drop-down list and select **Ping**.

- **Package Number –** Value specifies the number of ping requests to send.
- **Package Size –** Value specifies the ping packet size in bytes.
- **Target –** Enter the IPv4 address of the host to send pings to check network connectivity.

In the list, check the devices you would like to run the ping test, click **Submit.**



The submitted diagnostic test will appear in the list.

#	Modus	Operator	Time	Operation
1	Ping	XXXXXXXXXX	2021-02-10 13:48:08	

Under **Operation**

Click this button to show the test detail.

Click this button to delete the entry.

Under the test detail window, under **Details**, click view button for additional test detail for each device.

Detail

	Alias	MAC	Update Time	Status	Details
1	TPE-2840WSv2	XX-XX-XX-XX-XX-XX	2021-02-10 13:48:13	Execute successfully	
2	TEG-082WSv2	XX-XX-XX-XX-XX-XX	2021-02-10 13:48:13	Execute successfully	

Diagnostic Details

Reply Received From : 192.168.10.254, TimeTaken : 20 ms

Reply Received From : 192.168.10.254, TimeTaken : 10 ms

Reply Received From : 192.168.10.254, TimeTaken : 10 ms

Reply Received From : 192.168.10.254, TimeTaken : 10 ms

Reply Received From : 192.168.10.254, TimeTaken : 10 ms

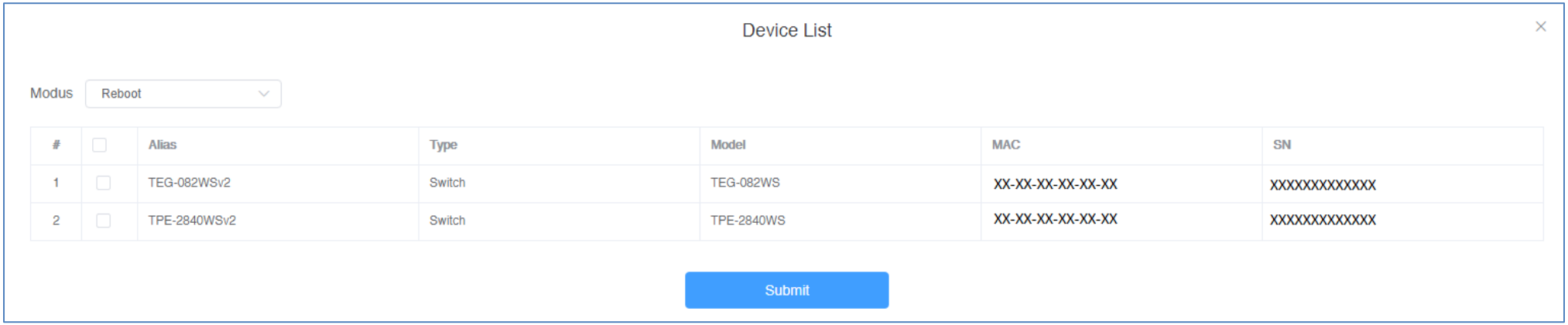
--- 192.168.10.254 Ping Statistics ---

5 Packets Transmitted, 5 Packets Received, 0% Packets Loss

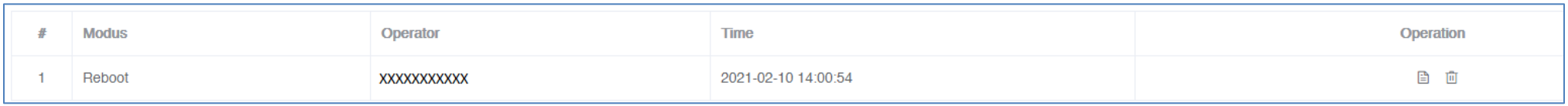
Device Reboot

To reboot devices, click the **Modus** drop-down list and select **Reboot**.

Check the devices you would like to reboot and click **Submit.**



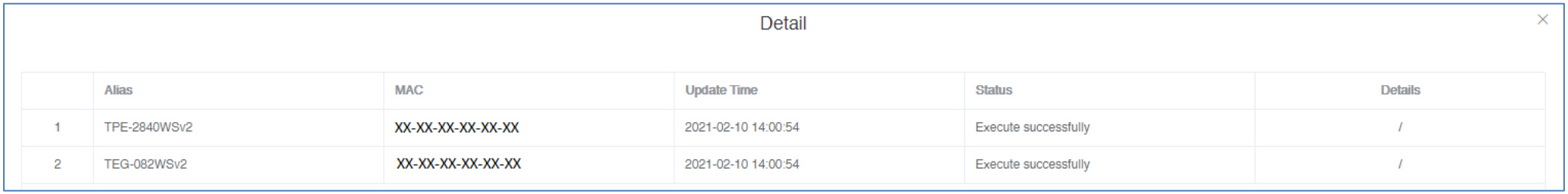
The submitted diagnostic test will appear in the list.



Under **Operation**

Click this button to show the test detail.

Click this button to delete the entry.

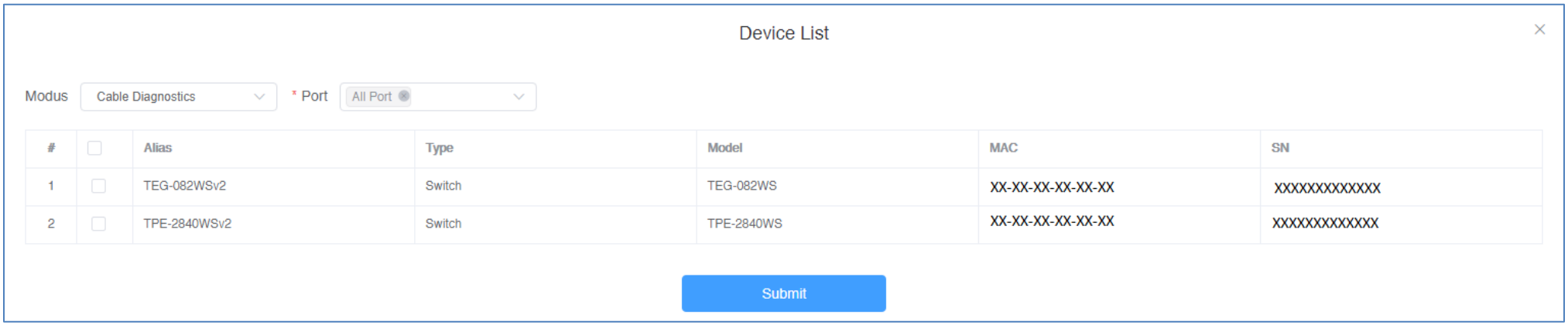


Cable Diagnostics

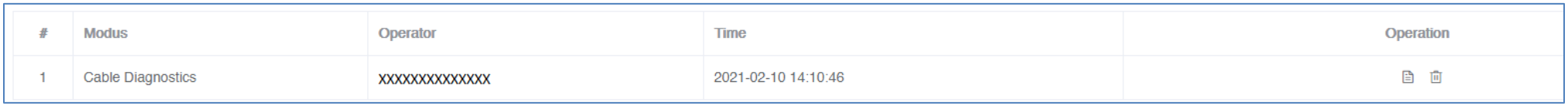
To run cable diagnostics, click the **Modus** drop-down list and select **Cable Diagnostics**.

Click the **Port** drop-down list to select a specific port to run cable diagnostic or select All port to run a cable diagnostic on all ports.

Check the devices you would like to run the cable diagnostic and click **Submit.**



The submitted diagnostic test will appear in the list.



Under **Operation**

Click this button to show the test detail.

Click this button to delete the entry.

Under the test detail window, under **Details**, click view button for additional test detail for each device.

Note: *The view button will be available after the diagnostic test has completed.*

Detail

	Alias	MAC	Update Time	Status	Details
1	TPE-2840WSv2	XX-XX-XX-XX-XX-XX	2021-02-10 14:10:47	In execution	/
2	TEG-082WSv2	XX-XX-XX-XX-XX-XX	2021-02-10 14:11:03	Execute successfully	

Diagnostic Details

Port	Test Result	Cable Fault Distance (meters)	Cable Length (meters) [in range]
Port 1	Pair 1 Open in Cable	Pair 1 0	N/A
	Pair 2 Open in Cable	Pair 2 0	
	Pair 3 Open in Cable	Pair 3 0	
	Pair 4 Open in Cable	Pair 4 0	
Port 2	Pair 1 Open in Cable	Pair 1 0	N/A
	Pair 2 Open in Cable	Pair 2 0	
	Pair 3 Open in Cable	Pair 3 0	
	Pair 4 Open in Cable	Pair 4 0	
Port 3	Pair 1 Open in Cable	Pair 1 0	N/A
	Pair 2 Open in Cable	Pair 2 0	
	Pair 3 Open in Cable	Pair 3 0	
	Pair 4 Open in Cable	Pair 4 0	

Account Settings

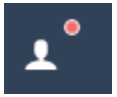
In the top right menu are the items below.

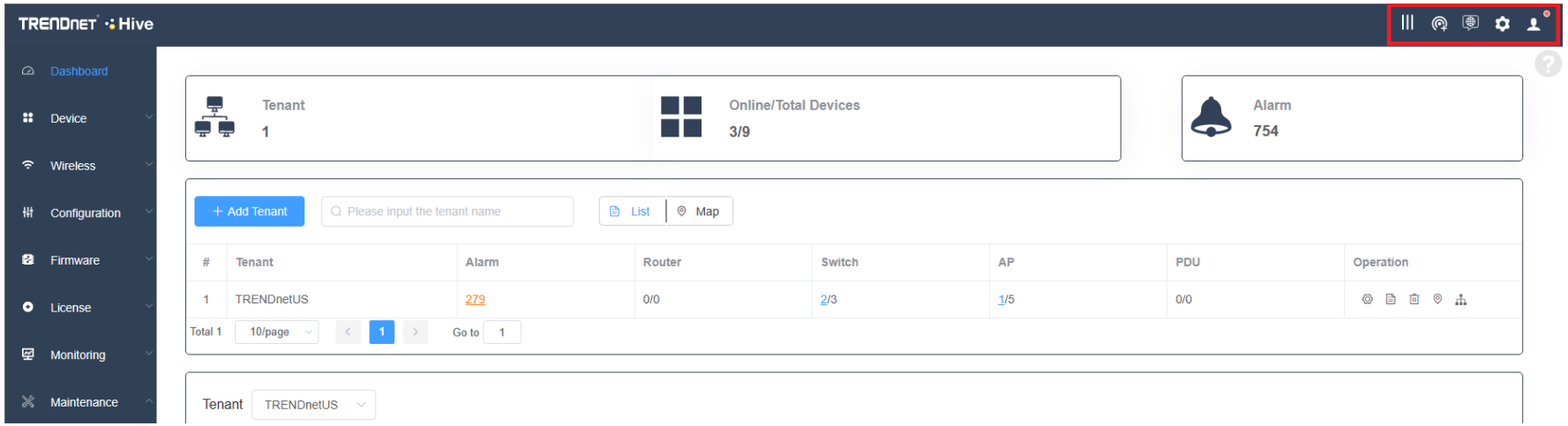

Expand/Collapse left navigation menu


Create new tenant


Select language

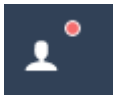

Alert notification settings


Account Settings and Logging



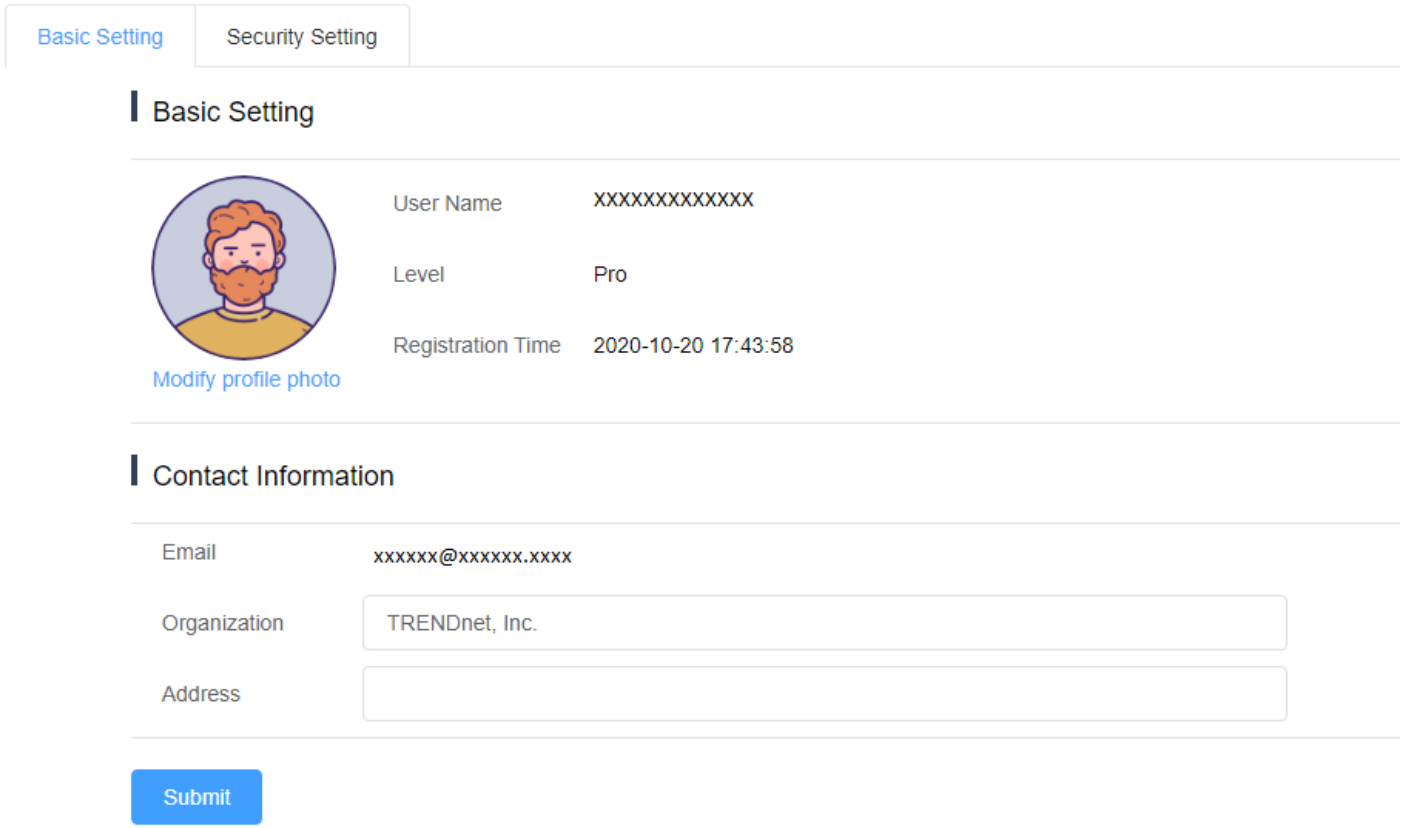
Modify Hive Account Settings

To modify your Hive personal account information, in the top right menu, click the **Account/Logging** button and click on **Personal Information.**



The **Basic Settings** tab wil display your Hive User Name, Hive Account/Level/Type, Registration Date and Time, and contact information. You can edit your profile photo/avatar, the organization and address for your Hive account on this tab. After you modify settings, click **Submit.**

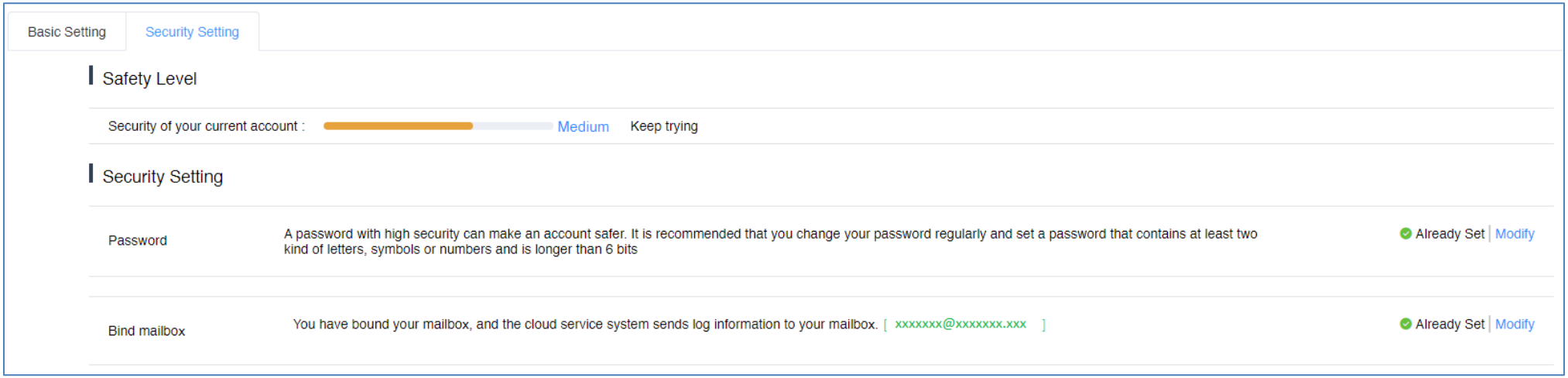
Note: *Additionally, this section displays a login history including the time/date, user account, country, city, time zone, and public IP address of the session.*



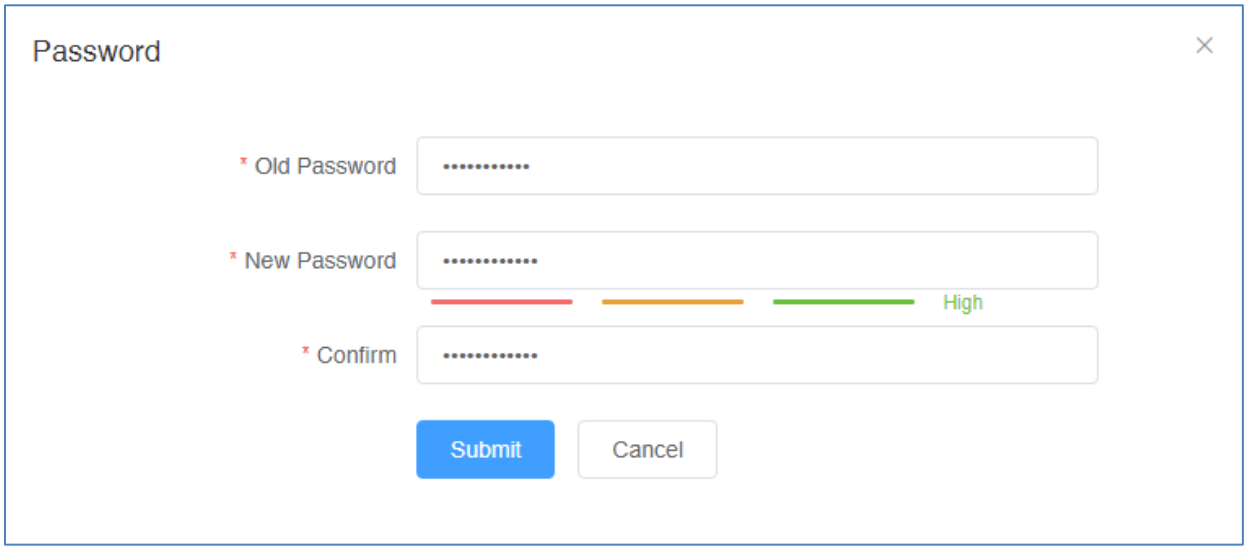
To edit your Hive account password, click on the **Security Settings** tab.

The Safety Level indicates the current security level of your account based on the complexity of your current Hive account password.

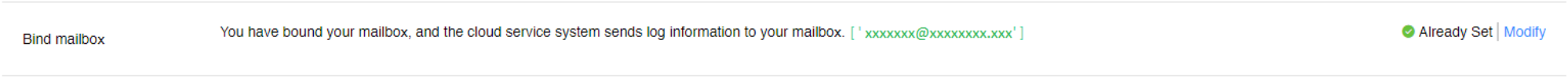
Note: *It is recommended to change your Hive account password with High security level rating.*



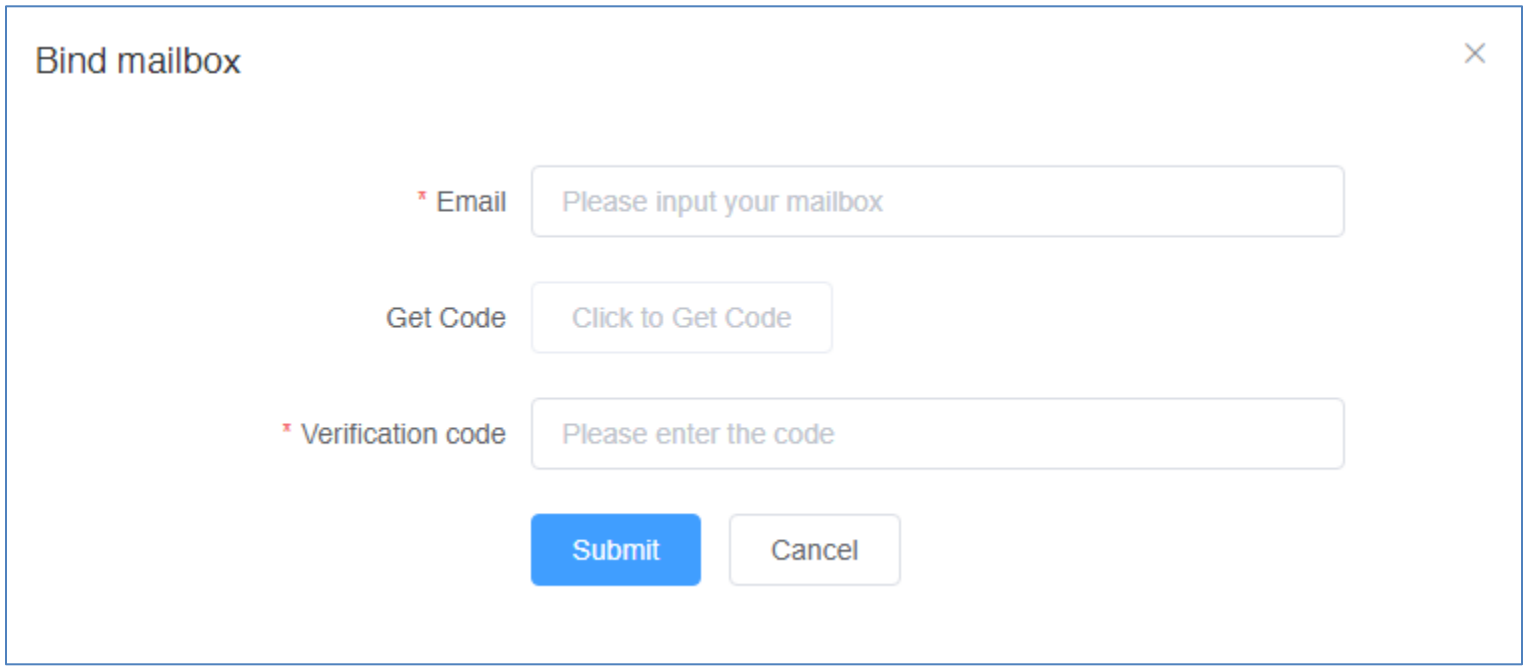
Under the Security Setting section, for the Password setting, click on **Modify** to modify your Hive account password.



To change the email address your Hive account is associated, under the Security Setting section, for Bind mailbox, click on **Modify** to modify your Hive email address.
The current email address the Hive account is associated will be displayed in green.

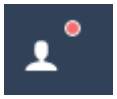


Enter the new email address in the field provided, then click **Get Code** to receive a verification from the Hive system at the new email address.
Check the new email mailbox and enter the verification code received in the field provided, then click **Submit.**

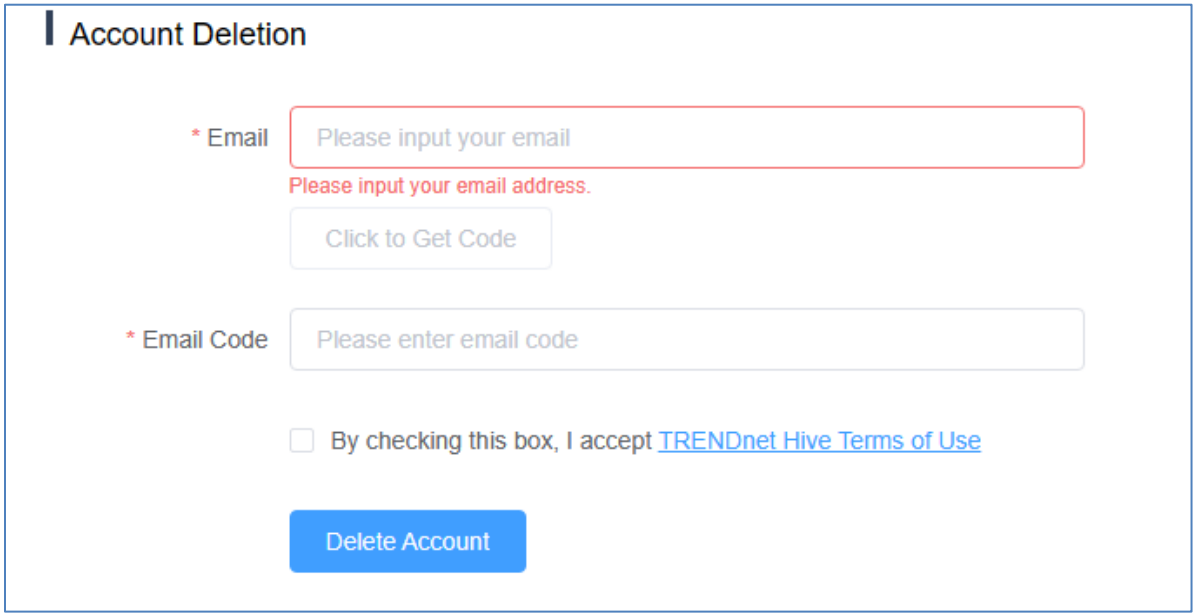


Delete Hive Account

To delete your Hive accout, in the top right menu, click the **Account/Logging** button and click on **Personal Information.**



To request for the Hive account to be deleted, click the **Account Deletion** tab.

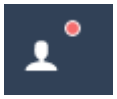


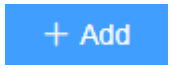
- **Email:** Enter the primary email address binded to the Hive Pro account and click the **Click to Get Code** button.
  Note: *This is the same email address listed under the* ***Basic*** *and* ***Security Settings*** *tabs.*
- **Email Code:** Check the email inbox for the verification code email and enter the code in this field once received to verify the email address for Hive account deletion.

Review and access the terms and click **Delete Account** to send an account deletion request.
Note: *You will receive a confirmation email that the account deletion was received.*

Create Users and Assign Permissions (Applies to Hive Pro only)

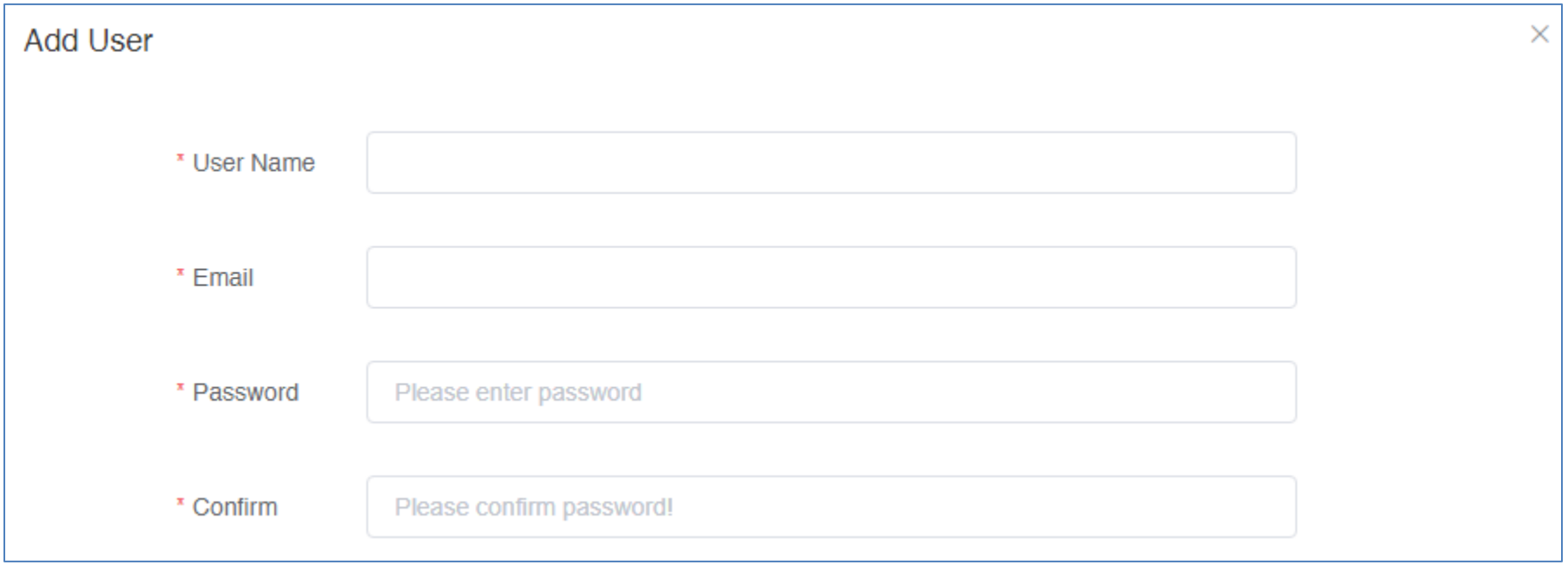
To modify your Hive personal account information, in the top right menu, click the **Account/Logging** button and click on **User Management.**



To add a new user, at the top, click the 

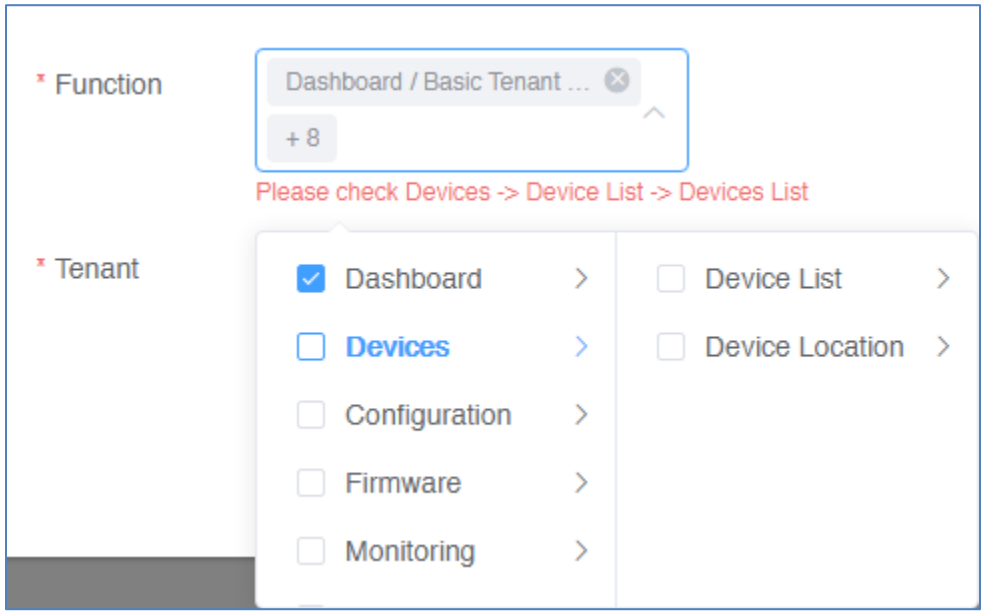
button.

Enter the user details such as **User Name**, **Email**, **Password.**



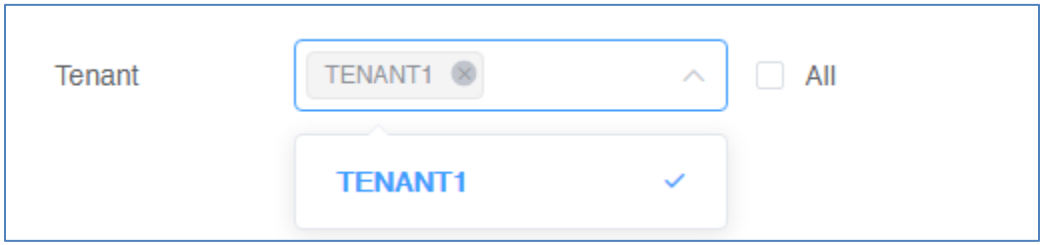
Click the **Function** drop-down to select the Hive section the user will have access. Any sections not seletected will not be accessible for the new user.

Note: *When checking sections, if dependency sections are required in order to access a selected section, a notification will appear in red indicating other specific dependencies that must also be checked in order for the user to access selected section.*



Click the **Tenant** drop-down list to select the specific tenant the user will have access. The user will only have access to the selected tenant. Then click **Submit** to create the new user.

Note: *To allow the user access to all tenants, check the All option.*



The new user will be displayed in the user list.

#	User Name	Email	Create Time	Operation
1	xxxxxxxxx	xxxxxx@xxxxxx.xxx	2021-02-10 17:42:21	

Under the **Operation** section

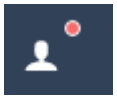
- Edit the user account settings. Allows you to modify the user email, access sections, and issue a reset password.

- Delete the user account.

View Hive System Messages

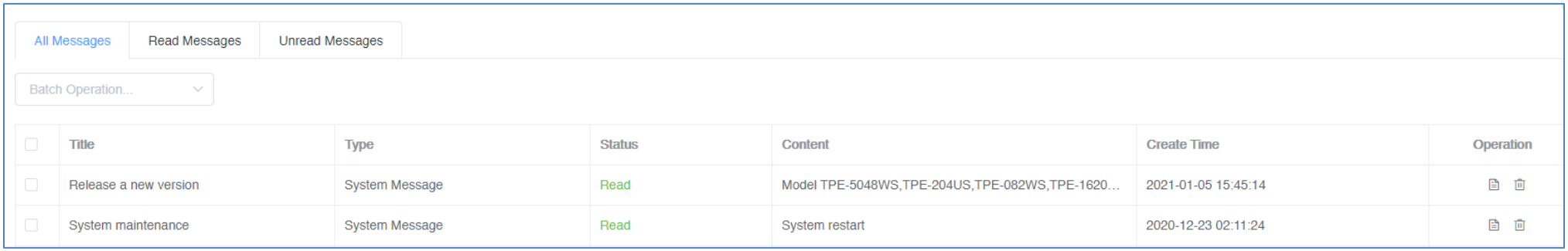
System messages related the Hive Management system internally. (ex: New device firmware update release in Hive Management System).

To view Hive system messages, click the **Account/Logging** button and click on **Message List.**



The system messages will display in the list.

Note: *You can click on the* ***Read Messages*** *tab to view messages that have already been read or click the* ***Unread Messages*** *tab to view messages that not yet been read.*



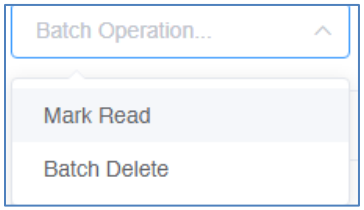
Under the **Operation** section for each message,

 - Click this button view the message details

 - Click this button to delete the message.

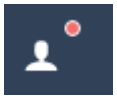
At the top left of the page, you can click the **Batch Operation** to mark multiple messages as Read (**Mark Read)** or delete multiple messages (**Batch Delete).**

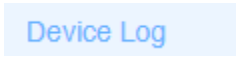
First, check all messages to apply the batch operation, then click the **Batch Operation** drop-down list and selected batch operation to use.



View Device Logging

To view Hive device logging, click the **Account/Logging** button and click on **Device Log**





This section displays device logging from devices managed from your Hive account.

At the top left, enter the keyword (if any) to search in device logging.

Select the **Start Date** and **End Date** range of device logging to display.

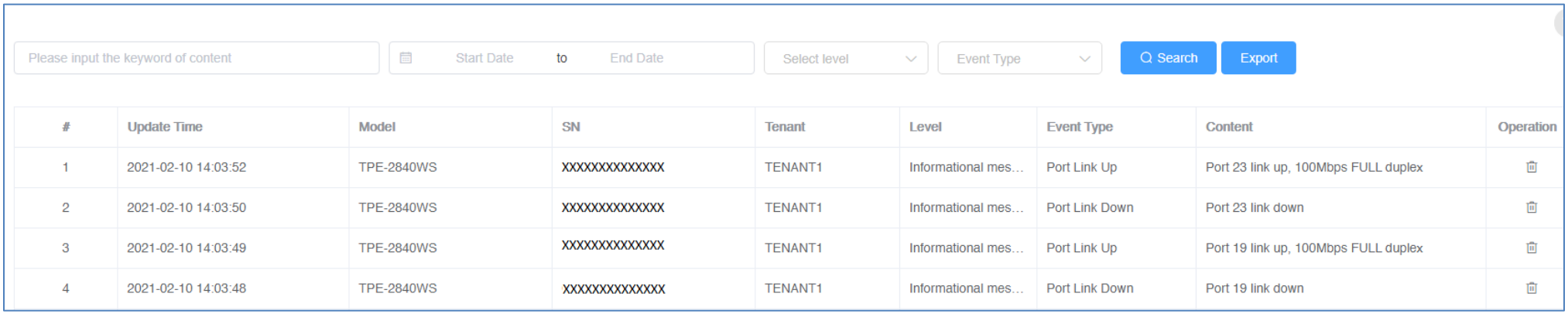
Note: *Logging data is limited only to 30 days prior to the current date.*

Click the **Select Level** drop-down list to select only specific types of logging to be displayed (optional, if none selected, logging will be displayed for all)

Click the **Event Type** drop-down list to select only specific events to be displayed (optional, if none selected, logging will be displayed for all)

Click **Search** to display logging within your defined filters.

After the search has completed, you can click **Export** to export logging to an excel (.xlsx) file.



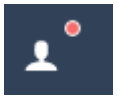
#	Update Time	Model	SN	Tenant	Level	Event Type	Content	Operation
1	2021-02-10 14:03:52	TPE-2840WS	XXXXXXXXXXXXX	TENANT1	Informational mes...	Port Link Up	Port 23 link up, 100Mbps FULL duplex	
2	2021-02-10 14:03:50	TPE-2840WS	XXXXXXXXXXXXX	TENANT1	Informational mes...	Port Link Down	Port 23 link down	
3	2021-02-10 14:03:49	TPE-2840WS	XXXXXXXXXXXXX	TENANT1	Informational mes...	Port Link Up	Port 19 link up, 100Mbps FULL duplex	
4	2021-02-10 14:03:48	TPE-2840WS	XXXXXXXXXXXXX	TENANT1	Informational mes...	Port Link Down	Port 19 link down	

Under the **Operation** section for each log entry,

 - Click this button to delete the logging entry.

View System Logging

To view Hive system logging, click the **Account/Logging** button and click on **System Log**



This section displays Hive system logging of activity in your Hive account and alarm notifications.

At the top left, enter the keyword (if any) to search in system logging.

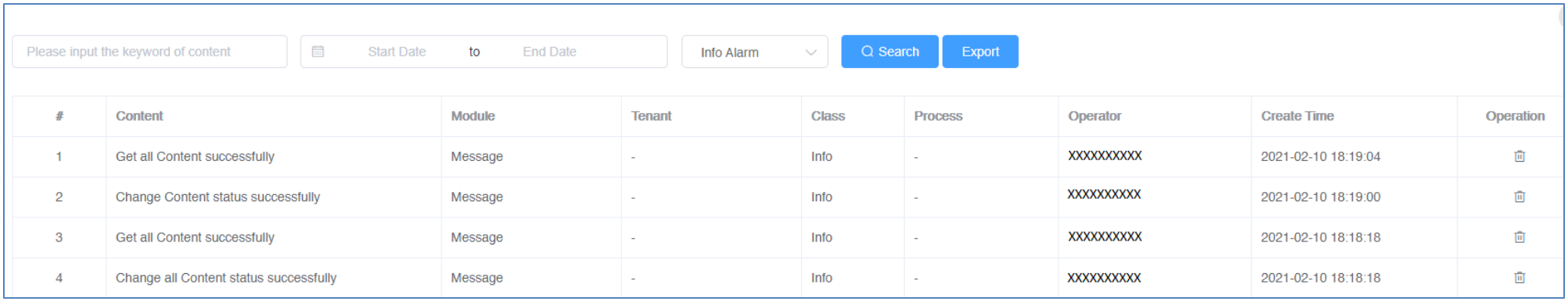
Select the **Start Date** and **End Date** range of system logging to display.

Note: *Logging data is limited only to 30 days prior to the current date.*

Click the **Info Alarm** drop-down list to select the class system logging to display.

Click **Search** to display logging within your defined filters.

After the search has completed, you can click **Export** to export logging to an excel (.xlsx) file.



#	Content	Module	Tenant	Class	Process	Operator	Create Time	Operation
1	Get all Content successfully	Message	-	Info	-	XXXXXXXXX	2021-02-10 18:19:04	
2	Change Content status successfully	Message	-	Info	-	XXXXXXXXX	2021-02-10 18:19:00	
3	Get all Content successfully	Message	-	Info	-	XXXXXXXXX	2021-02-10 18:18:18	
4	Change all Content status successfully	Message	-	Info	-	XXXXXXXXX	2021-02-10 18:18:18	

Under the **Operation** section for each log entry,

- Click this button to delete the logging entry.

Configure alert notifications

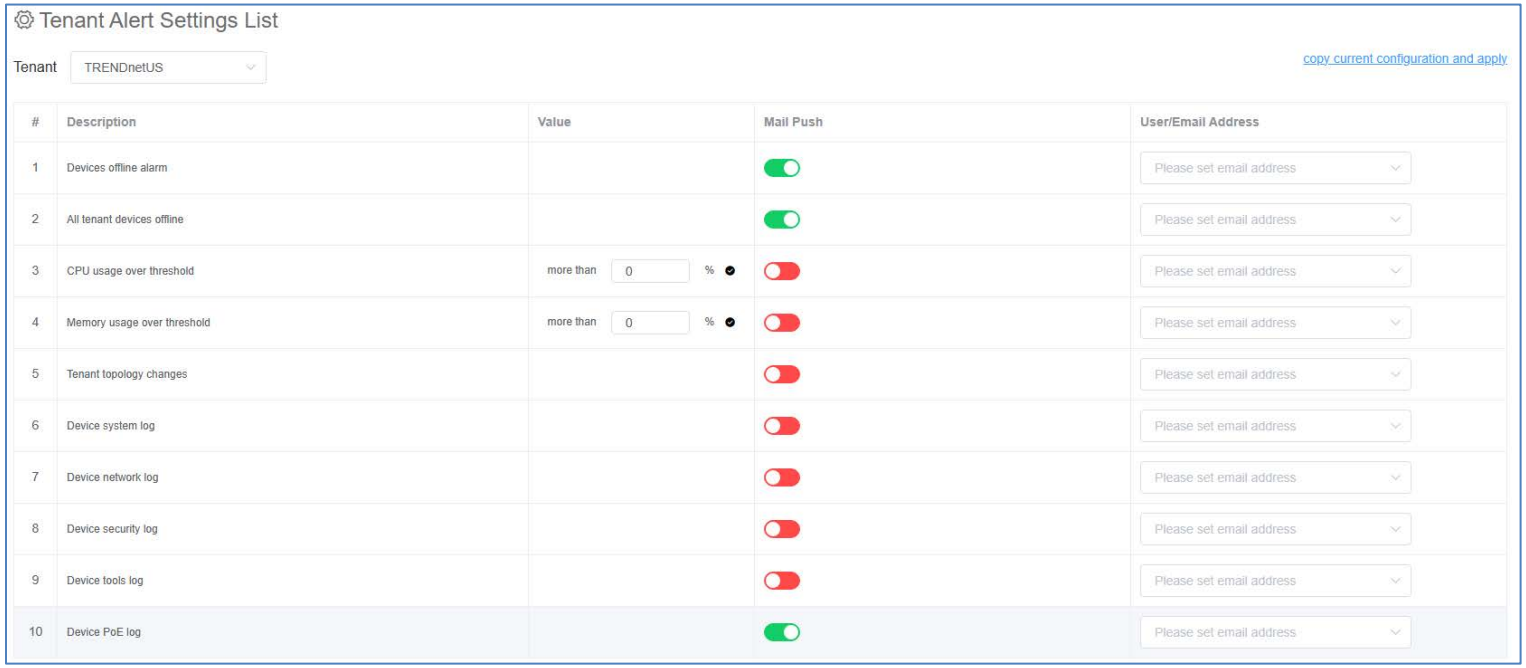
- To configure alert notifications, in the top right menu.

Click the Alert Notifications button  and click on **Alert Settings.**

Click the drop-down list in the left to select which tenant to configure the alert notification settings.

Enable/disable alert notificatons for **Mail Push** for email notifications. Click the **User/Email Address** to select specific email addresses for each alert notification. For multiple email addresses to be specified, the users with email addresses must be created under **Account/Logging** and **User Management** section (available in Hive Pro only)

Note: *Some alert settings require threshold percentages or data restrictions to be entered. You can also click the copy current configuration and apply link to apply the alert notification settings to a different tenant. (Available in Hive Pro only)*



- **Devices offline alarm:** Send an alert notification if any devices under the tenant are disconnected from your Hive account.
- **All tenant devices offline:** Send an alert notification only if all tenant devices are disconnected

Web Smart Switch Series Hardware Specifications

	TEG-082WS (2.0R)	TEG-204WS (1.0R)	TEG-284WS (1.0R)	TEG-524WS (1.0R)
Device Interface	LED Mode select button and LED indicators			
	8 x Gigabit ports	16 x Gigabit ports	24 x Gigabit ports	48 x Gigabit ports
	2 x SFP slots	4 x Shared Gigabit ports (RJ-45/SFP)		
Data Transfer Rate	Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex)			
	Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)			
	Gigabit Ethernet: 2000 Mbps (full duplex)			
Switch fabric	20 Gbps	40 Gbps	56 Gbps	104 Gbps
RAM buffer	4.1 Mbits			12 Mbits
MAC Address Table	8K entries			16K entries
Jumbo Frames	10 Kbytes			
Forwarding	14.9Mpps (64-byte packet size)	29.8Mpps (64-byte packet size)	41.7Mpps (64-byte packet size)	77.4Mpps (64-byte packet size)
HOL Blocking Prevention	HOL Blocking Prevention supported on all models			
Power Input	100 - 240V AC, 50/60 Hz, internal power supply			
Power Consumption	7.1 Watts (max.)	14.6 Watts (max.)	17.3 Watts (max.)	34.9 Watts (max.)
Fan Quantity	Fanless			
Noise Level	N/A (fanless)			
MTBF	1,092,872 hours	835,519 hours	787,004 hours	400,158 hours

	TEG-082WS (2.0R)	TEG-204WS (1.0R)	TEG-284WS (1.0R)	TEG-524WS (1.0R)
Operating Temperature	-5° – 50°C (23° - 122°F)			
Operating Humidity	Max. 95% non-condensing			
Dimensions	280 x 125.8 x 44 mm (11 x 5 x 1.74 in.)	280 x 180 x 44 mm (11 x 7 x 1.74 in.)	440 x 140 x 44mm (17.4 x 5.51 x 1.74 in.)	440 x 210 x 44mm (17.3 x 8.3 x 1.74 in.)
	Rack mountable 1U height			
Weight	0.98 kg (2.2 lbs.)	1.76 kg (3.88 lbs.)	2.15 kg (4.73 lbs.)	3.48 kg (7.67 lbs.)
Certifications	CE			
	FCC			
	UL			
Warranty	Lifetime			
Package Contents	In addition to the switch, the package contents include the following:			
	Quick Installation Guide			
	Rack mount kit			
	Power cord (1.8m/6 ft.)			

Web Smart Switch Series Software Specifications

Standards	• IEEE 802.1d • IEEE 802.1p • IEEE 802.1Q • IEEE 802.1s • IEEE 802.1w	• IEEE 802.1X • IEEE 802.1ab • IEEE 802.3 • IEEE 802.3u • IEEE 802.3x	• IEEE 802.3z • IEEE 802.3ab • IEEE 802.3ad • IEEE 802.3az
Management	• CLI (Telnet / SSHv2) for basic administration • HTTP/HTTPS (SSL v2/3 TLS) Web based GUI • SNMP v1, v2c, v3 • RMON v1	• Static Unicast MAC Address • Enable/disable 802.3az Power Saving • LLDP and LLDP-MED • Virtual Cable Diagnostics Test	• IPv6: IPv6 Neighbor Discovery, IPv6 Static IP, DHCPv6, Auto configuration • Dual image and configuration • TC Root/Protect
Hive Cloud Management (requires update to firmware 3.01.XXX to enable Hive capability)	• Configure, monitor, and manage through the TRENDnet Hive Cloud Management Portal remotely via PC or Mac web browser • Multi-device management • Provisioning through scheduled batch firmware or configuration updates for multiple switches	• Enable & disable PoE, set PD (powered device) alive check, configure PoE scheduling, and monitor PoE budget utilization (for PoE switches only) • Event/hardware network monitoring (CPU/memory utilization)	• Configure features such as IP address settings, VLANs, spanning tree, loopback detection, IGMP snooping, link aggregation, and bandwidth control through cloud management
MIB	• IP Forward Table MIB RFC 1354 • RMON MIB RFC 1271 • IPv4 MIB RFC 1213 • IPv6 MIB RFC 2465 • GVRP MIB IEEE 802.1Q-VLAN • LA MIB IEEE 802.3ad • LLDP MIB IEEE 802.1ab • IGMP Snooping MIB RFC 2933 • MLD Snooping MIB RFC 3019 • Private VLAN MIB IEEE 802.1Q	• DHCP Snooping MIB RFC 2026 • QoS MIB RFC 4323 • SNMP MIB RFC 3415 • STP MIB RFC 4318 • PNAC MIB IEEE 802.1x • VLAN MIB IEEE 802.1q • DNS MIB RFC 1611 • ACL MIB • Bandwidth CTRL MIB • LBD MIB	• Mirror MIB • IPv6 Neighbor MIB • SNTP MIB • Storm CTRL MIB • Statistics MIB • Tool MIB • Voice VLAN MIB • DoS MIB
Spanning Tree	• IEEE 802.1D STP (Spanning Tree protocol)	• IEEE 802.1w RSTP (Rapid Spanning Tree protocol)	• IEEE 802.1s MSTP (Multiple Spanning Tree protocol)
Link Aggregation	• Static Link Aggregation	• 802.3ad Dynamic LACP	

Quality of Service (QoS)	• 802.1p Class of Service (CoS) • DSCP (Differentiated Services Code Point)	• Bandwidth Control per port	• Queue Scheduling: Strict Priority, Weighted Round Robin (WRR)
VLAN	• Multiple management VLAN assignment • Asymmetric VLAN • 802.1Q Tagged VLAN	• Dynamic GVRP • MAC-based VLAN • Protocol-based VLAN	• Up to 256 VLAN groups, ID Range 1-4094 • Private VLAN (Protected Ports) • Voice VLAN (10 user defined OUIs)
Multicast	• IGMP Snooping v1, v2, v3 • MLD Snooping v1, v2	• IGMP fast leave • MVR (Multicast VLAN Registration)	• Static Multicast Address • Up to 256 multicast entries
Port Mirror	• RX, TX, or Both	• Many to one	
Access Control	• 802.1X Port-Based Network Access Control , RADIUS, TACACS+ • Local Dial In User Authentication • DHCP Snooping (per VLAN) • Loopback Detection	• Duplicated Address Detection • Trusted Host • Denial of Service (DoS) • IP MAC port binding	• Dynamic ARP inspection • Block unknown multicast
ACL IPv4 L2-L4 & IPv6	• MAC Address • VLAN ID • Ether Type (IPv4 only)	• IP Protocol 0-255 • TCP/UDP Port 1-65535 • 802.1p	• DSCP (IPv4 only) • IPv6 Address (IPv6 only)
Layer 3 Features	• IPv4 / IPv6 static routing • IP interfaces: Up to 6	• Routing table entries: Up to 32 (IPv4 / IPv6) • ARP table (up to 128 entries)	• Inter-VLAN routing
Compatibility	Optional Software Utility: Windows® 10, 8.1, 8, 7, Vista, XP, Windows® 2003/2008 Server		

Web Smart PoE Switch Series Hardware Specifications

	TPE-082WS (1.0R)	TPE-1620WS (2.0R)	TPE-1620WSF (1.0R)	TPE-2840WS (2.0R)	TPE-5028WS (1.0R)	TPE-5240WS (1.0R)	TPE-5048WS (1.0R)
Device Interface	LED Mode select button and LED indicators						
	8 x Gigabit PoE+ ports	16 x Gigabit PoE+ ports		24 x Gigabit PoE+ ports		48 x Gigabit PoE+ ports	
	2 x SFP slots	4 x Shared Gigabit ports (RJ-45/SFP)					
Data Transfer Rate	Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex)						
	Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)						
	Gigabit Ethernet: 2000 Mbps (full duplex)						
Switch fabric	20 Gbps	40 Gbps		56 Gbps		104 Gbps	
RAM buffer	4.1 Mbits					12 Mbits	
MAC Address Table	8K entries					16K entries	
Jumbo Frames	10 Kbytes						
Forwarding	14.9 Mpps (64-byte packet size)	29.8Mpps (64-byte packet size)		41.7Mpps (64-byte packet size)		77.4Mpps (64-byte packet size)	
HOL Blocking Prevention	HOL Blocking Prevention supported on all models						
Power Input	External power supply (54V DC, 1.67A)	100 - 240V AC, 50/60 Hz, internal power supply					
Power Consumption	82 Watts (max.)	226W (max.)	460W (max.)	256W (max.)	446W (max.)	479W (max.)	963W (max.)
PoE Type	802.3at: Up to 30W per port						
PoE Budget	75 Watts	185W	370W	185W	370W	740W	75 Watts
Fan Quantity	Fanless	2				3	5
Noise Level	N/A (fanless)	52 dBA (max.)				52.4 dBA (max.)	55 dBA (max.)
MTBF	862,966 hours	465,862 hours	192,382 hours	443,825 hours	277,604 hours	239,897 hours	338,601 hours

	TPE-082WS (1.0R)	TPE-1620WS (2.0R)	TPE-1620WSF (1.0R)	TPE-2840WS (2.0R)	TPE-5028WS (1.0R)	TPE-5240WS (1.0R)	TPE-5048WS (1.0R)
Operating Temperature	-5° – 50°C (23° - 122°F)						
Operating Humidity	Max. 95% non-condensing		Max. 90% non-condensing	Max. 95% non-condensing			
Dimensions	280 x 125.8 x 44 mm (11 x 5 x 1.74 in.)	440 x 250 x 44mm (17.3 x 9.8 x 1.74 in.)				440 x 430 x 44mm (17.3 x 17 x 1.74 in.)	
	Rack mountable 1U height						
Weight	0.92 kg (2 lbs.)	3.66kg (8 lbs.)	3.89kg (8.5 lbs.)	3.75kg (8.26 lbs.)	3.92kg (8.64 lbs.)	6.12kg (13.5 lbs.)	6.58kg (14.5 lbs.)
Certifications	CE						
	FCC						
	External Power Adapter (UL)	UL					
Warranty	Lifetime						
Package Contents	In addition to the switch, the package contents include the following:						
	Quick Installation Guide						
	Rack mount kit						
	Power adapter (54V DC, 1.67A)	Power cord (1.8m/6 ft.)					

Web Smart Switch Series Software Specifications

Standards	• IEEE 802.1d • IEEE 802.1p • IEEE 802.1Q • IEEE 802.1s • IEEE 802.1w • IEEE 802.1X	• IEEE 802.1ab • IEEE 802.1ax • IEEE 802.3 • IEEE 802.3u • IEEE 802.3x • IEEE 802.3z • IEEE 802.3ab	• IEEE 802.3ad • IEEE 802.3af • IEEE 802.3at • IEEE 802.3az
Management	• CLI (Telnet / SSHv2) for basic administration** • HTTP/HTTPS (SSL v2/3 TLS) Web based GUI • SNMP v1, v2c, v3 • RMON v1	• Static Unicast MAC Address • Enable/disable 802.3az Power Saving • LLDP (Basic/Dot1/Dot3 TLV Settings**) and LLDP-MED • Virtual Cable Diagnostics Test	• IPv6: IPv6 Neighbor Discovery, IPv6 Static IP, DHCPv6, Auto configuration • Dual image and configuration** • TC Root/Protect • Ping watchdog***
MIB	• IP Forward Table MIB RFC 1354 • RMON MIB RFC 1271 • IPv4 MIB RFC 1213 • IPv6 MIB RFC 2465 • GVRP MIB IEEE 802.1Q-VLAN • LA MIB IEEE 802.3ad • LLDP MIB IEEE 802.1ab • IGMP Snooping MIB RFC 2933 • MLD Snooping MIB RFC 3019 • Private VLAN MIB IEEE 802.1Q	• DHCP Snooping MIB RFC 2026 • QoS MIB RFC 4323 • SNMP MIB RFC 3415 • STP MIB RFC 4318 • PNAC MIB IEEE 802.1x • VLAN MIB IEEE 802.1q • DNS MIB RFC 1611 • ACL MIB • Bandwidth CTRL MIB • LBD MIB	• Mirror MIB • IPv6 Neighbor MIB • SNTP MIB • Storm CTRL MIB • Statistics MIB • Tool MIB • Voice VLAN MIB • DoS MIB
Spanning Tree	• IEEE 802.1D STP (Spanning Tree protocol)	• IEEE 802.1w RSTP (Rapid Spanning Tree protocol)	• IEEE 802.1s MSTP (Multiple Spanning Tree protocol)
Link Aggregation	• Static Link Aggregation	• 802.3ad Dynamic LACP	• 802.1ax Link Aggregation
Quality of Service (QoS)	• 802.1p Class of Service (CoS) • DSCP (Differentiated Services Code Point)	• Bandwidth Control per port	• Queue Scheduling: Strict Priority, Weighted Round Robin (WRR)
VLAN	• Multiple management VLAN assignment • Asymmetric VLAN • 802.1Q Tagged VLAN	• Dynamic GVRP • MAC-based VLAN • Protocol-based VLAN • Multicast VLAN**	• Up to 256 VLAN groups, ID Range 1-4094 • Private VLAN (Protected Ports) • Voice VLAN (10 user defined OUIs)

Multicast	• IGMP Snooping v1, v2, v3 • MLD Snooping v1, v2** • IGMP fast leave	• MVR (Multicast VLAN Registration)** • Static Multicast Address	• Multicast Filtering** • Up to 256 multicast entries
Port Mirror	• RX, TX, or Both	• Many to one	
Access Control	• 802.1X Port-Based Network Access Control , RADIUS, TACACS+ • Local Dial In User Authentication • DHCP Snooping (per VLAN) • Loopback Detection	• Duplicated Address Detection • Trusted Host • Denial of Service (DoS) • IP MAC port binding	• Dynamic ARP inspection** • Block unknown multicast • Port Security/MAC address learning restriction (Up to 64 entries per port)
ACL IPv4 L2-L4 & IPv6	• MAC Address • VLAN ID • Ether Type (IPv4 only)	• IP Protocol 0-255 • TCP/UDP Port 1-65535 • 802.1p	• DSCP (IPv4 only) • IPv6 Address (IPv6 only)
Layer 3 Features*	• IPv4 / IPv6 static routing • IP interfaces: Up to 6	• Routing table entries: Up to 32 (IPv4 / IPv6) • ARP table (up to 128 entries)	• Inter-VLAN routing
PoE Features**	• PoE Mode A: Pins 1, 2, 3, and 6 for power • PoE auto classification	• PoE port priority • PoE power scheduling	• PD alive check
TRENDnet Hive Features*** https://www.trendnet.com/hive (Requires subscription purchase) (Click here to view list of Hive compatible devices)	• Centralized network device management through cloud-based Hive portal • Overview of devices, client, and system logs • View user, traffic statistics, and device lists • Access, manage, configure, and troubleshoot devices remotely • Event/hardware monitoring	• Provisioning through schedule batch firmware or configuration updates • Backup, restore, copy device configuration to Hive cloud****** • Email alerts and notifications • Multi-site management • Google Maps™ location tracking (Pro version only)	• Multi-tenant management (Pro version only) • Multi-user roles and permissions (Pro version only) • Service-Level Agreement (SLA) guaranteed 99.9 percent uptime • Works with TRENDnet Hive enabled devices
Compatibility	Optional Software Utility: Windows® 10, 8.1, 8, 7, Vista, XP, Windows® 2003/2008 Server		

*Feature available with firmware version 2.10.010 or above. / **Feature only applies to TRENDnet Power over Ethernet (PoE) models / ***Feature available with firmware version 3.01.007 or above. / ******Feature available with firmware 3.01.012 or above.

Wireless Access Point Hardware Specifications

	TEW-821DAP (2.0R) AC1200	TEW-825DAP (1.0R) AC1750	TEW-826DAP (1.0R) AC2200	TEW-921DAP (1.0R) AX1800
Device Interface	LED indicator(s), power port (non-PoE installation), and Reset button			
	1 x PoE Gigabit LAN Port	1 x PoE+ Gigabit LAN Port	1 x PoE+ Gigabit LAN Port 1 x Gigabit LAN Port	1 x PoE+ Gigabit LAN Port
	802.11ac MU-MIMO WiFi 5 Concurrent Dual Band	802.11ac WiFi 5 Concurrent Dual Band	802.11ac MU-MIMO WiFi 5 Concurrent Tri-Band	802.11ax WiFi 6 Concurrent Dual Band
Speed	Up to 867Mbps (5GHz) 802.11ac Up to 300Mbps (2.4GHz) 802.11n	Up to 1300Mbps (5GHz) 802.11ac Up to 450Mbps (2.4GHz) 802.11n	Up to 867Mbps (5GHz1) 802.11ac Up to 867Mbps (5GHz2) 802.11ac Up to 300Mbps (2.4GHz) 802.11n	Up to 1201Mbps (5GHz) 802.11ax Up to 574Mbps (2.4GHz) 802.11ax
Streams	2x2	3x3	2x2	2x2
Frequency	• 2.4GHz: 2.412 – 2.472GHz • 5GHz: 5.180 – 5.825GHz	• 2.4GHz: 2.412 – 2.472GHz • 5GHz: 5.180 – 5.825GHz	• 2.4GHz: 2.412 – 2.472GHz • 5GHz1: 5.180 – 5.320GHz • 5GHz2: 5.500 – 5.825GHz	• 2.4GHz: 2.412 – 2.472GHz • 5GHz: 5.180 – 5.320GHz
Wireless Channels	• 2.4GHz: FCC: 1–11, ETSI: 1 – 13 • 5GHz: FCC: 36, 40, 44, 48, 149, 153, 157, 161 and 165, ETSI: 36, 40, 44, 48 (52, 56, 60, 64, 100,104,108,112,116, 132,136,140)**	• 2.4GHz: FCC: 1–11 • 5GHz: FCC: 36, 40, 44, 48, 149, 153, 157, 161 and 165	• 2.4GHz: FCC: 1–11 • 5GHz: FCC: 36, 40, 44, 48, 149, 153, 157, 161 and 165	• 2.4GHz: FCC: 1–11, ETSI: 1 – 13 • 5GHz: FCC: 36, 40, 44, 48, 149, 153, 157, 161 and 165, ETSI: 36, 40, 44, 48 (52, 56, 60, 64, 100,104,108,112,116, 132,136,140)**
Modulation	• DBPSK/DQPSK/CCK for DSSS technique • BPSK/QPSK/16-QAM/64-QAM/256-QAM for OFDM technique			• DBPSK/DQPSK/CCK for DSSS technique • BPSK/QPSK/16-QAM/64-QAM/256-QAM/1024-QAM for OFDM technique • OFDMA
Antenna Gain	• 2.4GHz: 2 x 3 dBi internal • 5GHz: 2 x 4 dBi internal	• 2.4 GHz: 3 x 4 dBi internal • 5 GHz: 3 x 4 dBi internal	• 2.4GHz: 2 x 4 dBi internal • 5GHz1: 2 x 4 dBi internal • 5GHz2: 2 x 4 dBi internal	• 2.4GHz: 2 x 3.2 dBi internal • 5GHz: 2 x 4.3 dBi internal
Wireless Output Power	• 802.11a: FCC: 19 dBm (max.) / CE: 19 dBm (max.) / IC: 19 dBm (max.)	• 802.11a: FCC: 23 dBm, (Max.) • 802.11b: FCC: 22 dBm (Max.) • 802.11g: 17 dBm (Max.)	• 802.11a: FCC: 33.18 dBm (max.) / IC: 33.18 dBm (max.) • 802.11b: FCC: 27.41 dBm (max.) / IC: 27.41 dBm (max.)	• 802.11a: FCC: 30 dBm (max.) / CE: 28 dBm (max.) • 802.11b: FCC: 29 dBm (max.) / CE: 18 dBm (max.)

	• 802.11b: FCC: 23 dBm (max.) / CE: 10 dBm (max.) / IC: 23 dBm (max.) • 802.11g: FCC: 19 dBm (max.) / CE: 12 dBm (max.) / IC: 19 dBm (max.) • 802.11n (2.4 GHz): FCC: 19 dBm (max.) / CE: 12 dBm (max.) / IC: 19 dBm (max.) • 802.11n (5 GHz): FCC: 19 dBm (max.) / CE: 19 dBm (max.) / IC: 19 dBm (max.) • 802.11ac: FCC: 18 dBm (max.) / CE: 18 dBm (max.) / IC: 18 dBm (max.)	• 802.11n: FCC: 17 dBm (Max.) • 802.11n: FCC: 23 dBm (Max.) • 802.11ac: FCC: 23 dBm, CE: 21 dBm (Max.)	• 802.11g: FCC: 32.23 dBm (max.) / IC: 32.23 dBm (max.) • 802.11n (2.4GHz): FCC: 32.41 dBm (max.) / IC: 32.41 dBm (max.) • 802.11n (5GHz): FCC: 33.37 dBm (max.) / IC: 33.37 dBm (max.) • 802.11ac: FCC: 30.55 dBm (max.) / IC: 30.55 dBm (max.)	• 802.11g: FCC: 29 dBm (max.) / CE: 19 dBm (max.) • 802.11n (2.4GHz): FCC: 29 dBm (max.) / CE: 19 dBm (max.) • 802.11n (5GHz): FCC: 30 dBm (max.) / CE: 28 dBm (max.) • 802.11ac: FCC: 30 dBm (max.) / CE: 28 dBm (max.) • 802.11ax (2.4GHz): FCC: 29 dBm / CE: 19 dBm • 802.11ax (5GHz): FCC: 30 dBm / CE: 28 dBm
Receiving Sensitivity	• 802.11a: -65 dBm (typical) @ 54 Mbps • 802.11b: -83 dBm (typical) @ 11 Mbps • 802.11g: -65 dBm (typical) @ 54 Mbps • 802.11n (2.4 GHz): -64 dBm (typical) @ 300 Mbps • 802.11n (5 GHz): -61 dBm (typical) @ 300 Mbps • 802.11ac: -51 dBm (typical) @ 867 Mbps	• 802.11a: -65 dBm (typical) @ 54 Mbps • 802.11b: -83 dBm (typical) @ 11 Mbps • 802.11g: -65 dBm (typical) @ 54 Mbps • 802.11n (2.4GHz): -61 dBm (typical) @ 450 Mbps • 802.11n (5GHz): -61 dBm (typical) @ 450 Mbps • 802.11ac: -54 dBm (typical) @ 1300 Mbps	• 802.11a: -70 dBm (typical) @ 54 Mbps • 802.11b: -85 dBm (typical) @ 11 Mbps • 802.11g: -72 dBm (typical) @ 54 Mbps • 802.11n (2.4 GHz): -67 dBm (typical) @ 400 Mbps • 802.11n (5 GHz): -67 dBm (typical) @ 400 Mbps • 802.11ac: -64 dBm (typical) @ 867 Mbps	• 802.11a: -75 dBm (typical) @ 54Mbps • 802.11b: -90 dBm (typical) @ 11Mbps • 802.11g: -77 dBm (typical) @ 54Mbps • 802.11n (2.4 GHz): -77 dBm (typical) @ 400Mbps • 802.11n (5 GHz): -71 dBm (typical) @ 400Mbps • 802.11ac: -71 dBm (typical) @ 867 Mbps • 802.11ax (2.4GHz): -65 dBm (typical) @ 574Mbps • 802.11ax (5GHz): -63 dBm (typical) @ 1201Mbps
Power	• IEEE 802.3af Type 1 PoE PD Class 3 • Input: 100 - 240V AC, 50/60Hz, Output: 12V DC, 1A external power adapter (optional)	• IEEE 802.3at Type 2 PoE PD Class 4 • Input: 100 - 240V AC, 50/60Hz, Output: 12V DC, 1.5A external power adapter (optional)	• IEEE 802.3at Type 2 PoE PD Class 4 • Input: 100 - 240V AC, 50/60Hz, Output: 12V DC, 2A external power adapter (optional)	• IEEE 802.3at Type 2 PoE PD Class 4 • Input: 100 - 240V AC, 50/60Hz, Output: 12V DC, 1.5A external power adapter (optional)

	• Max. consumption: 8W	• Max. consumption: 12.95W	• Max. consumption: 18.96W	• Max. consumption: 15W
	TEW-821DAP (2.0R) AC1200	**TEW-825DAP (1.0R) AC1750**	**TEW-826DAP (1.0R) AC2200**	**TEW-921DAP (1.0R) AX1800**
Operating Temperature	0° – 40°C (32° - 104°F)			
Operating Humidity	Max. 95% non-condensing			
Dimensions	163 x 165 x 44 mm (6.4 x 6.5 x 1.7 in.)	187 x 187 x 46 mm (7.3 x 7.3 x 1.8 in.)	214 x 214 x 36mm (8.4 x 8.4 x 1.4 in.)	160 x 160 x 34mm (6.3 x 6.3 x 1.34 in.)
Weight	372g (13.1 oz.)	416g (14.7 oz.)	684g (1.51 lbs.)	486g (1.07 lbs.)
Certifications	CE	N/A	N/A	CE
	FCC			
	IC	N/A	IC	N/A
Warranty	3-Year			
Package Contents	Newtork cable (1.5m / 5 ft.)			
	Quick Installation Guide			
	Mounting plate/cable guard	Mounting plate	Mounting plate/cable guard	Mounting plate
	Power adapter (12V DC/1A)	Power adapter (12V DC/1.5A)	Power adapter (12V DC/2A)	N/A

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

**Due to regulatory requirements, the wireless channels specified cannot be statically assigned, but will be available within the available wireless channels when set to auto.

All references to speed are for comparison purposes only. Product specifications, size, and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.

Wireless Access Point Software Specifications

<table>
<tr><th></th><th>TEW-821DAP (2.0R)
AC1200</th><th>TEW-825DAP (1.0R)
AC1750</th><th>TEW-826DAP (1.0R)
AC2200</th><th>TEW-921DAP (1.0R)
AX1800</th></tr>
<tr><td>Standards</td><td>• IEEE 802.3
• IEEE 802.3u
• IEEE 802.3x
• IEEE 802.3ab
• IEEE 802.3af
• IEEE 802.1Q
• IEEE 802.11a
• IEEE 802.11b
• IEEE 802.11g
• IEEE 802.11n (up to 300 Mbps)
• IEEE 802.11ac Wave 2 (up to 867 Mbps)</td><td>• IEEE 802.1Q
• IEEE 802.3
• IEEE 802.3u
• IEEE 802.3x
• IEEE 802.3ab
• IEEE 802.3at
• IEEE 802.11a
• IEEE 802.11b
• IEEE 802.11g
• IEEE 802.11n (up to 450 Mbps)
• IEEE 802.11ac (up to 1300 Mbps)</td><td>• IEEE 802.3
• IEEE 802.3u
• IEEE 802.3x
• IEEE 802.3ab
• IEEE 802.3at
• IEEE 802.1Q
• IEEE 802.11a
• IEEE 802.11b
• IEEE 802.11g
• IEEE 802.11n (up to 400Mbps @ 256QAM)
• IEEE 802.11ac Wave 2 (5GHz1: up to 867Mbps, 5GHz2: up to 867Mbps @ 256QAM)</td><td>• IEEE 802.3
• IEEE 802.3u
• IEEE 802.3x
• IEEE 802.3ab
• IEEE 802.3at
• IEEE 802.1Q
• IEEE 802.11a
• IEEE 802.11b
• IEEE 802.11g
• IEEE 802.11k
• IEEE 802.11n (up to 400Mbps)*
• IEEE 802.11r
• IEEE 802.11v
• IEEE 802.11w
• IEEE 802.11ac Wave 2 (up to 867Mbps)*
• IEEE 802.11ax (up to 1201Mbps)*</td></tr>
<tr><td rowspan="10">Features</td><td colspan="3">N/A</td><td>802.11ax</td></tr>
<tr><td colspan="3">N/A</td><td>OFDMA</td></tr>
<tr><td>802.11ac MU-MIMO Wave 2</td><td>802.11ac</td><td colspan="2">802.11ac MU-MIMO Wave 2</td></tr>
<tr><td colspan="2">Concurrent Dual Band</td><td>Concurrent Tri-Band</td><td>Concurrent Dual Band</td></tr>
<tr><td colspan="4">Band Steering</td></tr>
<tr><td colspan="4">WiFi Traffic Shaping</td></tr>
<tr><td colspan="4">802.11Q VLAN assignment per SSID</td></tr>
<tr><td colspan="4">IPv6 support (Link-Local, Static IPv6, Auto-Configuration (SLAAC/DHCPv6))</td></tr>
<tr><td colspan="4">Multi-Language Interface: English, French, Spanish, German, Russian</td></tr>
<tr><td colspan="4">LEDs on/off</td></tr>
</table>

	Captive Portal (Local/External UAM user account authentication, redirect URL, and customizable portal page)		
	802.11k intelligent resource management		
	RSSI Threshold		
	Airtime Fairness		
Operation Modes	Access Point		
	Client Bridge		
	WDS AP		
	WDS Bridge		
	WDS Station		
	Repeater		
Management/Monitoring	• Web based management • Software Utility* • SNMP v1/v3	• STP (Spanning Tree Protocol) • Event Logging • Ping Test	• Traceroute • Telnet • Reboot & Scheduled Reboot
Access Control	• WEP • WPA-Personal (PSK) / Enterprise (RADIUS) • WPA2-Personal (PSK) / Enterprise (RADIUS)	• WPA3-Personal (SAE)** • OWE (Opportunistic Wireless Encryption)**	• MAC Address Filter • Wireless Client Limit
Quality of Service (QoS)	• 802.1p Class of Service (CoS) • DSCP (Differentiated Services Code Point)	• Bandwidth Control per port	• Queue Scheduling: Strict Priority, Weighted Round Robin (WRR)
QoS	WMM and Bandwidth control per SSID or client		
SSID	Up to 8 SSIDs per wireless band		
TRENDnet Hive Features*** https://www.trendnet.com/hive (Requires subscription purchase) (Click here to view list of Hive compatible devices)	• Configure, monitor, and manage through the TRENDnet Hive Cloud Management Portal remotely via PC or Mac web browser, or through the mobile app • Multi-device management	• Provisioning through scheduled batch firmware or configuration updates for multiple access points • Event/hardware network monitoring (CPU/memory utilization)	• Configure features such as IP address settings, WiFi settings, operation modes, and LED control through cloud management

*The software utility and wireless hardware controller (TEW-WLC100/WLC100P) are only compatible with TEW-821DAP, TEW-825DAP, TEW-826DAP access point models. The software utility works with Windows® 10, 8.1, 8, 7, Vista, XP, Windows® 2003/2008 Server OS. The software utility cannot be used when the device is connected to TRENDnet Hive.

**WPA3 and OWE security protocols are only supported on the TEW-921DAP access point model.

Limited Warranty

TRENDnet warrants only to the original purchaser of this product from a TRENDnet authorized reseller or distributor that this product will be free from defects in material and workmanship under normal use and service. This limited warranty is non-transferable and does not apply to any purchaser who bought the product from a reseller or distributor not authorized by TRENDnet, including but not limited to purchases from Internet auction sites.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service. Specific warranty periods are listed on each of the respective product pages on the TRENDnet website.

- AC/DC Power Adapter, Cooling Fan, and Power Supply carry a one-year warranty.

Limited Lifetime Warranty

TRENDnet offers a limited lifetime warranty for all of its metal-enclosed network switches that have been purchased in the United States/Canada on or after 1/1/2015.

- Cooling fan and internal power supply carry a one-year warranty

To obtain an RMA, the ORIGINAL PURCHASER must show Proof of Purchase and return the unit to the address provided. The customer is responsible for any shipping-related costs that may occur. Replacement goods will be shipped back to the customer at TRENDnet's expense.

Upon receiving the RMA unit, TRENDnet may repair the unit using refurbished parts. In the event that the RMA unit needs to be replaced, TRENDnet may replace it with a refurbished product of the same or comparable model.

In the event that, after evaluation, TRENDnet cannot replace the defective product or there is no comparable model available, we will refund the depreciated value of the product.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use, or (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation, a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. International customers

shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

Refurbished product: Refurbished products carry a 90-day warranty after date of purchase. Please retain the dated sales receipt with purchase price clearly visible as evidence of the original purchaser's date of purchase. Replacement products may be refurbished or contain refurbished materials. If TRENDnet, by its sole determination, is unable to replace the defective product, we will offer a refund for the depreciated value of the product.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Visit http://www.trendnet.com/gpl or the support section on http://www.trendnet.com and search for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please visit http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP07172015v3 2021/09/13

TRENDnet®

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at http://www.trendnet.com/register

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA