Manage Customer Networks in MSP Mode

MSP (Managed Service Provider) mode allows you to know the status of your customers at a glance, and manage customers in the Omada platform.

- **Customer Monitoring**

  Keep you informed of accurate, real-time status of every customer.

- **Customer Management**

  Manage all customers to deploy the whole network.

- **Account Settings**

  Manage all administrative accounts.

This guide will introduce how to enable MSP mode and manage customer networks in MSP view.

CONTENTS

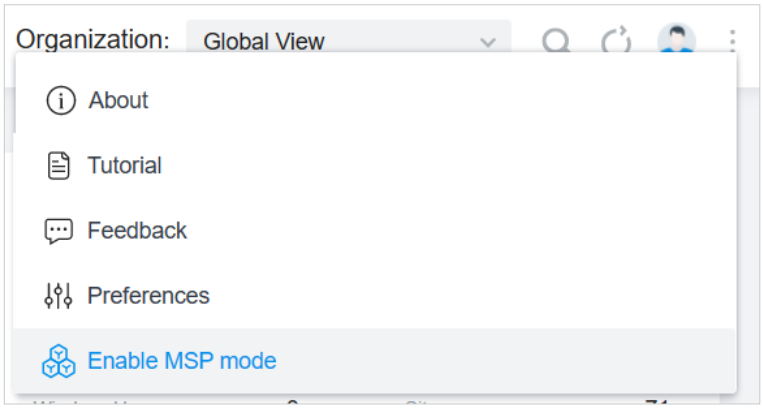
Chapter 1 Quick Start

1. 1 Enable the MSP Mode

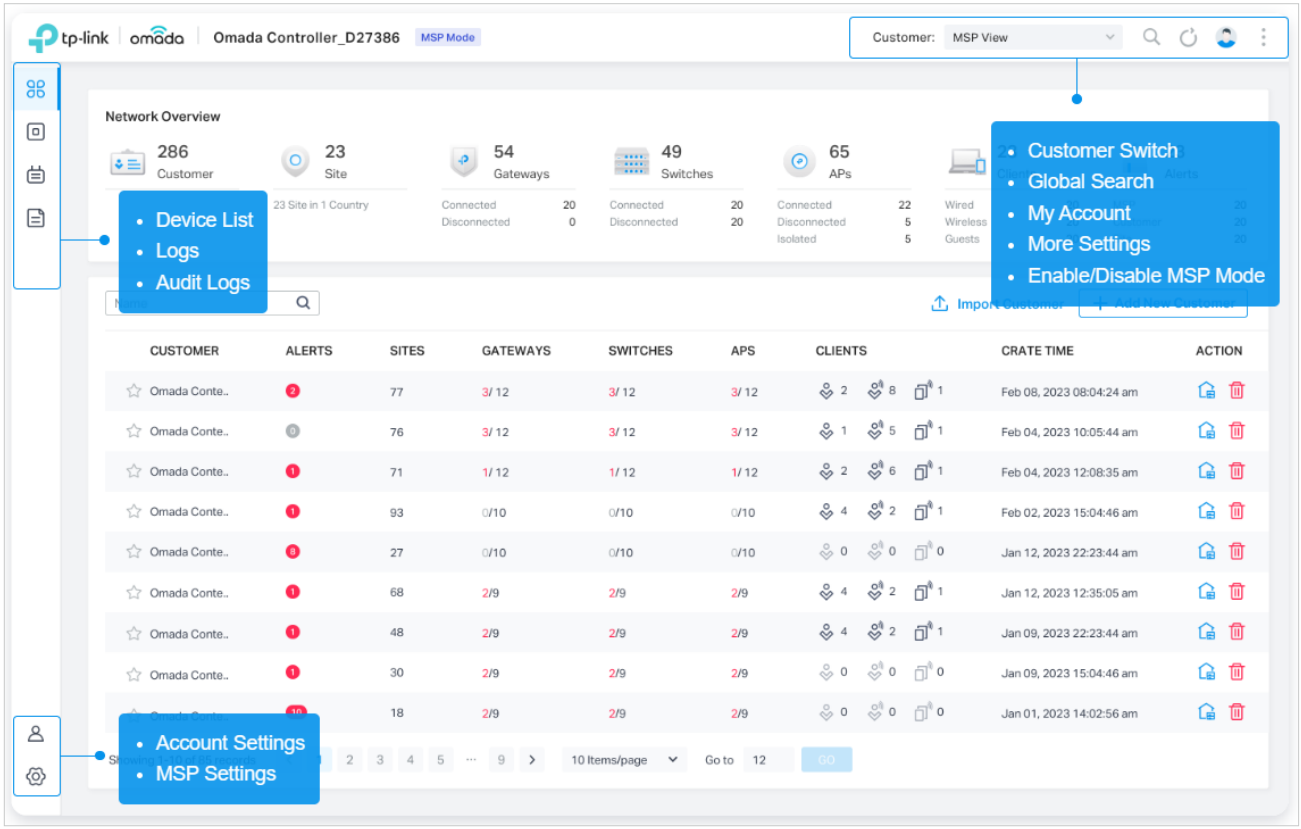
1. Launch your controller.
2. In Global View, click ⋮ in the top-right corner and click Enable MSP mode. In the dialog box that pops up, confirm the operation.

Note:

Enabling or disabling MSP mode may cause problems on the connected Cloud access page. In this case, re-enter the web page.



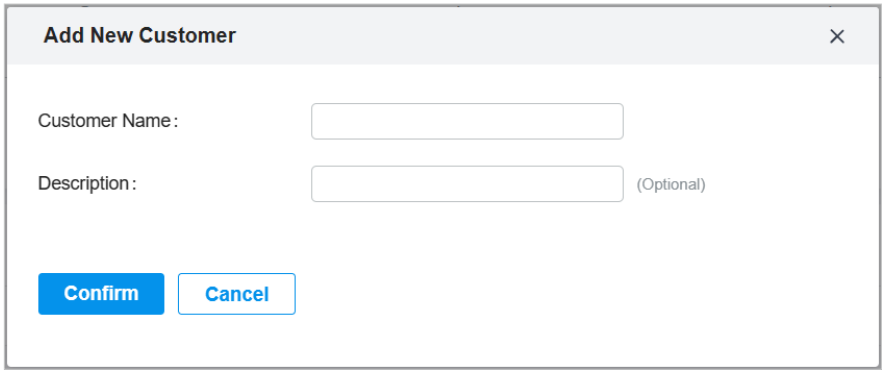
You will enter the MSP view.



1. 2 Add and Manage Customers

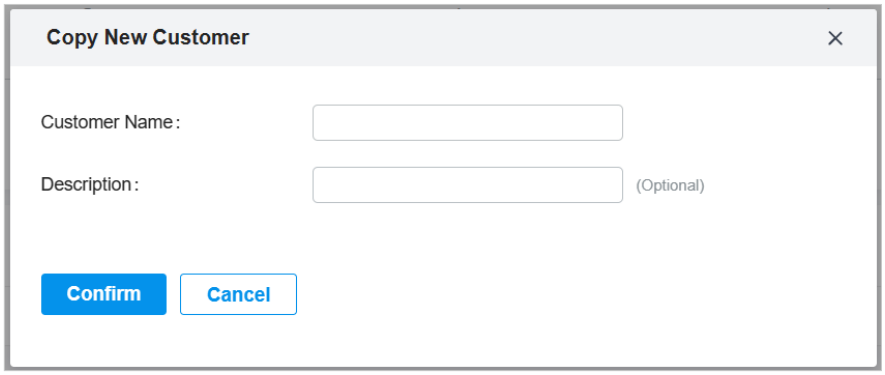
1. In MSP View, go to the Customer page.
2. Add customers by using one of the following methods:
   - **Add a new customer**

     Click Add New Customer above the customer list. Specify the customer name and enter a description. Then save the settings.



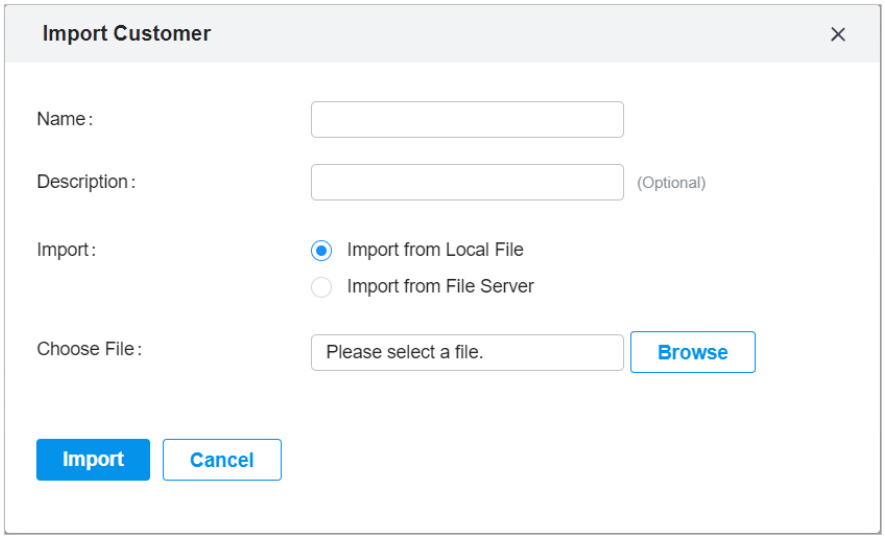
   - **Copy an existing site**

     Click the icon of a customer entry. Specify the customer name and enter a description. Then save the settings.



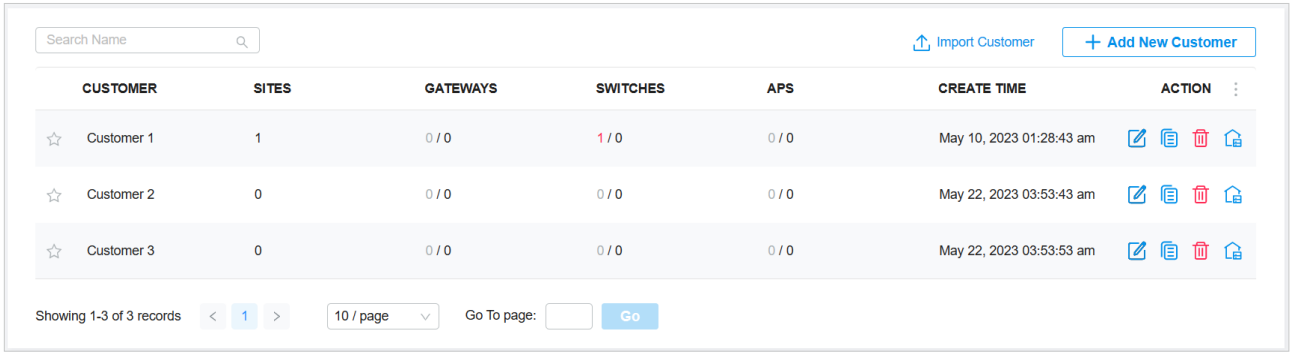
- **Import customers from another controller**

  Click Import Customer above the customer list. Specify the customer name and enter a description. Determine whether to retain device info according to your needs. Then import customer from a local file or from a file server.



3. The new customers will be added to the customer list and the drop-down list of Customers.

   In the customer list, you can view the customer information, and click the icons in the ACTION column to edit, copy, delete and launch the controller of each customer.

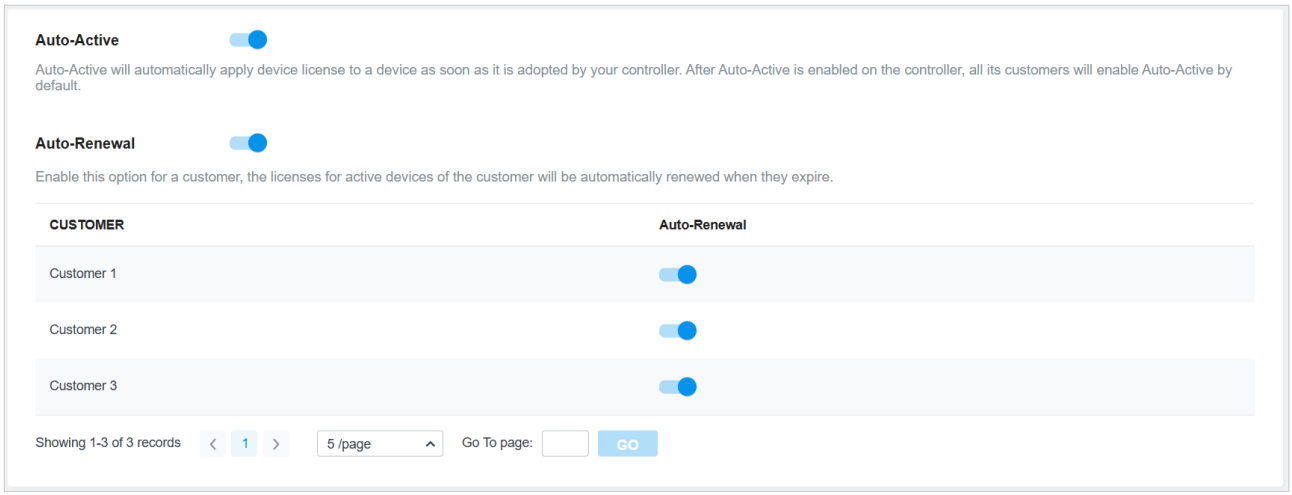


1. 3 Assign and Manage Licenses

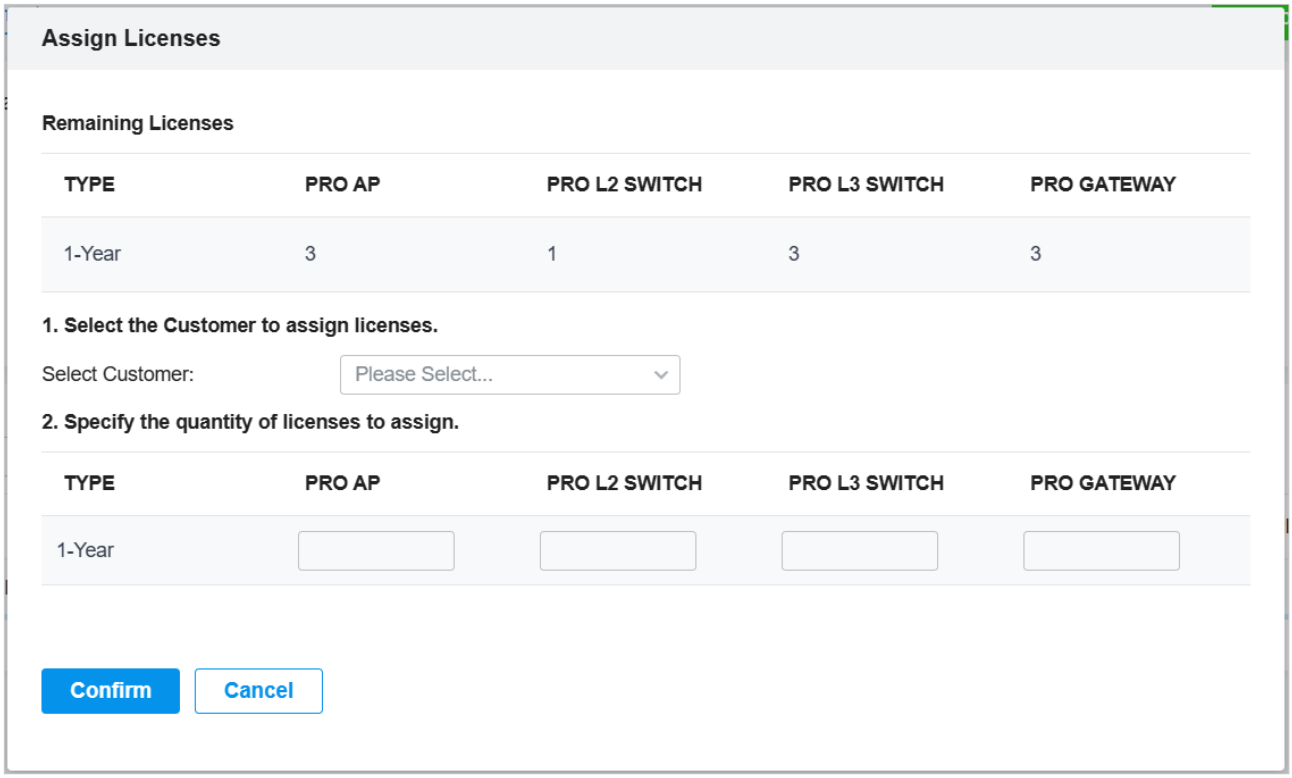
1. In MSP View, go to the License page.
2. Go to License > Licenses. Enable Auto-Active and Auto-Renewal if needed.

   Auto-Active will automatically apply device license to a device as soon as it is adopted by your controller. After Auto-Active is enabled on the controller, all its customers will enable Auto-Active by default.

When Auto-Renewal is enabled for a customer, the licenses for active devices of the customer will be automatically renewed when they expire.



3. Go to License > License Assignment, and click Assign Licenses. Select the customer and assign licenses.



After license assignment, you can click Revoke Licenses and select a customer to revoke licenses in case needed.

1. 4 Add Sites and Devices

1. Select a customer from the drop-down list of Customers in the top-right corner.

2. Add sites and adopt devices by referring to "Chapter 3 Manage Omada Managed Devices and Sites" of the ***Omada SDN Controller User Guide***, which can be found at https://www.tp-link.com/support/download/omada-software-controller/.

   You can also add devices on the Devices page in MSP View.

Chapter 2 Add and Manage Accounts

2. 1 Configure Role Settings

The system offers two types of roles:

- **MSP Role:** for manage settings in MSP view.
- **Customer Role:** for manage settings in global and site views.

Each role type has three default levels of access permissions: **Main Administrator**, **Administrator**, and **Viewer**. You can also create new account roles and customize their permissions to access different features.

- **Main Administrator**

  The Main Administrator has access to all features in the corresponding view.

  The account who first launches the controller will be the Main Administrator.

- **Administrator**

  Administrators have access to most features in the corresponding view except for some modules. For example, they have no permission to system migration and data auto-backup and have view-only permission to system license management and custom account roles.

- **Viewer**

  Viewers can view the status and settings of some features in the corresponding view.

- **Custom roles**

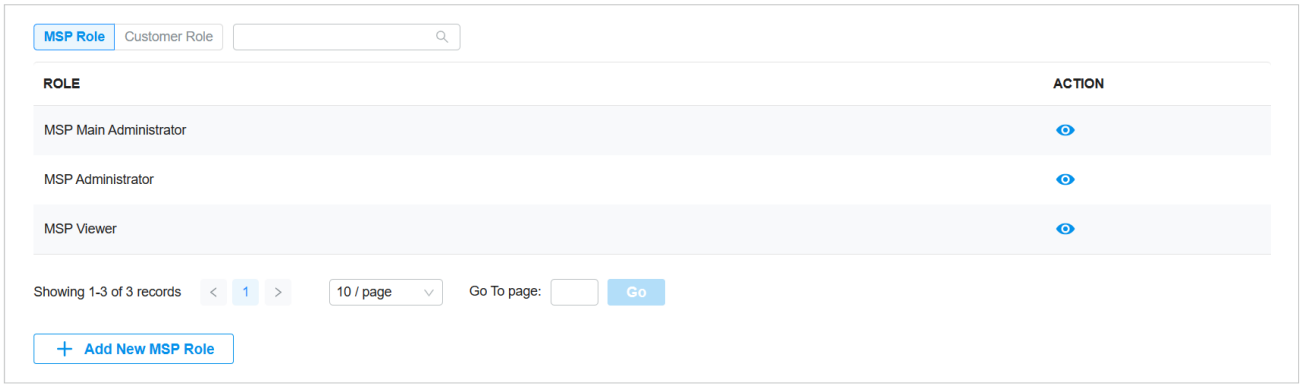
  Custom roles can be configured to access different features in the corresponding view.

Note:

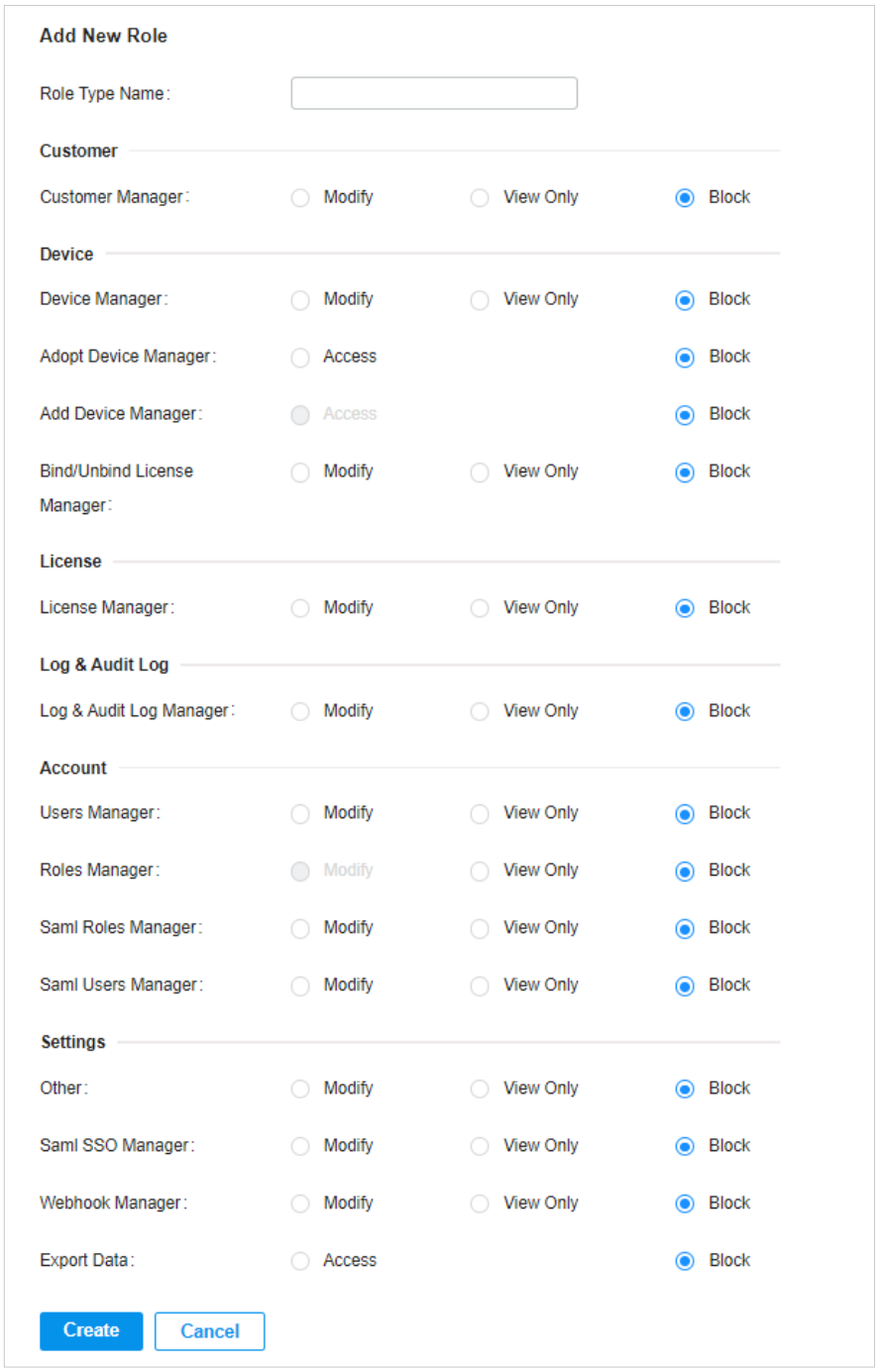
Please upgrade Omada APP to version 4.6 or later, otherwise you may not be able to log in with the accounts bound with customized roles.

To add a custom role, follow the steps below:

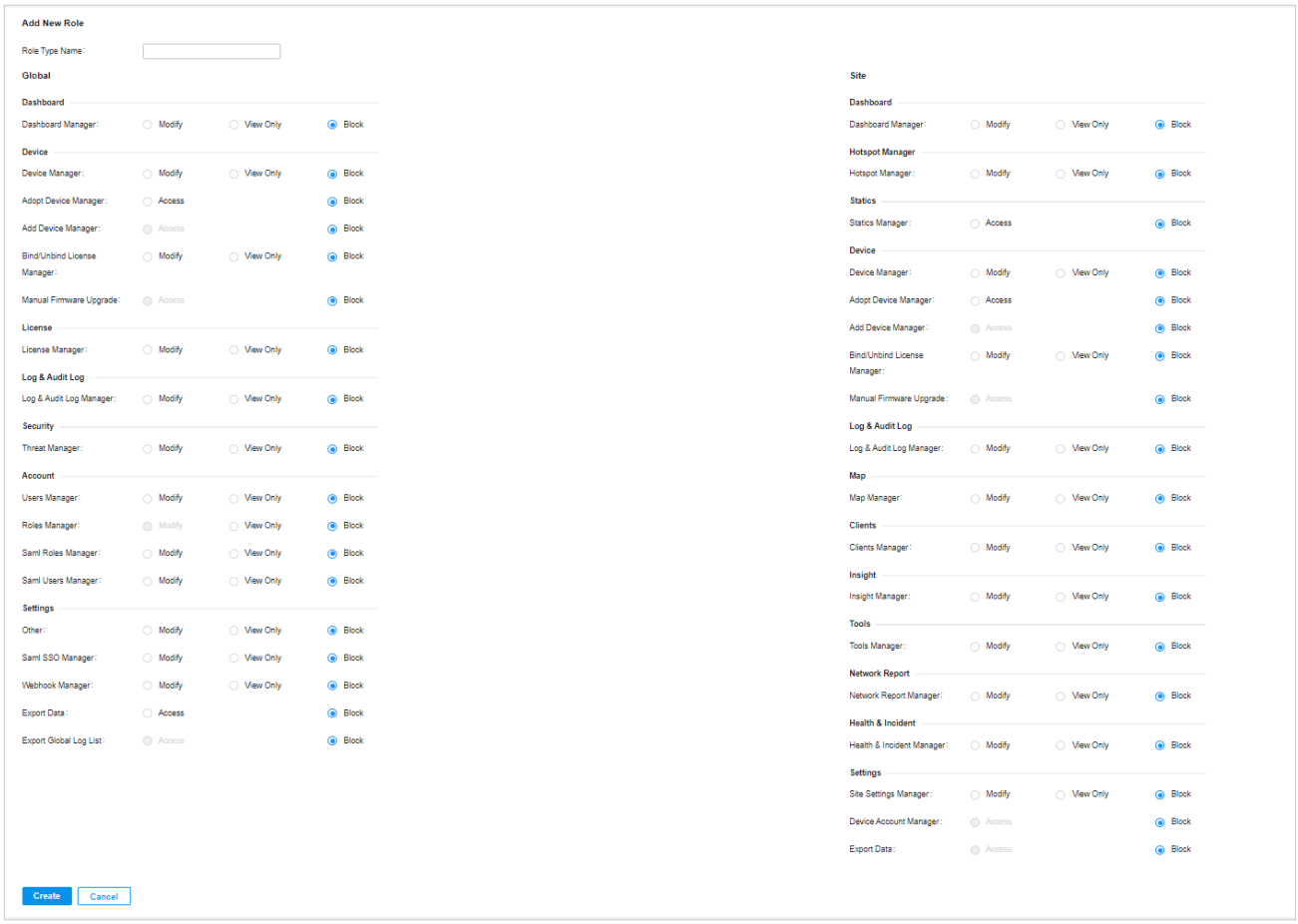
1. In MSP View, go to Account > Role.



2. On the MSP Role page, click Add New MSP Role. Specify the role type name and customize the permissions for the role. MSP roles are used for manage settings in MSP view.



3. On the Customer Role page, click Add New Customer Role. Specify the role type name and customize the permissions for the role. Customer roles are used for manage settings in global view and site view.

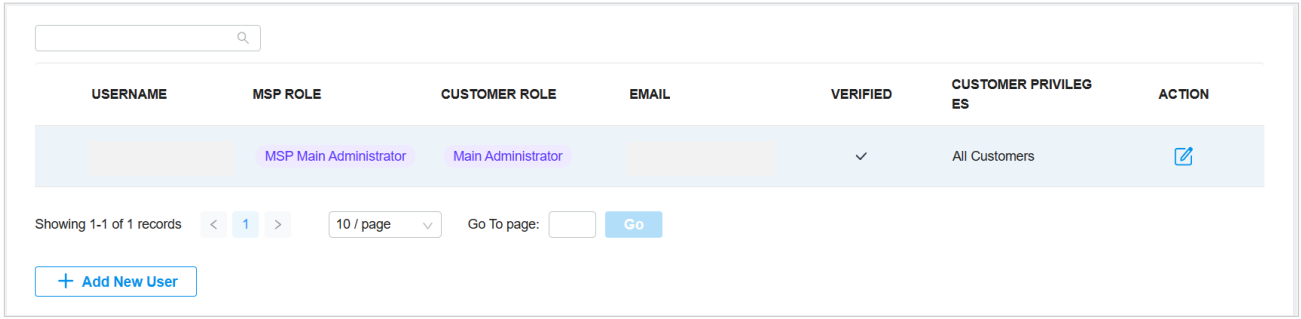


2. 2 Manage the Main Administrator Account

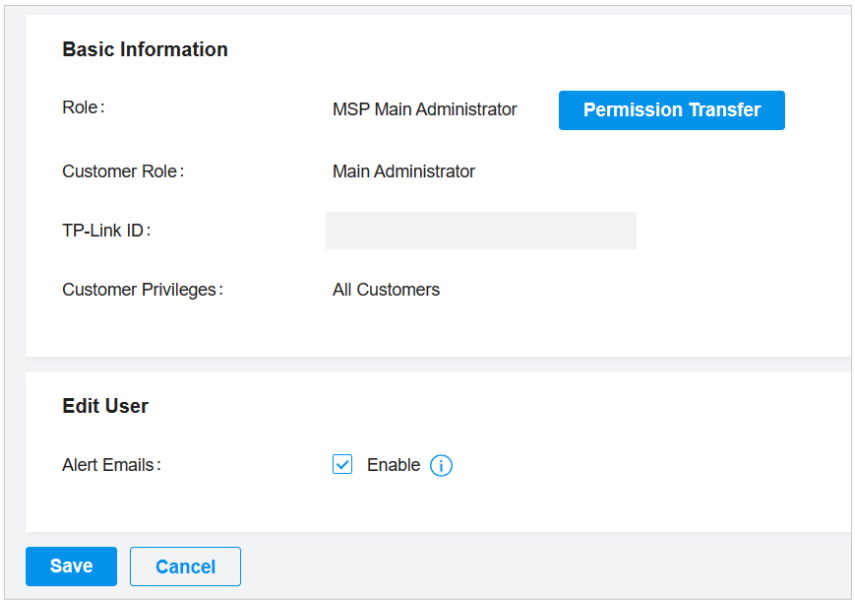
The account who first launches the controller will be the MSP Main Administrator (for managing settings in MSP View) and Main Administrator (for managing settings in Global View and Site View).

To edit the account settings, follow the steps below:

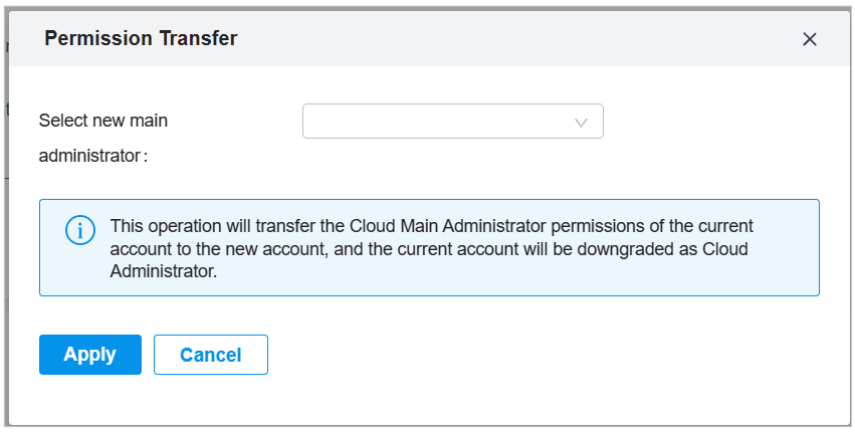
1. In MSP View, go to Account > User.



2. Click the Edit icon to change settings. You can enable Alert Emails if you want this account to receive emails about alerts.



3. If you want to transfer the permissions to another account, click Permission Transfer and specify the new account.

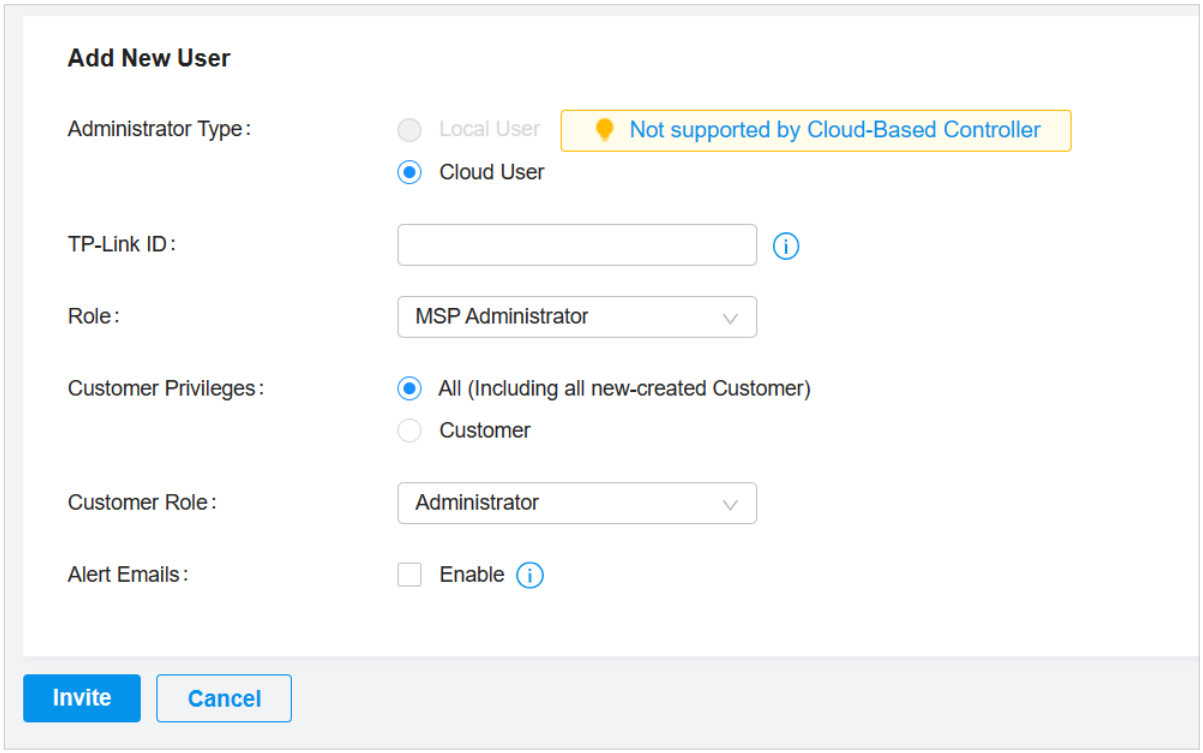


2. 3 Add New MSP User Accounts

To create and manage a local user account, follow these steps:

1. In MSP View, go to Account > User.

2. Click Add New User. Specify the parameters and click Invite.



Administrator Type	Specify whether to add a local user or cloud user. Local user is not supported by the cloud-based controller.
TP-Link ID	Enter an email address to send the invitation email. If the email address is already registered with a TP-Link ID, it will become a valid cloud user account after accepting the invitation. If not, it will be invited for registration, and automatically becomes a valid cloud user account after finishing the registration.
Role	Select a role for the user account. MSP Administrator: This role has access to most features in MSP View except for some modules. MSP Viewer: This role can view the status and settings of some features. Custom MSP roles: If you have created custom MSP roles, they will be displayed in the list.
Customer Privileges	Assign the customer permissions to the user account. All: The created user has device permissions of all customers, including all newly created ones. Customer: The created user has device permissions of only the customers you specify.

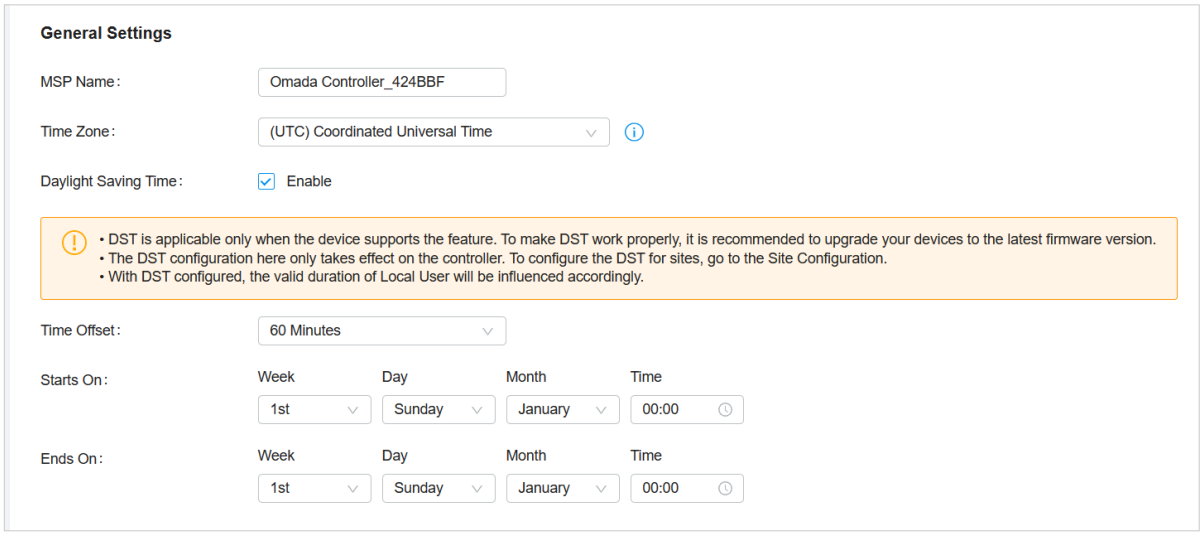
Customer Role	Administrator: Compared with the Customer Main Administrator, Customer Administrators have no permission to some modules in Global View and Site View, mainly including cloud access, migration, auto-backup and global view logs. They have read-only permission to some modules in Global View and Site View, such as license management and custom account roles. Viewer: Customer Viewers can view the status and settings of the network, and change the settings in Hotspot Manager. Custom Customer roles: If you have created custom Customer roles, they will be displayed in the list.
Alert Emails	Check the box if you want the created user to receive emails about alerts of the privileged customers.

Chapter 3 Manage System Settings

3. 1 Configure MSP Settings

3.1.1 General Settings

1. In MSP View, go to Settings > MSP Settings.
2. In General Settings, configure the parameters and save the settings.



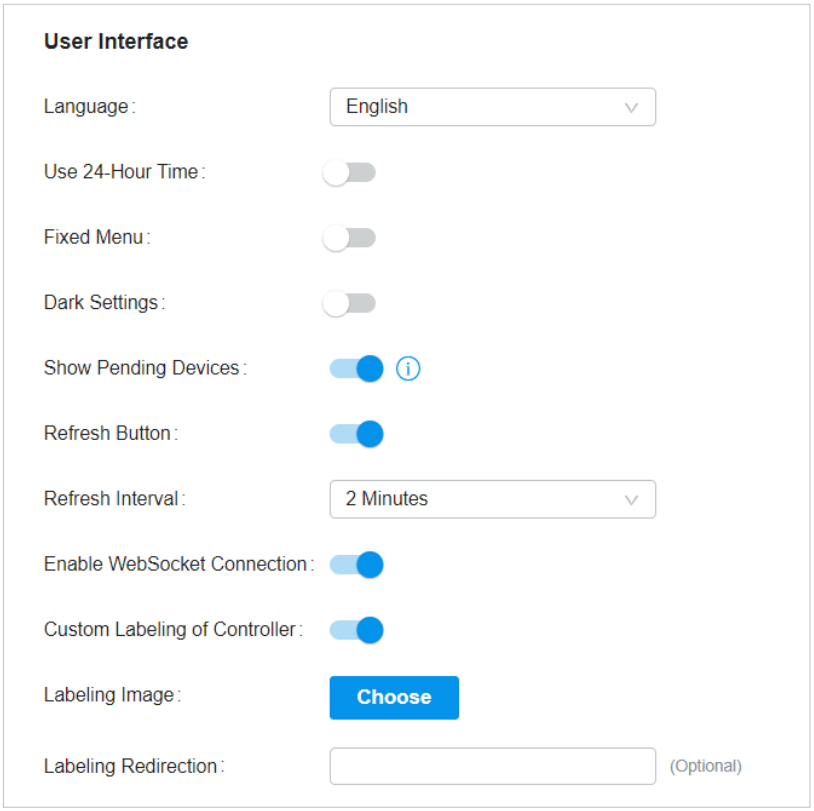
MSP Name	Specify a name to identify the controller.
Time Zone	Select the time zone of the controller according to your region. The time of the controller settings and statistics is displayed based on the time zone.

Daylight Saving Time	Enable the feature and configure the parameters if your country/region implement DST. Time Offset: Specify the time added in minutes when Daylight Saving Time starts. Starts On: Specify the time when the DST starts. The clock will be set forward by the time offset you specify. Ends On: Specify the time when the DST ends. The clock will be set back by the time offset you specify.

3.1.2 User Interface

You can customize the User Interface settings of the controller according to your preferences.

1. In MSP View, go to Settings > MSP Settings.
2. In User Interface, configure the parameters and save the settings.



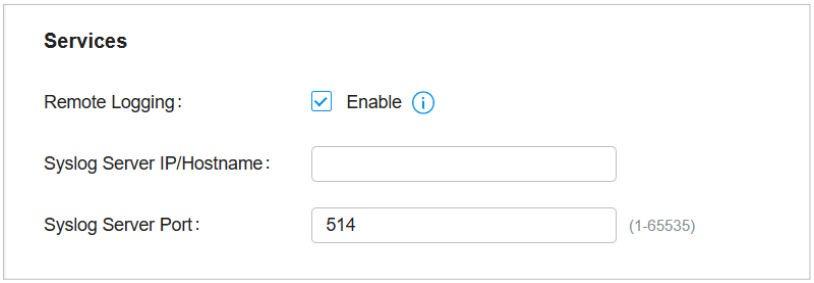
Language	Select the language to display the user interface.
Use 24-Hour Time	With Use 24-Hour Time enabled, time is displayed in a 24-hour format. With Use 24-Hour Time disabled, time is displayed in a 12-hour format.
Fixed Menu	With Fixed Menu enabled, the menu icons are fixed and do not prompt menu texts when your mouse hovers on them.

Dark Settings	When enabled, the system will switch to a dark theme.
Show Pending Devices	With this option enabled, the devices in Pending status will be shown, and you can determine whether to adopt them. With this option disabled, they will not be shown, thus you cannot adopt any new devices.
Refresh Button	Enable or disable Refresh Button in the upper right corner of the configuration page.
Refresh Interval	Select how often the controller automatically refreshes the data displayed on the page.
Enable WebSocket Connection	With this function enabled, the controller updates in real time some part of its data on the web interface, which is transmitted using the WebSocket service, so that you don't need to refresh them manually.
Custom Labeling of Controller	With this function enabled, you can upload your controller labeling and define the redirection URL.

3.1.3 Configure Remote Logging

With Remote Logging configured, the controller will send generated system logs to a log server.

1. In MSP View, go to Settings > MSP Settings.
2. In Services, enable Remote Logging, configure the parameters and save the settings.



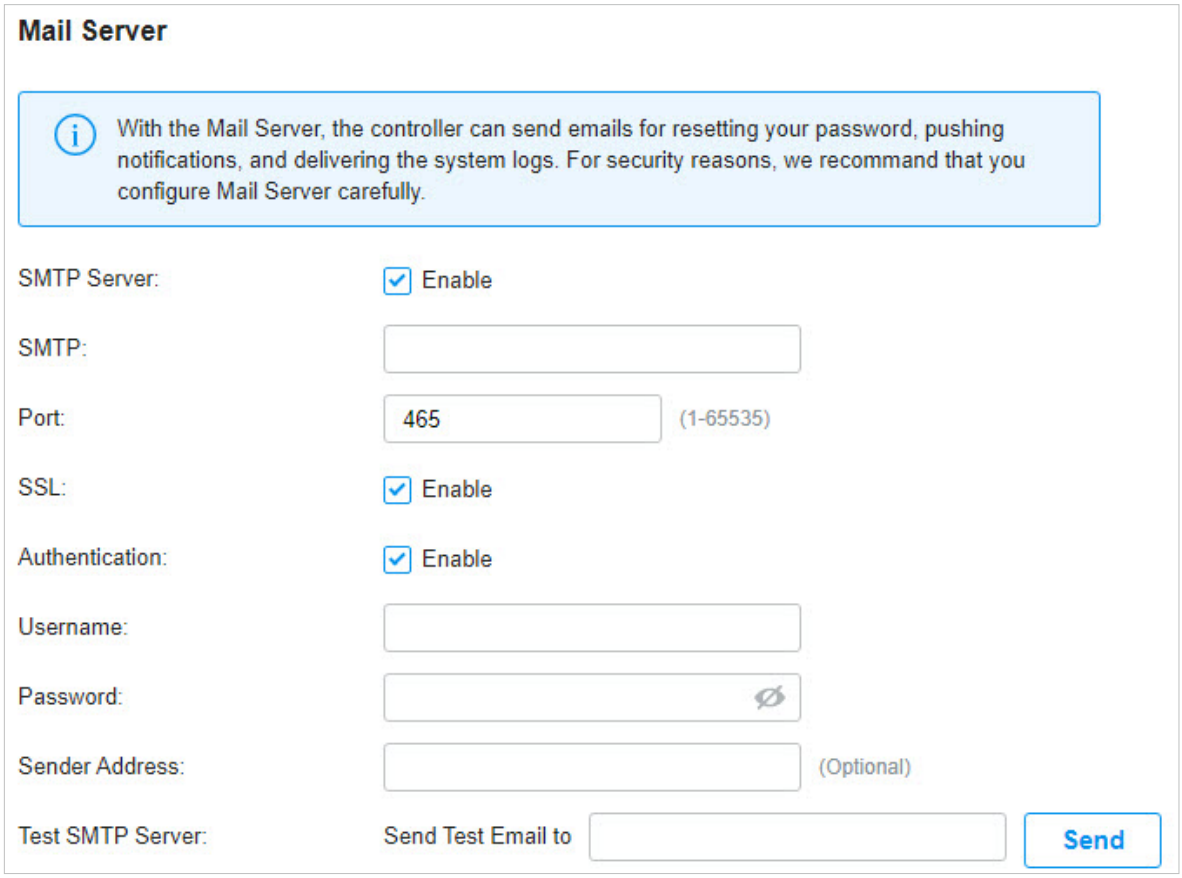
Syslog Server IP/Hostname	Enter the IP address or hostname of the syslog server.
Syslog Server Port	Enter the port of the syslog server.

3.1.5 Configure the Mail Server

With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. The Mail Server feature works with the SMTP (Simple Mail Transfer Protocol) service provided by an email service provider.

1. Log in to your email account and enable the SMTP (Simple Mail Transfer Protocol) Service. For details, refer to the instructions of your email service provider.

2. In MSP View, go to Settings > MSP Settings.
3. In Mail Server, enable SMTP Server and configure the parameters. Then save the settings.



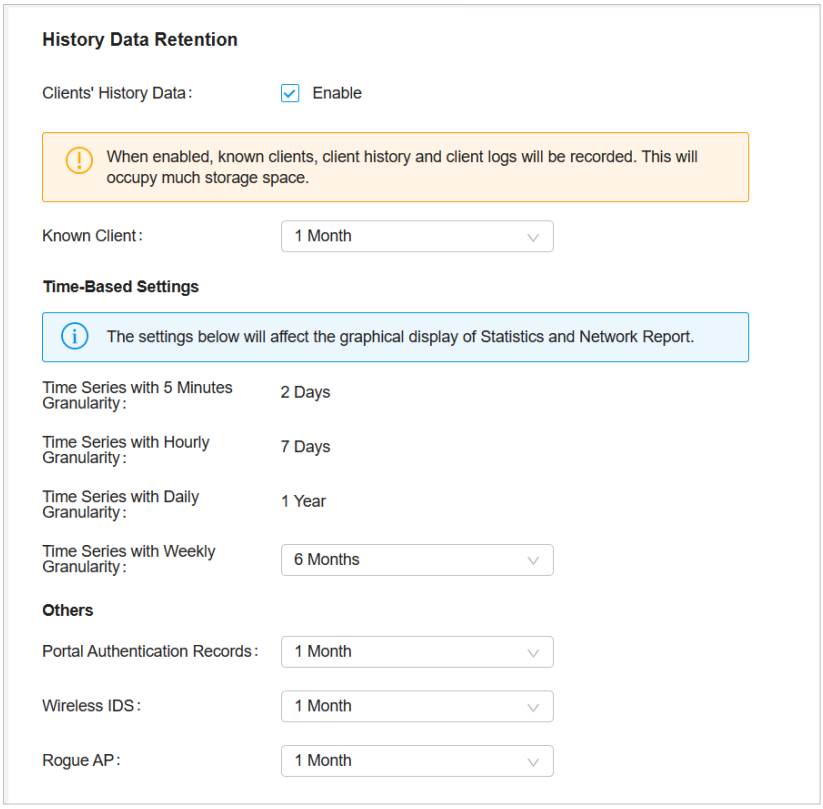
SMTP	Enter the URL or IP address of the SMTP server according to the instructions of the email service provider.
Port	Configure the port used by the SMTP server according to the instructions of the email service provider.
SSL	Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller and the SMTP server.
Authentication	Enable or disable Authentication according to the instructions of the email service provider. If Authentication is enabled, the SMTP server requires the username and password for authentication. Username: Enter your email address as the username. Password: Enter the authentication code as the password, which is provided by the email service provider when you enable the SMTP service.
Sender Address	Specify the sender address of the email. If you leave it blank, the controller uses your email address as the Sender Address.

Test SMTP Server	Test the Mail Server configuration by sending a test email to an email address that you specify.

3.1.6 History Data Retention

With History Data Retention, you can specify how the controller retains its data.

1. In MSP View, go to Settings > MSP Settings.
2. In History Data Retention, configure the parameters and save the settings.



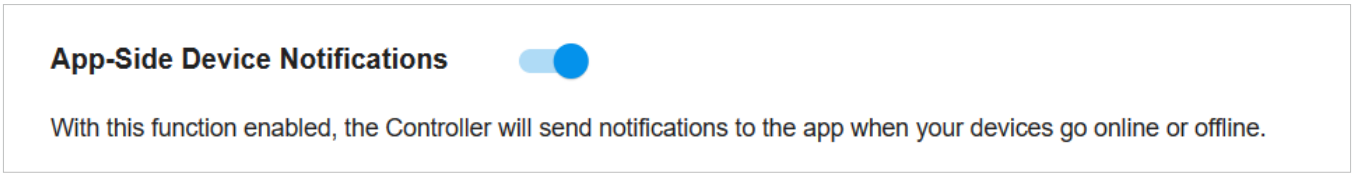
Clients' History Data	When enabled, known clients, client history and client logs will be recorded. This will occupy much storage space.
Known Client	Specify the retention time of known client data.
Time Series with 5 Minutes Granularity	Displays the retention time of AP, switch, gateway, and client data. Corresponding to 5-minute statistics.
Time Series with Hourly Granularity	Displays the retention time of AP, switch, gateway, and client data. Corresponding to hourly statistics.
Time Series with Daily Granularity	Specify the retention time of AP, switch, gateway, and client data. Corresponding to daily statistics.
Time Series with Weekly Granularity	Specify the retention time of client data. Corresponding to weekly statistics.

Portal Authentication Records	Specify the retention time of portal authorization records. Corresponding to Insight-Past Portal Authorization.
Wireless IDS	Specify the retention time of wireless IDS data.
Rogue AP	Specify the retention time of scanned Rogue APs. Corresponding to Insight-Rogue APs.

3.1.7 App-Side Device Notifications

With App-Side Device Notifications enabled, the Controller will send notifications to the app when your devices go online or offline.

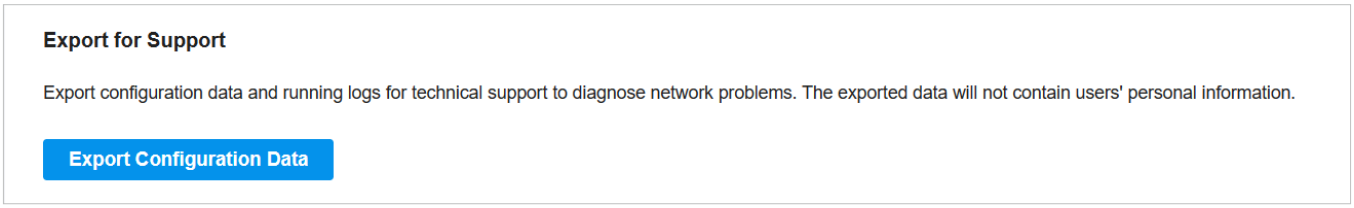
1. In MSP View, go to Settings > MSP Settings.
2. In App-Side Device Notifications, enable the feature and save the settings.



3. 2 Export for Support

You can export configuration data for technical support to diagnose network problems. The exported data will not contain users' personal information.

1. In MSP View, go to Settings > Maintenance.
2. Click Export Configuration Data to save the data file, then you can send it for technical support.

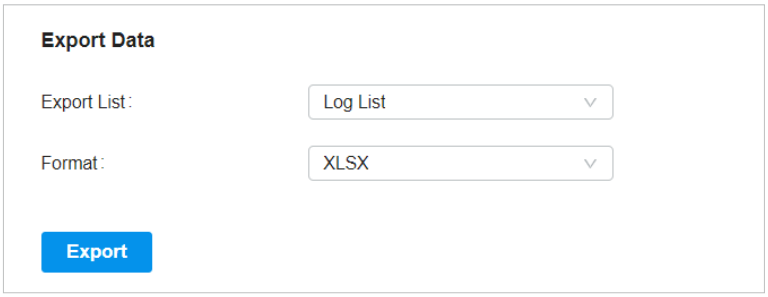


3. 3 Export Data

You can export data to monitor or debug your devices.

1. In MSP View, go to Settings > Export Data.

2. Configure the parameters and click Export.



Export List	Log List: Export the logs generated by the controller. Audit Log List: Export the audit logs generated by the controller.
Format	The data can be exported to the file in the format of .CSV or .XLSX.

3. 4 Platform Integration

3.4.1 Open API

Overview

Omada's Open API supports the REST API of most Controller services. This feature allows Omada users to write custom applications, embed APIs, or combine their own applications. The REST API supports HTTP GET and POST operations by providing specific URLs for each query, and the output of these operations is returned in JSON format.

To access the API securely, the Omada API framework supports the OAuth protocol for authentication and authorization, and supports the authorization code mode and client mode.

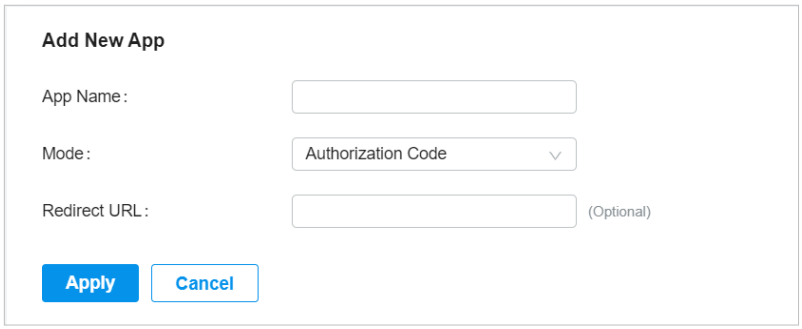
Access Token provides temporary and secure access to the API. For security reasons, Access Token has a limited lifespan. Access Token in authorization code mode uses the refresh API to obtain a new Access Token, and client mode obtains a new token through clientKey and clientSecret.

Configuration

1. In MSP View, go to Settings > Platform Integration > Open API.
2. Click Add New App.
3. Specify the App name, choose the access mode and configure the parameters.
   - **Authorization code mode**

   The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients. Since this is a redirection-based flow, the client must be capable

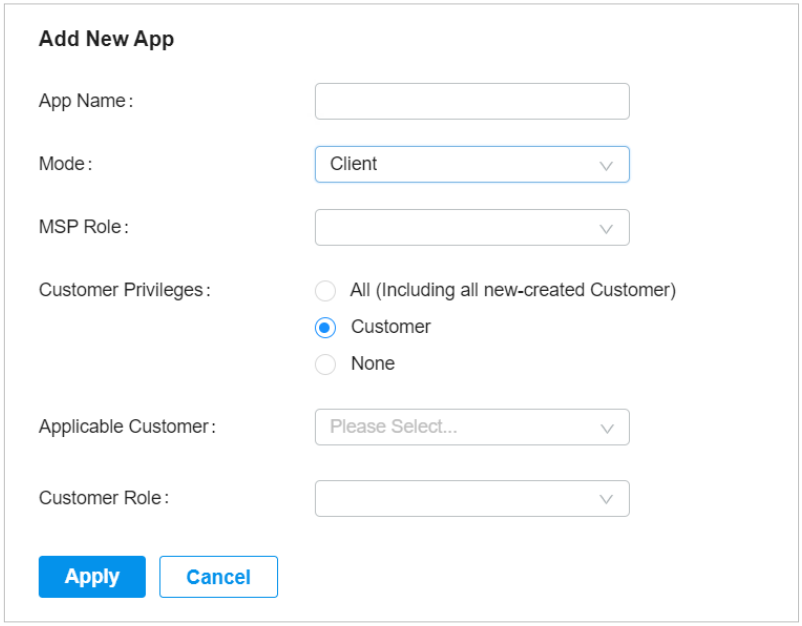
of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server.



Redirect URL	Specify the redirect URL for Oauth2.0 authorization flow.

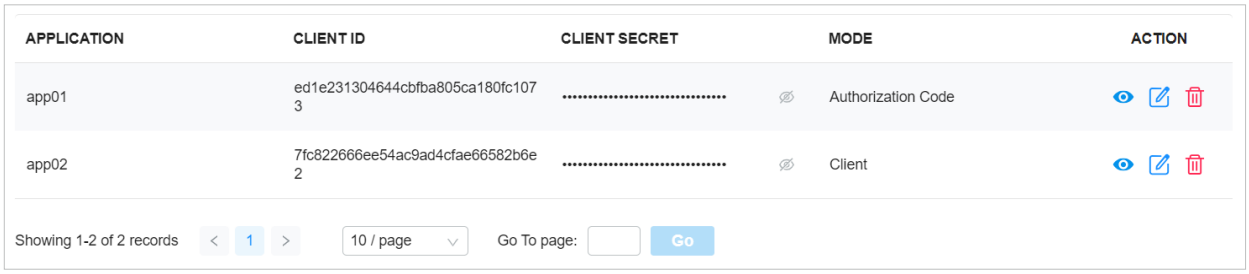
- **Client mode**

The client can request an access token using only its client credentials (or other supported means of authentication) when the client is requesting access to the protected resources under its control, or those of another resource owner that have been previously arranged with the authorization server (the method of which is beyond the scope of this specification).



MSP Role	Specify the authority MSP role of the client through the Open API.
Customer Privileges	Specify the customer privileges of the client through the Open API.
Applicable Customer	When Customer Privileges is set to Customer, select controllable customers.
Customer Role	Specify the authority customer role of the client through the Open API.

4. Apply the settings. The application will be added for Open API access.



You can click API Usage to monitor the API usage.

For more instructions, click Online API Document to get the Open API Access Guide.

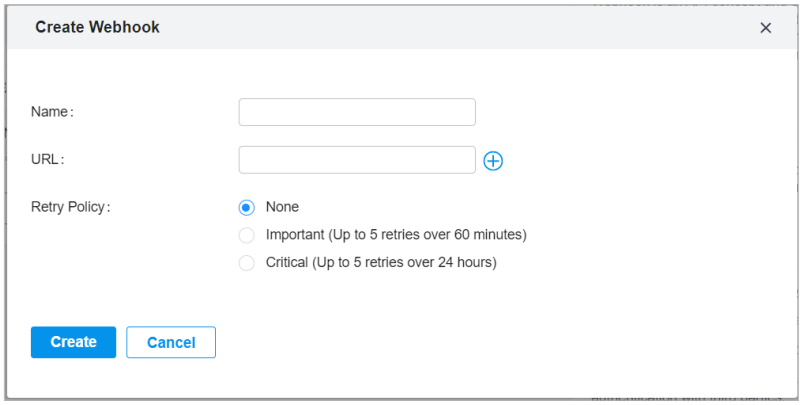
3.4.2 Webhooks

Overview

Webhook is an API concept and one of the usage paradigms of microservice APIs. It is also called a reverse API, that is, the front end does not actively send requests, but is completely pushed by the back end. In Omada, Webhook is used for the active push function of messages such as alerts.

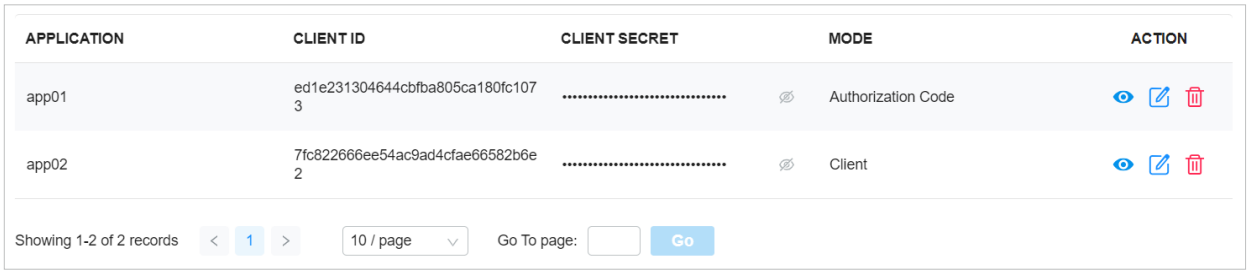
Configuration

1. In MSP View, go to Settings > Platform Integration > Webhooks.
2. Click Create New Webhook.



Name	Specify the Webhook entry name.
URL	Specify the Webhook URL address.
Retry Policy	Specify the Webhook retry policy: None (no retry), Important (up to 5 retries over 60 minutes), and Critical (up to 5 retries over 24 hours).

3. Save the settings. The webhook entry will be added.



You can click the icon in the ACTION column to test the connectivity, view the dispatch logs, and edit or delete the Webhook entry.

3. 5 SAML SSO

Overview

SAML (Security Assertion Markup Language) SSO (Single Sign On) enables clients to access multiple web applications using one set of login credentials. To complete the SAML SSO interconnection, the system administrator needs to configure the IdP (identity provider) information when the current system serves as the SP (service provider), or configure the SP information when the current system serves as the IdP.

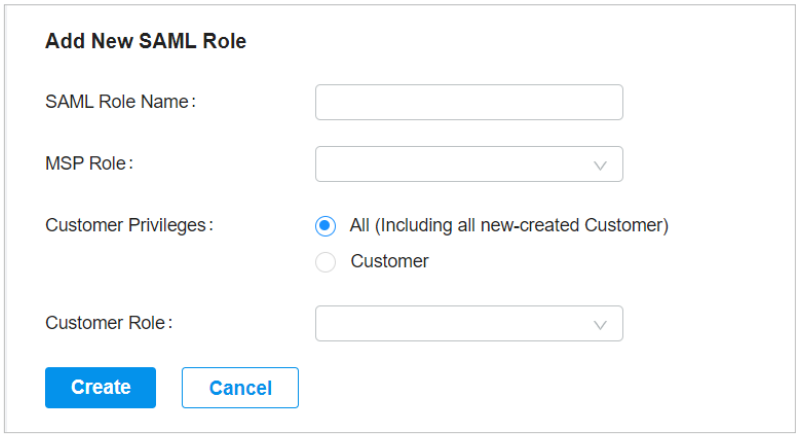
Prerequisites

- This chapter takes the configuration of the current system as an example to explain the operation. Other systems also need to be configured. SAML SSO works only after all systems are configured.
- If you need to connect with other systems that serve as the IdP, please obtain the metadata file of the IdP first, then configure the SP.
- If you need to connect with a third-party IdP, please configure the third-party IdP first and obtain its metadata file.

Configuration

1. Configure the SAML role.
   a. In MSP View, go to Account > SAML Role.

b. Click Add New SAML Role. Configure the parameters and click Create.



SAML Role Name	Specify the role name.
MSP Role	Specify the authority MSP role of the account.
Customer Privileges	Assign the customer permissions to the user account.
Customer Role	Specify the authority customer role of the account.

2. Configure the IdP.

Use a third-party system as the IdP and follow the steps below to configure the parameters:

a. Create an IdP. Fill in the initial information except the name.

b. Use the IdP metadata information for SP configuration on the Controller.

c. Edit the IdP information, including Entity ID, Sign-On URL, and Relay State.

Note:

- The above three parameters use the information of View SAML Attribute in SP configuration.
- Relay State is base64(resourceId_omadaId).

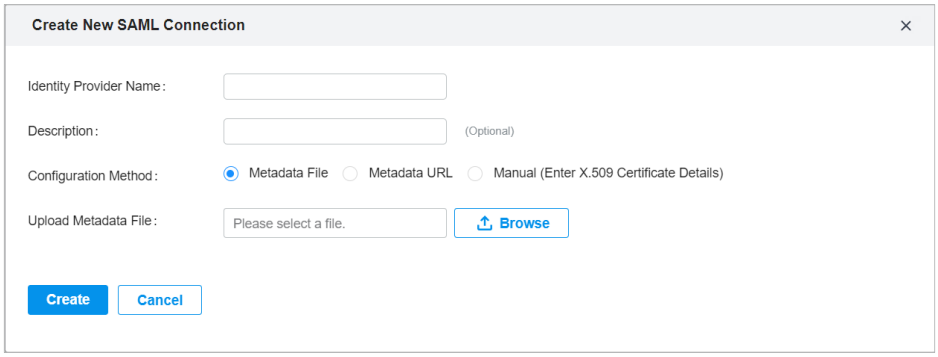
d. Edit the Attribute, and configure the username and usergroup_name.

3. Configure the SP.

Use the Controller as the SP and follow the steps below to configure the parameters:

a. In MSP View, go to Settings > SAML SSO.

b. Click Create New SAML Connection.



Identity Provider Name	Specify the IdP name.
Description	Enter a description for identification.
Configuration Method	Configure the metadata. You can upload the metadata file, use URL parsing, or manually fill in the information.

c. Click View SAML Attribute to view the SP configuration. This will be used for IdP configuration on the third-party system.

Subsequent Processing

After configuring all systems, verify whether the SAML SSO configuration is successful as follows:

1. In the configured IdP system, find the SP login entry and click to log in.
2. On the login page, enter the Username and Password to log in.
3. Go to the SP system and verify that the user has logged in.