Configure the Omada SDN Controller

Full version of Omada SDN Controller User Guide is available at **https://www.tp-link.com/support/download/omada-software-controller**

CONTENTS

1.Omada SDN Controller Solution Overview

2.Get Started with Omada SDN Controller

3.Configure the Omada SDN Controller

4.Manage Accounts of Omada SDN Controller

1

Omada SDN Controller Solution Overview

Omada SDN Controller Solution offers centralized and efficient management for configuring enterprise networks comprised of security gateways, switches, and wireless access points.

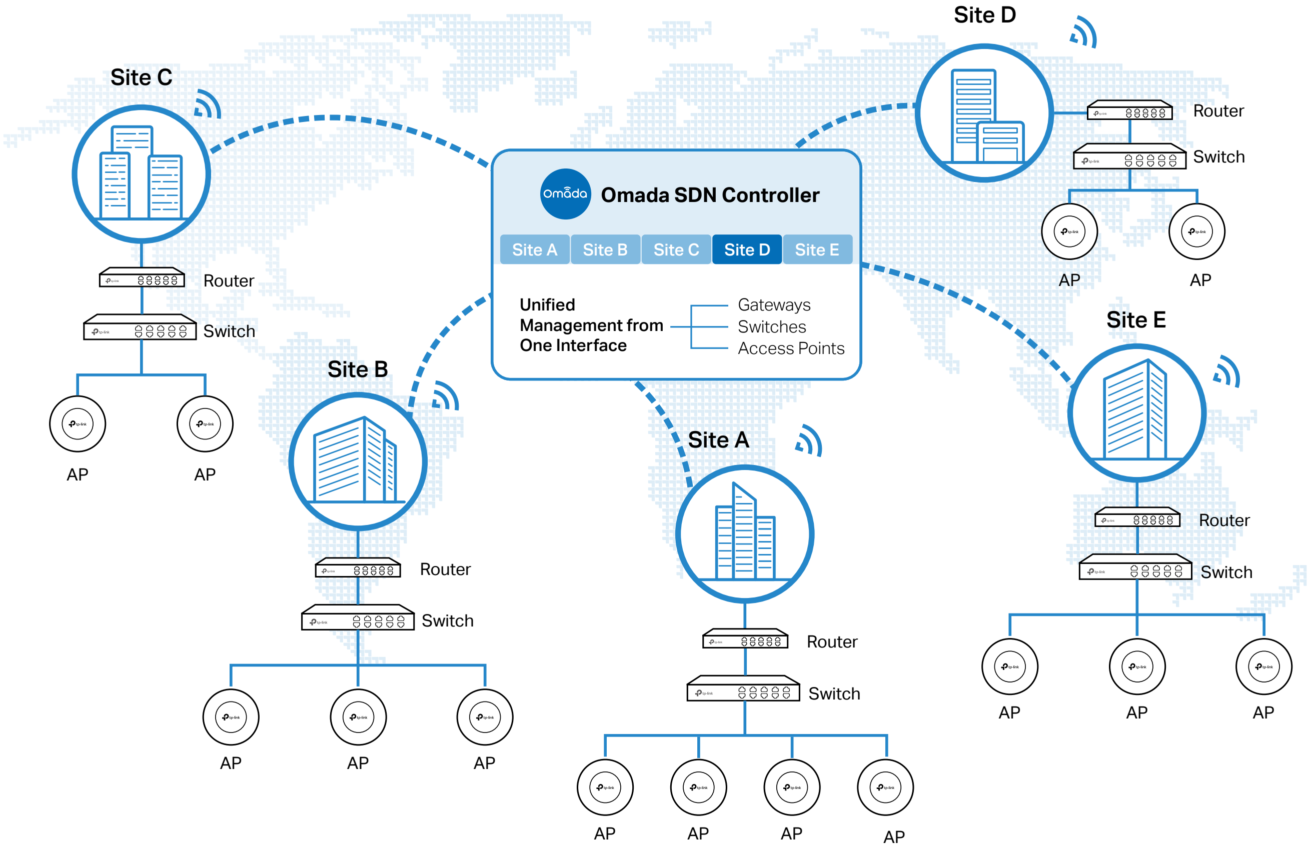
With a reliable network management platform powered by TP-Link Omada SDN Controller, you can develop comprehensive, software-defined networking across demanding, high-traffic environments with robust wired and wireless solutions.

The chapter includes the following sections:

1. 1 Overview of Omada SDN Controller Solution

Omada SDN Controller Solution is designed to provide business-class networking solutions for demanding, high-traffic environments such as campuses, hotels, malls, and offices. Omada SDN Controller Solution simplifies deploying and managing large-scale enterprise networks and offers easy maintenance, ongoing monitoring, and flexible scalability.

This figure shows a sample architecture of an Omada SDN enterprise network:



The interconnected elements that work together to deliver a unified enterprise network include: Omada SDN Controller, gateways, switches, access points, and client devices. Beginning with a base of client devices, each element adds functionality and complexity as the network is developing, interconnecting with the elements above and below it to create a comprehensive, secure wired and wireless solution.

Omada SDN Controller is a command center and management platform at the heart of the Omada network. With a single platform, the network administrators configure and manage enterprise networks comprised of routers, switches, and wireless access points in batches. This unleashes new levels of management to avoid complex and costly over-provisioning.

1. 2 Core Components

An Omada SDN network consists of the following core components:

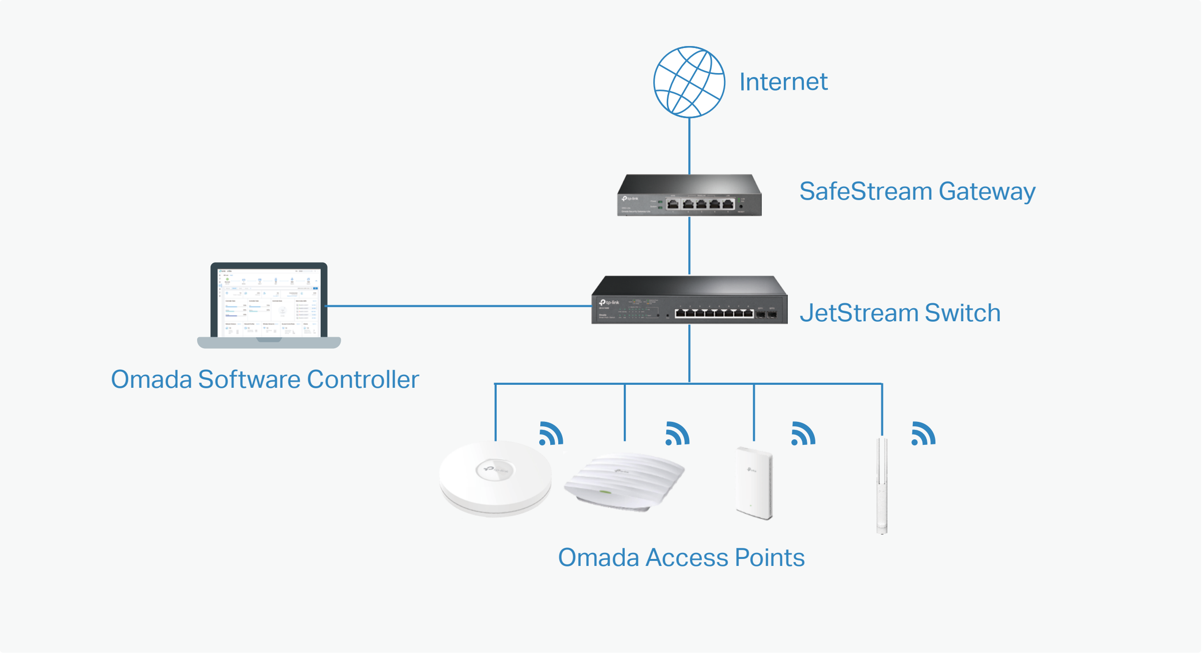
- Omada SDN Controller—a command center and management platform at the heart of Omada network solution for the enterprise. With a single platform, the network administrators configure and manage all Omada products which have all your needs covered in terms of routing, switching and Wi-Fi.
- Gateways—boast excellent data processing capabilities and an array of powerful functions, including IPsec/OpenVPN/PPTP/L2TP VPN, Load Balance, and Bandwidth Control, which are ideal for the business network where a large number of users require a stable, secure connection.
- Switches—offer flexible and cost-effective network solution with powerful Layer 2 features and PoE options. Advanced features such as Access Control, QoS, LAG and Spanning Tree will satisfy advanced business networks.
- Access Points (Omada EAPs)—satisfy the mainstream Wi-Fi Standard and address your high-density access needs with TP-Link's innovation to help you build the versatile and reliable wireless network for all business applications.

Omada SDN Controller

Tailored to different needs and budgets, Omada SDN Controller offers diverse deployment solutions. Omada Software Controller, Omada Hardware Controller, and Omada Cloud-Based Controller, each has their own set of advantages and applications.

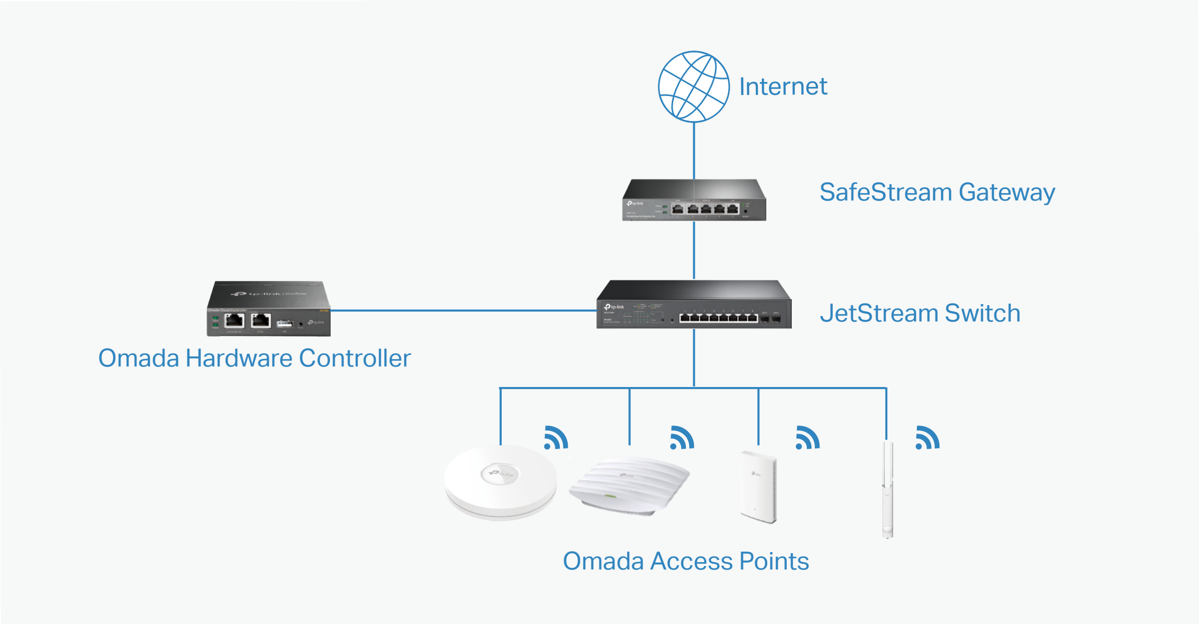
- Omada Software Controller

  Omada Software Controller is totally free, as well as all upgrades. The controller can be hosted on any computers with Windows or Linux systems on your network.



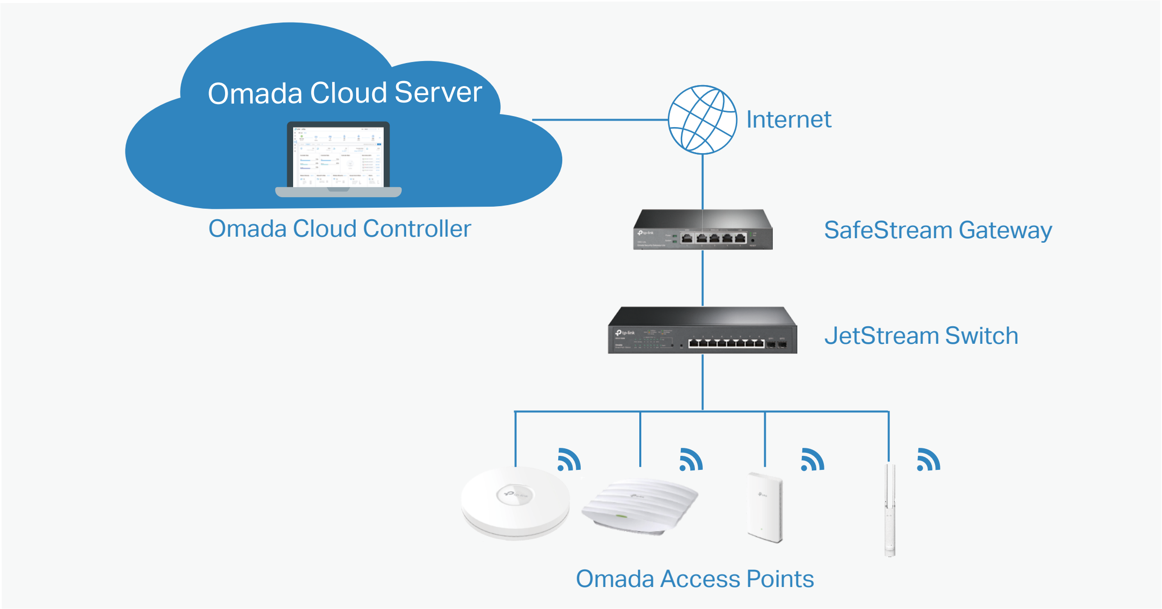
- Omada Hardware Controller

  Omada Hardware Controller is the management device which is pre-installed with Omada Software Controller. You just need to pay for the device, then the built-in Omada Controller software is free to use, no license fee or extra cost required. About the size of a mobile phone, the device is easy to deploy and install on your network.



- Omada Cloud-Based Controller

  Omada Cloud controller is deployed on the Omada Cloud server, providing paid license service with tiered pricing. With paid licenses bound to the devices on the controller, you can configure and manage the devices via Omada Cloud Service. And you need not purchase an additional hardware device or install the software on the host.



The controllers differ in forms, but they have almost the same browser–based management interface and serve the same functions of network management. In this guide, Omada Software Controller, Omada Hardware Controller, and Omada Cloud-Based Controller are referred to as the controller, unless we mention otherwise.

Omada Managed Gateways

TP-Link's Omada Router supports Gigabit Ethernet connections on both WAN and LAN ports which keep the data moving at top speed. Including all the routing and network segmentation functions that a business router must have, SafeStream VPN Router will be the backbone of the Omada SDN network. Moreover, the router provides a secure and easy approach to deploy site-to-site VPN tunnels and access for remote clients.

Managing the gateway centrally through Omada SDN Controller is available on certain models only. Please check the Omada Cloud SDN Platform Compatibility List for more information.

Omada Managed Switches

TP-Link's JetStream Switch provides high-performance and enterprise-level security strategies and lots of advanced features, which is ideal access-edge for the Omada SDN network.

Managing the switch centrally through Omada SDN Controller is available on certain models only. Please check the Omada Cloud SDN Platform Compatibility List for more information.

Omada Access Points

TP-Link's Omada Access Point provides business-class Wi-Fi with superior performance and range which guarantees reliable wireless connectivity for the Omada SDN network.

Managing the access points centrally through Omada SDN Controller is available on certain models only. Please check the Omada Cloud SDN Platform Compatibility List for more information.

2

Get Started with Omada SDN Controller

This chapter guides you on how to get started with Omada SDN Controller to configure the network. Omada Software Controller, Omada Hardware Controller, and Omada Cloud-Based Controller differ in forms, but they have almost the same browser–based management interface for network management. Therefore, they have almost the same initial setup steps, including building your network topology, deploying your controller, and logging in to the controller. The chapter includes the following sections:

2. 1 Set Up Your Software Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up Omada Software Controller:

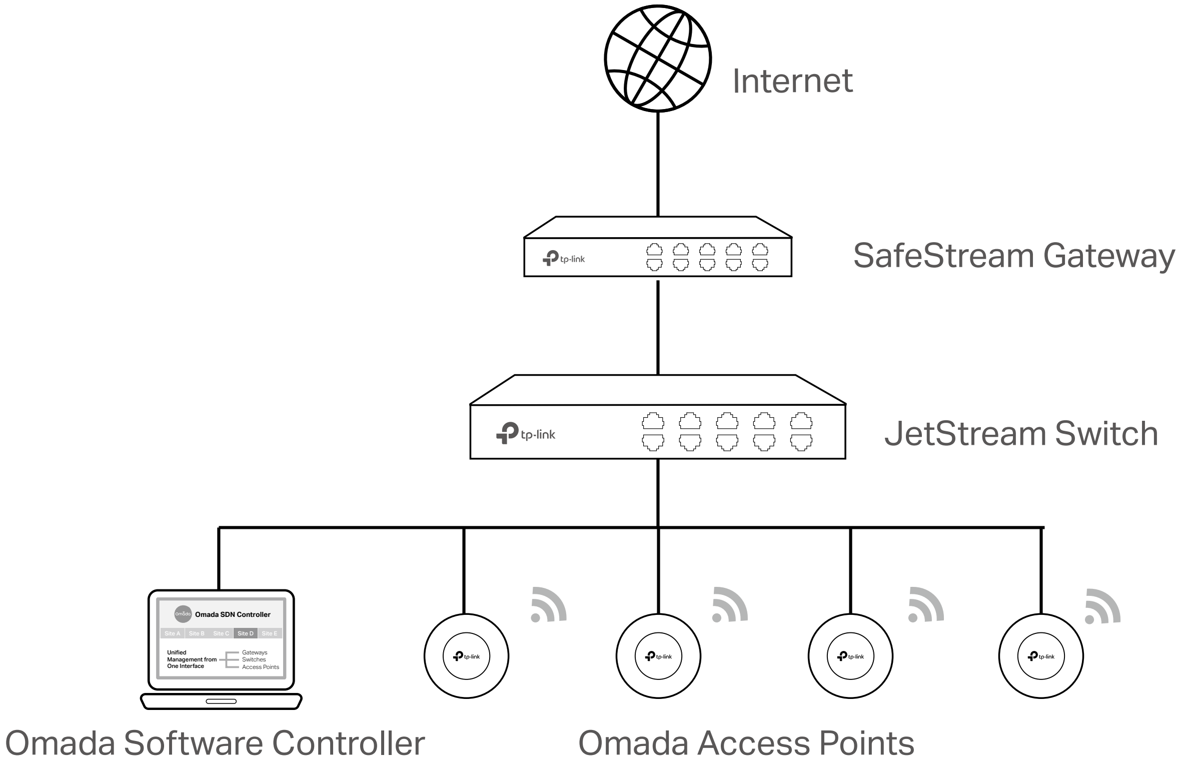
1) Determine the network topology.

2) Install Omada Software Controller.

3) Start and log in to the controller.

2. 1. 1 Determine the Network Topology

The network topology that you create for Omada SDN Controller varies depending on your business requirements. The following figure shows a typical topology for a high-availability use case.



ⓘ Note:

When using Omada SDN Controller, we recommend that you deploy the full Omada topology with supported TP-Link devices. If you use third-party devices, Omada SDN Controller cannot discover and manage them.

2. 1. 2 Install Omada Software Controller

Omada Software Controller is provided for both Windows and Linux operating systems. Determine your operating system and follow the introductions below to install Omada Software Controller.

Installation on Windows Host

Omada Software Controller can be hosted on any computers with Windows systems on your network. Make sure your PC's hardware and system meet the following requirements, then properly install the Omada Software Controller.

- **Hardware Requirements**

  Omada Software Controller can manage up to 1500 EAPs if the Controller Host has enough hardware resources. To guarantee operational stability for managing 1500 EAPs, we recommend that you use the hardware which meets or exceeds the following specifications:

  CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.

  Memory: 16 GB RAM or more.

- **System Requirements**

  Operating System: Microsoft Windows 7/8/10/Server. (We recommend that you deploy the controller on a 64-bit operating system to guarantee the software stability.)

  Web Browser: Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 11 (or above).

- **Install Omada Software Controller**

  Download the installation file of Omada Software Controller from the website. Then follow the instructions to properly install the Omada Software Controller. After a successful installation, a shortcut icon of the Omada Software Controller will be created on your desktop.

Installation on Linux Host

Two versions of installation package are provided: **.tar.gz** file and **.deb** file. Both of them can be used in multiple versions of Linux operating system, including Ubuntu, CentOS, Fedora, and Debian.

Make sure your PC's hardware and system meet the following requirements, then choose the proper installation files to install the Omada Software Controller.

- **Hardware Requirements**

  Omada Software Controller can manage up to 1500 EAPs if the Controller Host has enough hardware resources. To guarantee operational stability for managing 1500 EAPs, we recommend that you use the hardware which meets or exceeds the following specifications:

  CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.

  Memory: 16 GB RAM or more.

- **System Requirements**

  Operating System: 64-bit Linux operating system, including Ubuntu 14.04/16.04/17.04/18.04, CentOS 6.x/7.x, Fedora 20 (or above), and Debian 9.8.

  Web Browser: Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 11 (or above).

- **Install Omada Software Controller**

  Download the installation file of Omada Software Controller from the website. Check the prerequisites and follow the steps based on your file version to install the controller. Here takes Omada SDN Controller 4.2.8 as the example.

  - Prerequisites for installing

    To successfully install Omada Software Controller, ensure that you have performed the following tasks before your installation:

d. Ensure that the Java Runtime Environment (JRE) has been installed in your system. The controller requires that the system has Java 8 installed. Download the file according to your operating system from the website and follow the instructions to install the JRE.

   For Ubuntu16.04 or above, you can use the command: **apt-get install openjdk-8-jre-headless** to get the Java 8 installed.

e. Ensure that MongoDB has been installed in your system. The controller works when the system runs MongoDB 3.0.15–3.6.18. Download the file according to your operating system from the website and follow the instructions to install the MongoDB.

f. Ensure that you have **jsvc** and **curl** installed in your system before installation, which is vital to the smooth running of the system. If your system does not have **jsvc** or **curl** installed, you can install it manually with the command: **apt-get install** or **yum install**. For example, you can use the command: **apt-get install jsvc** or **yum install jsvc** to get **jsvc** installed. And if dependencies are missing, you can use the command: **apt-get -f install** to fix the problem.

  - Install the .tar.gz file

a. Make sure your PC is running in the root mode. You can use this command to enter root mode:

   sudo

b. Extract the tar.gz file using the command:

   tar zxvf Omada_Controller_v4.2.8_linux_x64_targz.tar.gz

c. Install Omada Controller using the command:

   sudo bash ./install.sh

  - Install the .deb file

a. Make sure your PC is running in the root mode. You can use this command to enter root mode:

   sudo

b. Install the .deb file using the command:

   dpkg -i Omada_Controller_v4.2.8_linux_x64.deb

If dependencies are missing during the installation, you can use the command: **apt-fix-broken install** to fix the problem.

After installing the controller, use the following commands to check and change the status of the controller.

a. **tpeap start** — start the controller, use the command.

b. **tpeap stop** — stop running the Omada Controller.

c. **tpeap status** — show the status of Controller.

For more detailed information about the installation on Linux hosts, refer to the installation instructions.

Note:

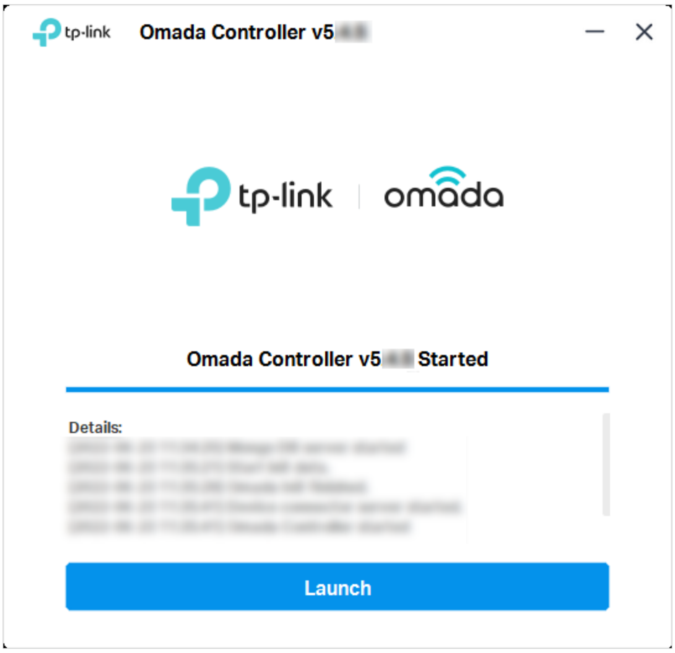
- For installing the .tar.gz, if you want Omada Controller to run as a user (it runs as root by default) you should modify OMADA_USER value in bin/control.sh.
- To uninstall Omada Controller, go to the installation path: /opt/tplink/EAPController, and run the command: sudo bash ./uninstall.sh.
- During uninstallation, you can choose whether to back up the database. The backup folder is /opt/tplink/eap_db_backup.
- During installation, you will be asked whether to restore the database if there is any backup database in the folder /opt/tplink/eap_db_backup.

2. 1. 3 Start and Log In to the Omada Software Controller

Launch Omada Software Controller and follow the instructions to complete basic configurations, and then you can log in to the management interface.

Launch Omada Software Controller

Double-click the icon and the following window will pop up. After a while, your web browser will automatically open.



Omada Controller v5

Omada Controller v5 Started

Details:

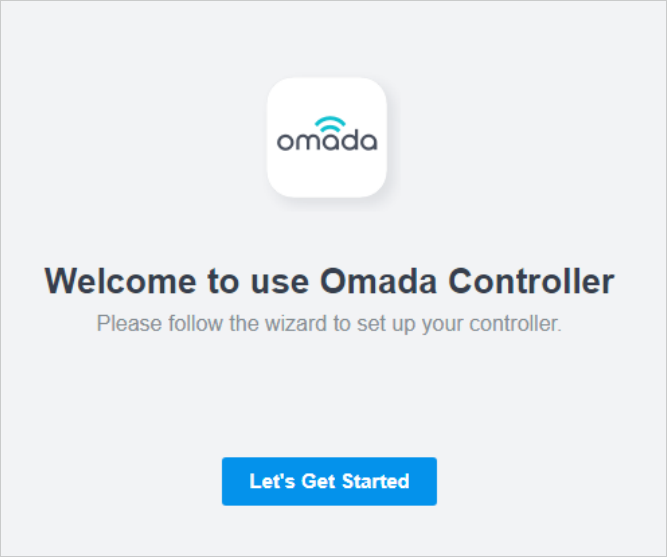
ⓘ Note:

- If your browser does not open automatically, click Launch. You can also launch a web browser and enter http://127.0.0.1:8088 in the address bar.
- If your web browser opens but prompts a problem with the website's security certificate, click Continue.

Complete Basic Configurations

In the web browser, you can see the configuration page. Follow the setup wizard to complete the basic settings for Omada Controller.

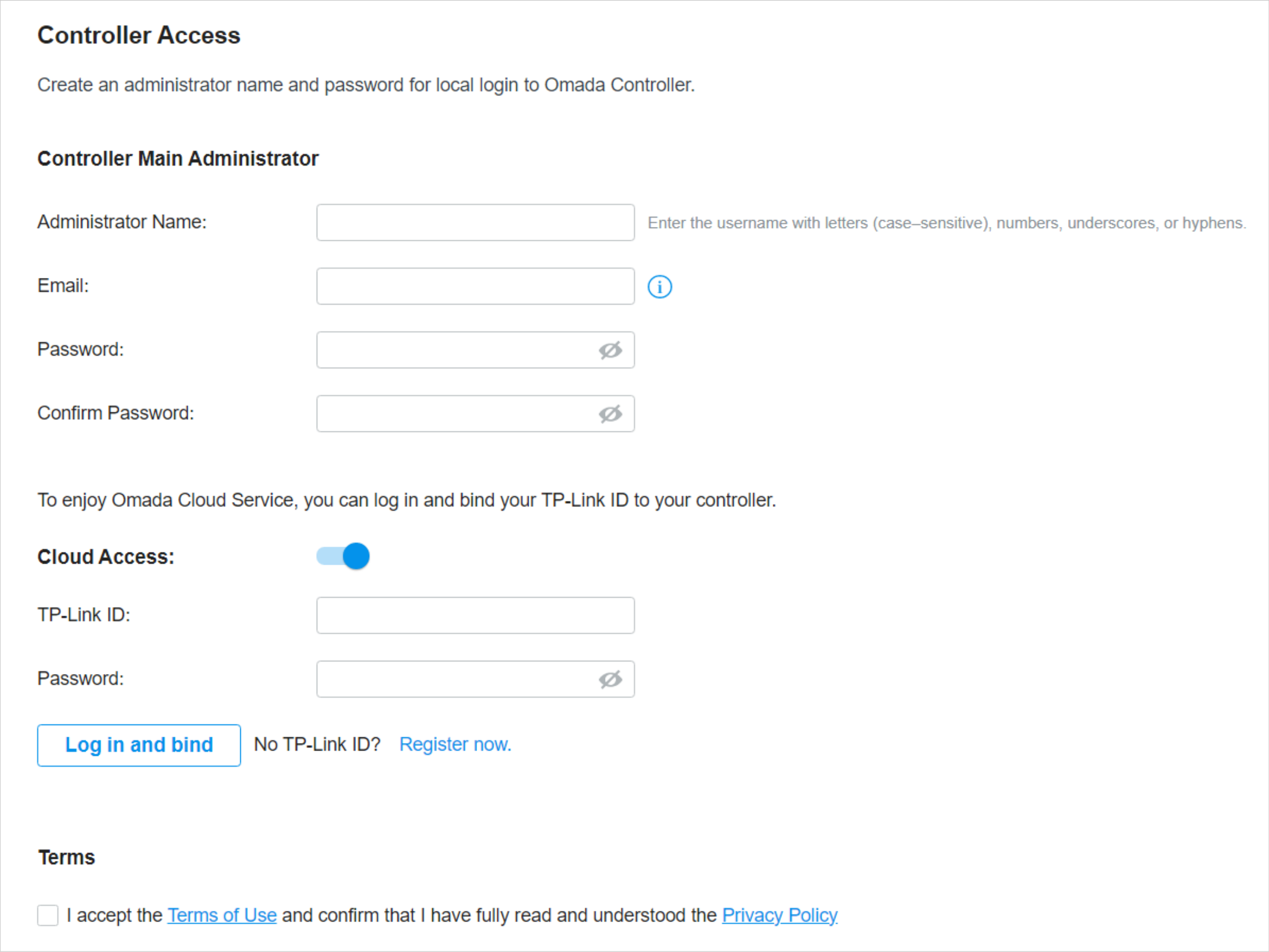
1. Click Let's Get Started.



Welcome to use Omada Controller

Please follow the wizard to set up your controller.

2. Set up controller access settings.



Controller Access

Create an administrator name and password for local login to Omada Controller.

Controller Main Administrator

Administrator Name: Enter the username with letters (case–sensitive), numbers, underscores, or hyphens.

Email:

Password:

Confirm Password:

To enjoy Omada Cloud Service, you can log in and bind your TP-Link ID to your controller.

Cloud Access:

TP-Link ID:

Password:

No TP-Link ID? Register now.

Terms

□ I accept the Terms of Use and confirm that I have fully read and understood the Privacy Policy

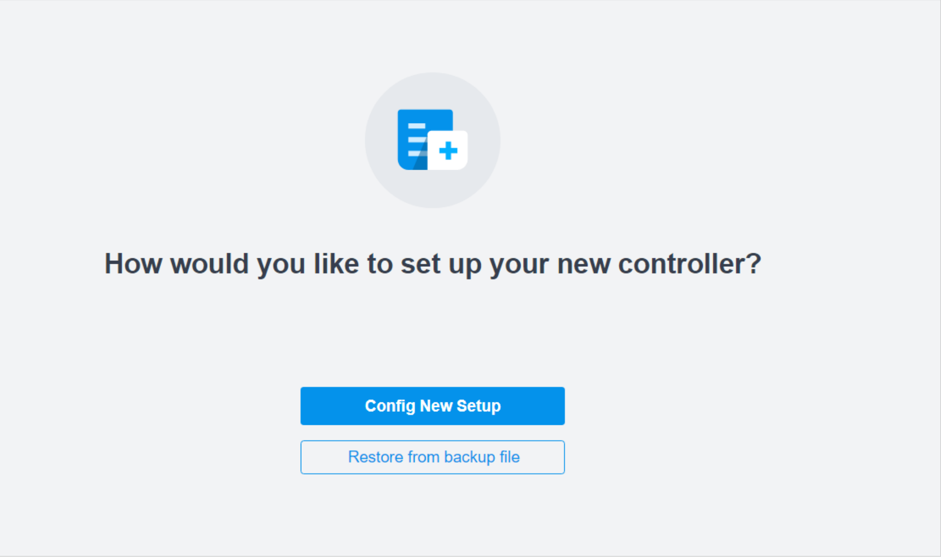
a. Create an Administrator username and password for login to the Omada controller. Specify the email address for resetting your password in case that you forget the password. After logging into Omada Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to 8. 6. 3 Notifications.

b. If you want to access the controller to manage networks remotely, enable Cloud Access, and bind your TP-Link ID to your Omada Controller. For more details about Omada Cloud, please refer to 5. 2 Manage Your Controller Remotely via Cloud Access.

c. Read and agree to TP-Link's Terms of Use.

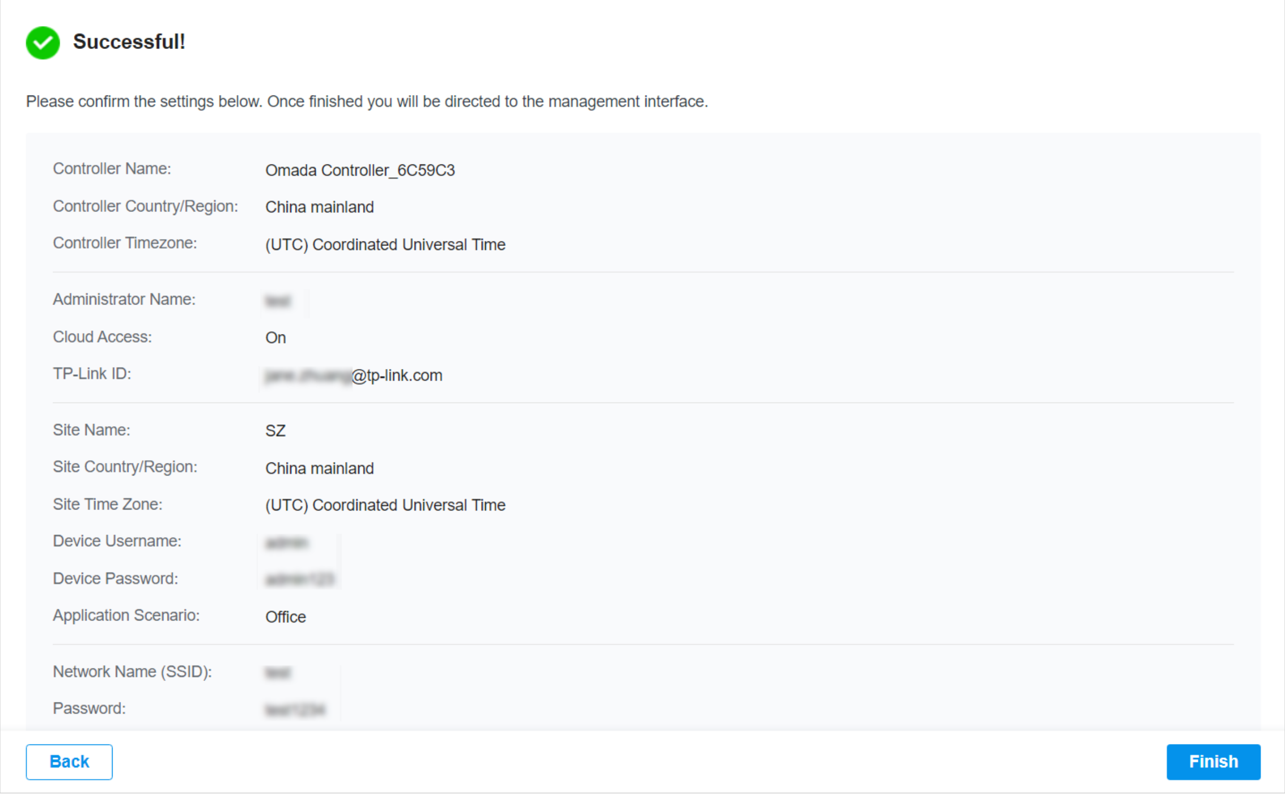
d. Click Next.

3. Choose how would you like to set up your new controller. You can configure a new setup or restore from backup file.



How would you like to set up your new controller?

4. Follow the setup wizard to set up the controller.



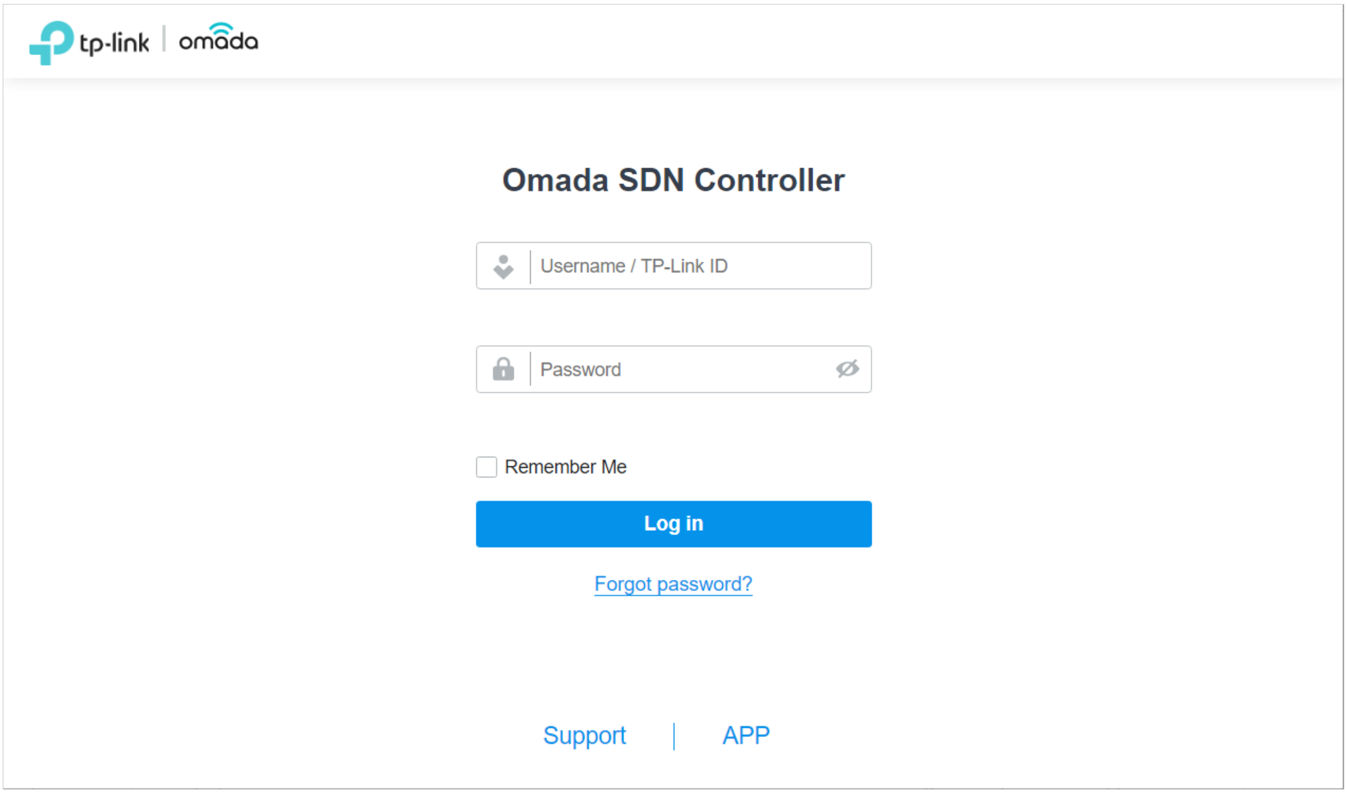
Successful!

Please confirm the settings below. Once finished you will be directed to the management interface.

Controller Name:	Omada Controller_6C59C3
Controller Country/Region:	China mainland
Controller Timezone:	(UTC) Coordinated Universal Time
Administrator Name:	[redacted]
Cloud Access:	On
TP-Link ID:	[redacted]@tp-link.com
Site Name:	SZ
Site Country/Region:	China mainland
Site Time Zone:	(UTC) Coordinated Universal Time
Device Username:	[redacted]
Device Password:	[redacted]
Application Scenario:	Office
Network Name (SSID):	[redacted]
Password:	[redacted]

Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.



Note:

In addition to the Controller Host, other hosts in the same LAN can also manage EAPs via remote access to the Controller Host. For example, if the IP address of the Controller Host is 192.168.0.100 and Omada Controller is running normally on this host, you can enter https://192.168.0.100:8043, or http://192.168.0.100:8088 in the web browser of other hosts in the same LAN to log in to the Omada Controller and manage EAPs. Or you can log in to Omada Controller using other management devices through Omada Cloud service.

2. 2 Set Up Your Hardware Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up Omada Hardware Controller:

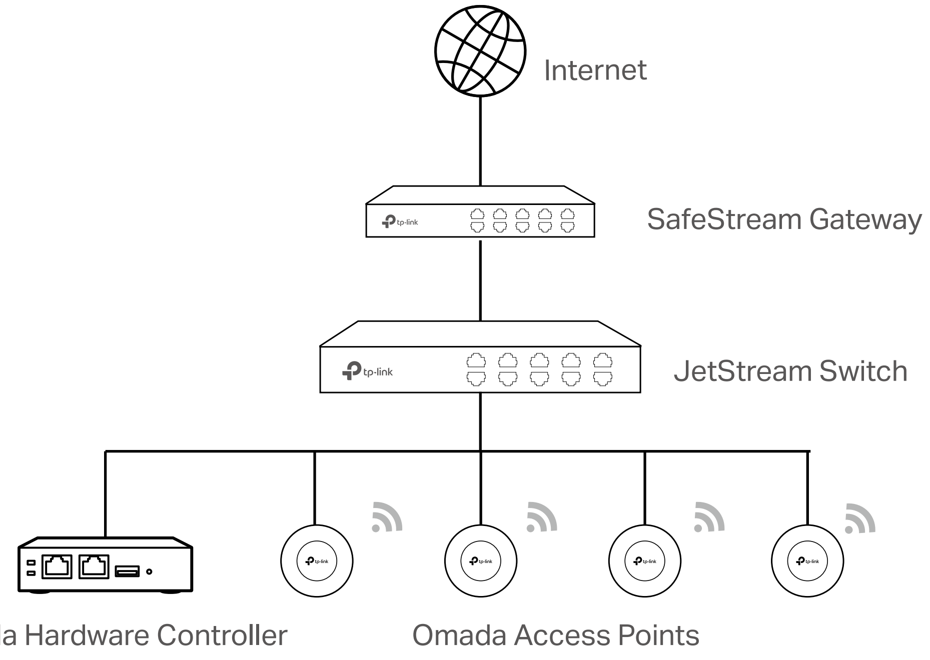
1) Determine the network topology.

2) Deploy Omada Hardware Controller.

3) Start and log in to the controller.

2. 2. 1 Determine the Network Topology

The network topology that you create for Omada SDN Controller varies depending on your business requirements. The following figure shows a typical topology for a high-availability use case.



Note:

When using Omada SDN Controller, we recommend that you deploy the full Omada topology with supported TP-Link devices. If you use third-party devices, Omada SDN Controller cannot discover and manage them.

2. 2. 2 Deploy Omada Hardware Controller

Omada Hardware Controller comes with the pre-installed controller software, so installation is not necessary. After deploying Omada Hardware Controller on your network infrastructure, proceed to configure the controller.

2. 2. 3 Start and Log in to the Controller

Log In to the Management Interface

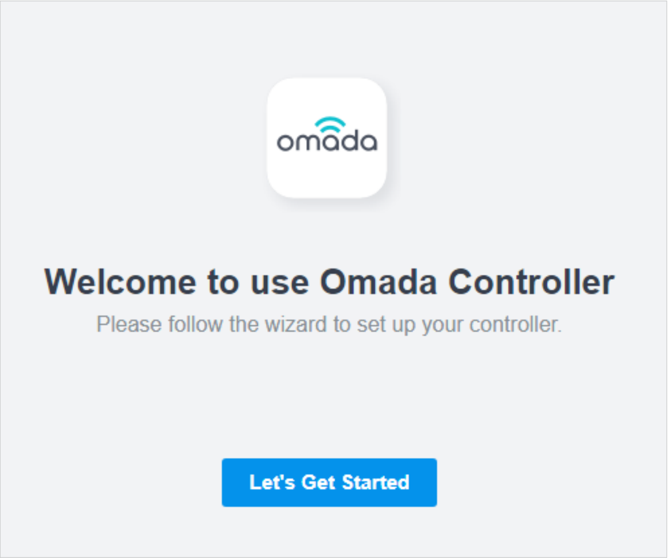
Follow the steps below to enter the management interface of Omada Hardware Controller:

1. Make sure that your management device has the route to access the controller.
2. Check the DHCP server (typically a router) for the IP Address of the controller. If the controller fails to get a dynamic IP address from the DHCP server, the default fallback IP address 192.168.0.253, is used.
3. Launch a web browser and type the IP address of the controller in the address bar, then press **Enter** (Windows) or **Return** (Mac).

Complete Basic Configurations

In the web browser, you can see the configuration page. Follow the setup wizard to complete the basic settings for Omada Controller.

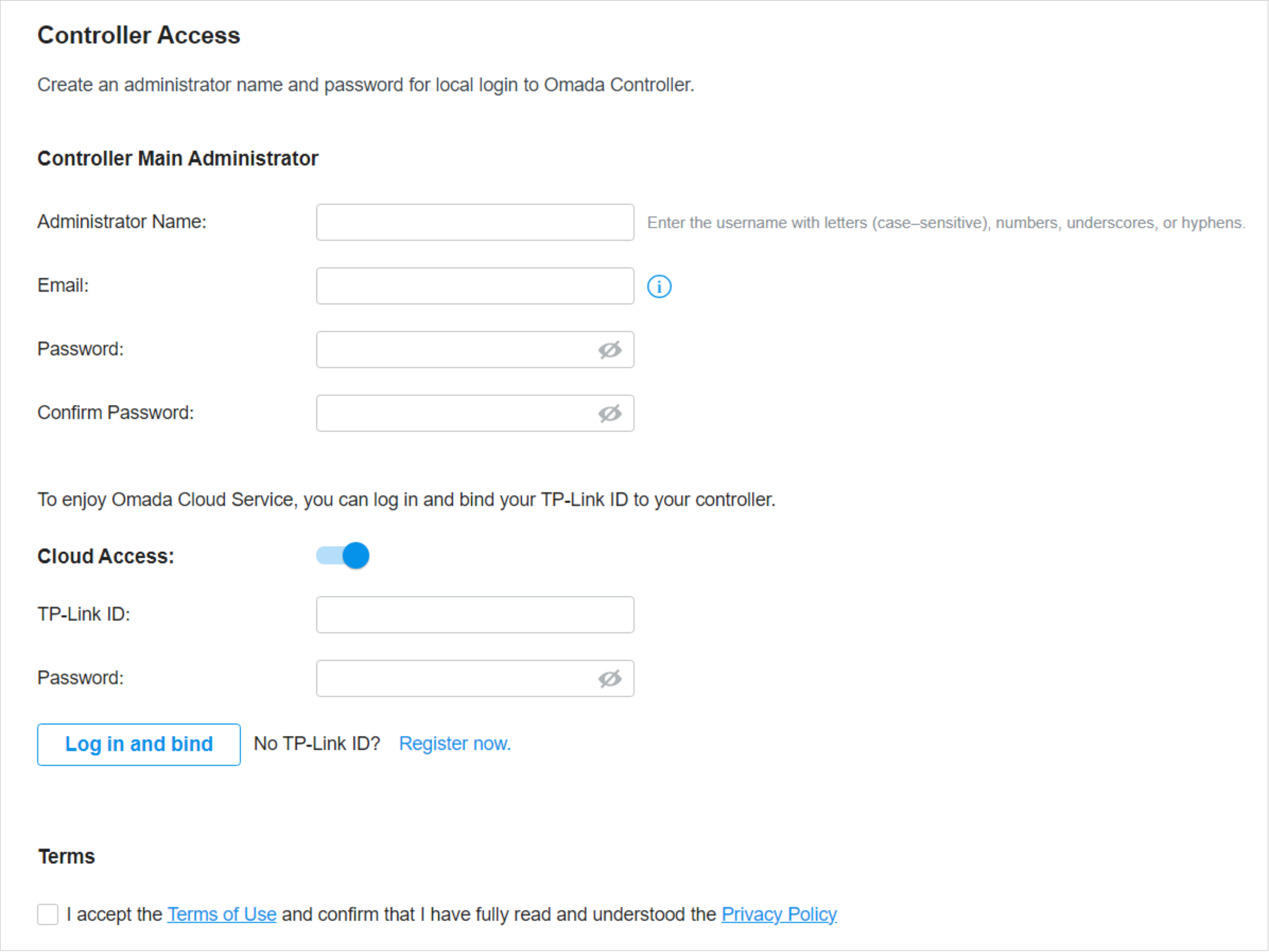
1. Click Let's Get Started.



Welcome to use Omada Controller

Please follow the wizard to set up your controller.

2. Set up controller access settings.



Controller Access

Create an administrator name and password for local login to Omada Controller.

Controller Main Administrator

Administrator Name: Enter the username with letters (case–sensitive), numbers, underscores, or hyphens.

Email:

Password:

Confirm Password:

To enjoy Omada Cloud Service, you can log in and bind your TP-Link ID to your controller.

Cloud Access:

TP-Link ID:

Password:

Log in and bind No TP-Link ID? Register now.

Terms

□ I accept the Terms of Use and confirm that I have fully read and understood the Privacy Policy

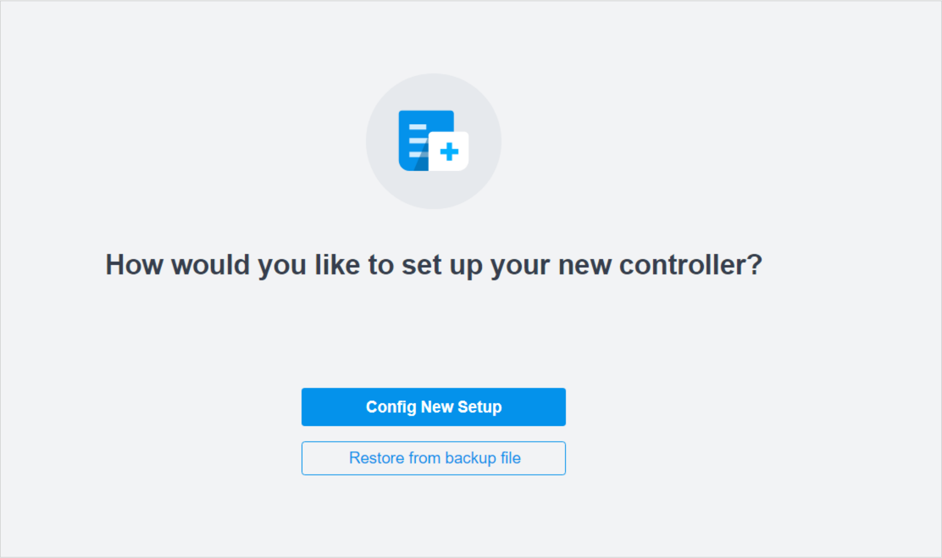
a. Create an Administrator username and password for login to the Omada controller. Specify the email address for resetting your password in case that you forget the password. After logging into Omada Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to 8. 6. 3 Notifications.

b. If you want to access the controller to manage networks remotely, enable Cloud Access, and bind your TP-Link ID to your Omada Controller. For more details about Omada Cloud, please refer to 5. 2 Manage Your Controller Remotely via Cloud Access.

c. Read and agree to TP-Link’s Terms of Use.

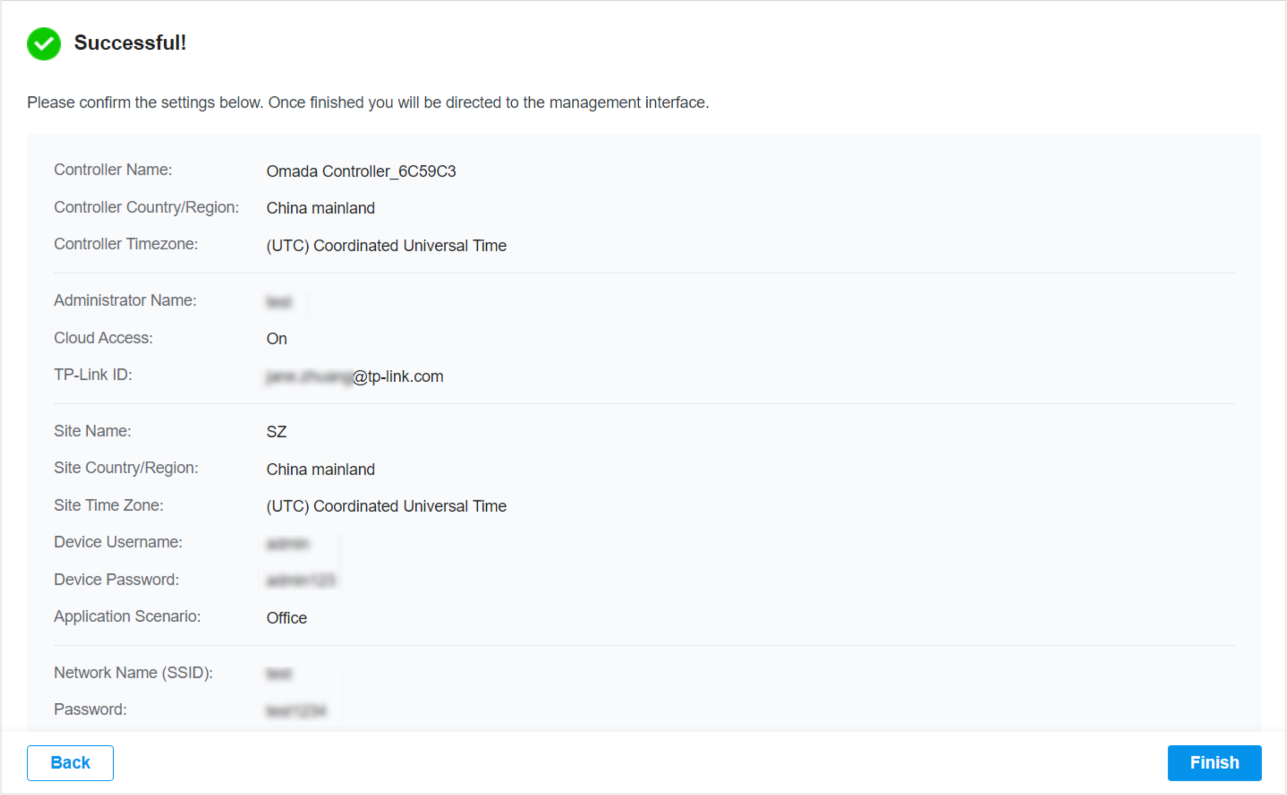
d. Click Next.

3. Choose how would you like to set up your new controller. You can configure a new setup or restore from backup file.



How would you like to set up your new controller?

4. Follow the setup wizard to set up the controller.



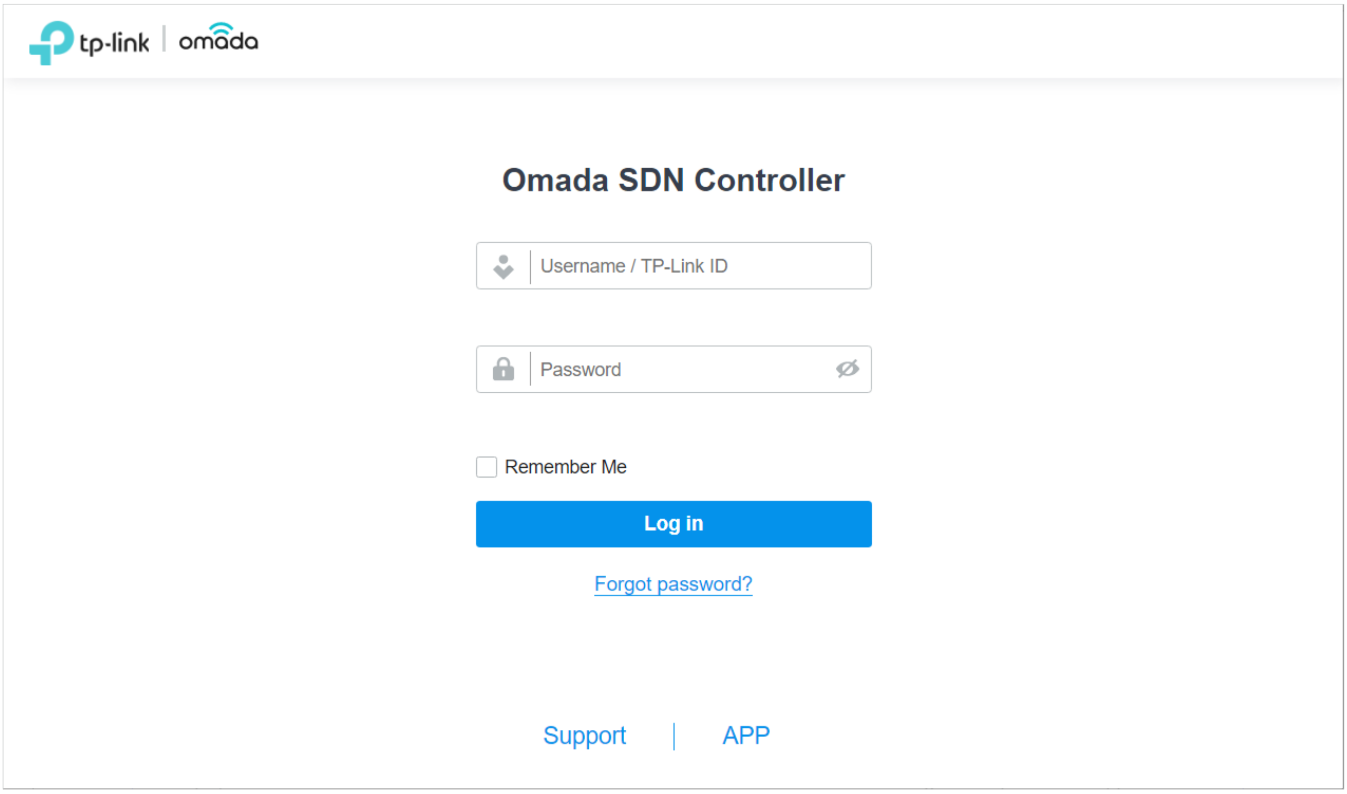
Successful!

Please confirm the settings below. Once finished you will be directed to the management interface.

Controller Name:	Omada Controller_6C59C3
Controller Country/Region:	China mainland
Controller Timezone:	(UTC) Coordinated Universal Time
Administrator Name:	[redacted]
Cloud Access:	On
TP-Link ID:	[redacted]@tp-link.com
Site Name:	SZ
Site Country/Region:	China mainland
Site Time Zone:	(UTC) Coordinated Universal Time
Device Username:	[redacted]
Device Password:	[redacted]
Application Scenario:	Office
Network Name (SSID):	[redacted]
Password:	[redacted]

Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.



Note:

In addition to the Controller Host, other hosts in the same LAN can also manage EAPs via remote access to the Controller Host. For example, if the IP address of the Controller Host is 192.168.0.100 and Omada Controller is running normally on this host, you can enter https://192.168.0.100:8043, or http://192.168.0.100:8088 in the web browser of other hosts in the same LAN to log in to the Omada Controller and manage EAPs. Or you can log in to Omada Controller using other management devices through Omada Cloud service.

2. 3 Set Up Your Cloud-Based Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up Omada Cloud-Based Controller:

1) Launch a web browser and enter https://omada.tplinkcloud.com in the address bar. Enter your TP-Link ID and password to log in. If you do not have a TP-Link ID, create a TP-Link ID first.

2) Click Add Controller and register for an Omada Cloud-Based Controller. Follow the instructions to complete the setup process.

3) Add devices with the serial number, make sure the devices are online and in factory default.

4) Assign appropriate licenses in order to manage and configure the devices on the cloud-based controller. Then wait until your controller is deployed

For detailed information about device-based licensing, refer to Know more about licensing.

ⓘ Note:

Only when you have available licenses can you register for the Cloud-Based Controller and manage the devices. To successfully register for a Cloud-Based Controller, purchase appropriate licenses.

3

Configure the Omada SDN Controller

Controller Settings control the appearance and behavior of the controller and provide methods of data backup, restore and migration:

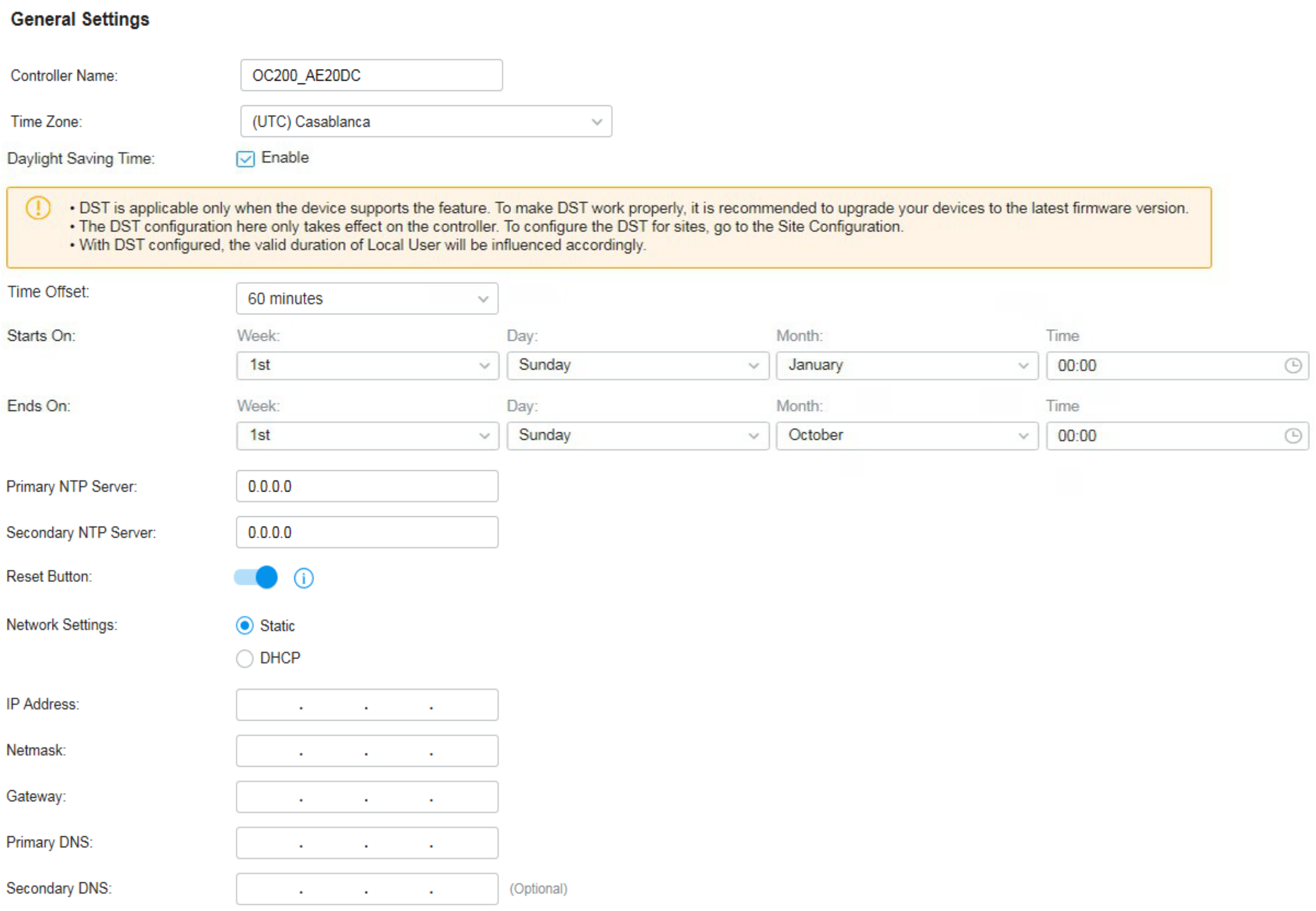
3. 1 Manage the Controller

3. 1. 1 General Settings

Configuration

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Controller. In General Settings, configure the parameters and click Save.

■ **For Omada Hardware Controller**



General Settings

Controller Name: OC200_AE20DC

Time Zone: (UTC) Casablanca

Daylight Saving Time: ☑ Enable

- DST is applicable only when the device supports the feature. To make DST work properly, it is recommended to upgrade your devices to the latest firmware version.
- The DST configuration here only takes effect on the controller. To configure the DST for sites, go to the Site Configuration.
- With DST configured, the valid duration of Local User will be influenced accordingly.

Time Offset: 60 minutes

	Week:	Day:	Month:	Time
Starts On:	1st	Sunday	January	00:00
Ends On:	1st	Sunday	October	00:00

Primary NTP Server: 0.0.0.0

Secondary NTP Server: 0.0.0.0

Reset Button: ●

Network Settings: ● Static ○ DHCP

IP Address: . . .

Netmask: . . .

Gateway: . . .

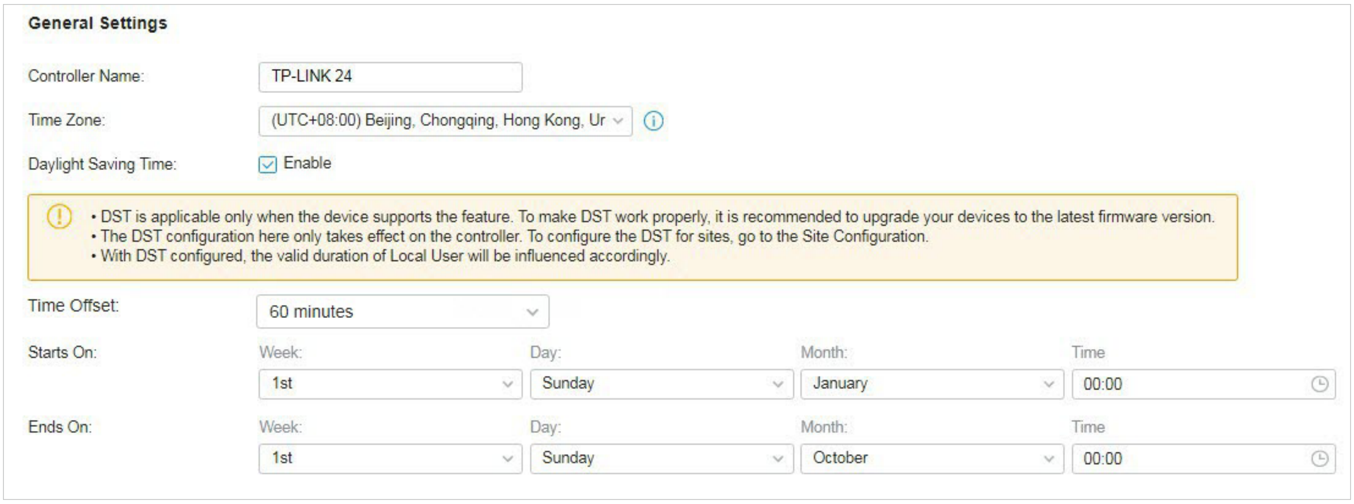
Primary DNS: . . .

Secondary DNS: . . . (Optional)

Controller Name	Specify the Controller Name to identify the controller.
Time Zone	Select the Time Zone of the controller according to your region. For controller settings and statistics, time is displayed based on the Time Zone.
Daylight Saving Time	Enable the feature if your country/region implements DST. When it is enabled, the icon DST will appear on the upper right, showing the DST settings and status.

Time Offset	Select 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.
Primary NTP Server/ Secondary NTP Server	Enter the IP address of the primary and secondary NTP (Network Time Protocol) server. NTP servers assign network time to the controller.
Reset Button	With this feature enabled, the controller can be reset via reset button.
Network Settings	Select one way for the controller to get IP settings. Static: You need to specify the IP address, Netmask, Gateway, Primary DNS, and Secondary DNS for the controller. DHCP: The controller get IP settings from the DHCP server. If the controller fails to get IP settings from the DHCP server, it will use the Fallback IP Address and Fallback Netmask.

■ For Omada Software Controller / Omada Cloud-Based Controller



General Settings

Controller Name: TP-LINK 24

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Ur

Daylight Saving Time: ☑ Enable

- DST is applicable only when the device supports the feature. To make DST work properly, it is recommended to upgrade your devices to the latest firmware version.
- The DST configuration here only takes effect on the controller. To configure the DST for sites, go to the Site Configuration.
- With DST configured, the valid duration of Local User will be influenced accordingly.

Time Offset: 60 minutes

Starts On: Week: 1st Day: Sunday Month: January Time 00:00

Ends On: Week: 1st Day: Sunday Month: October Time 00:00

Controller Name	Specify the Controller Name to identify the controller.
Time Zone	Select the Time Zone of the controller according to your region. For controller settings and statistics, time is displayed based on the Time Zone.
Daylight Saving Time	Enable the feature if your country/region implements DST.

Time Offset	Select 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 Mail Server

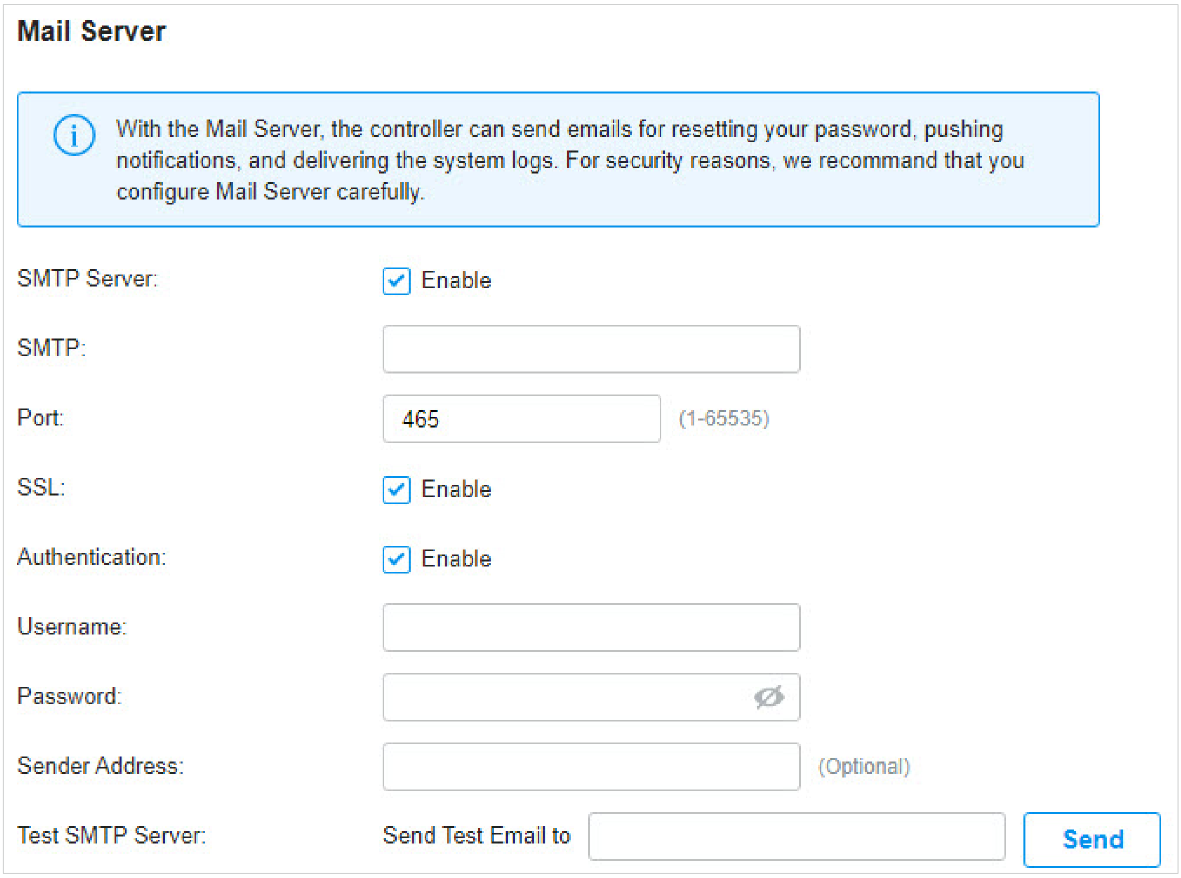
Overview

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.

Configuration

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. Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Controller Settings. In Mail Server, enable SMTP Server and configure the parameters. Then click Save.



Mail Server

With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. For security reasons, we recommand that you configure Mail Server carefully.

SMTP Server:	☑ Enable
SMTP:	
Port:	465 (1-65535)
SSL:	☑ Enable
Authentication:	☑ Enable
Username:	
Password:	
Sender Address:	(Optional)
Test SMTP Server:	Send Test Email to

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	When Authentication is enabled, enter your email address as the username.
Password	When Authentication is enabled, enter the authentication code as the password, which is provided by the email service provider when you enable the SMTP service.

Sender Address	(Optional) 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.

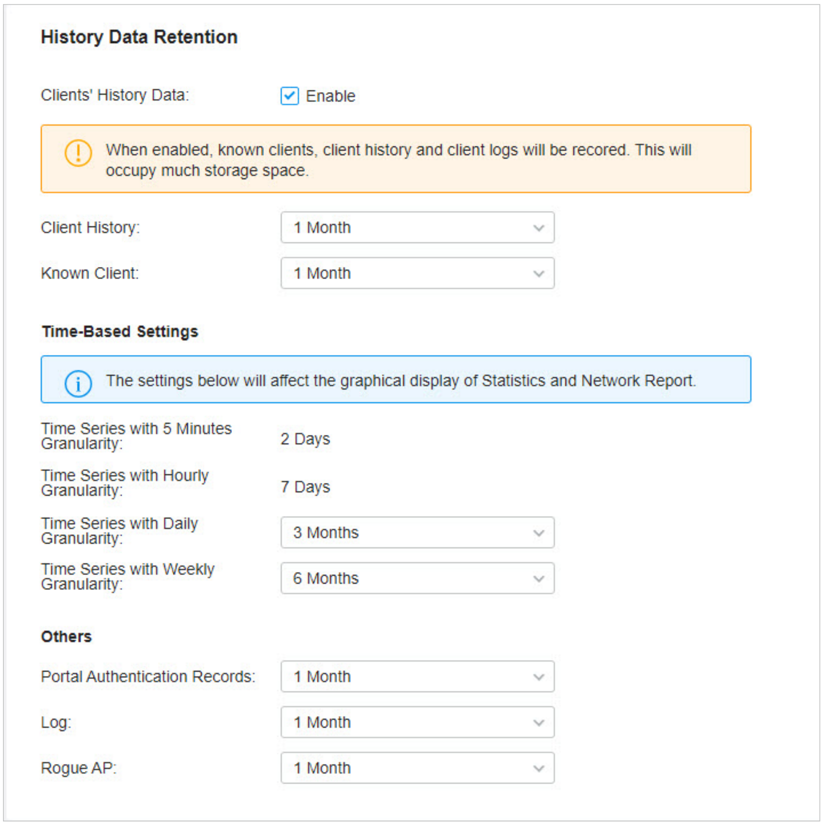
3. 1. 3 History Data Retention

Overview

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

Configuration

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Controller Settings. In History Data Retention, configure the parameters and click Save.



History Data Retention

Clients' History Data: ☑ Enable

When enabled, known clients, client history and client logs will be recored. This will occupy much storage space.

Client History: 1 Month

Known Client: 1 Month

Time-Based Settings

The settings below will affect the graphical display of Statistics and Network Report.

Time Series with 5 Minutes Granularity: 2 Days

Time Series with Hourly Granularity: 7 Days

Time Series with Daily Granularity: 3 Months

Time Series with Weekly Granularity: 6 Months

Others

Portal Authentication Records: 1 Month

Log: 1 Month

Rogue AP: 1 Month

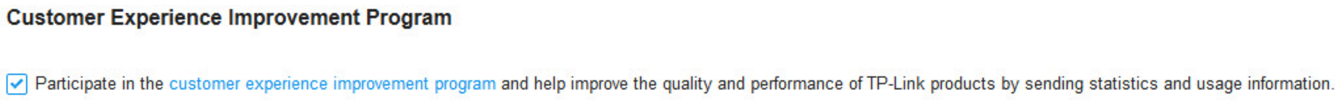
Clients' History Data	When enabled, known clients, client history and client logs will be recorded. This will occupy much storage space.
Client History	Specify the retention time of client online and offline records. Corresponding to Insight-Past Connection.

Known Client	Specify the retention time of known client data. Corresponding to Insight-Known Clients.
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.
Log	Specify the retention time of logs.
Rogue AP	Specify the retention time of scanned Rogue APs. Corresponding to Insight-Rogue APs.

3. 1. 4 Customer Experience Improvement Program

Configuration

Click the checkbox if you agree to participate in the customer experience improvement program and help improve the quality and performance of TP-Link products by sending statistics and usage information.



Customer Experience Improvement Program

☑ Participate in the customer experience improvement program and help improve the quality and performance of TP-Link products by sending statistics and usage information.

3. 1. 5 HTTPS Certificate

Overview

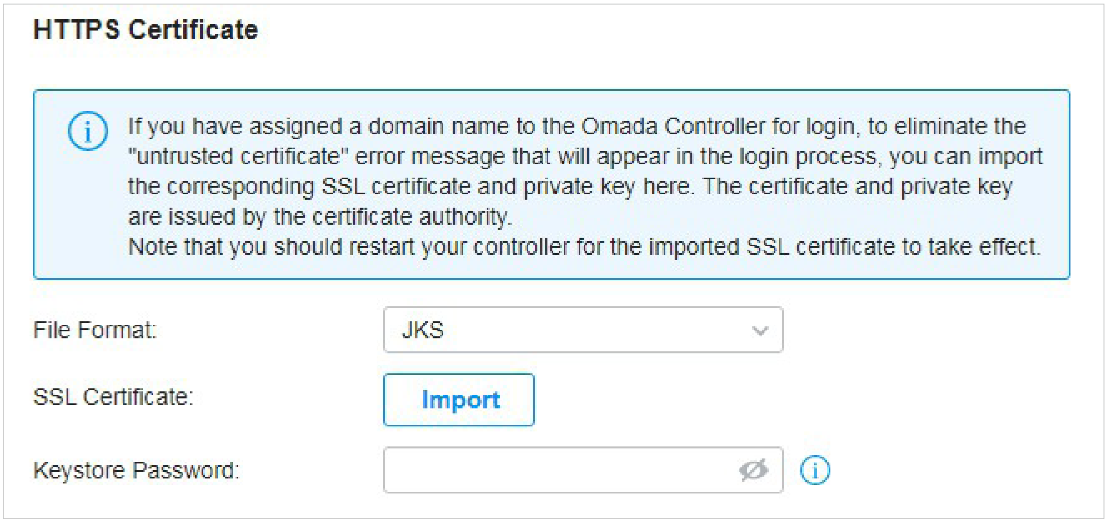
If you have assigned a domain name to the controller for login, to eliminate the "untrusted certificate" error message that will appear in the login process, you can import the corresponding SSL certificate and private key here. The certificate and private key are issued by the certificate authority.

Note:

- HTTPS Certificate configuration is only available for Omada Software Controller and Omada Hardware Controller.
- You need to restart you controller for the imported SSL certificate to take effect.

Configuration

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Controller Settings. In HTTPS Certificate, select your file format, import your SSL certificate and configure the parameters. Then click Save.



HTTPS Certificate

If you have assigned a domain name to the Omada Controller for login, to eliminate the "untrusted certificate" error message that will appear in the login process, you can import the corresponding SSL certificate and private key here. The certificate and private key are issued by the certificate authority.
Note that you should restart your controller for the imported SSL certificate to take effect.

File Format: JKS

SSL Certificate: Import

Keystore Password:

File Format	Select the format of your certificate, and import the certificate file.
Keystore Password	(For JKS) Enter the keystore password if your SSL certificate has the keystore password. Otherwise, leave it blank.
Private Key Password	(For PFX) Enter the private key password if your SSL certificate has the private key password. Otherwise, leave it blank.

Note:

For the PEM-formatted certificate:

- Starts with: -----BEGIN CERTIFICATE-----
- Ends with: -----END CERTIFICATE-----
- Certificate chain is supported and no blank line is allowed between two certificate chains.

For the PEM-formatted key:

- RSA encryption is required.
- Starts with: -----BEGIN RSA PRIVATE KEY-----
- Ends with: -----END RSA PRIVATE KEY -----
- The key can be placed behind certificate file, and they can be imported together.

3. 1. 6 Access Config

Overview

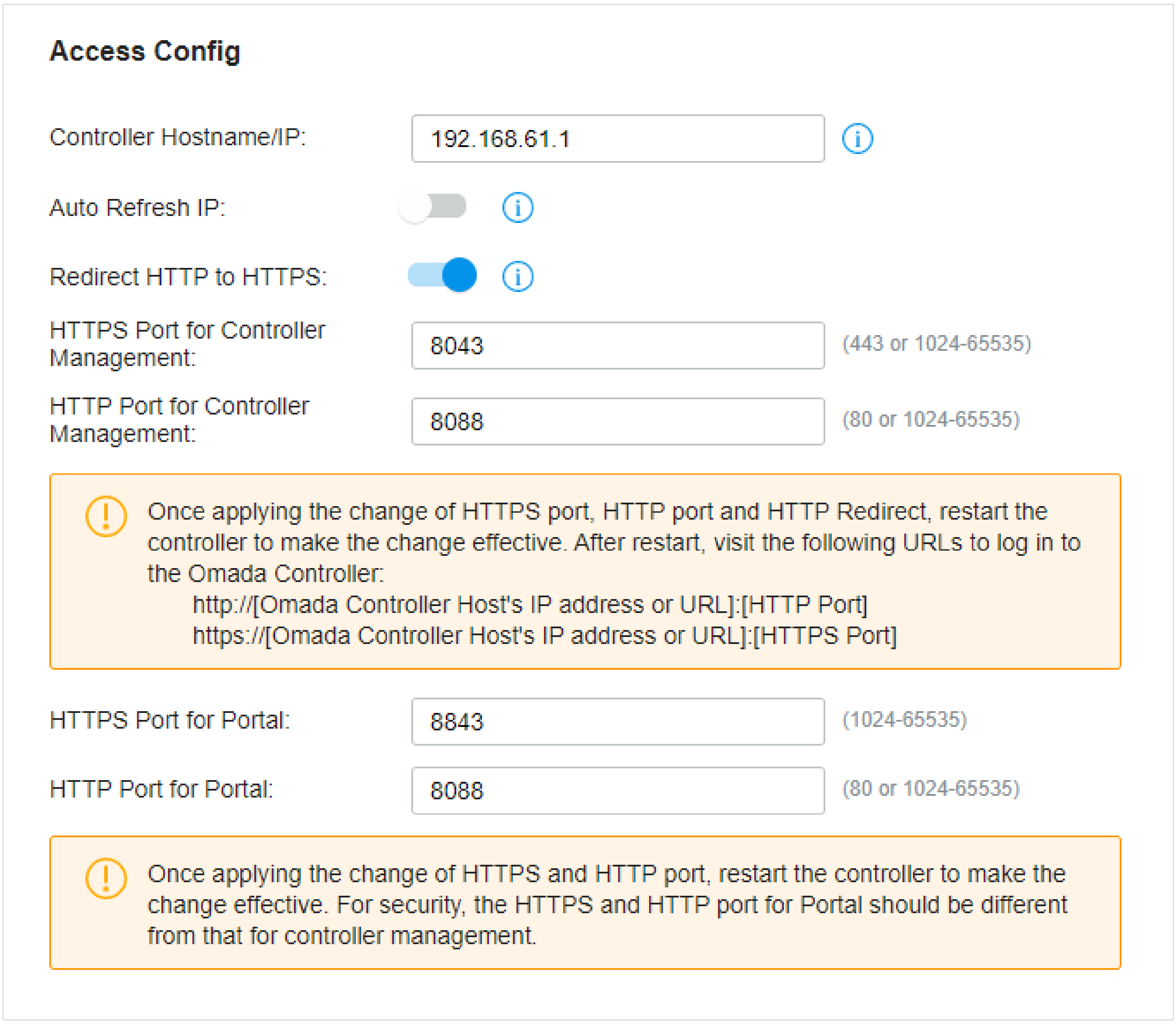
With Access Config, you can specify the port used by the controller for management and portal.

Note:

- Access Config is only available on Omada Software Controller and Omada Hardware Controller.
- Once applying the change of HTTPS and HTTP port, restart the controller to make the change effective.
- For security, the HTTPS and HTTP port for Potal should be different from that for controller management.

Configuration

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Controller Settings. In Access Config, configure the parameters and click Save.



Access Config

Controller Hostname/IP: 192.168.61.1

Auto Refresh IP: ○

Redirect HTTP to HTTPS: ●

HTTPS Port for Controller Management: 8043 (443 or 1024-65535)

HTTP Port for Controller Management: 8088 (80 or 1024-65535)

Once applying the change of HTTPS port, HTTP port and HTTP Redirect, restart the controller to make the change effective. After restart, visit the following URLs to log in to the Omada Controller:

http://[Omada Controller Host's IP address or URL]:[HTTP Port]
https://[Omada Controller Host's IP address or URL]:[HTTPS Port]

HTTPS Port for Portal: 8843 (1024-65535)

HTTP Port for Portal: 8088 (80 or 1024-65535)

Once applying the change of HTTPS and HTTP port, restart the controller to make the change effective. For security, the HTTPS and HTTP port for Portal should be different from that for controller management.

Controller Hostname/IP	Enter the hostname or IP address of the controller which will be used as the Controller URL in the notification email for resetting your controller password. You can keep it default and IP address recognized by the controller will be used as the Controller URL.
Auto Refresh IP	(Only for hardware controller) Enable the feature and the hardware controller will refresh its IP address automatically.
Redirect HTTP to HTTPS	With this option enabled, HTTP requests will be redirected to HTTPS connections.
HTTPS Port for Controller Management	Specify the HTTPS port used by the controller for management. After setting the port, you can visit https://[Omada Controller Host's IP address or URL]:[HTTPS Port] to log in to the Omada Controller.
HTTP Port for Controller Management	Specify the HTTP port used by the controller for management. After setting the port, you can visit https://[Omada Controller Host's IP address or URL]:[HTTP Port] to log in to the Omada Controller.
HTTPS Port for Portal	Specify the HTTPS port used by the controller for Portal.
HTTP Port for Portal	Specify the HTTP port used by the controller for Portal.

3. 2 Manage Your Controller Remotely via Cloud Access

Overview

With Cloud Access, it's convenient for you to manage your controller from anywhere, as long as you have access to the internet.

Configuration

To manage your controller from anywhere, follow these steps:

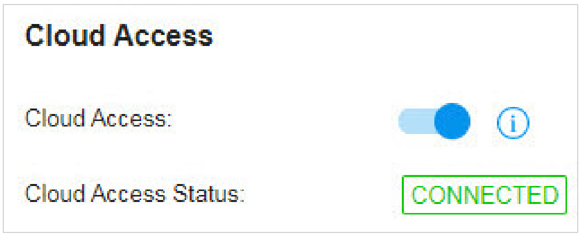
1. Prepare your controller for Cloud Access

■ **For Omada Software Controller / Omada Hardware Controller:**

Note:

- Before you start, make sure your Omada Software Controller Host or Omada Hardware Controller has access to the internet.
- If you have enabled cloud access and bound your TP-Link ID in the quick setup wizard, skip this step.

1) Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Cloud Access. Enable Cloud Access.

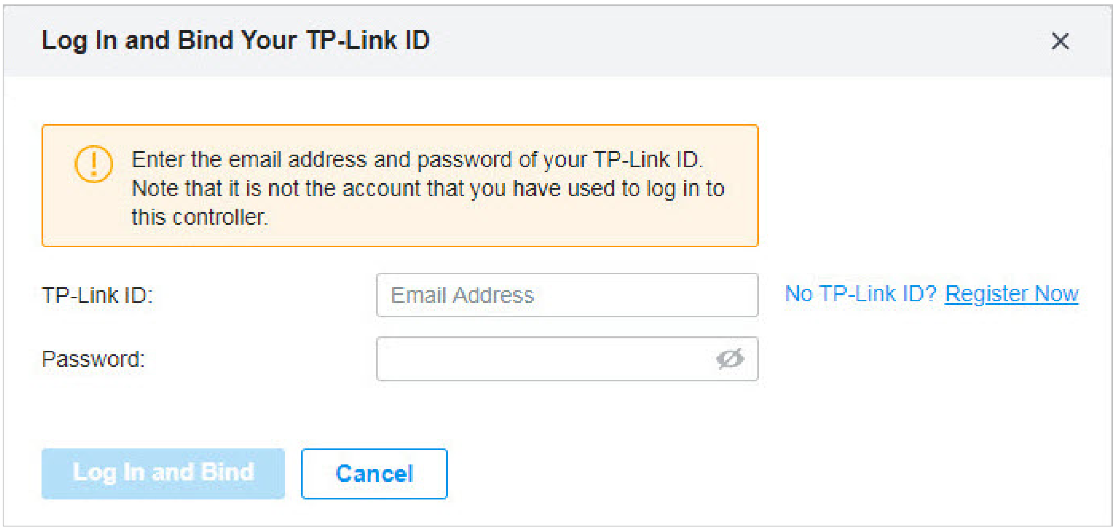


Cloud Access

Cloud Access: ●

Cloud Access Status: CONNECTED

2) Enter your TP-Link ID and password. Then click Log In and Bind.



Log In and Bind Your TP-Link ID

Enter the email address and password of your TP-Link ID. Note that it is not the account that you have used to log in to this controller.

TP-Link ID: Email Address

No TP-Link ID? Register Now

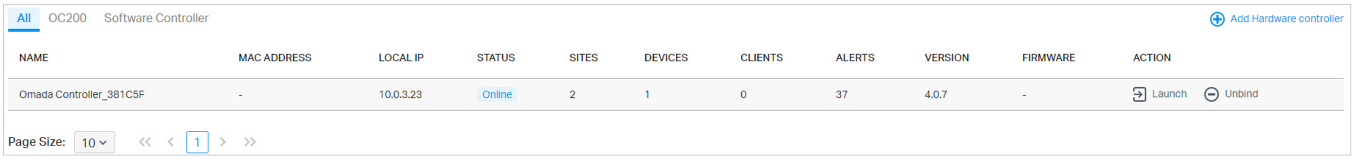
Password:

- **For Omada Cloud-Based Controller**

Your Omada Cloud-Based Controller is based on the Cloud, so it’s naturally accessible through Cloud Service. No additional preparation is needed.

2. Access your controller through Cloud Service

Go to Omada Cloud and login with your TP-Link ID and password. A list of controllers that have been bound with your TP-Link ID will appear. Then click Launch to manage the controller.



All OC200 Software Controller

Add Hardware controller

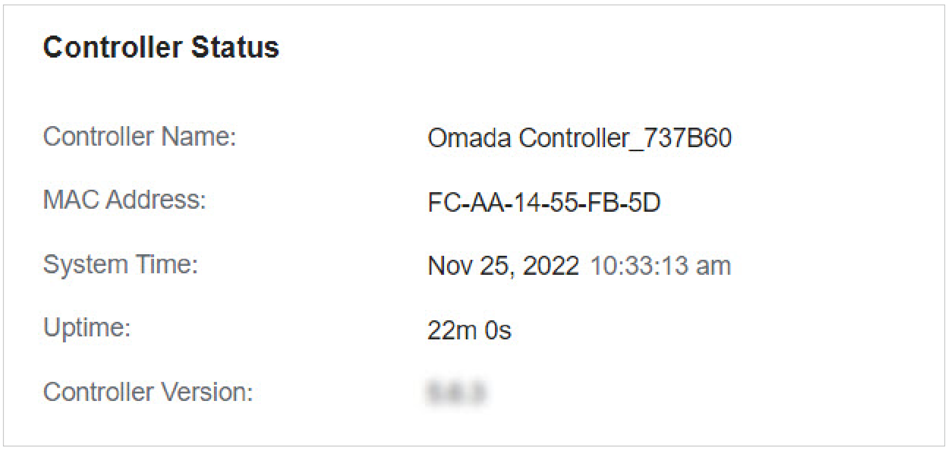
NAME	MAC ADDRESS	LOCAL IP	STATUS	SITES	DEVICES	CLIENTS	ALERTS	VERSION	FIRMWARE	ACTION
Omada Controller_381C5F	-	10.0.3.23	Online	2	1	0	37	4.0.7	-	Launch Unbind

Page Size: 10

3. 3 Maintenance

3. 3. 1 Controller Status

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Maintenance. In Controller Status, you can view the controller-related information and status.



Controller Status

Controller Name: Omada Controller_737B60

MAC Address: FC-AA-14-55-FB-5D

System Time: Nov 25, 2022 10:33:13 am

Uptime: 22m 0s

Controller Version: [redacted]

Controller Name	Displays the controller name, which identifies the controller. You can specify the controller name in 5. 1. 1 General Settings.
MAC Address	Displays the MAC address of the controller.
System Time	Displays the system time of the controller. The system time is based on the time zone which you configure in 5. 1. 1 General Settings.
Uptime	Displays how long the controller has been working.
Controller Version	Displays the software version of the controller.

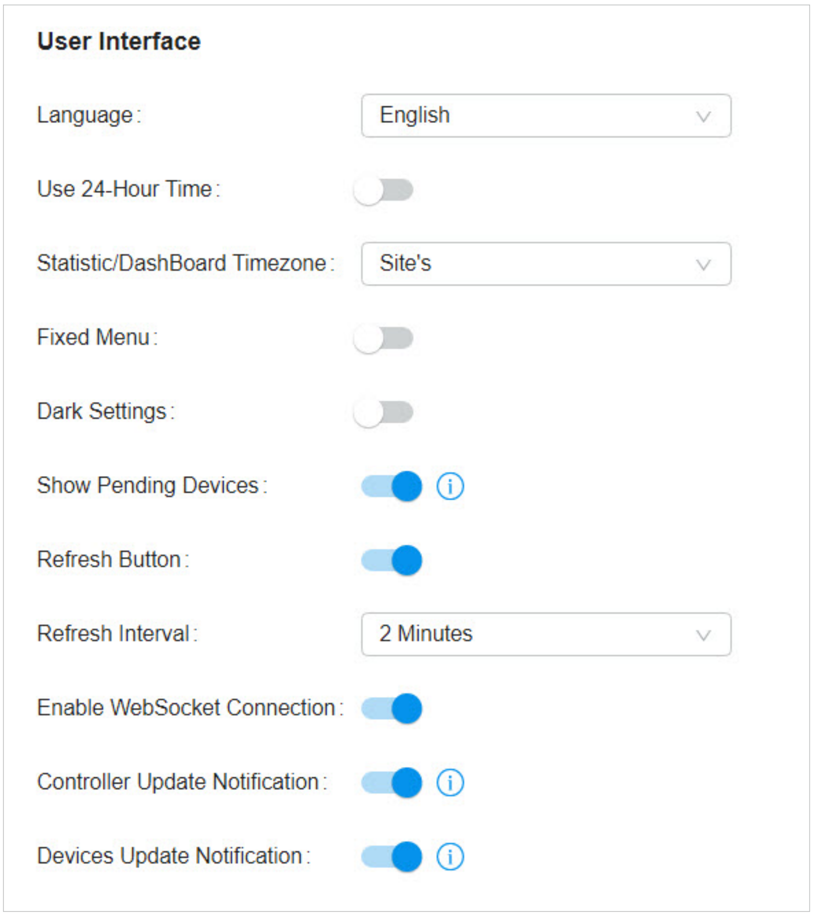
3. 3. 2 User Interface

Overview

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

Configuration

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Maintenance. In User Interface, configure the parameters and click Apply.



User Interface

Language: English

Use 24-Hour Time: ○

Statistic/DashBoard Timezone: Site's

Fixed Menu: ○

Dark Settings: ○

Show Pending Devices: ● ⓘ

Refresh Button: ●

Refresh Interval: 2 Minutes

Enable WebSocket Connection: ●

Controller Update Notification: ● ⓘ

Devices Update Notification: ● ⓘ

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.
Statistic/Dashboard Timezone	Select which Timezone the time of statistics and the dashboard is based on. Site's: Site's Timezone is set in Site Configuration of the corresponding site. Browser's: Browser's Timezone is synchronized with the browser configuration. Controller's: Controller's Timezone is set in General Settings of the controller. UTC: UTC (Coordinated Universal Time) is the common time standard across the world.
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 WebSocket Connection 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.
Controller Update Notification	With this feature enabled, you will receive an update notification when a new controller version is available.
Devices Update Notification	With this feature enabled, you will receive an update notification when a new firmware version for your device is available.

3. 3. 3 Backup & Restore

Overview

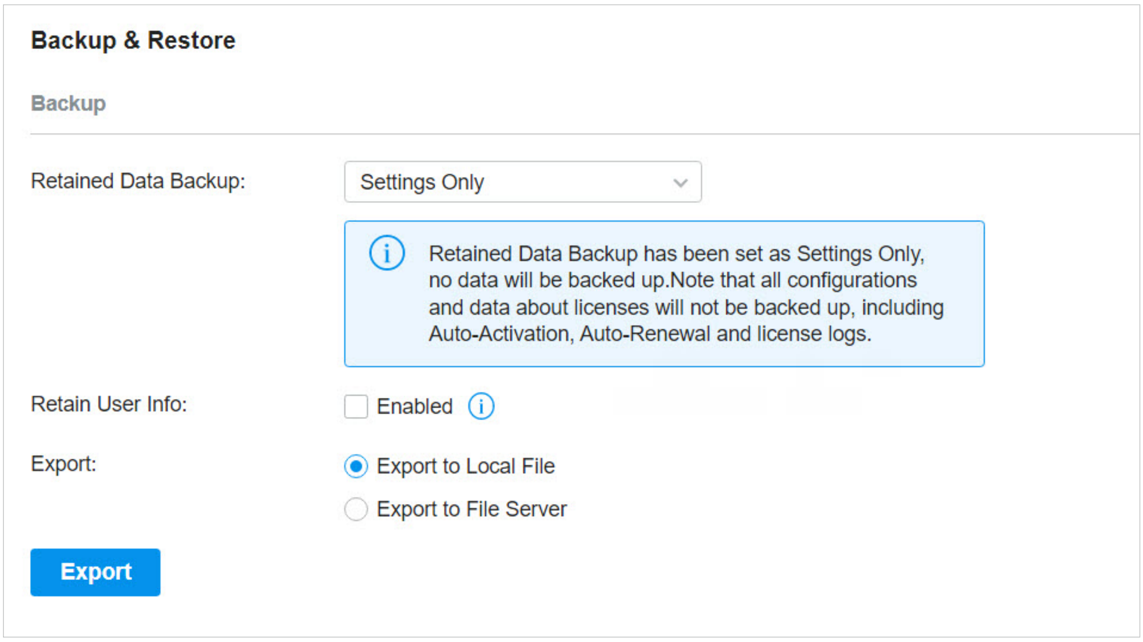
You can backup the configuration and data of your controller to prevent any loss of important information. If necessary, restore the controller to a previous status using the backup file.

Configuration

- **Backup**

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Maintenance > Backup & Restore > Backup, click Export to export and save the backup file.

If you want to export the data to a file server, configure the parameters accordingly and click Export.



Backup & Restore

Backup

Retained Data Backup: Settings Only

Retained Data Backup has been set as Settings Only, no data will be backed up.Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

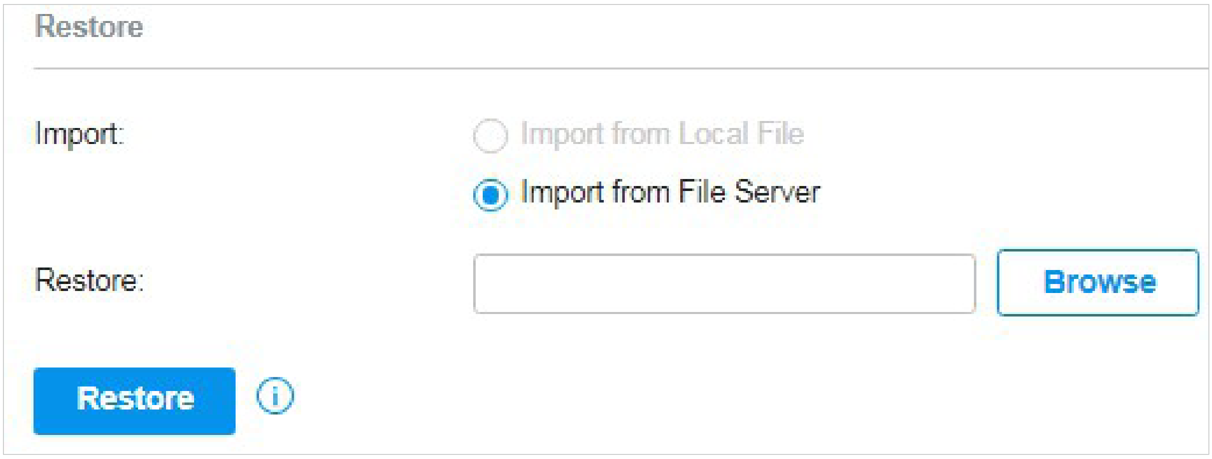
Retain User Info: □ Enabled

Export: ● Export to Local File ○ Export to File Server

Retained Data Backup	Select the time range in the drop-down menu of Retained Data Backup. Only configuration and data within the time range is backed up. If you select Settings Only, only configuration (no data) is backed up.
Retain User Info	Select this option if you want to retain local and cloud user information.
Export	Select where you want to export the data to. Export to Local File: Export and save the data locally. It is not supported when accessing the controller via cloud. Export to File Server: Export and save the data to a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.

- **Restore**

Go to Settings > Maintenance > Backup & Restore > Restore. In Backup & Restore section, Click Browse and select a backup file from your computer or file server. Click Restore.



Restore

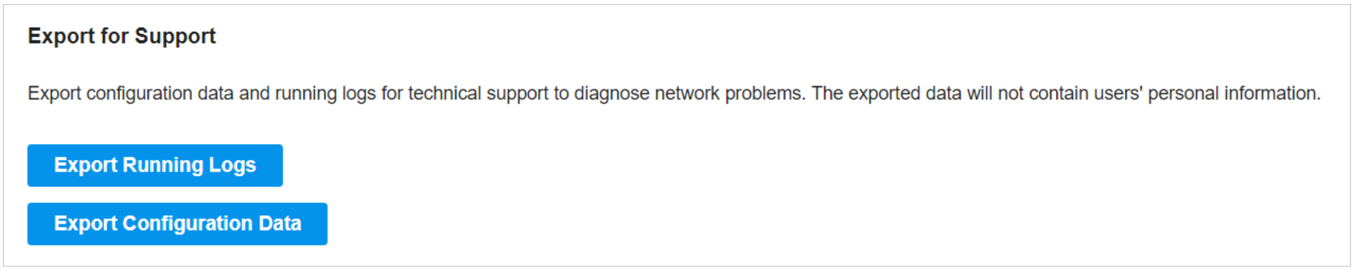
Import: ○ Import from Local File ● Import from File Server

Restore:

Import	Select where you store the restore file. Import from Local File: Import the data locally. It is not supported when accessing the controller via cloud. Import from File Server: Import the data from a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.
Restore	Select the backup file to restore the information.

- **Export for Support**

Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Maintenance > Export for Support. You can export configuration data and running logs for technical support to diagnose network problems. The exported data will not contain users' personal information.



Export for Support

Export configuration data and running logs for technical support to diagnose network problems. The exported data will not contain users' personal information.

Export Running Logs	Click to export running logs.
Export Configuration Data	Click to export configuration data.

Note:

Configuration data cannot be imported into the controller through restore.

3. 4 Migration

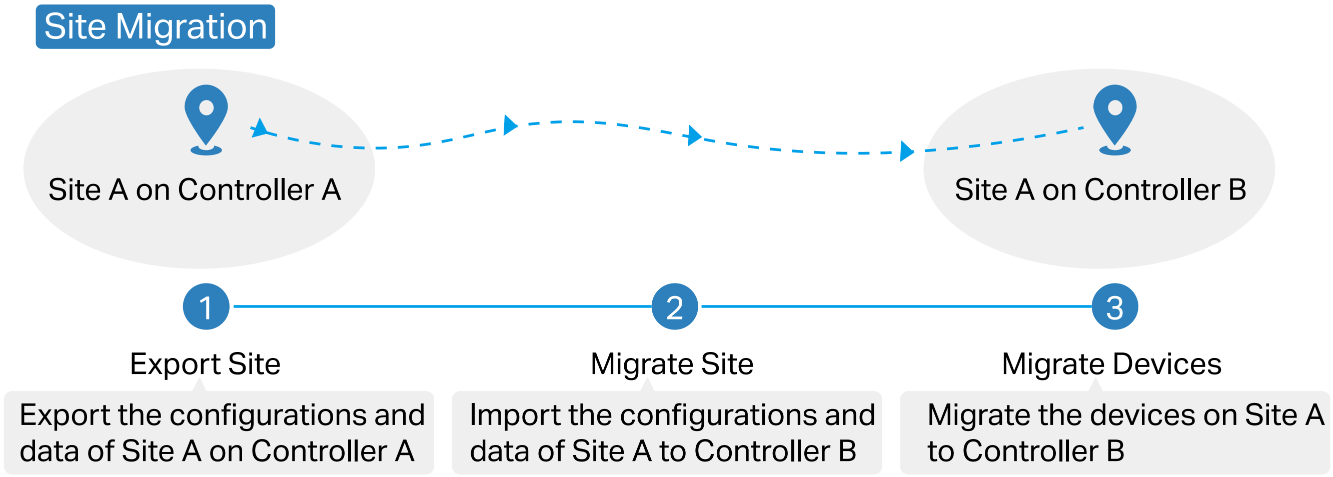
Migration services allow users to migrate the configurations and data to any other controller. Migration services include 5. 4. 1 Site Migration and 5. 4. 2 Controller Migration, covering all the needs to migrate both a single site and the whole controller.

3. 4. 1 Site Migration

Overview

Site Migration allows the administrators to export a site from the current controller to any other controller that has the same version. All the configurations and data of the site will be migrated to the target controller.

The process of migrating configurations and data from a site to another controller can be summarized in three steps: Export Site, Migrate Site and Migrate Devices.


Site Migration
Site A on Controller A
Site A on Controller B
1
Export Site
Export the configurations and data of Site A on Controller A
2
Migrate Site
Import the configurations and data of Site A to Controller B
3
Migrate Devices
Migrate the devices on Site A to Controller B

Step1: Export Site

Export the configurations and data of the site to be migrated as a backup file.

Step2: Migrate Site

In the target controller, import the backup file of the original site.

Step3: Migrate Devices

Migrate the devices which are on the original site to the target controller.

Configuration

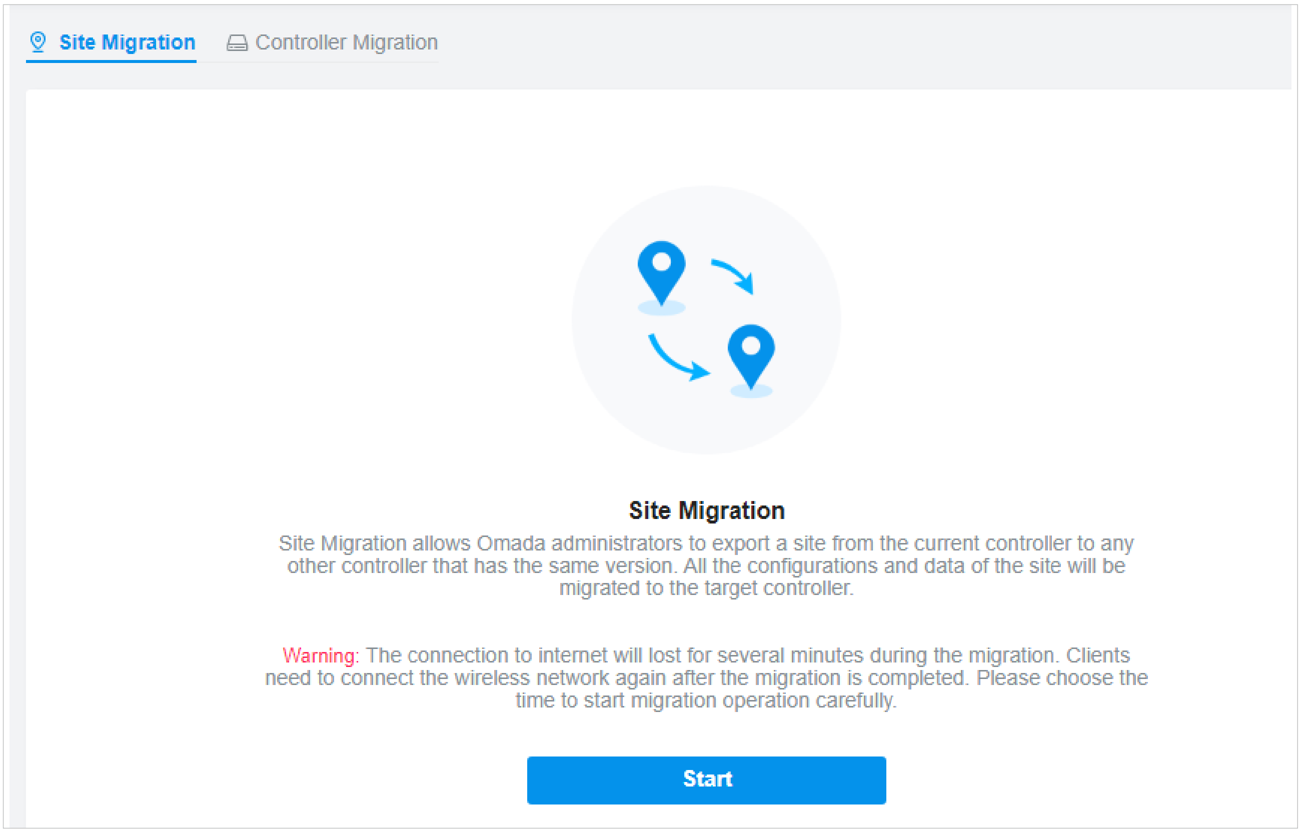
To migrate a site to another controller, follow these steps below.

Note:

The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Export Site
Migrate Site
Migrate Devices

1. Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Migration. On the Site Migration tab, click start button on the following page.

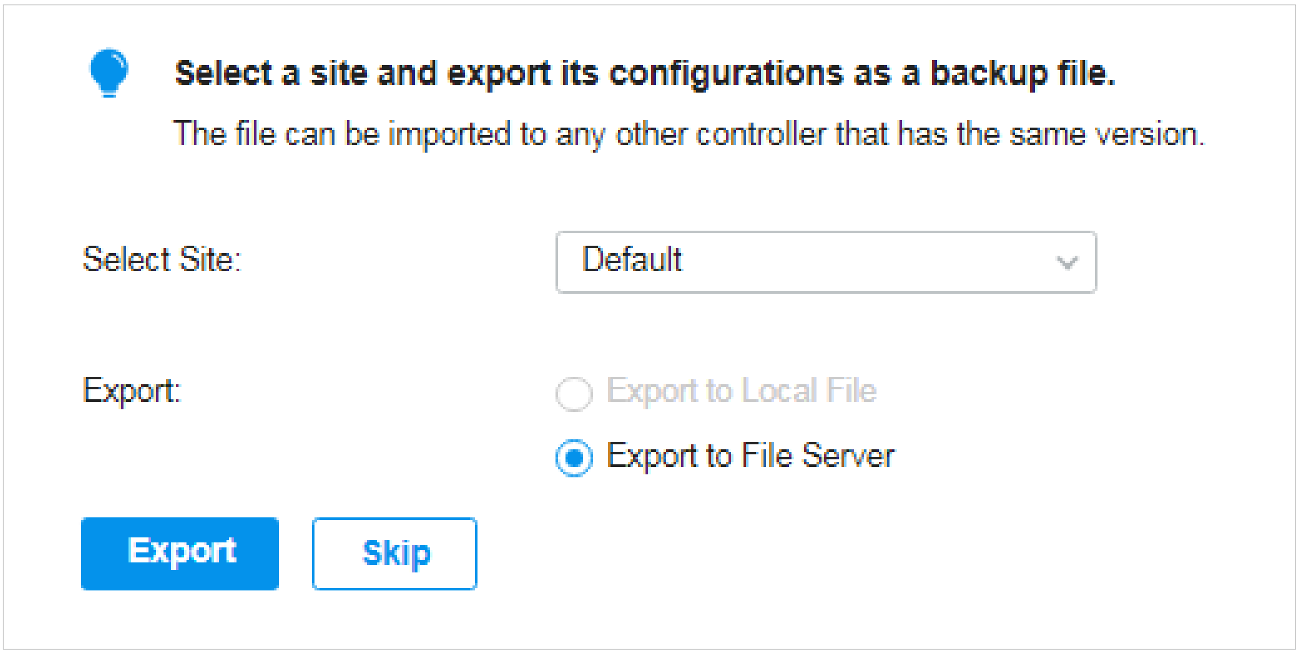


Site Migration

Site Migration allows Omada administrators to export a site from the current controller to any other controller that has the same version. All the configurations and data of the site will be migrated to the target controller.

Warning: The connection to internet will lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

2. Select the site to be imported into the second controller in the Select Site drop-down list. Select where you want to export and save the backup file. Click Export to download the file of the current site. If you have backed up the file, click Skip.



Select a site and export its configurations as a backup file.

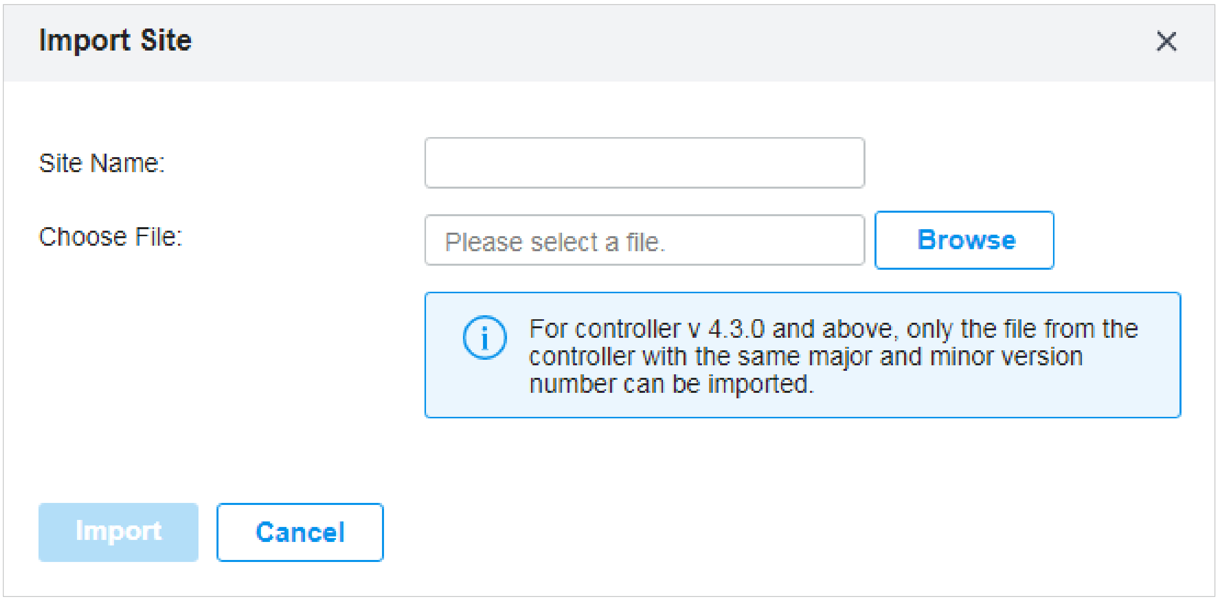
The file can be imported to any other controller that has the same version.

Select Site: Default

Export: ○ Export to Local File ● Export to File Server

Export Site › **Migrate Site** › Migrate Devices

1. Start and log in to the target controller, click Sites: Site A the top right corner of the screen and select Import Site, and then the following window will pop up. Note that for controller v 4.3.0 and above, only the file from the controller with the same major and minor version number can be imported.



Import Site

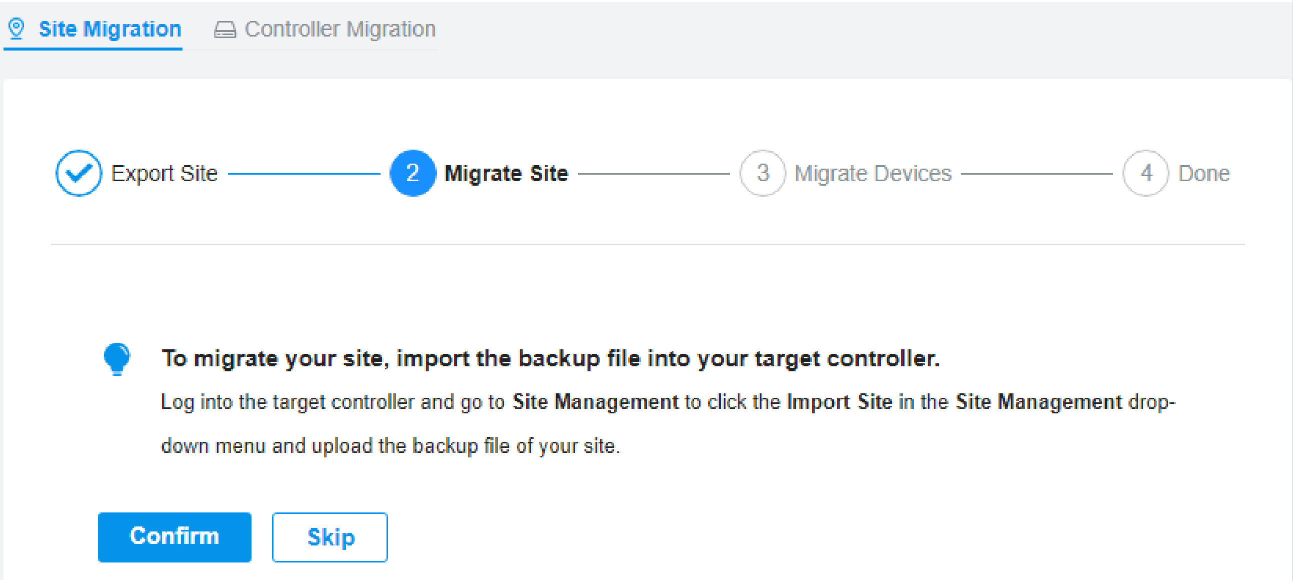
Site Name:

Choose File: Please select a file. Browse

For controller v 4.3.0 and above, only the file from the controller with the same major and minor version number can be imported.

2. Enter a unique name for the new site. Click Browse to upload the file of the site to be imported and click Import to import the site.

3. After the file has been imported to the target controller, go back to the previous controller and click Confirm.

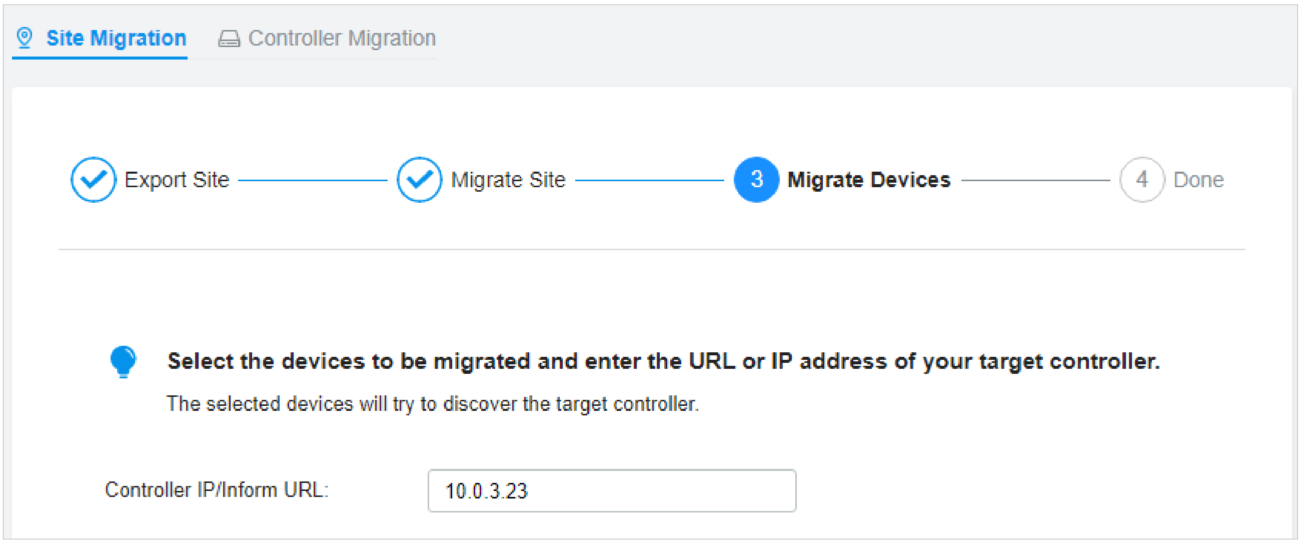


To migrate your site, import the backup file into your target controller.

Log into the target controller and go to **Site Management** to click the **Import Site** in the **Site Management** drop-down menu and upload the backup file of your site.

Export Site → Migrate Site → **Migrate Devices**

1. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



Select the devices to be migrated and enter the URL or IP address of your target controller.

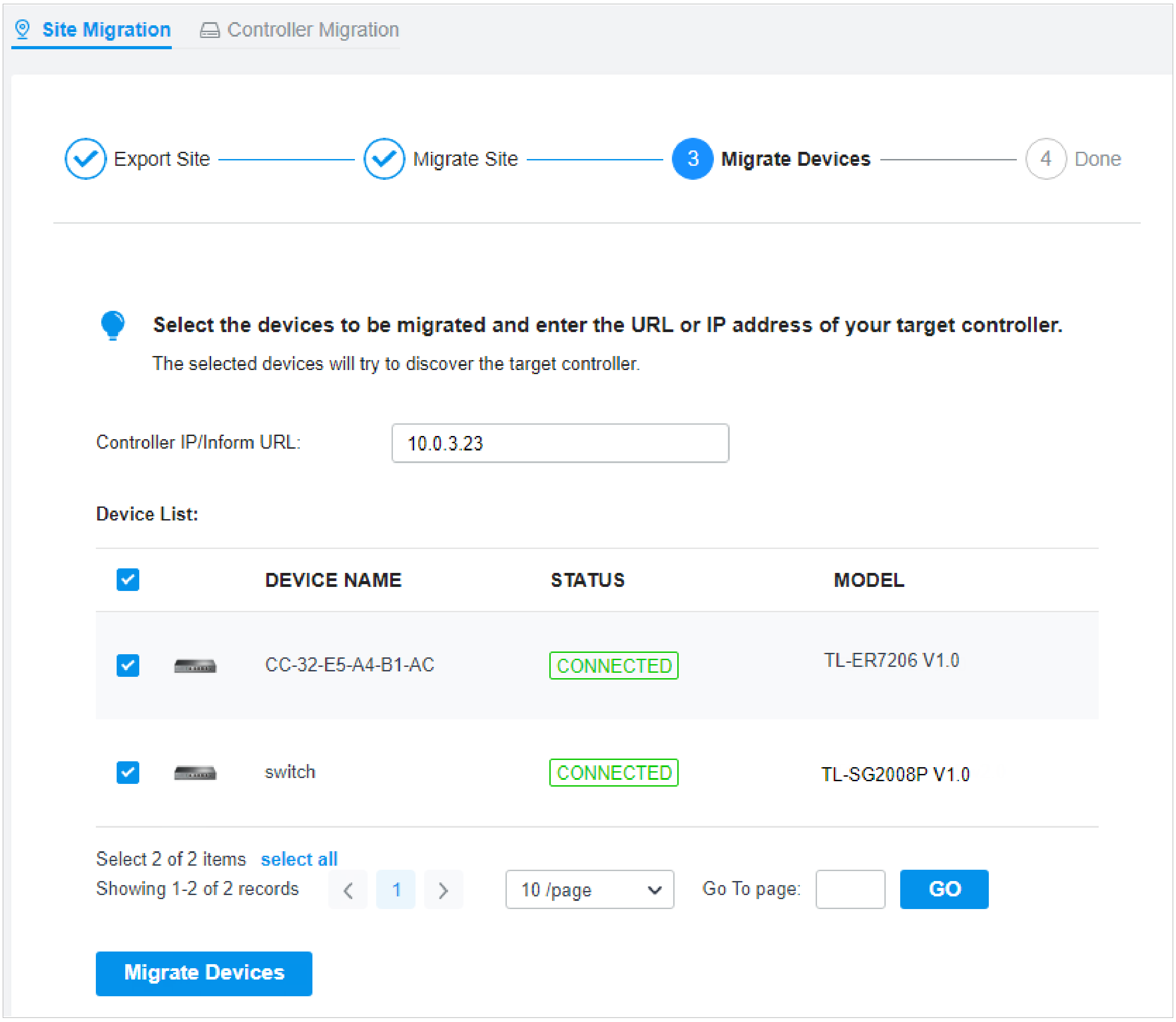
The selected devices will try to discover the target controller.

Controller IP/Inform URL: 10.0.3.23

Note:

Make sure that you enter the correct IP address or URL of the target controller to establish the communication between Omada managed devices and your target controller. Otherwise Omada managed devices cannot be adopted by the target controller.

2. Select the devices that are to be migrated by clicking the box next to each device. By default, all the devices are selected. Click Migrate Devices to migrate the selected devices to the target controller.



Select the devices to be migrated and enter the URL or IP address of your target controller.

The selected devices will try to discover the target controller.

Controller IP/Inform URL: 10.0.3.23

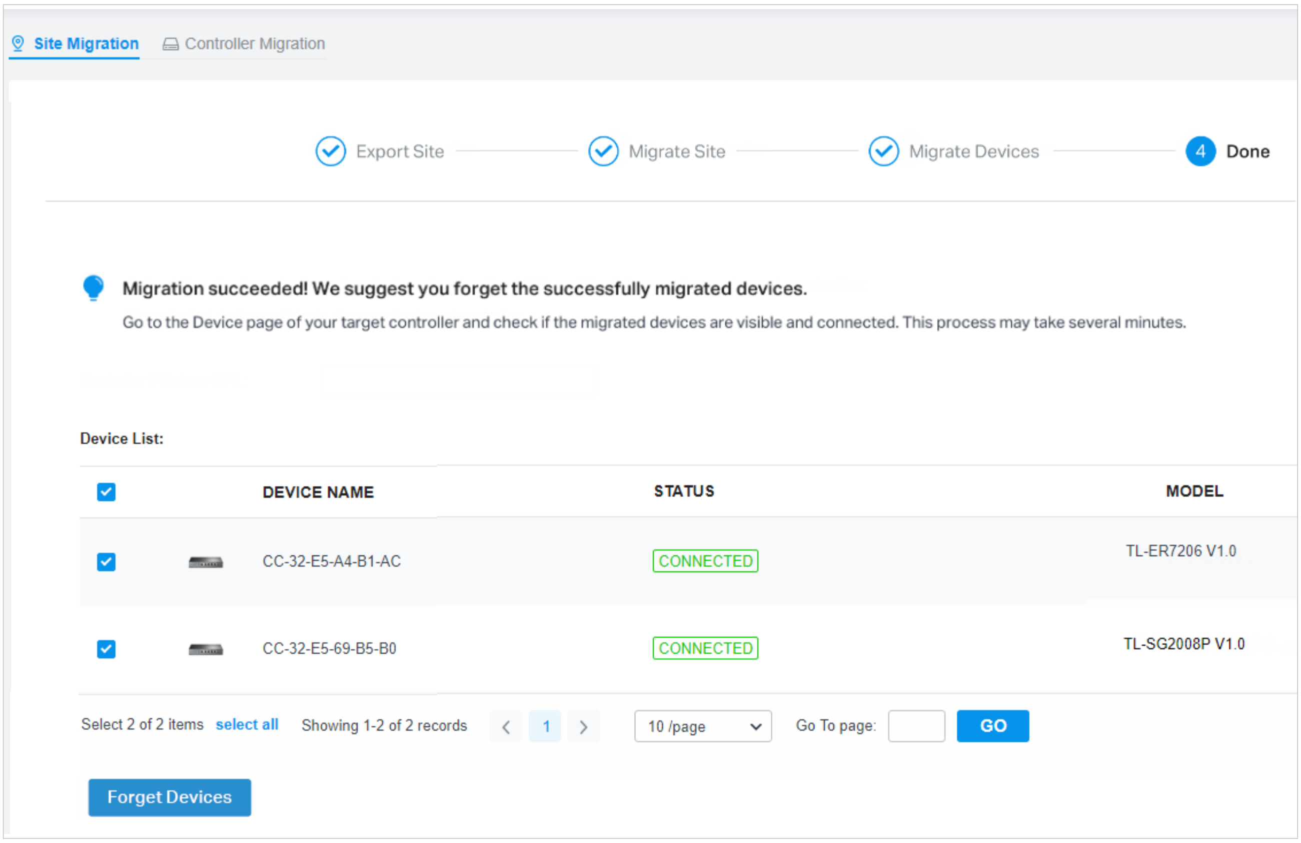
Device List:

☑	DEVICE NAME	STATUS	MODEL
☑	CC-32-E5-A4-B1-AC	CONNECTED	TL-ER7206 V1.0
☑	switch	CONNECTED	TL-SG2008P V1.0

Select 2 of 2 items select all

Showing 1-2 of 2 records

3. Verify that all the migrated devices are visible and connected on the target controller. When all the migrated devices are in Connected status on the Device page on the target controller, click Forget Devices to finish the migration process.



Migration succeeded! We suggest you forget the successfully migrated devices.

Go to the Device page of your target controller and check if the migrated devices are visible and connected. This process may take several minutes.

Device List:

☑		DEVICE NAME	STATUS	MODEL
☑		CC-32-E5-A4-B1-AC	CONNECTED	TL-ER7206 V1.0
☑		CC-32-E5-69-B5-B0	CONNECTED	TL-SG2008P V1.0

Select 2 of 2 items select all Showing 1-2 of 2 records < 1 > 10 /page Go To page:

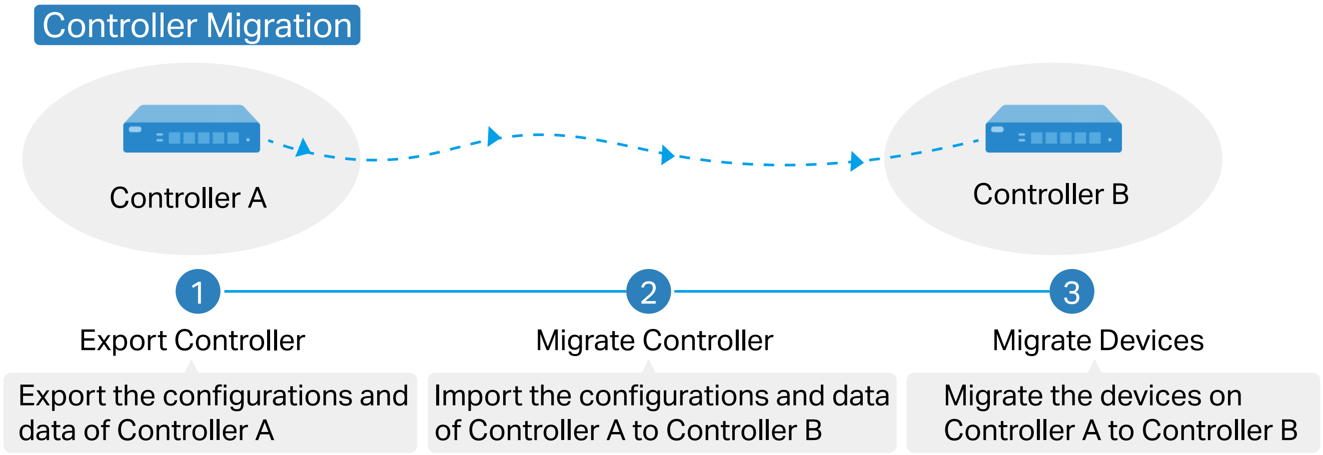
4. When the migration process is completed, all the configuration and data are migrated to the target controller. You can delete the previous site if necessary.

3. 4. 2 Controller Migration

Overview

Controller Migration allows Omada administrators to migrate the configurations and data from the current controller to any other controller that has the same version.

The process of migrating configurations and data from the current controller to another controller can be summarized in three steps: Export Controller, Migrate Controller and Migrate Devices.



Export the configurations and data of Controller A

Import the configurations and data of Controller A to Controller B

Migrate the devices on Controller A to Controller B

Step1: Export Controller

Export the configurations and data of the current controller as a backup file.

Step2: Migrate Controller

In the target controller, import the backup file of the current controller.

Step3: Migrate Devices

Migrate the devices on the current controller to the target controller.

Configuration

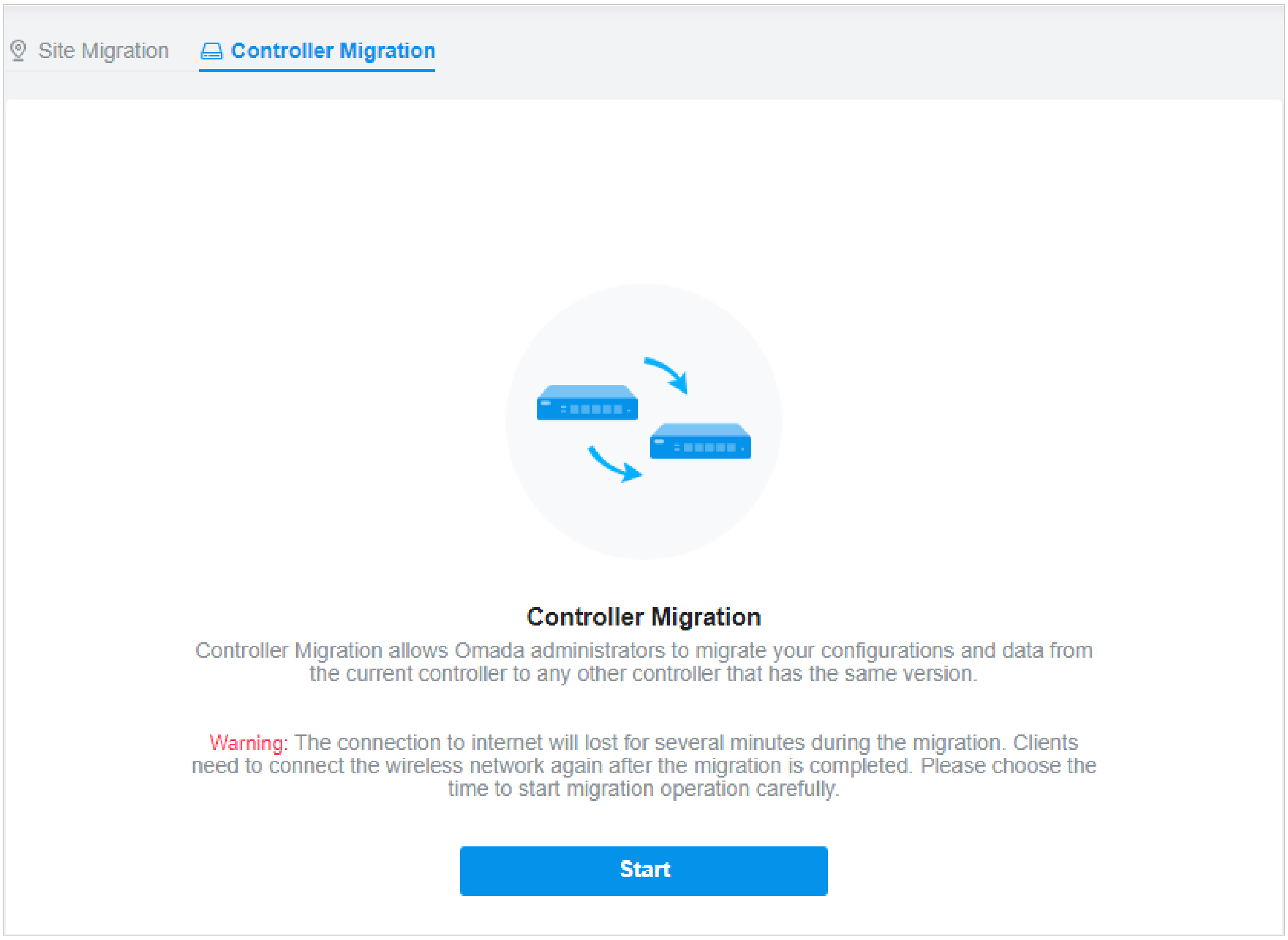
To migrate your controller, follow these steps below.

Note:

The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Export Controller | Migrate Controller | Migrate Devices

1. Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Migration. On the Controller Migration tab, click start button on the following page.

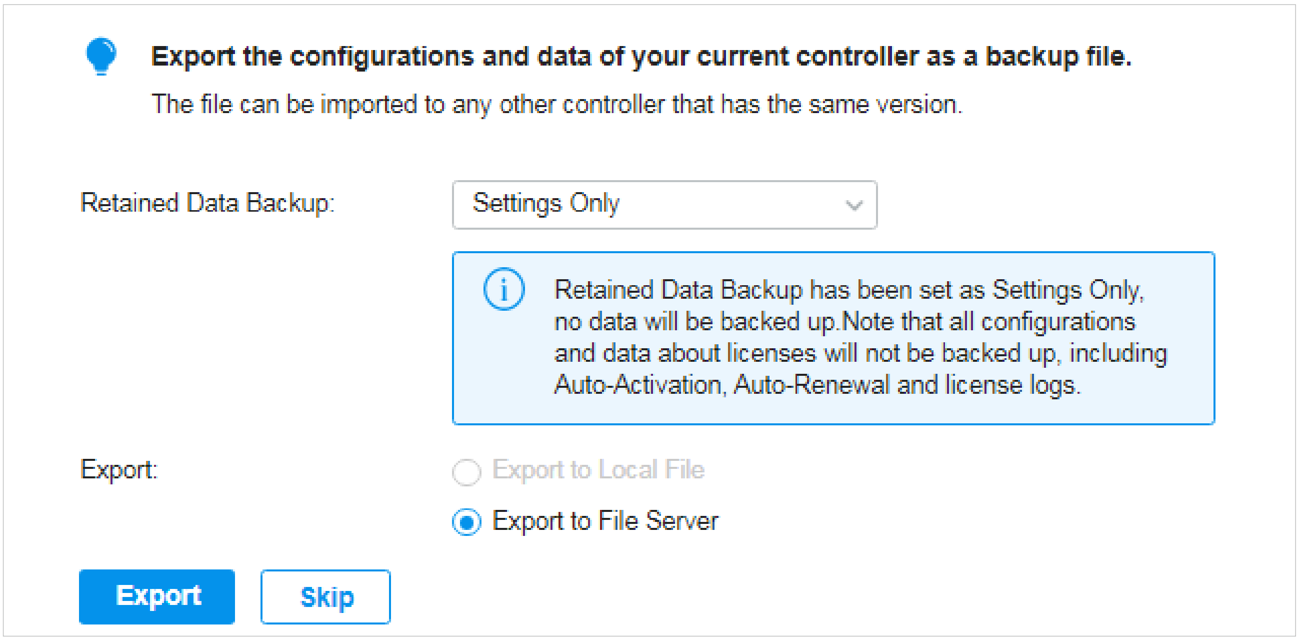


Controller Migration

Controller Migration allows Omada administrators to migrate your configurations and data from the current controller to any other controller that has the same version.

Warning: The connection to internet will lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

2. Select the length of time in days that data will be backed up in the Retained Data Backup, and where you want to export and save the data. Click Export to export the configurations and data of your current controller as a backup file. If you have backed up the file, click Skip.



Export the configurations and data of your current controller as a backup file.

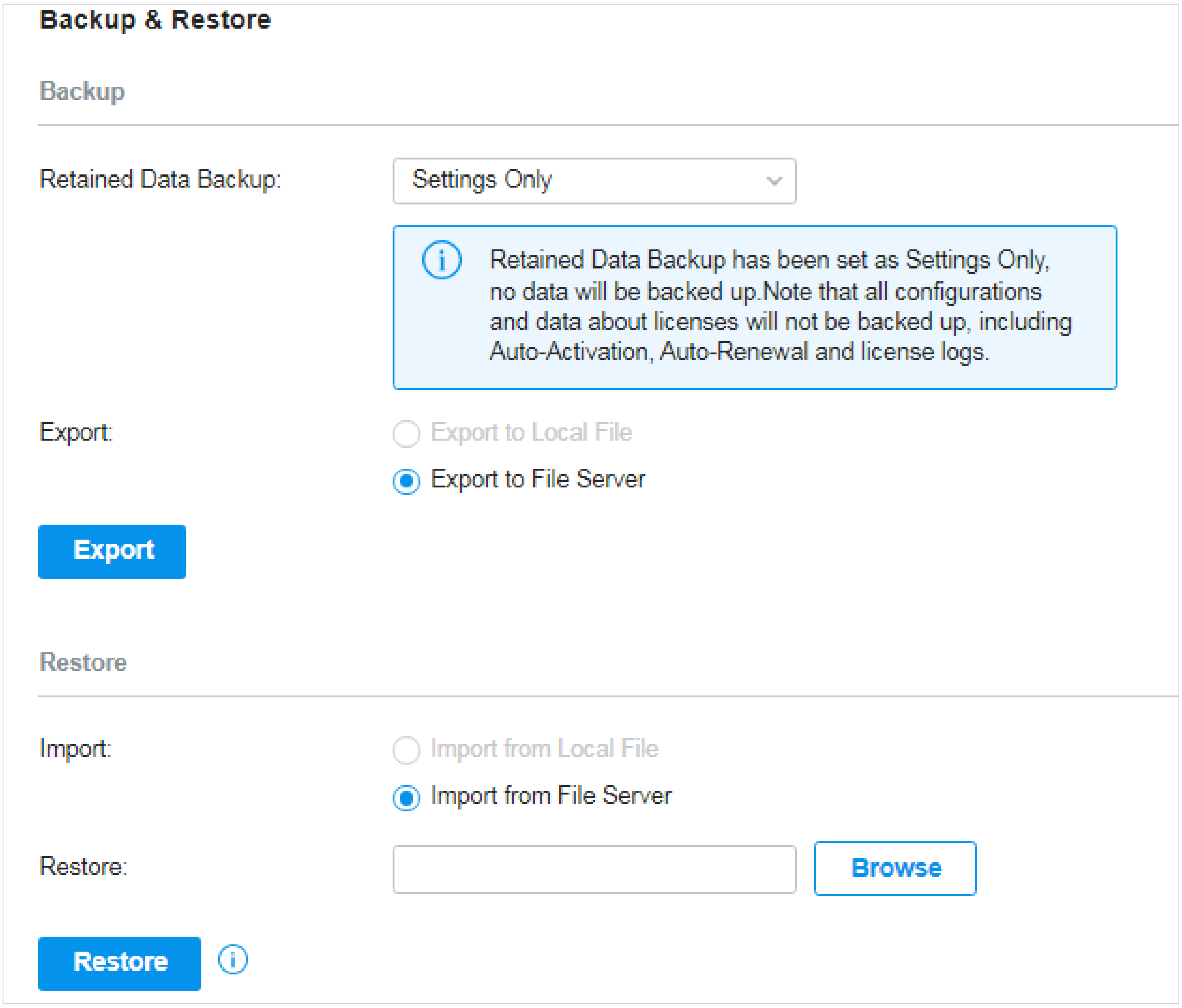
The file can be imported to any other controller that has the same version.

Retained Data Backup: Settings Only

Retained Data Backup has been set as Settings Only, no data will be backed up.Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

Export: ○ Export to Local File ● Export to File Server

1. Log in to the target controller. Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Maintenance > Backup & Restore. Click Browse to locate and choose the backup file of the previous controller. Then click Restore to upload the file.



Backup & Restore

Backup

Retained Data Backup: Settings Only

Retained Data Backup has been set as Settings Only, no data will be backed up.Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

Export: ○ Export to Local File ● Export to File Server

Export

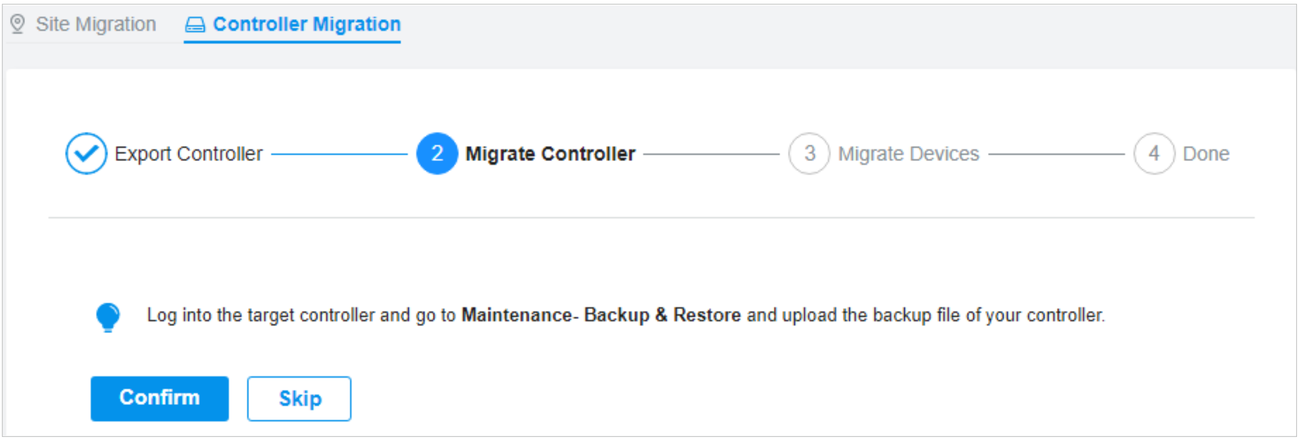
Restore

Import: ○ Import from Local File ● Import from File Server

Restore: Browse

Restore

2. After the file has been imported to the target controller, go back to the previous controller and click Confirm.



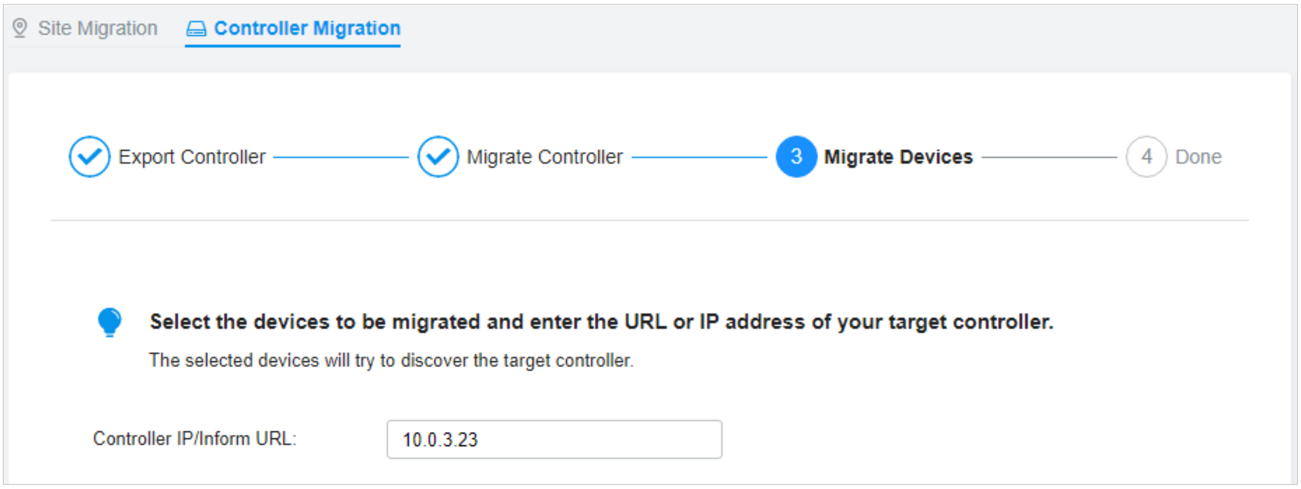
Site Migration Controller Migration

✓ Export Controller — 2 Migrate Controller — 3 Migrate Devices — 4 Done

Log into the target controller and go to **Maintenance- Backup & Restore** and upload the backup file of your controller.

Confirm Skip

1. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



Select the devices to be migrated and enter the URL or IP address of your target controller.

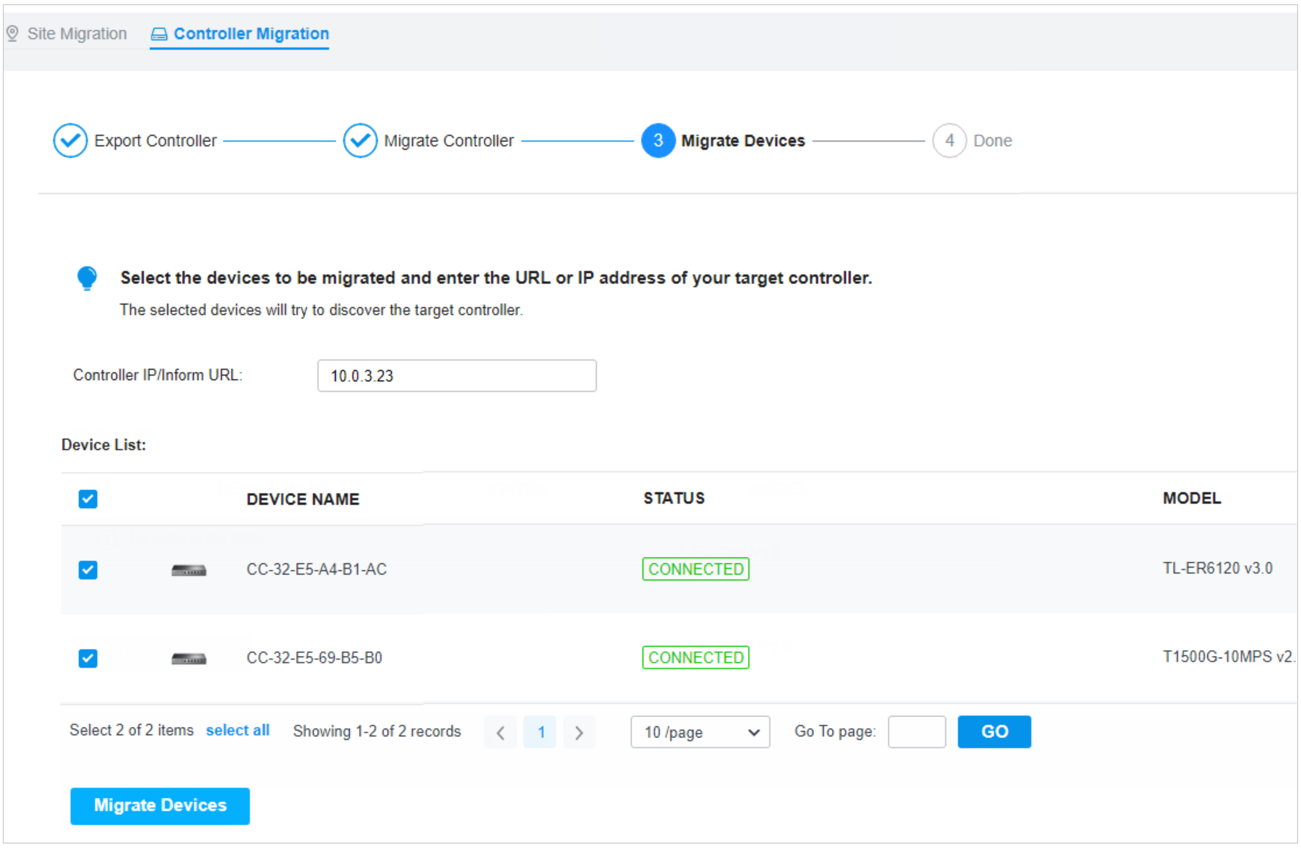
The selected devices will try to discover the target controller.

Controller IP/Inform URL: 10.0.3.23

Note:

Make sure that you enter the correct IP address or URL of the target controller to establish the communication between Omada managed devices and your target controller. Otherwise Omada managed devices cannot be adopted by the target controller.

2. Select the devices that are to be migrated by clicking the box next to each device. By default, all the devices are selected. Click Migrate Devices to migrate the selected devices to the target controller.



Select the devices to be migrated and enter the URL or IP address of your target controller.

The selected devices will try to discover the target controller.

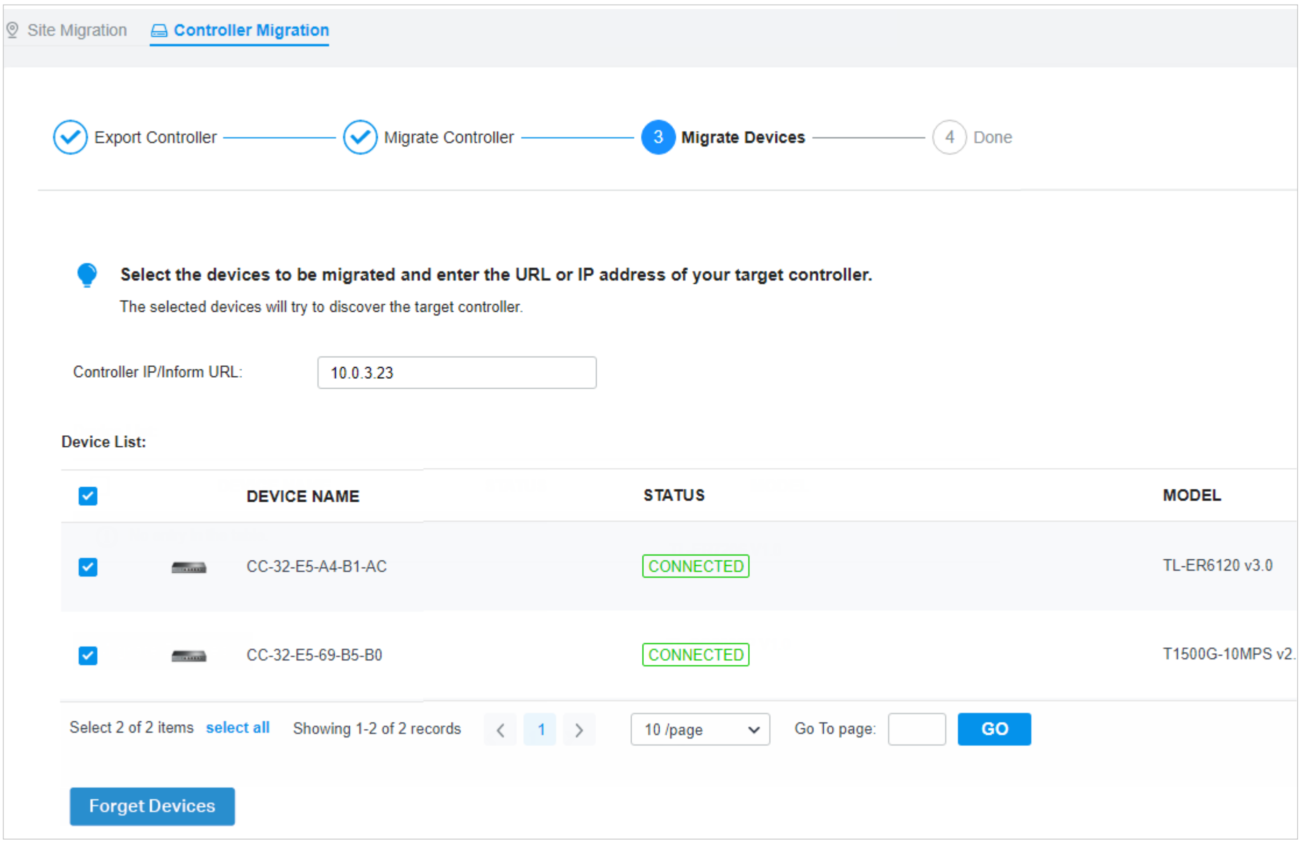
Controller IP/Inform URL: 10.0.3.23

Device List:

☑	DEVICE NAME	STATUS	MODEL
☑	CC-32-E5-A4-B1-AC	CONNECTED	TL-ER6120 v3.0
☑	CC-32-E5-69-B5-B0	CONNECTED	T1500G-10MPS v2.

Select 2 of 2 items select all Showing 1-2 of 2 records < 1 > 10 /page Go To page: GO

3. Verify that all the migrated devices are visible and connected on the target controller. When all the migrated devices are in Connected status on the Device page on the target controller, click Forget Devices to finish the migration process.



Select the devices to be migrated and enter the URL or IP address of your target controller.

The selected devices will try to discover the target controller.

Controller IP/Inform URL: 10.0.3.23

Device List:

☑	DEVICE NAME	STATUS	MODEL
☑	CC-32-E5-A4-B1-AC	CONNECTED	TL-ER6120 v3.0
☑	CC-32-E5-69-B5-B0	CONNECTED	T1500G-10MPS v2.

Select 2 of 2 items select all Showing 1-2 of 2 records 1 10 /page Go To page: GO
Forget Devices

When the migration process is completed, all the configuration and data are migrated to the target controller. You can uninstall the previous controller if necessary.

3. 5 Auto Backup

Overview

With Auto Backup enabled, the controller will be scheduled to back up the configurations and data automatically at the specified time. You can easily restore the configurations and data when needed.

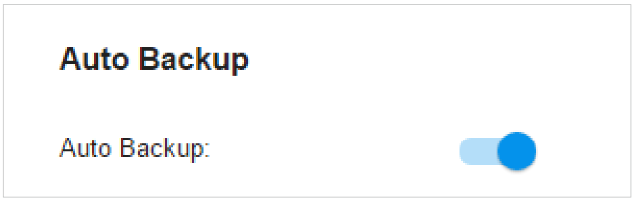
Note:

- For OC200, Auto Backup is available only when it is powered by a PoE device and a storage device is connected to its USB port.
- On Omada Cloud-Based Controller, you have no need to configure Auto Backup. It will automatically save your configurations and data on the cloud.

Configuration

To configure Auto Backup, follow these steps:

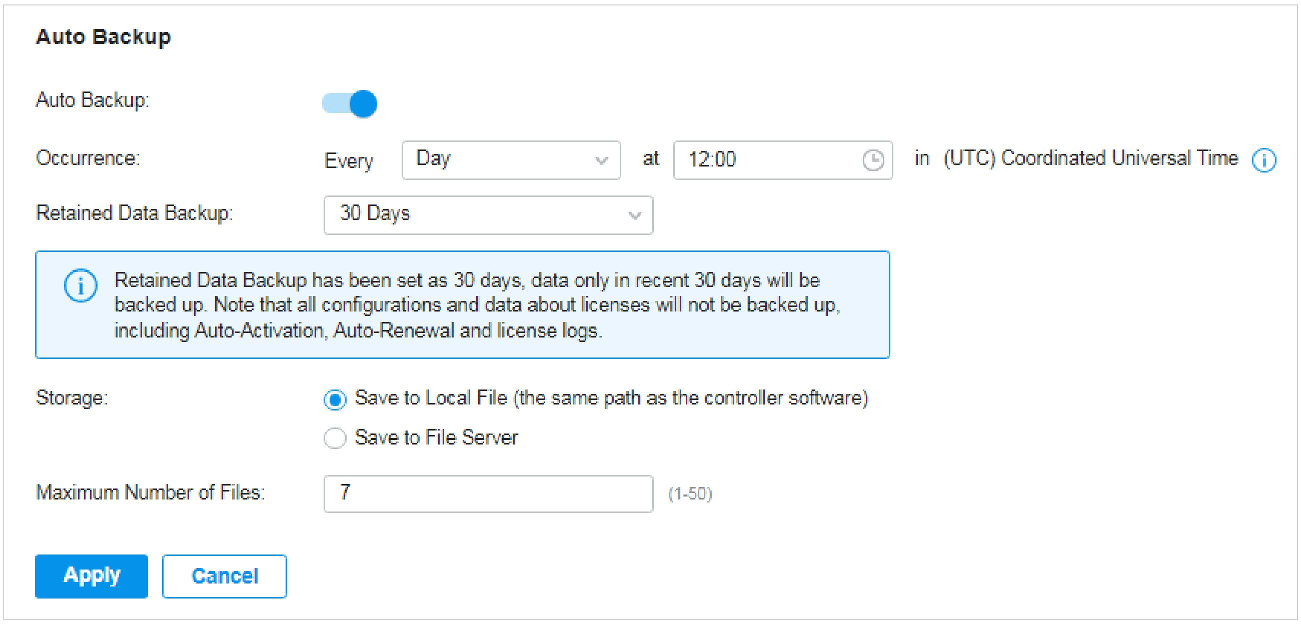
1. Select Global from the drop-down list of Organization in the upper right corner. Go to Settings > Maintenance > Auto Backup. Click ○ to enable Auto Backup.



Auto Backup

Auto Backup: ●

2. Configure the following parameters to specify the rules of Auto Backup. Click Apply.



Auto Backup

Auto Backup: ●

Occurrence: Every Day at 12:00 in (UTC) Coordinated Universal Time

Retained Data Backup: 30 Days

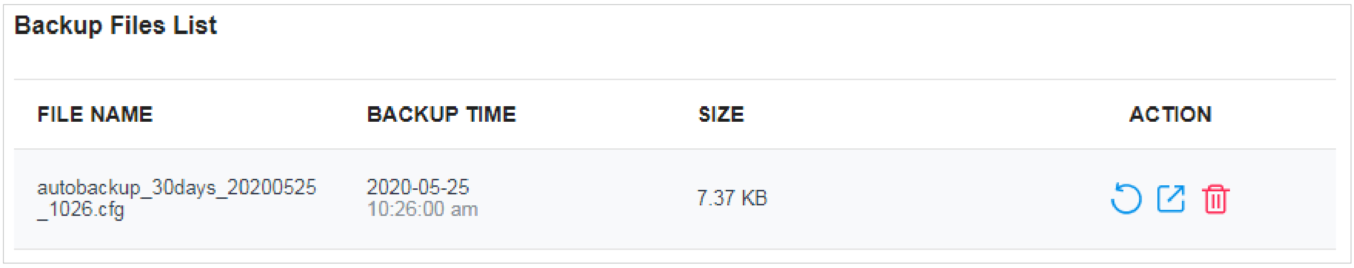
Retained Data Backup has been set as 30 days, data only in recent 30 days will be backed up. Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

Storage: ● Save to Local File (the same path as the controller software)
○ Save to File Server

Maximum Number of Files: 7 (1-50)

Occurrence	Specify when to perform Auto Backup regularly. Select Every Day, Week, Month, or Year first and then set a time to back up files. Note the time availability when you choose Every Month. For example, if you choose to automatically backup the data on the 31st of every month, Auto Backup will not take effect when it comes to the month with no 31st, such as February, April, and June.
Retained Data Backup	Select the length of time in days that data will be backed up. Settings Only: Back up controller settings only. 7 Days/1 Month/2 Months/3 Months/6 Months/1 Year: Back up the data in the recent 7 days/1 month/2 months/3 months/6 months/1 year. All Time: (Only for Omada Software Controller) Back up all data in the controller.
Storage	Select where you want to save the backup file. Save to Local File: The backup file will be saved as a local file. Save to File Server: The backup file will be saved in the specified file server. Four types of file server are available: FTP, TFTP, SFTP, and SCP.
Saving Path	(Only for Omada Hardware Controller) Select a path to save the backup files.
Maximum Number of Files	Specify the maximum number of backup files to save.

You can view the name, backup time and size of backup files in Backup Files List.



Backup Files List

FILE NAME	BACKUP TIME	SIZE	ACTION
autobackup_30days_20200525_1026.cfg	2020-05-25 10:26:00 am	7.37 KB	↻ ↗ 🗑

To restore, export or delete the backup file, click the icon in the Action column.

↻	Restore the configurations and data in the backup file. All current configurations will be replaced after the restoration. To keep the backup data safe, please wait until the operation is finished. This will take several minutes.
↗	Export the backup file. The exported file will be saved in the saving path of your web browser.
🗑	Delete the backup file.

ⓘ Note:

- If the backup file is saved to file server and the type SCP / TFTP is selected, it will not included in the Backup Files List, and it cannot be exported, restored, or deleted.
- To back up data manually and restore the data to the controller, refer to 5. 3. 3 Backup & Restore to configure Backup&Restore.
- The configuration of cloud users can be neither backed up nor restored. To add cloud users, please refer to 9. 3 Manage and Create Cloud User Accounts.

4

Manage Accounts of Omada SDN Controller

This chapter gives an introduction to different user levels of controller accounts and guides you on how to create and manage them. The chapter includes the following sections:

- 4. 1 Introduction to User Accounts
- 4. 3 Manage and Create Local User Accounts
- 4. 4 Manage and Create Cloud User Accounts

4. 1 Introduction to User Accounts

Omada SDN Controller offers three levels of access available for users: **master administrator**, **administrator**, and **viewer**. You can also create new account roles and customize their permissions to access different features.

Since the controller can be accessed both locally and via cloud access, users can be further grouped into local users and cloud users.

Multi-level administrative account presents a hierarchy of permissions for different levels of access to the controller as required. This approach ensures security and gives convenience for management.

Moreover, in the user accounts list of the main administrator, all accounts created by the main administrator will be displayed. The accounts created by each administrator will be hidden by default, making the interface more systematic and to the point.

■ Master Administrator

The master administrator has access to all features.

The account who first launches the controller will be the master administrator. It cannot be changed and deleted.

■ Administrator

Administrators have no permission to some modules, mainly including cloud access, migration, auto-backup and global view logs. They have read-only permission to some modules, such as global view license management and custom account roles.

Administrators can be created and deleted only by the master administrator.

■ Viewer

Viewers can view the status and settings of the network, and change the settings in Hotspot Manager.

The entrance to Account page is hidden for viewers, and they can be created or deleted by the master administrator and administrators.

■ Custom roles

Custom roles can be configured to access different features.

They can be created or deleted only by the master administrator.

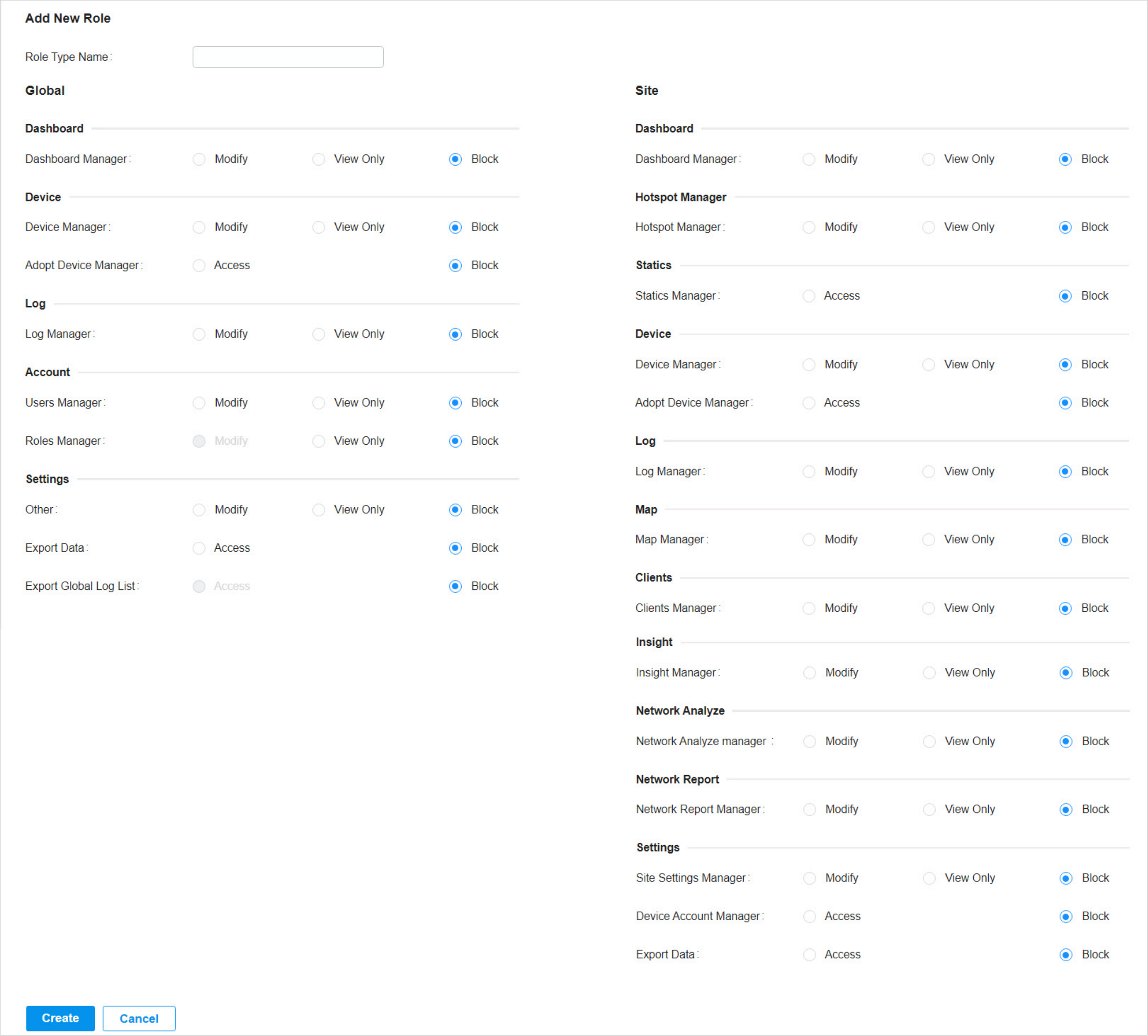
ⓘ Note:

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.

4. 2 Create and Manage Custom Account Roles

1. Select Global from the drop-down list of Organization in the top-right corner. Go to Account > Role.

2. Click Add New Role. Specify the role type name and customize the permissions for the role.



Add New Role

Role Type Name:

Global

Dashboard

Dashboard Manager: ○ Modify ○ View Only ● Block

Device

Device Manager: ○ Modify ○ View Only ● Block

Adopt Device Manager: ○ Access ● Block

Log

Log Manager: ○ Modify ○ View Only ● Block

Account

Users Manager: ○ Modify ○ View Only ● Block

Roles Manager: ○ Modify ○ View Only ● Block

Settings

Other: ○ Modify ○ View Only ● Block

Export Data: ○ Access ● Block

Export Global Log List: ○ Access ● Block

Site

Dashboard

Dashboard Manager: ○ Modify ○ View Only ● Block

Hotspot Manager

Hotspot Manager: ○ Modify ○ View Only ● Block

Statics

Statics Manager: ○ Access ● Block

Device

Device Manager: ○ Modify ○ View Only ● Block

Adopt Device Manager: ○ Access ● Block

Log

Log Manager: ○ Modify ○ View Only ● Block

Map

Map Manager: ○ Modify ○ View Only ● Block

Clients

Clients Manager: ○ Modify ○ View Only ● Block

Insight

Insight Manager: ○ Modify ○ View Only ● Block

Network Analyze

Network Analyze manager: ○ Modify ○ View Only ● Block

Network Report

Network Report Manager: ○ Modify ○ View Only ● Block

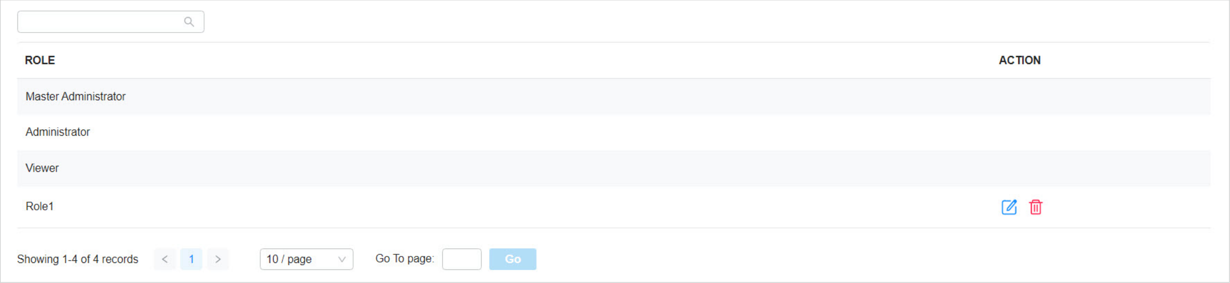
Settings

Site Settings Manager: ○ Modify ○ View Only ● Block

Device Account Manager: ○ Access ● Block

Export Data: ○ Access ● Block

3. Click Create. The new role will be displayed in the role list.



ROLE	ACTION
Master Administrator	
Administrator	
Viewer	
Role1	✎ 🗑

Showing 1-4 of 4 records

To edit/delete a custom role, click the ✎/🗑 icon in the ACTION Column.

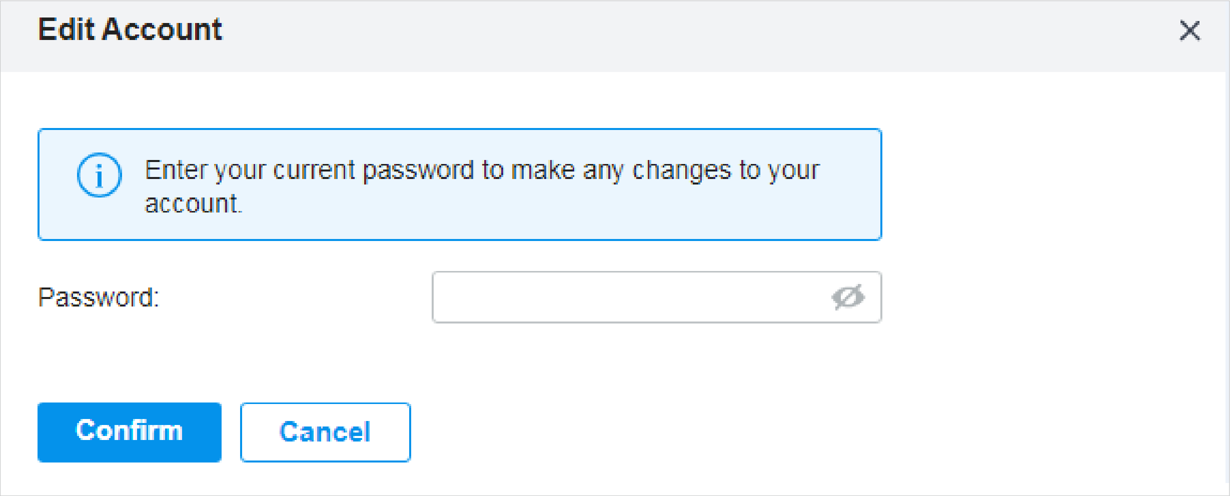
4. 3 Manage and Create Local User Accounts

By default, Omada SDN Controller automatically sets up a local user with the role called master administrator as the primary administrator. The username and password of the master administrator are the same as that of the controller account by default. The master administrator cannot be deleted, and it can create, edit, and delete other levels of user accounts.

4. 3. 1 Edit the Master Administrator Account

To view basic information and edit the master administrator account, follow these steps:

1. Select Global from the drop-down list of Organization in the top-right corner. Go to Account > User.
2. Click ✎ in the Action column. Enter the password and click Confirm (by default, the password of the master administrator is the same as the controller account).

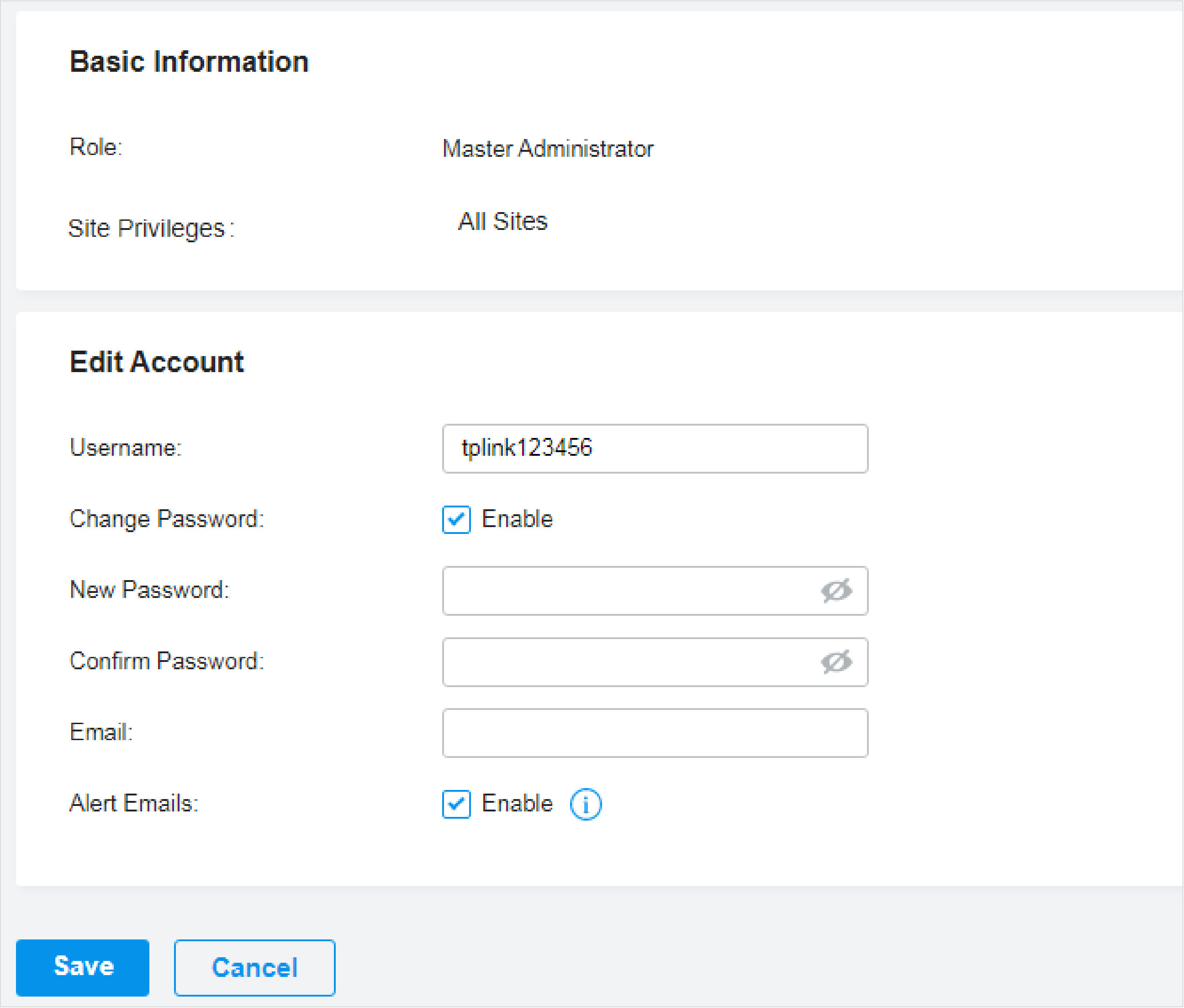


Edit Account

Enter your current password to make any changes to your account.

Password:

3. Check the basic information, change the password, or enable alert emails according to your needs. Click Save.



Basic Information

Role: Master Administrator

Site Privileges : All Sites

Edit Account

Username: tplink123456

Change Password: ☑ Enable

New Password:

Confirm Password:

Email:

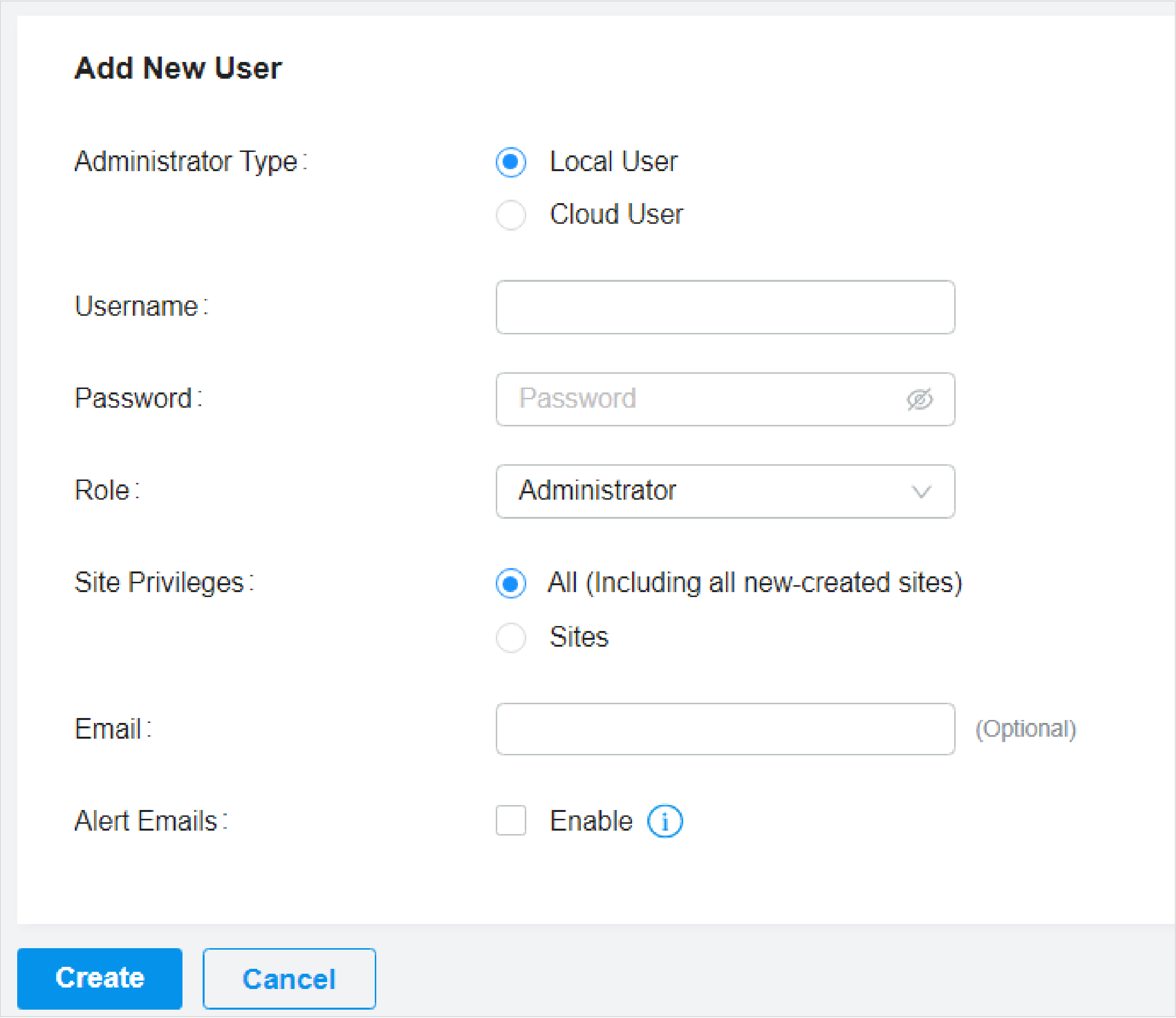
Alert Emails: ☑ Enable

4. 3. 2 Create and Manage Other Local Accounts

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

1. Select Global from the drop-down list of Organization in the top-right corner. Go to Account > User.
2. Click Add New User.

3. Select Local User for the administrator type in the pop-out window. Specify the parameters and click Create.



Add New User

Administrator Type: ● Local User ○ Cloud User

Username:

Password: Password

Role: Administrator

Site Privileges: ● All (Including all new-created sites) ○ Sites

Email: (Optional)

Alert Emails: □ Enable

Username	Specify the username. The username should be different from the existing ones.
Password	Specify the password.
Role	Select a role for the created user account. Administrator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete master administrator and other administrator accounts. Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself. Custom roles: If you have created custom roles, they will be displayed in the list. To create custom roles, refer to 9. 2 Create and Manage Custom Account Roles.

Site Privileges	Assign the site permissions to the created local user. All: The created user has device permissions in all sites, including all new-created sites. Sites: The created user has device permission in the sites that are selected. Select the sites by checking the box before them.
Email (optional)	Enter an email address for receiving alert emails.
Alert Emails	Check the box if you want the created user to receive emails about alerts of the privileged sites. For detailed configurations, refer to 4. 2. 2 Services.

To edit and delete the accounts, click icons in the Action Column.

✎	To edit the parameters for the user. Master administrator can edit all user accounts, Administrator can edit itself and viewer accounts of its privileged sites, and viewer can only edit itself.
🗑	To delete the account. Master administrator can delete all user accounts apart from itself, administrator can delete viewer accounts of its privileged sites, and viewer cannot delete any accounts.

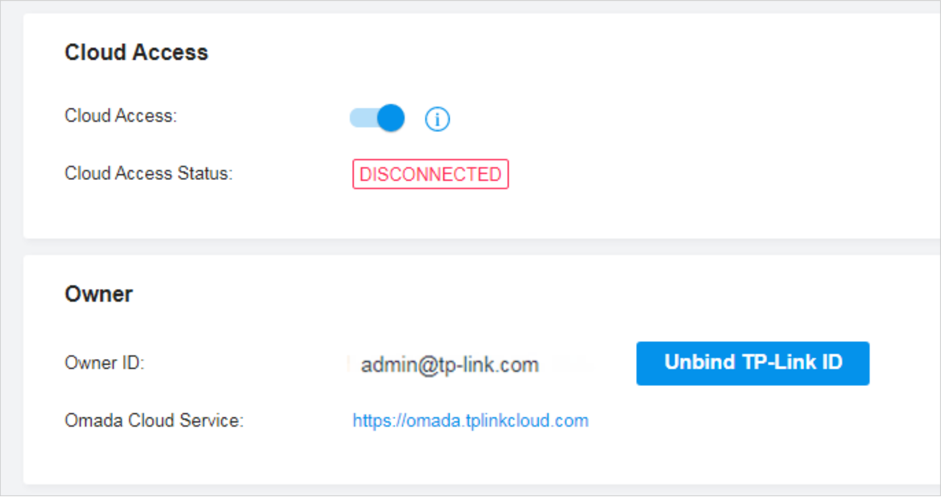
4. 4 Manage and Create Cloud User Accounts

For cloud-based controller, the cloud access is enabled by default, and the controller automatically sets up the cloud master administrator. Software and hardware controller automatically sets up the cloud master administrator if you have enabled cloud access and bound the controller account with a TP-Link ID in the quick setup. The username and password is the same as that of the TP-Link ID. The cloud master administrator is cannot be deleted, and it can create, edit, and delete other levels of user accounts.

4. 4. 1 Set Up the Cloud Master Administrator

For software and hardware controller, if you have not enabled the cloud access and bound the controller with a TP-Link ID in quick setup, to set up the cloud master administrator, follow these steps:

1. Select Global from the drop-down list of Organization in the top-right corner. Go to Settings > Cloud Access to enable Cloud Access and bind your TP-Link ID.



Cloud Access

Cloud Access: ●

Cloud Access Status: DISCONNECTED

Owner

Owner ID: admin@tp-link.com

Omada Cloud Service: https://omada.tplinkcloud.com

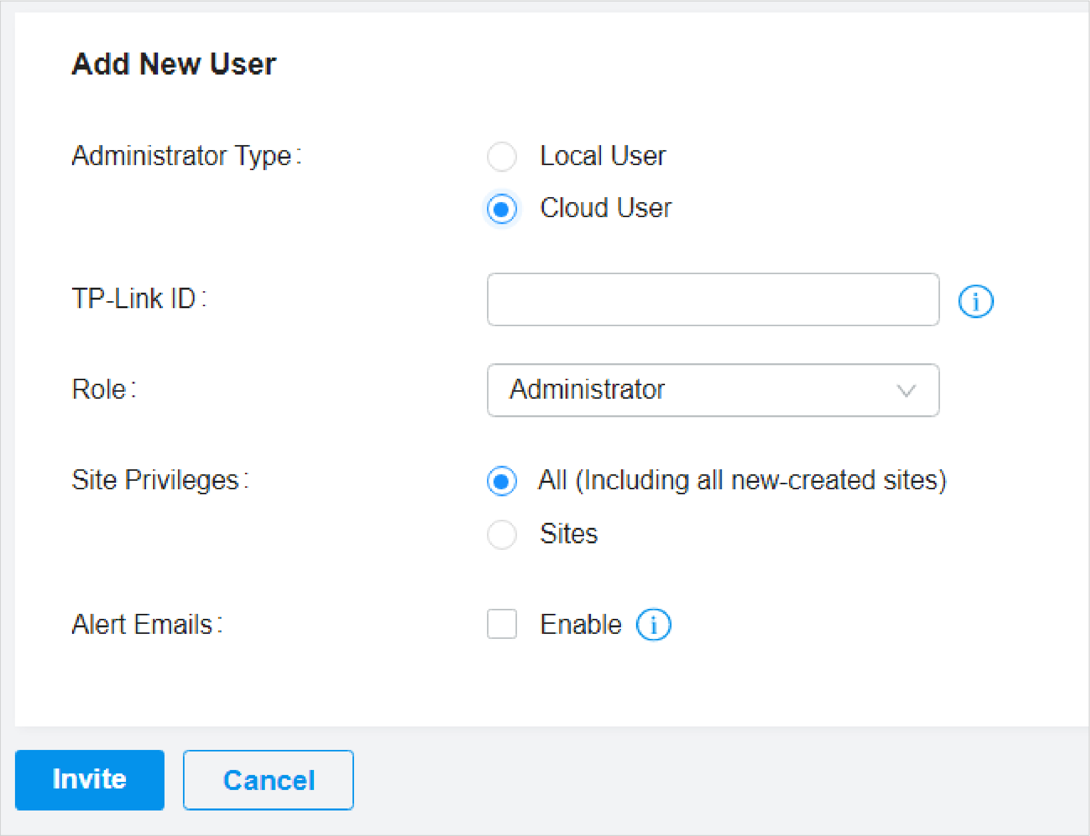
2. Go to Account > User. A cloud master administrator with the same username as the TP-Link ID will be automatically created. The Cloud Master Administrator cannot be deleted. You can log in with the cloud master administrator when the cloud access is enabled.

4. 4. 2 Create and Manage Other Cloud Accounts

To create and manage cloud user account, follow these steps:

1. Select Global from the drop-down list of Organization in the top-right corner. Go to Account > User.
2. Click Add New User.

3. Select Cloud User for the administrator type in the pop-out window. Specify the parameters and click Invite.



Add New User

Administrator Type : ○ Local User ● Cloud User

TP-Link ID :

Role : Administrator

Site Privileges : ● All (Including all new-created sites) ○ Sites

Alert Emails : □ Enable

TP-Link ID	Enter an email address of the created cloud user, and then an invitation email will be sent to the email address. If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. If the email address has not been registered, it will receive an invitation email for registration. After finishing registration, it will automatically becomes a valid cloud user.
Role	Select a role for the created cloud user. Administrator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete master administrator and other administrator accounts. Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself. Custom roles: If you have created custom roles, they will be displayed in the list. To create custom roles, refer to 9. 2 Create and Manage Custom Account Roles.
Site Privileges	Assign the site permission to the created cloud user. All: The created user has permission in all sites, including all new-created sites. Sites: The created user has permission in the sites that are selected. Select the sites by checking the box before them.

Alert Emails	Check the box if you want the created user to receive emails about alerts of the privileged sites. For detailed configurations, refer to 4. 2. 2 Services.

To edit and delete the accounts, click icons in the Action Column.

✎	To edit the parameters for the user. Cloud master administrator can edit all user accounts, administrator can edit itself and viewer accounts of its privileged sites, viewer can only edit itself.
🗑	To delete the account. Cloud master administrator can delete all user accounts apart from master administrator and itself, administrator can delete viewer accounts of its privileged sites, viewer cannot delete any accounts.