



Manage Omada Managed Devices and Sites

CONTENTS

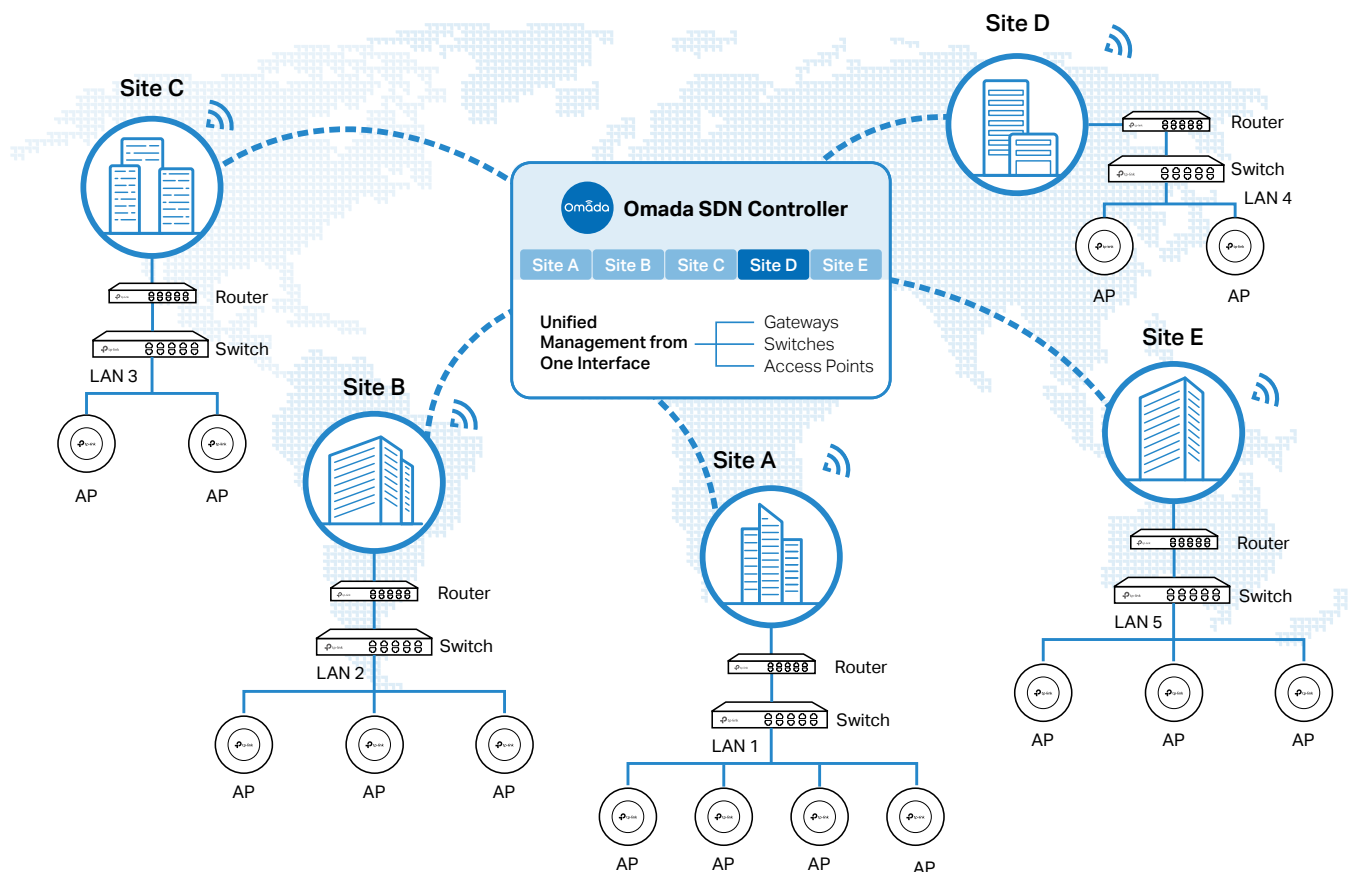
1. Manage Omada Managed Devices and Sites

1.1	Create Sites.....	2
1.2	Adopt Devices.....	6
1.3.1	For Omada Software Controller / Omada Hardware Controller	6
1.3.2	For Omada Cloud-Based Controller (Coming Soon).....	17

♥ 1.1 Create Sites

Overview

Different sites are logically separated network locations, like different subsidiary companies or departments. It's best practice to create one site for each LAN (Local Area Network) and add all the devices within the network to the site, including the router, switches and APs.



Devices at one site need unified configurations, whereas those at different sites are not relative. To make the best of a site, configure features simultaneously for multiple devices at the site, such as VLAN and PoE Schedule for switches, and SSID and WLAN Schedule for APs, rather than set them up one by one.

Configuration

To create and manage a site, follow these steps:

- 1) Create a site.
- 2) View and edit the site.
- 3) Go into the site.

Create a Site

View and Edit the Site

Go Into the Site

To create a site, choose one from the following methods according to your needs.

■ Create a site from scratch

1. In Global view, click [Add New Site](#) in the [Site List](#) section.
2. Enter a [Site Name](#) to identify the site, and configure other parameters according to where the site is located. Create a username and password for login to newly adopted devices. Then click [Apply](#). The new site will be added to the [Site List](#) and the drop-down list of [Organization](#).

Add New Site ×

Site Configuration

Name:

Country/Region:

Time Zone:

Application Scenario:

Longitude:
(Optional, -180~180, with a maximum of 16 decimal places.)

Latitude:
(Optional, -90~90, with a maximum of 16 decimal places.)

Address: (Optional) [Refresh](#)

Device Account ⓘ

Username:

Password:

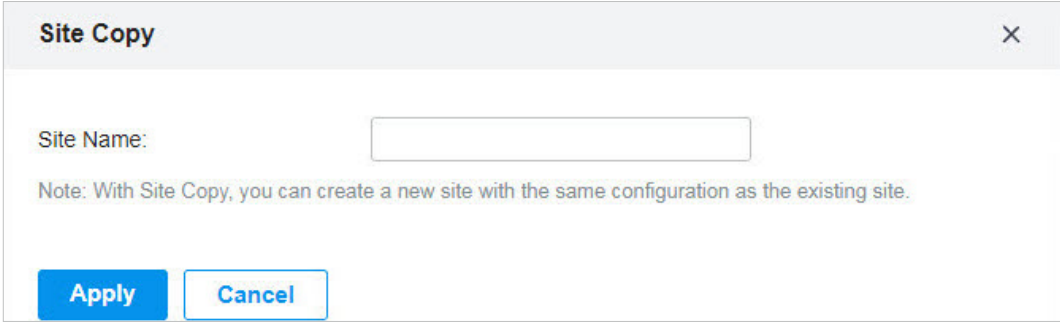
[Apply](#) [Cancel](#)

■ Copy an existing site

You can quickly create a site based on an existing one by copying its site configuration, wired configuration, and wireless configuration among others. After that, you can flexibly modify the new site configuration to make it different from the old.

1. In the [Site List](#), click  in the ACTION column of the site which you want to copy.

2. Enter a [Site Name](#) to identify the new site. Click [Apply](#). The new site will be added to the [Site List](#) and the drop-down list of [Organization](#).



Site Copy ×

Site Name:

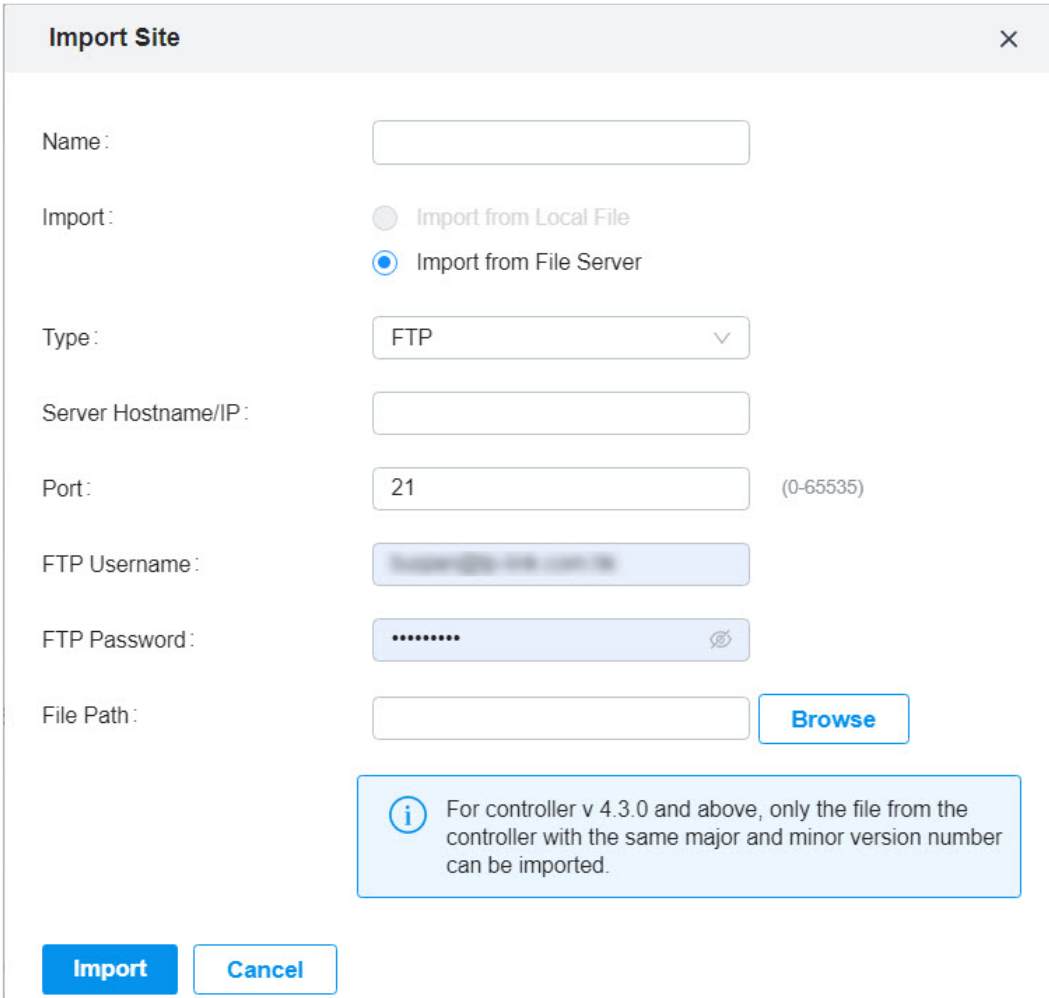
Note: With Site Copy, you can create a new site with the same configuration as the existing site.

[Apply](#) [Cancel](#)

■ Import a site from another controller

If you want to migrate seamlessly from an old controller to a new one, import the site configuration file of the old controller into the new. Before that, you need to export the site configuration file from the old controller, which is covered in [5. 4. 1 Site Migration](#).

1. Click [↑ Import Site](#) in the [Site List](#) section.
2. Enter a [Site Name](#) to identify the site, and configure other parameters according to actual site needs. Browse your file explorer and choose a site configuration file. Click [Import](#). The new site will be added to the [Site List](#) and the drop-down list of [Organization](#).



Import Site ×

Name:

Import: Import from Local File
 Import from File Server

Type: ▼

Server Hostname/IP:

Port: (0-65535)

FTP Username:

FTP Password: 🔗

File Path: [Browse](#)

i 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.

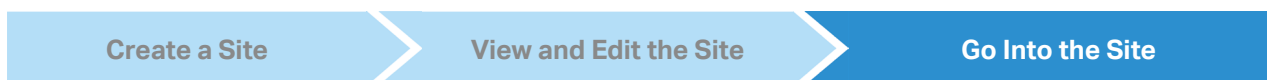
[Import](#) [Cancel](#)



After you create the site, you can view the site status in the [Site List](#). You can click the icons in the ACTION column to edit, copy, delete and launch the site.

NAME	COUNTRY/REGION	ALERTS	GATEWAY	CONNECTED SWITCHES	DISCONNECTED SWITCHES	CONNECTED APs	DISCONNECTED APs	ISOLATED APs	USERS	GUESTS	ACTION
☆ default	China mainland	1	🌐	1	0	1	0	0	👤 2 🗑️ 0	🗑️ 0	✏️ 📄 🗑️ 🏠
☆ SZ	China mainland	0	🌐	0	0	0	0	0	👤 0 🗑️ 0	🗑️ 0	✏️ 📄 🗑️ 🏠

Showing 1-2 of 2 records < 1 > 10 / page Go To page: Go



To monitor and configure a site, you need first go into the site.

Click the 🏠 icon of the site in the Site List to go into the site. Alternatively, select the site from the drop-down list of [Organization](#).

Organization: Global View

Search Site name

Global

SZ

default

NAME	COUNTRY/REGION	ALERTS	GATEWAY	CONNECTED SWITCHES	DISCONNECTED SWITCHES	CONNECTED APs	DISCONNECTED APs	ISOLATED APs	USERS	GUESTS	ACTION
☆ default	China mainland	1	🌐	1	0	1	0	0	👤 2 🗑️ 0	🗑️ 0	✏️ 📄 🗑️ 🏠
☆ SZ	China mainland	0	🌐	0	0	0	0	0	👤 0 🗑️ 0	🗑️ 0	✏️ 📄 🗑️ 🏠

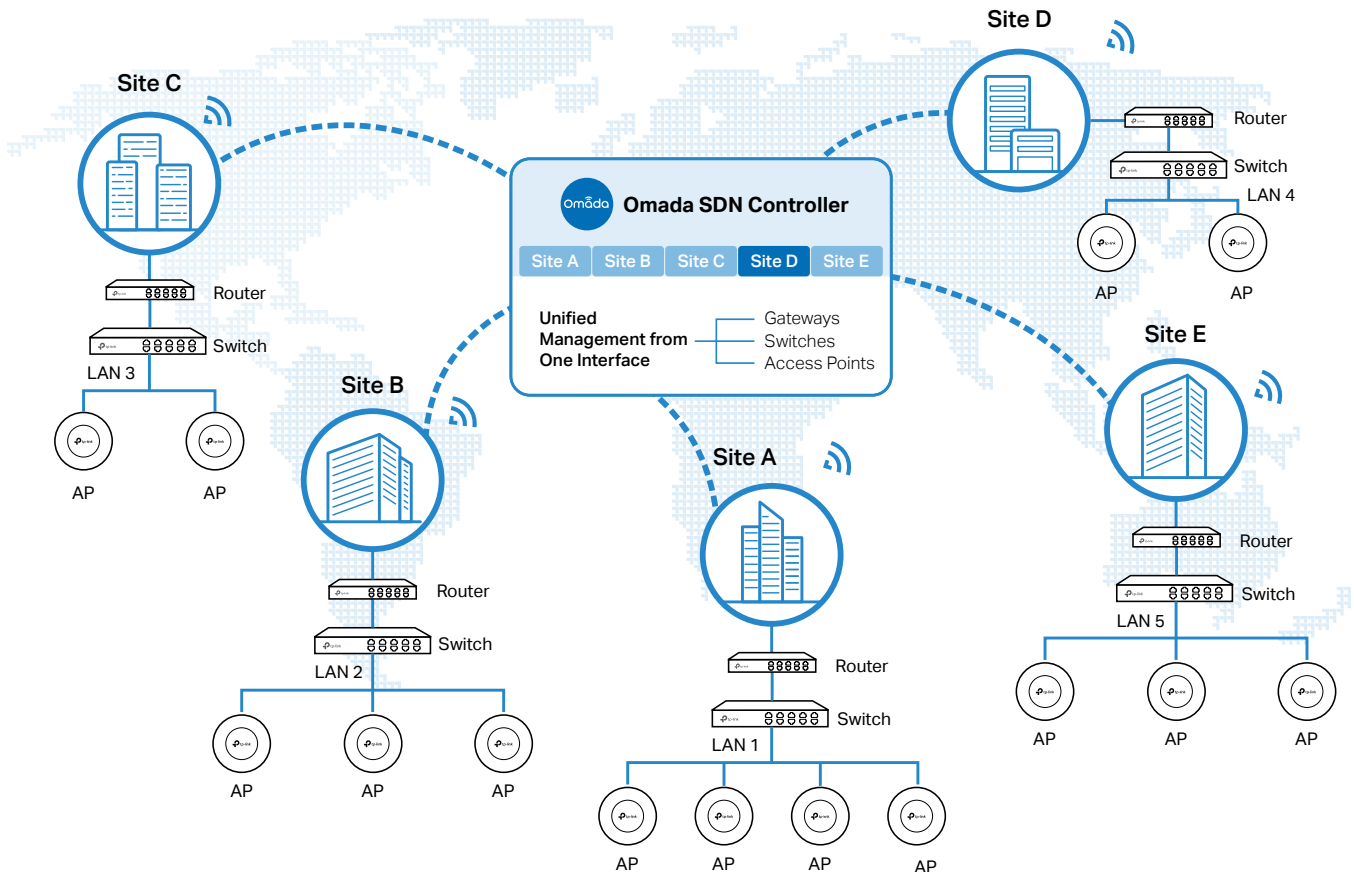
Showing 1-2 of 2 records < 1 > 10 / page Go To page: Go

The [Organization](#) field indicates the site which you are currently in. Some configuration items in the menu are applied to the site which you are currently in, whereas others are applied to the whole controller.

♥ 1.2 Adopt Devices

Overview

After you create a site, add your devices to the site by making the controller adopt them. Make sure that your devices in each LAN are added to the corresponding site so that they can be managed centrally.



Configuration

Choose a procedure according to the type of your controller:

- [3.3.1 For Omada Software Controller / Omada Hardware Controller](#)
- [3.3.2 For Omada Cloud-Based Controller \(Coming Soon\)](#)

1.3.1 For Omada Software Controller / Omada Hardware Controller

To adopt the devices on the controller, follow these steps:

- 1) Prepare for communication between the controller and devices.
- 2) Prepare for device discovery.
- 3) Adopt the devices.

**Prepare for Communication**

Prepare for Device Discovery

Adopt the Devices

ⓘ Note:

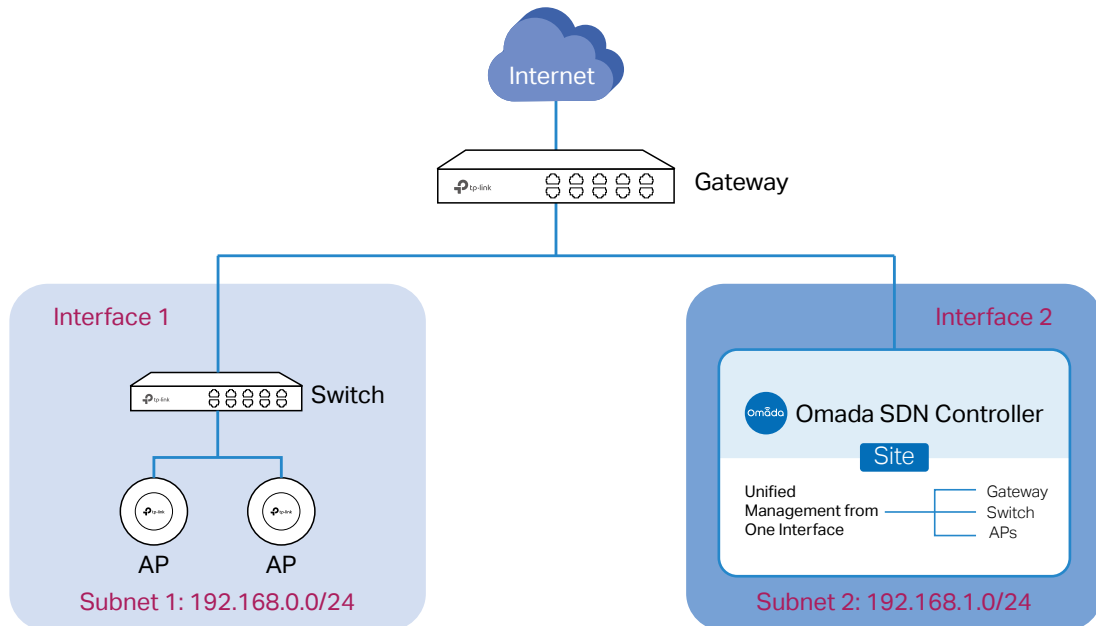
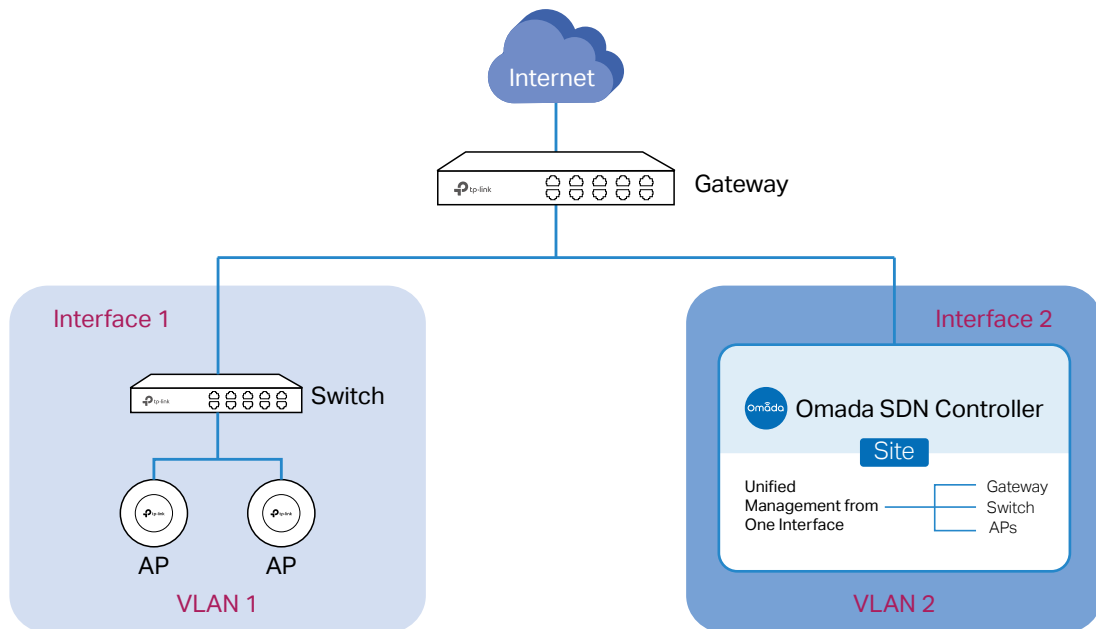
If the controller and devices are in the same LAN, subnet and VLAN, skip this step.

Make sure that the controller can communicate with the devices. Otherwise, the controller cannot discover or adopt the devices by any means. If the controller and devices are in different LANs, subnets or VLANs, use the following techniques to build up the connection according to your scenario.

1. Set up the Network

■ Scenario 1: Across VLANs or Subnets

As shown in the following figures, the controller and devices are in different VLANs or subnets. You need to set up a layer 3 interface for each VLAN or subnet, and make sure the interfaces can communicate with each other.



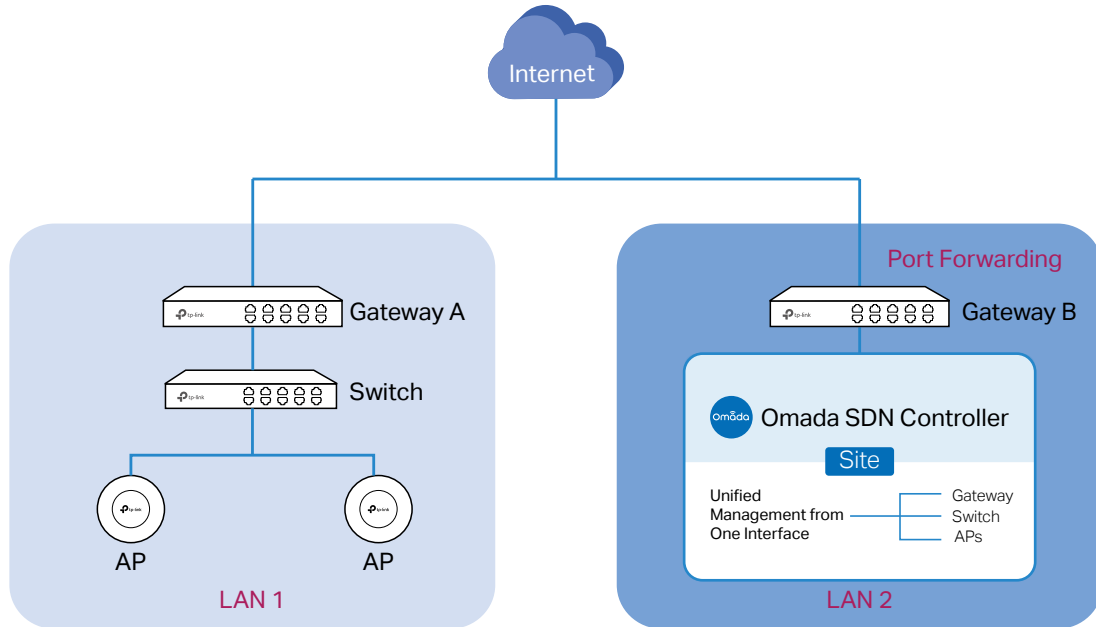
■ Scenario 2: Across LANs

As shown in the following figure, the controller and devices are in different LANs. You need to establish communication across the internet and the gateways.

By default, devices in LAN 1 cannot communicate with the controller in LAN 2, because Gateway B is in front of the controller and block access to it. To make the controller accessible to the devices, you can use Port Forwarding or VPN.

- Use Port Forwarding

Configure Port Forwarding on Gateway B and open port 29810-29813 for the controller, which are essential for discovering and adopting devices. If you are using firewalls in the networks, make sure that the firewalls don't block those ports.



To configure Port Forwarding on Gateway B, you need first adopt Gateway B on the controller. For how to adopt Gateway B, refer to [Adopt the Devices](#). Go to [Settings](#) > [Transmission](#) > [NAT](#) > [Port Forwarding](#). Click [+ Create New Rule](#) to load the following page. Specify a name to identify the Port Forwarding rule, check Enable for Status, select Any as Source IP, select the desired WAN port

as Interface, disable DMZ, specify 29810-29813 as Source Port and Destination Port, specify the controller’s IP address as Destination IP, and select All as Protocol. Then click [Create](#).

Create New Rule

Name:

Status: Enable

Source IP: Any
 Limited IP Address

Interface:

DMZ: Enable

Source Port: (1-65535. e.g. 80 or 80-100)

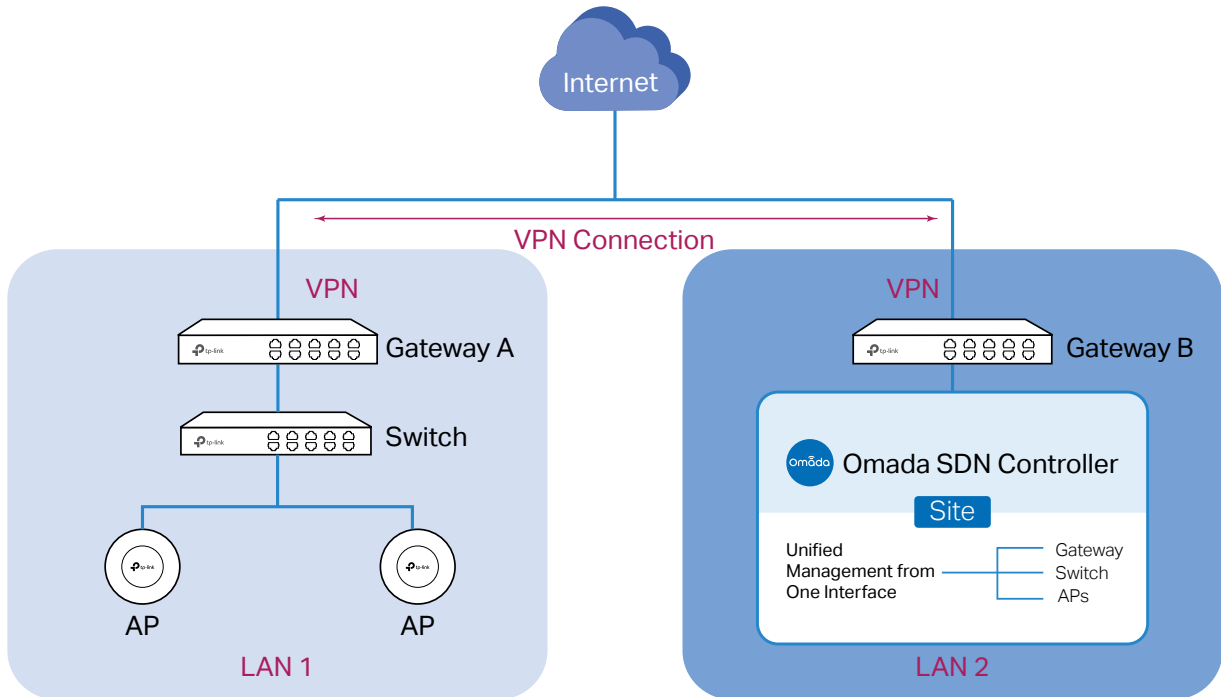
Destination IP:

Destination Port: (1-65535. e.g. 80 or 80-100)

Protocol: All
 TCP
 UDP

- Use VPN

Set up a VPN connection between Gateway A and Gateway B in Standalone Mode. For details about VPN configuration, refer to the User Guide of the gateways.



2. (Optional) Test the network

If you are not sure whether the controller and devices can establish communication, it's recommended to do the ping test from the devices to the controller.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Then Go to [MAINTENANCE](#) > [Network Diagnostics](#) > [Ping](#) to load the following page, and specify Destination IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click [Ping](#).

ⓘ Note:

To ping the router, please turn off Block WAN Ping on the [Settings](#) > [Network Security](#) > [Attack Defense](#) page.

Ping Config

Destination IP: (Format: 192.168.0.1 or 2001::1)

Ping Times: (1-10)

Data Size: bytes (1-1500)

Interval: milliseconds (100-1000)

[Ping](#)

Ping Result

Pinging 192.168.0.26 with 64 bytes of data:

Reply from 192.168.0.26 : bytes=64 time=19ms TTL=64

Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64

Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64

Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64

Ping statistics for 192.168.0.26 :

Packets: Sent=4, Received=4, Loss=0 (0%Loss)

Approximate round trip times in milliseconds:

Maximum=19ms, Minimum=3ms, Average=7ms

If the ping result shows the packets are received, it implies that the controller can communicate with the devices. Otherwise, the controller cannot communicate with the devices, then you need to check your network.

Prepare for Communication

Prepare for Device Discovery

Adopt the Devices

ⓘ Note:

If the controller and devices are in the same LAN, subnet and VLAN, skip this step. In this scenario, the controller can discover the devices directly, and no additional settings are required.

Make sure that the controller can discover the devices.

When the controller and devices are in different LANs, subnets or VLANs, the controller cannot discover the devices directly. You need to choose [Controller Inform URL](#), [Discovery Utility](#), or [DHCP Option 138](#) as the method to help the controller discover the devices.

■ Controller Inform URL

Controller Inform URL informs the devices of the controller's URL or IP address. Then the devices make contact with the controller so that the controller can discover the devices.

You can configure Controller Inform URL for devices in Standalone Mode. Let's take a switch for example. Log into the management page of the switch in Standalone Mode and go to [SYSTEM](#) > [Controller Settings](#) to load the following page. In [Controller Inform URL](#), specify Inform URL/

IP Address as the controller's URL or IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click [Apply](#).

Cloud-Based Controller Management ?

Connection Status: Disabled

Cloud-Based Controller Management: Enable

Notes:
To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number.
You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.

Controller Inform URL

Inform URL/IP Address:

Notes:
Enter the inform URL or IP address of your controller to tell the device where to discover the controller.
This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.

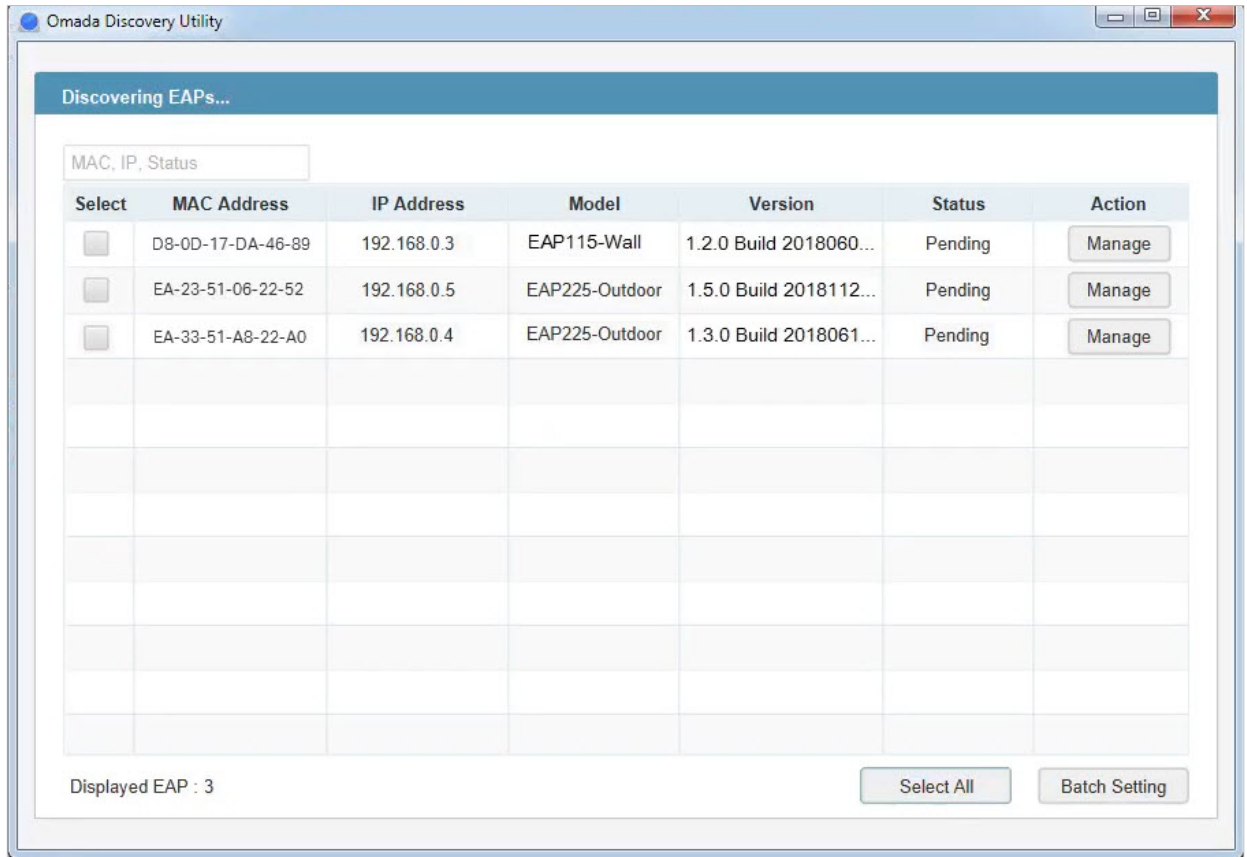
[Apply](#)

■ Discovery Utility

Discovery Utility can discover the devices in the same LAN, subnet and VLAN, and inform the devices of the controller's IP address. Then the devices make contact with the controller so that the controller can discover the devices.

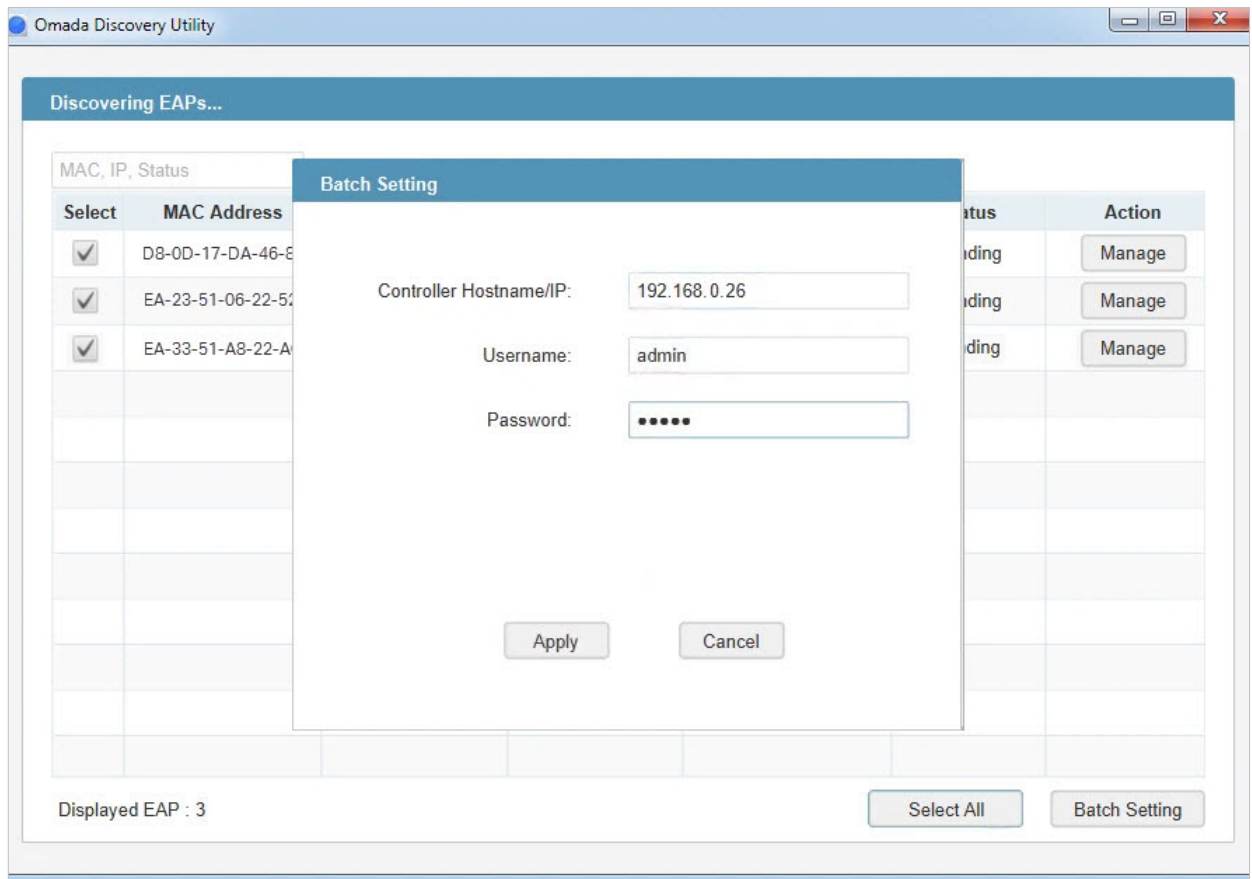
1. Download Discovery Utility from the [website](#) and then install it on your PC which should be located in the same LAN, subnet and VLAN as your devices.

- 2. Open Discovery Utility and you can see a list of devices. Select the devices to be adopted and click [Batch Setting](#).



- 3. Specify Controller Hostname/IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead), and

enter the username and password of the devices. By default, the username and password are both admin. Then click [Apply](#). Wait until the setting succeeds.



■ DHCP Option 138

DHCP Option 138 informs a DHCP client, such as a switch or an EAP, of the controller's IP address when the DHCP client sends DHCP requests to the DHCP server, which is typically a gateway.

1. To use DHCP Option 138, you need to adopt the gateway on the controller first, which may require other techniques like [Controller Inform URL](#) or [Discovery Utility](#) if necessary.
2. After the gateway is adopted, go to [Settings > Wired Networks > LAN > Networks](#), and click [✎](#) in the ACTION column of the LAN where the DHCP clients are located. Enable DHCP Server and configure common DHCP parameters. Then click [Advanced DHCP Options](#) and specify Option

138 as the controller’s IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Click [Save](#).

Edit Network

Name:

Purpose: Interface
 VLAN

LAN Interfaces: WAN/LAN2 WAN/LAN3 LAN1

VLAN: (1-4090) ⓘ

Gateway/Subnet: / ⓘ [Update DHCP Range](#)

Gateway IP	192.168.1.1
Network Broadcast IP	192.168.1.255
Network IP Count	254
Network IP Range	192.168.1.1 - 192.168.1.254
Network Subnet Mask	255.255.255.0

Domain Name: (Optional)

IGMP Snooping: Enable ⓘ

DHCP Server: Enable

DHCP Range: -

DNS Server: Auto
 Manual

Lease Time: minutes (2-2880)

Default Gateway: Auto
 Manual

DHCP Omada Controller: (Optional) ⓘ

Legal DHCP Servers: Enable ⓘ

Advanced DHCP Options

Option 60: (Optional) ⓘ

Option 66: (Optional) ⓘ

Option 138: (Optional) ⓘ

[Save](#) [Cancel](#)

- To make DHCP Option 138 take effect, you need to renew DHCP parameters for the DHCP clients. One possible way is to disconnect the DHCP clients and then reconnect them.

Prepare for Communication

Prepare for Device Discovery

Adopt the Devices

1. Decide which site you want to add the devices to. On the controller configuration page, select the site from the drop-down list of **Organization**.

The screenshot shows the Omada Controller configuration page for 'Omada Controller_6DF81B'. The 'Organization' dropdown menu is open, showing a search bar and a list of sites: 'Global' and 'SZ default'. Below the menu, the 'Site List' table is visible, showing two sites: 'default' and 'SZ'. The table columns include NAME, COUNTRY/REGION, ALERTS, GATEWAY, CONNECTED SWITCHES, DISCONNECTED SWITCHES, CONNECTED APs, DISCONNECTED APs, ISOLATED APs, USERS, GUESTS, and ACTION.

NAME	COUNTRY/REGION	ALERTS	GATEWAY	CONNECTED SWITCHES	DISCONNECTED SWITCHES	CONNECTED APs	DISCONNECTED APs	ISOLATED APs	USERS	GUESTS	ACTION
default	China mainland	1	1	1	0	1	0	0	2	0	[Edit] [Refresh] [Delete] [Add]
SZ	China mainland	0	0	0	0	0	0	0	0	0	[Edit] [Refresh] [Delete] [Add]

2. Go to **Devices**, and devices which have been discovered by the controller are displayed.

The screenshot shows the 'Devices' page in the Omada Controller. The table displays discovered devices with columns for DEVICE NAME, IP ADDRESS, STATUS, MODEL, VERSION, UPTIME, and ACTION. The status column shows 'CONNECTED', 'MANAGED BY OTHERS', and 'PENDING'.

DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTION
1C-61-B4-C5-48-83	192.168.0.1	CONNECTED	ER605 v2.0	2.1.0	4day(s) 20h 22m ...	[Refresh]
00-FF-00-05-40-5D	192.168.0.18	CONNECTED	TL-SG2428P v1.0	1.1.7	22day(s) 19h 49...	[Refresh] [Power] [Add]
00-00-FF-FC-30-82	--	MANAGED BY OTHERS	EAP770 v1.0	--	--	[Checkmark]
00-00-FF-FF-0D-28	--	PENDING	EAP225 v5.0	--	--	[Checkmark]
00-00-FF-FF-0F-BB	--	PENDING	EAP225 v5.0	--	--	[Checkmark]

3. Click in the ACTION column of the devices which you want to add to the site. Wait until the STATUS turns into **Connected**. Then the devices are adopted by the controller and added to the current site. Once the devices are adopted, they are subject to central management in the site.

1.3.2 For Omada Cloud-Based Controller (Coming Soon)

To adopt the devices on the controller, follow these steps:

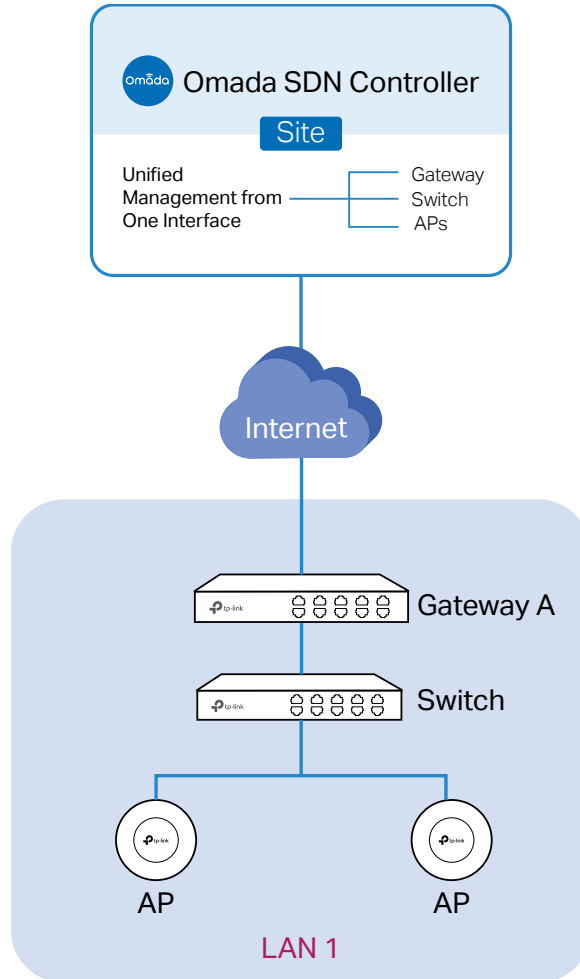
- 1) Connect to the internet.
- 2) Prepare for controller management.

3) Adopt the devices.



1. Set up the network.

Make sure that your devices are connected to the internet.



If you are using firewalls in your network, make sure that the firewall doesn't block traffic from the controller. To configure your firewall policy, you may want to know the URL of the controller. After you open the web page of the controller, you can get the URL from the address bar of the browser.

2. (Optional) Test the network.

If you are not sure whether the devices are connected to the internet, it's recommended to do the ping test from the devices to a public IP address, such as 8.8.8.8.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Go to **MAINTENANCE > Network Diagnostics > Ping** to load the following page. Specify Destination IP as a public IP address, such as 8.8.8.8. Then click **Ping**.

Ping Config

Destination IP: (Format: 192.168.0.1 or 2001::1)

Ping Times: (1-10)

Data Size: bytes (1-1500)

Interval: milliseconds (100-1000)

Ping

Ping Result

Pinging 8.8.8.8 with 64 bytes of data:

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Ping statistics for 8.8.8.8 :

Packets: Sent=4, Received=4, Loss=0 (0%Loss)

Approximate round trip times in milliseconds:

Maximum=3ms , Minimum=3ms, Average=3ms

If the ping result shows the packets are received, it implies that the devices are connected to the internet. Otherwise, the devices are not connected to the internet, then you need to check your network.

Connect to the Internet

Prepare for Controller Management

Adopt the Devices

ⓘ Note:

If your devices are on the factory default setting, skip this step.

The Cloud-Based Controller Management feature allows the devices to be adopted by Omada Cloud-Based Controller. Make sure Cloud-Based Controller Management is enabled on the devices. For details, refer to the User Guide of your devices, which can be downloaded from the [TP-Link download center](#).

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Go to [SYSTEM](#) > [Controller Settings](#) to load the following page. In [Cloud-Based Controller Management](#), enable Cloud-Based Controller Management and click [Apply](#).

Cloud-Based Controller Management ?

Connection Status: Off-line

Cloud-Based Controller Management: [Enable](#)

Notes:
To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number.
You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.

Controller Inform URL

Inform URL/IP Address:

Notes:
Enter the inform URL or IP address of your controller to tell the device where to discover the controller.
This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.

[Apply](#)

Connect to the Internet

Prepare for Controller Management

Adopt the Devices

On the controller configuration page, go into the site where you want to add the devices. Go to [Devices](#) and click [Add Devices](#). Then add your devices to the controller. Once the devices are adopted, they are subject to central management in the site.