

How to Use an Omada Controller to Manage Omada Devices Across Different Subnets Over the Internet

Knowledgebase Configuration Guide

🕒 05-28-2026 👁 9065

[Introduction](#)

[Requirements](#)

[Configuration](#)

[Scenario 1: Via Port Forwarding & Omada discovery utility/Inform URL/DHCP option 138](#)

[Scenario 2: Via VPN Tunnel & DHCP option 138](#)

[Conclusion](#)

[QA](#)

Introduction

In enterprise networks, devices are often deployed across different subnets, making it common for Omada devices and the Omada Controller to reside in separate network segments. Supporting device adoption and management across subnets enables centralized control without changing existing network designs. This capability simplifies deployment, reduces maintenance costs, and improves scalability and operational efficiency, which is essential for distributed, campus, and multi-branch network environments.

This article introduces different methods for adopting devices across subnets over the Internet and using Omada Controller v6 and higher.

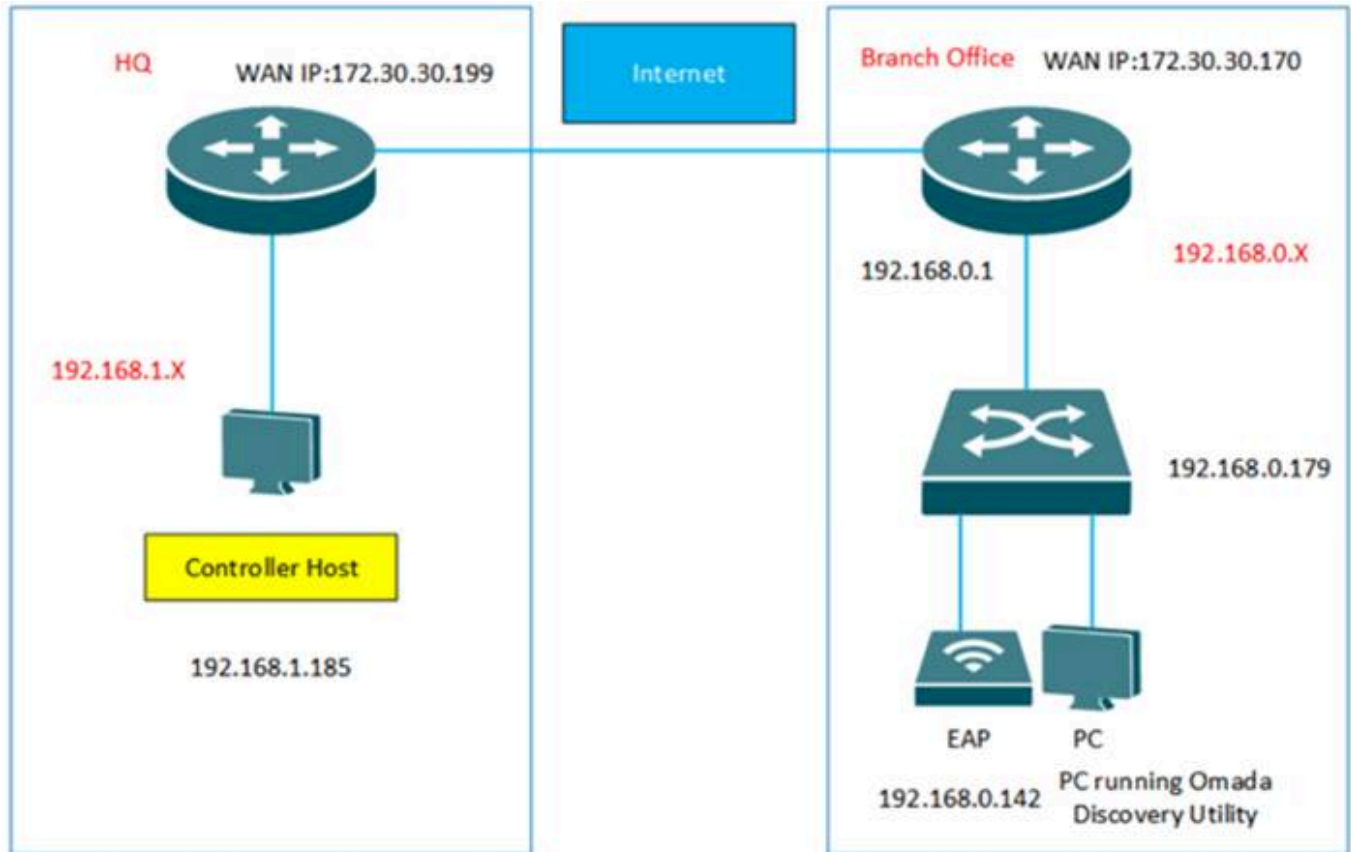
Requirements

- Omada Discovery Utility
- Omada Software/Hardware/Cloud-Based Controller
- Omada Devices (Gateway/EAP/Switch)

Check compatible devices here: [Omada Controller Compatibility List](#)

Scenario 1: Via Port Forwarding & Omada discovery utility/Inform URL/DHCP option 138

A classic office scenario is shown below. The headquarters and the branch office are connected via the Internet. In HQ, there is an Omada Controller and a gateway in subnet 192.168.1.0/24. In the Branch Office, there is an EAP, a switch and a gateway in subnet 192.168.0.0/24.



Step 1. Configure Port Forwarding rules on gateway (taking ER605 as an example) in HQ for Controller Host (192.168.1.185). Please go to **Transmission > NAT > Virtual Server** and configure a virtual server for TCP&UDP port, ranging from 29810 to 29817.

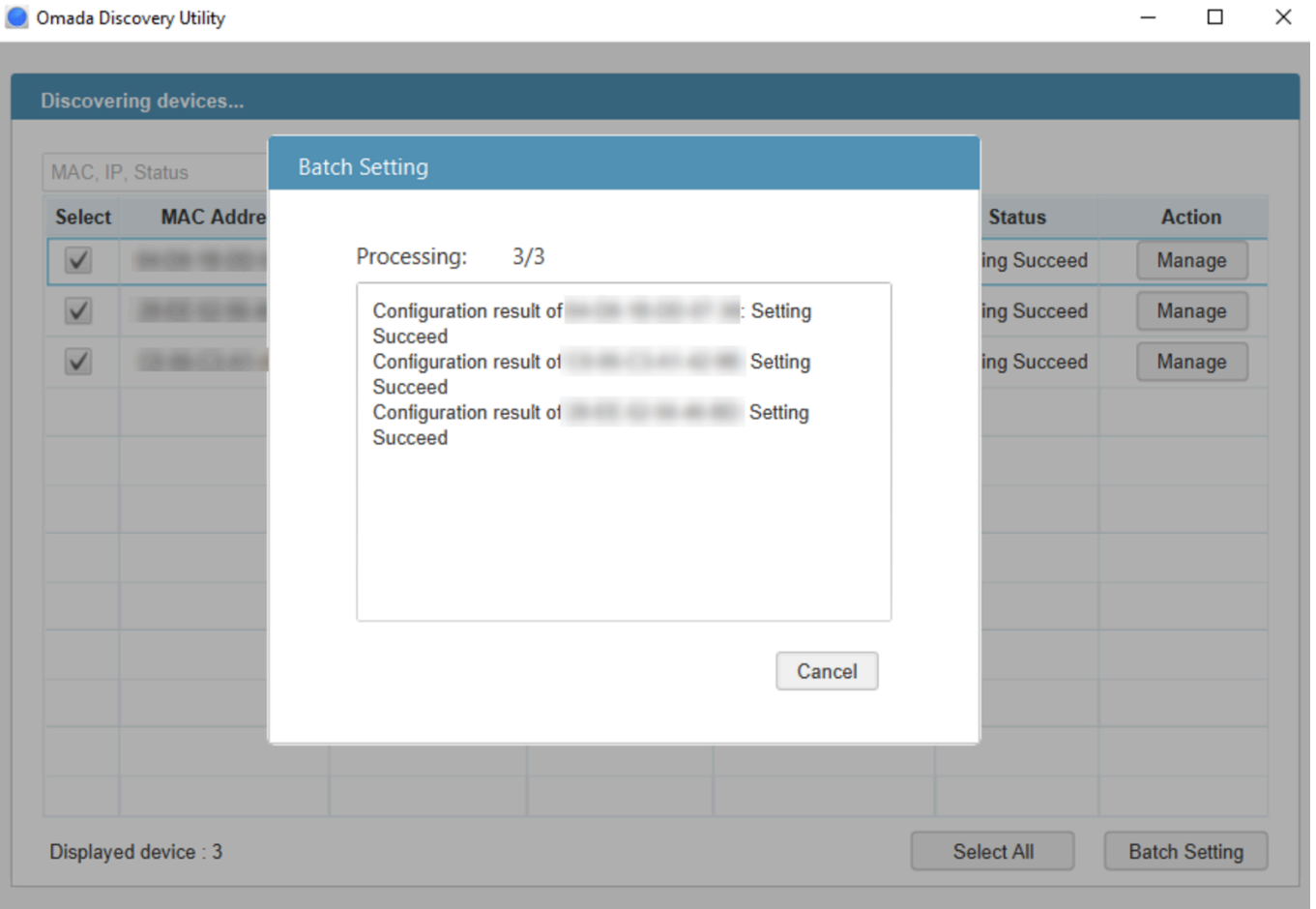
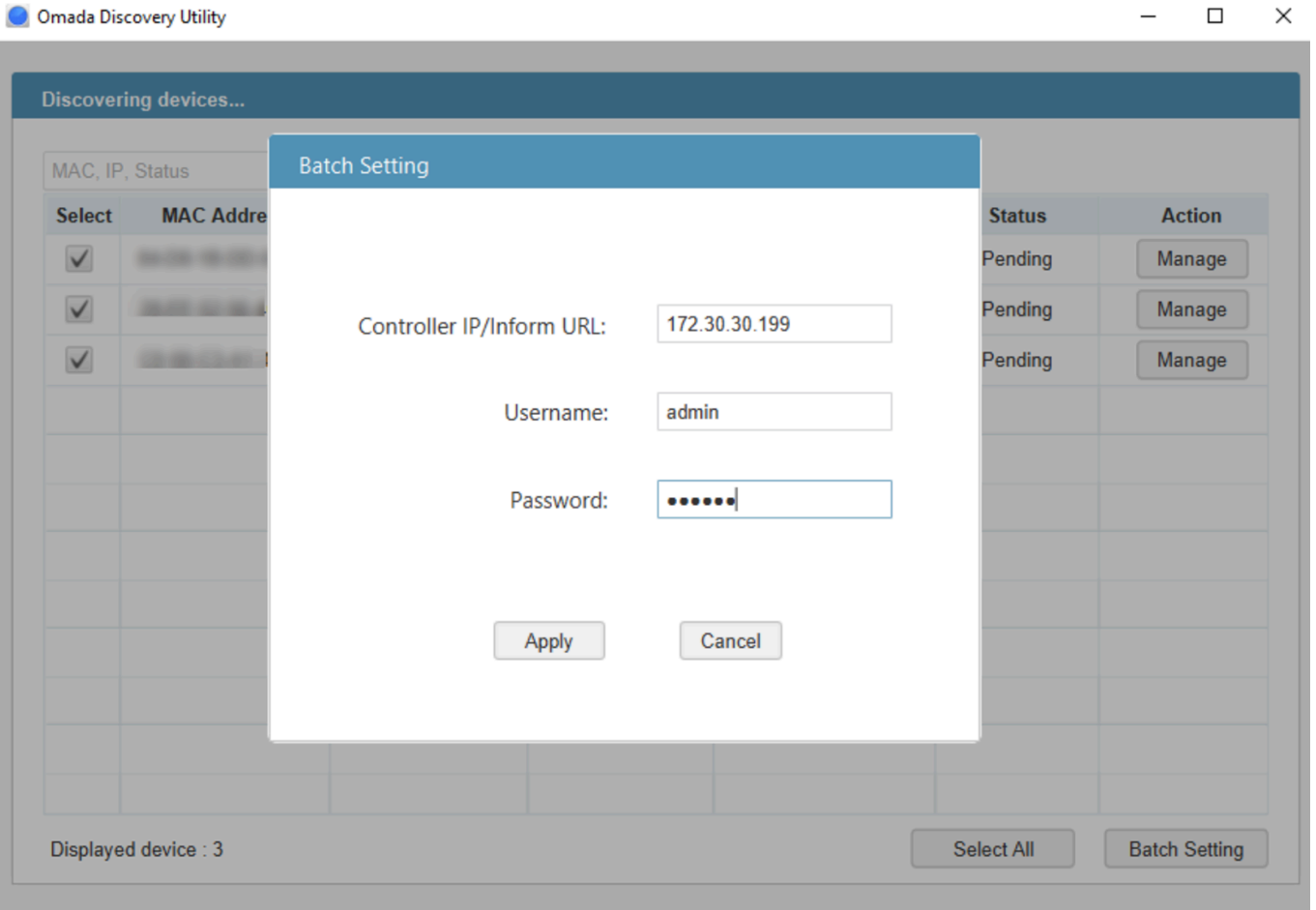
The screenshot shows the Omada Gigabit VPN Gateway web interface. The top navigation bar includes the Omada logo and the device model 'ER605 | Omada Gigabit VPN Gateway'. The main menu on the left is expanded to 'Transmission', with 'NAT' selected. The 'Virtual Servers' tab is active, showing a 'Virtual Server List' table with columns for ID, Name, Interface, WAN IP, External Port, Internal Port, Internal Server IP, Protocol, Status, and Operation. Below the table is a configuration form for a new virtual server. The form fields are: Name (controller_address), Interface (WAN1), WAN IP (---), External Port (29810-29817), Internal Port (29810-29817), Internal Server IP (192.168.1.185), Protocol (ALL), and Status (checked 'Enable'). The 'OK' button is highlighted with a red box.

Note: If your devices are not crossing the Internet and are all under the same gateway, with only different VLANs, you can skip this step.

Step 2. Three methods for Omada Controller to discover the Omada devices in the Branch Office.

- **Method 1: Omada Discovery Utility**

Run Omada Discovery Utility in Branch Office, select the Omada devices, and click "Batch Setting". Fill in the Controller Hostname/IP with WAN IP address of ER605 in HQ which is 172.30.30.199 and the Username/Password of the Omada devices. At last, click "Apply". The default username/Password of the devices is admin/admin. If the Username and Password of Omada devices are not the same, please manage the devices one by one.



In Standalone mode, please go to System Tools/System-Controller settings of every Omada device, fill in the Controller IP/Inform URL with the WAN IP address of ER605 in HQ which is 172.30.30.199. Then click Save.

The screenshot shows the 'Controller Settings' page in a web interface. On the left is a navigation menu with items: Status, Network, USB, Preferences, Transmission, Firewall, Behavior Control, VPN, Authentication, Services, System Tools (expanded), Admin Setup, and Management. Below this are 'Controller Settings', SNMP, Diagnostics, Time Settings, and System Log. The main content area is titled 'Controller Settings' and contains two sections. The first section, 'Cloud-Based Controller Management', shows 'Connection Status' as 'Disabled', 'Cloud-Based Controller Management' as 'Enable' (unchecked), and a checkbox for accepting terms of use. A 'Save' button is below. The second section, 'Controller Inform URL', has a text input field for 'Inform URL/IP Address' containing '172.30.30.199', which is highlighted with a red box. A 'Save' button is below this field.

Configuration screenshot of switch Controller Settings in standalone mode.

The screenshot shows the 'Controller Settings' page for an EAP660 device. It features a teal header with 'Controller Settings'. A note at the top states: 'You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.' Below this is the 'Controller Inform URL' section, which includes a text input field for 'Inform URL/IP Address' containing '172.30.30.199'. A 'Notes' section follows, explaining that the inform URL or IP address is used to tell the device where to discover the controller and that this feature is commonly used for Layer 3 deployments. An 'Apply' button is located at the bottom right.

Configuration screenshot of EAP660 Controller Settings in standalone mode.

Controller Inform URL

Inform URL/IP Address:

Note:

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.

Save

• Method 3: DHCP Option 138

Use Omada Discovery Utility or set Controller Inform URL to adopt the ER605 in Branch Office on another site. And then go to **Network Config > LAN**, click **Edit/Add** button 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, which is the WAN IP of ER605 in HQ. Click Save.

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

Note: If you do not use Omada Gateway, you also can use DHCP Server which supports the option 138 feature to finish the configuration.

+ Advanced Settings

- Advanced DHCP Options

Option 2	<input type="text" value=""/>	Seconds	(Optional) ⓘ
Option 42	<input type="text" value="."/>	<input type="text" value="."/>	(Optional) ⓘ
Option 44	<input type="text" value="."/>	<input type="text" value="."/>	(Optional) ⓘ
Option 60	<input type="text" value="."/>	<input type="text" value="."/>	(Optional) ⓘ
Option 66	<input type="text" value="."/>	<input type="text" value="."/>	(Optional) ⓘ
Option 67	<input type="text" value="."/>	<input type="text" value="."/>	(Optional) ⓘ
Option 138	<input type="text" value="172 . 30 . 30 . 199"/>		(Optional) ⓘ

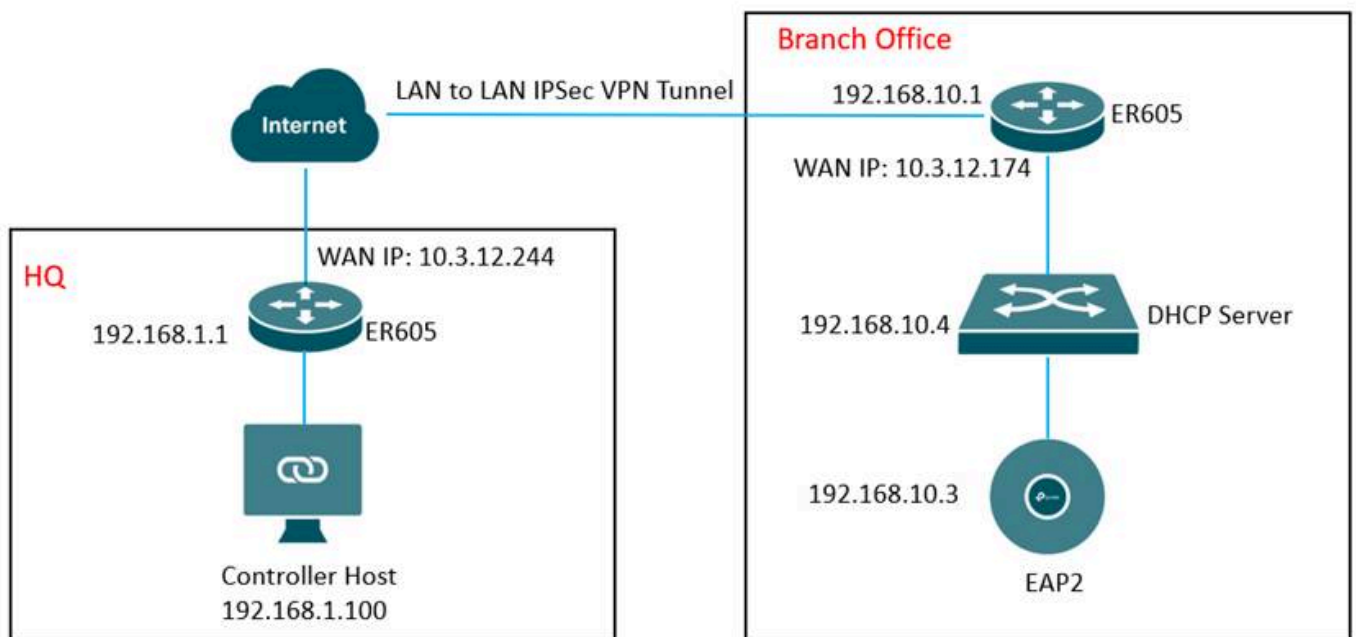
Step 3. After finishing the configuration of the Omada devices in the Branch Office will appear on the "PENDING" list of Omada Controller. which means you can adopt and manage these

DEVICE NAME	IP ADDRESS	STATUS	HEALTH	ACTION
[Device Name]	192.168.1.1	PENDING	-	[Checkmark]
[Device Name]	192.168.0.179	PENDING	-	[Checkmark]
[Device Name]	192.168.0.142	PENDING	-	[Checkmark]

Note: If you have adopted a gateway in the default site, please click "Add New Site" in the drop-down list of Sites and configure the parameters of the Branch Office. Because one site can only adopt one gateway.

Scenario 2: Via VPN Tunnel & DHCP option 138

As shown below, the HQ and Branch Office are connected with each other through the IPsec VPN tunnel. In HQ, there is an Omada Controller and an ER605 (VPN router) in subnet 192.168.1.0/24. In the Branch Office, there is an EAP2, a switch as the DHCP Server (supporting DHCP option 138), and an ER605 (VPN router) in subnet 192.168.10.0/24.



Step 1. Configurations on the switch in the Branch Office.

Change the switch's default IP address to 192.168.10.4 to avoid IP conflict with the gateway.

Routing Table >

ARP >

Interface

Static Routing >

DHCP Service >

VRRP

RIP

OSPF

Back

Modify IPv4 Interface

Interface ID: VLAN1

Admin Status: Enable

Interface Name: VLAN10 (Optional. 1-128 characters)

IP Address Mode: None Static DHCP BOOTP

IP Address: 192.168.10.4 (Format: 192.168.0.1)

Subnet Mask: 255.255.255.0 (Format: 255.255.255.0)

Apply

Secondary IP Table

+ Add - Delet

<input type="checkbox"/>	Index	IP Address	Subnet Mask
No entries in this table.			
Total: 0			

Enable DHCP Server Function on switch and set DHCP Option138 as the IP address of Remote Omada Controller Host (192.168.1.100). And then the DHCP Server will tell the EAPs where the Omada Controller is, so that the Omada Controller and EAPs can communicate with each other among different subnets.

Omada
by tp-link

SYSTEM L2 FEATURES **L3 FEATURES** QoS SECURITY MAINTENANCE Save Log Out

Routing Table >

ARP >

Interface

Static Routing >

DHCP Service v

DHCP Server

DHCP Relay

DHCP L2 Relay

VRRP

DHCP Server Pool Setting Manual Binding DHCP Pool Options DHCP Client List Packet Statistics ?

Global Config

DHCP Server: Enable

Option 60: (Optional. 1-64 characters)

Option 138: 192.168.1.100 (Optional. Format: 192.168.0.1)

Apply

Ping Time Config

Configure the DHCP IP Address Pool (192.168.10.0/24) for EAP in the Branch Office.

The screenshot shows the Omada Controller web interface. The top navigation bar includes 'SYSTEM', 'L2 FEATURES', 'L3 FEATURES', 'QoS', 'SECURITY', and 'MAINTENANCE'. The left sidebar lists various network services, with 'DHCP Service' expanded. The main content area shows the 'DHCP Server' configuration page, with 'Pool Setting' selected. A 'DHCP Server Pool' configuration dialog is open, displaying the following fields:

Field	Value	Notes
Pool Name	VLAN10	(8 characters maximum)
Network Address	192.168.10.0	(Format: 192.168.0.0)
Subnet Mask	255.255.255.0	(Format: 255.255.255.0)
Lease Time	120	(Optional. 1-2880 min, Default: 120)
Default Gateway	192.168.10.1	(Optional. Format: 192.168.0.1)
DNS Server	8.8.8.8	(Optional. Format: 192.168.0.1)
NetBIOS Server		(Optional. Format: 192.168.0.1)
NetBIOS Node Type		(Optional, b/p/m/h/none)
Next Server Address		(Optional. Format: 192.168.0.1)
Domain Name		(0 to 200 characters)
Bootfile		(0 to 128 characters)

The dialog also features 'Cancel' and 'Create' buttons at the bottom right.

Step 2. Set up Site-to-Site Manual IPsec VPN Tunnels.

- Create a new VPN policy on the Gateway managed by Omada Controller in headquarter

Note: IPsec VPN is used as an example for demonstration. Establishing other types of VPN tunnels can also be used to achieve device adoption.

Create a new VPN policy on the Gateway managed by Omada Controller in HQ. Go to **Network Config > VPN > Site-to-Site VPN** and click **Create New Site-to-Site VPN**.

The screenshot displays the Omada Controller's configuration interface. On the left, a sidebar menu is visible with categories: Management (Dashboard, Devices, Clients), Monitoring (Map, Insights, Logs), Configuration (Network Config, Device Config, Hotspot), and Maintenance (Network Tools, IntelliRecover BETA). The main content area is titled 'Site-to-Site VPN' and includes a diagram of a secure two-way tunnel between two sites. Below the diagram, the text reads: 'Establishes a secure two-way tunnel between two sites, enabling devices at both locations to communicate as if they were on the same network.' A green button labeled '+ Create New Site-to-Site VPN' is highlighted with a red rectangular box.

Configure the parameters for the new VPN policy. Enter a name to identify the VPN policy, select the VPN Type for the new entry as IPsec and the Mode as Manual. Then configure the corresponding parameters and save them.

← Edit Site-to-Site VPN

VPN Type WireGuard IPsec

Name

Status Enable

Interface

IPsec Failover ⓘ Enable

Remote Gateway

Remote Subnets /

[+ Add Subnet](#)

Pre-Shared Key 🗑️ 🔄

Local Network Type Network Custom IP

Local Networks ⓘ

Interface	Select the WAN port on which the VPN tunnel will be established.
Remote Gateway	Enter the WAN IP address of Gateway in the Branch Office (10.3.12.174).
Remote Subnets	Enter the IP address range of the LAN in the Branch Office (192.168.10.1/24).
Local Networks	Select the networks in the headquarters (LAN 1), and the VPN policy will be applied to the selected

Pre-Shared Key	Enter the Pre-Shared Key (PSK) that serves as an authentication key. The gateway in the headquarters and the Branch Office must use the same PSK for authentication.
----------------	---

Note: When gateway in Branch Office is in standalone mode, click Advanced Settings and select IKEv1 as Key Exchange Version. IKEv1 only supports a single local network.

– Advanced

Phase-1 Settings

Key Exchange Version

IKEv1 IKEv2

If the Omada Gateway is behind a NAT device, make sure that UDP port 500 and UDP port 4500 are open on the NAT device, and set up the Local ID Type / Remote ID Type as Name.

Advanced

Phase-1 Settings

Key Exchange Version IKEv1 IKEv2

Proposal SHA1 - AES256 - DH2

Exchange Mode Main Mode Aggressive Mode

Negotiation Mode Initiator Mode Responder Mode

Local ID Type IP Address Name

Local ID Local_ID

Remote ID Type IP Address Name

Remote ID Remote_ID

- Create a new VPN policy on the gateway in the branch office

Disable the DHCP server function on ER605 in the Branch Office.

Navigation: Status > LAN DHCP Client List Address Reservation LAN DNS

ID	Name	Vlan	Isolation Status	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation
1	LAN	1	Deisolated	192.168.10.1	255.255.255.0	Enabled	Disabled	

LAN Configuration Details:

- Name: LAN
- IP Address: 192.168.10.1
- Subnet Mask: 255.255.255.0
- Mode: Normal Bridge
- Network Isolation: Enable
- Vlan: 1 (1-4086)
- DHCP Mode: DHCP Server DHCP Relay

Go to **VPN > IPsec > IPsec Policy** and click **Add**.

Remote Gateway	Enter the WAN IP address of the Gateway in the Branch Office (10.3.12.244).
WAN	Select the WAN port on which the VPN tunnel will be established.
Local Networks	Select the networks in the headquarters (LAN), and the VPN policy will be applied to the selected networks.
Remote Subnet	Enter the IP address range of the LAN in the Branch Office (192.168.1.0/24).
Pre-Shared Key	Enter the Pre-Shared Key (PSK) that serves as an authentication key. The gateway in the headquarters and the Branch Office must use the same PSK for authentication.
Status	Check the box to enable the VPN tunnel.

Note: If the router is behind a NAT device, make sure that UDP port 500 and UDP port 4500 are open on the NAT device, and set up the Local ID Type / Remote ID Type as Name in Phase-1

Local ID Type: IP Address NAME

Local ID: (1-28 non-blank characters)

Remote ID Type: IP Address NAME

Remote ID: (1-28 non-blank characters)

Alt text: The position of Local ID and Remote ID in gateway standalone mode.

For the Omada managed gateway in headquarters, go to **Network Config > VPN Status > Site-to-Site VPN > IPsec** and check the IPsec entries.

Local ID Type: IP Address NAME

Local ID: (1-28 non-blank characters)

Remote ID Type: IP Address NAME

Remote ID: (1-28 non-blank characters)

For ER605, go to **VPN > IPsec > IPsec SA** and check the IPsec SA entries. When corresponding entries are displayed in the tables, the VPN tunnel is successfully established.

IPsec Policy [IPsec SA](#)

IPsec SA List

Entry Count: 2

[Refresh](#)

<input type="checkbox"/>	ID	Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
<input type="checkbox"/>	1	IPSec_tunnel	3344772439	in	10.3.12.174<->10.3.12.244	192.168.10.0/24 <-> 192.168.1.0/24	ESP	--	SHA1	AES-256
<input type="checkbox"/>	2	IPSec_tunnel	3313139314	out	10.3.12.174->10.3.12.244	192.168.10.0/24 -> 192.168.1.0/24	ESP	--	SHA1	AES-256

Step 3. Run the Omada Controller. The EAP will appear on Omada Controller's "pending" list, which means you adopt and manage this EAP now shown in the list.

Device List | Device Group | Configuration Result

Gateway: No Device | Switches: No Devices | APs: No Devices | OLTs: No Devices

Name, SN, MAC, IPv4, Model or L... [All \(3\)](#) Gateway/Switches (2) OLTs (0) APs (1) [All \(3\)](#) ● Good (0) ● Fair (0) ● Poor (0) ● No Data (0)

[Export](#) [Batch Action](#) [+ Add Devices](#)

DEVICE NAME	IP ADDRESS	STATUS	HEALTH	ACTION
	192.168.1.1	PENDING	-	✓

Conclusion

This article describes how to discover and adopt devices across subnets on the Omada Controller under two classic office network scenarios.

Get to know more details of each function and configuration please go to [Download Center](#) to download the manual of your product.

QA

Q1: If devices are not across the Internet but only across different subnets, which steps in this document should be followed to discover and manage the devices?

A1: You can still use the Omada Discovery Utility//Inform URL/DHCP option 138 methods mentioned in Scenario 1 and enter the IP address of the Omada Controller.

Please Rate this Document



Related Documents

How to manage Omada devices at different sites across Internet using Omada Controller

[Configuration Guide](#) [Controller](#) [Gateway](#)

🕒 06-27-2022 👁 46208

How to manage EAPs at different sites across Internet using EAP Controller (via VPN Tunnel with DHCP Option138)

[Configuration Guide](#) [Controller](#)

🕒 06-28-2022 👁 23572

[Configuration Guide](#) [Controller](#) [VPN](#)

🕒 06-28-2022 👁 25244

How to manage EAPs at different sites across Internet using EAP Controller (via NAT Port Forwarding for Controller Host with DHCP Option138)

[Configuration Guide](#) [Controller](#)

🕒 06-28-2022 👁 24461

How to manage EAPs in different subnets using EAP controller (via EAP Discover Utility)

[Configuration Guide](#) [Controller](#)

🕒 06-28-2022 👁 28246

Subscription

Email Address

[Sign Up](#)

Follow Us

About

Press

Learning Center

Saudi Arabia / English

©2026 TP Link Limited one person Co and its affiliated companies. All rights reserved.