

User Guide

Omada Controller Software

1910012573 REV 3.3.0 May 2019

CONTENTS

1	Qui	ck Start	1
	1.1	Determine the Network Topology	2
		1.1.1 Management on the local Network	2
		1.1.2 Management via Cloud Access	4
	1.2	Install Omada Controller Software	5
		1.2.1 Installation on Windows Host	5
		1.2.2 Installation on Linux Host	5
	1.3	Inform the EAPs of the Controller Host's Address	7
	1.4	Start and Log In to the Omada Controller	8
		1.4.1 Launch Omada Controller	8
		1.4.2 Do the Basic Configurations	9
		1.4.3 Log In to the Management Interface	12
	1.5	Create Sites and Adopt EAPs	12
		1.5.1 Create Sites	13
		1.5.2 Adopt the EAPs	15
	1.6	Monitor and Manage the EAPs	16
2	Моі	nitor and Manage the Network	18
	2.1	View the Statistics of the Network	19
		2.1.1 View the Client Distribution on SSID	19
		2.1.2 Have a Quick Look at EAPs and Clients	19
		2.1.3 View Current Usage-Top EAPs	20
		2.1.4 View Recent Activities	20
	2.2	Monitor the Network with the Map	21
		2.2.1 Add a Map	21
		2.2.2 Monitor the EAPs on the Map	24
	2.3	Monitor and Manage the EAPs	25
		2.3.1 Manage the EAPs in Different Status	25

		2.3.2 View the Detailed Information of EAPs	26
		2.3.3 Manage the EAPs in the Action Column	26
	2.4	Monitor and Manage Clients	28
		2.4.1 View the Current Information of Clients	28
		2.4.2 Manage Clients in the Action Column	28
	2.5	View Clients Statistics During the Specified Period	29
		2.5.1 Select a Specified Period	29
		2.5.2 View the History Information of Clients	30
		2.5.3 Manage Clients in the Action Column	30
	2.6	Manage the Rogue APs List	30
		2.6.1 Manage the Untrusted Rogue APs List	31
		2.6.2 Manage the Trusted Rogue APs List	31
	2.7	View Past Guest Authorization	32
	2.8	View Logs	32
	_		
3	Con	nfigure the EAPs Globally	34
3	Con 3.1	Ifigure the EAPs Globally	
3			35
3		Wireless Network	35 35
3		Wireless Network 3.1.1 Add Wireless Networks	35 35 45
3		Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters	35 35 45 47
3		Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters 3.1.3 Configure Band Steering	35 45 47 48
3	3.1	Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters 3.1.3 Configure Band Steering 3.1.4 Configure Mesh	35 35 45 47 48 53
3	3.1 3.2	Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters 3.1.3 Configure Band Steering 3.1.4 Configure Mesh Access Control	35 45 47 48 53 54
3	3.1 3.2	Wireless Network. 3.1.1 Add Wireless Networks. 3.1.2 Configure Advanced Wireless Parameters . 3.1.3 Configure Band Steering . 3.1.4 Configure Mesh. Access Control . Portal Authentication.	35 35 45 47 48 53 55
3	3.1 3.2	Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters 3.1.3 Configure Band Steering 3.1.4 Configure Mesh Access Control Portal Authentication 3.3.1 No Authentication	35 35 45 47 48 53 55 59
3	3.1 3.2	Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters 3.1.3 Configure Band Steering 3.1.4 Configure Mesh Access Control Portal Authentication 3.3.1 No Authentication 3.3.2 Simple Password	35 35 45 47 48 53 54 55 59 63
3	3.1 3.2	Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters 3.1.3 Configure Band Steering 3.1.4 Configure Mesh Access Control Portal Authentication 3.3.1 No Authentication 3.3.2 Simple Password 3.3.3 Local User	35 35 45 47 48 53 53 55 59 63 71
3	3.1 3.2	Wireless Network. 3.1.1 Add Wireless Networks. 3.1.2 Configure Advanced Wireless Parameters. 3.1.3 Configure Band Steering. 3.1.4 Configure Mesh. Access Control. Portal Authentication. 3.3.1 No Authentication. 3.3.2 Simple Password 3.3.3 Local User. 3.3.4 Voucher.	35 35 45 47 48 53 53 55 59 63 71 78
3	3.1 3.2	Wireless Network 3.1.1 Add Wireless Networks 3.1.2 Configure Advanced Wireless Parameters 3.1.3 Configure Band Steering 3.1.4 Configure Mesh Access Control Portal Authentication 3.3.1 No Authentication 3.3.2 Simple Password 3.3.3 Local User 3.3.4 Voucher 3.3.5 SMS	35 35 45 47 48 53 53 54 55 63 71 78 83

		3.3.8 External Portal Server	90
	3.4	Free Authentication Policy	91
	3.5	MAC Filter	92
	3.6	Scheduler	94
	3.7	QoS	96
	3.8	Site Settings	99
		3.8.1 LED	
		3.8.2 Device Account	
		3.8.3 Reboot Schedule	100
		3.8.4 Log Settings	100
		3.8.5 Batch Upgrade	102
		3.8.6 SSH	104
		3.8.7 Management VLAN	105
4	Om	ada Cloud Service	106
	4.1	Configure the Cloud Access	
		4.1.1 Enable Cloud Access	107
		4.1.2 Manage the Cloud Users	107
	4.2	Manage the Controller via Omada Cloud	109
		4.2.1 Access the controller via Omada Cloud	110
		4.2.2 Change your TP-Link ID information	112
5	Con	nfigure the EAPs Separately	
	5.1	View the Information of the EAP	
		5.1.1 Active Channel Information	114
		5.1.2 Overview	115
		5.1.3 LAN	115
		5.1.4 Radio	
	5.2	View Clients Connecting to the EAP	116
		5.2.1 User	116
		5.2.2 Guest	117

	5.3	View Mesh Information of the EAP	117
		5.3.1 Uplinks	117
		5.3.2 Downlinks	118
	5.4	Configure the EAP	118
		5.4.1 Basic Config	118
		5.4.2 IP Setting	119
		5.4.3 Radio	120
		5.4.4 Load Balance	121
		5.4.5 WLANs	122
		5.4.6 LED	122
		5.4.7 Trunk Settings (Only for EAP330)	123
		5.4.8 Rogue APs Detection	123
		5.4.9 Local LAN Port Settings (Only for EAP115-Wall and EAP225-Wall)	124
		5.4.10 Forget this AP	124
6	Mar	hage the Omada Controller	125
	6.1	User Account	
	6.2	General Setting	127
		6.2.1 Configure Controller Name	127
		6.2.2 Configure Mail Server	127
	6.3	History Data Retention	129
	6.4	Backup&Restore	130
	6.5	Auto Backup	130
	6.6	Migrate	133
		6.6.1 Controller Migrate	133
		6.6.2 Site Migrate	137
	6.7	Information About the Software	141
7	Δnn	plication Example	142
1	7.1	Basic Configuration	
	7.2	Advanced Settings	
		-	

	7.2.1	Monitor the EAPs with Map	
	7.2.2	Configure Portal Authentication	144
	7.2.3	Create a SSID for the Employees	146
	7.2.4	Configure Scheduler	147
Арре	endix	: Omada App	149
1	Instal	I Omada App on the Mobile Device	150
2	Mana	ge your Network in Standalone Mode	150
3	Mana	ge your Network in Controller Mode	153
	3.1	Locally manage your EAPs using the Omada App	153
	3.2	Remotely manage your EAPs using the Omada App	

1 Quick Start

Omada Controller is a management software for TP-Link EAPs. With this software, you can centrally manage your EAPs, such as configure EAPs in batches and conduct real-time monitoring of EAPs locally or remotely through Omada Cloud service.

Follow the steps below to complete the basic settings of Omada Controller.

- 1. Determine the Network Topology
- 2. Install Omada Controller Software
- 3. Inform the EAPs of the Controller Host's Address
- 4. Start and Log In to the Omada Controller
- 5. Create Sites and Adopt the EAPs
- 6. Monitor and Manage the EAPs

1.1 Determine the Network Topology

There are two methods to centrally manage EAPs via Omada Controller:

- Management on the Local Network
- Management via Cloud Access

Determine your management method according to your need and refer to the following introductions to build your network topology.

Tips:

Omada app offers a convenient way to access the Omada Controller and adopt EAPs. With Local Access and Cloud Access function on the Omada app, you can manage the controller at local and remote sites. For more detailed information about Omada app, refer to **Appendix: Omada App**.

1.1.1 Management on the local Network

There are two kinds of network topologies to centrally manage EAPs on the local network:

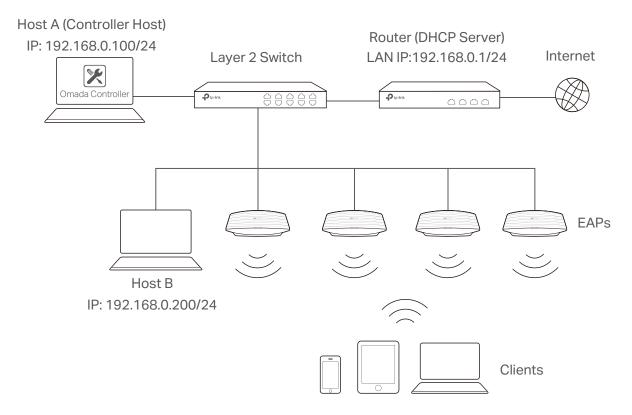
- Omada Controller and EAPs are in the same subnet.
- Omada Controller and EAPs are in different subnets.

Determine your management method according to your need and refer to the following introductions to build your network topology.

Management in the Same Subnet

If your Omada Controller and EAPs are in the same subnet, refer to the following network topology.

A router acts as a DHCP server to assign IP addresses to EAPs and clients. Omada Controller should be installed on one host, which is called as Controller Host. The other hosts in the same LAN can access the Controller Host to manage the network. Taking the following topology as an example, you can enter "https://192.168.0.100:8043" in a web browser on Host B to visit the Omada Controller interface on Host A. It's recommended to set a static IP address to the Controller Host for the convenient login to the Omada Controller interface.



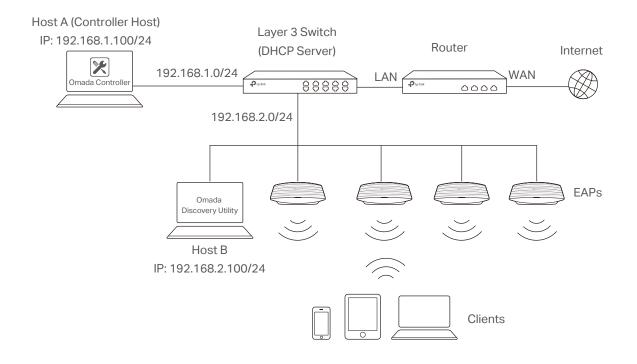
Note:

- Omada Controller must be running all the time when you manage the network.
- Omada Controller can be running on only one host in a LAN. When other users in the LAN try to launch Omada Controller on their own hosts, they will be redirected to the host that is already running Omada Controller.

Management in Different Subnets

If your Omada Controller and EAPs are in different subnets, refer to the following topology.

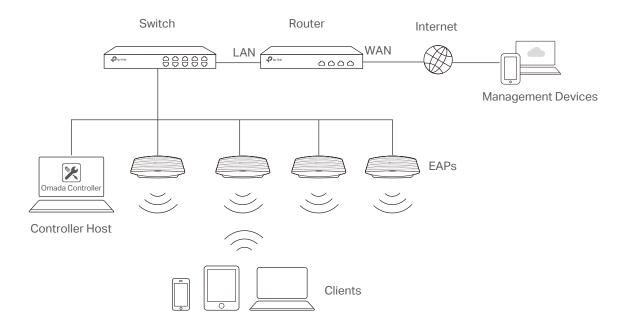
A router acts as the gateway of the network. A layer 3 switch acts as a DHCP server to assign IP addresses to EAPs and clients. The Controller Host and the EAPs are connected to the switch's different network segments. To help EAPs find the Controller Host, Omada Discover Utility should be installed on Host B which is in the same subnet with the EAPs. For how to use Omada Discovery Utility, refer to Inform the EAPs of the Controller Host's Address.



1.1.2 Management via Cloud Access

With Cloud Access enabled on the Omada Controller, you can use <u>https://omada.tplinkcloud.com</u> to remotely access and monitor multiple controllers. If you want to manage EAPs remotely via Omada Cloud, refer to the following topology.

A router acts as the gateway of the network. A Layer 3 switch acts as a DHCP server to assign IP addresses to EAPs and clients. The management device is not on the local network. On the management device, you can launch a web browser to remotely launch Omada Controller to manage EAPs via Omada Cloud. For more details about Cloud Access, refer to <u>Omada Cloud</u> <u>Service</u>.



1.2 Install Omada Controller Software

We provide Omada Controller for both Windows and Linux operating systems. Determine your operation system and follow the introductions below to install Omada Controller.

1.2.1 Installation on Windows Host

Make sure your PC meets the following system requirements and then properly install the Omada Controller software.

System Requirements

Operating System: Microsoft Windows 7/8/10/Server.

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

Note:

We recommend that you deploy Omada Controller on a 64-bit operating system to guarantee the software stability.

Install Omada Controller

Download the installation file of Omada Controller from the website https://www.tp-link.com/ en/download/EAP-Controller.html. Then follow the instructions to properly install the Omada Controller software. After successful installation, a shortcut icon 🔀 of the Omada Controller will be created on your desktop.

1.2.2 Installation on Linux Host

Two versions of installation package are provided: .tar.gz file and .deb file. The .tar.gz file can be used in multiple versions of Linux operating system. And the .deb file can be used in Ubuntu and Debian.

Make sure your PC meets the following system requirements and then choose the proper installation files to install the Omada Controller software.

System Requirements

Operating System: 64-bit Linux operating system, including Ubuntu 14.04/16.04/17.04, 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 the Omada Controller

Download the installation file of Omada Controller from our website https://www.tp-link.com/en/ download/EAP-Controller.html.

Make sure 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** 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

Follow the steps below to install Omada Controller on your Linux PC:

- 1. Make sure your PC is running in root mode. You can use this command to enter root mode: sudo
- Extract the tar.gz file using the command: tar zxvf Omada_Controller_v3.0.5_linux_x64_targz.tar.gz
- Install Omada Controller using the command: sudo./install.sh

Install the .deb file

Follow the steps below to install Omada Controller on your Linux PC:

- 1. Make sure your PC is running in root mode. You can use this command to enter root mode: sudo
- 2. Install the .deb file using the command:

dpkg -i Omada_Controller_v3.0.5_linux_x64.deb

Tips:

- 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 ./uninstall.sh.
- During uninstallation, you can choose whether to backup 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.

1.3 Inform the EAPs of the Controller Host's Address

If your Controller Host and EAPs are in the same network segment, you can skip this section.

If your Controller Host and EAPs are in different subnets, you need to install Omada Discovery Utility on a host that is in the same network segment with the EAPs. Omada Discovery Utility can help EAPs find the Controller Host.

System Requirements

Windows 7/8/10/Server

Mac OS X 10.7/10.8/10.9/10.10/10.11

Install and Use Omada Discovery Utility

Follow the steps below to install Omada Discovery Utility and use it to inform the EAPs of the Controller Host's IP address:

- 1. Download the installation file with the latest version from the website https://www.tp-link.com/ en/download/EAP-Controller.html#EAP_Discovery_Tool.
- Make sure you have JRE (Java Runtime Environment) with version1.8 installed on your system before installation. If your system loses JRE, download JRE from the website https://www. oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html and install it on your system.
- 3. For Windows OS, run the start-omada-discovery-utility.bat to open the Omada Discovery Utility. For Mac OS, use the command java –jar ** to open the Omada Discovery Utility. Then the following window will pop up. This window shows the information of all EAPs in the same LAN.

	ng cuit					
in.	Ala					
6.64	MAC NUMERIA	Britania .	Ski kr	No.461	3.4 c	Listen -
	F (1994) 19 87 12	TV EXT TH	19-10-29	18 (Kan235) (P	Protein 1	Al rep.
	discharge .	INTERNAL	. L'étaceturales :	A., 30403-20079	Park 9	Ri aye
	PV 23-51-50-52-52	12,047,167	Extra Collect	5.56-0475-075-0	Percint	Denned
	CAN S				See. 4	Kat Sing

- 4. Click Manage in the Action column or select multiple EAPs and click Batch Setting.
- 5. Enter the hostname or IP address of the Controller Host.
- 6. Enter the EAP's username and password (both are admin by default).

De vice information	
States.	Directory.
Market	EM 976
D. A. B. ev.	1911-1623-0-16-04
DOUT AND THE SECOND	42 CA 64 TO 64 CM
Carle dar Harbare JP	16/10/11/00
Decisions	- Arrest
Financial	
- Agis	12 m

7. Click **Apply** to inform the EAP of the Controller Host's hostname or IP address. And then the connection can be established between the EAP and the Controller Host.

1.4 Start and Log In to the Omada Controller

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

1.4.1 Launch Omada Controller

Double click the icon k and the following window will pop up. You can click **Hide** to hide this window but do not close it. After a while, your web browser will automatically open.



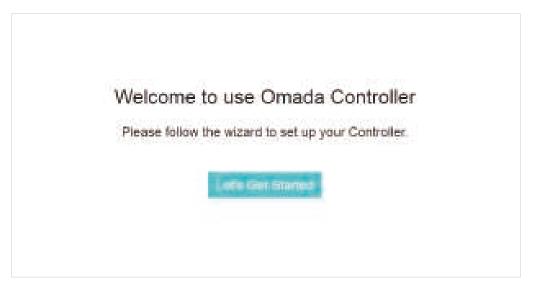
Note:

- If your browser does not open automatically, click Launch a Browser to Manage Wireless Network. 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.
- Only one Omada Controller can run in a LAN. If an Omada Controller has already been running on a host that is in your LAN, you will be redirected to the Omada Controller interface on that host.

1.4.2 Do the 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.



2. Specify a name for Omada Controller. Click Next.

Give a controller:	Grade Camatar Select 11-32 converses
1000946633	

3. Specify a username and password for the login account. Specify the email address for resetting your password in case that you forget the password. After logging in 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 Configure Mail Server. Click Next.

let up a Usernam	e and Pennword for local log	(h)	
ladek perjar	administration -		H-M (Farrente)
Tanana T.		ø	(F-2) drawnerses, only terminer, and believe (
andre Passandi		ø	
and Address	administration@ww.inspin.com		Contension Zones you'r leifod i ddonor 20 ywlanor wedd he' nearddog ynai adarwand. Thw -

4. The setup page displays all the detected EAPs in the network. Select one or more EAPs to be managed and click **Next**.

Sec. 1	and a pair in the set of the set in
2 Madei	4 Handsore Mercine
EXPERION:	1400
Anni di yay	elt frants

 Set an SSID name (wireless network name) and password for the EAPs to be managed. Omada Controller will create two wireless networks, a 2.4GHz one and a 5GHz one, both encrypted in WPA2-PSK mode. Click Next.

		O O O O
Create a windes		
Former's Tames	sagr	17 (El Descrine)
Pathoetit	<u></u>	4.0 modeled
Acres 1		

6. If you want to manage EAPs via Omada Cloud, enable the Cloud Access button, and bind your TP-Link ID to your Omada Controller, and then click Next. If you want to manage EAPs on the local network, you can just click Skip. For more details about Omada Cloud, please refer to <u>Omada Cloud Service</u> in chapter 4.

Log in and bird	your TP-Line ID		
Daul Assess	10		
Enai	site geographicam		
Passant		429	
	Transfer to Th	Lost 107 (Lossoft, April	

7. Review your settings and click **Finish**.

THE HOUSE	ent.	Wireless N	letwork	Cloud Acc	886
-	americant	Manufact Harne	\$6.0n	Gloud Accesse	-
	10141	Personal	12342610	TP-Sim da	Buttingerite

1.4.3 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/login, or 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 on the management devices through Omada Cloud service.

1.5 Create Sites and Adopt EAPs

Omada Controller can manage multiple EAP networks, which are called sites. Multiple sites are logically separated, and each site has its own configurations. There is an initial site named **Default**. The **Default** site cannot be deleted. If you have no need to manage EAPs with different sites, you can edit the default site and skip the **Create Sites** section. However, **Adopt the EAPs** is a necessary step to manage the EAPs.

1.5.1 Create Sites

There are three methods to create sites: Add sites, Import sites, and Copy sites. Determine the method according to your need and refer to the following introductions to create sites.

Add Sites

Follow the steps below to add a new site directly.

1. Click **See Deal** in the top left corner of the page and select **Replaced**, and then the following window will pop up.

(Silv Hoves Q.						() (rest	(): O (
‡ Alte Name	t Alema	‡ Connected	¢ Disconnected	t isolated	÷ lisers	‡ Gurten	Action
166.44	6	ít.	ě2	õ	1 E.	-31	
(Def)	Ŵ	19	Ϊ.	10 - E	10°	- 35	0.0
Sec.	30	- (g	x 2.	168	10 C	- CF	RS IT

2. Click () and enter a unique name for the new site.

Add Site	6	2
Site Name.	Office A	
Apply		

3. Click Apply to create the site.

Import sites

You can import the site from another controller. The site settings and EAPs in the site will be imported to the new site. Note that the site to be imported must come from a different controller.

1. Click we be in the top left corner of the page and select , and then the following window will pop up.

Signara Q						(Chapter	a. o
4 Sela Nome	4 Alwis	# Connected	4 Disconnected	• isolation	4 Osers	# Guests	Action
Defection		3 6		- 34	W.	- 42 L	13
100	10 10	2.01	10	- 34	Ū.	- a	DØ
2562	30	Sec	36	- 92	- 10 C	- 32	15.00

2. Click 🔔 Import Ste and enter a unique name for the new site.

Import Site	,	3
	e-3 axe select a file Urowsc Import	

3. Click Browse to upload the backup file of other site and click Import to import the site.

Import Site		0
Site Name: Choose I IIe:	Site_A_aitebackup.clg	Urowse Import

Tips:

To export sites (including site settings and EAPs in the sites) from one controller to another, use the Migrate function. For more details about Migrate, refer to Migrate.

Copy Sites

With **Site Copy**, you can create a new site with the same settings as the existing sites on your controller. Note that only Note that only the site settings will be copied. The EAPs will be still managed at the original site.

1. Click window will pop up.

Sile Name 🔍 🔍						() mod	an 🗛
‡ Site Name	÷ ARMS	¢ connècted	÷ Disconnected	\$ Isofatio	¢ üsers	¢ Calesis	Action
(Delta II)	- 10 ²	ંદ	- ar	Ť.	- 12 1	1	3
1947	- 10 10	ંદ	аř.	ай.	(E)	್ಟ್	C) 🖛 🖬
560.2	16 -	6	<u>3</u>	100	- 10 C	10	0.0

2. Select a site that you want copy all the settings and click in the Action column. Then enter a unique name for the new site.

Site Copy	0
Note: With Site Copy, you can create a new site with the same configuration as the existing site.	
Apply	

3. Click Apply to create the site.

1.5.2 Adopt the EAPs

Omada Controller can discover all EAPs currently connected in the network and display their connection status. All EAPs are in **Pending** status when first discovered by Omada Controller. To manage the EAPs, you need to adopt them. In the quick setup process, Omada Controller will automatically adopt the selected EAPs using the default username and password (both are admin). However, if you have changed the username or password of your EAPs before, Omada Controller cannot automatically adopt them, and you need to refer to the following steps to adopt them manually.

To ensure that all EAPs are adopted, follow the steps below:

 Select a site and go to Access Points > Pending. The table displays all the EAPs that have not been adopted.

P . 14	e en 1	-		14 14		ha da na	in the second se				0.01
-		*** 1.2*							W925	12-12	1 T=
	$i=j_{1}\lambda_{1}$	10.00	10.0	- Jesa - J	$C_{\rm ACC}^{\rm max}$	Conversion	Sec.	Sec. and	Sec.	364	
and the second	and a contra	10 (cm) (d)	-	Creation and	- 564			1. H	1.00	10.0	10
1. The second second									112 111	X CO	1. The second

2. Click the **Retry** button in the **Action** column and enter the current username and password of the EAP. Click **Apply**.

им атактыка это разристо нарти	63	8
the second s	we been changed by Data MC Die County Database en and y actes Diametrical accounter and parametric	
Vernamis		
Perivert	65	
- furth		

Tips:

- If you have a new discovered EAP, you can click the **Adopt** button in the **Action** column to adopt the EAP. Omada Controller will automatically adopt the EAP using the default username and password (both are admin).
- If you have multiple new discovered EAPs, and all of them have the default username and password (both are admin), you can click the **Batch Adopt** button to adopt them in batch. But if there are any EAPs with the Retry button, it means that the username and password of these EAPs have been changed. You need to first adopt them before batch adopt the rest EAPs.
- 3. After EAPs are adopted, the status will change from **Pending** to **Connected**. All the EAPs' username and password will become the same as those of the Controller's administrator account you created in the <u>Basic Configuration</u>.

Tips:

If you want to change the EAPs' username and password, refer to <u>Device Account</u>.

1.6 Monitor and Manage the EAPs

When all the configurations above are finished, you can centrally monitor and manage the EAPs via the Omada Controller's management interface. The management interface is divided into three sections as the following figure shows.

		VIEW PARTY IN LAST	14	kab		100
Q)	ad in		4	-	
lat =	- www.			and any first	distant in	1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -
n Naad (Sa	in de	n 200000	anas en	22	0 m 1 m - 0 m	A
	200 44 200 100 40 200				÷.,	
Section A	у	ou can click 🖸	to refresh the	e status of EAPs a current page, cl sign out from the	ick 💿 to globall	y configure the
				you to group yo r to <u>Create Sites</u>		anage them in
Section B	l Ir	n Section B, you	can centrally m	onitor the EAPs a	nd clients.	

2 Monitor and Manage the Network

With Omada Controller you can monitor the EAPs and centrally manage your wireless network. This chapter includes the following sections:

- View the Statistics of the Network
- Monitor the Network with the Map
- Monitor and Manage the EAPs
- Monitor and Manage Clients
- View Clients Statistics during the Specified Period
- Manage the Rogue APs List
- View Past Guest Authorization
- View Logs

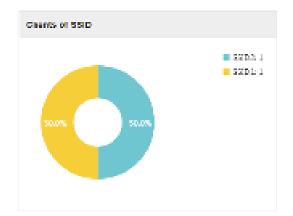
2.1 View the Statistics of the Network

Omada Controller collects all statistics of the managed EAPs and displays the statistical information via graphs, pie charts and tables, providing an overview of your wireless network.

	THE OTHER PROPERTY.				
					1000
no second approximation	international Bu		1997 B		5.00 M
	a. 00 a			**	W.
	loon an oline				e 104 k 19
17 8 1997 8 1997 19	A 19944			=(1+)	
CALC: NO.			1	1.1	-
	DO ED DO AD DO AD DO THE DO THE DO AD DO A	an well it an well it an well and an	Exception Response Exception Respons	Provide and a second seco	Interval Interval Interval Interval Interval Interval

2.1.1 View the Client Distribution on SSID

A visual pie chart shows the client distribution on each SSID. For example, the SSID1 has one client, which occupies 50% of all the clients.



2.1.2 Have a Quick Look at EAPs and Clients

This tab displays the **Most Active AP**, the **Most Active Clients** and the **All-Time Top Client**. You can click the MAC address of the EAP or the client to see more details.

	Quick Look				
	 Most Active AP: 	LA 23-51 0 Download Upload:	<u>16 22 52</u> 30.65 M 022.94 K		
	 Most Active Client: 	<u>(Phone</u> Download Uplead:	769.69 K 112.29 K		
	 All time Top Client 	<u>unknown</u> Deration Download: Upload	46m 12a 14.17 M 3.22 M		
Most Active AP	The current conne	ected AP wit	h the maximu	m traffic.	
Most Active Client	The current conne	ected client	with the maxir	num traffic.	
All-time Top Client	The client with t accessed the EAP		m traffic am	ong all the clients that ha	ve e

2.1.3 View Current Usage-Top EAPs

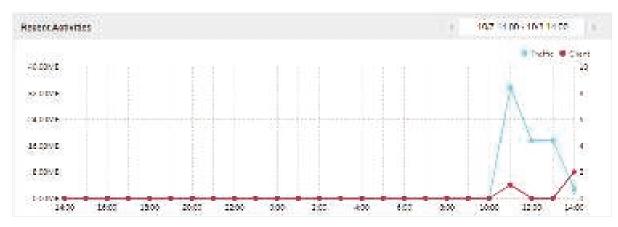
This tab lists the number of connected clients and the data traffic condition of the ten APs that use the most traffic currently.

Carrent Usage - Top -	AFo				11 0.10		
÷	e.	Clients	Notients	Traffic(MD)	%Traffic		
16.9.9	a v a	2	005	4.0	- 124		
18.8.03	96 A 12	-	es		- 6%		
Clients	The amou	unt of clients con	nected to this EAP.				
%Clients	The prop	The proportion of current connected clients to the Top EAPs' total client amount.					
Traffic (MB)	The total amount of data transmitted by this EAP, which equals the sum of the transmission traffic of all the current clients that connect to the AP.						
%Traffic		ortion of the EAP sion amount.	's current data trans	mission amoun	t to the Top EAPs' total		

2.1.4 View Recent Activities

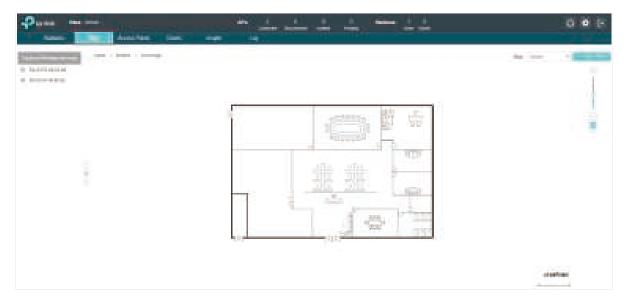
The **Recent Activities** statistics can be toggled between a view for the past specific 24 hours and one for the past specific 30 days.

The left ordinate axis indicates the traffic and the right one represents the number of the clients. The abscissa axis shows the selected time period. **Traffic** indicates a visual graph of the network traffic during the selected time period. **Client** indicates a visual graph of the number of the connected clients during the selected time period. For example, the statistics information at 15:00 indicates the traffic size and client number from 14:00 to 15:00. In the following figure, at 11 o'clock, the traffic is about 34MB and there is 1 clients connected to the AP.



2.2 Monitor the Network with the Map

You can upload your local map images and monitor the status and coverage range of each EAP with the map. When you initially launch Omada Controller, a default map is displayed as the following figure shows. Follow the instructions below to add your own map and manage the EAPs via the map.



2.2.1 Add a Map

Prepare a map image in .jpg, .jpeg, .gif, .png, .bmp, .tiff format. And then follow the steps below to add the map to the Omada Controller.

1. Click Configure Maps on the upper right corner of the Map page and click Add.

Configure Nape	0
	0 10
Default.	GI

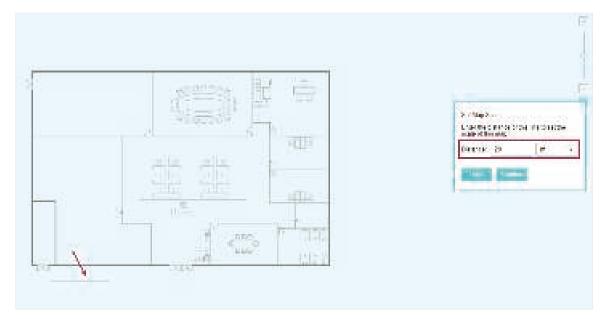
2. Enter the map description, select your map image, and click **Create**.

figure Maps		
		🕒 Ada
Provide a descripti computer	ion for the map and browse for an in	nage on your
Description:	Roam	
Upload an Image:		
Upload an Image: " jpg," jpeg," gif,"	png," imp," till - Prosee	
	_	

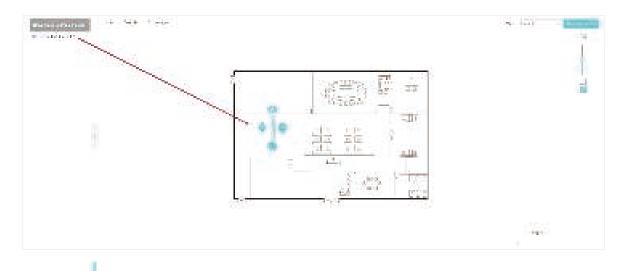
3. Select your local map from the drop-down list on the upper right corner of the map area.



4. Click in Draw a line on the map and enter the distance the line represents. Then the Omada Controller will compute and generate the map scale automatically based on your configuration.



5. Drag the EAPs from the **Unplaced APs** list to the appropriate locations on the map according to their actual locations.



You can click to reveal additional options:



0	Lock the selected EAP in the current location on the map.
0	Unlock the selected EAP and you can drag it to another location.
0	Display the EAP's details and configure the wireless parameters. Refer to <u>Configure</u> <u>the EAPs Separately</u> .
۰	Remove the selected EAP back into the Unplaced APs list.
0	Flash the LED of the EAP on the map. Then the LED will flash for 10 minutes or until the cancel button is clicked again.
0	Click the button to stop the LED from flashing.

2.2.2 Monitor the EAPs on the Map

Click any of the following options to display EAP Label, Details, and Coverage on the map.

	Label Details Coverage
Label	Display the EAP's name. The default name is the MAC address of the EAP.
Details	Display the EAP's name, MAC address, IP address, transmitting/receiving channel, number of connected users, and number of connected guests.
Coverage	Display a visual representation of the wireless range covered by EAPs. The actual signal coverage may be smaller than the visual coverage on the map because the obstacles around the EAPs will weaken the signal.

3	el l	Details	Coverage

2.3 Monitor and Manage the EAPs

Omada Controller can discover all the EAPs currently connected to the network and display the information of them on the **Access Points** page.

Pir +	ore No I			an. Ang an							C P 1
A. Terrare state at the	1.20	a static free	100	1995 - 1995 1995						- Weiter and	ante de la
14.94	-	0.044797	1.41	18.945	27	6. arman a mar	8.92 Y		1.000	rij se	22
1111 A.R.A	****	distant.	100 a. a. d	140000	1.05		10.00	- 102		100	1.81.2.5
and a second sec	Provide State	7.9. 9	14	about the p	1	Press and a rest of	1.00		1000	nia Linearage	a de la Calencia. Notas de la Calencia d

2.3.1 Manage the EAPs in Different Status

According to their connection status, EAPs are divided into four categories: **Connected**, **Disconnected**, **Isolated** and **Pending**. You can view the EAPs in different status on different pages:

	All	Connected	Disconnected	Isolated		Pending	
--	-----	-----------	--------------	----------	--	---------	--

All	Displays the information of all EAPs in different status.
Connected	Displays the connected EAPs.
	The status of connected EAPs includes two cases: Connected and Connected (Wireless) .
	Connected: After you adopt a wired EAP in Pending status, its status will become Provisioning, then Configuring and Connected eventually.
	Connected (Wireless) : In a mesh network, if an EAP has a successful wireless uplink, its status will become Adopting (Wireless) and then Connected (Wireless).
	Only connected EAPs can be managed. A connected EAP will turn into a pending one after you forget it. You can refer to <u>Forget this AP</u> to forget an EAP or click Forget All on the page to forget all the connected EAPs.
Disconnected	Displays the disconnected EAPs.
	If a connected EAP powers off or disconnects from the Omada Controller, it will be in Disconnected status. When a disconnected EAP is reset to factory defaults or forgot, it will turn into a pending one again. You can refer to <u>Forget this AP</u> to forget a EAP or click Forget All on the page to forget all the disconnected EAPs.
Isolated	Displays the isolated EAPs.
	In a mesh network, when the EAP which has been managed before by Omada Controller connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state. The isolated EAP searches for wireless uplink and the LED on the device turns green and flashes off every 5 seconds. To know more about mesh network, refer to <u>Configure Mesh</u> .

Pending	Displays the pending EAPs.
	The status of pending EAPs includes three cases: Pending , Pending (Wireless) and Managed by others .
	Pending: All the EAPs with wired network connection are in pending status by default when first discovered by Omada Controller.
	Pending (Wireless): The factory default EAP with mesh functions and no wired network connection is in Pending (Wireless) status when first discovered by Omada Controller.
	Managed by others: An EAP is located on the same network as the controller, but has been already managed by an existing controller before. You can provide the username/password to unbind the EAP from the existing controller and begin adoption in current controller.
	Only after pending EAPs are adopted and connected, you can manage them. To adopt pending EAPs, refer to <u>Adopt the EAPs</u> .

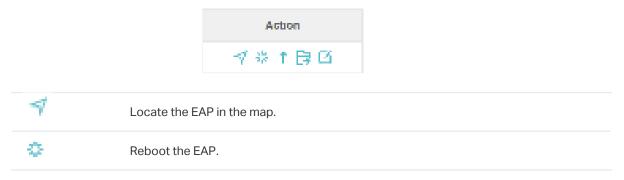
2.3.2 View the Detailed Information of EAPs

You can click **Overview**, **Config**, **Performance** or **Mesh Network** tab to view different detailed information of EAPs.

	Overview Config Performance Mesh Network
Overview	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, channel number of connected clients and download/upload bytes.
Config	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, WLAN Group bounded with the 2G and 5G of the EAP, and radio of the 2G and 5G.
Performance	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, number of connected 2G clients and 5G clients, TX(Downloaded Traffic), RX(Uploaded Traffic), TX 2G and TX 5G.
Mesh Network	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, number of connected clients, hops, uplink APs and downlink APs.

2.3.3 Manage the EAPs in the Action Column

You can execute the corresponding operation to the EAP by clicking an icon in the Action column.



Upgrade the EAP.

Two options are available for upgrading: upgrade online and upgrade manually.

Upgrade online: With Cloud Access enabled on the controller and a TP-Link ID bound with the controller, the latest firmware for the EAP can be detected by the controller automatically. And you can upgrade the EAP online by clicking **Upgrade Now**. For more details about Cloud Access, refer to <u>Omada Cloud Service</u>.

Upgrade manually: Click **Browse** to locate and choose the upgrade file in your computer, then click **Upgrade** to install the latest EAP firmware. The Status will appear as **Upgrading** until the process is complete and the EAP reconnects to the Omada Controller.

0.000		
	Reconcernant and a second of a	
	Fig. 200 The second state of the second sta	
	The second secon	
And speed	Second State	

En l

Move the EAP to a site.

Select a site that has been created and click **Apply**. You can group all the EAPs by this way and centrally manage them on each site.

NAME AND A DESCRIPTION OF A DESCRIPTIONO			0
Marcine Ci	W b	-	
	100.0		
1000	Access (
	400 B		
	1		

 \mathbb{Z}^{n}

Configure the EAP.

For detailed instructions about how to configure the EAP on this window, refer to <u>Configure the EAPs Separately</u>.

CHE HARD	A COLUMN T	
	in the last the	al Son and
THE REPORT OF		a second
135 600		20 2.44
en l'antenna a	4.3	200
	8	the states
and the second		
Protect and		7.9
Sile Contained	81.54.8 (a).55.85	
0 declarer	10,0 .	
Note	BANDIN COLLEC	
ffer van Vindaa	Same Private as t	
17.10	(19)	
Marineen.		
1	in my conversion of	
111		

t

Note:

- Only managed EAPs can be rebooted or upgraded.
- The EAP which is managed by the controller can not be logged in to its own management interface. To log in to the EAP's own management interface, forget the EAP in the controller first.

2.4 Monitor and Manage Clients

The **Clients** tab displays the clients connected to the EAP network.

P	ant even. Na rege	-			" and the	den side	-	an : 				0 • •
der (1997 - State State)	ne di			12							100	1001224
1 Bindanian	and states	2011 Aug	100000		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The Ball of States	a support	a de la composition	e track and	14 A.A.	194	1.44
Ens.	1		1447 40414	- 26	-	2.00	21.40	×2	92	1.4	-	A 1414

2.4.1 View the Current Information of Clients

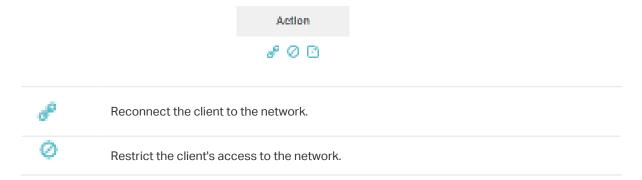
The clients are divided into two types: User and Guest. Users are the clients connected to the EAP wireless network without the <u>Portal Authentication</u>. Guests are the clients connected to the EAP wireless network with the <u>Portal Authentication</u>.

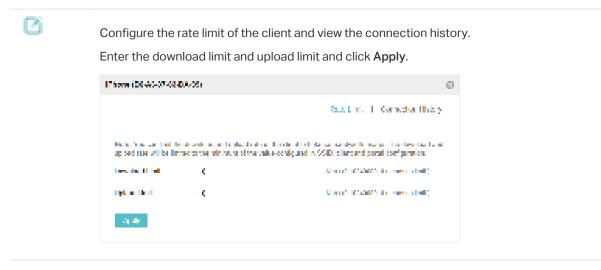
You can click the following tabs to respectively view the detailed information of users and guests.

	All Clients Users Guests
All Clients	The page displays the information of all clients including users and guests.
Users	The page displays the information of Users.
Guests	The page displays the information of Guests.

2.4.2 Manage Clients in the Action Column

You can execute the corresponding operation to the EAP by clicking an icon in the Action column:





0

If the client is a Guest, you can click this icon to cancel the authorization for it.

2.5 View Clients Statistics During the Specified Period

The **Clients Statistics** page under the **Insight** tab displays the information of clients that have connected to the EAPs network during a specified period.

Posta las con		14	e energia dire inci			5 0 1
and the second second				a standa	nu	
Check Labolity				Same and	and the second second	And December (1994)
	int wind rate la 💽 1	nan araka 🔅	5			
(Income)	100 A.M. 100	19-4-44	10 A and 1	15.040	4 - 3 -	1.4.4
Las	B-010-01	10.	100	(the the)	COMPANY STATE	1.1
0.778	Concentration.	- 15 P	9.2	1997.1	A DEL SUS	
$q_{\rm eff} = \overline{ \mathbf{x}_{\rm eff} }$					N.N. (1978).44	an fan de anne 👘 🚺

2.5.1 Select a Specified Period

Select a period from the drop-down menu. Then the page will display clients that have connected to the EAPs network during the period.

Last Seen: All 🔹 👻
Last Seen, All
Last Seen: 1 Day
Last Seen, 3 Days
Last Seen: 7 Days
Last Seen, 14 Days
Last Seen: 30 Days

2.5.2 View the History Information of Clients

You can click the client's MAC address to get its connection history and configure the Rate Limit feature for this client. In addition, you can click the following tabs to view the information of different types of clients:

	All User Guest Blocked Rate Limited
All	The page displays the history information of all the clients.
User	The page displays the history information of Users. Users are the clients connected to the EAP wireless network without the <u>Portal</u> <u>Authentication</u> .
Guest	The page displays the history information of Guests. Guests are the clients connected to the EAP wireless network with the <u>Portal</u> <u>Authentication</u> .
Blocked	The page displays the clients that have been blocked.
Rate Limited	The page displays the clients that have been limited upload or download rate.

All Office Only

All	The page displays the history information of all clients.
Offline Only	The page displays the history information of the off-line clients.

2.5.3 Manage Clients in the Action Column

You can execute the corresponding operation to the EAP in the Action column:

Ø	Block the client's access to the network.
Ó	Resume the client's access.
Ø	Configure the rate limit of the client and view the connection history.
•	Remove the limit to the client's upload or download rates.

2.6 Manage the Rogue APs List

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. The Omada Controller can scan all channels to detect all nearby EAPs. If rogue APs are detected, they will be shown on the **Untrusted Rogue APs** list. Besides, you can move the untrusted rogue APs to the **Trusted Rogue APs** list.

By default, the Rogue AP Detection feature is disabled. To allow your EAP to detect nearby APs, you need to enable this feature for this EAP. You can refer to <u>Rogue AP Detection</u>.

2.6.1 Manage the Untrusted Rogue APs List

The Untrusted Rogue APs page displays the detailed information of untrusted rogue APs.

	anı.	NO - 7712	**		ein annar d	der en		C 🕈 P
SINS S	HI WALLA							
a sa elfone Vi							The second se	The second s
1.000								
1949	101	10.4	19.00	1.000	Contract of the	10.00	A CONTRACTOR OF	(#3#F)
- 44 M - 100 C	7.44	1000	1.5			10	C 2004 1211	-
2010 C 10 C 10 C		164		100		100	$(p_{i}) \in [m_{i}] \setminus [m_{i}]$	1.1
Sec. Sec. Sec.		100	80	14			(1997) (1997) (1997)	- T . (
101-111-1	(1966)	1.10	10			11	en an en an estad	
in succession	wir .	16	6		11		A 174 (a 1	
The bar strike of	and the first state of the	+	18 g		10	+1	2.200.000	
11.00 A.M.	20		35	- 35	11	34	2.2.2.2.4.2.2.2.1	
A. P. M. M. M	79.777	1.000		81	- H		(2+7,27) (
14.715.0	Sec. A sec.	1 A .	49	90 C	2.5	188	second count-	
15101.54	the ory		65	e	41		44.004.04.0	
$(a_1,a_2,\ldots,a_{n-1},a_{n-1},\ldots,a_{n-1},a_{n-1},\ldots,a_{n-1}$	Sec.		212	225			The second second	ner ogs

You can execute the corresponding operation to the EAP in the Action column:



2.6.2 Manage the Trusted Rogue APs List

The Trusted Rogue APs page displays the detailed information of trusted rogue APs.

Plane de rer			nin sin me			591
10.52		277 B (1999				
						01-3-
1948	1.000	1.054	1.10.00	100477	6 6 M H	1000
100 P 100	1.4.14	244			5 W 000 L 094 5	
Ar 1.47 (1997)	(1) (a (a (1)))	<u></u>	345	14 C	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
0.04 (1)						ant fall and 🔤 🎫

You can execute the corresponding operation to the EAP by clicking an icon in the Action column:

Q

🙆 Export

Move the trusted rogue AP to the Untrusted Rogue APs list.

Export and download the current Trusted Rogue APs list and save it on your PC.



Import a saved Trusted Rogue APs list. If the MAC address of an AP appears in list, it will not be detected as a rogue AP.

Import Trusted AP List		0
Import Mode	🛞 Replace 🔿 Merge	
Import Source File	Please select a file.	
Import		

Please follow the steps below:

- 1. Select **Replace** (replace the current Trusted Rogue APs list with the one you import) or **Merge** (add the APs in the file to the current Trusted Rogue APs list).
- 2. Click Browse to locate the file and choose it.
- 3. Click Import to import the Trusted Rogue APs list.

2.7 View Past Guest Authorization

The Past Guest Authorization page displays the details about all the clients that accessed the network during a certain time period. You can select a period in the drop-down list.

Pre-		and the second second second	-	C		30.
States a		ALC: NO. OF STREET, ST	Ditta and a second			
n Den Aster Kellen				(Sec. 1. (N. 1))		1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
	1975	94 - C	the second	1 m	(14 - 14 A)	100-
10.001	19.1	414	Section 1	The second second	1.00	1224
(c) (<u>- (-</u>)						1 10 10 and 10 a

2.8 View Logs

The logs of Omada Controller can effectively record, classify and manage the system information of the managed EAPs, providing powerful support for you to monitor network operation and diagnose malfunctions. The Log page displays the log's module, level, content, operator and occurred time.

Press inter	47. 18 - 1944-181	an an an an an an an an	~~		2.4.1
(P) (100000000					1110.00
free and a straight	1000 P				(c) - 44.4
10.04	DOM:		- Artesta	37.4	4.74
	144	and a set of second second second second		in the state of the	o.
2.2011	- Marson	Committee Conception Provide	100	ALCOND. 11	11
	Sec. 20	the first second second second second second second	-	The second second	14
1.000	PROPERTY.	And the second second second second second	100	where the	
1000	11	The first stands of the strength of the standard first	÷.	1 A.M. (1997)	
20	1944	The second		 Minimum 	
2.5	1999	man a dependent der begehnten eine mit der Armennen		1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	
1.000	3.75	والمراجع وال	2.00	- marine i	.0
	1010	IN THE CONTRACT OF A DESCRIPTION		THE CONTRACTOR	0
0	directly.	and the second of the second second second second	<i>7</i> 2	1. 1. A. 1. A. 1.	. 4
143. A. A. A.				THE NEW W	2010/00/00/00/00/00/00/00/00/00/00/00/00/

You can view the alerts on a separate page by clicking Alerts in the top right corner of the page. As

follows, you can click \square to mark the alerts as read.

Pine ore			server 1 1 server		64
1					11
1967	0014	* coult	\$ Carta	12.4	404
£ 5		the constant of constant sectors in the		102254(2411)	8.0
4.64.5				HIN I HAD	agent Page 1

Note:

The logs and alerts of the controller with version 3.0.5 or below will be discarded after the controller is upgraded to version 3.1.4 or above.

3 Configure the EAPs Globally

This chapter introduces the global configurations applied to all the managed EAPs. To configure a specific EAP, please refer to <u>Chapter 5 Configure the EAPs Separately</u>.

In global configurations, you can configure the following items:

- Wireless Network
- Access Control
- Portal Authentication
- Free Authentication Policy
- MAC Filter
- Scheduler
- QoS
- Site Settings

3.1 Wireless Network

In addition to the wireless network you created in Quick Start, you can add more wireless networks and configure the advanced wireless parameters to improve the network quality.

3.1.1 Add Wireless Networks

To add wireless networks, follow the steps below.

1. Go to Wireless Settings > Basic Wireless Setting.

<u> </u>	MALIGNO SC.	1000 7410 256 80	Ages	est Weeless				
- 0		Joka I	MAN Cases					
o Action	Rate Limit	Access Control Rale	Portal	Galact Nationly	kand	: Security	† 980 Name	0
19 M	Cat of	News	Cook /	General	2404.504	WHY Pas	- 850 A	4

- 2. Click 💽 at the right of Maximum Termin to add a WLAN group. Creating WLAN groups is an easy way to quickly deploy EAPs by creating a template-based set of SSIDs with wireless parameters. Different WLAN groups can be applied to different EAPs. If you have no need to group your wireless networks, you can use the default WLAN group and skip this step.
- 3. Specify a name for the group and click Apply.

WLAN Group		0
Maria	thang)	
Apply		

- 4. Select the WLAN group working in and click () Add to add an SSID to the specific WLAN group.
- 5. Configure the parameters in the following window.

Basia linto		*
SSID Name	1	
Bead	📃 2.4GFb 🗟 2.6Fb	
Gileat Network	Endline 🛞	
Security Mode	WP4-P5K +	
Vireless Paseword	ø	
Advanced Settings		

SSID Name	Enter an SSID name using up to 32 characters.
Band	Select the radio band to add the SSID.
Guest Network	With this option enabled, the network act as a guest network. All the clients connecting to the SSID will be blocked from reaching any private IP subnet.
Security Mode	Select the security mode of the wireless network. None: The hosts can access the wireless network without authentication. WEP/WPA-Enterprise/WPA-PSK: The hosts need to get authenticated before accessing the wireless network. For the network security, you are suggested to encrypt your wireless network. Settings vary in different security modes and the details are in the following introduction.

Note:

- 8 SSIDs can be created on each band at most.
- The SSID on different radio band with the same name will be regarded as an identical SSID entry. When you upgrade your controller or restore the backup files from the controller with the version 3.0.5 or below, the SSID entries with the same name will be merged if they are on 2.4GHz and 5GHz in the same WLAN group. All the configurations in the entry will be changed to the parameters of the original SSID on the 2.4GHz radio band.

Following is the detailed introduction of None, WEP, WPA-Enterprise and WPA-PSK.

None

The hosts can access the wireless network without authentication. Configure th advanced parameters in the following window.

Basic Into			Y
Administ Settings			
SSID Broadcast:	- Fostia		
Wireless VEAN	🚬 Freible		
Wreless VL/WTD:	•	(1 4034)	
RADIUS MAC Authentication:	2 Freible		
Nutrientication Server IP:			
Authentication Server Port	ikt2	(1.05535)	
Authentinetion Server Password	ø		
MAC Address Format	aabbeeddeeff +	8	
Empty Password	®		
Access Control Rule:	None +		
Rate Limit:	🗠 Eceble 🌚		
Jownload Limit		Köps (8.16340306, 8 mözns so limit.)	
Jpload Limit		Ktpt. (3-10240306, 0 mpane to limit.)	
Section			

SSID Broadcast With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP.

The option is enabled by default.

Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other.
	To set a wireless VLAN for the wireless network, enable the option and set a VLAN ID in the Wireless VLAN ID .
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 1 to 4094.
RADIUS MAC Authentication	With this option enabled, the EAP will send the MAC address of the client to the RADIUS server as the username and password for authentication. If the authorization succeeds, the RADIUS server grants the client access to the network.
	To set RADIUS MAC Authentication, enable the option and configure the following parameters: Authentication Server IP, Authentication Server Port, Authentication Server Password, MAC Address Format, and Empty Password.
Authentication Server IP	With RADIUS MAC Authentication enabled, enter the IP address of the authentication server.
Authentication Server Port	With RADIUS MAC Authentication enabled, enter the port number you have set on the RADIUS server for authentication requests. The default setting is 1812.
Authentication Server Password	With RADIUS MAC Authentication enabled, enter the authentication password. The authentication server and the controller use the password to encrypt passwords and exchange responses.
MAC Address Format	With RADIUS MAC Authentication enabled, select the format to convert a client's MAC address to the RADIUS username.
Empty Password	With the option enabled, a blank password for RADIUS MAC Authentication will be allowed. With the option disabled, the password will be the same as the username.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to <u>Access</u> <u>Control</u> .
Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details.
	Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Download Limit	With Rate Limit enabled, specify the limit of download rate. 0 means unlimited.
Upload Limit	With Rate Limit enabled, specify the limit of upload rate. 0 means unlimited.

WEP

WEP is based on the IEEE 802.11 standard and less safe than WPA-Enterprise and WPA-PSK.

Note:

WEP is not supported in 802.11n mode or 802.11ac mode. If WEP is applied in 802.11n, 802.11 ac or 802.11n/ ac mixed mode, the clients may not be able to access the wireless network. If WEP is applied in 11b/g/n mode (2.4GHz) or 11a/n (5GHz), the EAP may work at a low transmission rate.

Security Mode:	WLP	
Key Selected:	Key1	Ŧ
Key Value:	weblaw	

Key Selected Select one key to specify. You can configure four keys at most.

Key Value Enter the WEP keys. The length and valid characters are affected by key type.

Basic info		
Advanced Settings		
Typa.	🛞 Auto 👘 Open System 🔿 Shared Key	
WEP Key Format	ASCII O Hexadecimal	
Key type	📲 6484 🙄 12031 🙄 15204	
SSID Roscicaat	Trable	
Windows VLAN	🕑 Lindele	
Wireless VLAN ID:	(1-4094)	
Access Control Rule:	None	
Hate Limit	-/ Enable (9)	
Download I intil	Keps (3-12240000). Streesess on line (
Upload Limit.	Kirps (0-107400007) it means to the final d	

Configure th advanced parameters in the following window.

Туре	Select the authentication type for WEP.
	Auto: The Omada Controller can select Open System or Shared Key automatically based on the wireless station's capability and request.
	Open System : Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission.
	Shared Key : Clients have to input password to pass the authentication, otherwise it cannot associate with the wireless network or transmit data.
WEP Key Format	Select ASCII or Hexadecima as the WEP key format.
	ASCII: ASCII format stands for any combination of keyboard characters of the specified length.
	Hexadecimal : Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.
Кеу Туре	Select the WEP key length for encryption.
	64Bit: Enter 10 hexadecimal digits or 5 ASCII characters.
	128Bit: Enter 26 hexadecimal digits or 13 ASCII characters.
	152Bit: Enter 32 hexadecimal digits or 16 ASCII characters.
Key Value	Enter the WEP keys. The length and valid characters are affected by key type.
SSID Broadcast	With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP.
	The option is enabled by default.
Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other.
	To set a wireless VLAN for the wireless network, enable the option and set a VLAN ID in the Wireless VLAN ID .
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 1 to 4094.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.
Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details.
	Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.

Upload Limit

WPA-Enterprise

The WPA-Enterprise mode requires a RADIUS server to authenticate clients. Since the WPA-Enterprise can generate different passwords for different clients, it is much safer than WPA-PSK. However, it costs much more to maintain and is usually used by enterprise.

Security Mode	WPA-Finterprise T	
RADIUS Server IP	0.0.0.0	
RADIUS Port	0	(1-65535,0 means detault port 1812)
RADIUS Proceed		
RADIUS Accounting		
Accounting Server IP		
Accounting Server Port	1013	(1-85535)
Accounting Server Passwood		
Interim Update	🖓 Lnable 🧭	
Interim Update Interval	600	(x, 604164100)

RADIUS Server IP	Enter the IP address of the RADIUS Server.
RADIUS Port	Enter the port number of the RADIUS Server.
RADIUS Password	Enter the shared secret key of the RADIUS server.
RADIUS Accounting	Enable or disable RADIUS Accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server.
Accounting Server Password	Enter the shared secret key of the accounting server.
Interim Update	With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled.
	Enter the appropriate duration between updates for EAPs in Interim Update Interval.
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.

Configure th advanced parameters in the following window.

Add SSID		0
Basic Into		*
Advinced Gellings		
Version	O Avite O WPA 👋 WP92	
Lnotyption:	O Mate O LKIP	
Croup Key Update Period	Ó	pecon (c) 77-6640300, 0 means no upgrode)
SSID Broadcast	IV Enable	
Wireless VLAN	🖓 Enable	
Revealed M AN ID	1	(44094)
Arcess Crettel Rule	None .	
Date Timit	🕞 Enable 💮	
Download Line		Repart-Int/1000 - Dimension in firms (
Ladual Linis		Race (0-10/42000 Consects in Arrith
Version	Select the version of WPA-Enter Auto: The EAP will automatically	erprise. y choose the version used by each client devi
	WPA/WPA2: Two versions of W	i-Fi Protected Access.
Encryption	Select the Encryption type.	
	Auto: The default setting is automatically based on the clie	Auto and the EAP will select TKIP or Ant device's request.
	802.11ac mode or 802.11n/a 802.11 ac or 802.11n/ac mixed	rotocol. TKIP is not supported in 802.11n mo ac mixed mode. If TKIP is applied in 802.1 mode, the clients may not be able to access TKIP is applied in 11b/g/n mode (2.4GHz) or 1 work at a low transmission rate.
	AES : Advanced Encryption State the encryption type because it	andard. We recommend that you select AES is more secure than TKIP.
Group Key Update Period	Specify a group key update period, which instructs the EAP how often it shou change the encryption keys. The value can be either 0 or 30~8640000 second 0 means no change of the encryption key anytime.	

SSID Broadcast	With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP. The option is enabled by default.
Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other. To set a wireless VLAN for the wireless network, enable the option and set a VLAN ID in the Wireless VLAN ID .
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 1 to 4094.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.
Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details. Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Download Limit	With Rate Limit enabled, specify the limit of download rate. 0 means unlimited.
Upload Limit	With Rate Limit enabled, specify the limit of upload rate. 0 means unlimited.

WPA-PSK

Based on a pre-shared key, WPA-PSK is characterized by high safety and simple settings and is mostly used by common households and small businesses.

	Security Mode	WBA-PSK	Ŧ		
	Wineless Pessword		ø		
Wireless	Configure the wir	eless password with ASCII or H	exadecimal characters.		
Password	numbers, letters	For ASCII, the length should be between 8 and 63 characters with combination of numbers, letters (case-sensitive) and common punctuations. For Hexadecimal, the length should be 64 characters (case-insensitive, 0-9, a-f, A-F).			

Configure th advanced parameters in the following window.

Add SSID		0
Basic Info		
Advanced Settings		A
Varisian	O Auto ○ WPA-PSK ● WPA	12:P9K
Encryption:	O Auto O TRIP 🛞 AES	
George Key Update Heriod	â	seconds(30 8640000, 0 means no upgrate;
SSID Broadcast	() Enside	
Wireless VLAW	- Endle	
Wireless VLAN ID:	1	(1-4094)
Access Control Rule	Note	
Rate Limit	🕞 Eneble 🥘	
Download Limit		Kips (5-15240356 Urbaars million)
Liphord Limit.	0	Klipis (5-105200399); (1 (marine dochrod))
Version	Select the version of WPA-En Auto: The EAP will automatica	terprise. Ily choose the version used by each client devic
	WPA/WPA2: Two versions of	Wi-Fi Protected Access.
Encryption	Select the Encryption type.	
	Auto: The default setting automatically based on the cli	is Auto and the EAP will select TKIP or AE entrequest.
	802.11ac mode or 802.11n 802.11 ac or 802.11n/ac mixe wireless network of the EAP. I	Protocol. TKIP is not supported in 802.11n moc /ac mixed mode. If TKIP is applied in 802.11 d mode, the clients may not be able to access th f TKIP is applied in 11b/g/n mode (2.4GHz) or 11 y work at a low transmission rate.
	AES : Advanced Encryption S the encryption type for it is me	tandard. We recommend that you select AES a pre secure than TKIP.
Group Key Update Period	change the encryption keys. 1	eriod, which instructs the EAP how often it shou The value can be either 0 or 30~8640000 second will not be changed all the time.

Upload Limit	With Rate Limit enabled, specify the limit of upload rate. 0 means unlimited.
Download Limit	With Rate Limit enabled, specify the limit of download rate. 0 means unlimited.
	Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLA ID are grouped to a VLAN. The value ranges from 1 to 4094.
	To set a wireless VLAN for the wireless network, enable the option and set VLAN ID in the Wireless VLAN ID .
Wireless VLAN	With this option enabled, the EAP can work together with the switche supporting 802.1Q VLAN. Traffic from the clients in different wireless network is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directl communicate with each other.
	that those hosts can find the wireless network identified by this SSID. If thi option is disabled, users must enter the SSID manually to connect to the EAP. The option is enabled by default.

3.1.2 Configure Advanced Wireless Parameters

Proper wireless parameters can improve the network's stability, reliability and communication efficiency. The advanced wireless parameters consist of **Fast Roaming**, **Beacon Interval**, **DTIM**

Period, RTS Threshold, Fragmentation Threshold and Airtime Fairness.

To configure the advanced wireless parameters, follow the steps below.

1. Go to Wireless Settings > Advanced Wireless Setting.

Mineleon Settings	Witeve Conitol	Gile Sellinya	Cloud Assan	Controller Settings	v
		Sayle Wileleva	Colliny Advanced Whee	ve Setting Durid Clocking	Hideve
Roaming Setting					
Lad Saming	Frankler 👔				
Apab					
2,10,12, 2,412					
De soon internatio	100	w-041100			
DTIM Period	i	11,241,1			
RTS Threehold	2017	(1.2342)			
Fregmentalkh Threshok	2010	(200-2548) services	e y combre de la combre		
Airthe Fubreau	n - Eine Alex 🚷				
- Sector					

2. Enable Fast Roaming and configure the corresponding parameters.

	Roaming Setting		
	Fast Roaming	🖓 Lnable 🧭	
	Dual Band 11k Report	🗌 Lnable 🧭	
	Force-disassociation	🗏 Lnable 🕅	
Fast Roaming	With this option enabled, 7 roaming experience when m		nts can have improved fast rent APs.
Dual Band 11k Report	With this feature disabled, the controller provides candidate AP report that contains the APs in the same band as the clients. With this feature enabled, the controller provides candidate AP report that contains the APs in both 2.4GHz and 5GHz bands.		
Force-disassociation	The controller dynamically monitors the link quality of every associated client. When the client's current link quality drops below the predefined threshold and there are some other APs with better signal, the current AP issues an 11v roaming suggestion to the client.		
	With Force-disassociation suggestion, but whether to r		AP only issues a roaming mined by the client.
	suggestion but also disass	ociates the client are to a better AP. The	not only issues a roaming after a while. Thus the client his function is recommended

3. Click Apply.

- 4. Select the band frequency
- 5. Configure the following parameters.

Beacon Interval	Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients. Beacon Interval value determines the time interval of the beacons sent by the device. You can specify a value between 40 and 100ms. The default is 100ms.
DTIM Period	The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the EAP has buffered data for client devices. The DTIM Period indicates how often the clients served by this EAP should check for buffered data still on the EAP awaiting pickup.
	You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating clients check for buffered data on the EAP at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend that you keep it by default.
RTS Threshold	RTS (Request to Send) can ensure efficient data transmission. When RTS is activated, the client will send a RTS packet to EAP to inform that it will send data before it send packets. After receiving the RTS packet, the EAP notices other clients in the same wireless network to delay their transmitting of data and informs the requesting client to send data, thus avoiding the conflict of packet. If the size of packet is larger than the RTS Threshold , the RTS mechanism will be activated.
	If you specify a low threshold value, RTS packets are sent more frequently and help the network recover from interference or collisions that might occur on a busy network. However, it also consumes more bandwidth and reduces the throughput of the packet. We recommend that you keep it by default. The recommended and default value is 2347.
Fragmentation Threshold	The fragmentation function can limit the size of packets transmitted over the network. If a packet exceeds the Fragmentation Threshold , the fragmentation function is activated and the packet will be fragmented into several packets.
	Fragmentation helps improve network performance if properly configured. However, too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.
Airtime Fairness	With this option enabled, each client connecting to the EAP can get the same amount of time to transmit data, avoiding low-data-rate clients to occupy too much network bandwidth and improving the network throughput. We recommend that you enable this function under multi-rate wireless networks.

6. Click Apply.

3.1.3 Configure Band Steering

A client device that is capable of communicating on both the 2.4GHz and 5GHz frequency bands will typically connect to the 2.4GHz band. However, if too many client devices are connected to an EAP on the 2.4GHz band, the efficiency of communication will be diminished. Band Steering can steer

dual-band clients to the 5GHz frequency band which supports higher transmission rates and more client devices, and thus to greatly improve the network quality.

To configure Band Steering, follow the steps below.

1. Go to Wireless Settings > Band Steering.

Winders Settings	Wircless Control	Sile Sedingv	Olsuel Asymp	Controller Sellings	~
		Davis Wildow Se	aling – Advanced Wirek	in Solling Datid Skipling	Not
Hand Sterning	Hadde 🔿				
sterna ber Hinsink I	Λ.	-242 📆			
Coloran as the aduals	4	- 1943 (3)			
Max Lodana.	ч.	- 241.22 🕅			
- Apply					
Serve in an the Karat Sire care defined and reaches	ning hurdien en 1990), pierre e oprover d	is in the SATE cart all relian	2018 A stant As" – A formation is	trade even its yits we its own	

- 2. Check the box to enable the Band Steering function.
- 3. Configure the following parameters to balance the clients on both frequency bands:

Connection Threshold/ Difference Threshold	Connection Threshold defines the maximum number of clients connected to the 5GHz band. The value of Connection Threshold is from 2 to 40, and the default is 20.
	Difference Threshold defines the maximum difference between the number of clients on the 5GHz band and 2.4GHz band. The value of Difference Threshold is from 1 to 8, and the default is 4.
	When the following two conditions are both met, the EAP prefers to refuse the connection request on 5GHz band and no longer steers other clients to the 5GHz band:
	1. The number of clients on the 5GHz band reaches the Connection Threshold value.
	2. The difference between the number of clients on the 2.4GHz band and 5GHz band reaches the Difference Threshold value.
Max Failures	If a client repeatedly attempts to associate with the EAP on the 5GHz band and the number of rejections reaches the value of Max Failures , the EAP will accept the request.
	The value is from 0 to 100, and the default is 10.

4. Click Apply.

3.1.4 Configure Mesh

Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the EAPs can be configured and managed within Omada controller in the same way as wired EAPs. Meanwhile, because of the ability to self-organize and self-configure, mesh also can efficiently reduce the configuration overhead.

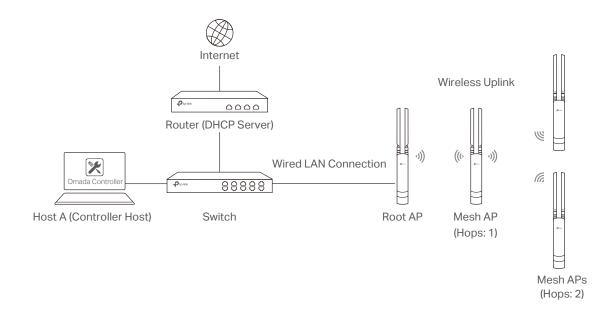
Note:

- Only EAP225-Outdoor with specific firmware (version 1.3 or above) is available for mesh function currently.
- Only the EAPs in the same site can establish a mesh network.

To understand how mesh can be used, the following terms used in Omada Controller will be introduced:

- Root AP: The AP is managed by Omada Controller with a wired data connection that can be configured to relay data to and from mesh APs (Downlink AP).
- Isolated AP: When the EAP which has been managed before by Omada Controller connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.
- Mesh AP: An isolated AP will be mesh AP after establishing a wireless connection to the AP with network access.
- Uplink AP/Downlink AP: Among mesh APs, the AP that offers the wireless connection for other APs is Uplink AP. A Root AP or an intermediate AP can be the Uplink AP. And the AP that connects to the Uplink AP is called Downlink AP. An uplink AP can offer direct wireless connection for 4 Downlink APs at most.
- Wireless Uplink: The action that a Downlink AP connects to the uplink AP.
- Hops: In a deployment that uses a root AP and more than one level of wireless uplink with intermediate APs, the uplink tiers can be referred to by root, first hop, second hop and so on. The hops cannot be more than 3.

In a basic mesh network as shown below, there is a root AP that is connected by Ethernet cable, while other isolated APs have no wired data connection. Mesh allows the isolated APs to communicate with pre-configured root AP on the network. Once powered up, factory default or unadopted EAPs can sense the EAP in range and make itself available for adoption within the Omada controller.



After all the EAPs are adopted, a mesh network is established. Then the EAPs connected to the network wirelessly also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

To establish a mesh network, follow the steps below.

- Enable Mesh Function.
- Adopt the Root AP.
- Set up wireless uplink by adopting APs in Pending (Wireless) or Isolated status.
- 1. Go to Wireless Settings > Mesh.

Marches - Arthoppe	Windows Cardini	Site Ard map	Court Survey.	Cambridge Sadinary	
		Area Winds	w Aldung – Advanted Ward	s Astropo Rom Marcon [No A
Meah:	P to the				
	Research the Neutrinetter is disabled.	de contected with	len Afrikelikse veromede	r.	
Anti-dentile ser	📙 Ende 🥴				
Considerly the edge	(\mathfrak{g}) Andre (Dermannen er $\mathfrak{g})$ (\mathfrak{g}) Germannen \mathfrak{g}	nn IP Actioner	$D_{\beta} \ln h D \neq h h \to \infty$	3	
Full Areko 1948	🗹 Drakk 🐇				
- Apple					

- 2. Check the box to enable the Mesh function.
- 3. Configure the following parameters to maintain the mesh network:

Auto Failover	Enable or disable Auto Failover. Auto Failover is used to automatically maintain the mesh network for the controller. With this feature enabled, the controller can automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. Thus the controller will automatically select a new uplink AP for the mesh EAPs when the original uplink fails.
Connectivity Detection	Specify the method of Connection Detection.
	In a mesh network, the APs can send ARP request packets to a fixed IP address to test the connectivity. If the link fails, the status of these APs will change to Isolated.
	Auto (Recommended): Select this method and the mesh APs will send ARP request packets to the default gateway for the detection.
	Custom IP Address: Select this method and specify a desired IP address. The mesh APs will send ARP request packets to the custom IP address to test the connectivity. If the IP address of the AP is in different network segments from the custom IP address, the AP will use the default gateway IP address for the detection.
Full-Sector DFS	With this feature enabled, when radar signals are detected on current channel by one EAP, the other EAPs in the mesh network will be also informed. Then all EAPs in the mesh network will switch to an alternate channel.

4. Click Apply.

5. Go to Access Points > Pending and adopt the Root AP. Then the status of the Root AP will change into Connected.

P . 14 **				ar 30	<u> </u>	l server	L.			10 a
N 1	- -	UTC 0.4		100 C			100015	5.40.24	the little state	
Second Styles In			5146	100.000		1912/02/12/1		- Marchaeler	242 220	
1.0000	CAPITURA X	The Party of		Links Links Science	Transferration.	10.400 - 200	10,179,00.1	1.000	0.00.241	549 B.S.
1.0.00			1000		1.	The law a prove 1		10110	1244	

- 6. Install the EAP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The EAPs that is waiting for Wireless Uplink includes two cases: factory default EAPs and EAPs that has been managed by Omada Controller before.
 - For the factory default EAP, after powering on the device, the EAP will be in Pending (Wireless) status shown in the controller. Go to Access Points > Pending and adopt the EAPs in Pending (Wireless) status.

e •						1. er ar				0 37
1.4.4				41.00			1.17.4			
and A de la seconda de la second								1. 23		
1201000	20.00		1.474	200		at water as	-	7464 00	CARD 1	
0.2.00		interest and the second se	Second Street, or other	1 M 1 M 1	12	10222003280	10-000 00000		15.4	1.1.1.1
a. 1				1 1000420011			663		1. 1. Mar. 19.	2011 (T

After adoption begins, the status of Pending (Wireless) EAP will become Adopting (Wireless) and then Connected (Wireless). It should take roughly 2 minutes to show up Connected (Wireless) within your controller.

For the EAP that has been managed by Omada Controller before and cannot reach the gateway, it goes into Isolated status when it is discovered by controller again. Go to Access Points > Isolated, click .

				w						12 6
a Charlesson and	1998 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -		1.0.0	Contraction of the local distance of the loc	100000000		Acres and			
la and								11111040	and the second	The second
Sector Sector	1000									014
1.01101	Casa Salest	1154211	1.044	1000	THE REPORT	Concerned and	1.496 (1197)	ning da	1,050	- 100 C
14141-014	1.4.4.54.50141		1.10-00	1.000356.000	-	$0.01{\pm}0.0$		444	11-2	4.61
eesse is in								11.1	10 mil 1000	9 HH

The following page will shown, go to **Mesh**, then click to connect the Uplink AP.

	The	lads tises	Gnest	Mestr C	iontigueiatio
		W			
Uplinks					
					lerc
¢ AP Name	¢ Channel	¢ Signal	‡ Нор	¢ Downlink	Action
EA-33-51-A8-22-A0	48	-54 dBm	D	D	Link
		ο οο Λ	total of 1 pag	e(s) Page to:	-0
Downlinks					

Once adoption has finished, your device can be managed by the controller in the same way as a wired EAP. You can click the EAP's name on the Access Points tab to view and configure the mesh parameters of the EAP on the pop-up window. Please refer to <u>View Mesh Information of the EAP</u>.

Tips:

- You can manually select the uplink AP that you want to connect in the uplink EAP list. To build a mesh network with better performance, we recommend that you select the Uplink AP with the strongest signal, least hop and least Downlink AP.
- You can enable **Auto Failover** to make the controller automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. And the controller will automatically select a new uplink AP for the mesh EAPs when the original uplink fails.

3.2 Access Control

Access Control is used to block or allow the clients to access specific subnets. To configure Access Control rules, follow the steps below.

1. Go to Wireless Control > Access Control.



2. Click control rule. to add a new Access Control rule.

Add Access Control R	ule		0
Role Name			
Role Mode	Rlock	Ŧ	
Role Members			
Submets	0.0.0.0/24	Add New	
Fedule Subrets	0.0.0.0/24	Add New	
Apply			

3. Configure the following parameters.

Rule Name	Specify a name for this rule.
Rule Mode	Select the mode for this rule. Block: Select this mode to block clients to access the specific subnets. Allow: Select this mode to allow clients to access the specific subnets.
Rule Members	Specify the member subnets for this rule. Subnets: Enter the subnet that will follow the rule mode in the format X.X.X.X/X and click
	Except Subnets : Enter the excepted subnet in the format X.X.X.X/X and click

4. Click Apply.

 Go to Wireless Settings > Basic Wireless Setting and enable Access Control function of a selected SSID.

3.3 Portal Authentication

Portal authentication enhances the network security by providing authentication service to the clients that just need temporary access to the wireless network. Such clients have to log into a web page to establish verification, after which they will access the network as guests. What's more, you can customize the authentication login page and specify a URL which the newly authenticated clients will be redirected to.

To configure Portal Authentication, go to Wireless Control > Portal and click 🕂 Add a New Portal .

w v	ческо селотори	WINNEL C	antara i	are seringe		a. sanatanin	reemigis 🔄
	COMPLEX CONTROL		nikanan Polisy J	and then the	s i ne souscianten	Service (Service	n (BASAIITICH - 1961)
Note - 1	ana ny sy na s	te ISA the same is the f	d ed verster to to es	n des pille - Perchai de	n 18 f		O Ada See Pek
D	+	Partal Nome	SS D		• Authentication	Тарн	Action
5.0	ni na						

adda Geo Yeand							ö
							- 1
$\mathcal{D}_{\mathrm{ext}} = \mathcal{D}_{\mathrm{ext}}$	ĺ.						
хe	· Term Seator						
$a \in \operatorname{sub-sub-sub-} T_{p} =$	the Autor servation	-					
Ad a shake them		-					
	111300 0						
TTTS Tabler	E						
6 Feel	11						
eter influid.							
Liphenga							3 4 3
Sector rates	0		S-10-0	Page Frend	8201-5	S	
An in the Astron	10000 (C)						
	BORNES .+			2			
1.000							

Then the following window will pop up:

These authentication methods are available: <u>No Authentication</u>, <u>Simple Password</u>, <u>Local User</u>, <u>Voucher</u>, <u>SMS</u>, <u>Facebook</u>, <u>External RADIUS Server</u> and <u>External Portal Server</u>. The following sections introduce how to configure each Portal authentication.

3.3.1 No Authentication

With No Authentication configured, clients can access the network without any authentication.

Follow the steps below to configure No Authentication:

- 1. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

Resardada		
Potel Same		
SSID:	- Please Select-	
Astrendordon Type:	No Authentication	•
Astronological Timedus	111sar	-
	The style and the	
ITT12 Sednet:	⊇ Loater (5)	
Deditect	Thata 🔿	
Rednes URL:		

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select No Authentication.
Authentication Timeout	With Daily Limit disabled, the client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network.
	Options include 1 Hour, 8 Hours, 24 Hours, 7 Days and Custom . Custom allows you to define the time in days, hours and minutes. The default value is one hour.
	With Daily Limit enabled, the client's authentication will expire after the time period you set and the client cannot log in again in the same day.
	Options include 30 Minutes, 1 Hour, 2 Hours, 4 Hours and Custom . Custom allows you to define the time in hours and minutes. The default value is 30 minutes.
Daily Limit	With Daily Limit enabled, after authentication times out, the user cannot get authenticated again in the same day.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.
	With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the Login Page section, configure the login page for the Portal.

14 mg				
Serven	Cost faile Cost		and the total and to	C Hereine
Awayaan Ahaa	(mail) =			T
Acco whee	(1999) (1999) = -		P	
The photo see			- 394 - 595	
Secul			and the second second	
		a presentation and the	Company and and	
t- Maria				
	1			
000000				
			B 92	

Background	Select the background type. Two types are supported: Solid Color and Picture .
Background Color	If Solid Color is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If Picture is selected, click the Choose button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click Confirm .
Logo Picture	Click the Choose button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click Confirm. In addition, you can click I and configure the logo position. The options include Middle, Upper and Lower.

Welcome Information

Specify the welcome information.

In addtion, you can click 🔝 and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Copyright

Specify the copyright information.

In addition, you can click 🔝 and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.



Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service	🔽 Enable	

Button

Click 🔢 and configure the button.

Button Position: Set the position of the login button. The options include Middle, Upper and Lower.

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



4. In the **Advertisement** section, select whether to display advertisement pictures for users and configure the related parameters.

Address and			•
Advertisements	That's		
Пошн Внем хис	Type of The		
A testhement Davides Time		$trianic \in 24$	
Palación en la real		$i \in \text{sum}(i \in D)$	
Allow Users To Stip Allow Users To Stip	_ Crabe		
April			

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow Users To Skip Advertisement . The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
	Supported.

Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the Skip button to skip the advertisement.

5. Click Apply.

3.3.2 Simple Password

With this Simple Password configured, clients are required to enter the correct password to pass the authentication.

Follow the steps below to configure No Simple Password Portal:

- 1. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

Mark IVS		
Pedal Variet		
30481	Provide L	
$\Delta due de due type$	Zingk Derson I	
Detweed		579
Advention to solution	1 Hour	
NULX Initial	🗹 Lases 🕅	
D. do et	🗆 Lawee 🐹	
Dollary Filter		

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select Simple Password.
Password	Set the password for authentication.

Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network.
	Options include 1 Hour, 8 Hours, 24 Hours, 7 Days and Custom . Custom allows you to define the time in days, hours and minutes. The default value is one hour.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.
	With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the Login Page section, configure the login page for the Portal.

التقدي المسرقية	3 Mar	Look Party Table?	- CS Petters
ter seerit in 👘 🚛 🖓			
	8		
Winter Martin	1.5 (() () () () () () () () ()	12-8-12	
Augusta n -		A DESCRIPTION OF THE OWNER OWNER OF THE OWNER OWNER OF THE OWNER OWNER OF THE OWNER	
9.001	2000 (em effers 10)		
weenoone 1		Contraction of the	
entrados II.			
U40 61		and the second se	

Background	Select the background type. Two types are supported: Solid Color and Picture .
Background Color	If Solid Color is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If Picture is selected, click the Choose button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click Confirm .

Logo Picture	Click the Choose button and select a picture from your PC. Drag and s the clipping region to edit the picture and click Confirm . In addtion, you can click I and configure the logo position. The opt include Middle, Upper and Lower .		
	Logo Picture: Logo Positian:	Chucase 🕐 🛪	
Welcome Information		e information. n click 🔝 and select your desir n through the color picker or by e	
	Welgome Information, Welgome Information Celo:	-m	(1.31 characters) > (RGS value)
Copyright		ht information. click 📧 and select your desired to the color picker or by entering th	

Lappin	(5.010) character (\pm
Toppign Lolar	(RGB value)

Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service	🖂 Loable
	Å

Input Box

Click 🔝 and configure the input box.

Select your desired color for the input box through the color picker or by entering the RGB value manually.



Button

Click 🔢 and configure the button.

Button Position: Set the position of the login button. The options include Middle, Upper and Lower.

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



4. In the **Advertisement** section, select whether to display advertisement pictures for users and configure the related parameters.

Anterstein einen d			•
Advertisements	= Loato		
Figure Descured	Type of the		
A two the next Distributions Time		$r = arch \in 2.0$	
$Psime(S_{i}, result(blue_{i}))$		in senie (* 18	
Allow Users To Ship Allow Issues	Drab +		
Appy			

Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow Users To Skip Advertisement . The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the Skip button to skip the advertisement.

5. Click Apply.

3.3.3 Local User

With this Local User configured, clients are required to enter the correct username and password of the login account to pass the authentication. You can create multiple accounts and assign different accounts for different users.

Configure Local User Portal

Follow the steps below to configure Local User Portal:

- 1. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

MARIE INS		
Facal Name		
orp.	Fine - Schel	
Addres testas type	Logil Ups	-
	User Nanagament	
1111 PSC He der all	-1 Torrest (2)	
Ratio	Turkie 🗇	
Selection.		

Configure the following parameters:

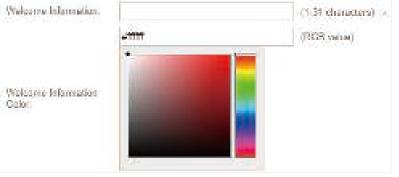
Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select Local User.
User Management	You can click this button to configure user accounts for authentication later. Please refer to <u>Create Local User Accounts</u> .
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.
	With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the Login Page section, configure the login page for the Portal.

design, d	to delution = wider		Denot and Second	Office -
ta laport d'Aller	The state of the s			
app File (a)	1222 0 -		÷.	
Televine Protostan		(1/Televati) in T	12-672	
Nalesana te Kraadise Dagwiging			and the second se	
		Net OPP 11-		
			the same of	
Present Roothin			and the second se	
the Pro-	法			
340	14		and the second second second second	

Background	Select the background type. Two types are supported: Solid Color and
	Picture.

Background Color	If Solid Color is selected, configure your desired background color through the color picker or by entering the RGB value manually.		
Background Picture	If Picture is selected, click the Choose button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click Confirm .		
Logo Picture	Click the Choose button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click Confirm . In addition, you can click 💽 and configure the logo position. The options include Middle , Upper and Lower . Logo Picture: Chross 🕐 🛪		
Welcome Information	Specify the welcome information. In addtion, you can click 💽 and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.		



Copyright

Specify the copyright information.

In addtion, you can click 🔝 and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.

n séringer		(3-300 chaoschos)
	#A7A34C	(RGB value)
Copyright Color	*	

Input Box

Click 🔝 and configure the input box.

Select your desired color for the input box through the color picker or by entering the RGB value manually.

	(RG8 value)
#480000	(6000 Antha)
	#4acbd6

Button

Click 🔢 and configure the button.

Button Position: Set the position of the login button. The options include Middle, Upper and Lower.

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



4. In the **Advertisement** section, select whether to display advertisement pictures for users and configure the related parameters.

data sebaran seb			
Advertisements	= trate		
Реши Биолог	Type of the second second		
A technical Davies Tine		$\alpha := \min \{ i \in \mathcal{D}_i \}$	
Palace Control Island		er samle (* 191	
Allow Users To Skip Allow Users To Skip	_ Crabie		
Appy			

Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow Users To Skip Advertisement . The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the Skip button to skip the advertisement.

5. Click Apply.

Create Local User Accounts

Follow the steps below to create the user accounts for authentication:

 In the Basic Info section on the portal configuration page, click User Management. The management page will appear. Go to the User page and click 4 Greate User.

Pale same				5
Zeed Service Area	Sec. 1			
				en e
i ta an	State and the	and the second	1000	Salar
1.91				

2. The following window will pop up. Configure the required parameters and click Apply.

serna me:		(1-100 letters, digits ar special characters)
assword	ø	(1-100 killers, digits or special character()
whentication Timeout:	2018-12-31	(Famul YYYYAW DD)
AAC Address Binding ype:	No Binding •	
Maximum Users	1	(1-20-68)
Name		(1-90 characters, Optione)
Telephone.		(1-60 duracters, Optonel)
Rate Limit (Download)	Enable	
Rate Limit (Download):		Kbps (0-10040000)
Rate Limit (Upload)	Enable	
Rate Limit (Upload)		Nbps (8-10249000)
Traffic Limit:	Enable	
Traffic Limit		MBylas (5-1048570)

Username	Specify the username. The username should not be the same as any existing one.
Password	Specify the password. Users will be required to enter the username and password when they attempt to access the network.
Authentication Timeout	Specify the authentication timeout for formal users. After timeout, the users need to log in again on the web authentication page to access the network.
MAC Address Binding Type	There are three types of MAC binding: No Binding, Static Binding and Dynamic Binding .
	Static Binding: Specify a MAC address for this user account. Then only the user with the this MAC address can use the username and password to pass the authentication.
	Dynamic Binding: The MAC address of the first user that passes the authentication will be bound. Then only this user can use the username and password to pass the authentication.

Maximum Users	Specify the maximum number of users able to use this account to pass the authencitation.
Name	Specify a name for identification.
Telephone	Specify a telephone number for identification.
Rate Limit (Download)	Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate.
Rate Limit (Upload)	Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate.
Traffic Limit	Select whether to enable traffic limit. With this option enabled, you can specify the total traffic limit for the user. Once the limit is reached, the user can no longer use this account to access the network.

 In the same way, you can add more user accounts. The created user accounts will be displayed in the list. Users can use the username and password of the account to pass the portal authentication.

By default, the account Status is (), which means that the user account is enabled and valid. You can also click this button to disable the user account. The icon will be changed to), which means that the user account is disabled.

P e tes	N. MAR				5
- Dece	l Noole Jan	Sec. 19			
2	5				energy energy and
÷	1 x 10 0 0	Statistical and	and the second second	1000	Same
1.0		2000 B. 10		10 A	E B
-		1988-00-1		40 A	K a
ng ta in					 A more thing by types

Additionally, you can click () Exercises to backup all the user account information into a CSV

file or XLS file and save the file to your PC. If needed, you can click (2) Import Users and select the file to import the account information to the list.

Note:

Using Excel to open the CSV file may cause some numerical format changes, and the number may be displayed incorrectly. If you use Excel to edit the CSV file, please set the cell format as text.

Manage the Guests

On the Guest page, you can view the information of clients that have passed the portal authentication and manage the clients.

hana mini								
	in ch	1.1.1						
Charle Same	1.61	(market)		$(1, \omega_{1}, \omega_{1})_{ij}$	(Dec.es-	1.144	1.4	
the state	199	144	· · · · · · ·	Second and a	1.00	24-2	NAMES AND ADDRESS OF	Parties.
							section in the black of	

You can select an icon to execute the corresponding operation:

¶₀	Disconnect client.
G	Extend the effective time.

Create Operator Accounts

Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL https://Omada Controller Host's IP Address:8043/hotspot (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the portal management page.

Note:

- Make sure the host that is used to enter the portal management page with operator account can visit the Controller host.
- Only the user that log in to the controller with the administrator role can add or remove the operator account for portal management.
- The users who enter the portal management page by operator account can only create local user accounts and vouchers and manage the clients.

Follow the steps below to create Operator account.

1. Go to the **Operator** page.

P. 66 . 85. 851			<u>6</u>
And Nordes Are	Over the		
New Arrival Mills - Sy			 an enco
1 Kara	Sec. Sec.	i esa	Sava (
B.11			

2. Click 🙀 Create Operator and the following window will pop up.

A set a	Open de 1		
Record 6	••••	യ	
N.e.s.	the second		
Ma Pashages	Official A	-	

- 3. Specify the Name, Password and Notes of the Operator account.
- 4. Select **Site Privileges** from the drop-down list (multiple options available) for the Operator account.
- 5. Click **Apply** to create an Operator account. Then other users can use this account to enter the hotspot management page.

3.3.4 Voucher

With Voucher configured, you can distribute the vouchers automatically generated by the Omada Controller to the clients. Clients can use the vouchers to access the network.

Configure Voucher Portal

Follow the steps below to configure Voucher Portal:

- 1. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

Denic Info		
Probable and		
3015	Heat Stard	
N distributes does 1, pr	An and say	,
	Manifest Manager	
LITTES Radiance	🗢 Perioda 🔿	
Fedrec:	The state 😟	
Rednet URL		

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select Voucher.
User Management	You can click this button to configure vouchers for authentication later. Please refer to <u>Create Vouchers</u> .
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.
	With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the Login Page section, configure the login page for the Portal.

the state			
Free-road Scill Vide	1 Deter	Postince Latio	
Teanader as	N		
Less York	les .	0	
New Yorks in	D. 1049233	sp-sna	
Copylet		a second s	
14540	HIPPO STATE AND A DESCRIPTION OF A DESCR	State Andreases	
Same Marker			
HWD-			
Lose II			

Background	Select the background type. Two types Picture .	s are supported: Solid Color and
Background Color	If Solid Color is selected, configure your the color picker or by entering the RGB va	
Background Picture	If Picture is selected, click the Choose your PC. Drag and scale the clipping re Confirm .	
Logo Picture	Click the Choose button and select a pic the clipping region to edit the picture and In addtion, you can click I and configu- include Middle, Upper and Lower . Logo Picture: Omesse (?) R Logo Position: Middle	d click Confirm .
Welcome Information	Specify the welcome information. In addition, you can click i and select welcome information through the color p manually.	
	Welcome Information Color:	(RGR value)

1. Applinght		(0-000 characters)
Conversion L'olar	латазас	(RGB yalkac)
		is option enabled, specif
Terms of Service	✓ Lnable	
Select your desire	ed color for the input box	through the color picker o
	+490b06	(RGB value)
Input Box Color		
	In addition, you calinformation through In addition, you calinformation through Interpretended Enable or disable terms of service in Terms of Service Click I and com Select your desire entering the RGB Input Box Input Box	Copyright Loter Enable or disable Terms of Service. With the terms of service in the following box. Terms of Service Click I and configure the input box. Select your desired color for the input box entering the RGB value manually. Input Box Imput Box

Button

Click 🔢 and configure the button.

Button Position: Set the position of the login button. The options include Middle, Upper and Lower.

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



4. In the **Advertisement** section, select whether to display advertisement pictures for users and configure the related parameters.

data da ancest			•
Advertisements	Thats		
Пецик Внолки	Tylese (11)		
A les forment families Time		an canada 🦿 201	
$Path_{r}(S,rend) \neq btres_{r}(s)$		recent (* 14	

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow Users To Skip Advertisement . The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.

Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the Skip button to skip the advertisement.

5. Click Apply.

Create Vouchers

Follow the steps below to create vouchers for authentication:

1. In the Basic Info section, click Voucher Manager. The voucher management page will appear. Go

to the Voucher page and click $\overline{\mathbf{m}}_{\mathbf{k}}$ Create Vouchers .

Stad Acciler Socials				
The Million			s	and a set of the set o
1 DEV DEVEN	0.200	1.0.2020	17 C	320 B.
11 M P				

2. The following window will pop up. Configure the required parameters and click Apply.

Create Vouchers			Θ
Code Length	6	(6 10)	
Amount	10	(1 500)	
Турн	Single Use 👻		
Dustion	8 hours –		
Rete Limit (Download)	T Lnable		
Rete Limit (Download)		Kbps (0 10240000)	
Refe Limit (Uplose)	T Linable		
Refe Limit (Uplose)		Kbps (0 10240000)	
Traffic Limit	Linable		
Traffic Limit		MBytes (1 1048576)	
Note		(Optional)	
Apply			

Code Length	Specify the length of the voucher codes to be created.
Amount	Enter the voucher amount to be generated.
Туре	Select Single Use or Multi Use.
	Single Use means one voucher can only be distributed to one client. Multi Use means one voucher can be distributed to several clients, who can use the same voucher to access the network at the same time.
	If you select Multi Use, enter the value of Max Users . When the number of clients who are connected to the network with the same voucher reaches the value, no more clients can use this voucher to access the network.
Duration	Select the period of validity of the Voucher.
	The options include 8 hours , 2 days and User-defined . The period of valid of the voucher is reckoned from the time when it is used for the first time.
Rate Limit (Download)	Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate.
Rate Limit (Upload)	Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate.
Traffic Limit	Specify the total traffic limit for one voucher. Once the limit is reached, the client can no longer access the network using the voucher.
Notes	Enter a description for the Voucher (optional).

3. The Vouchers will be generated and displayed on the page.

100 A						
					AD 100 - AT 100	4
	1.000	Contraction of the	1 Court	Tion III.	7.00	See.
	1.00	5474.445		(here)	Name of street	E 🛃
	10 A 10 A 10 A	40.0224.00		1.00		6.0
		1111 A 114		10.74	Series and a	F
	0.10	414 54 54 1		Ball N	Salating at the second	-
	+* %	and a second		1000		de su
		5.000 CO.		100.00	Same and the set	E
2		101515-010		14737	many services	0.45
	100	54.00 auto		1.1.1	Same and an	
				5.1.1	Sec. of a	a. 19
	1. Sec. 1.	182 4 184		44716	20000000	6.

Click is to print a single voucher; click is Print Scienced Vouchers, to print your selected vouchers; click is Print All Unused Vouchers to print all unused vouchers.

WHERE WE	1.11.23	Value Are St.	Note and
131720	202206	393597	SCOUDE
William .		Villa ba St	A.1.67
637139	463676	17,2707	457433
Andrea Maria	1.11.1.25 C.3.10 (10)		
385855	921414		

- 5. Distribute the vouchers to clients, and then they can use the codes to pass authentication.
- 6. When the vouchers are invalid, you can click 🔟 to delete the Voucher or click 🛄 Delete to delete the selected vouchers.

Manage the Guests

On the Guest page, you can view the information of clients that have passed the portal authentication and manage the clients.

Dening Street								
		100.2						
110	000000							
Starts Jam	194	(market)	1.4	the set of the	Charles .	and the set	14	-
there are a set	1.14	144	4.11.	Second and a	1.04	54.2	NAME ADDRESS OF	Parita.
5 - 6 - 6 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1							STREET, DOCUMENTS	200

You can select an icon to execute the corresponding operation:

¶₀	Restrict the client to access the network.
G	Extend the effective time.

Create Operator Accounts

Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL https://Omada Controller Host's IP Address:8043/hotspot (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the portal management page.

Note:

- Make sure the host that is used to enter the portal management page with operator account can visit the Controller host.
- Only the user that log in to the controller with the administrator role can add or remove the operator account for portal management.
- The users who enter the portal management page by operator account can only create local user accounts and vouchers and manage the clients.

Follow the steps below to create Operator account.

1. Go to the **Operator** page.

P _{alinia} second Sect North An ∎Sec	÷.		5
The second se			t, an our
1 mars	Net with	i anus	Save
B 11			

2. Click 🖕 Create Operator and the following window will pop up.

Name	Open de la		
M. room of		ø	
Nation 1	for some		
Ma Pashque	Ole a A		

- 3. Specify the Name, Password and Notes of the Operator account.
- 4. Select **Site Privileges** from the drop-down list (multiple options available) for the Operator account.
- 5. Click **Apply** to create an Operator account. Then other users can use this account to enter the hotspot administrative system.

3.3.5 SMS

With SMS portal configured, client can get verification codes using their mobile phones and enter the received codes to pass the authentication.

Follow the steps below to configure SMS Portal:

- 1. Go to <u>www.twilio.com/try-twilio</u> and get a Twilio account. Buy the Twilio service for SMS. Then get the account information, including ACCOUNT SID, AUTH TOKEN and Phone number.
- 2. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 3. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

-		
Priol Sec.		
5 H	- Second Marcol	
$\lambda \dim \operatorname{sum} \nabla_{\mathcal{G}} n$		
	ana Bara sakata tana santakan I	
240.2.5		
A De Las		
Films Sector		$d_{\rm eff} \sim 100~{\rm eV}^{-1}$
Maximum 1 how		$(1,1) \in \mathbb{R}^{n} \setminus \{0,1\}$
$\Gamma_{\rm c}$ on Δm is the		the convert
$(1,1,\dots,1,n) \in \mathbb{R}^{n}$		
NTN foil or	Firms 3:	
Param	L hale 3	
De las 178		

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select SMS.
Twilio SID	Enter the Account SID for Twilio API Credentials.
Auth Token	Enter the Authentication Token for Twilio API Credentials.
Phone Number	Enter the phone number that is used to send verification messages to the clients.
Maximum Users	A telephone can get several codes via messages one by one, and different clients can use different codes to pass the authentication. However, the number of clients that is allowed to be authenticated using the same telephone at the same time has a upper limit. Specify the upper limit in this field.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network. Options include 1 Hour, 8 Hours, 24 Hours, 7 Days and Custom . Custom allows you to define the time in days, hours and minutes. The default value is one hour.
Preset Country Code	Set the default country code that will be filled automatically on the authentication page.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

4. In the Login Page section, configure the login page for the Portal.

Aug inge				
diagonal.	- Secondaria Provid		Proteiner & edit.	C.H. der
diplops of Salari	1000			
ing Print	1		÷	
Other (Index)		(10) Annothis (12)	1.24	
P-4			The Owner of the	
		1.1.1.1.1.1.1.2.2.	110 mm	
			Particular of the second	
Press Cross	-			
field Cox.	10.			
202	1 3			

Background	Select the background type. Two types are supported: Solid Color and Picture .
Background Color	If Solid Color is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If Picture is selected, click the Choose button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click Confirm .
Logo Picture	Click the Choose button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click Confirm. In addition, you can click 💽 and configure the logo position. The options include Middle, Upper and Lower. Logo Picture: Choose 🕐 🛪 Logo Picture: Middle 🔭

Welcome Information

Specify the welcome information.

In addtion, you can click 🔝 and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Copyright

Specify the copyright information.

In addition, you can click 🔝 and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.



Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service	🔽 Enable	

Input Box

Click 🔝 and configure the input box.

Select your desired color for the input box through the color picker or by entering the RGB value manually.

Input Bloc	田	
	#4acbd6	(RG8 value)
Input Box Color		

Button

Click 🔢 and configure the button.

Button Position: Set the position of the login button. The options include Middle, Upper and Lower.

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



5. In the **Advertisement** section, select whether to display advertisement pictures for users and configure the related parameters.

dates to ensert			۰
Advertisements	= mate		
Picure Descuse:	Type of 10.00		
Δ is a linear of Δ with a Table 1 Table 1		α such ≤ 2.0	
$P_{s}(u_{r}) \leq u_{r}(u_{r}) + d_{r}(u_{r})$		science (* 13)	

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow Users To Skip Advertisement . The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the Skip button to skip the advertisement.

6. Click Apply.

For more details about how to configure SMS Portal, you can go to <u>https://www.tp-link.com/en/</u> <u>configuration-guides.html</u> and download the configuration guide for SMS Portal.

3.3.6 Facebook

With Facebook Portal configured, when clients connect to your Wi-Fi, they will be redirected to your Facebook page. To access the internet, clients need to pass the authentication on the page.

Note:

Omada Controller will automatically create Free Authentication Policy entries for the Facebook Portal. You don't need to create them manually.

Follow the steps below to configure Facebook Portal:

- 1. Go to <u>www.facebook.com</u> and get a Facebook account. Create your Facebook page according to your needs.
- 2. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 3. Go back to the Portal configuration page. In the **Basic Info** section, complete the settings for the portal authentication.

WOLK I NO				x
Data Norm				
XXII:	i ne z Seteri			
As the set of the $1_{\rm A}$ pc	Final fields	-		
Latakash Kaya Canigaraha	Configuration -			
Landowic Chercher Landow	Here.			
IIII IE2 Kalin J	Emailair 👔			

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select Facebook.
Facebook Page Configuration	Click this button to specify the Facebook Page.
Facebook Checkin Location	If the Facebook page is successfully got by the Omada Controller, the name of the Facebook page will be displayed here.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

For more details about how to configure Facebook Portal, you can go to <u>https://www.tp-link.com/</u> <u>en/configuration-guides.html</u> and download the configuration guide for Facebook Portal.

3.3.7 External RADIUS Server

If you have a RADIUS server, you can configure External RADIUS Server Portal. With this type of portal, you can get two types of portal customization: Local Web Portal and External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the controller. The External Web Portal is provided by external portal server.

Note:

Omada Controller will automatically create Free Authentication Policy entries for the External RADIUS Portal.

Follow the steps below to configure External RADIUS Server Portal:

- 1. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

(Dimension)				
Para New				
22.2	- Nerra Select-			
Julianshaller Tree	Element Red US Gener	25		
Jakastaler Teaste	(ik)s	5		
ENERGIA Server Pr				
NO SAH	7,12		period.	
PACKS Network		44		
And endedon North	ter.			
627 T	18.00			
Pd7 - 5 Geven office	E) 20 SF			
Annual States of Party				
Array of Array Part	80		(1490.24)	
and a state of the second second		- (1)		
Sala in Operan	the case of the ca			
lak bally-detron	34		0.60475	
e lingthe internet	weither 70 ki	- 22		
+ TOK Dealership	Dette ()			
1.46	Date 1			
8 - 🗰 (- 1910)				

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select External RADIUS Server.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network.
	Options inclde 1 Hour, 8 Hours, 24 Hours, 7 Days, Custom . Custom allows you to define the time in days, hours, and minutes. The default value is one hour.
RADIUS Server IP	Enter the IP address of the RADIUS server.
RADIUS Port	Enter the port number you have set on the RADIUS server.
RADIUS Password	Enter the password you have set on the RADIUS server.
Authentication Mode	Select the authentication protocol for the RADIUS server. Two authentication protocols are available: PAP and CHAP .

NAS ID	Configure a Network Access Server Identifier (NAS ID) using 1 to 64 characters on the portal. The NAS ID is sent to the RADIUS server by the controller through an authentication request packet. With the NAS ID which classifies users to different groups, the RADIUS server can send a customized authentication response. The default value is TP-Link .
RADIUS Accounting	Enable or disable RADIUS Accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server. The default port number is 1813.
Accounting Server Password	Enter the shared secret key of the accounting server.
Interim Update	With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled.
	Enter the appropriate duration between updates for EAPs in Interim Update Interval.
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.
Portal Customization	Select Local Web Portal or External Web Portal.
	Local Web Portal : If this option is selected, refer to step 3 to configure the login page and step 4 to configure the advertisement.
	External Web Portal: If this option is selected, follow the steps below.
	1. Configure the external RADIUS server.
	Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field.
	Note that you should update the External Web Portal after you upgrade your controller with old version to version 3.1.4 or above. Otherwise, the External Web Portal will not take effect.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.
	With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
	It is disabled by default.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. Local Web Portal is configured, configure the login page for the Portal in the Login Page section.

-19 1100				
dedges id	:- Velution = within		Generation Second	Other
talge strate	Distantia (P.			
app Total and	10-11 (P =		÷	
Paginana in Kraatan		11/ Information Trans	C-arg	
Series			and the second se	
		nee comente -	4 (mm +	
			i	
The state of the second			and the second se	
the Part	it.			
340	14			
				1.45

Background	Select the background type. Two types Picture .	are supported: Solid Color an
Background Color	If Solid Color is selected, configure your d the color picker or by entering the RGB val	<u> </u>
Background Picture	If Picture is selected, click the Choose by your PC. Drag and scale the clipping reg Confirm .	
Logo Picture	Click the Choose button and select a pictor the clipping region to edit the picture and configure include Middle , Upper and Lower .	click Confirm.
Welcome Information	Specify the welcome information. In addtion, you can click 💽 and select welcome information through the color pic manually.	
	Welcome Information	(3.31 characters) >< (RGR value)

nybiti ðu		(South characters)
Copyrgin L'olar	MATABAC	(RGB value)
		is option enabled, specify
Terms of Service	C Lnable	
Select your desire	ed color for the input box t	through the color picker o
Input Box	+4acbd6	(RG8 value)
Input Box-Color		
	In addition, you calinformation through In addition, you calinformation through Interpretended Enable or disable terms of service in Terms of Service Click I and com Select your desire entering the RGB Input Box Input Box	Copyright Loter Enable or disable Terms of Service. With the terms of service in the following box. Terms of Service Click I and configure the input box. Select your desired color for the input box fentering the RGB value manually. Input Box Input Box

Button

Click 🔢 and configure the button.

Button Position: Set the position of the login button. The options include Middle, Upper and Lower.

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



4. If Local Web Portal is configured, select whether to display advertisement pictures for users and configure the related parameters in the Advertisement section, .

data da ancest			•
Advertisements	Thats		
Пецик Внолки	Tylese (11)		
A les frence l'Andres Time		an canada 🦿 201	
$P_{0}(\mathbf{n} \cdot 0) = (0, \mathbf{n} \cdot \mathbf{n}) + (0, \mathbf{n} \cdot \mathbf{n})$		recent (* 14	

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow Users To Skip Advertisement . The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.

Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the Skip button to skip the advertisement.

5. Click Apply.

3.3.8 External Portal Server

The option of External Portal Server is designed for the developers. They can customized their own authentication type according to the interface provided by Omada Controller, e.g. message authentication and WeChat authentication etc.

- 1. Go to Wireless Settings > Basic Wireless Settings and create an SSID for the Portal.
- 2. Go back to the Portal configuration page. In the **Basic Info** section, complete the settings for the portal authentication.

Point the			
NRC .	- THER SHEEP		
AJDEMENDO (OR		+	
Long Converse			
11-17, 14040	- mar (1)		
No.			

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select External Portal Server.
External Portal Server	Enter the complete authentication URL that redirect to an external portal server, for example: http://192.168.0.147:8880/portal/index.php or http://192.168.0.147/ portal/index.html
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

3. Click Apply.

3.4 Free Authentication Policy

Free Authentication Policy allows some specified clients to access the network resources without authentication. Follow the steps below to add free authentication policy.

1. Go to Wireless Control > Free Authentication Policy.



2. Click 🚭 🚈 and the following window will pop up.

лаанажу				ō
Pully Roma				
No No	P Machaeler	-		
$X_{\rm eff} \sim 10~{\rm Mm}~{\rm pc}$		2	E(n, n, n)	
Colorised Stronge		2	Ephanic	
$X_{\rm curr} \sim 10731$		$\leq \eta \ln r \cdot 1$		
Dividentian Pert		Çiyine di		
2. de 1	_ LNOF			
- Kapla				

3. Configure the following parameters. When all conditions are met, the client can access the network without authentication.

Policy Name	Specify a name for the policy.
Match Mode	Select the match mode for the policy. Two options are provided:
	URL : With this option selected, configure an URL that is allowed to be visited by the clients without authentication.
	IP-MAC Based : With this option selected, configure Source IP Range, Destination IP Range, Source MAC and Destination MAC to specify the specific clients and service that will follow the Free Authentication feature.
URL	Set the URL.
Source IP Range	Set the Source IP Range with the subnet and mask length of the clients.
Destination IP Range	Set the Destination IP Range with the subnet and mask length of the server.
Source MAC	Set the MAC address of client.
Destination Port	Enter the port the service uses.
Status	Check the box to enable the policy.

4. Click **Apply** and the policy is successfully added.

3.5 MAC Filter

MAC filter can be used to allow or block the listed clients to access the network. Thereby it can effectively control the client's access to the wireless network.

Follow the steps below to configure MAC Filter.

1. Go to Wireless Control > MAC Filter to add MAC Filter group and group members.

ланын жалар	WITH BUD COPIES	жана села турк	(3161,91343)	Constant Settings	
ANNO CONTR	- stat i se sumerosant - sis	(No. 1 MAT AND	iner costos ation conecting	SKARCING ASSociation	0.00
				0.445	Grau
	t waar dan e	anguranan		Action	
Mer-mild in					

1) Click 🗿 🐝 🕬 🔹 and specify a name for the group.

And a comp	0
MR LIPPIN TO	
4.6	
100	

2) Click Apply and the group will be successfully added as shown below.

			🔘 Adda oo
	2 MBC Ltd. Contoperators		And one
	Orcupi		E 🛯
924C Address C.	8 174	Comp Mandatan 👩 Papar Diang D	Nonise 🕘 Antis Carga Marine
n	M 817 Bald a	Description	And and
No Chates,			
		Asral	cf f or gall() = spin to 1

3) Click 🔂 Add a Group Member and enter a MAC address in the format as shown below.

алы ал тыр кетере		0
LINE COLOR	25.000.001101010	
Los de l	Uva 1	
Apple		

4) Click **Apply** to add the MAC address into the MAC filter group.

			🖨 Acda Gro
	c while Lieb doinguistion		Action
	$\Omega_{\rm c} \approx 10^{-11}$		Øi
MAC Advice to	0 0	Hang Marakan - 🙆 Laga Laka	, Menel Santo 👩 Zelidor Henrice Marchen
12	Mixe Address	Design proof	A2360
I	AN RECOURSEE FE	- a 1	3 i
		$\omega_{\rm c} = 1 - 1 - \infty$	A field of the So
		an a gira sa Aki	dal Lyne St. Pagerss 📃 🖻

2. You can add more groups or members according to your need.

Note:

You can click Department to export the group members to a excel file and save the file on your PC. If needed, you can also click Department to import the group members to the Omada Controller.

3. Go to Wireless Control > MAC Filter Association to associate the added MAC Filter group with SSID.

With the co	Sidens. Wester	- Gambadi	Shi Adimy	Court Survey	- Controller?	édine.
Annez	Salat Polat - Free A	Bandarah Mataw	MACCENTER DATE: N	la Assesso	Zahadaka – Ashadaka	Azeria altaren Caris
RAC Fishing	🔽 the Ma					
Apply						
уштны в	(H) Datiel	-				
D	• SSID Name	Dand	MAO Filiter No	m+	Action	Setting
•	2.3121	24 MID	No. 4	-	Allow -	$-\lambda_{\rm eff} \lambda_{\rm eff}$
			1.1	(-1)	${\rm Subt}(x) = {\rm Subt}(x) = {\rm Subt}(x)$	(27)

- 1) Check the box and click Apply to enable MAC Filtering function.
- 2) Select a band frequency (2.4GHz or 5GHz) and a WLAN group.
- 3) In the MAC Filter Name column of the specified SSID, select a MAC Filter group in the dropdown list. Then select Allow/Deny in the Action column to allow/deny the clients in the MAC Filter group to access the network.
- 4) Click Apply in the Setting column.

3.6 Scheduler

With the Scheduler, the EAPs or its' wireless network can automatically turn on or off at the time you set. For example, you can use this feature to schedule the radio to operate only during the office working time in order to achieve security goals and reduce power consumption. You can also use the Scheduler to make clients can only access the wireless network during the time period you set in the day.

Follow the steps below to configure Scheduler.

1. Go to Wireless Control > Scheduler.



1) Click 🚹 Md a Fronte and specify a name for the profile.

4112.0010		¢.
Part of Second	Le la l	
the state		

2) Click Apply and the profile will be added.

				(D
	i	Protes Cambguration		A12.04
		Polis 1		
				Q
6	Day of them	start Time	and firms	Actor
10.0000				

3) Click 🕒 Add an Item and configure the parameters to specify a period of time.

data an Irea	0
Day Mode	& Weeking $-\odot$ Weekind $-\odot$ Decydig $-\odot$ Custom
	$\nabla_{j} \operatorname{New} [\overline{p}] \operatorname{La}_{n} = \overline{p} \operatorname{New} [\overline{p}] \operatorname{La}_{n} = \overline{p} \operatorname{La}_{n} = \overline{p} \operatorname{La}_{n} = \overline{p} \operatorname{New}$
• •	I all des Al factors
Start Free	<u>Б.) т</u> 3. т
Loc Loca	<u>Б.) т</u> 3. т
Apple	

- 4) Click Apply and the profile is successfully added in the list.
- 2. Go to Wireless Control > Scheduler Association.

Wheelers, Ard	-r. *	index. And of	Alt Kilon	e Chinik	Varies, Cambrid	ka Astrop
Sec. 22.15	alad Parist -	sa Autoritation P	ing [1990] et a	MACE IN A 2014	inn Steine <mark>Nink</mark>	la Astanta da Asta
Schedule t	= Loal	ч				
An odistor Note	Aller 1	eid sith SOID				
$-\delta_{\rm SF} \delta_{\rm T}$						
_						
2.6736/ 3.004	Default		-			
D C	GD Name	Dansi	Γττ.	dia Nome	Action	Setting
•	2011 PL	24305	Maria	-	$ G_{\mathcal{M}}(f_{\mathcal{M}}(x, \theta)) = 0$	$-\mathcal{L}_{\mathbf{p}}(d_{\mathbf{p}})$
				$w_{i} \in \{1,2\}$	o shahifi payoo 1	and a state

- 1) Check the box to enable Scheduler function.
- 2) Select Associated with SSID (the profile will be applied to the specific SSID on all the EAPs) or Associated with AP (the profile will be applied to all SSIDs on the specific EAP). Then click Apply.
- 3) Select a band frequency (2.GHz or 5GHz) and a WLAN group.
- 4) In the Profile Name column of the specified SSID or AP, select a profile you added before in the drop-down list. Select Radio Off/Radio On to turn off or on the wireless network during the time interval set for the profile.
- 5) Click Apply in the Setting column.

3.7 QoS

The Omada Controller software allows you to configure the quality of service (QoS) on the EAP for optimal throughput and performance when handling differentiated wireless traffic, such as Voice-over-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the EAP, you should set parameters on the transmission queues for different types of wireless traffic and specify minimum and maximum wait times (through contention windows) for transmission. In normal use, we recommend that you keep the default values for the EAPs and station EDCA (Enhanced Distributed Channel Access).

Follow the steps below to configure QoS.

1. Go to Wireless Control > QoS.

Wire cav Solling a	Wireless Cantool	Sile Seluisys	Claud Activate	Controler Skillings 💦 🖉
Avecus Control 1 Pe	stall. Prov Automication Policy	section theorem	a Asvedicijan – Skrivetujur	Schedaler Association 605
V 2014-00 (9120)				
Percerano Default Values:	Renore			
We shall be the WMM ($= \frac{1}{2}$	<u>/</u> Crette			
References by work	_ Cnitle			
Unichedulet Automatic Provin Xura Balance	<u>/</u> Cratte			
We Mac w Hard Metalli				v
Station PO7A Pasander				~
Apple				

2. Enable or disable the following features.

Wi-Fi Multimedia (WMM)	By default enabled. With WMM enabled, the EAPs have the QoS function to guarantee the high priority of the transmission of audio and video packets.
	If 802.11n only mode is selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz), the WMM should be enabled. If WMM is disabled, the 802.11n only mode cannot be selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz).
No Acknowledgment	By default disabled. You can enable this function to specify that the EAPs should not acknowledge frames with Qos No Ack. Acknowledgeable is recommended if VoIP phones access the network through the EAP
Unscheduled Automatic Power Save Delivery	By default enabled. As a power management method, it can greatly improve the energy-saving capacity of clients.

3. Click **AP EDCA Parameters** and the following page will appear. AP EDCA parameters affect traffic flowing from the EAP to the client station. We recommend that you use the defaults.

196 A Paramatan.						
Dava	An estados - 1 De es	Norman Ve	Contentro altern	^a en cuit Par		Pours deux
Ista Weset		2	-	2	-	P.0
$1 \leq d_{\rm eff} < $	•		-	10.		100.5
$(\alpha,\beta,\alpha,\beta,\alpha)$		· .		1		
Vir. Mergine (- i -	620	-	4

Queue	Queue displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters.
	Data 0 (Voice) —Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
	Data 1 (Video) —High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
	Data 2 (Best Effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
	Data 3 (Background) —Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
Arbitration Inter- Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values for Arbitration Inter-Frame Space are from 0 to 15.
Minimum Contention Window	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.
	This value can not be higher than the value for the Maximum Contention Window .
Maximum Contention Window	The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.
	This value must be higher than the value for the Minimum Contention Window .

Maximum Burst

Maximum Burst specifies the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

4. Click **Station EDCA Parameters** and the following page will appear. Station EDCA parameters affect traffic flowing from the client station to the EAP. We recommend that you use the defaults.

а, как	arana sa kan tiyata 1995	аналык таларт та Иналта	алар сана на селанот разости	10.2108
$h \in H^{1}_{1}(m,m)$		1	· · ·	1.00
Level (1992)	2		P	1.00
San 1,5 m Minis	<u> </u>	E -	62	•
Ada Sharaha santi	1	p -	822	

Queue displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters.
Data 0 (Voice) —Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
Data 1 (Video) —High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
Data 2 (Best Effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
Data 3 (Background) —Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
A wait time for data frames. The wait time is measured in slots. Valid values for Arbitration Inter-Frame Space are from 0 to 15.
A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value can not be higher than the value for the Maximum Contention Window .
The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.
This value must be higher than the value for the Minimum Contention Window.
The TXOP Limit is a station EDCA parameter and only applies to traffic flowing from the client station to the EAP. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME client station has the right to initiate transmissions onto the wireless medium (WM) towards the EAP. The valid values are multiples of 32 between 0 and 8192.

5. Click Apply.

3.8 Site Settings

You can configure the site-specific settings on the **Site Settings** page. To switch sites, select a different site from the **Sites** drop-down menu at the top of any screen.



3.8.1 LED

You can change the LED light status on the EAPs on the page Site Settings > LED.

Wile cay Sollingy	Mindoary Control	Sile Settings	Cloud Acousty	Controler Settings 💦 💌
	LCC Device Ac	ovent - Repuel Schedule	Log Solungs – Saloh Up	girde 15511 Stanayorien, VLAN
	-			
T G				

By default, the LED status is , which means that the LED lights of all the EAPs on the site are on. You can click this button to change the LED light status. The icon will be changed to , which means that all the LED lights are off.

3.8.2 Device Account

When the EAPs are adopted at the first time, their username and password will become the same as those of the Omada Controller which are specified at Basic Configurations. You can specify a new username and password for the adopted EAPs in batches.

Follow the steps below to change the username and password of EAPs.

1. Go to Site Settings > Device Account.

Wine a web Section as	We show a Constant	Rate Rollingy.	Coult Survey.	Conduction	Selline . 🛛 💆
	100 Damas A	and Arnol Mitadala	$\log \Delta d = p - \Delta d d$	Opposite SSR	An approx. 9120
Ourner: Dearnaise	tánia.				
Current Fastroord:		65			
New Osemanic					
New Prenadst		65			
- Arets					

- 2. Specify a new username and password for the EAPs.
- 3. Click Apply.

Note:

- The new account will be applied to EAPs but not the Omada Controller. To change the Omada Controller's username and password, please refer to <u>User Account</u>.
- Device account can be only viewed and changed when you log in to the controller as the administrator. While the operator and observer accounts do not have the permission.

3.8.3 Reboot Schedule

You can reboot all the EAPs in the network periodically as needed. Follow the steps below to configure Reboot Schedule.

1. Go to Site Settings > Reboot Schedule.

Weakton Sallings	Witchus Dontrol	Site Settings	Cloud Actus	Controller Soldings	v
	LED – Device Av	era i Rekol Schedale	Ley Sellingo – Balen Upy	aso 1011 Menagene	NVLV.
Galerae Maleratoria	Final de				
n mga Masia	п.,				
Salar, Inc.	<u>- 6</u> 2	-			
補助					

- 2. Check the box to enable the function.
- 3. Choose **Daily**, **Weekly** or **Monthly** in the **Timing Mode** drop-down list and set a specific time to reboot the EAPs.
- 4. Click Apply.

3.8.4 Log Settings

Follow the steps below to choose the way to receive system logs.

1. Go to Site Settings > Log Setting.



2. Check the box to choose the ways to receive system logs and click **Apply**. Two ways are available: **Auto Mail Feature** and **Server**. You can choose more than one way.

Note:

The logs and alerts of the controller with version 3.0.5 or below will be discarded after the controller is upgraded to version 3.1.4 or above.

Auto Mail Feature

If Auto Mail Feature is enabled, system logs will be sent to a specified mailbox. Check the box to enable the feature and configure the parameters.

2 Anto Malternation 🍈		
Kasherat Addisory		
SMDF Station		
e e	<u>x</u>)	79-00-04
>>	Facility	
Auffrag sale e	Facility	
1 Martine and 1		
Para weet	ø	
Standar Calcinets		
TIMEMORE	A Tatalon The C Tellod Three	
Foster Time	X - 0 - 11223	

Receiver Address	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address or domain name of the SMTP server.
Port	The SMTP server uses port 25 as default. If SSL is enabled, the port number will automatically change to 465.
SSL	You can check the box to enable SSL (Security Socket Layer) to enhance secure communications over the internet.
Authentication	You can check the box to enable mail server authentication. Enter the sender's mail account name and password.

Username	Enter the sender's mail account name.
Password	Enter the sender's mail password.
Sender Address	Enter the sender's E-mail address.
Time Mode	Select Time Mode. System logs can be sent at specific time or time interval.
Fixation Time	If you select Fixation Time, specify a fixed time to send the system log mails. For example, 08:30 indicates that the mail will be sent at 8:30 am everyday.
Period Time	If you select Period Time, specify a period time to regularly send the system log mail. For example, 6 indicates that the mail will be sent every six hours.

Server

If Server is enabled, system logs will be sent to a server. Check the box to enable the feature and configure the parameters.

	On Log Server Product Syseem Log Server Prod Syseem Log Server Prod State More Ollero Decall Log:
System Log Server IP	Enter the IP address of the server.
System Log Server Port	Enter the port of the server.
More Client Detail Log	With the option enabled, the logs of clients will be sent to the server.

3.8.5 Batch Upgrade

You can upgrade your EAPs of the same model in batches using Batch Upgrade. Two options are available for upgrading: upgrade online and upgrade manually.

Upgrade Online

With Cloud Access enabled, the latest firmware for the EAPs can be detected by the controller automatically. And you can upgrade the EAPs online. Thus you need not to save the firmware files locally in advance.

Follow the steps below to upgrade the EAPs online according to their model.

- 1. Go to **Cloud Access**. Click the button to enable Cloud Access and log in and bind with your TP-Link ID. For more details about Cloud Access, please refer to <u>Omada Cloud Service</u>.
- 2. Go to **Site Settings > Batch Upgrade**. The device model, amount, current firmware and available firmware will appear on the **Firmware list**.

_		TT Delle Storter Geoch	Serence of Sectors Description	301 [satisfiered a
innware List				S. Overseeder
Denve Wedel	Connected	Periet Futtoes	As elable Ferrie ate	. ector
541225(50)33	39	150 Bad 201901 (17a), 62.61	2013 844 3613633 843 32612 👩	4.4
ENFORE CREAKER	199	170 Build Printing a Store	lists of m	A 4.

3. Click \pm in the Action column to upgrade the device.

After upgrading, the device will reboot automatically.

Tips:

- You can click **The Internet of the latest firmware is available.**
- You can click in the Available Firmware column to view the release note of the firmware, which can help you know the new features or improvements of this firmware.

Upgrade Manually

The latest firmware files can be downloaded in the download center of TP-Link Website. Then you can upgrade the EAPs manually.

Follow the steps below to upgrade the EAPs manually according to their model.

1. Visit <u>http://www.tp-link.com/en/support/download/</u> to download the latest firmware file of the corresponding model.

2. Go to Site Settings > Batch Upgrade.

		The Device Ansatz Report	Severite organization for	SSI [waracemed/#)
innwere List				
				De Destandare
Deerce Violat	Connected	Conset Pureven	As adable Provisate	Action
E41725(50)30	35	2.5.0 Build 2013.0 10 (w), 62.01	200 Brie Strateau Roi 54612 💼	1.4
ande states est	193	CTED BORDON BALSING	Lines day.	A. 1.

3. Click 🙏 in the Action column to upgrade the device.

Upload Firmware			0
Upgrade File:	Please select a file	Drowse Upgrade	

- 4. Click **Browse** to locate and choose the proper firmware file for the model.
- 5. Click **Upgrade** to upgrade the device.

After upgrading, the device will reboot automatically.

Note:

- The EAP cannot be upgraded manually when you access the controller via Omada Cloud.
- To avoid damage, please do not turn off the device while upgrading.

3.8.6 SSH

SSH is a protocol working in application layer and transport layer. It can provide a secure, remote connection to a device. After enabling SSH Login here, you can log in to the EAPs via SSH.

1. Go to Site Setting > SSH. Enter the port number of the SSH server.

Wickes Sollings	I	Wildow Centrel	Site Settings	Cloud Actua	Caribalka Salilinga	v.
		LED Device Ave	surt - Rebeat Schedule	Ley Sellinge – Balen G	pyrasis CSII Munaparisat	VDO
55 - Mayor Mari	\mathcal{F}		117 1020-400080			
22 Loga	-1					
$\{x_i\}_{i \in \mathcal{A}}$. Such that the set $\{x_i\}_{i \in \mathcal{A}}$	I					
Apply						

- Check the box to enable SSH Login. If you want to log in to the EAP from a different subnet via SSH, enable Layer-3 Accessibility.
- 3. Click Apply.

3.8.7 Management VLAN

Management VLAN provides a safer way for you to manage the EAP. With Management VLAN enabled, only the hosts in the management VLAN can manage the EAP. Since most hosts cannot process VLAN TAGs, connect the management host to the network via a switch, and set up correct VLAN settings for the switches on the network to ensure the communication between the host and the EAP in the management VLAN.

Follow the steps below to configure Management VLAN.

1. Go to Site Setting > Management VLAN. Check the box to enable Management VLAN.

	ingv 🐣 👘
LCC Device Account Report Schedule Log Schlings Salch Upginde SSH Ma	ngorikit, VLAN
Management & CM 🔰 En Ma 🔞	
Kanagement & AND 1 1-10-23	
40(B)	

- 2. Specify the Management VLAN ID. The default VLAN ID is 1.
- 3. Click Apply.

4 Omada Cloud Service

TP-Link Omada Cloud Service provides a better way to realize remote management. With Cloud Access enabled on the controller and a TP-Link ID bound with your controller, and you can easily monitor and manage your wireless network. To ensure that your EAPs stay new and get better over time, the Omada Cloud will notify you when a newer firmware upgrade is available. Surely you can also manage multiple Omada Controllers with a single TP-Link ID.

Follow the steps below to configure Cloud Access and access the controller via Omada Cloud:

- 1. Configure the Cloud Access
- 2. Manage the Controller via Omada Cloud

4.1 Configure the Cloud Access

4.1.1 Enable Cloud Access

You can configure the controller via Omada Cloud only when Cloud Access is enabled on the controller and you have been added as a Cloud User.

On the page **Cloud Access** you can configure Cloud Access. Click the button to enable the **Cloud Access**. The Cloud Access status is _____, which means that the Cloud Access is enabled.

Wild-cay Schige	Mickey Control	SHC Skillings	Cloud Access	Controller Scillings	×.
Cloud Access					
Charl Provide	•				

4.1.2 Manage the Cloud Users

To configure and manage Omada Controller through Cloud service, you need to have a TP-Link ID, and bind your TP-Link ID to the controller. Then you can remotely access the controller as a Cloud User.

Note:

To register a TP-Link ID and bind it to your controller, make sure that the controller host can access the internet.

Register a TP-Link ID

In the Quick Setup process, you can register a TP-Link ID and bind it to your controller. If you have skipped the registration during the Quick Setup process, you can go to **Cloud Access**. Click **Register Now** and follow the instructions to register a TP-Link ID.

Mic cay Sullings	Whickeys Control	Sile Sellingu	Cloud Access	Controller Schlinge	×
Cloud Access					
October 2 Courses	1 0				
Logic and blocky and P. I	leb III				
Crait					
Prozent		4,5			
	No DELINATO <mark>Regularizase</mark>				
	Engine and Love I				

Log in and bind your TP-Link ID

After activating your TP-Link ID, come back to **Cloud Access** page to log in and bind your TP-Link ID to your controller.

Werkess Killer	ga 📔 Wateley, Saala	d Ada Kalenya	Chief Anersy.	45 dan ke 85 dinas.	v
Cloud Access					
Cloud Access	a a				
β equals the state β as	THE ALL				
Has I	is belief should be $\mathcal{M}_{1}(y)$ with				
Frees all		425			
	No 17-Link ID2 Regimen	nas.			
	Login and bird				

The TP-Link ID which is bound with the controller for the first time will be automatically bound as an administrator. And only one TP-Link ID can be bound with the controller as an administrator. An administrator account can add or remove other TP-Link IDs to or from the same controller as Cloud Users.

Wis co Sellino	Wadeov Cooled	l Skildage	Cloud Access	Canadar Solinga 🔛
Cloud Access				OTTAIN
Callebore 📲				
TP-UPA(D(Decsel) adole	lavargalikor 📲	1 million and		
	CARA.			Telliani -
4 TP-Lask D	Role	\$1.0	Stavad Dina	Actes
the delegant of the	at of determine	48 Shee	12010-06-14 11 21:20	
			F 1 A SK Abbielt	pagage Pagata

Add new Cloud Users

After you have an administrator TP-Link ID, you can add new Cloud Users. Click 🔁 Add Cloud User , enter another TP-Link ID as needed and click **Save**.

Add Cloud User			0
IP Link ID:			
	No TP Link ID7 <u>Register no</u>	<u>K</u>	
Role:	Operator	Ŧ	
Site Privilages:	Please Select	-	
Apply			

TP-Link ID	Enter the TP-Link ID that you want to add as the new Cloud User. If you do not have another TP-Link ID, you can click Register Now and follow the instructions to register a TP-Link ID.
Role	Select the role for the new Cloud User from the drop-down list. Two options are provided:
	Operator: An Operator account can change the settings of the privileged sites that are given by the administrator. And the Operator account cannot manage the cloud users and change controller settings.
	Observer : An Observer account can only view the status and settings of the privileged sites that are given by the administrator but not change the settings.
	Both the Operator and Observer accounts cannot manage the cloud users and controller settings. Thus Operator and Observer accounts can only be created or deleted by the administrator.
Site Privileges	Select the privileged sites (multiple options available) for the Operator or Observer accounts from the drop-down list.

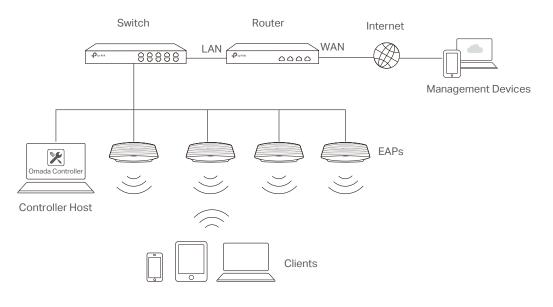
Unbind a TP-Link ID

You can click **Unbind** to unbind your administrator TP-Link ID. Note that Unbind operation cannot be performed when you log in to the controller through Omada Cloud service.

loud Access				Ciel.
and Acouse	- m			
Filink ID Swarth excitation	nangip-inkana 🚺			
				O Portesto
S TP CINS ID	1991 le	500	Created time	Action
= 119-Carro 10 edministratio (glassi mucant	inter internet	500 Al 0 km	Created time	Action
	a consider	00000		A0000
edministration (glass muchon)	ahtiisaan maaka	Al 9 ker	510 D 00 10 78 45	200000

4.2 Manage the Controller via Omada Cloud

With Cloud Access enabled, you can manage your controller remotely using your TP-Link ID. You can refer to the following topology.

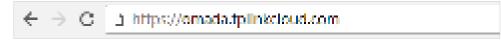


Before you remotely access your controller, make sure that the following requirements have been met:

- Cloud Access is enabled on the controller.
- Your controller has been bound with a TP-Link ID. If you don't have a TP-Link ID, refer to <u>Register</u> <u>a TP-Link ID</u> to get one.
- Both your Controller Host and management devices have internet access.

4.2.1 Access the controller via Omada Cloud

 Launch a web browser and type https://omada.tplinkcloud.com in the address bar, then press Enter (Windows) or Return (Mac).



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

Log in	- 32 - 12	
Enter with your TP-L	, ng ID and pessivol	6
Frati		
nampgsampic.com		
Pakkwara		
Remember Me		
Forgot Password*		

3. After you log in to Omada Cloud, a list of controllers that has been bound with your TP-Link ID will appear. If the controller does not appear on the list, you can click 🔂 to refresh the current page.

										. () (m an) (m
143	4.45	200 H	646.6	100	1.1440	10.000	$(\mathbf{x}_{i}) \in \mathbf{A}_{i}$	1.00	1.6.97	
and a second			Allen T		-		-	146		1 mar 2 -
sugar and search			0.04		÷.	- 2 5	Ŧ	196		There & set
and the second	14		1000	1.1	14	14	1	194	80	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
and the second second		1.19 h 1.	1.000		144	14		250		Times & set
terrere and the			100					1.00		T 11 11 (C - 547

i: 0 P . 14 10 an 1 marray 12 and 2 <u> 25 - 25 -</u> and the second E S STI 65 0.00 and the 1.000 weeks ($ddet_{i}$ ġ. Sec. 14 A section of . 1.6 and shares 6.45.45 (F) (F) (F) When the $\pm i$ - 14 1000 a sta ar in ÷ saide. 1.1.1.1.1.1.1.1.1 1.00 21 1002 2 din. Constant American Argon an la tari President all all a

Click Launch to access your controller. Then you can configure and manage your controller.

Note:

- To Refresh the page, click 0 . Automatic refreshing is not available when accessing the controller via Omada Cloud. .
- To remove the Omada Controller from your cloud account, you can click 🌔 📭 .
- To log out Omada Cloud, click 📑 and select Log Out. •

4.2.2 Change your TP-Link ID information

You can change your TP-Link ID information on the Omada Cloud page. Click 🛃 and select My TP-Link ID, the cloud accounting settings will appear.

You can have a nickname for your TP-Link ID. Enter your nick name and click Save.

Parte Canada	
+ Oracitation	

You can also change the password of your TP-Link ID. Enter the current password, then a new password twice and click Save.

-₽aper - analaza			÷
	No. In a	da se in cort	
	1.479.1		
	20 G.W.W		
	100 1000		
	-		

5 Configure the EAPs Separately

In addition to global configuration, you can configure the EAPs separately and the configuration results will be applied to a specified EAP.

To configure a specified EAP, please click the EAP's name on the **Access Points** tab or click connected EAP on the map. Then you can view the EAP's detailed information and configure the EAP on the pop-up window.

This chapter includes the following contents:

- View the Information of the EAP
- View Clients Connecting to the EAP
- View Mesh Information of the EAP
- Configure the EAP

5.1 View the Information of the EAP

5.1.1 Active Channel Information

The active channel information on each radio band will be displayed in a bar graph, which indicates its percentages of the following: Rx Frames (blue), Tx Frames (green), Interference (orange), and Free bandwidth (gray). The percentage of channel utilization is also displayed with the corresponding evaluation.

	and a long water	entil Longers
I same	1. 240	م الماليون (
al events	4.7%	CRN, United
	Constant Constant Constant	100 Value
SHOW.		
-24		
1920101		0.3

You can click a point on either bar graph for more details:

Tx Pkts/Bytes	673096171.11 G
Hx Pkts/Bytes	392000527-0.72 G
Ix Liner/Dropped	0.0% / 0.0%
Hx Lirror/Uropped	0.0% / 0.0%
Ch.Utl.(Busy/Ho/Dx)	30% / 20% / 1%

Tx Pkts/Bytes	Displays the amount of data transmitted as packets and bytes.
Rx Pkts/Bytes	Displays the amount of data received as packets and bytes.
Tx Error/Dropped	Displays the percentage of transmit packets that have errors and the percentage of packets that were dropped.
Rx Error/Dropped	Displays the percentage of receive packets that have errors and the percentage of packets that were dropped.
Ch.Util.(Busy/Rx/Tx)	Displays channel utilization statistics.
	Busy : This number is the sum of Tx, Rx, and also non-WiFi interference, which indicates how busy the channel is.
	Rx : This number indicates how often the radio is in active receive mode.
	Tx : This number indicates how often the radio is in active transmit mode.

5.1.2 Overview

Click **Overview** to view the basic information of the EAP which includes EAP's MAC address (or name you set), IP address, model, firmware version, the usage rate of CPU and Memory and uptime (indicates how long the EAP has been running without interruption).

A REAL PROPERTY AND A REAL	Concerned Concerned	
	inter (name)	(241) (2142)210
to desire b	<i>a</i> ,	Looperates
Constant of the		232 [M.m.
a		1 Auto
		122 Miles
Section 1	alam Indana Ita	10 C - C - C - C - C - C - C - C - C - C
And the state of t		
MIT # 18 mm	111131-1113	
The design	200.1 - 4	
Medel		
Howard Vietne	TRANSFORMED AND T	
738	25	
Memory	101	
Lola at	C days (C) 10 (O)	
Lin		
KSCIE .		

5.1.3 LAN

Click LAN to view the traffic information of the LAN port, including the total number of packets, the total size of data, the total number of packets loss, and the total size of error data in the process of receiving and transmitting data.

H Istoria a	-		(right)
	-		MA SHOT
AS INTERACT	2		2,000
-			in valari
Ratara I	l (a) sidas 🛛 🔳 🖬	e here en al de la companya de la co	
CARN IN			
1.000			
In Pariste	2012-0		
50 G	1.5 Store 1		
Kally an	1.8. V.V.		
Ro Onto Packetes	a de la companya de la compa		
Entern a	10.00		
is Faches:	- 101 - 4E		
To Paper 9	1721-757 B		
P. Dup An Olman	Areas -		
1. Entered	20.00		

5.1.4 Radio

Click **Radio** to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. You can also view parameters of receiving/ transmitting data on each radio band.

an marine	() i vi virta	
	(mail (in (1/2 - 1) -	na) (Si Aparina
H opened y	-	Most ref
		- 10° (0 1.0
41 million in 18		
-		- 75 V. OI
History II	termine Shinese Com	
WHEN DOLL		
LAT		
Aug St.		
Rude.	1000 (K.2) (See	
(Include)	i sun yela Manazartek	
1. Pray	2011 (1997) 2012	
100000	The tax	
California Surfayeer		
To Day Parlan	hee	
Set, in a	Sec. 1	
Is hearing	*** Tra	
To Party	1.67%	
11.5 ap Perkaha		
Sylamatic .	C Age and	

5.2 View Clients Connecting to the EAP

5.2.1 User

The **User** page displays the information of clients connecting to the SSID with Portal disabled, including their MAC addresses and connected SSIDs. You can click the client's MAC address to get its connection history.



5.2.2 Guest

The **Guest** page displays the information of clients connecting to the SSID with Portal enabled, including their MAC addresses and connected SSIDs. You can click the client's MAC address to get its connection history.

******		C (24)	en de la compañía de	
		Def a Liber	i Canal interv	xoongi u tan
0.0120000	ic)			
36	tier and the		10.8	
100	ao amin'ny faritr'o ao		250	
	SHELL	1.1.1.1.1.1.1.1	control bacterio Pagas	

5.3 View Mesh Information of the EAP

The Mesh page is used to view and configure the mesh parameters of the EAP.

5.3.1 Uplinks

Here you can view the parameters of the uplink APs or click [1] to change the uplink AP.

					@ R
Ad None	• Channel	4 Signal	€ Hop	4 Deanlink	Action
EA-23-61-35-22-52	. 49	-35 dom	1.9	95	(K
EA 33-81-08-22-40	-40	28 6 0	3	20	[194]

Tips:

- You can click 🔘 🛤 to search the available uplink APs and the Uplink list will refresh.
- To build a mesh network with better performance, we recommend that you select the Uplink AP with the strongest signal, least hop and least Downlink AP.

5.3.2 Downlinks

Here you can view the downlink APs.

5A-03-51-AS-22-A0	Connected (Windows)	0
	Delute Line Doel Linet	Serrigi Scient
upleks		
llumint)s		1
AP Nam	e Signal	
A0 64.05.02	E0 CE 53 cBo 📕	

5.4 Configure the EAP

The **Configuration** page is used to configure the EAP. All the configurations will only take effect on this device.

A-20-51-66-25-52	Occurrented	
	Details User Guest Herb	Contiguation
David Config		
Hara	EA23-61-06-02-62	
Auto-		
iP secting		
Rode		
Load Galance		
MLANS		
Regue AP Detection		
Forget this AP		

5.4.1 Basic Config

Here you can change the name of the EAP.

wate contra		٨
н	HA 25 M POLY M	
- Apple		

5.4.2 IP Setting

You can configure an IP address for this EAP. Two options are provided: DHCP and Static.

🗧 DHICH 🛛 🔵 State			
Falback P	🖃 Ensble 🧐		
Falback P Address	192,383.0.264		
Felfback (P Mask	755 755 255 0		
Fallback Sateway:		(Optionzi)	

Get a Dynamic IP Address From the DHCP Server

- 1. Configure your DHCP server.
- 2. Select **DHCP** on the page above.
- 3. Enable the Fallback IP feature. When the device cannot get a dynamic IP address, the fallback IP address will be used.
- 4. Set IP address, IP mask and gateway for the fallback address and click Apply.

Manually Set a Static IP Address for the EAP

- 1. Select Static.
- 2. Set the IP address, IP mask and gateway for the static address and click Apply.

5.4.3 Radio

Radio settings directly control the behavior of the radio in the EAP and its interaction with the physical medium; that is, how and what type of signal the EAP emits.

24982			
Shite	- Enable		
Victo	102 Hamile, misso	-	
Same Web	2014018044-6	1. A	
Channel Linds	Fixthe		
Note : in El-Franker Schliefte is het uitvere		neder, In the Inecuery Single 5 (50) b	
dicent	4446	•	
ic wants dit	1 di	-	

Select the frequency band (2.4GHz/5GHz) and configure the following parameters.

Status	Enabled by default. If you disable the option, the radio on the frequency band will turn off.
Mode	Select the IEEE 802.11 mode the radio uses.
	When the frequency of 2.4GHz is selected, 802.11b/g/n mixed, 802.11b/g mixed, and 802.11n only modes are available:
	802.11b/g/n mixed : All of 802.11b, 802.11g, and 802.11n clients operating in the 2.4GHz frequency can connect to the EAP. We recommend that you select the 802.11b/g/n mixed mode.
	802.11b/g mixed: Both 802.11b and 802.11g clients can connect to the EAP.
	802.11n only: Only 802.11n clients can connect to the EAP.
	When the frequency of 5GHz is selected, 802.11 n/ac mixed, 802.11a/n mixed, 802.11 ac only, 802.11a only, and 802.11n only modes are available:
	802.11n/ac mixed : Both 802.11n clients and 802.11ac clients operating in the 5GHz frequency can connect to the EAP.
	802.11a/n mixed : Both 802.11a clients and 802.11n clients operating in the 5GHz frequency can connect to the EAP.
	802.11ac only: Only 802.11ac clients can connect to the EAP.
	802.11a only: Only 802.11a clients can connect to the EAP.
	802.11n only: Only 802.11n clients can connect to the EAP.
Channel Limit	For the EAPs that support DFS in EU version, there is a Channel Limit option. If you want to use your EAP outdoors, enable this option to comply with the laws in your country.

Channel Width	Select the channel width of the EAP. The available options differ among different EAPs.
	For some EAPs, available options include 20MHz, 40MHz and 20/40MHz.
	For other EAPs, available options include 20MHz , 40MHz , 80MHz and 20/40/80MHz .
	The 20/40 MHz and 20/40/80MHz channels enable higher data rates but leave fewer channels available for use by other 2.4GHz and 5GHz devices. When the radio mode includes 802.11n, we recommend that you set the channel bandwidth to 20/40 MHz or 20/40/80MHz to improve the transmission speed.
Channel	Select the channel used by the EAP to improve wireless performance. The range of available channels is determined by the radio mode and the country setting. If you select Auto for the channel setting, the EAP scans available channels and selects a channel where the least amount of traffic is detected.
Tx Power (EIRP)	Select the Tx Power (Transmit Power) in the 4 options: Low, Medium, High and Custom . Low, Medium and High are based on the Min. Txpower (Minimum transmit power) and Max. TxPower (Maximum transmit power. It may vary among different countries and regions).
	Low: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (round off the value)
	Medium : Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (round off the value)
	High: Max. TxPower
	Custom: Enter a value manually.

5.4.4 Load Balance

By setting the maximum number of clients accessing the EAPs, Load Balance helps to achieve rational use of network resources.

Load Balance			*
2.4GHz SGHz			
Max Associated Clienta	T Lnable		
	1	(1.99)	
RSSI Threshold	🗍 Lnable		
	0	(95 0 dBm)	
Apply			

Select the frequency band (2.4GHz/5GHz) and configure the parameters.

Max Associated	Enable this function and specify the maximum number of connected clients. While
Clients	more clients requesting to connect, the EAP will disconnect those with weaker
	signals.

RSSI Threshold

Enable this function and enter the threshold of **RSSI** (Received Signal Strength Indication). When the clients' signal is weaker than the **RSSI Threshold** you've set, the clients will be disconnected from the EAP.

5.4.5 WLANs

You can specify a different SSID name and password to override the previous SSID. After that, clients can only see the new SSID and use the new password to access the network. Follow the steps below to override the SSID.

WLAN Groups	C els uls	-	
Name	10 10		ACC 1
× 65.	2.46° - 67, 50.045		ø

- 1. Select the WLAN group.
- 2. Click 🚺 and the following window will pop up.

D Overseite	011		1
Eson	English On AP		
81.44	Die warie	(Contrast)	
380	560-9		
Pin	paint.	es restation.	

- 3. Check the box to enable the feature.
- You can join the overridden SSID in to a VLAN. Check the Use VLAN ID box and specify a VLAN ID.
- 5. Specify a new name and password for the SSID.
- 6. Click **Apply** to save the configuration.

5.4.6 LED

You can change the LED status of each EAP.

185				
() the Shelder by	< 2	$\subset \mathcal{O}$		
- Amily -				

Using Site Setting	The LED status will be the same as the site settings.		
On	Turn on the LED.		
Off	Turn off the LED.		

5.4.7 Trunk Settings (Only for EAP330)

The trunk function can bundles multiple Ethernet links into a logical link to increase bandwidth and improve network reliability.

	Trunk Settings	8 ×	
	2 Labora	1 Frank	
	Meda (MACT REPEALACE RATE A	
	Apoly .		
Status	Th	ble this function. EEAP330 has two 1000Mbps Ethernet ports. If the Trunk function is enable the ports are in the speed of 1000Mbps Full Duplex, the whole bandwidth trunk link is up to 4Gbps (2000Mbps * 2).	
Mode	Se	ect the applied mode of Trunk Arithmetic from the drop-down list.	
		C_DA+MAC_SA : When this option is selected, the arithmetic will be based of source and destination MAC addresses of the packets.	on
		C_DA : When this option is selected, the arithmetic will be based on th tination MAC addresses of the packets.	he
		C_SA : When this option is selected, the arithmetic will be based on the source C addresses of the packets.	се

5.4.8 Rogue APs Detection

With this option enabled, the EAP will detect rogue APs in all channels. You can view the results in **Insight > Untrusted Rogue APs** page.

Rogue AP Detection	R
Sism	

Note:

For some specific versions of the firmware, some EAPs will detect rogue APs automatically when this option is enabled.

5.4.9 Local LAN Port Settings (Only for EAP115-Wall and EAP225-Wall)

Local LAN Post Schops, 😵 ø 1.02 **V1.05** | En Mi 1-1-1-2 MINK. 📙 En ide CT D: INC Dec 🖂 Line 🖬 🛛 VLAN: 🗖 ta da See.

You can configure the LAN port of the EAP.

VLAN	Enable this feature and specify the VLAN that the EAP is added to, and then the hosts connected to this EAP can only communicate with the devices in this VLAN. The valid values are from 1 to 4094, and the default is 1.
PoE Out	If your EAP has PoE OUT port, you can enable this option to supply power to the connected device on this port.
	The EAP that has no PoE OUT port does not support this feature.

5.4.10 Forget this AP

If you no longer want to manage this EAP, you may remove it. All the configurations and history about this EAP will be deleted. It is recommended to back up the configurations of this EAP before you forget it.



6

Manage the Omada Controller

This chapter mainly introduces how to manage the user account and configure system settings. This chapter includes the following contents.

- User Account
- General Setting
- History Data Retention
- Backup&Restore
- Auto Backup
- Migrate
- Information About the Software

6.1 User Account

You can use different user account to log in to the Omada Controller. User has three roles: administrator, operator and observer. The administration authority varies among different roles.

Administrator	The first administrator account is created in the Basic Configuration process and this account can not be deleted. An administrator can change the settings of the EAP network and create and delete user accounts.
Operator	An operator account can be created or deleted by the administrator. The operator can change the settings of the EAP network.
Observer	An observer account can be created or deleted by the administrator. The observer can only view the status and settings of the EAP network but not change the settings.

Follow the steps below to add user account.

1. Go to Controller Settings > User Account.

Wrekes Serlings	ndest Setlings with an and a characterized and		Classification	Controller Settings
	intervenues de servición	daga (Di Kata Dista Rese	etan. Tack pARentse	yan Bacing - Migrate 1,526
berara Taul Sea	Q			
32220020010	Secol	Role	Created Time	Action
: Userkonia		57.50		10000

2. Click 🚺 👦 and the following window will pop up.

Add user				0
Ur zer Vran er				
in all			Qiyina di	
13 de	Official and	т	0	
Paramet		43-		
Carl on Press at		43		
$\mathrm{SL} \cdot \mathrm{Pitchey} \sim$	Panes Ariset	т		
Sec.				

- 3. Specify the username, Email and password of the account.
- 4. Select the role from the drop-down list.
- If you select operator or observer, you also need to select the Site Privileges.

- If you select administrator, the Site Privileges option will not appear and all sites are available for the administrator user.
- 5. Click **Apply** to add the user account.

Note:

- You can refer to the **Role** page to view the user role's type, description information, permission scope and created time.
- The user account cannot be used to log in to the Omada Controller through Omada Cloud Service. To
 access the controller via Cloud Access, you should be a cloud user. To add a cloud user, refer to <u>manage</u>
 <u>the cloud users</u>.

6.2 General Setting

6.2.1 Configure Controller Name

Omada Controller is given a default name in the format **Omada Controller_XXXXXX**. You can give your controller a descriptive name in the **Controller Settings** > **General Setting** page and click **Apply**.

Arrevess Serings	wireless Compa	set serings	CASHE ACCESS	Costroller Battings	
	TherAppent annual	Setting Delays Overs	Reneal ten (Forstand Resile	 Auto Seckop (Pzigote 	Wadai
these wetrops					
Somethics Karne	Onace Consoler_558655				
- Angen					

6.2.2 Configure Mail Server

With the Mail Server, you can reset the login password of the user account if necessary. An email with the link of resetting password will be sent from the Omada Controller. It is different from the SMTP Server, which is just for the system log emails sending.

Follow the steps below to configure mail server.

1. Go to Controller Settings > General Setting and click Mail Server.

Windows Settings	Windess Cor	ritol Site	• Settings	Circuit Access	Controller Settings	
	User Account.	Ceneral settings	HISION Data	rætorbon Backupskæsk	re Aulo Backup Migrate	About
Basio Bettings						×
Nall Server 🛞						8
Controller Hestnamed P	127.0.0.1					
Enable SMIP Server						
Apply						

 Enter the hostname or IP address of the Omada Controller. The default IP address of the Omada Controller is 127.0.0.1. You can keep it or customize the hostname or IP address which can be visited by the Controller host.

When the email with the link of resetting password are sent out, the Controller hostname or IP address will be specified in the Controller URL in every message.

3. Check the box to enable SMTP Server, and then the following screen will appear.

et in max for imp	Weekers Con	mi 284	Serlaga Cla	vi ivrea	Control ler Sec	tings E
	User Account	Concession and	Lancy Cola Researce		Auto Radrup	Migole 1 Abort
Boart Sellings						
Wat Server /2						
Contra esticularmente.	129042					
I (Croke ShiTE Server						
Ve Serve						
39y0	35					
	🖂 Enalde SSL					
🖂 Europhi Asily						
(harnina)						
Postand		92				
Specify Sender Address						
(Arra)						

4. Configure the following parameters.

Mail Server	Enter the IP address or domain name of SMTP Server.				
Port	The SMTP server uses port 25 as default.				
	You can enable SSL (Security Socket Layer) to enhance secure communications over the Internet. If SSL is enabled, the port number will automatically change to 465.				
Enable Auth	Check the box to enable authentication (Optional).				
Username/Password	If you enable authentication, enter the username and password required by the mail server.				
Specify Sender Address	Specify the sender's mail address. Enter the email address that will appear as the sender for resetting password.				

5. Click **Apply** to save the configuration.

Note:

Specify the account email address based on the Mail server to receive the email for resetting password.

6.3 History Data Retention

History Data Retention allows users to determine the retention of logs and client statistics. The logs and client statistics beyond the specified number of days will be cleared. For example, with **7 days** selected, only the logs and client statistics in recent 7 days will be retained, and the data beyond 7 days will be cleared from the controller.

Follow the steps below to configure Historical Data Retention:

1. Go to **Controller Settings > History Data Retention**.

without contracting	W MEAC CONTO	ana karaga	C GID ASYADA	conto ner saturge
	user socialiti perieta	antinga Timbo Ista	execution Execution variable	е инстистр (израте изон
Hodesteal Color Defined as	964 Daya	-		
Serve the contemporate set scalars	e la collècte de la collecte de la collèce	galeticalitest en lag	n at electricities is you'll	ensed is taken to a day with a
- Apple				

- 2. Select the length of time in days that data will be retained from the drop-down list. Seven options are provided: **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, **365 days**, or **All time**.
- 3. Click Apply.

6.4 Backup&Restore

You can save the current configuration and data in the controller as a backup file and if necessary, restore the configuration using the backup file. We recommend that you back up the settings before upgrading the device. This function is available only for local logged-in users.

Follow the steps below to backup and restore the configuration.

1. Go to **Controller Settings > Backup&Restore.**

ware easy seeings.	eenseas.commi	ала салгара	Const Anders	Control en sectings.	
	USPACEMENT SPECIFIC	amiya - Listory Lata i	erenand 1 903 See Stor	 A state investig = signate 	And it
\mathbf{D}_{i} is inverse to be a Back up to the term of term	2 dia produ	-			
	. Note that the link of the state δ and	even as the Settings Geb_{2}	quive a set of the data of		
	Deckap				
Decore The	Photo schola din	Errore R	101		
	l Bosto The configurations in all the				

- Select the length of time in days that data will be backed up in the Retained Data Backup dropdown list. For example, with 7 days selected, the data only in recent 7 days will be backed up.
- 3. Click **Backup** to save the backup file.
- 4. If necessary, click **Browse** to locate and choose the backup file. Then click **Restore** to restore the configuration.

Note:

- If you do not want to back up historical data, you can select **Settings only** to get only the controller setting saved in the backup files.
- If you do not want to back up data manually, you can enable the Auto Backup function. Please refer to <u>Auto</u> <u>Backup</u>.
- To keep the backup data safe , please wait without any operations while restoring the backup file.

6.5 Auto Backup

With Auto Backup enabled, the controller will be scheduled to back up the configuration and data automatically at the specified time.

Follow the steps below to configure Auto Backup function.

1. Go to Controller Settings > Auto Backup.

алтенкос желтікур	W NAMES CONTROL	ana karanga	Cialia Aprena	controller straings	
	user consum service	seniego (Herory Ford)	orannan (Trassipskarura	viro manle indua	2308
Ander Anela in	🗹 Endle				
Contraction of the	12 mile	-			
Stelays Low	(0 = 0) -				
$D = \log (n + 1) \log (n + 2 \log n)$	2. Illu po ele	-			
	$\mathbf{R} = \mathbf{r} + \mathbf{r} + \mathbf{r}$ by Hisin Scelap,	is a because the Avellanys ()	ϕ_{1} as defined by matrix ϕ_{1}		
$M_{\rm eV}$ is a N mass of Lie .	<i>i</i>	11 M.)			
Apply					
наскор и ме оте:					2

- 2. Check the box to enable Auto Backup function.
- Select how often to perform Auto Backup in the Occurrence. You can choose Daily, Weekly, Monthly or Yearly from drop-down list. Then set an appropriate time to back up files in the Backup Time.
 - **Note:** When you choose the Occurrence as Monthly, please carefully choose the backup date in Backup Time. For example, if you choose to automatically backup the data on the 31th day of every month. When it comes to June, which is only 30 days long, the auto backup will not take effect
- 4. Select the length of time in days that data will be backed up in the **Retained Data Backup**. For example, with **7 days** selected, the data only in recent 7 days will be backed up.
- 5. Specify the maximum number of backup files to save in the **Maximum Number of Files**. The default is 7.

White Set Inge	l We	eles Cara	N.	Salas Sector	da.		Che	el Acia	a.	Controlle	r Settings	
		Assessed - V	Samal Su	uno Inna	(Y.10)	in their	000	Bach	apsili, ina	y Antoi that is	- Migrate	Aboy
Avec Backup	⊡ briel											
Occurrance.	(Peek y			43								
	⊒ Wor	E lov	= Ked	III (m								
Er, Aug Ten	Thi	□ Sec.	San		$\left\{ \mu \right\}$	26	$\langle \Psi \rangle$	30	3 3]			
Setviced Data Factors	7.0350			23								
	Shore as	Netwine Calific	abtatai	un interes	20,0	dala biy	1990,00	aiti7.¢	eya kitibe	sarked ap.		
Maximum Number of Direct	7			314	t)							
a trans												
Harman Ales Lint												
FD	e Marne			Backe	e Tira	2			ine		Action	
aussbackup Tole,	e dataked	1-1000 dg		135 (51	10.10	50 50			546		0.01	
			124	18.8	192	10/3	in an	i anti a	l'Agent			1.1

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

You can execute the corresponding operation to the backup files by clicking an icon in the Action column.

Ċ	Restore the data and configurations in the backup file.
0	Download the backup file.
ā	Delete the backup file.

Note:

- To back up data manually and restore the data to the controller, configure Backup&Restore function.
 Please refer to <u>Backup&Restore</u>.
- If you do not want to back up historical data, you can select **Settings only** to get only the controller setting saved in the backup files.
- The auto backup files will be stored in data/ autobackup folder of the controller installation location.
- The configuration of the cloud users will not be backed up. Thus the configuration of the cloud users cannot be restored. To add cloud users, please refer to <u>Manage the Cloud Users</u>.
- To keep the backup data safe , please wait without any operations while restoring the backup file.

6.6 Migrate

Migrate function allows users to migrate the configurations and data to any other site or controller.

For Migrating all the configurations and data from the current controller to any other controller, refer to Controller Migrate.

For Migrating the configurations and data from the existing site to any other controller, refer to Site Migrate.

6.6.1 Controller Migrate

With Controller Migrate function, you can migrate your configurations and data from the current controller to any other controller that has the same or higher 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.

Follow the steps below to migrate your controller.

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
- 1. Go to Controller Settings > Migrate > Controller Migrate.

Watchess Settings	WYCESS CONTRA	SHE BOXINGS	Cloud Appens	Controller Settings
	User Account Cores	or Stange - Asing Date	edagaan (manapathea	ora - Auto Backay Meguna Ale
Worksy lik conside regularity consided	ar is informal of the loss for your Please choose the time to start	eral mito ala during ili e migral migrallor operation caretaly	en Clena nect la consoc	the observe network again after the
Competer Megrado				
FootSchola -	[2 Mg (1 0 +	inte 24	Ng. 675 6	- @1.491
	anard consolial, doctoac fire post cancel confiction in carry of		a a legist where	
Salood Dava Races y	Scilegi etti	3 9		
interRetained Data Data	is the beau art in Settings Ce	is no determini be bestied op.		
Served Server	74L W			
62 M 1977 19				

 Select the length of time in days that data to be imported into the second controller in the Retained Data Backup drop-down list. For example, with 7 days selected, the data only in recent 7 days will be imported into the second controller.

- 3. Click **Download Backup File** to download the file of the current controller. If you have backed up the file, click **Skip**.
- Migrate Controller
- Start and log in to the second controller, go to Controller Settings > Backup&Restore > Restore File.

eare accounting t	eenseas compo	оны селтора	(3497,74240)	Control en sectings	
	CONVERSION SERVICE	omingin – Likeby Lana	- energiese in the second second	A VICE HINARD - MIGHTA	ondit
\mathbf{B}_{i} inio et Todo Kashop	Z dia paole	-			
	Rene tek bestilikin Soelapikov	here α is defined by Orb_{1}	quive an will which as		
	Deckup				
Decore The	Means satisfied white	Erevite R	87.344		
	Botac The configurations in all de	e sies vill be bedeet up o	NER		

- 2. Click **Browse** to locate and choose the file of your controller to be imported. Then click **Restore** to upload the file.
- 3. After the file has been restored to the second controller, go back to the export controller and click **Confirm**.

Weeksa Sedinga	Wittless Canadi	Sác Solanga	Dead Assas	Controller Settings	ľ
	Shar Asian (Davies	Silaye (Thiry Ond	adardar Bedaşdiğarl	ana (Ana Santan (1779) in (1	h
and the second second					
regration is completed. Pa	as the state of the firm to starting	pation operation caretuly.	at. Coestineed to correct	the scheles restor it spale about the	
Sector Magazia					
Fourt Contains	Distance Course	10 mm	State Bullet	- Other	
July a constant	Competence and	то D44			
Weaters happen but	tania, mpelikuta yan awa menaka taning iki kadalara		Sanda Saiga Saig	وطعقو لحداد أنطع	
the backup the of y	our control et			10 M	
Contract of Contract					
te Vigrate					

- Migrate Devices
- 1. Click **Browse** to locate and choose the file of your controller to be imported. Then click **Restore** to upload the file.

2. Enter the IP address or URL of your second controller into **Controller URL/IP** input filed. In this case, the IP address of the second controller is 10.0.3.23.

Wavese Setting	Windows Costrol	Sile Section	Cost Arres	Controllar Sattings
	The Account General	Sections: [1] Interview Controls	election (FactorpiSee)	aw I yan geoor 1 manie 1 wa
Warning: The connection to i mighting in condense. Pieze	internet All, be Bat for sever	i minutes curring the might	ion Cleans made to constant	the coveral rescoid again after the
The second s		Transient ready		
surre-lat biguts				
Cases Controller	📑 Miganis Corrol	ler	li gran Devices	
C Vgulv Laakead Friespork 1-14	enew open solved ora tes till type versione	5a 		
omaliant(20.025				
111322				
Ewan None Vider	.a.			

Note:

Make sure that you enter the correct IP address of the second controller to establish the communication between EAPs and your second controller. Otherwise the EAPs cannot be adopted by the second controller.

3. Select the devices that are to be migrated by clicking the boxes next to each devices. By default,

all the devices are selected.

Weinlass S	ettres V	Vandenis Colorinol	Las Settros	Gent An	Cast	roller Settings
	ÿ	Accust 1969443	erigi (Lewy D	n Selector (Fac	apàResione (Auto I	whit where a
Waterings Th responses in a	e panetadar ta ktera revularati Pisasa da	er all beloc to swart ske no dra to clan a	reintes clifts to n action contribution	gerles Client new V 2	to contact the scieles.	which applicates the
orrestat N	wate					
🔓 Elser Canaler — 💦 Maan Geraler —		v	U gran Divikas	©:	6m)	
e ise IP.Dedicere	se por de Le bilan	er bistar second condr ML biggen second con				
in D.3.25 Traini Marce	waa s	a.				
T.	÷ Devree Name		Sta	‡ Stabus	4. Mictor	÷ Напенай Чарал
4	Elizabilitazia	t <u>.</u> 19	N Nolis	Ganalia	EN1529-Valaciator	11/2
3	C4-3351-83-33-4	0	rute	Curracted	EAP203-Outdoor(Dk)	10
elected 2 ,512	t terme		10	1.1.2.20	Attained 3 pepping 3	wyc: 👘

4. Click **Migrate Devices** to migrate the selected devices to the second controller.

5. Verify that all the migrated devices are visible and connected on the second controller. Note that this may take several minutes. When all the migrated devices are in **Connected** status on the **Access Points** page on the second controller, click **Forget Devices** to finish the migration process.

0 1	This for a pass possion log-	the background is the second of	10.00		d Urganiza
Dominitar	52.1				
E)	† Device Name	ti Sita	# Status	t Nodel	t Hardware Version
14.	54-03-51-02-0543	Detail	Corrected	EAF35FOrecor(E.)	(0.42
6	56 73 81 46 72 63	Default	Second	FARME Contraction	- CA S

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

whereas Settings	Warners Control	I BRE-SHIT	ngs Date Ac	tess (b)	ntraker Settings
	Uso Accost Ger	and Selfrique - Har	on Data Seantan (Bas	artWestern Aut	name input [200
Mandag: The consecut i reparts a complete Ple	is internet will be had for a wate blinders the time to d	arvent minules during infilm spatian operation	i de migrator. O esta rees o Carelo e	to context the value	a statut age table to
armiter Migrate					
Depot Controller -	📄 👘 Stignalis C	ontroller	— 👌 Vipcala Devicas	@	Cole .
To told the regard Prove set is as introduced in an encoder	for process, forger the ex- vice page in compression in a los	rzewiały nigrad o oprzeka na starki s	R.N.M. 18 of the Papalet Second	te of a sector	ant the second
Arroy Netwo Note	Q				
D	e Picarne	9 Scie	# Status	÷ Model	A Bandware Website
No every to the table					
The contract of the second					

6.6.2 Site Migrate

With Site Migrate function, you can migrate your configurations and data of a site to any other controller that has the same version.

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.

Follow the steps below to migrate a site to anther controller.

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
- 1. Go to Controller Settings > Migrate > Site Migrate.

Oser-Account General	ward framework		197	
	search funderinger	ReckarGoon Bachepa	Scolaro Aulo Backop Mapun, A	bu
annel will be loat for service choose the lime to playtom	i nin das durng die nigs ginder operation carefully	dan Carlenad Issan	westworks are network upon all or tax	
				1
ER Physics Str.	C2 March D	ut.11	() Use	
		0000000		
20		a gi an chi acci.		
7	1 m			
	choose the line to start of EQUIPULATE Star (Be, down bied the backup f mentione to any other starts	choose the line to start might be carefully EQUID on the line to start might be carefully EQUID on the line to a second the mentioned the second the mentioned the second the	choose the line to starting extension speed for sample). EQUIPULATERS	ER Manas Mar - Compose Contrar - Olive De, courded the backup file med die to stry zher scholer had has hie sette schigter weeks.

- 2. Select the site to be imported into the second controller in the Select Site drop-down list.
- 3. Click **Download Backup File** to download the file of the current site. If you have backed up the file, click **Skip**.
- Migrate Site
- 1. Start and log in to the second controller, click **See Real** in the top left corner of the page and select **Berlinger**, and then the following window will pop up.

Sav Haves Q							(H) O (
‡ Alte Karne	t sliens	‡ Connected	2 Disconnected	t isobred	¢ lisers	÷ Guess	Action
166.44	ð.	(it	ê0	ð C	- £3	- 31	
(Def	Ŵ	(ig.	R ()		1°	- 31	0.01
teat .	90	- (Q	x 2.	162	18 A	- Cir	PS IT

2. Click 🕘 Import Ste and enter a unique name for the new site.

Import Site		0
Site Name:	Sile-3	
Choose I lie:	Please select a file	Urowse Import

3. Click **Browse** to upload the file of the site to be imported and click **Import** to import the site.

Import Site			Θ
Site Name:	Sile-3		
Choose I IIe:	Site_A_sitebackup.clg	Urowse Import	

4. After the file has been imported to the second controller, go back to the export controller and click **Confirm**.

Use Accorn [Denen	化合物学系统 化分子输送器 化化合金			and the second second second
	Sectore South States	ALISONANON BOCKEL	Stream Are brown 1	Heat: Mos
ran bidlar sa dha saya Gaine basan ba data		adan Badarah Ing	nan dite medan enimalen	enter.
📑 Sectoral		(Fier)	800	
part films your second on by clicking free import Sile	oroller In Sal Sile Variagemen	C drost down and upload	ing the best-up file of your effe	
	🖹 Yeskii —	E Ngulani (1 Vaul	The Mandel Contract	

- Migrate Devices
- 1. Enter the IP address or URL of your second controller into **Controller URL/IP** input filed. In this case, the IP address of the second controller is 10.0.3.14.

Western Settings	WYERSS SONOR	Bile Settings	Cloud Arbez	Centroller Bottings	
	See Account Core	а хелор, Трякороска	octoretati î saceapeareat	с тим яки; посн 1	20.0
	eduiden Sachterber für Ger Sachtere für Leis Kridati	dan talan dan ya	ka Skala serila senara	te ani en el anti que che fa	10
Controller Vigrate					
an estru					4
1; ::::::::::::::::::::::::::::::::::::	— = Physic =		vas ©		
	riad Verdena ni yana talah bi na inform UKL karyour talah di s				
Selection (Harth)					
1012.01					
English Street, Mark V	0				
100000000000000000000000000000000000000					

Note:

Make sure that you enter the correct IP address of the second controller to establish the communication between EAPs and your second controller. Otherwise the EAPs cannot be adopted by the second controller.

2. Select the devices that are to be migrated by clicking the boxes next to each devices. By default, all the devices are selected.

Wittens Setting	n 🕴 Windess Co	ntmi 🔰 Siller Settinge	Cloud Acres	Controller Settings
	User Arrown	Oeveral Settings, Livistory	Data Artendos - L Bierstup (Artendo	ne Laux Sector Munch At
Warring: The con-	retton In marry will be but det Press choice the line	(for period minutes) during the (to start migration nearables) re-	regretors. Charta vasot to connact i Wile	the sense as not set of a part of an item.
oritroller Nigrate				
de Migrate				
Exect file	El Moraia S		n Davitas Pi	Curre
	indiacted devices to your se ride the Vitaria URL to your			
ontrofiler UNLAPI				
10.0.1.14				
Davine Marine, Mari	a Q			
10 O	Device Name	0 Status	8 Model	9 Harstware Version
B 9	-23-51-08-22-53	Corrected	EAP225-Custon(EU)	14
B P	55-51-65-22-40	Corrected	EAP228 Outdoor(EU)	1.0

- 3. Click **Migrate Devices** to migrate the selected devices to the second controller.
- 4. Verify that all the migrated devices are visible and connected on the second controller. Note that this may take several minutes. When all the migrated devices are in **Connected** status on the **Access Points** page on the second controller, click **Forget Devices** to finish the migration process.

	Joer Auguant.	Control School Hol	oy can be writer. Is	Russector Aces	acrop 1 Higher 140
0 4	I tel los tigados jovenos, voja-	In his smalle in grad a	e co.		Constant State
	y tulis enversi musika			are appretiated	d bapaza
John Tar	AV DE MILL				
0	t Device Nome	to Sites	e Statua	t Nodel	B Hardware Version
14.1	54-03-51-02-05-02	Detail	Connected	CAPSCONDO(E.)	042
Ð.	55,23,52,46,22,83	Dolard.	Second!	EVEX Control Filt	1983
	(2 amme)			A total of Langello P	ver e

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

	16ergeraat 19e	energi Sattings, Thirdney,	Inta Selention Good philiped	ore i Auto Seckut - Mayore I Ato
Warning: the convector k nightnee is condisted. Play	a miernel will bei dei kon NGC 22 SADE the Streets e	anara misika dang tari Mangolah tarihin dan	ngalar. Danla awa ta samad Aliy	he version relative again after the
ntroller kligrase				
la Migiute				
East Sk	- Er Highlick	(\$N_T	k Printe 🔗	Done
		010358	5575793	26625
10 want beingek	NETSON & BUT PACKED	n vadali, is galeti da na natioke entimati dalah	The congraded sides are used in a	errainfal in gene
() New Solida Sec	NETSON & BUT PACING	tativity are than being		en namen al fre sense
C v mait de regels Felder relifie der etty sterrared to		tativity are than being		en constall. Interpreter

6.7 Information About the Software

You can view the Omada Controller's version and copyright information on the **Controller Settings** > **About** page.



Application Example

A restaurant has a wireless network with three EAPs managed by the Omada Controller. The network administrator wants to :

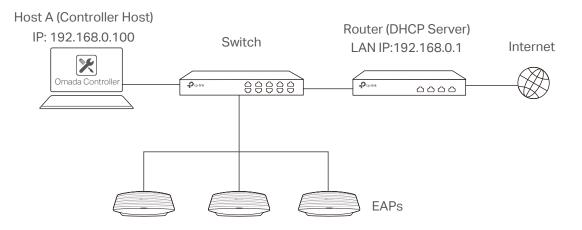
- Monitor the EAPs with the Map.
- Enable Portal function to drive customers' attention to the ads of the supermarket when customers attempt to access the network. The costumers need to use a simple password to pass the authentication.
- Allow the employees of the restaurant to access the network resources without portal authentication.
- Schedule the radio to operate only during the working time (8:00 am to 22:00 pm) in order to reduce power consumption.

Follow the steps below to achieve the requirements above.

7.1 Basic Configuration

Follow the steps below to do the basic configuration.

1. Connect the hardware by referring to the following topology.



- 2. Install the Omada Controller on Host A.
- 3. Launch the software and follow the instructions to complete some initial configurations.
- 4. Log into the management interface.
- 5. Adopt the pending EAPs.

7.2 Advanced Settings

After the basic configuration, refer to the following content to meet the network administrator's requirements.

7.2.1 Monitor the EAPs with Map

Follow the steps below to create a map and monitor the EAPs with the map.

- 1. Go to the Map.
- 2. Import a local map and set the map scale.
- 3. Drag the EAPs to the appropriate locations on the map.
- 4. Click **Coverage** and you can see the representation of the EAPs' wireless coverage.



7.2.2 Configure Portal Authentication

Follow the steps below to configure Portal function.

1. Go to Wireless Settings > Basic Wireless Settings and edit the SSID we created in the basic configuration.

E	dit SSID		٥
	Basic Into	ł	R
	SSID Name	SSID1	
	Rend	🔽 2.4GHz 🖂 9GHz	
	Guest Network:	🔄 Fushle 🍘	
	Security Mode:	None -	
	Advanced Settings		81
	Apply		

To make it easier for customers to connect, change the Security Mode from **WPA-PSK** to **None**. Customers can connect to the EAPs without password and be redirected to the Portal Authentication where the correct password will be required.

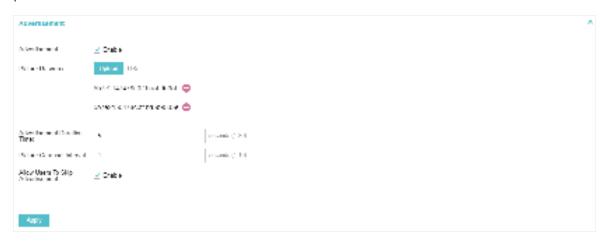
- 2. Open the global configuration window and go to Wireless Control > Portal. Click 🕂 Add a New Portal The configuration window will pop up.
- 3. In the **Basic Info** section, complete the basic settings for the portal.

kin New Portal		
Danik initi		
Partal Maria	Carrol	
50.001	55.12	
Δa^{\dagger} is a final fraction of γ parameters γ	Xingaa Marawarat	-
Karawa I		ø
Administration in secol	111 mil	-
$1111 \leq \ell < \min < \ell$	2 Handler 🌧	
Reduced	Z Hand Cr 🔿	
Redenal U-1	bits decreased with a set even	

- 1) Specify a name for the portal.
- 2) Select an SSID for the portal.
- 3) Select the Authentication Type as Simple Password. Specify a simple password for the guests.
- 4) Select the Authentication Timeout. For example, 1 Hour is suitable for the customers at the restaurant.
- 5) Enable the **Redirect** to drive the costumers to the restaurant's homepage after successful login. We can put some promotion information on the page.
- 4. In the **Login Page** section, configure the login page.

LOR POPOL				
ter mare	Chatelin Ohmer		ane, 4	Gunes
Tar original Caler	RC107	347 Salis	<u>.</u>	
lan Yege Water bigget of	All and a second	564 (<mark>0</mark> 33 7 ¹⁰ falance a T	La recept Description	
Kapalon ()) Silosi (Silosi)	Tengenga 2019	3 00 mar - 1 ⁰		
Here is a service	E.			
100.000	0			

5. In the Advertisement section, upload two pictures of the restaurant and set the related parameters.



6. Click Apply.

7.2.3 Create a SSID for the Employees

We have created a SSID in the basic configuration for the customers. Here we need to create another SSID for the employees to allow them to access the network without portal authentication. In addition, the new SSID should be invisible for the customers.

Follow the steps below to create a SSID for the employees.

1. Open the global configuration window and go to Wireless Settings > Basic Wireless Settings.

Blask, Initia		
SSID Name	55/02	
Band	📑 2.4GHz 🛄 SGHz	
Guest Network	🗌 Enable 🔘	
Security Mode	WPA.PSK +	
Wreless Password		
Advanced Settings		

2. Click Add to add a new SSID.

Configure the parameters.

- 1) Disable the SSID Broadcast to hide this SSID from the customers.
- Specify the SSID Name, Security Mode and Wireless Password. Let the employees manually enter the SSID name and password, and choose the security mode you set to access the network.
- 3) Click Apply to save the configuration.

7.2.4 Configure Scheduler

Follow the steps below to schedule the radio to operate only during the working time (from 8:00 to 22:00).

- 1. Open the global configuration window and go to Wireless Control > Scheduler.
 - 1) Add a profile.

Add a Frofile		0
Produ Banna	We keep the lat	
Apply		

2) Add an item for the profile. The parameters are set as shown on the following screen.

Add an Item							0
Day Mode:	O Weekday	C Wee	kend 🛞 L	Lvoryday	O Custo	m	
	🖂 Muri - 🗹	Tue 🖂 V	//ed _ ⊴ Thu	🖂 Fri	⊴́ Sat	🖂 Sun	
Тітін	🖂 all day 24	haurs					
Start Time	08 . .	00 y	,				
End Time	22 . .	00 y	-				
Apply							

2. Go to Scheduler Association tab.

1.65	ofen CORI		Prop. Aufternit		Internet I Intern		navites médica		i terrer in terrer [1]
white	i.	2.64							
and the	- Mode	Ann	castori === 5540		*				
_									
State of the local division of the local div									
	_	Delet in							
	1010	Debut		•					
0	100-12 1 550	10.15124	Dand		Protive Nam			Action	lating
		Harrie	Barel 2.45ec		Profile Nam	•		Radia OK +	
0	1 550	Horne (· Profile Nat			and the second second	01010-0

- 1) Enable the function and select Associated with SSID. Click Apply.
- 2) In the Profile Name column of both SSIDs, select the profile we just created.
- 3) In the Action column of both SSIDs, select Radio On.
- 4) Click Apply in the Setting column of both SSIDs.
- 5) Select **5GHz** and do the same configurations as above.

Appendix: Omada App

Omada app is a mobile application designed for Omada series EAP products. It allows you to conveniently monitor and manage your network. The Omada app can be used for Standalone and Controller modes.

This appendix introduces how to use Omada app to manage your network and includes the following sections:

- Install Omada App on the Mobile Device
- Manage your Network in Standalone Mode
- Manage your Network in Controller Mode

1 Install Omada App on the Mobile Device

Omada app runs on iOS and Android devices, such as smart phones and tablets. Launch the Apple App Store (iOS) or Google Play store (Android) and search "TP-Link Omada" or simply scan the QR code to download and install the app.

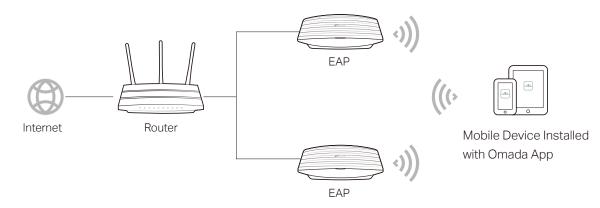


2 Manage your Network in Standalone Mode

For a relatively small-scale network which has a few EAPs (usually less than three) and only basic functions are required, standalone mode is recommended. You can use a mobile device to configure each EAP individually for basic functionality without configuring a Omada Controller. Note that the EAP which is managed by Omada Controller is inaccessible in standalone mode.

Refer to the topology below, make sure that the following requirements have been met:

- An Ethernet connection from your Omada EAP to the LAN with a DHCP server.
- The supported firmware version of the EAP. EAP245, EAP225, EAP115, EAP110, EAP225-Outdoor, EAP110-Outdoor, EAP115-Wall and EAP225-Wall are currently supported. To check the firmware versions of the supported EAPs, please refer to <u>www.tp-link.com/omada_</u> <u>compatibility_list</u>. More products will be supported by Omada app in the near future as firmware updates are released.
- A compatible iOS or Android device with Omada app.

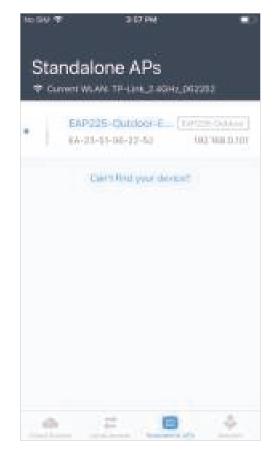


Follow the steps below to manage your network via Omada app in standalone mode. The following page is exampled with the iOS version of the app. The Android version is similar.

 Connect your mobile device to the EAP by using the default SSID (format: TP-Link 2.4GHz/5GHz_XXXXX) printed on the label.



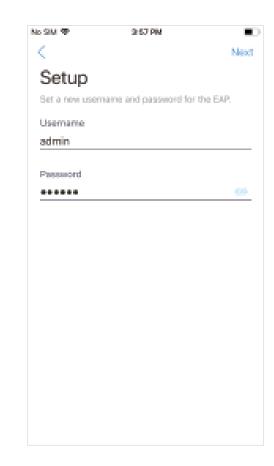
Launch the Omada app, tap Standalone
 APs and wait for the EAP device to be discovered.



Tips:

All the EAP devices in the same subnet will be discovered by Omada app and shown on the page. You can tap the discovered EAP device to configure directly.

 Tap on the EAP device appearing on the page. Set a new username and password for your login account of the EAP.



 Edit the default SSID and password to keep your wireless network secure. Tap Next.



Note:

The settings will take effect after several minutes. For operation system differences, the wireless network connection will be different. When the default SSID of the EAP device is changed, normally mobile device join the new wireless network automatically. For the unsupported operation system, you should manually connect to the new SSID.

5. You can view the name of the EAP device and other information including wireless parameters and clients. And you can tap to change the settings of radio, SSID and device account.

њач е <	3:55 PM	-
	AP225-Outdoor AP225-Outloor	-EA-23
Overview		
IP Address 192.168.0.101		
MAC Addres EA-33-51-06		
Firmware Ve 1.3.0 Built 20	ension 180614 Aut. 50359	
Hardware Vi 1.0	ersion	
LED		
Witeless		
Radio		2

Tips:

- Omada app is designed to help you quickly configure some basic settings. For advanced configuration, you can use controller mode. And when your EAP is managed by the controller, you can not use standalone mode.
- In standalone mode, only one user is allowed to log in to the management page of the EAP at the same time. Thus the management web page of the EAP cannot be logged in to when using the Omada app and vice versa. Also only one user can log in to the EAP via Omada app.

3 Manage your Network in Controller Mode

For a large-scale network which has mass EAPs and advanced functions are required, controller mode is recommended. Controller mode allows you to configure and automatically synchronize unified wireless settings to all EAPs in the network.

Omada app offers a convenient way to access the Omada Controller and adopt EAPs. With Local Access and Cloud Access function on the Omada app, you can manage the controller at local and remote sites.

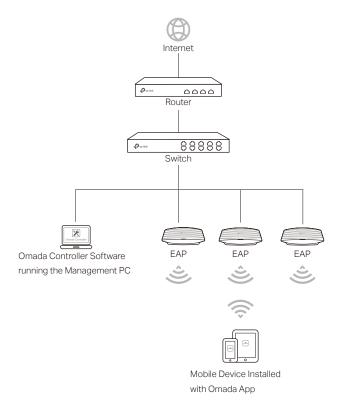
Note:

Omada Controller needs to be kept running when using Omada app to access the controller.

3.1 Locally manage your EAPs using the Omada App

Local Access function on Omada app is designed for accessing the controller which is in the same subnet with your mobile devices. Refer to the topology below, make sure that the following requirements have been met:

- An Ethernet connection from your Omada EAP to the LAN with a DHCP server.
- The version of the Omada Controller is 3.0.2 or above.
- A compatible iOS or Android device with Omada app.

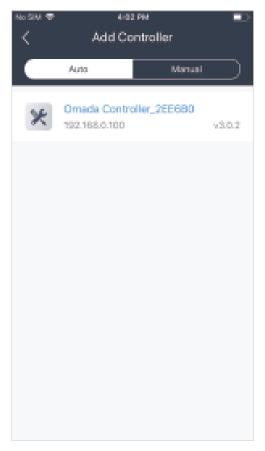


Follow the steps below to manage your network via Omada app in controller mode locally. The following page is exampled with the iOS version of the app. The Android version is similar.

 Connect your mobile device to the EAP by using the default SSID (format: TP-Link 2.4GHz/5GHz_XXXXX) printed on the label. Note that the EAP should be in the same subnet with the controller.



2. Launch the Omada app, go to Local Access, tap the + button on the upper-right corner to add the Omada controller. Normally Omada app will discover the controller which is in the same subnet. If the controller cannot be found, you can add the controller by entering the IP address and port of the controller host in the manual column.



3. Tap the Omada Controller, the controller login page will show. Enter the username and password of the controller, then tap **Log In** to launch the controller.

No SIM 👁	4/03 PM	
<		
Login		
	ge your controller.	
Usemanie		
admin		
Password		
*****		<u>6</u>
🛛 🛃 Auto Logi		
	Log in	

4. On the APs screen, tap the EAP that is pending for the adoption. And you can use the functions at the bottom to navigate various screens of the Omada Controller including the wireless statistics, clients information and basic settings.

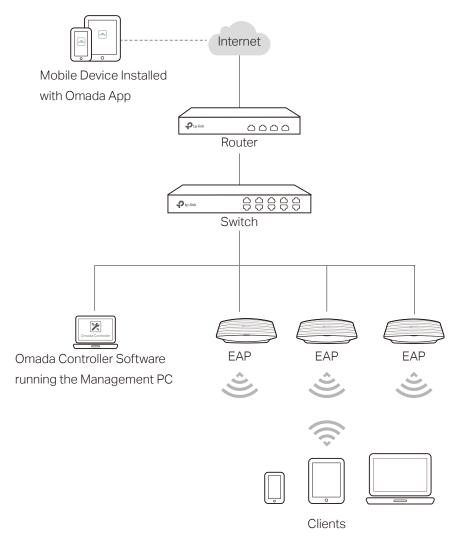


3.2 Remotely manage your EAPs using the Omada App

Cloud Access function on Omada app is designed for accessing the controller via Omada Cloud service. Thus, you can configure your controller and manage EAPs at any time, from anywhere.

Refer to the topology below, make sure that the following requirements have been met:

- Both your Controller Host and mobile device have internet access.
- The version of the Omada Controller is 3.0.2 or above.
- A compatible iOS or Android device with Omada app.
- Cloud Access is enabled on the controller. The controller has been bound with a TP-Link ID. For more details about the Cloud Access on the controller, refer to the <u>Omada Cloud Service</u>.



Follow the steps below to manage your network via Omada app in controller mode remotely. The following page is exampled with the iOS version of the app. The Android version is similar.

 Launch the Omada app, go to Cloud Access and tap Go to Log In to log in to Omada Cloud with your TP-Link ID.

ной у 🗢	4100 MM	•
<		
Login		
l og in talman	age yn i newr i'r len	
Uemane		
admin		
Pres word		
******		46
🔽 Arco Log	l T	
	Login	

 All the online controller which are bound with your TP-Link ID will appear on the page. Tap the controller to launch and configure the controller.



 On the APs screen, tap the EAP that is pending for the adoption. And you can use the functions at the bottom to navigate various screens of the Omada Controller including the wireless statistics, clients information and basic settings.



COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **Ptp-link** is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2019 TP-Link Technologies Co., Ltd. All rights reserved.