



i12 Wireless Access Point

User Guide

Copyright Statement

© 2017 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Tenda is a registered trademark legally held by Shenzhen Tenda Technology Co., Ltd. Other brand and

product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! Please read this user guide before you start with i12.

Conventions

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	System > Live Users
Parameter and value	Bold	Set User Name to Tom.
Variable	Italic	Format: XX:XX:XX:XX:XX:XX
UI control	Bold	On the Policy page, click the OK button.
Message	u »	The "Success" message appears.

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
₽TIP	This format is used to highlight a procedure that will save time or resources.

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
АР	Access Point
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMZ	Demilitarized Zone
DNS	Domain Name System
IPTV	Internet Protocol Television
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol

Acronym or Abbreviation	Full Spelling
MPPE	Microsoft Point-to-Point Encryption
РРР	Point To Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
РРТР	Point to Point Tunneling Protocol
SSID	Service Set Identifier
STB	Set Top Box
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WISP	Wireless Internet Service Provider
WPS	WiFi Protected Setup

Additional Information

For more information, search this product model on our website at http://www.tendacn.com.

Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.



Contents

1	Get to Know Your Device	7
	1.1 Overview	7
	1.2 Packing List	7
	1.3 Appearance	3
	1.3.1 LED Indicator	3
	1.3.2 Button and Port	3
	1.3.3 Label	Э
2	Installing the AP	1
	2.1 Preparing for Installation	1
	2.1.1 Precautions	1
	2.1.2 Preparing Tools12	1
	2.2 Installing the AP	1
	2.3 Connecting the Power Supply	5
	2.4 Connecting the AP	5
3	Managing the AP18	3
	3.1 Management Modes	3
	3.2 Logging In to the Web UI of the AP	3
	3.3 Logging Out of the Web UI of the AP 20	C
	3.4 Common Buttons on the Web UI	1
4	Functions	2
	4.1 Status	2
	4.1.1 System Status 22	2
	4.1.2 Wireless Status	2
	4.1.3 Traffic Statistics	3
	4.1.4 Client List	4
	4.2 Quick Setup	5
	4.2.1 AP Mode	5

	4.2.2 WDS Mode	
	4.2.3 AP+Client Mode	
4.	.3 Network Settings	
	4.3.1 LAN Setup	
	4.3.2 DHCP Server	
4.	.4 Wireless Settings	40
	4.4.1 Basic Settings	40
	4.4.2 Radio Settings	49
	4.4.3 Channel Scan	50
	4.4.4 Advanced Settings	52
	4.4.5 Access Control	54
	4.4.6 QVLAN Settings	56
4.	.5 SNMP	60
4.	.6 Tools	61
	4.6.1 Firmware Upgrade	61
	4.6.2 Date & Time	62
	4.6.3 Logs	65
	4.6.4 Configuration Management	68
	4.6.5 Accounts	71
	4.6.6 Diagnostics	73
	4.6.7 Reboot	73
	4.6.8 LED Control	76
Appen	dixes	77

1 Get to Know Your Device

1.1 Overview

i12 is a Tenda ceiling-mounted wireless access point (AP) that offers a wireless transmission capacity of up to 300 Mbps. It supports DC and PoE power supplies, and can be managed using the web UI of the AP or a Tenda AP controller (AC) such as M3. The AP is an optimum choice for providing wireless coverage in indoor areas such as enterprises, hotels, and restaurants.

The following table provides the specifications of i12.

Model	Product Name	Power Supply		
		DC	РоЕ	
i12	Wireless access point (25 clients)	12V 1A	IEEE 802.3at PoE	

1.2 Packing List

Tenda	Ceiling-mounted AP		Mounting bracket	Ethernet cable
Installation guide	Installation guide	(1030008)-	Screw x 4	Sleeve anchor x 4

1.3 Appearance

1.3.1 LED Indicator



LED Indicator	Status	Description	
System indicator	Solid on	The system is booting or faulty.	
	Blinking	The system is running properly.	
	Off	The system is powered off or the LED indicator is turned off.	

1.3.2 Button and Port



Reset button

After the AP is powered on, you can hold down this button for 8 seconds to restore the factory settings.

RJ45 port

This port is used to connect to a PoE power supply and exchange data.

Model	Rate	Connection Description
i12	10/100/1000 Mbps auto negotiation	If the AP is powered using a DC adapter, connect this port to a switch. If the AP must be powered through PoE, connect this port to an

Model	Rate	Connection Description
		IEEE 802.3at PoE switch.
		The AP allows a PoE power supply distance of not longer than 100 meters.

Power jack

The power jack is used to connect to a DC adapter for supplying power to the AP.

Model	Power Specifications		
	Input	Output	
i12	100V-240V, 50/60Hz AC	12V 1A DC	

1.3.3 Label

The label is located on the rear panel of the AP. For details of the label, see the following figure.





- (1): Name of the AP.
- (2): Model of the AP.

- (3): Default IP address of the AP. You can use this IP address to log in to the web UI of the AP.
- (4): Default user name and password of the web UI of the AP.
- (5): MAC address of the AP. The default primary SSID of the AP is Tenda_XXXXXX, where XXXXXX indicates the last 6 characters of this MAC address.
- (6): Serial number of the AP. If the AP is faulty, you need to provide this serial number when sending the AP for repair.

2 Installing the AP

2.1 Preparing for Installation

Before installing the AP, follow the instructions in this section to make preparation.

2.1.1 Precautions

To prevent damaging the AP or causing a personal injury, pay attention to the following precautions:

Ensure that the temperature and humidity requirements specified in the following table are met.

Environment	Temperature	Humidity
Operating environment	0°C - 45°C	10%RH - 90%RH (non-condensing)
Storage environment	-40°C - 70°C	5%RH - 90%RH (non-condensing)

- Ensure that the AP is mounted on a place free of accumulated water and water drips. Do not install the AP in a wet environment.
- Do not open or remove the housing of the AP.
- Keep the AP clean.
- Before cleaning the AP, disconnect it from the power supply. Do not scrub the AP with any liquid.

2.1.2 Preparing Tools

You may need a rubber hammer, a marker, a hammer drill, a spirit level, a measuring tape, a 6 mm drill bit, a Phillips screwdriver, ESD gloves, and a ladder during installation. Prepare them yourself.

	Rubber hammer		Marker	17	Hammer drill
P 0 11111	Spirit level	(D	Measuring tape		6 mm drill bit
	Phillips screwdriver	**	ESD gloves	A	Ladder

2.2 Installing the AP

Step 1 Place the mounting bracket onto the target position of the ceiling and mark the positions of the screw

holes.

If the AP is powered using a DC adapter, a receptacle must be available within 1 meter from the mounting position on the ceiling.



Step 2 Create holes in the marked positions. Each hole measures at 6 mm in diameter and 25 mm to 30 mm in depth.



Step 3 Use the rubber hammer to knock the sleeve anchors into the holes.



Step 4 Place the Ethernet cable (CAT5 or better cable) to be connected to the AP into the cable tray. If you use a DC adapter to supply power to the AP, place the power cable into the cable tray as well.



Step 5 Lead the screws through the screw holes of the mounting bracket into the sleeve anchors and use the Phillips screwdriver to fasten the screws.



Step 6 Connect the Ethernet cable to the RJ45 port. If you use a DC adapter to supply power to the AP, connect the power cable to the power jack of the AP.



Step 7 Insert the hooks of the AP inside the slots of the mounting bracket to fix the AP onto the mounting bracket.



2.3 Connecting the Power Supply

The AP can be powered using the DC adapter accompanying the AP or a piece of IEEE 802.3at PoE power supply equipment.



If you power the AP through PoE, connect the Ethernet cable (\leq 100 meters) connected to the RJ45 port of the AP to an IEEE 802.3at PoE switch.



After the AP is connected to a power supply, it initializes. During initialization, the LED indicator turns solid on for 5 to 7 seconds, and then blinks. When the indicator blinks, the AP is working properly.

2.4 Connecting the AP

If you need to install only a small number of APs, connect the APs using the following topology, which allows you to log in to the web UI of each AP to manage the AP.



If you need to install a large number of APs, connect the APs to an M3 (Tenda AC) using the following topology so that you can manage all the APs in a centralized manner.



3 Managing the AP

3.1 Management Modes

The AP can be managed on the web UI of the AP or using M3 (Tenda AC).

When the AP is connected to a network with M3, the AC automatically detects the AP. The AP can be used without being configured. You can log in to the web UI of the AC to manage the AP.

You can download the user guide for M3 from http://www.tendacn.com.

The following sections describe how to log in to the web UI of the AP to manage the AP.

3.2 Logging In to the Web UI of the AP

You can use a web browser to log in to the web UI of the AP. The following table provides default login information of the AP.

Parameter	Default Value
IP address	192.168.0.254
User name	admin
Password	admin

Procedure for logging in to the web UI using the default login information:

Step 1 Set IP address of your local area connection to 192.168.0.X (X: 2 - 253) and Subnet mask to 255.255.255.0.

Internet Protocol Version 4 (TCP/IPv4)	Properties 💦 🔀
General	
You can get IP settings assigned auton this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator
💿 Obtain an IP address automatical	у
• Use the following IP address:	
IP address:	192.168.0.10
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	
Obtain DNS server address autom	natically
• Use the following DNS server add	resses:
Preferred DNS server:	
<u>A</u> lternate DNS server:	
Validate settings upon exit	Ad <u>v</u> anced
	OK Cancel

Step 2 Access 192.168.0.254 using a web browser.



Step 3 Enter **admin** as the user name and password and click **Login**.

i12V1.0		
2	The default username is admin The default password is admin	
Q	English	
	Login	
	Forget your password?	

If this page is not displayed, refer to <u>Q1</u> in Appendix A "FAQ."

----End

You can view and modify the configuration of the AP on the web UI. For details about how to configure the AP, see <u>Chapter 4 "Functions."</u>

Te	e nd a			
				A durinistante un durin
৵	Status	System Status		Administrator.admin
	System Status Wireless Status	System Status		Help
	Traffic Statistics	Device Name	i12V1.0	
	Client List	System Time	2017-01-06 16:26:50	
\$	Quick Setup	Up Time	00h 00m 55s	
	Network	Wireless Clients	0	
(¢	Wireless	Firmware Version	V1.0.0.8(3856)	
*	SNMP	Hardware Version	V1.0	
ø,	Tools	LAN Status		
-		MAC Address	00:90:4C:12:46:4C	
		IP Address	192.168.0.254	
		Subnet Mask	255.255.255.0	
		Primary DNS Server	192.168.0.1	
		Secondary DNS Server		~

3.3 Logging Out of the Web UI of the AP

After you log in to the web UI of the AP, the system logs you out if you perform no operation on the web UI within the <u>client timeout interval</u>. (The default interval is 5 minutes and can be changed.)

When you close the web browser, the system logs you out as well.

When you are logged out, the system does not save the current configuration. Therefore, it is recommended that you save the current configuration before logging out.

If you close the web browser tab page used to log in to the web UI of the AP instead of the web browser, you are not logged out.

Web UI Layout

The web UI is composed of three parts, including the level-1 and level-2 navigation bar, level-3 navigation bar, and configuration area. See the following figure.

The functions and parameters dimmed on the web UI indicates that they are not supported by the AP or cannot be changed in the current configuration.

Te	enda				
		\frown	\		
4	Status	System Status)		Administrator:admin
	System Status				
	Wireless Status	System Status			Пер
	Traffic Statistics	Device Name	i12V1.0		
	Client List	System Time	2017-01-06 16:26:50		
\$	Quick Setup	Up Time	00h 00m 55s		
	Network	Wireless Clients	0		
(i:-	Wireless	Firmware Version	V1.0.0.8(3856)		
*	SNMP	Hardware Version	V1.0		
Ø,	Tools	LAN Status			
-	\bigcap	MAC Address	00:90:4C:12:46:4C		
		IP Address	192.168.0.254	\bigcirc	
		Subnet Mask	255.255.255.0	3	
		Primary DNS Server	192.168.0.1		
		Secondary DNS Server			~

No.	Name	Description	
1	Level-1 and level-2 navigation bar	The navigation bars display the function menu of the AP. When you select a function in navigation bar, the configuration of the	
2	Level-3 navigation bar	function appears in the configuration area.	
3	Configuration area	It enables you to view and modify configuration.	

3.4 Common Buttons on the Web UI

Description of common buttons

Button	Description
Refresh	It is used to update the content of the current page.
Save	It is used to save the configuration on the current page and enable the configuration to take effect.
Restore	It is used to change the current configuration on the current page back to the original configuration.
Help	It is used to view help information corresponding to the settings on the current page.

4 Functions

4.1 Status

4.1.1 System Status

To view the system status and LAN status of the AP, choose Status > System Status.

Te	enda					
<u>_</u>	Status	System Status		Ac	lministrator: admi	n
	System Status					^
	Wireless Status	System Status			Help	
	Traffic Statistics	Device Name	i12V1.0			
	Client List	System Time	2017-01-06 16:26:50			
\$	Quick Setup	Up Time	00h 00m 55s			
	Network	Wireless Clients	0			
Ŕ	Wireless	Firmware Version	V1.0.0.8(3856)			
*	SNMP	Hardware Version	V1.0			
Ø.	Tools	LAN Status				
~¢	10013	MAC Address	00:90:4C:12:46:4C			
		IP Address	192.168.0.254			
		Subnet Mask	255.255.255.0			
		Primary DNS Server	192.168.0.1			
		Secondary DNS Server				~

4.1.2 Wireless Status

To view the radio status, SSID status, and WDS status (available when the AP works in WDS mode) of the AP, choose **Status** > **Wireless Status**.

Tenda

- Status
System Status
Wireless Status
Traffic Statistics
Client List
 Quick Setup
Network
Manual
wireless
SNMP
Tools

4.1.3 Traffic Statistics

To view the total transmitted traffic, total received traffic, total number of transmitted packets, and total number of received packets corresponding to each SSID of the AP, choose **Status** > **Traffic Statistics**.

Te	enda						
*	Status	Traffic Statistics					Administrator:admin
-	System Status Wireless Status	SSID	Total RX Traffic (MB)	Total RX Packets	Total TX Traffic (MB)	Total TX Packets	Help
	Traffic Statistics Client List	Tenda_12464C	0.00MB	0	0.01MB	173	Refresh
4	Quick Setup	Tenda_12464E	0.00MB	0	0.00MB	0	_
	Network	Tenda_12464F	0.00MB	0	0.00MB	0	
<i></i> ≈	Wireless SNMP						
ಥ್	Tools						

You can click **Refresh** to view the latest traffic statistics.

4.1.4 Client List

To view the MAC address, IP address, connection uptime, transmit speed, and receive speed of each wireless client connected to the AP, choose **Status** > **Client List**.

Te	enda							
.∿	Status	Client List					A	dministrator:admin
	System Status	This section	on displays information o	f connected client	s.			Help
	Traffic Statistics	The conne	ected client list:		Ter	da_12464C	\checkmark	
4	Client List Quick Setup	ID	MAC Address	IP	Connection Duration	TX Rate	RX Rate	
۲	Network			No clients cor	nnected!			
(ķ	Wireless							
*	SNMP							
\$	Tools							

You can select an SSID from the drop-down list box in the upper-right corner to view information about the wireless clients connected to the AP using the SSID.

4.2 Quick Setup

Choose **Quick Setup**. The page displays the parameters that enable you to quickly configure the AP so that wireless clients can connect to the WiFi network of the AP and access the internet through the AP

Te	e n da				
*	Status	Quick Setup			Administrator:admin
4	Quick Setup	Mode (● AP Mode ○ WDS Mode	○ APClient Mode	Save
•	Network	SSID	Tenda_12464C		Restore
*	SNMP	Security Mode	None		Help
\$	Tools				

The AP can work in <u>AP</u>, <u>WDS</u>, or <u>AP+Client</u> mode. By default, it works in AP mode.

4.2.1 AP Mode

In this mode, the AP connects to the internet using an Ethernet cable and converts wired signals into wireless signals to provide wireless network coverage. The following figure shows the topology.



Procedure:

The Mixed WPA/WPA2-PSK security mode and AES encryption algorithm are used as an example to describe the configuration procedure. If you need to use another security mode, refer to <u>Section 4.4.1</u> <u>"Basic Settings."</u>

- **Step 1** Set **Mode** to **AP Mode**.
- **Step 2** (Optional) Set **SSID** to a wireless network name.
- **Step 3** Set **Security Mode** to **Mixed WPA/WPA2-PSK**, **Cipher Type** to **AES**, and **Security Key** to the password of the wireless network.
- Step 4 Click Save.

----End

4.2.2 WDS Mode

In this mode, the AP is used to set up a distributed wireless system that features broader wireless network coverage.

Te	enda				
		Quick Satur			Administrator:admin
≁	Status	<u>Quick Setup</u>			
\$	Quick Setup	Mode	○ AP Mode	APClient Mode	Save
	Network	SSID	Tenda_12464C		Restore
ŝ	Wireless	Security Mode	None]	Trestore
*	SNMP	MAC Address		(Status:Unknow)	Help
۵,	Tools	MAC Address		(Status:Unknow)	
		MAC Address		(Status:Unknow)	
		MAC Address		(Status:Unknow)	
		Remote AP's Network Mode			
		Remote AP's channel	Auto]	
		Remote AP's Channel			
		Remote AP's Extension			
		Channel	Fachie Sam		
			Enable Scan		
					~

WDS mode parameter description

Parameter	Description
Mode	It specifies the working mode of the AP. In WDS mode, the AP can be bridged with a maximum of 4 APs at the same time.
SSID	It specifies the SSID of a peer AP. You can click Enable Scan and select the SSID of the peer AP from the detected SSIDs.
Security Mode	It specifies the security mode of a peer AP. When you click Enable Scan and select the SSID of the peer AP from the detected SSIDs, the local AP automatically obtains related security settings (including Security Mode , Cipher Type , Authentication Type , and Default Key) of the peer AP except Security Key .
MAC Address	It specifies the MAC address corresponding to the SSID of a peer AP. When you click Enable Scan and select the SSID of the peer AP from the detected SSIDs, the local AP automatically sets the corresponding MAC Address parameter to the SSID of the peer AP.
Remote AP's channel	It specifies the channel of a peer AP. When you click Enable Scan and select the SSID of the peer AP from the detected SSIDs, the local AP automatically obtains related channel settings (including Remote AP's Network Mode, Remote AP's channel, Remote AP's Channel Bandwidth , and Remote AP's Extension Channel) of the peer AP.

Enable Scan	It is used to detect information about nearby wireless signals of wireless devices, including SSIDs, MAC addresses, network modes, signal bandwidth, channels, extension channels, security modes, and signal strength.

- The WDS function must be configured on all the APs to be bridged in WDS mode. All the APs must share the same SSID, channel, security mode, and security key.
- The APs to be bridged in WDS mode must be assigned different IP addresses belonging to the same network segment.

Example Application of the WDS Mode

An AP has been installed in a hotel. Nevertheless, the signal of the AP is weak in some rooms because of limited wireless coverage of the AP and blockage such as walls. As a result, guests in the rooms are unable to properly access the internet through the AP.

To improve the signal in the other rooms, you can install one AP in each room and use the additional APs to repeat the wireless signal of the original AP in WDS mode, so as to extend wireless coverage and enable guests in the rooms to properly access the internet.

1-to-1 WDS bridging

The following figure shows the topology.



Procedure:

Step 1 Log in to the web UI of AP1 and check the basic information about AP1. Assume that AP1 has the basic information described in the following table.

IP Address	SSID	Security Mode	Security Key (Wireless Network Password)
192.168.0.254	Tenda_1	Mixed WPA/WPA2-PSK	87654321

- Step 2 Log in to the web UI of AP2, change its IP address to an IP address that is different from the IP address of AP1 but belongs to the same network segment of AP1, such as 192.168.0.253. For details, refer to Section 4.3.1 "LAN Setup."
- **Step 3** Use the new IP address to log in to the web UI of AP2, and configure AP2 to repeat the wireless signal of AP1 in WDS mode.

1. Choose Quick Setup, set Mode to WDS Mode, and click Enable Scan.

Tenda				
A Status	Quick Setup			Administrator:admin
Quick Setup	Mode	○ AP Mode	PClient Mode	Save
 Wireless 	SSID	Tenda_12464C		Restore
X SNMP	MAC Address		(Status:Unknow)	Help
🍇 Tools	MAC Address		(Status:Unknow)	
	MAC Address MAC Address		(Status:Unknow) (Status:Unknow)	
	Remote AP's Network Mode			
	Remote AP's channel Remote AP's Channel Bandwidth Remote AP's Extension]	
	Channel	Enable Scan		
				~

- 2. Select the SSID of AP1 from the detected SSIDs. In this example, the SSID of AP1 is Tenda_1.
- **3.** Set **Security Key** to the wireless network password of AP1. In this example, the security key is 87654321.
- 4. Click Save.

The SSID of AP2 changes to the SSID of AP1 when the configuration is saved.

Tenda								
							Admir	istrator:admin
小 Status	Quick Setup							
💠 Quick Setup	Мос	de 🔿 AP Mode (WDS N	lode 🔿 AP(Client Mo	de		Save
Wetwork	SS	ID Tenda_1						Restore
🛜 Wireless	Security Mod	de Mixed WPA/WF	PA2 - PSK	~				
🗙 SNMP	Cipher Typ	De ⊛ AES ⊖ TK		CIP&AES				Help
🤹 Tools	Security K	ey 87654321						
	MAC Addre	ss C8:3A:35:11:11	:11		(Status:U	nknow)		
	MAC Addre	SS			(Status:U	nknow)		
	MAC Addre	55			(Status:U	nknow)		
	MAC Addre	ss			(Status:U	nknow)		
	Remote AP's Netwo Moo	rk bgn						
	Remote AP's chann	el 10		\checkmark				
	Remote AP's Chann Bandwid	el 20						
	Remote AP's Extensio	none						
	Chann	el)isable Sca	an				
	Select SSID	MAC Address	Networ Mode	c Channel Bandwidth	Channe	Extension Channel	Security	Signal Strength
	Tenda_1	C8:3A:35:11:11:11	bgn	20	10	none	wpa&wpa2/aes	-81dBm
	O : Tenda_009DB0	C8:3A:35:00:9D:B0	bgn	40	11	upper	none	-62dBm 🗸

Step 4 Log in to the web UI of AP1 and perform step 3 to configure AP1 to repeat the wireless signal of AP2 in WDS mode. After configuration is complete, Connected appears to the right of the corresponding MAC address, indicating that bridging is successful. See the following figure.

Te	enda				
		Quick Setup			Administrator:admin
Ŷ	Status	Quick Setup			
4	Quick Setup	Mode	○ AP Mode	PClient Mode	Save
۲	Network	SSID	Tenda_1		Pestara
((:-	Wireless	Security Mode	Mixed WPA/WPA2 - PSK		Restore
*	SNMP	Cipher Type	● AES _ TKIP _ TKIP&AES		Help
۵,	Tools	Security Key	87654321]	
		MAC Address	C8:3A:35:11:11:11	(Status: Connected)	
		MAC Address		(Status:Unknow)	
		MAC Address		(Status:Unknow)	
		MAC Address		(Status:Unknow)	
		Remote AP's Network Mode	bgn]	
		Remote AP's channel	1]	
		Remote AP's Channel Bandwidth	20]	
		Remote AP's Extension Channel	none]	

----End

1-to-many (maximum: 4) WDS bridging

The following figure shows the topology.



Procedure:

Step 1 Log in to the web UI of AP1 and check the basic information about AP1. Assume that AP1 has the basic information described in the following table.

IP Address	SSID	Security Mode	Security Key (Wireless Network Password)
192.168.0.254	Tenda_1	Mixed WPA/WPA2-PSK	87654321

The IP addresses of AP2, AP3, AP4, and AP5 must be different from the IP address of AP1 but belong to the same network segment as the IP address of AP1. For example, you can set them to 192.168.0.2, 192.168.0.3, 192.168.0.4, and 192.168.0.5.

- **Step 2** Log in to the web UIs of AP2, AP3, AP4, and AP5, change the LAN port IP addresses of the APs, and configure the APs to repeat the wireless signal of AP1 in WDS mode. For details about the wireless signal repeating, refer to step <u>3</u> in 1-to-1 WDS bridging.
- **Step 3** Log in to the web UI of AP1 and configure AP1 to repeat the wireless signals of the other APs.
 - 1. Choose Quick Setup, set Mode to WDS Mode, and click Enable Scan.
 - 2. Select the entries of AP2, AP3, AP4, and AP5 on the scan result list. (The SSIDs of the APs on the list are the same as the SSID of AP1, which is Tenda_1 in this example.)
 - 3. Set Security Key to the wireless network password of AP1, which is 87654321 in this example.
 - 4. Click Save.

Te	enda											
		Ouid	:k Setup							Admin	istrator:adm	in
^ -	Status Quick Setup		Mod	le	() AP Mode	WDS	Mode () AP	Client Mo	de		Save	^
۲	Network		SSI	D	Tenda_1						Restore	
Ģ	Wireless		Security Mod	le	Mixed WPA/	WPA2 - PSI	< 🗸					
*	SNMP		Cipher Typ	e	● AES ○	TKIP ()	TKIP&AES				Help	
۵,	Tools		Security Ke	ey.	87654321							
			MAC Addres	55	C8:3A:35:22	22:22		(Status:U	Inknow)			
			MAC Addres	55	C8:3A:35:33	33:33	(Status:Unknow)					
			MAC Addres	55	C8:3A:35:44	i:44:44:44 (Status:Unknow)						
			MAC Addres	55	C8:3A:35:55	55:55	5:55 (Status:Unknow)					
		R	emote AP's Networ Mod	rk le	bgn							
			Remote AP's channe	el	10		\checkmark					
		F	Remote AP's Channe Bandwidt	el :h	20							
		Re	emote AP's Extensio	n	none							
			citati	-		Disable So	an					
		Select	SSID	м	AC Address	Netwo Mode	rk Channel Bandwidth	Channe	Extension Channel	Security	Signal Strength	
		0	Tenda_1	C8:3	A:35:22:22:2	2 bgn	20	10	none	wpa&wpa2/aes	-81dBm	
		0	Tenda_1	C8:3	A:35:33:33:3	3 bgn	20	10	none	wpa&wpa2/aes	-62dBm	~
		0	Tenda_1	C8:3	A:35:44:44:4	4 bgn	20	10	none	wpa&wpa2/aes	-81dBm	
		۲	Tenda_1	C8:3	A:35:55:55:5	5 bgn	20	10	none	wpa&wpa2/aes	-62dBm	

----End

After configuration is complete, Connected appears to the right of the corresponding MAC addresses, indicating that bridging is successful. See the following figure.

Te	enda				
					Administrator:admin
-∿-	Status	Quick Setup			
4	Quick Setup	Mode	○ AP Mode	PClient Mode	Save
•	Network	SSID	Tenda_1]	Bustan
ę	Wireless	Security Mode	Mixed WPA/WPA2 - PSK]	Restore
*	SNMP	Cipher Type	● AES ○ TKIP ○ TKIP&AES		Help
್ಮ	Tools	Security Key	87654321]	
		MAC Address	C8:3A:35:22:22:22	(Status: Connected)	
		MAC Address	C8:3A:35:33:33:33	(Status: Connected)	
		MAC Address	C8:3A:35:44:44	(Status: Connected)	
		MAC Address	C8:3A:35:55:55	(Status: Connected)	
		Remote AP's Network Mode	bgn]	
		Remote AP's channel	10		
		Remote AP's Channel Bandwidth	20]	
		Remote AP's Extension Channel	none]	

4.2.3 AP+Client Mode

In this mode, you can enable this AP to repeat the wireless signal of a peer AP for broader wireless network coverage simply by configuring this AP.

Te	enda				
*	Status	Quick Setup			Administrator:admin
4	Quick Setup	Mode	○ AP Mode ○ WDS Mode	APClient Mode	Save
۲	Network	SSID	Tenda_123456		Restore
(î:-	Wireless	Security Mode	None		Restore
*	SNMP	Remote AP's channel	Auto	\checkmark	Help
ø,	Tools		Enable Scan		

Example Application of the AP+Client Mode

An AP has been installed in a restaurant. Nevertheless, the signal of the AP is weak in some rooms because of limited wireless coverage of the AP and blockage such as walls. As a result, guests in the rooms are unable to properly access the internet through the AP.

To improve the signal in the rooms, you can install one or more APs and use the additional APs to repeat the wireless signal of the original AP in AP+Client mode, so as to extend wireless coverage and enable guests in the rooms to properly access the internet.

The following figure shows the topology.



Procedure:

Step 1 Log in to the web UI of AP1 and check the basic information about AP1. Assume that AP1 has the basic information described in the following table.

IP Address	SSID	Security Mode	Security Key (Wireless Network Password)
192.168.0.254	Tenda_1	Mixed WPA/WPA2-PSK	87654321

- Step 2 Log in to the web UI of AP2, change its IP address to an IP address that is different from the IP address of AP1 but belongs to the same network segment of AP1, such as 192.168.0.253. For details, refer to Section 4.3.1 "LAN Setup."
- **Step 3** Use the new IP address to log in to the web UI of AP2, choose **Quick Setup**, set **Mode** to **APClient** mode, and click **Enable Scan**.

Tenda		
♣ Status	Quick Setup	Administrator:admin
💠 Quick Setup	Mode 🔿 AP Made 🔿 WDS Made 🕥 APClient N	Inde Save
Metwork	SSID Tenda_123456	Bostoro
🛜 Wireless	Security Mode None	Residie
X SNMP	Remote AP's channel Auto	Help
🖏 Tools	Enable Scan	

- Step 4 Select the SSID of AP1 from the detected SSIDs. In this example, the SSID of AP1 is Tenda_1.
- **Step 5** Set **Security Key** to the wireless network password of AP1, which is **87654321** in this example.
- Step 6 Click Save.

Te	enda									
M	Status	Quic	k Setup						Admin	istrator:admi
4	Quick Setup		Mod	e 🔿 AP Mode		1ode 💿 APC	Client Mod	de		Save
€	Network Wireless		SSID Tenda_1 Security Mode Mixed WPA/WPA2 - PSK					Restore		
* *	SNMP Tools		Cipher Typ Security Ke	е	IP () T	KIP&AES				Неір
		F	Remote AP's channe	el 10)isable Sca	an				
		Select	SSID	MAC Address	Networ Mode	k Channel Bandwidth	Channe	Extension Channel	Security	Signal Strength
		0	Tenda_5D7AA0	C8:3A:35:5D:7A:A0	bgn	40	11	upper	none	-44dBm
		۲	Tenda_1	C8:3A:35:11:11:11	bgn	20	10	none	wpa&wpa2/aes	-67dBm

----End

After AP2 repeats the wireless signal of AP1, wireless devices such as smart phones can search for and connect to the wireless signal of AP2, and access the internet through AP2. (In this example, the SSID of AP2 is Tenda_123456.)

4.3 Network Settings

4.3.1 LAN Setup

To view the MAC address, device name, IP address obtaining mode, and other related information of the LAN port of the AP, choose **Network** > LAN Setup.

Te	enda				
*	Status	LAN Setup			Administrator:admin
\$≻ ⊕	Quick Setup Network	MAC Address	00:90:4C:12:46:4C		Save
	LAN Setup DHCP Server	IP Address Subnet Mask	192.168.0.254 255.255.255.0	For example: 192.168.1.1 For example: 255.255.255.0	Restore
≈ *	Wireless SNMP	Gateway Primary DNS Server	192.168.0.1		
¢,	Tools	Secondary DNS Server Device Name	i12V1.0	(optional)	
		Ethernet Mode	●Auto-negotiation○10M half-du	ıplex	

The AP supports the Static IP and Dynamic IP modes for obtaining an IP address for the LAN port.

If you change the IP address of the LAN port, change the IP address of your management computer as well so that the two IP addresses belong to the same network segment. Then, use the new IP address of the LAN port to log in to the web UI of the AP.

IP Address Obtaining Mode – Static IP

This mode enables you to set the IP address, subnet mask, gateway IP address, primary DNS server, and secondary DNS server of the AP. It is applicable to a scenario with only one or a few APs.

Procedure:

Assume that the AP IP address is 192.168.1.254, and the default gateway IP address and DNS server IP address are 192.168.1.1.

- **Step 1** Set Address Mode to Static IP.
- Step 2 Set IP Address.
- Step 3 Set Subnet Mask to the subnet mask of the IP address. Generally the subnet mask is 255.255.255.0.
- **Step 4** Set **Gateway** to the IP address of the gateway of the AP.
- **Step 5** Set **Primary DNS Server** to the IP address of the primary DNS server of the AP. If another DNS server is available, set **Secondary DNS Server** to the IP address of the additional DNS server.

Step 6 Click Save.

enda				
♣ Status	LAN Setup			Administrator:adm
 Quick Setup Network 	MAC Address	00:90:4C:12:46:4C	1	Save
LAN Setup DHCP Server	IP Address	192.168.1.254	For example: 192.168.1.1	Restore Help
WirelessSNMP	Gateway	192.168.1.1	Por example: 235.235.255.0	
😋 Tools	Secondary DNS Server		(optional)	
	Ethernet Mode	●Auto-negotiation○10M half-du	uplex	

IP Address Obtaining Mode – Dynamic IP

This mode enables the AP to automatically obtain an IP address, subnet mask, gateway IP address, primary DNS server IP address, and secondary DNS server IP address from a DHCP server in the network. If a large number of
APs are deployed, you can adopt this mode to prevent IP address conflicts and effectively reduce your workload.

Procedure:

- **Step 1** Set Address Mode to Dynamic IP.
- Step 2 Click Save.

Te	enda			
h	Status	LAN Setup		Administrator:admin
4	Quick Setup	MAC Address	00:90:4C:12:46:4C	Save
۲	Network	Address Mode	Dynamic IP	Restore
	LAN Setup DHCP Server	Device Name		Help
((t:	Wireless	Ethemet wode	CAuto-negotiation	
*	SNMP	_		
¢,	Tools			



Parameter Description

Parameter	Description
MAC Address	It specifies the MAC address of the LAN port of the AP. The default primary SSID of the AP is Tenda_ <i>XXXXXX</i> , where <i>XXXXXX</i> indicates the last 6 characters of this MAC address.
Address Mode	 It specifies the IP address obtaining mode of the AP. The default option is Static IP. Static IP: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is set manually. Dynamic IP: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is obtained from a DHCP server in your LAN. If Address Mode is set to Dynamic IP, you can log in to the web UI of the AP only with the IP address assigned to the AP by the DHCP server. The IP address is specified on the client list of the DHCP server.
IP Address	It specifies the IP address of the AP if Address Mode is set to Static IP . The default IP address is 192.168.0.254 and you can change it as required. Image: It is IP address also functions as the management IP address of the AP. You can use this IP address to log in to the web UI of the AP to manage the AP.
Subnet Mask	It specifies the subnet mask of the IP address of the AP if Address Mode is set to Static IP . The default subnet mask is 255.255.255.0 and you can change it as required.
Gateway	It specifies the gateway of the AP if Address Mode is set to Static IP. The default

Parameter	Description
	gateway IP address is 192.168.0.1 and you can change it as required.
Primary DNS Server	It specifies the primary DNS server of the AP if Address Mode is set to Static IP . The default IP address of the primary DNS server is 192.168.0.1 and you can change it as required.
Secondary DNS Server (optional)	It specifies the secondary DNS server of the AP if Address Mode is set to Static IP . This IP address is optional.
Device Name	It specifies the device name of the AP. The default device name is in the format of <i>Model+Hardware version number</i> . You are recommended to change the device name so that you can quickly locate the
	AP when managing the AP remotely.

4.3.2 DHCP Server

DHCP Server

The DHCP server function of the AP can automatically assign IP addresses to clients connected to the AP. To configure the function, choose **Network** > **DHCP Server**.

Te	enda				
					Administrator:admin
\mathbf{r}	Status	DHCP Server DHCP C	lient List		
\$	Quick Setup	DHCP Server	Enable		Save
۲	Network	Start IP	192.168.0.100		Postero
	LAN Setup	End IP	192.168.0.200		Resole
	DHCP Server	Lease Time	1 dav		Help
((ı:	Wireless	Subnet Mask	255.255.255.0		
*	SNMP	Gateway	192.168.0.254		
۵,	Tools	Primary DNS Server	192.168.0.254		
		Secondary DNS Server		(optional)	

Procedure for enabling and configuring the DHCP server function:

- **Step 1** Select the **Enable** check box of **DHCP Server**.
- **Step 2** Set **Start IP** to the start IP address of the IP address pool, which contains the IP addresses that can be assigned by the DHCP server to clients.
- **Step 3** Set **End IP** to the end IP address of the IP address pool.
- **Step 4** Set **Lease Time** to the time when an IP address is available to a client. The default option **1 day** is recommended.
- Step 5 Set Subnet Mask to the subnet mask of the IP addresses. The default value 255.255.255.0 is recommended.

- **Step 6** Set **Gateway** to the gateway IP address to be assigned by the DHCP server to clients.
- **Step 7** Set **Primary DNS Server** to the IP address of the primary DNS server assigned by the DHCP server to clients. If another DNS server IP address is available, set **Secondary DNS Server** to that IP address.

Step 8 Click Save.

----End

If another DHCP server is available in your LAN, ensure that the IP address pool of the AP does not overlap the IP address pool of that DHCP server. Otherwise, IP address conflicts may occur.

Parameter description

Parameter	Description
DHCP Server	It specifies whether to enable the DHCP server function. To enable it, select the check box. To disable it, deselect the check box. By default, it is disabled.
Start IP	It specifies the first IP address that can be assigned by the DHCP server to a client. The default value is 192.168.0.100 .
End IP	It specifies the last IP address that can be assigned by the DHCP server to a client. The default value is 192.168.0.200 .
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. The default value is 1 day .
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to clients. The default value is 255.255.255.0 .
Gateway	It specifies the gateway IP address assigned by the DHCP server to clients. The default value is 192.168.0.254 . When a client accesses a server or host located outside the network segment where the client resides, the data from and to the client must be forwarded by the gateway. Generally, the IP address of the gateway is the LAN IP address of the router in your LAN.
Primary DNS Server	It specifies the primary DNS server IP address assigned by the DHCP server to clients. The default value is 192.168.0.254 . IDE To enable clients to access web pages using domain names, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server (optional)	It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This IP address is optional.

DHCP Client List

To view information about the clients that obtain IP addresses from the DHCP server function of the AP, choose **Network** > **DHCP Server** and click the **DHCP Client List** tab.

Te	enda						
						۸dm	inistratoradmin
৵	Status	DHCP S	erver DHCP Client List			Auto	inistrator.aumin
\$	Quick Setup	Once D	HCP is enabled, client list will	be refreshed automatic	ally every five seconds.	Refresh	
	Network					rteireen	
	LAN Setup	ID	Hostname	IP Address	MAC Address	Lease Time	
	DHCP Server	1	android-e4b0b4f2d626	192.168.0.164	00:66:4b:7c:7b:14	23:59:46	
((ŗ	Wireless		· · · · · · · · · · · · · · · · · · ·				,
*	SNMP						
ø,	Tools						

You can click **Refresh** to view the latest client information.

4.4 Wireless Settings

4.4.1 Basic Settings

To view basic wireless settings of the AP, choose **Wireless** > **Basic**.

Te	enda				
M	Status	Basic			Administrator:admin
\$	Quick Setup	SSID	Tenda_123456		Save
	Network	Enable	2		Restore
((ŗ	Wireless	Broadcast SSID	Enable	\checkmark	TROSPICE
	Basic	AP isolation	Disable O Enable		Help
	Radio	WMF	Disable O Enable		
	Site Survey Advanced	Client limit	16	(Rangle:1-64)	
	Access Control	SSID	Tenda_123456		
	QVLAN	Chinese SSID Encode	UTF-8	\checkmark	
*	SNMP	Security Mode	None	~	
ø,	Tools				
		1			

Procedure:

If there is no special requirement regarding the parameters not described in this procedure, retain the default settings.

- **Step 1** Select the SSID to be configured from the **SSID** drop-down list box.
- **Step 2** Select the **Enable** check box to enable the selected SSID.
- **Step 3** Set **Client limit** to the maximum number of wireless clients that can be connected to the AP using the selected SSID.
- **Step 4** Change the value of the **SSID** text box to a required wireless network name.
- **Step 5** (Skip this step if your SSID does not include Chinese characters.) Set **Chinese SSID Encode** to an encoding format of the Chinese characters in your SSID.
- **Step 6** Select a security mode from the **Security Mode** drop-down list box for your SSID. For the detailed security mode configuration procedure, refer to <u>Security Mode</u>.
- Step 7 Click Save.

----End

Parameter description

Parameter	Description
SSID	It specifies the SSID to be configured. The AP allows 4 SSIDs. The default SSID is the primary SSID of the AP, which is Tenda_XXXXXX, where XXXXXX indicates the last 6 characters in the MAC address specified on the label on the external surface of the AP.
Enable	It specifies whether to enable the selected SSID. By default, the primary SSID is enabled and the other SSIDs are disabled. You can enable them as required.
Broadcast SSID	 It specifies whether to broadcast the selected SSID. Enable: It indicates that the AP broadcasts the SSID and the SSID can be detected by clients. Disable: It indicates that the AP does not broadcast the SSID and the SSID cannot be detected by clients. If a user wants to connect to the wireless network corresponding to this SSID, the user must enter the SSID manually. It is AP can automatically hide its SSID. When the number of clients connected to the AP with an SSID of the AP reaches the <u>upper limit</u>, the AP stops broadcasting the SSID.
AP isolation	 It specifies whether to isolate the wireless clients connected to the AP with the selected SSID. Enable: It indicates that the wireless clients connected to the AP with the selected SSID cannot communicate with each other. This improves wireless network security. Disable: It indicates that the wireless clients connected to the AP with the selected SSID can communicate with each other.
WMF	It specifies whether to forward multicast packets through unicast tunnels. Generally, multicast packets are usually transmitted at the lowest rate, such as 1 Mbps, leading to poor transmission efficiency. WMF leverages the high auto-negotiated rate, reliable feedback mechanism, and other advantages of unicast packets to address multicast problems such as video playback stalls caused by packet loss and long delays over a

Parameter	Description
	wireless network.
Client limit	It specifies the maximum number of wireless clients that can connect to the AP with the selected SSID.
	After this upper limit is reached, the AP rejects new connection requests from clients.
SSID	It enables you to change the selected SSID. Chinese characters are allowed in an SSID.
Chinese SSID	It specifies the encoding format of Chinese characters in an SSID. The default value is UTF8 .
Encode	If 2 or more SSIDs of the AP are enabled, you are recommended to set this parameter to UTF-8 for some SSIDs and to GB2312 for the other SSIDs, so that any wireless client can identify one or both SSIDs that contain Chinese characters.
Security Mode	It specifies the encryption type of the selected SSID. None indicates that any wireless client can connect to the AP using the selected SSID. This option is not recommended because it affects network security.
	The AP supports the WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2 security modes, which are elaborated in the following section.

WEP

Wired Equivalent Privacy (WEP) uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. If this encryption algorithm is used, the AP can reach a maximum wireless transmission rate of 54 Mbps.

WEP supports the Open, Shared, and 802.1x encryption types.

Security Mode	WEP		
Encryption Type	Open Shared		
Default Key	802.1x		
WEP Key 1	12345	ASCII	~
WEP Key 2	12345	ASCII	\checkmark
WEP Key 3	12345	ASCII	~
WEP Key 4	12345	ASCII	\checkmark

Many smart phones can use only WEP key 1 to connect to a WEP-encrypted wireless network with the encryption type being Open or Shared. Therefore, if **Security Mode** is set to **WEP** and **Encryption Type** is set to **Open** or **Shared**, set **Default Key** to the value of **WEP Key 1**.

Procedure for configuring the basic wireless settings with the authentication type being Open or Shared:

Assume that WEP key 1 is the default WEP key and the key is set to 54321 and ASCII.

- **Step 1** Select the SSID to be configured from the SSID drop-down list box, such as **Tenda_123456**.
- **Step 2** Set **Security Mode** to **WEP**.
- **Step 3** Set **Encryption Type** to **Open** or **Shared**.
- **Step 4** Set **Default Key** to **Security Key 1**.
- Step 5 Set WEP Key 1 to 54321 and ASCII.
- Step 6 Click Save.

Tenda				
A. Chature	Basic			Administrator:admin
→ Status				^
分 Quick Setup	SSID	Tenda_123456		Save
Metwork	Enable	V		Restore
🛜 Wireless	Broadcast SSID	Enable	\checkmark	ricolor o
Basic	AP isolation	Disable Disable		Help
Radio	WMF	Disable Disable		
Site Survey	Client limit	16	(Rangle:1-64)	
Advanced	SSID	Tenda_123456		
Access Control	Chinese SSID Encode	UTF-8		
X SNMP	Security Mode	WEP		
🖏 Tools	Encryption Type	Shared		
•	Default Key	Security Key 1		
	WEP Key 1	54321	ASCII 🔽	
	WEP Key 2	12345	ASCII 🔽	
	WEP Key 3	12345	ASCII 🔽	
	WEP Key 4	12345	ASCII 🔽	
				~

----End

Procedure for configuring the basic wireless settings with the authentication type being 802.1x:

Assume that the IP address, port number, and password of the RADIUS server are 192.168.0.88, 1812, and 12345678 respectively.

- **Step 1** Select the SSID to be configured from the SSID drop-down list box, such as **Tenda_123456**.
- **Step 2** Set **Security Mode** to **WEP**.
- **Step 3** Set **Encryption Type** to **802.1x**.
- Step 4 Set RADIUS Server to the IP address 192.168.0.88 of the RADIUS server.
- Step 5 Set RADIUS Port to the authentication port number 1812 of the RADIUS server.

- **Step 6** Set **RADIUS Password** to the password **12345678** of the RADIUS server.
- Step 7 Click Save.

				Administrator:a
Status	Basic			
Quick Setup	SSID	Tenda_123456		Save
Network	Enable	2		Postoro
Wireless	Broadcast SSID	Enable	\checkmark	T CSLOTE
Basic	AP isolation	Disable Disable		Help
Radio	WMF	Disable Disable		
Site Survey	Client limit		(Panale(1-64))	
Advanced	Client limit	10	(Nangle.1-04)	
Access Control	SSID	Tenda_123456		
QVLAN	Chinese SSID Encode	UTF-8	\checkmark	
SNMP	Security Mode	WEP		
Tools	Encryption Type	802.1x	\checkmark	
	RADIUS Server:	192.168.0.88		
	RADIUS Port:	1812	(Rangle: 1-65535,default: 1812	0
	RADIUS Password:	•••••		

---End

WEP parameter description

Parameter	Description
Encryption Type	It specifies the encryption type for the WEP security mode of the AP. The options include Open , Shared , and 802.1x . The options share the same encryption process.
Open	It specifies that authentication is not required if the WEP security mode is used. In this case, a wireless client can connect to the AP without being authenticated, and the data exchanged between them is encrypted in WEP security mode.
Shared	It specifies that a shared key is used for authentication if the WEP security mode is used. In this case, a wireless client must use a preset WEP key to connect to the AP. The wireless client can be connected to the AP only if the WEP key is the same as that of the AP.
802.1x	It specifies that 802.1x authentication is required if the WEP security mode is used. In this case, ports are enabled when authenticated clients connect to the AP, and disabled when non-authenticated users connect to the AP.
Default Key	It specifies the default WEP key for the Open and Shared encryption types. For example, if the default key is set to WEP key 2, a wireless client can connect to the

Parameter	Description
	AP only with WEP key 2.
ASCII	It allows 5 or 13 ASCII characters in a WEP key.
Hex	It allows 10 or 26 hexadecimal characters in a WEP key.
RADIUS Server	It specifies the IP address of the RADIUS server for authentication.
RADIUS Port	It specifies the port number of the RADIUS server for authentication.
RADIUS Password	It specifies the password of the RADIUS server for authentication.

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK

WPA-PSK is formulated based on IEEE 802.11i draft 3, whereas WPA2-PSK is formulated based on the final IEEE 802.11i release. Therefore, WPA2-PSK features higher security than WPA-PSK.

Both WPA-PSK and WPA2-PSK adopt a preshared key for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes WPA-PSK and WPA2-PSK suitable for ensuring security of home wireless networks. Nevertheless, because the initial preshared key for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes WPA-PSK and WPA2-PSK not suitable for scenarios where high security is required.

Chinese SSID Encode	None	
Security Mode	WPA - PSK	
Cipher Type	Mixed WPA/WPA2 - PSK WPA WPA	
Key	12345676	
Key Update Interval	0	(Range: 0 or 60—999999 seconds.)

Procedure for configuring the WPA-PSK, WPA2-PSK, or Mixed WPA/WPA2-PSK security mode:

Assume that Cipher Type and Key are AES and 87654321 respectively.

- **Step 1** Select the SSID to be configured from the SSID drop-down list box, such as **Tenda_123456**.
- **Step 2** Set **Security Mode** to **Mixed WPA/WPA2-PSK**, **WPA-PSK**, or **WPA2-PSK**.
- **Step 3** Set **Cipher Type** to **AES**.
- **Step 4** Set **Key** to **87654321**.
- Step 5 Click Save.

Te	enda			
*	Status	Basic		Administrator: admin
 ◆	Quick Setup Network	SSID	Tenda_123456	Save
(îŗ	Wireless Basic	Broadcast SSID AP isolation		Restore
	Radio Site Survey	WMF Client limit	Disable C Enable)
	Access Control QVLAN	SSID Chinese SSID Encode	Tenda_123456	
* *	SNMP Tools	Security Mode Cipher Type	Mixed WPA/WPA2 - PSK	
		Key Update Interval	0 (Range: 0 o	r 60—99999 seconds.)

----End

Parameter description

Parameter	Description
Security Mode	It specifies the encryption type of the selected SSID. Select WPA-PSK , WPA2-PSK , or Mixed WPA/WPA2-PSK .
WPA-PSK	This encryption type supports the AES and TKIP encryption algorithms.
WPA2-PSK	This encryption type supports the AES, TKIP, and TKIP&AES encryption algorithms.
Mixed WPA/WPA2-PSK	It indicates that the AP works in the Mixed WPA/WPA2-PSK security mode, and wireless clients adopting the WPA-PSK or WPA2-PSK security mode can connect to the AP.
Cipher Type	It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK , this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK , this parameter has the AES , TKIP , and TKIP&AES values.
AES	It is short for Advanced Encryption Standard. If this encryption algorithm is used, the AP can reach a maximum wireless transmission rate of 300 Mbps.
ТКІР	It is short for Temporal Key Integrity Protocol. If this encryption algorithm is used, the AP can reach a maximum wireless transmission rate of 54 Mbps.
TKIP&AES	It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the AP based on TKIP or AES.
Кеу	It specifies a preshared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.

Parameter	Description
Key Update Interval	It specifies the automatic update interval of the key for data encryption. A shorter interval results in higher data security.

WPA and WPA2

To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate data encryption—oriented root keys. WPA and WPA2 use the root keys to replace the preshared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

WPA and WPA2 uses 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage. In addition, each time a client connects to the AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the client. This makes it difficult for attackers to obtain the key. These features of WPA and WPA2 help significantly increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.

SSID	None WEP	
Chinese SSID Encode	WPA - PSK WPA2 - PSK	
Consults Mode	Mixed WPA/WPA2 - PSK	
Security Mode	WPA WPA2	
RADIUS Server:	192.168.0.88	
RADIUS Port:	1812	(Rangle: 1-65535,default: 1812)
RADIUS Password:	•••••	
Cipher Type	● AES ○ TKIP ○ TKIP&AES	
Key Update Interval	0	(Range: 0 or 60—999999 seconds.)

Procedure for configuring the WPA or WPA2 security mode:

Assume that the IP address, port number, and password of the RADIUS server are 192.168.0.88, 1812, and 12345678 respectively, and the encryption algorithm is AES.

- **Step 1** Select the SSID to be configured from the SSID drop-down list box, such as **Tenda_123456**.
- **Step 2** Set **Security Mode** to **WPA** or **WPA2**.
- Step 3 Set RADIUS Server to the IP address 192.168.0.88 of the RADIUS server.
- Step 4 Set RADIUS Port to the authentication port number 1812 of the RADIUS server.
- Step 5 Set RADIUS Password to the password 12345678 of the RADIUS server.
- **Step 6** Set **Cipher Type** to **AES**.
- Step 7 Click Save.

Te	enda								
h	Status	Basic						Administrator:admin	
4	Quick Setup	ſ	SSID	Tenda_123456	1	~]		Save	^
•	Network		Enable			_		Restore	
~	Basic	Bro	adcast SSID AP isolation	Enable	Enable	~		Help	
	Radio Site Survey		WMF Client limit	Disable ()	Enable	(Ra	ingle:1-64)		
	Advanced Access Control	Chinese	SSID	Tenda_123456	5				
*	QVLAN SNMP	See	curity Mode	WPA	[
۵,	Tools	RAI	DIUS Server: ADIUS Port:	192.168.0.88		(R	angle: 1-65535,default: 1812)		
		RADIU	S Password:	•••••					
		Key Upo	late Interval	O AES () TKI	IP () TKIP&AES	(R	ange: 0 or 60—999999 seconds.	.)	
									~

----End

Parameter description

Parameter	Description
Security Mode	It specifies the security mode of the selected SSID. Select WPA or WPA2 .
WPA	This encryption type supports the AES and TKIP encryption algorithms.
WPA2	This encryption type supports the AES, TKIP, and TKIP&AES encryption algorithms.
RADIUS Server	It specifies the IP address of the RADIUS server for authentication.
RADIUS Port	It specifies the port number of the RADIUS server for authentication.
RADIUS Password	It specifies the password of the RADIUS server for authentication.
Cipher Type	It specifies the encryption algorithm corresponding to the selected security mode. The available options include AES, TKIP, and TKIP&AES.
AES	It is short for Advanced Encryption Standard. If this encryption algorithm is used, the AP can reach a maximum wireless transmission rate of 300 Mbps.
ТКІР	It is short for Temporal Key Integrity Protocol. If this encryption algorithm is used, the AP can reach a maximum wireless transmission rate of 54 Mbps.
TKIP&AES	It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the AP based on TKIP or AES.

Parameter	Description
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.

4.4.2 Radio Settings

To view the radio parameters of the AP, choose **Wireless** > **Radio**. If the AP works in AP+Client or WDS mode, the radio parameters cannot be changed.

end a			
小 Status	Radio		Administrato
Quick Setup	Enable Wireless	2	Save
Network	Country	China	Rest
🛜 Wireless	Network Mode	11b/g/n mixed	Resu
Basic	Channel	Auto	Help
Radio	Channel Bandwidth	0 20MHz 0 40MHz 0 20/40MHz	
Site Survey Advanced	Extension Channel	Auto	
Access Control	Channel Lockout		
QVLAN	SSID isolation	● Disable ○ Enable	
× SNMP	WMM Capable	Enable Oisable	
🖏 Tools	APSD Capable	○ Enable	
	Ageing Time	5 minutes	

Parameter description

Parameter	Description
Enable Wireless	It specifies whether to enable the wireless function of the AP.
Country	It specifies the country or region where the AP is used. Different countries or regions have different channel regulations.
Network Mode	 It specifies the 802.11 network mode of the AP. By default, the AP works in 11b/g/n mixed mode. 11b: It indicates that only clients working in the 11b network mode can connect to the AP. In this network mode, the AP can reach a maximum wireless transmission rate of 11 Mbps. 11g: It indicates that only clients working in the 11g network mode can connect to the AP. In this network mode, the AP can reach a maximum wireless transmission rate of 54 Mbps. 11b/g mixed: It indicates that only clients working in the 11b or 11g network mode can connect to the AP. In this network mode, the AP can reach a maximum wireless transmission rate of 54 Mbps.

Parameter	Description
	 transmission rate of 54 Mbps. 11b/g/n mixed: It indicates that only clients working in the 11b, 11g, or 11n network mode can connect to the AP. In this network mode, the AP can reach a maximum wireless transmission rate of 300 Mbps.
Channel	It specifies the operating channel of the AP.
Channel Bandwidth	It specifies the bandwidth of the operating channel of the AP. This parameter is effective only for the 802.11b/g/n mixed network mode. The 20/40 option offers a maximum wireless transmission rate almost twice of that offered by the 20 option.
Expansion Channel	It specifies an additional channel used to increase the channel bandwidth if the AP works in the 802.11b/g/n mixed network mode and the channel bandwidth option 20/40 is selected.
Channel Lockout	It is used to lock the selected channel. After a channel is locked, parameters of the channel cannot be changed, including Country , Network Mode , Channel , Channel Bandwidth , and Expansion Channel .
SSID Isolation	 It specifies whether to isolate the wireless clients connected to the AP with different SSIDs. Disable: It indicates that the wireless clients connected to the AP with different SSIDs can communicate with each other. Enable: It indicates that the wireless clients connected to the AP with different SSID cannot communicate with each other. This improves wireless network security.
WMM Capable	It is short for Wi-Fi Multimedia, which helps improve multimedia data (such as data of online videos) transmission performance of wireless networks. It is recommended that you enable this function.
APSD Capable	It is short for Automatic Power Save Delivery, and is effective only if the WMM function is enabled. It is recommended that you disable this function.

4.4.3 Channel Scan

This function is used to detect nearby wireless networks of the AP, as well as the MAC addresses, network modes, channels, channel bandwidths, security modes, and signal strengths of the wireless networks. To use the function, choose **Wireless** > **Site Survey**.

Te	end a	
÷	Status	Site Survey
\$	Quick Setup	Click "Enable Scan" to find the best channel.
	Network	Enable Scan Help
((¢	Wireless	
	Basic	
	Radio	
	Site Survey	
	Advanced	
	Access Control	
	QVLAN	
*	SNMP	
¢,	Tools	

By default, the channel scan function of the AP is disabled. You can click **Enable Scan** and wait a moment for the scan result. See the following figure.

e	nda													
M	Status	Site S	Site Survey Administrator:admin											
47	Ouick Setup	cl'-l												
•	Network	Click	Click "Enable Scan" to find the best channel.											
((r-	Wireless	ID	SSID	MAC Address	Network Mode	Channe	Bandwidt	n Security	Signal					
	Basic	1	12345678	C8:3A:35:1E:91:70	bgn	1	20	none	-85dBm	-				
	Site Survey	2	Tenda_abcde	50:2B:73:F2:87:C1	bgn	2	20	wpa&wpa2/aes	-78dBm	1				
	Advanced	3	TENDA_AP_0	C8:3A:35:00:00:5D	bgn	2	20	none	-80dBm					
	Access Control	4	TENDA_AP	C8:3A:33:22:33:45	bgn	3	40	none	-85dBm	1				
	QVLAN	5	pintai-e10-1	9C:01:23:45:67:89	bgn	2	20	wpa2/aes	-81dBm	1				
Ķ	SNMP	6	ETAPAEP_IBA-wq	C8:32:11:12:33:01	bgn	3	20	wpa&wpa2/tk	-81dBm	1				
	Tools	7	Tenda_1E5F00	C8:3A:35:1E:5F:01	bgn	3	20	none	-82dBm	1				
		8	TP2.4G-C9	14:CC:20:E5:F7:31	bgn	4	40	wpa&wpa2/tk	-76dBm	1				
		9	Tenda_F009F8	50:2B:73:F0:09:F9	bgn	5	20	none	-84dBm	1				
		10	Everest_guaji_V300	C8:3A:35:03:13:29	bgn	5	40	wpa2/aes	-84dBm	1				
		11	WQB	C8:3A:3C:AC:15:B1	bgn	5	20	wpa2/aes	-78dBm	1				
		12	GDDX-2.4G	C8:3A:35:1F:3D:A9	bgn	1	20	none	-80dBm	1				

According to the scan result, you can select the least-used channel as the operating channel of the AP for better wireless transmission efficiency.

4.4.4 Advanced Settings

To view the advanced parameters for configuring the wireless performance of the AP, choose **Wireless** > **Advanced**.

It is recommended that you change the settings only under the instruction of professional personnel, so as to prevent decreasing the wireless performance of the AP.

Te	enda			
[Advanced		Administrator:admin
Ŷ	Status	Advanced		
4	Quick Setup			Sava
	N. J.	Beacon Interval	100 (Range: 20 - 999; Default: 100)	Save
	Network	Fragment Threshold	2346 (Range: 256 - 2346; Default: 2346)	Restore
((i·	Wireless	RTS Threshold	2347 (Range: 1 - 2347; Default: 2347)	
	Basic	DTIM Interval	1 (Range: 1 - 255; Default: 1)	Help
	Radio	Receive Signal strength	-90 (dBm.Range: -9060: Default: -90)	
	Site Survey			
	Advanced	Interference mitigation	3 (Range: 1 - 4; Default: 3)	
	Access Control	Output Power	23 (dBm,Range: 8 - 23; Default: 23)	
	QVLAN	Power Lockout	$\mathbf{\nabla}$	
*	SNMP	Preamble	Long Preamble O Short Preamble	
ø,	Tools	Signal Transmission	⊖ coverage-oriented	
		Signal Reception	Default Coverage-oriented Capacity-oriented	

Parameter description

Parameter	Description
	It specifies the interval for transmitting the Beacon frame. The value range is 20 to 999. The unit is millisecond.
Beacon Interval	The Beacon frame is transmitted at the specified interval to announce the presence of a wireless network. Generally, a smaller interval enables wireless clients to connect to the AP more quickly, while a larger interval ensures higher data transmission efficiency.
	It specifies the threshold of a fragment. The value range is 256 to 2346. The unit is byte.
Fragmont	Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented.
Threshold	 In case of a high error rate, you can reduce the threshold to enable the AP to resend only the fragments that have not been sent successfully, so as to increase the frame throughput.
	• In an environment without interference, you can increase the threshold to reduce the number of acknowledgement times, so as to increase the frame throughput.

Parameter	Description
	It specifies the frame length threshold for triggering the RTS/CTS mechanism.
	If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The value range is 1 to 2347. The unit is byte.
RTS Threshold	Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	It is short for Delivery Traffic Indication Message, and specifies the countdown before the AP transmits broadcast and multicast frames in its cache. The value range is 1 to 255. The unit is Beacon interval. For example, if DTIM Interval is set to 1 , the AP transmits all cached frames at the Beacon interval.
	It specifies the minimum strength of received signals acceptable to the AP.
Receive Signal Strength	If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to the AP. An appropriate value of this parameter ensures that wireless clients connect to APs with strong signals.
Output Power	It specifies the transmit power of the AP. The unit is dBm. The value range is 8 dBm to 23 dBm. A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.
Power Lockout	It specifies whether the current transmit power settings of the AP can be changed.
Preamble	It specifies the time when data is transmitted between a wireless client and the AP. The time is notified to other wireless clients to prevent conflicts. During transmission, the preamble as well as the synchronization signal and frame interval is transmitted before working data. In data frames for wireless transmission, a long preamble results in short working data. Therefore, a short preamble can be used to improve wireless transmission efficiency. It is optional for 802.11b devices to support short preambles. It is mandatory for 802.11g
	It energifies the signal transmission mode for a specific scenario
Signal Transmission	 Coverage-oriented: This mode enables the AP to provide broader coverage when the AP is deployed in an area with low AP density, such as an office, a warehouse, or a hospital. Capacity-oriented: This mode reduces inter-AP interference when the AP is deployed in an area with high AP density, such as a venue, an exhibition hall, a banquet hall, a stadium, a college classroom, or a departure lounge.
Signal Reception	It specifies the signal reception mode for a specific scenario. • Coverage-oriented: This mode enables more wireless devices to connect to the AP in an

Parameter	Description
	area with low AP density.
	• Capacity-oriented : This mode ensures that each wireless device in an area with high AP density connects to the AP with the strongest signal.
	• Default : This mode enables the AP to achieve a balance between the other two modes.

4.4.5 Access Control

To control access of wireless clients to the AP by MAC address, choose Wireless > Access Control.

Te	enda						
*	Status	Access C	ontrol				Administrator:admin
• •	Quick Setup	Specify a	list of the wireless cli SSID	ents permitted or Tenda_123456	prohibite to connect to	o this device	Save
-) ((:-	Wireless		MAC Filter Mode	Disable			Restore
	Basic Radio	ID	MAC Address	IP	Connection Duration	Add to List	Theip
	Site Survey	1	C8:3A:35:C9:15:9	6 192.168.0	.222 00:03:54	Add	
	Advanced						
	Access Control						
	QVLAN						
*	SNMP						
¢,	Tools						

Parameter description

Parameter	Description
SSID	It specifies the SSID that requires wireless client access control.
	It specifies the mode for filtering MAC addresses.
	• Disable : It indicates that access control is disabled.
MAC Filter Mode	• Allow: It indicates that only the wireless clients on the access control list can connect to the AP with the selected SSID.
	• Deny : It indicates that only the wireless clients on the access control list cannot connect to the AP with the selected SSID.

This page also displays a list of wireless clients that have connected to the AP with the selected SSID. You can select wireless clients from the list to implemented access control.

Te	enda									
								Administrator:admin		
∿	Status	Access C	ontrol							
\$	Quick Setup	Specify a	list of the wireless cli	ents p	permitted or prohib	ite to connect to this	device	Save		
	Network		SSID	Ten	da_123456	\checkmark				
((t-	Wireless		MAC Filter Mode	Disa	able	\checkmark		Restore		
	Basic		MAC Address		TD	Connection	Add to List	Help		
	Radio		MAC Address		15	Duration		_		
	Site Survey	1	C8:3A:35:C9:15:9	6	192.168.0.222	00:03:54	Add			
	Advanced									
	Access Control									
	QVLAN					Wirolocc	client list			
*	SNMP					VVII EIESS	chefti list			
ø,	Tools									

Example Application of Wireless Control

Networking requirement

The laptops whose MAC addresses are C8:3A:35:12:12:12 and C8:3A:35:14:14:14 are not allowed to connect to the AP with the SSID Tenda_123456.

Procedure

Step 1 Set SSID to Tenda_123456 and MAC Filter Mode to Deny.

Te	enda						
		Access	Control				Administrator:admin
-∿- 45	Status Quick Setup	Accessio					
•	Network	Specify a	SSID	its permitted or prohib Tenda_123456	Dite to connect to th	is device	Save
((t-	Wireless		MAC Filter Mode	Deny			Restore
	Basic Badio	ID	MAC Address	IP	Connection Duration	Add to List	Help
	Site Survey	1	C8:3A:35:C9:15:96	192.168.0.222	00:03:54	Add	
	Advanced Access Control						
	QVLAN]	Add	
*	SNMP						
۵,	Tools						

- Step 2 Enter C8:3A:35:12:12:12 in the MAC Address text box and click Add.
- Step 3 Change the value of the MAC Address text box to C8:3A:35:14:14:14 and click Add.

Administrator:admin	Te	enda								
Administrator:admi										
♀ Quick Setup Specify a list of the wireless clients permitted or prohibite to connect to this device Save ● Network SSID Tenda_123456 ♥ Restore ● Wireless MAC Filter Mode Deny ♥ Help ● MAC Filter Mode Deny ♥ Help ● MAC Address IP Connection Add to List ● Advanced 1 C8:3A:35:C9:15:96 192.168.0.222 00:03:54 Add ● Quick Setup MAC Address Action Add Image: Sinther Si	Ą.	Status	A	ccess Co	ontrol					Administrator:admin
● Network SSID Tenda_123456 ✓ ● Wireless MAC Filter Mode Deny ✓ Basic Basic ID MAC Address IP Connection Add to List 1 C8:3A:35:C9:15:96 192.168.0.222 Advanced MAC Address IP Outwation Advanced MAC Address Action Add QVLAN C8 3A 35 14 14 MAC 1 C8:3A:35:12:12:12 In able Delete 1 C8:3A:35:14:14:14 In able Delete 2 C8:3A:35:14:14:14 In able Delete	\$	Quick Setup		Specify a	list of the wireless cli	ents	permitted or prohib	ite to connect to thi	s device	Save
♥ Wireless MAC Filter Mode Deny Restore Basic Basic Radio Site Survey Advanced Access Control QVLAN ♥ Tools MAC Address ID MAC Address IP Duration Add to List 1 C8:3A:35:C9:15:96 192.168.0.222 00:03:54 Add MAC Address Action C8:3A:35:14:14:14 Add I C8:3A:35:12:12:12 I C8:3A:35:14:14:14 Delete 2 C8:3A:35:14:14:14		Network			SSID	Те	nda_123456	\checkmark		
Basic ID MAC Address IP Connection Duration Add to List Advanced 1 C8:3A:35:C9:15:96 192.168.0.222 00:03:54 Add Advanced MAC Address Action Add QVLAN C8:3A:35:14:14:14 Add ★ SNMP 1 C8:3A:35:12:12:12 Image: Centre of the second se	((ı:	Wireless			MAC Filter Mode	De	ny	\checkmark		Restore
Kadio Junch Site Survey 1 C8:3A:35:C9:15:96 192.168.0.222 00:03:54 Add Advanced MAC Address Action QVLAN C8:3A:35:14:14:14 Add X SNMP 1 C8:3A:35:12:12:12 Image: C8:3A:35:12:12:12 Image: Red of the second seco		Basic		ID	MAC Address		IP	Connection	Add to List	Help
Advanced MAC Address Action QVLAN C8 3A 35 14 14 14 Add SNMP 1 C8:3A:35:12:12:12 Enable Delete 2 C8:3A:35:14:14:14 Z Delete		Site Survey		1	C8:3A:35:C9:15:9	6	192.168.0.222	00:03:54	Add	
Access Control MAC Address Action QVLAN C8 3A 35 14 14 14 Add SNMP 1 C8:3A:35:12:12:12 Image: Delete Qold Image: Delete Delete Question Image: Delete Delete Question Image: Delete Delete Question Image: Delete Delete		Advanced								
QVLAN C8 3A 35 14 14 14 Add X SNMP 1 C8:3A:35:12:12:12 Image: C8 Delete Delete Image: C8 Tools Image: C8 Image: C		Access Control				MA	C Address		Action	
★ SNMP 1 C8:3A:35:12:12:12 ☑ Enable Delete ☎ Tools 2 C8:3A:35:14:14:14 ☑ Enable Delete		QVLAN								
Cols C8:3A:35:14:14:14 Image: C8:3A:35:14:14:14	*	SNMP		1	C8:3	A:35	5:12:12:12	☑ Enable	Delete	
	್ಧ	Tools		2	C8:3	A:35	5:14:14:14	☑ Enable	Delete	
						_				7



						Administrator:ad
 Status 	Access Co	ontrol				
Quick Setup	Specify a	list of the wireless cl	ients permitted or p	rohibite to connect to tl	his device	Save
Network	1	SSID	Tenda_123456	\checkmark		
Wireless		MAC Filter Mode	Deny	\checkmark		Restore
Basic	ID	MAC Address	IP	Connection	Add to List	Help
Radio				Duration		
Site Survey	1	C8:3A:35:C9:15:9	96 192.168.0.2	22 00:03:54	Add	
Advanced						
Access Control			MAC Address		Action	
QVLAN		C8 : 3A	35 14 14	: 14	Add	
SNMP	1	C8:	3A:35:12:12:12	☑ Enable	Delete	
Tools	2	C8:	3A:35:14:14:14	☑ Enable	Delete	

----End

4.4.6 QVLAN Settings

This AP supports IEEE 802.1Q VLANs. After the QVLAN function is enabled, the AP can work with a switch that supports the QVLAN function to set up multiple wireless VLANs. Wireless clients connected to different VLANs cannot communicate with each other.

To configure the function, choose **Wireless** > **QVLAN**.

Tenda

				Administrator
≁	Status	QVLAN Setup		
\$	Quick Setup	Enable	, 🗆	Save
	Network	PVID	1	
((:-	Wireless	Manage VLAN	1	Resto
	Basic	2.4G SSID	VLAN ID (1-4094)	Help
	Radio	Tenda_123456	1000	
	Site Survey			5
	Advanced			
	Access Control			
	QVLAN			
*	SNMP			
ø,	Tools			

Parameter description

Parameter	Description
Enable	It specifies whether to enable the QVLAN function. By default, it is disabled.
PVID	It specifies the ID of the default native VLAN of the trunk port. The default ID is 1.
Manage VLAN	It specifies the ID of the AP management VLAN. The default ID is 1. After changing the management VLAN, you can manage the AP only after connecting your computer to the new management VLAN.
SSID	It specifies the wireless network names of the AP.
VLAN ID	It specifies VLAN IDs corresponding to SSIDs. The default VLAN ID is 1000. The VLAN ID range is 1 to 4094.

Example Application of QVLAN Configuration

Requirement

A hotel needs to enable its guests to access the internet by both wired and wireless means in the lounge and rooms, its employees to access its LAN server, and its senior managers to access both the internet and LAN server.

Solution

Define 802.1Q VLANs on its core switch to isolate the three groups of users.

- Deploy i12 and configure multiple SSIDs and the QVLAN function to enable the AP to interwork with the VLANs defined on the core switch.
- Separately implement wireless network encryption for each SSID and assign different SSIDs to different groups of users.

- There are three groups of users and the AP has four SSIDs. The SSID not assigned to the users can be handled using either of the following methods:
 - Assign the SSID to the largest group of users, such as the group of guests. This SSID must adopt the same security mode and VLAN ID as the SSID originally assigned to the group. The SSIDs must be different. (This method is used as an example for description in this document.)
 - Disable the SSID.

Network topology

See the following figure.



Configuration description

VLANs defined on the core switch

Port Connected To	VLAN	Link Type	PVID
Guests	2	Access	2
Employees	3	Access	3
Senior managers	4	Access	4
АР	1,2,3,4	Trunk (Traffic of all the VLANs can pass through the port.)	1
LAN server	3,4	Trunk (Only traffic of VLAN3 and	1

Port Connected To	VLAN	Link Type	PVID
		VLAN4 can pass through the port.)	
Gateway with internet connectivity	2,4	Trunk (Only traffic of VLAN3 and VLAN4 can pass through the port.)	1

SSIDs and VLANs defined on the AP

User Group	SSID	VLAN ID
Guests	Hotel1	VLAN2
Employees	Office	VLAN3
Senior managers	Management	VLAN4
Guests	Hotel2	VLAN2

- AP configuration
- **Step 1** Log in to the web UI of the AP and choose **Wireless** > **Basic**.
- **Step 2** Enable the 4 SSIDs, change the SSIDs to **Hotel1**, **Office**, **Management**, and **Hotel2**, configure security modes for the SSIDs, and save the change.
- Step 3 Choose Wireless > QVLAN, enable the QVLAN function, change the VLAN IDs of the SSIDs, and click Save.

∿	Status	QVLAN Setup	Administrator:admir
\$	Quick Setup	Enable 🗹	Save
	Network	PVID 1	
((ı-	Wireless	Manage VLAN 1	Restore
	Basic	2.4G SSID VLAN ID (1-4094)	Help
	Radio	Hotel1 2	
	Site Survey	Office 3	
	Advanced	Management 4	
	Access Control	Hotel2 2	
*	SNMP		
ø,	Tools		

4.5 SNMP

This AP supports the SNMP agent function. Therefore, you can use SNMP management software to manage the AP. To configure the function, choose **SNMP**.

Tenda		
♪ Status	SNMP	Administrator:admin
4 Quick Setup	Here you can configure SNMP settings. SNMP v1 and v2c are supported.	Save
Network Wireless	SNMP	Restore
× SNMP		Help
🖏 Tools		

By default, the SNMP agent function is disabled. To enable it, set **SNMP** to **Enable**.

Te	enda			
4	Status	SNMP		Administrator:admin
\$	Quick Setup	Here you can configure S	SNMP settings. SNMP v1 and v2c are supported.	Save
۲	Network	SNMP	⊖ Disable	
((ı:	Wireless	Administrator Name	Administrator	Restore
*	SNMP	Device Name	i12V1.0	Help
ø,	Tools	Location	ShenZhen	
		Read Community	public	
		Read/Write Community	private	

Parameter description

Parameter	Description
SNMP	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled.
Administrator Name	It specifies the name of the administrator of the AP. The default name is Administrator.
Device Name	It specifies the device name of the AP. The default device name is in the format of <i>Model+Hardware version number</i> . For example, the device name of i12 is i12V1.0.
Location	It specifies the location where the AP is used.
Read Community	It specifies the read password shared between the SNMP manager and SNMP agent. The

	default password is public. The SNMP agent function of the AP allows an SNMP manager to use the password to read variables in the MIB of the AP.
Read/Write	It specifies the read/write password shared between the SNMP manager and SNMP agent. The default password is private.
Community	The SNMP agent function of the AP allows an SNMP manager to use the password to read/write variables in the MIB of the AP.

4.6 Tools

4.6.1 Firmware Upgrade

You can download a later firmware version for the AP from <u>http://www.tendacn.com</u> to upgrade the firmware of the AP for more functions and higher stability. To upgrade the firmware, choose **Tools**.

2	nda
ŀ	Status
₽	Quick Setup
€	Network
0	Mercland
÷	vvireiess
*	SNMP
ø,	Tools
	Firmware Upgrade
	Time & Date
	Logs
	Configuration
	Administrator
	Diagnostics
	Reboot
	LED
	Uplink Detection

Do not power off the AP during an upgrade. Otherwise, the AP may be damaged. If a power failure occurs during an upgrade, perform the upgrade again. If you cannot access the web UI of the AP after the power failure, contact the aftersales service for a repair.

Procedure:

Step 1 Download the package of a later firmware version for the AP from <u>http://www.tendacn.com</u> to your local computer, and decompress the package.

- **Step 2** Log in to the web UI of the AP and choose **Tools**.
- **Step 3** Click **Browse** and choose the AP upgrade file.
- Step 4 Click Upgrade.

----End

Wait until the upgrade and reboot process is complete. Choose **Tools** and check whether the upgrade is successful based on **Current Firmware Version**.

4.6.2 Date & Time

The AP provides the system time and login timeout modules for time management.

The time information of the AP is lost when the AP is powered off. If the function for synchronizing the system time through the internet is enabled, the AP synchronizes the system time after being reconnected to the internet. Logs can be recorded correctly and the reboot schedule can be executed correctly only when the system time is correct.

System Time

To configure the system time of the AP so that logs can be recorded correctly and the reboot schedule can be executed correctly, choose **Tools** > **Time & Date**.

Te	e nd a		
		Administr	rator:admin
*	Status	System time rage timeout	
~ ⊕	Network	This page is used to set the device's system time. You can select either to set the time manually or get the GMT time from Internet and system will automatically connect to NTP server to synchronize the	Save
((r-	Wireless	Note: System time will be lost when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet.	Restore
*	SNMP	Sync with Internet time servers Sync Interval: 30 minutes	lelp
۵,	Tools	Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei	
	Firmware Upgrade	(Note: GMT time will be updated automatically only when the device is connected to Internet)	
	Time & Date	Set Time and Date Manually:	
	Logs	2017 Year 01 Month 10 Day 14 h 33 m 45 s Sync with Your PC	
	Configuration		
	Administrator		
	Diagnostics		
	Reboot		
	LED		
	Uplink Detection		

You can choose whether to synchronize the system time through the internet or manually set the system time. By default, the AP synchronizes the system time through the internet.

Synchronizing the system time with internet time servers

The AP synchronizes the system time at a specified interval with the time server over the internet.

The AP can perform synchronization only after being connected to the internet. To connect the AP to the internet, choose **Network > LAN Setup** and set the IP address, subnet mask, gateway, and DNS server of the AP.

Procedure:

- **Step 1** Select Sync with Internet time servers.
- **Step 2** Set **Sync Interval** to the synchronization interval. **30 minutes** is recommended.
- **Step 3** Set **Time Zone** to your time zone.
- Step 4 Click Save.

Te	enda		
		Admi	nistrator:admin
Ŷ	Status		
\$	Quick Setup	This page is used to set the device's system time. You can select either to set the time manually or get	Save
	Network	the GMT time from Internet and system will automatically connect to NTP server to synchronize the time.	
((r.	Wireless	Note: System time will be lost when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet.	Restore
*	SNMP	Sync with Internet time servers Sync Interval 30 minutes	Help
۵,	Tools	Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei	
	Firmware Upgrade	(Note: GMT time will be updated automatically only when the device is connected to Internet)	
	Time & Date	Set Time and Date Manually:	
	Logs	2017 Year 01 Month 10 Day 14 h 33 m 45 s Sync with Your PC	
	Configuration		
	Administrator		
	Diagnostics		
	Reboot		
	LED		
	Uplink Detection		

----End

Manually setting the system time

You can manually set the system time of the AP.

Procedure:

- **Step 1** Deselect **Sync with Internet time servers**.
- **Step 2** Enter a correct date and time, or click **Sync with Your PC** to synchronize the system time of the AP with the system time (ensure that it is correct) of the computer being used to manage the AP.
- Step 3 Click Save.

2			
		Admi	nistrator:adr
r	Status		
₽	Quick Setup	This page is used to set the device's system time. You can select either to set the time manually or get	Save
₽	Network	the GMT time from Internet and system will automatically connect to NTP server to synchronize the	care
lle-	Wireless	ume. Note: System time will be lost when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet.	Restore
Ķ	SNMP	Sync with Internet time servers Sync Interval: 30 minutes	Help
L.	Tools	Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei	
	Firmware Upgrade	(Note: GMT time will be updated automatically only when the device is connected to Internet)	
	Time & Date	Set Time and Date Manually:	
	Logs	2017 Year 01 Month 10 Day 14 h 41 m 22 s Sync with Your PC	
	Configuration		
	Administrator		
	Diagnostics		
	Reboot		
	LED		
	Uplink Detection		

Page Timeout

If a user logs in to the web UI of the AP and performs no operation within the login timeout interval, the AP logs the user out. To set the interval, choose **Tools** > **Time & Date** > **Page Timeout**.

Ter	nda	
小 Sta	atus	System Time Page Timeout
4 Qu	uick Setup	Save
Ne	etwork	Page Timeout 5 (1~60 minutes)
奈 Wi	ireless	Restore
🗙 SN	IMP	Help
🖏 To	ols	
Fi	irmware Upgrade	
Ti	ime & Date	
Lo	ogs	
Co	onfiguration	
Ad	dministrator	
Di	iagnostics	
Re	eboot	
LE	ED	
U	plink Detection	

The default interval is 5 minutes. You can change it as required within the range from 1 minute through 60

minutes.

4.6.3 Logs

View Logs

To view the logs of events that occur after the startup of the AP, choose **Tools** > **Logs**.

You are recommended to choose **Tools** > **Time & Date** and verify the system time of the AP to ensure that the times of logs are correct. This facilitates real-time network condition monitoring and network fault diagnosis.

Tenda

A. Shahar	View Loo	ıs Log Server			Administrator:admin
Quick Setup					
A Notwork				Log Type All	✓ Refresh
	Index	Time	Туре	Log Content	Clear
ক Wireless	150	2017-01-10 14:53:25	system	web 192.168.0.169 login	
X SNMP	149	2017-01-10 14:46:55	system	web 192.168.0.169 login time expired	
🖏 Tools	148	2017-01-10 14:40:12	system	web 192.168.0.169 login	
Firmware Upgrade	147	2017-01-10 14:38:55	system	web 192.168.0.169 login time expired	
Time & Date	146	2017-01-10 14:33:41	system	web 192.168.0.169 login	
Configuration	145	2017-01-10 14:32:55	system	web 192.168.0.169 login time expired	
Administrator	144	2017-01-10 14:27:01	system	web 192.168.0.169 login	
Diagnostics	143	2017-01-10 14:18:55	system	web 192.168.0.169 login time expired	
Reboot	142	2017-01-10 14:13:33	system	web 192.168.0.169 login	
LED	141	2017-01-10 14:10:55	system	web 192.168.0.169 login time expired	
Uplink Detection	140	2017-01-10 14:05:03	system	2.4G Wifi UP	
	139	2017-01-10 14:04:54	system	2.4G Wifi UP	
	138	2017-01-10 14:04:48	system	24G Wifi UP	

To view the latest logs of the AP, click **Refresh**. To clear the logs on the page, click **Clear**.

- When the AP reboots, the previous logs are lost.
- The AP reboots when the AP is powered on after a power failure, the QVLAN function is configured, the firmware is upgraded, an AP configuration is backed up or restored, or the factory settings are restored.

Log Server

To set the number of logs and log servers, choose **Tools** > **Logs**.

Tenda

s	View Logs	Log Server			Adr	ninistrator:a
Setup	Number of Lo	0qs 150	(Defa	ult-150 Range-10	0~300)	Save
ork	🗆 Enable 🛛 (T	o use the following rule	s, you must check this b	xx.)	,	Destars
:55	ID	Log Server IP	Log Server Port	Enable	Action	Restore
Р			I			Help
s					Add	
ware Upgrade						
ne & Date						
gs						
nfiguration						
nfiguration						
nfiguration ninistrator gnostics						
ntiguration ministrator gnostics poot						
ninistraton ninistrator gnostics oot						

Number of logs

You can set the maximum number of logs that can be displayed on the page. The value range is from 100 to 300. By default, a maximum of 150 logs can be displayed.

Log server settings

After a log server is specified, the AP sends its logs to the log server. You can view all the historical logs of the AP on the log server.

Procedure for adding a log server:

Step 1 Click Add.

nda
Status
Quick Setup
Network
Wireless
SNMP
Tools
Firmware Upg
Time & Date
Logs
Configuration
Administrator
Diagnostics
Reboot
LED
Uplink Detecti

- **Step 2** Set **Log Server IP** to the IP address of a log server (192.168.0.88 in this example) over the network.
- **Step 3** Set **Log Server Port** to the UDP port number used to send and receive system logs. The default port number 514 is recommended.
- **Step 4** Select **Enable** to enable the log server function.
- Step 5 Click Save.

Te	enda			
*	Status	View Logs Log Server		Administrator:admin
\ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Status Quick Setup Network Wireless SNMP Tools Firmware Upgrade Time & Date Logs Configuration	View Logs Log Server Log Server IP Log Server Port Enable	192.168.0.88 514	Save Restore Help
	Diagnostics Reboot LED Uplink Detection			

Step 6 Select **Enable (To use the following rules, you must check this box.)** and click **Save**.

• Status	View Logs	Log Server			Ad	lministrato
Quick Setup	Number of	Logs 150	(Defai	It:150 Range:1	00~300)	Save
Network	☑ Enable	(To use the following rule	es you must check this b	ох.)	,	
Wireless	ID	Log Server IP	Log Server Port	Enable	Action	Rest
SNMP	1	192.168.0.88	514	Enable	Edit Delete	Help
Tools						
Firmware Upgrade					Add	
Time & Date						
Logs						
Configuration						
Administrator						
Diagnostics						
Reboot						
LED						
Uplink Detection						

----End

To change the settings of a log server, click **Edit** corresponding to the log server. To delete the settings of a log server, click **Delete** corresponding to the log server.

To ensure that system logs can be sent to a log server, choose **Network** > **LAN Setup** and set the IP address, subnet mask, and gateway of the AP for communicating with the log server.

4.6.4 Configuration Management

Backup & Restore

To access the page for backing up or restoring a configuration, choose **Tools** > **Configuration**.

Tenda

∿	Status	Backup & Restore Restore to Factory Default
\$	Quick Setup	This section allows you to save current settings or restore previous settings.
۲	Network	Save Settings to Local Drive Backup
((ı:	Wireless	Load Settings from Local Drive Browse Restore
*	SNMP	
ø,	Tools	
	Firmware Upgrade	
	Time & Date	
	Logs	
	Configuration	
	Administrator	
	Diagnostics	
	Reboot	
	LED	
	Uplink Detection	

Backing up the current configuration

After the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration.

To back up the configuration, click **Backup** and follow the on-screen instructions to perform operations.

Restoring a configuration

By restoring an earlier configuration that has been backed up, you can apply the same configuration to multiple APs or recover an AP after the configuration of the AP is changed unexpectedly.

To restore a configuration, click **Browse**, select the backup file of the configuration, click **Restore**, and follow the on-screen instructions to perform operations.

Restore to Factory Default

If you cannot locate the cause for a failure to access the internet, you can restore the factory settings of the AP to address the problem. To restore the factory, choose **Tools** > **Configuration** > **Restore to Factory Default** and click **Restore to Factory Default**.

Tenda

		Administrator:admi
♣ Status	Backup & Restore Restore to Factory Default	
✤ Quick Setup	Click this button to reset the device to factory default values.	Help
Metwork	Restore to Factory Default	
🛜 Wireless		
🗙 SNMP		
🖏 Tools		
Firmware Upgrade		
Time & Date		
Logs		
Configuration		
Administrator		
Diagnostics		
Reboot		
LED		
Uplink Detection	1	

You can also use the reset button on the AP to restore the factory settings. If you forget your login information, such as the IP address, user name, or password for the AP, you are recommended to use the reset button to restore the factory settings.

Procedure:

Step 1 After the AP is powered on, hold down the reset button for 8 seconds.



Step 2 Wait about 45 seconds.



After the factory settings are restored, the IP address of the web UI of the AP changes to 192.168.0.254 and the login user name and password change to **admin**. For other default settings, refer to <u>Appendix C</u> <u>Default Parameter Settings</u>.

4.6.5 Accounts

You are recommended to change the default user name and password of the Administrator account to prevent unauthorized users from logging in to the web UI of the AP as the administrator and changing the AP configuration. To manage accounts, choose **Tools** > **Administrator**.

The AP allows an administrator account and a user account. The administrator account is assigned all AP management permissions. The user account is allowed only to view AP settings.

ſe	e nd a					
.∿-	Status	Administrator				Administrator:a
\$	Quick Setup	Use this section to cha	ange vour login user name	and password		Caura
•	Network	Note: User name and	password can only include	1~32 letters, numbe	ers or underscore!	Save
((ı-	Wireless	Access Mode	User Name	Enable	Action	Restore
*	SNMP	Administrator	admin	Z	Change	Help
ö,	Tools	User	user	1	Delete Change	
	Firmware Upgrade					
	Time & Date					
	Logs					
	Configuration					
	Administrator					
	Diagnostics					
	Reboot					
	LED					
	Uplink Detection					

By default, the AP has one administrator account and one user account. Both the user name and password of the administrator account are **admin**. Both the user name and password of the user account are **user**.

To change the user name and password of an account, click **Change** corresponding to the account. For example, you can click **Change** corresponding to the administrator account.

Tenda

	Ctature	Administrator				Administrator:admin
4	Quick Setup	Use this section to chan	ge your login user name	and password.		Save
	Network	Note: User name and pa	Destar			
((:-	Wireless	Access Mode	User Name	Enable	Action	Restore
*	SNMP	Administrator	admin		Change	Help
ø,	Tools	User	user	1	Delete Change	
	Firmware Upgrade	Old User Nan				
	Time & Date	Old Passwo	Old Password			
	Logs	New User Nam				
	Administrator	New Passwo				
	Diagnostics	Confirm New Passwo	rd			
	Reboot					
	LED					
	Uplink Detection					

Change the user name and password as required and click **Save**. The AP displays the login page. Use the new user name and password to log in.

To delete the user account, click **Delete** corresponding to the account, and click **Save**.

Tend a							
					Administrator admi		
♣ Status	Administrator						
Quick Setup	Use this section to change your login user name and password						
Metwork	Note: User name and password can only include 1~32 letters, numbers or underscore!						
🛜 Wireless	Access Mode	User Name	Enable	Action	Restore		
X SNMP	Administrator	admin		Change	Help		
🔍 Tools	User	user	☑ (1	Delete Change			
• Firmware Upgrade							
Time & Date							
Logs							
Configuration							
Administrator							
Diagnostics							
Reboot							
LED							
Uplink Detection							
To add the user account after deleting it, click **Change** corresponding to the account.

4.6.6 Diagnostics

If a network connection fails, you can use the Ping tool included with the AP to locate the faulty node. To use the tool, choose **Tools > Diagnostics**.



4.6.7 Reboot

Reboot

To manually reboot the AP, choose **Tools** > **Reboot**, and click **Reboot**.

When the AP reboots, all wireless connections are released. You are recommended to reboot the AP at an idle hour.

Tenda

≁	Status	Reboot	Time Reboot	
\$	Quick Setup	Click the	- 'Reboot' button to restart your dev	ice
	Network	CHER THE	Report Batton to restart your dev	Reboot
((:-	Wireless			
*	SNMP			
್ಕ	Tools			
	Firmware Upgrade			
	Time & Date			
	Logs			
	Configuration			
	Administrator			
	Diagnostics			
	Reboot			
	LED			
	Uplink Detection			

Time Reboot

You can specify an AP reboot schedule to enable the AP to reboot at an idle hour to ensure AP performance. To specify a reboot schedule, choose **Tools** > **Reboot** and click the **Time Reboot** tab.

Tenda			
♪ Status	Reboot <u>Time Reboot</u>		Administrator:admin
4 Quick Setup	Enable		Save
Metwork	Reboot Type	Interval	Destaur
🛜 Wireless	Reboot Interval	1440 (minute,Range : 10-7200)	Restore
X SNMP			Help
🖏 Tools			
Firmware Upgrade			
Time & Date			
Logs			
Configuration			
Administrator			
Diagnostics			
Reboot			
LED			
Uplink Detection			

The AP can reboot at an interval or at a specified time. Choose either as required.

- Rebooting the AP at an interval
 Configuration procedure:
- **Step 1** Select the **Enable** check box.
- **Step 2** Set **Reboot Type** to **Interval**.
- **Step 3** Set **Reboot Interval** to **1440**.
- Step 4 Click Save.

Te	enda			
	Ctatur	Reboot Time Reboot		Administrator:admin
4	Quick Setup	Enable		Save
(¢	Network Wireless	Reboot Type Reboot Interval	Interval V 1440 (minute,Range : 10-7200)	Restore
*	SNMP Tools			Help
	Firmware Upgrade Time & Date			
	Logs Configuration			
	Administrator Diagnostics			
	Reboot LED			
	Uplink Detection			

----End

- Rebooting the AP at specified time
 Procedure:
- **Step 1** Select the **Enable** check box.
- **Step 2** Set **Reboot Type** to **Schedule**.
- **Step 3** Select the day or days when the AP reboots.
- **Step 4** Set the time when the AP reboots, such as **23:59**.
- Step 5 Click Save.

 Status 	Reboot	Time Reboot								Adm	ninistrator:a
Quick Setup											Save
Network		Enable Reboot Type	Schedu	le							oure
Wireless		Dav		Mon	V Tuc	Ver l	Thur	Z Eri	□ 5 2 +	C Sur	Restore
SNMP		Time	23:59	VINON	eg: 23:59	Vieu	V mar	V FII	Jat	_ Sun	Help
Tools											
Firmware Upgrade											
Time & Date											
Logs											
Configuration											
Administrator											
Diagnostics											
Reboot											
LED											
Uplink Detection											

----End

4.6.8 LED Control

To turn on or off the LED indicator, choose **Tools** > **LED**.

_		
Tenda		
1	IFD	Administrator:admin
小 Status		
✤ Quick Setup	This sector is used to Switch on or Switch off the LED light.	Help
Metwork		
🛜 Wireless	Switch off LEDs	
X SNMP		
🖏 Tools		
Firmware Upgrade		
Time & Date		
Logs		
Configuration		
Administrator		
Diagnostics		
Reboot		
LED		
Uplink Detection		

When you click **Disable all LEDs**, the LED indicator of the AP turns off.

Appendixes

A. FAQ

Q1. I cannot access the web UI of the AP after entering 192.168.0.254. What should I do?

A1. Check the following items:

- Verify that the IP address of your computer is 192.168.0.X (X: 2~253).
- Clear the cache of your web browser or replace the web browser, and try login again.
- Disable the firewall of your computer or replace the computer, and try login again.
- If two or more APs are connected to your network without an AP controller, connect one of the APs to your network and change the IP address of the AP. Repeat this procedure to change the IP addresses of the other APs.
- The AP may be being managed by an AP controller and therefore its IP address is no longer 192.168.0.254. In that case, log in to the web UI of the AP controller to view the new IP address of the AP, and log in to the AP using the new IP address.
- If you have manually changed the IP address of the AP, change the IP address of your computer to another IP address that belongs to the same network segment as the new IP address of the AP and log in again using the new IP address of the AP.
- If the problem persists, restore the factory settings of the AP and try login again.

Q2. My wireless AP controller cannot find the AP. What should I do?

A2. Check the following items:

- Verify that the devices are connected properly and the AP has started.
- If VLANs have been defined on your network, verify that the corresponding VLAN has been added to your AP controller.
- Restart the AP or restore the factory settings of the AP, and try scanning the AP again.

Q3. Can I log in to the web UI of the AP to configure the AP after using an AC to manage the AP?

A3. Yes. You are recommended to change the user name and password of the administrator account (see <u>Section</u> <u>4.6.5 "Accounts."</u>) if you use an AC to manage the AP. This improves network security.

For more technical assistance, visit our website at <u>http://www.tendacn.com</u> or send your question to <u>support@tenda.cn</u>. We will help you resolve your problem as soon as possible.

B. Setting the IP Address of Your Computer (Example: Windows 7)

- Step 1Choose Start > Control Panel, click Network and Internet, click Network and Sharing Center, and click
Change adapter settings.
- Step 2 Right-click Local Area Connection and choose Properties. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.

🖞 Local Area Connection Properties 📃 💌									
Networking Sharing									
Connect using:									
Intel(R) 82583V Gigabit Network Connection									
Configure									
 Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder 									
Install Uninstall Properties									
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.									
OK Cancel									

Step 3 Select **Use the following IP address**. Set **IP address** to an IP address that is different from the IP address of the LAN port of the AP but belongs to the same network segment as the IP address of the LAN port of the AP. Set **Subnet mask** to **255.255.0**. Click **OK**.

Internet Protocol Version 4 (TCP/IPv4) Properties								
General								
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.								
Obtain an IP address automatically								
• Use the following IP address:								
IP address:	192.168.0.10							
S <u>u</u> bnet mask:	255 . 255 . 255 . 0							
Default gateway:	· · ·							
Obtain DNS server address autom	natically							
• Use the following DNS server add	resses:							
Preferred DNS server:								
Alternate DNS server:								
Vajidate settings upon exit								
OK Cancel								

The Local Area Connection Properties dialog box appears.

Step 4 Click OK.

---End

C. Default Parameter Settings

The following table lists the factory settings of the AP.

Parameter		Default Value		
	IP		192.168.0.254	
Login	Liser Name/Password	Administrator	admin/admin	
		User	user/user	
	Address Mode		Static IP	
	IP Address (management IF	Paddress)	192.168.0.254	
I AN Setun	Subnet Mask		255.255.255.0	
LAN Setup	Gateway	192.168.0.1		
	Primary DNS Server	192.168.0.1		
	Secondary DNS Server		None	

Parameter				Default Value
	Device Name			<i>Model+Hardware version number,</i> such as i12V1.0
DHCP Server		Disable		
	SNMP Agent			Disable
			Administrator Name	Administrator
SNMP			Device Name	<i>Model+Hardware version number,</i> such as i12V1.0
	SNMP Paramete	rs	Location	ShenZhen
			Read Community	public
			Read/Write Community	private
			Sync with Internet Time Servers	Enable
	System Time		Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei
Tools	Page Timeout			5 minutes
	Number of Logs			150
	Time Reboot			Disable
	LED Control			Switch on LEDs
		Enable Wireless		Enable
		Country		China
		Network Mode		11/b/g/n mixed
		Channel		Auto
Wireless	Radio Settings	Channel	Bandwidth	20/40
Settings	Radio Settings	Expansion Channel		Auto
		Channel Lockout		Enable
		SSID Isol	ation	Disable
		WMM C	apable	Enable
		APSD Ca	pable	Disable

Parameter		Default Value		
	Pacie Sottinge	SSID	Primary SSID	Tenda_XXXXXX, where XXXXXX indicates the last 6 characters in the MAC address specified on the label on the external surface of the AP
			Secondary SSID 1	Tenda_XXXXXX, where XXXXXX indicates the last 6 characters in the MAC address specified on the label on the external surface of the AP plus 1
			Secondary SSID 2	Tenda_XXXXXX, where XXXXXX indicates the last 6 characters in the MAC address specified on the label on the external surface of the AP plus 2
			Secondary SSID 3	Tenda_XXXXXX, where XXXXXX indicates the last 6 characters in the MAC address specified on the label on the external surface of the AP plus 3
	5	SSID Status	Primary SSID	Enable
			Secondary SSID	Disable
		Broadcast SSID		Enable
		AP Isolation		Disable
		Client Limit		16
		WMF		Disable
		Chinese SSID Encode		UTF-8
		Security Mode		None
		Beacon Interval		100ms
		Fragment Threshold		2346
	Advanced Settings	RTS Threshold		2347
		DTIM Interval		1
		Receive Signal Strength		-80dBm

Parameter		Default Value	
		Output Power	23dBm
		Power Lockout	Enable
		Preamble	Long Preamble
	Access Control		Disable
	QVLAN		Disable

Safety and Emission Statement

CE

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

Declaration of Conformity

Hereby, SHENZHEN TENDA TECHNOLOGY CO., LTD. declares that the radio equipment type i12 is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: http://www.tendacn.com/en/service/page/ce.html

Operate Frequency: 2412-2472 MHz EIRP Power (Max.): 19.8 dBm Software Version: V1.0.0



RECYCLING

This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.

User has the choice to give his product to a competent recycling organization or to the retailer when he buys new electrical or electronic equipment.



FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your

body.

Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.