

CHAPTER 7

Wireless

7.1 Wireless Overview

This chapter describes the Zyxel Device's **Network Setting > Wireless** screens. Use these screens to set up your Zyxel Device's WiFi connection and security settings.

7.1.1 What You Can Do in this Chapter

This section describes the Zyxel Device's **Wireless** screens. Use these screens to set up your Zyxel Device's wireless connection.

- Use the **General** screen to enable WiFi, enter the SSID and select the wireless security mode ([Section 7.2 on page 89](#)).
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device ([Section 7.3 on page 94](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device ([Section 7.4 on page 98](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 7.5 on page 100](#)).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications ([Section 7.6 on page 102](#)).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold ([Section 7.7 on page 103](#)).
- Use the **Channel Status** screen to scan WiFi channel noises and view the results ([Section 7.8 on page 105](#)).

7.1.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there are a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See [Section 7.9 on page 106](#) for advanced technical information on wireless networks.

7.2 Wireless General Settings

Use this screen to enable WiFi, enter the SSID and select the wireless security mode. These are basic elements for starting a wireless service. It's recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

Note: If you are configuring the Zyxel Device from a computer connected to WiFi and you change the Zyxel Device's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Zyxel Device's new settings.

Note: If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically.

Note: Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.

Click **Network Setting > Wireless** to open the **General** screen.

Figure 47 Network Setting > Wireless > General

A Wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than no security to protect your data from unauthorized access or damage via wireless network.

Wireless

Wireless ☒ Keep the same settings for 2.4G and 5G wireless networks

Wireless Network Setup

Band: 2.4GHz

Wireless: ☒

Channel: Auto Current : / MHz

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Company

Max Clients: 32

☐ Hide SSID Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.

☒ Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note

- (1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.
- (2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.
- (3) If Max. Upstream/Downstream Bandwidth is empty, the device sets the value automatically.
- (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID

Security Level

No Security More Secure (Recommended)

Security Mode: WPA2-PSK

☐ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password: Strength: strong

☒

Cancel Apply

The following table describes the general WiFi labels in this screen.

Table 19 Network Setting > Wireless > General


LABEL	DESCRIPTION
Wireless	
Wireless	Select Keep the same settings for 2.4G and 5G wireless networks and the 2.4 GHz and 5 GHz wireless networks will use the same SSID <u>and wireless security settings</u> .
Wireless Network Setup	
Band	This shows the wireless band which this radio profile is using. 2.4GHz is the frequency used by IEEE 802.11b/g/n/ax wireless clients while 5GHz is used by IEEE 802.11a/n/ac/ax wireless clients.
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Channel	<u>Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.</u> Use Auto to have the Zyxel Device automatically determine a channel to use.
Bandwidth	Select whether the Zyxel Device uses a wireless channel width of 20MHz , 40MHz , 20MHz/40MHz , 20MHz/40MHz/80MHz or 20MHz/40MHz/80MHz/160MHz . A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher. Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. <u>Because not all devices support 40 MHz and/or 160 MHz channels, select 20/40MHz or 20MHz/40MHz/80MHz/160MHz to allow the Zyxel Device to adjust the channel bandwidth automatically.</u>
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to 40MHz or 20MHz/40MHz . Set whether the control channel (set in the Channel field) should be in the Lower or Upper range of channel bands.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set Identity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This check box is grayed out if the WPS function is enabled in the Network Setting > Wireless > WPS screen.
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
Security Level	

Table 19 Network Setting > Wireless > General (continued)

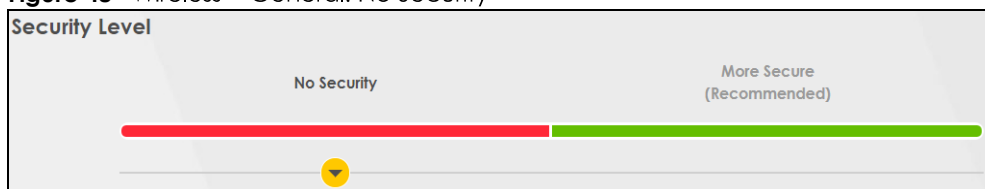
LABEL	DESCRIPTION
Security Mode	Select More Secure (Recommended) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

7.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the [Zyxel Device](#) without any data encryption or authentication.

Note: If you do not enable any wireless security on your Zyxel Device, your network is accessible to any wireless networking device that is within range.

Figure 48 Wireless > General: No Security



The following table describes the labels in this screen.

Table 20 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose No Security to allow all wireless connections without data encryption or authentication.

7.2.2 More Secure (Recommended)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the Zyxel Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Setting > Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA2-PSK** or **WPA2-EAP** from the **Security Mode** list.

Figure 49 Wireless > General: More Secure: WPA2-PSK

Security Level

No Security More Secure
(Recommended)

Security Mode: WPA2-PSK

☐ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password:

Strength: strong

Encryption: AES

Timer: 3600 sec

The following table describes the labels in this screen.

Table 21 Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select More Secure to enable WPA2-PSK- or WPA2-EAP data encryption.
Security Mode	Select WPA2-PSK - or WPA2-EAP from the drop-down list box.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	<p>Select Generate password automatically or enter a Password.</p> <p>The password has two uses.</p> <ol style="list-style-type: none"> 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. <p>Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it is hidden.</p>
	Click this to show more fields in this section. Click again to hide them.
Encryption	This field shows the AES type of data encryption.
WPA2 Pre-authentication	<p>This option is available only when you select WPA2-EAP in the Security Mode field. When the switch goes to the right , the function is enabled. Otherwise, it is not.</p> <p>Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Click this switch to turn on pre-authentication in WAP2.</p>

Table 21 Wireless > General: More Secure: WPA2-PSK (continued)

LABEL	DESCRIPTION
Network Re-auth Interval	This option is available only when you select WPA2-EAP in the Security Mode field. Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 2147483647 seconds. Note: If wireless client authentication is done using a RADIUS server, the re-authentication timer on the RADIUS server has priority.
Timer	The Timer is the rate at which the RADIUS server sends a new group key out to all clients.

7.3 Guest/More AP

This screen allows you to configure a guest wireless network that allows access to the Internet only through the Zyxel Device. You can also configure additional wireless networks, each with different security settings, in this screen.







Click **Network Setting > Wireless > Guest/More AP**. The following screen displays.

The following table introduces the supported wireless networks.

Table 22 Supported Wireless Networks

WIRELESS NETWORKS	WHERE TO CONFIGURE
Main/1	Network Setting > Wireless > General screen
Guest/3	Network Setting > Wireless > Guest/More AP screen

Figure 50 Network Setting > Wireless > Guest/More AP

This device can enable up to 4 wireless networks to work at the same time. Assign a name and a security level (if needed) to start the 2nd, 3rd, and 4th wireless network services.					
#	Status	SSID	Security	Guest WLAN	Modify
1		ZyxeL_9DE5_guest1	WPA2-Personal	External Guest	
2		ZyxeL_9DE5_guest2	WPA2-Personal	External Guest	
3		ZyxeL_9DE5_guest3	WPA2-Personal	External Guest	

The following table describes the labels in this screen.

Table 23 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active, while a gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the Zyxel Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.

Table 23 Network Setting > Wireless > Guest/More AP (continued)

LABEL	DESCRIPTION
Guest WLAN	<p>This displays if the guest WiFi function has been enabled for this wireless LAN.</p> <p>If Home Guest displays, clients can connect to each other directly.</p> <p>If External Guest displays, clients are blocked from connecting to each other directly.</p> <p>N/A displays if guest WLAN is disabled.</p>
Modify	Click the Edit icon to configure the SSID profile.

7.3.1 The Edit Guest/More AP Screen

Use this screen to create Guest and additional wireless networks with different security settings.

Note: If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.

Click the **Edit** icon next to an SSID in the **Guest/More AP** screen. The following screen displays.

Figure 51 Network Setting > Wireless > Guest/More AP > Edit

More AP Edit

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless

Security Level

Wireless Network Name

Zyxel_9DE5_guest2_5G

Hide SSID

Guest WLAN

Access Scenario

External Guest

Max. Upstream Bandwidth

Kbps

Max. Downstream Bandwidth

Kbps

Note

(1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.

(2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.

(3) If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

(4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID

00:00:00:00:00:00

SSID Subnet

DHCP Start Address

DHCP End Address

SSID Subnet Mask

LAN IP Address

Security Level

No Security

More Secure (Recommended)

Security Mode

WPA2-PSK

Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password

Strength

weak

Encryption

AES

Timer

3600

sec

Cancel

OK

The following table describes the fields in this screen.

Table 24 Network Setting > Wireless > Guest/More AP > Edit





LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue  , the function is enabled; otherwise, it is not.
Security Level	
Wireless Network Name	The SSID (Service Set Identity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WiFi for home and external clients. Select the WiFi type in the Access Scenario field.
Access Scenario	If you select Home Guest , clients can connect to each other directly. If you select External Guest , clients are blocked from connecting to each other directly.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
SSID Subnet	Click on this switch to Enable this function if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients. This option cannot be used if the WPS function is enabled in the Network Setting > Wireless > WPS screen or if the Keep the same settings for 2.4G and 5G wireless networks check box is selected in Network Setting > Wireless > General .
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool. The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	Select More Secure (Recommended) to add security on this wireless network. The wireless clients which want to associate to this network must have the same wireless security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 92 for more details about this field.
Security Mode	Select WPA2-PSK or WPA2-EAP from the drop-down list box.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.

Table 24 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. If you did not select Generate password automatically , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it is hidden.
	Click this  to show more fields in this section. Click again to hide them.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Zyxel Device. The key must be the same on the external authentication server and the Zyxel Device. The key is not sent over the network.
Encryption	This field shows the AES type of data encryption.
WPA2 Pre-authentication	This option is available only when you select WPA2-EAP in the Security Mode field. When the switch goes to the right , the function is enabled. Otherwise, it is not. Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Click this switch to turn on pre-authentication in WAP2.
Network Re-auth Interval	This option is available only when you select WPA2-EAP in the Security Mode field. Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 2147483647 seconds. Note: If wireless client authentication is done using a RADIUS server, the re-authentication timer on the RADIUS server has priority.
Timer	The Timer is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

7.4 MAC Authentication

This screen allows you to configure the Zyxel Device to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the Zyxel Device (**Deny**) based on the device(s) MAC address. Every Ethernet device has a unique MAC (Media Access Control) address. It is assigned at the factory and consists of six pairs of hexadecimal characters; for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the device(s) you want to allow/deny to configure this screen.

Note: You can have up to 25 MAC authentication rules.

Use this screen to view your Zyxel Device's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless > MAC Authentication**. The screen appears as shown.

Figure 52 Network Setting> Wireless > MAC Authentication

MAC Authentication can allow or block the access of the device(s) to your wireless network. Edit the list in the table to decide the rule of the access on device(s)

General

SSID: Zyxel_8760

MAC Restrict Mode: ☐ Disable ☐ Deny ☒ Allow

MAC address List

+ Add new MAC address

#	MAC Address	Modify

Note
A maximum of 25 MAC Authentication rules can be configured.

Cancel Apply

The following table describes the labels in this screen.

Table 25 Network Setting > Wireless > MAC Authentication

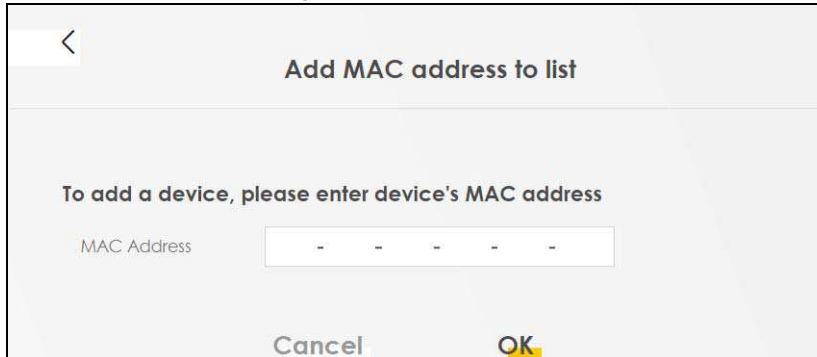
LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	<p>Define the filter action for the list of MAC addresses in the MAC Address table.</p> <p>Select Disable to turn off MAC filtering.</p> <p>Select Deny to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device.</p> <p>Select Allow to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device.</p>
MAC Address List	
Add New MAC Address	<p>This field is available when you select Deny or Allow in the MAC Restrict Mode field.</p> <p>Click this if you want to add a new MAC address entry to the MAC filter list below.</p>
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the Zyxel Device.
Modify	<p>Click the Edit icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).</p> <p>Click the Delete icon to delete the entry.</p>
Cancel	Click Cancel to restore your previously saved settings .
Apply	Click Apply to save your changes.

7.4.1 Add/Edit MAC Addresses

Click **Add new MAC address** in the **Network Setting > Wireless > MAC Authentication** screen to add a new MAC address. You can also click the Edit icon next to a MAC authentication rule to edit the rule.

Enter the MAC addresses of the wireless devices that are allowed or denied access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

Figure 53 Network Setting> Wireless > MAC Authentication > Add/Edit



7.5 WPS Settings

WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your wireless client supports it. See [Section 7.9.8.3 on page 114](#) for more information about WPS.

Note: The Zyxel Device applies the security settings of the main SSID (SSID1) profile (see [Section 7.2 on page 89](#)). ~~If you want to use the WPS feature, make sure you have set the security mode of SSID1 to WPA2-PSK or No Security.~~

Note: If WPS is enabled, UPnP will automatically be turned on.

Note: The WPS switch is grayed out when WiFi is disabled.

Click **Network Setting > Wireless > WPS**. The following screen displays. Click this switch and makes it turn blue. Click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.


Figure 54 Network Setting > Wireless > WPS

Enabling Wireless Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS.

General


WPS ☒

Add a new device with WPS Method

 **Method 1**
PBC ☒

Step1. Click WPS button **WPS**


Step2. Press the WPS button on your new wireless client device within 120 seconds

 **Method 2**
PIN ☐

Step1. Enter the PIN of your new wireless client device and then click Register

Register

Step2. Press the WPS button on your new wireless client device within 120 seconds

 **Method 3** ☐

Enter AP's PIN Number in wireless Client


Current state Configured

1 Please release configuration if you want to configure the wireless settings

Release Configuration

2 Enter current PIN number on your wireless client

Generate New PIN

 **Note**

(1) If WPS is Enabled, UPnP will automatically be turned on.
 (2) This feature is available only when WPA2-PSK or No Security mode is configured.
 (3) The WPS button will be grey-out when wireless or WPS is disabled

Cancel **Apply**

The following table describes the labels in this screen.

Table 26 Network Setting > Wireless > WPS


LABEL	DESCRIPTION
General	
WPS	Click this switch to activate or deactivate WPS on this Zyxel Device. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click Apply to activate WPS method 1 on the Zyxel Device.
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the Zyxel Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the WPS button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the Zyxel Device. Click this switch and make it turn blue. Click Apply to activate WPS method 2 on the Zyxel Device.

Table 26 Network Setting > Wireless > WPS (continued)

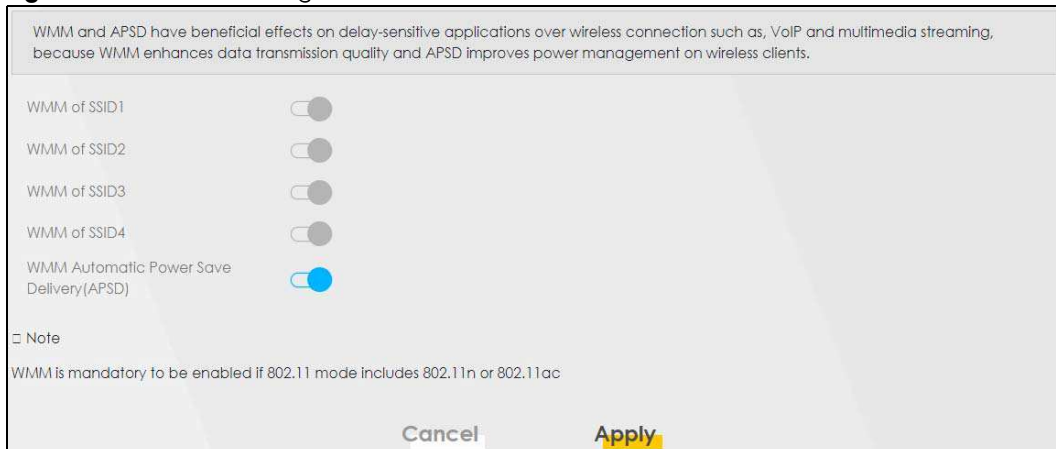
LABEL	DESCRIPTION
Register	<p>Enter the PIN of the device that you are setting up a WPS connection with and click Register to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Zyxel Device.</p>
Method 3	<p>Use this section to set up a WPS wireless network by entering the PIN of the Zyxel Device into the client. Click this switch and make it turn blue. Click Apply to activate WPS method 3 on the Zyxel Device.</p>
Release Configuration	<p>The default WPS status is configured.</p> <p>Click this button to remove all configured wireless and wireless security settings for WPS connections on the Zyxel Device.</p>
Generate New PIN	<p>If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS.</p> <p>The PIN is not necessary when you use the WPS push-button method.</p> <p>Click the Generate New PIN button to have the Zyxel Device create a new PIN.</p>
Cancel	<p>Click Cancel to restore your previously saved settings.</p>
Apply	<p>Click Apply to save your changes.</p>

7.6 WMM Settings

Use this screen to enable WiFi MultiMedia (**WMM**) and **WMM Automatic Power Save (APSD)** in wireless networks for multimedia applications. **WMM** enhances data transmission quality, while **APSD** improves power management of wireless clients. This allows delay-sensitive applications, such as voice and videos, to run more smoothly.

Click **Network Setting > Wireless > WMM** to display the following screen.

Figure 55 Network Setting > Wireless > WMM



Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

The following table describes the labels in this screen.

Table 27 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM of SSID1~4	Select On to have the Zyxel Device automatically give the wireless network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. If the 802.11 Mode in Network Setting > Wireless > Others is set to include 802.11n or 802.11ac, WMM cannot be disabled.
WMM Automatic Power Save Delivery (APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Zyxel Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Zyxel Device until the Zyxel Device "wakes up". The Zyxel Device wakes up periodically to check for incoming data. Note: This works only if the wireless device to which the Zyxel Device is connected also supports this feature.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

7.7 Others Settings

Use this screen to configure advanced wireless settings, such as additional security settings, power saving, and data transmission settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See [Section 7.9.2 on page 108](#) for detailed definitions of the terms listed in this screen.

Figure 56 Network Setting > Wireless > Others

The configurations below are the advanced wireless settings.

RTS/CTS Threshold	2347	
Fragmentation Threshold	2346	
Output Power	100%	
Beacon Interval	100	ms
DTIM Interval	1	ms
802.11 Mode	802.11b/g/n/ax Mixed	
802.11 Protection	Auto	
Preamble	Long	
Protected Management Frames	Capable	

Cancel Apply

The following table describes the labels in this screen.

Table 28 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: 20%, 40%, 60%, 80% or 100%.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50 ms to 1000 ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	<p>For 2.4 GHz frequency WiFi devices:</p> <ul style="list-style-type: none"> • Select 802.11b Only to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select 802.11g Only to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11b/g/n Mixed to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11b/g/n/ax Mixed to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. <p>For 5 GHz frequency WiFi devices:</p> <ul style="list-style-type: none"> • Select 802.11a Only to allow only IEEE 802.11a compliant WiFi devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select 802.11ac Only to allow only IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. • Select 802.11a/n Mixed to allow either IEEE 802.11a or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11n/ac Mixed to allow either IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11a/n/ac Mixed to allow IEEE 802.11a, IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11a/n/ac/ax Mixed to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.

Table 28 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select Off to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network.</p> <p>This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.</p>
Preamble	<p>Select a preamble type from the drop-down list box. Choices are Long or Short. See Section 7.9.7 on page 111 for more information.</p> <p>This field is configurable only when you set 802.11 Mode to 802.11b or 802.11b/g Mixed.</p>
Protected Management Frames	<p>This option is only available when using WPA2-PSK as the Security Mode and AES Encryption in Network Setting > Wireless > General. Management frame protection (MFP) helps prevent wireless DoS attacks.</p> <p>Select Disable if you do not want to use MFP.</p> <p>Select Capable to encrypt management frames of wireless clients that support MFP. Clients that do not support MFP will still be allowed to join the wireless network, but remain unprotected.</p> <p>Select Required to allow only clients that support MFP to join the wireless network.</p>
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

7.8 Channel Status Settings

Use the **Channel Status** screen to scan WiFi channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **Scan** to scan the wireless LAN channels. You can view the results in the **Channel Scan Result** section.

Note: If the current channel is a DFS channel, the warning 'Channel scan process is denied because current channel is a DFS channel (Channel: 52~140). If you want to run channel scan, please select a non-DFS channel and try again.' appears.

Figure 57 Network Setting > Wireless > Channel Status

7.9 Technical Reference

This section discusses WiFi in depth. For more information, see [Appendix B on page 283](#).

7.9.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

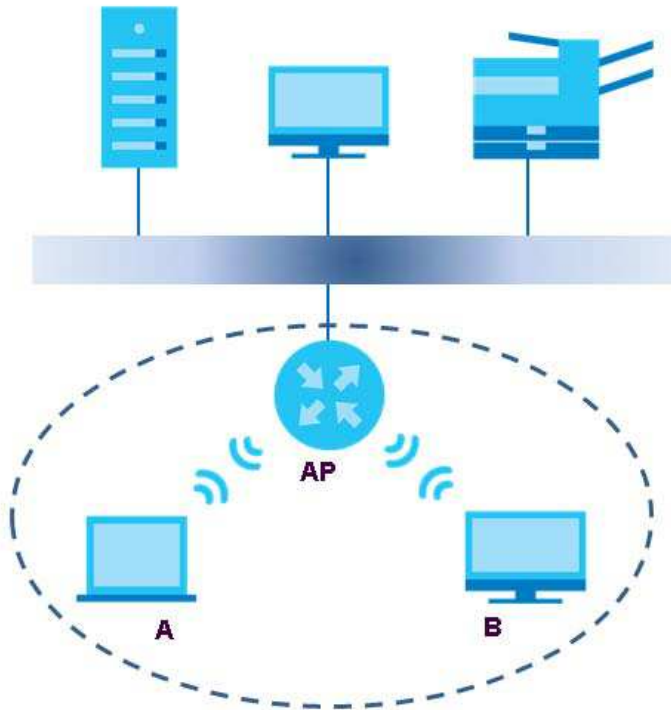
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 58 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set Identifier.
- If two wireless networks overlap, they should use a different channel.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

7.9.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the Zyxel Device's Web Configurator.

Table 29 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the Zyxel Device. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the Zyxel Device.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the Zyxel Device does, it cannot communicate with the Zyxel Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

7.9.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is

Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

7.9.3.1 SSID

Normally, the Zyxel Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the Zyxel Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

7.9.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the Zyxel Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

7.9.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

-
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

7.9.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

7.9.4 Signal Problems

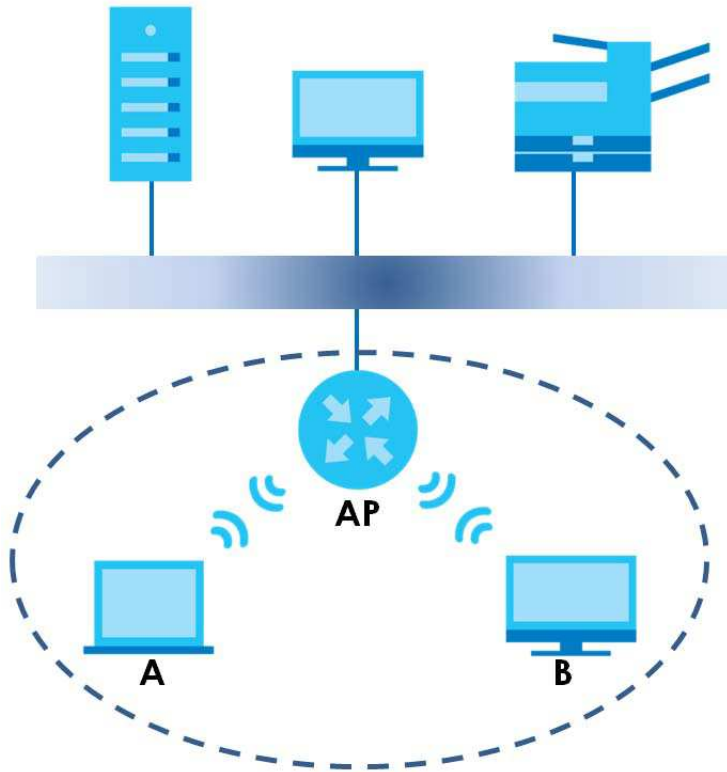
Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.9.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 59 Basic Service set

7.9.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Zyxel Device's MBSSID (Multiple Basic Service Set Identifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

7.9.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

7.9.7 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the Zyxel Device uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

7.9.8 WiFi Protected Setup (WPS)

Your Zyxel Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.9.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Zyxel Device, see [Section 7.6 on page 102](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the Zyxel Device you must press the WPS button for more than five seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.9.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

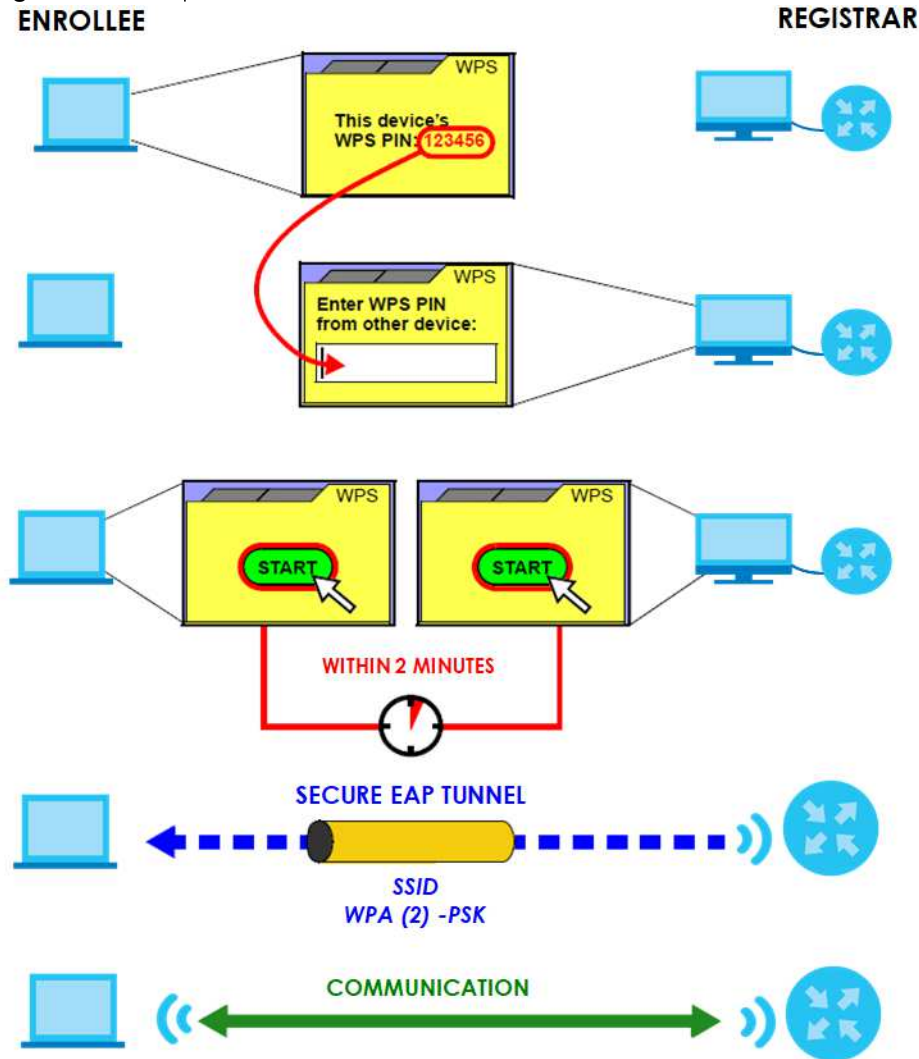
When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the Zyxel Device, see [Section 7.5 on page 100](#)).
- 4 Enter the client's PIN in the AP's configuration interface.
- 5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6 Start WPS on both devices within two minutes.
- 7 Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

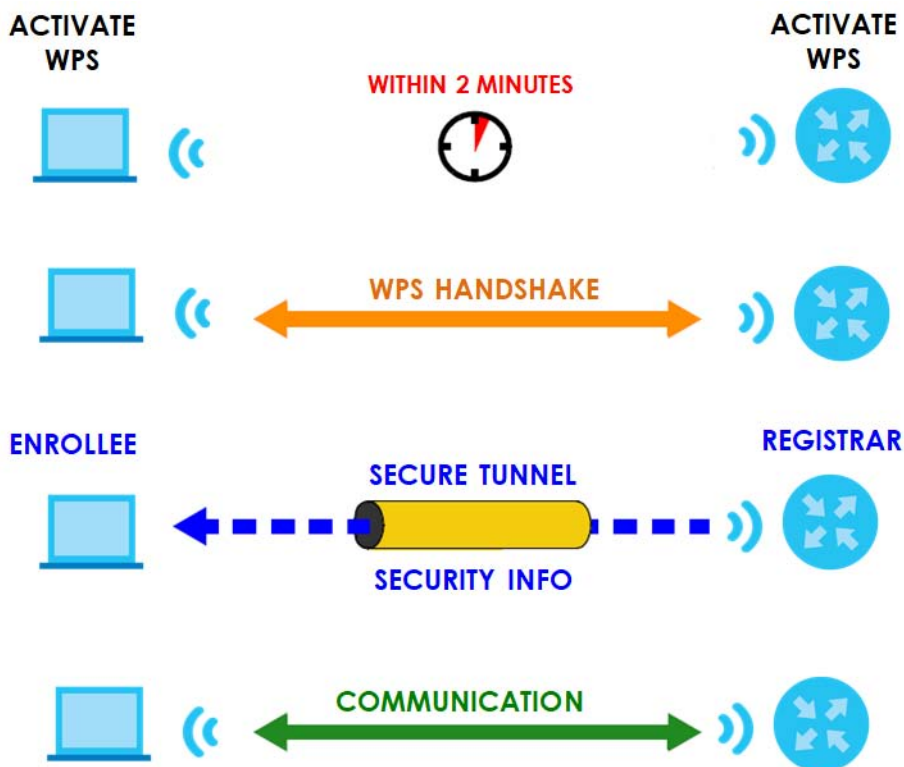
The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 60 Example WPS Process: PIN Method

7.9.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA2-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 61 How WPS works

The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS device is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

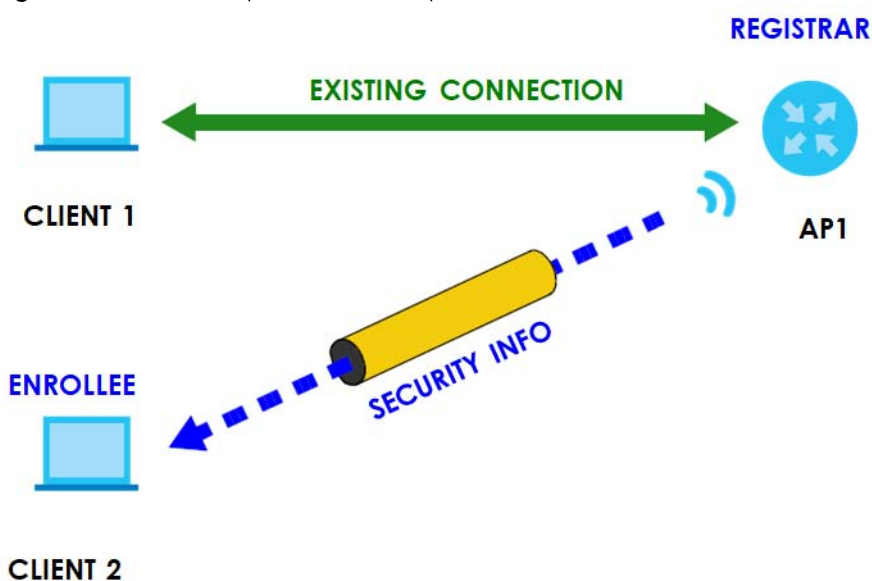
7.9.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

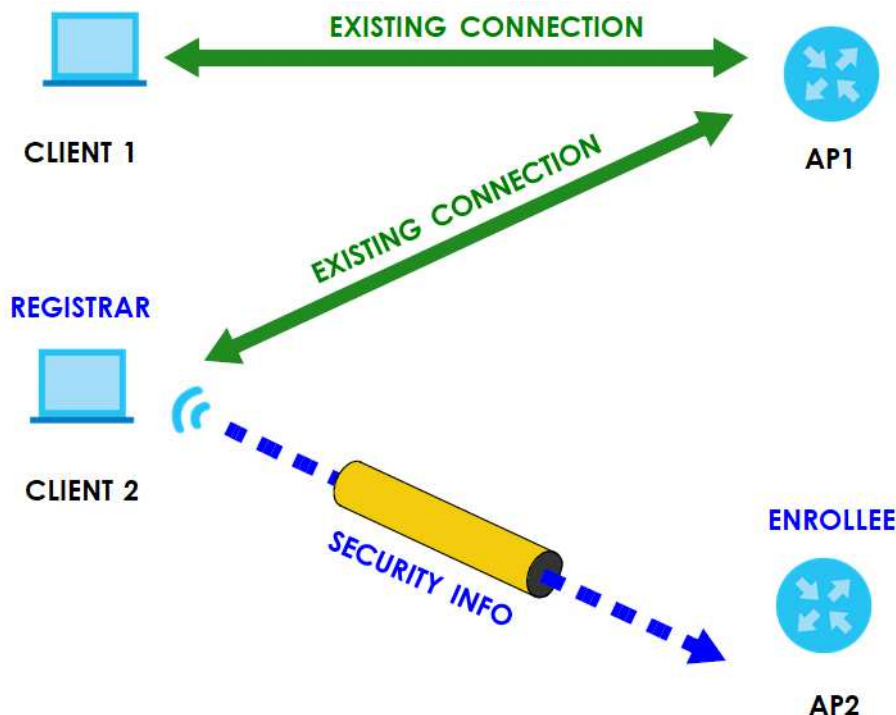
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 62 WPS: Example Network Step 1

In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 63 WPS: Example Network Step 2

In step **3**, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 64 WPS: Example Network Step 3

7.9.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously; you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access

point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.