## Contents

**Introduction**
- Before you begin .................................................. 9
- How this guide is organized ....................................... 9

**Introduction to wireless networking** 11
- Wireless concepts .................................................. 11
  - Bands and channels .............................................. 11
  - Power ............................................................... 12
  - Antennas .......................................................... 12
- Security .............................................................. 12
  - Whether to broadcast SSID ...................................... 12
  - Encryption ......................................................... 12
  - Separate access for employees and guests .................. 13
  - Captive portal ................................................... 13
  - Power ............................................................... 13
  - Monitoring for rogue APs ...................................... 13
  - Suppressing rogue APs ......................................... 14
- Authentication ....................................................... 14
- Wireless networking equipment ................................... 14
  - FortiWiFi units ................................................... 14
    - Using a FortiWiFi unit as a managed AP ....................... 15
  - FortiAP units .................................................... 16
  - Third-party WAPs ................................................ 16
- Deployment considerations ......................................... 16
  - Types of wireless deployment ................................ 16
  - Deployment methodology ....................................... 16
    - Evaluating the coverage area environment ................ 16
    - Positioning access points ................................... 17
    - Selecting access point hardware ............................ 18
  - Single access point networks ................................ 18
  - Multiple access point networks ............................... 18
  - Fast Roaming .................................................... 19
- Automatic Radio Resource Provisioning .......................... 19

**Configuring a WiFi LAN** 21
- Overview of WiFi controller configuration ..................... 21
  - About SSIDs on FortiWiFi units ............................... 22
  - About automatic AP profile settings ........................ 22
  - Process to create a wireless network ........................ 23
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting your geographic location</td>
<td>23</td>
</tr>
<tr>
<td>Creating a custom AP Profile</td>
<td>23</td>
</tr>
<tr>
<td>Defining a wireless network interface (SSID)</td>
<td>25</td>
</tr>
<tr>
<td>Configuring DHCP for WiFi clients</td>
<td>26</td>
</tr>
<tr>
<td>Configuring security</td>
<td>26</td>
</tr>
<tr>
<td>WPA-Personal security</td>
<td>27</td>
</tr>
<tr>
<td>WPA-Enterprise security</td>
<td>27</td>
</tr>
<tr>
<td>Captive Portal security</td>
<td>28</td>
</tr>
<tr>
<td>Adding a MAC filter</td>
<td>29</td>
</tr>
<tr>
<td>Configuring user authentication</td>
<td>30</td>
</tr>
<tr>
<td>WPA-Enterprise authentication</td>
<td>30</td>
</tr>
<tr>
<td>Creating a wireless user group</td>
<td>30</td>
</tr>
<tr>
<td>Configuring firewall policies for the SSID</td>
<td>31</td>
</tr>
<tr>
<td>Customizing captive portal pages</td>
<td>32</td>
</tr>
<tr>
<td>Modifying the login page</td>
<td>32</td>
</tr>
<tr>
<td>Changing the logo</td>
<td>33</td>
</tr>
<tr>
<td>Modifying text</td>
<td>33</td>
</tr>
<tr>
<td>Modifying the login failed page</td>
<td>34</td>
</tr>
<tr>
<td>Modifying the Disclaimer page</td>
<td>34</td>
</tr>
<tr>
<td>Modifying the Declined Disclaimer page</td>
<td>36</td>
</tr>
<tr>
<td>Enabling the disclaimer page</td>
<td>36</td>
</tr>
<tr>
<td>Configuring the built-in access point on a FortiWiFi unit</td>
<td>37</td>
</tr>
<tr>
<td>Access point deployment</td>
<td>39</td>
</tr>
<tr>
<td>Overview</td>
<td>39</td>
</tr>
<tr>
<td>Network topology for managed APs</td>
<td>39</td>
</tr>
<tr>
<td>Discovering and authorizing APs</td>
<td>40</td>
</tr>
<tr>
<td>Configuring the network interface for the AP unit</td>
<td>41</td>
</tr>
<tr>
<td>Configure the DHCP server for AP units</td>
<td>41</td>
</tr>
<tr>
<td>Enabling a discovered AP</td>
<td>42</td>
</tr>
<tr>
<td>Configuring a managed AP</td>
<td>42</td>
</tr>
<tr>
<td>Updating FortiAP unit firmware</td>
<td>44</td>
</tr>
<tr>
<td>Updating FortiAP firmware from the FortiGate unit</td>
<td>44</td>
</tr>
<tr>
<td>Updating FortiAP firmware from the FortiAP unit</td>
<td>44</td>
</tr>
<tr>
<td>Advanced WiFi controller discovery</td>
<td>45</td>
</tr>
<tr>
<td>Controller discovery methods</td>
<td>45</td>
</tr>
<tr>
<td>Static IP configuration</td>
<td>45</td>
</tr>
<tr>
<td>Broadcast request</td>
<td>45</td>
</tr>
<tr>
<td>Multicast request</td>
<td>45</td>
</tr>
<tr>
<td>DHCP</td>
<td>46</td>
</tr>
<tr>
<td>Connecting to the FortiAP CLI</td>
<td>46</td>
</tr>
<tr>
<td>Configuring a FortiWiFi unit as a WiFi AP</td>
<td>47</td>
</tr>
<tr>
<td>Setting the discovery mode</td>
<td>47</td>
</tr>
</tbody>
</table>
Completing configuration ...................................................... 47
Multi-AP networks ............................................................... 47
Configuration of a WLAN with multiple APs ......................... 48

Wireless network monitoring .................................................. 49
Monitoring wireless clients ..................................................... 49
Monitoring rogue APs ............................................................. 49
  On-wire rogue AP detection technique .................................. 50
  Exact MAC address match .................................................... 50
  MAC adjacency .................................................................... 50
  Limitations ........................................................................... 50
  Logging ................................................................................ 50
Rogue AP scanning as a background activity ............................. 51
  Configuring rogue scanning ................................................ 51
  Exempting an AP from rogue scanning ................................. 52
  Monitoring with a FortiWiFi unit .......................................... 52
  Using the Rogue AP Monitor .............................................. 52
Suppressing rogue APs .............................................................. 53

Configuring wireless network clients ......................................... 55
Windows XP client ................................................................. 56
Windows 7 client ................................................................. 60
Mac OS client ........................................................................ 61
Linux client ............................................................................ 63
Troubleshooting ..................................................................... 65
  Checking that the client has received IP address and DNS server information ....................................... 65

Wireless network examples ....................................................... 67
Basic wireless network ............................................................. 67
  Configuring authentication for wireless users ....................... 67
  Configuring the SSID ............................................................. 68
  Configuring firewall policies ............................................... 69
  Connecting the FortiAP units .............................................. 70
A more complex example .......................................................... 71
  Scenario .............................................................................. 71
  Configuration ...................................................................... 72
Configuring authentication for employee wireless users .......... 72
Configuring authentication for guest wireless users ................. 72
Configuring the SSIDs .......................................................... 74
Configuring the custom AP profile ......................................... 76
Configuring firewall policies .................................................. 77
Customizing the captive portal ............................................... 79
Connecting the FortiAP units .................................................. 79
**Using a FortiWiFi unit as a client**  
Use of client mode ..................................................... 81  
Configuring client mode ............................................. 82

**WiFi Reference** .......................................................... 83  
Wireless radio channels ................................................. 83

**WiFi Controller Reference** ........................................... 85  
WiFi Controller overview ............................................... 85  
WiFi Network ............................................................... 86  
SSID list ........................................................................... 86  
SSID configuration settings ............................................. 88  
Rogue AP Settings ......................................................... 89  
Managed access points ................................................... 90  
Local WiFi Radio configuration settings ......................... 90  
Managed FortiAP list ....................................................... 91  
Managed FortiAP configuration settings ......................... 92  
Custom AP Profiles ....................................................... 93  
Custom AP Profile Settings ............................................ 94

**Monitor** ........................................................................ 95  
Client Monitor ............................................................... 95  
Rogue AP Monitor ......................................................... 96

**Appendix** ...................................................................... 98  
Document conventions .................................................. 98  
IP addresses ................................................................. 98  
Example Network configuration ..................................... 100  
Cautions, Notes and Tips ............................................... 101  
Typographical conventions ........................................... 102  
CLI command syntax conventions .................................. 102  
Entering FortiOS configuration data ................................. 104  
Entering text strings (names) ......................................... 104  
Entering numeric values ............................................... 105  
Selecting options from a list ......................................... 105  
Enabling or disabling options ........................................ 105  
Registering your Fortinet product ................................... 105  
Fortinet products End User License Agreement .................. 105  
Training .......................................................................... 106  
Documentation ................................................................ 106  
Fortinet Tools and Documentation CD ............................ 106  
Fortinet Knowledge Base .............................................. 106  
Comments on Fortinet technical documentation ................ 106  
Customer service and technical support ......................... 106
Index

107
Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This document describes how to configure wireless networks with FortiWiFi, FortiGate, and FortiAP units.

This chapter contains the following topics:
- Before you begin
- How this guide is organized

Before you begin

Before you begin using this guide, please ensure that:
- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- FortiGuard Analysis & Management Service is properly configured.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:
- Introduction to wireless networking explains the basic concepts of wireless networking and how to plan your wireless network.
- Configuring a WiFi LAN explains how to set up a basic wireless network, prior to deploying access point hardware.
- Access point deployment explains how to deploy access point hardware and add it to your wireless network configuration.
- Wireless network monitoring explains how to monitor your wireless clients and how to monitor other wireless access points, potentially rogues, in your coverage area.
- Configuring wireless network clients explains how to configure typical wireless clients to work with a WPA-Enterprise protected network.
- Wireless network examples provides two examples. The first is a simple WiFi network using automatic configuration. The second is a more complex example of a business with two WiFi networks, one for employees and another for guests or customers.
- Using a FortiWiFi unit as a client explains how to use a FortiWiFi unit as a wireless client to connect to other WiFi networks. This connection can take the place of an Ethernet connection where wired access to a network or to the Internet is not available.
WiFi Reference provides information about WiFi radio channels.

WiFi Controller Reference details the web-based manager pages that configure the WiFi controller, manage access points, and monitor your WiFi network.

Appendix contains documentation conventions, information about using the CLI, and customer support information.
Introduction to wireless networking

This chapter introduces some concepts you should understand before working with wireless networks, describes Fortinet’s wireless equipment, and then describes the factors you need to consider in planning deployment of a wireless network.

The following topics are included in this section:

- Wireless concepts
- Security
- Authentication
- Wireless networking equipment
- Deployment considerations
- Automatic Radio Resource Provisioning

Wireless concepts

Wireless networking is radio technology, subject to the same characteristics and limitations as the familiar audio and video radio communications. Various techniques are used to modulate the radio signal with a data stream.

Bands and channels

Depending on the wireless protocol selected, you have specific channels available to you, depending on what region of the world you are in.

- IEEE 802.11a,b,and g protocols provide up to 14 channels in the 2.400-2.500 GHz Industrial, Scientific and Medical (ISM) band.
- IEEE 802.11a,n (5.150-5.250, 5.250-5.350, 5.725–5.875 GHz, up to 16 channels) in portions of Unlicensed National Information Infrastructure (U-NII) band

Note that the width of these channels exceeds the spacing between the channels. This means that there is some overlap, creating the possibility of interference from adjacent channels, although less severe than interference on the same channel. Truly non-overlapping operation requires the use of every fourth or fifth channel, for example ISM channels 1, 6 and 11.

The capabilities of your wireless clients is the deciding factor in your choice of wireless protocol. If your clients support it, 5GHz protocols have some advantages. The 5GHz band is less used than 2.4GHz and its shorter wavelengths have a shorter range and penetrate obstacles less. All of these factors mean less interference from other access points, including your own.

When configuring your WAP, be sure to correctly select the Geography setting to ensure that you have access only to the channels permitted for WiFi use in your part of the world.

For detailed information about the channel assignments for wireless networks for each supported wireless protocol, see “Wireless radio channels” on page 83.
Power

Wireless LANs operate on frequencies that require no license but are limited by regulations to low power. As with other unlicensed radio operations, the regulations provide no protection against interference from other users who are in compliance with the regulations.

Power is often quoted in dBm. This is the power level in decibels compared to one milliwatt. 0dBm is one milliwatt, 10dBm is 10 milliwatts, 27dBm, the maximum power on Fortinet FortiAP equipment, is 500 milliwatts. The FortiGate unit limits the actual power available to the maximum permitted in your region as selected by the WiFi controller country setting.

Received signal strength is almost always quoted in dBm because the received power is very small. The numbers are negative because they are less than the one milliwatt reference. A received signal strength of -60dBm is one millionth of a milliwatt or one nanowatt.

Antennas

Transmitted signal strength is a function of transmitter power and antenna gain. Directional antennas concentrate the signal in one direction, providing a stronger signal in that direction than would an omnidirectional antenna.

FortiWiFi units have detachable antennas. However, these units receive regulatory approvals based on the supplied antenna. Changing the antenna might cause your unit to violate radio regulations.

Security

There are several security issues to consider when setting up a wireless network.

Whether to broadcast SSID

Users who want to use a wireless network must configure their computers with the wireless service set identifier (SSID) or network name. Broadcasting the SSID makes connection to a wireless network easier because most wireless client applications present the user with a list of network SSIDs currently being received. This is desirable for a public network.

To obscure the presence of a wireless network, do not broadcast the SSID. This does not prevent attempts at unauthorized access, however, because the network is still detectable with wireless network “sniffer” software.

Encryption

Wireless networking supports the following security modes for protecting wireless communication, listed in order of increasing security.

None — Open system. Any wireless user can connect to the wireless network.

WEP64 — 64-bit Web Equivalent Privacy (WEP). This encryption requires a key containing 10 hexadecimal digits.

WEP128 — 128-bit WEP. This encryption requires a key containing 26 hexadecimal digits.

WPA — 256-bit Wi-Fi Protected Access (WPA) security. This encryption can use either the TKIP or AES encryption algorithm and requires a key of either 64 hexadecimal digits or a text phrase of 8 to 63 characters. It is also possible to use a RADIUS server to store a separate key for each user.
WPA2 — WPA with security improvements fully meeting the requirements of the IEEE 802.11i standard. Configuration requirements are the same as for WPA.

For best security use the WPA2 with AES encryption and a RADIUS server to verify individual credentials for each user. WEP, while better than no security at all, is an older algorithm that is easily compromised. With either WEP or WAP, changing encryption passphrases on a regular basis further enhances security.

Separate access for employees and guests

Wireless access for guests or customers should be separate from wireless access for your employees. This does not require additional hardware. Both FortiWiFi units and FortiAP units support multiple wireless LANs on the same access point. Each of the two networks can have its own SSID, security settings, firewall policies, and user authentication.

A good practice is to broadcast the SSID for the guest network to make it easily visible to users, but not to broadcast the SSID for the employee network.

Two separate wireless networks are possible because multiple virtual APs can be associated with an AP profile. The same physical APs can provide two or more virtual WLANs.

Captive portal

As part of authenticating your users, you might want them to view a web page containing your acceptable use policy or other information. This is called a captive portal. No matter what URL the user initially requested, the portal page is returned. Only after authenticating and agreeing to usage terms can the user access other web resources.

For information about setting up a captive portal, see “Captive Portal security” on page 28.

Power

Reducing power reduces unwanted coverage and potential interference to other WLANs. Areas of unwanted coverage are a potential security risk. There are people who look for wireless networks and attempt to access them. If your office WLAN is receivable out on the public street, you have created an opportunity for this sort of activity.

Monitoring for rogue APs

It is likely that there are APs available in your location that are not part of your network. Most of these APs belong to neighboring businesses or homes. They may cause some interference, but they are not a security threat. There is a risk that people in your organization could connect unsecured WiFi-equipped devices to your wired network, inadvertently providing access to unauthorized parties. The optional On-Wire Rogue AP Detection Technique compares MAC addresses in the traffic of suspected rogues with the MAC addresses on your network. If wireless traffic to non-Fortinet APs is also seen on the wired network, the AP is a rogue, not an unrelated AP.

Decisions about which APs are rogues are made manually on the Rogue AP monitor page. For detailed information about monitoring rogue APs, see “Monitoring rogue APs” on page 49.
Supressing rogue APs

When you have declared an AP to be a rogue, you have the option of suppressing it. To suppress and AP, the FortiGate WiFi controller sends reset packets to the rogue AP. Also, the MAC address of the rogue AP is blocked in the firewall policy. You select the suppression action on the Rogue AP monitor page. For more information, see “Suppressing rogue APs” on page 53.

Authentication

Wireless networks usually require authenticated access. FortiOS authentication methods apply to wireless networks the same as they do to wired networks because authentication is applied in the firewall policy.

The types of authentication that you might consider include:

- user accounts stored on the FortiGate unit
- user accounts managed and verified on an external RADIUS, LDAP or TACACS+ server
- Windows Active Directory authentication, in which users logged on to a Windows network are transparently authenticated to use the wireless network.

This Wireless chapter of the FortiOS Handbook will provide some information about each type of authentication, but more detailed information is available in the Authentication chapter.

What all of these types of authentication have in common is the use of user groups to specify who is authorized. For each wireless LAN, you will create a user group and add to it the users who can use the WLAN. In the identity-based firewall policies that you create for your wireless LAN, you will specify this user group.

Some access points, including FortiWiFi units, support MAC address filtering. You should not rely on this alone for authentication. MAC addresses can be "sniffed" from wireless traffic and used to impersonate legitimate clients.

Wireless networking equipment

Fortinet produces two types of wireless networking equipment:

- FortiWiFi units, which are FortiGate units with a built-in wireless access point/client
- FortiAP units, which are wireless access points compliant with the CAPWAP standard that you can control from any FortiGate unit that supports the WiFi Controller feature.

FortiWiFi units

A FortiWiFi unit can:

- Provide an access point for clients with wireless network cards. This is called Access Point mode, which is the default mode.
- Connect the FortiWiFi unit to another wireless network. This is called Client mode. A FortiWiFi unit operating in client mode can only have one wireless interface.
or

- Monitor access points within radio range. This is called Monitoring mode. You can designate the detected access points as Accepted or Rogue for tracking purposes. No access point or client operation is possible in this mode. But, you can enable monitoring as a background activity while the unit is in Access Point mode.

FortiWiFi unit capabilities differ by model as follows:

### Table 1: FortiWiFi model capabilities

<table>
<thead>
<tr>
<th>Model</th>
<th>Radio</th>
<th>Simultaneous SSIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>20C</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td></td>
<td>802.11 a/n 5GHz</td>
<td></td>
</tr>
<tr>
<td>30B</td>
<td>802.11 b/g 2.4GHz</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td>40C</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td></td>
<td>802.11 a/n 5GHz</td>
<td></td>
</tr>
<tr>
<td>50B</td>
<td>802.11 b/g 2.4GHz</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td>60B</td>
<td>802.11 b/g 2.4GHz</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td></td>
<td>802.11 a 5GHz</td>
<td></td>
</tr>
<tr>
<td>60C</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td></td>
<td>802.11 a/n 5GHz</td>
<td></td>
</tr>
<tr>
<td>80/81CM</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td></td>
<td>802.11 a/n 5GHz</td>
<td></td>
</tr>
</tbody>
</table>

### Using a FortiWiFi unit as a managed AP

A FortiWiFi unit can also be used much like a FortiAP unit to provide an access point managed by another FortiGate unit. To use a FortiWiFi unit as a managed WAP, you need to switch it to wireless terminal mode by using the CLI as follows:

```
config system global
set wireless-mode wtp
end
```

FortiWiFi-80CM supports WTP mode only in FortiOS 4.3 patch 2 or later.

The wireless functionality of a FortiWiFi unit in wireless terminal mode cannot be controlled from the unit itself.

If there are firewall devices between the WiFi controller FortiGate unit and the managed FortiWiFi units, make sure that ports 5246 and 5247 are open. These ports carry, respectively, the encrypted control channel data and the wireless network data. If needed, you can change these ports in the CLI:

```
config system global
set wireless-controller-port <port_int>
end
```

This command sets the control channel port. The data channel port is always the control port plus one. The port setting must match on the access controller and all access points.
FortiAP units

FortiAP series wireless access points are controlled by a FortiGate unit over Ethernet. Capabilities differ by model as follows:

### Table 2: FortiAP model capabilities

<table>
<thead>
<tr>
<th>Model</th>
<th>Radio 1</th>
<th>Radio 2</th>
<th>Simultaneous SSIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>210B (indoor)</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>N/A</td>
<td>7 for AP, 1 for monitoring</td>
</tr>
<tr>
<td>220A (indoor)</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>802.11 a/n 5GHz</td>
<td>14 for AP, 2 for monitoring</td>
</tr>
<tr>
<td>220B (indoor)</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>802.11 a/n 5GHz</td>
<td>14 for AP, 2 for monitoring</td>
</tr>
<tr>
<td>222B (outdoor)</td>
<td>802.11 b/g/n 2.4GHz</td>
<td>802.11 a/n 5GHz</td>
<td>14 for AP, 2 for monitoring</td>
</tr>
</tbody>
</table>

Dual-band radios can function as an AP on either band or as a dual-band monitor. The monitoring function is also available during AP operation if Background Scan is enabled in the custom AP profile for the device.

Third-party WAPs

FortiOS implements the CAPWAP standard.

Deployment considerations

Several factors need to be considered when planning a wireless deployment.

### Types of wireless deployment

This Handbook chapter describes two main types of wireless deployment: single WAP and multiple WAP. You will know which type of deployment you need after you have evaluated the coverage area environment.

### Deployment methodology

1. Evaluate the coverage area environment.
2. Position access point(s).
3. Select access point hardware.
4. Install and configure the equipment.
5. Test and tune the network.

### Evaluating the coverage area environment

Consider the following factors:

- **Size of coverage area** — Even under ideal conditions, reliable wireless service is unlikely beyond 100 metres outdoors or 30 metres indoors. Indoor range can be further diminished by the presence of large metal objects that absorb or reflect radio frequency energy. If wireless users are located on more than one floor of a building, a minimum of one WAP for each floor will be needed.
Bandwidth required — Wireless interface data rates are between 11 and 150 Mb/s, depending on the 802.11 protocol that is used. This bandwidth is shared amongst all users of the wireless data stream. If wireless clients run network-intensive applications, fewer of them can be served satisfactorily by a single WAP. Note that on some FortiWiFi units you can define up to four wireless interfaces, increasing the available total bandwidth.

Client wireless capabilities — The 802.11n protocol provides the highest data rates and has channels in the less interference-prone 5GHz band, but it is supported only on the latest consumer devices. The 802.11g protocol is more common but offers lower bandwidth. Some older wireless client equipment supports only 802.11b with a maximum data rate of 11Mb/s. WAP radios support the protocol that you select with backward compatibility to older modes. For example, if you select 802.11n, clients can also connect using 802.11g or 802.11b.

The most important conclusion from these considerations is whether more than one WAP is required.

Positioning access points

When placing the access point, your main concern is providing a strong signal to all users. A strong signal ensures a fast connection and efficient data transfer. A weaker signal means a greater chance of data transmission errors and the need to re-send information, slowing down data transfer.

Consider the following guidelines when placing access points:

- Physical barriers can impede the radio signals. Solid objects such as walls, furniture and people absorb radio waves, weakening the signal. Be aware of the physical barriers in your office space that may reduce a signal. If there is enough physical interference, you may encounter dead spots that receive no signal.
- Ensure the access point is located in a prominent location within a room for maximum coverage, rather than in a corner.
- Construction materials used in a building can also weaken radio signals. Rooms with walls of concrete or metal can affect the signal strength.

If you cannot avoid some of these impediments due to the shape of the office or building materials used, you may need to use multiple access points to help distribute the radio signal around the room. Figure 1 shows how positioning two FortiAP-220A units within a uniquely shaped office space helps to distribute signals around the area.
This sample office has washrooms, a stairwell and an elevator shaft in the center of the building, making it impossible to use a single access point effectively. The elevator shaft and multiple metal stalls in the washrooms can cause signal degradation. However, placing access points in diagonally opposite areas of the office provides maximum coverage.

When using multiple access points, set each access point to a different channel to avoid interference in areas where signals from both access points can be received.

**Selecting access point hardware**

For a single WAP installation, you could deploy a single FortiWiFi unit. If the site already has a FortiGate unit that supports the WiFi controller feature, adding a FortiAP unit is the most economical solution.

For a multiple WAP deployment you need a FortiGate unit as a WiFi controller and multiple FortiAP units. A FortiWiFi unit can be used as a managed WAP, but it is more expensive.

The FortiAP unit offers more flexible placement. FortiWiFi units either sit on a shelf or are rack mounted. FortiAP units can be attached to any wall or ceiling, enabling you to locate them where they will provide the best coverage.

**Single access point networks**

A single access point is appropriate for a limited number of users in a small area. For example, you might want to provide wireless access for a group of employees in one area on one floor of an office building.

A good rule of thumb is that one access point can serve 3000 to 4000 square feet of space, with no user more than 60 feet from the access point. Walls and floors reduce the coverage further, depending on the materials from which they are made.

**Multiple access point networks**

To cover a larger area, such as multiple floors of a building, or multiple buildings, multiple access points are required.
In the WiFi controller, you configure a single virtual access point, but the controller manages multiple physical access points that share the same configuration. A feature known as “fast roaming” enables users to move from one physical access point coverage area to another while retaining their authentication.

**Fast Roaming**

Users in a multi-AP network, especially with mobile devices, can move from one AP coverage area to another. But, the process of re-authentication can often take seconds to complete and this can impair wireless voice traffic and time sensitive applications. The FortiAP fast roaming feature solves this problem and is available only when moving between FortiAP units managed by the same FortiGate unit.

Fast roaming uses two standards-based techniques:

- **Pairwise Master Key (PMK) Caching** enables a RADIUS-authenticated user to roam away from an AP and then roam back without having to re-authenticate. To accomplish this, the FortiGate unit stores in a cache a master key negotiated with the first AP. This enables the 802.11i-specified method of “fast roam-back.”

- **Pre-authentication or “fast-associate in advance”** enables an 802.11 AP associated to a client to bridge to other APs over the wired network and pre-authenticate the client to the “next” AP to which the client might roam. This enables the PMK to be derived in advance of a roam and cached. When the client does roam, it will already have negotiated authentication in advance and will use its cached PMK to quickly associate to the next AP. This capability will ensure that wireless clients that support Pre-authentication to continue the data transfer without noticeable connection issues.

**Automatic Radio Resource Provisioning**

To prevent interference between APs, the FortiOS WiFi Controller includes the Automatic Radio Resource Provisioning (ARRP) feature. When enabled in an access point profile, this feature measures utilization and interference on the available channels and selects the clearest channel at each access point. The measurement can be repeated periodically to respond to changing conditions.
Configuring a WiFi LAN

When working with a FortiGate WiFi controller, you can configure your wireless network before you install any access points. If you are working with a standalone FortiWiFi unit, the access point hardware is already present but the configuration is quite similar. Both are covered in this section.

The following topics are included in this section:

- Overview of WiFi controller configuration
- Setting your geographic location
- Creating a custom AP Profile
- Defining a wireless network interface (SSID)
- Configuring user authentication
- Configuring firewall policies for the SSID
- Customizing captive portal pages
- Configuring the built-in access point on a FortiWiFi unit

Overview of WiFi controller configuration

The FortiGate WiFi controller configuration is composed of three types of object, the SSID, the AP Profile and the physical Access Point.

- An SSID defines a virtual wireless network interface, including security settings. One SSID is sufficient for a wireless network, regardless how many physical access points are provided. You might, however, want to create multiple SSIDs to provide different services or privileges to different groups of users. Each SSID has separate firewall policies and authentication. Each radio in an access point can support up to 8 SSIDs. A more common use of the term SSID is for the identifier that clients must use to connect to the wireless network. Each SSID (wireless interface) that you configure will have an SSID field for this identifier. In Managed Access Point configurations you choose wireless networks by SSID values. In firewall policies you choose wireless interfaces by their SSID name.

- An AP Profile defines the radio settings, such as band (802.11g for example) and channel selection. The AP Profile names the SSIDs to which it applies. Managed APs can use automatic profile settings or you can create custom AP profiles.

- Managed Access Points represent local wireless APs on FortiWiFi units and FortiAP units that the FortiGate unit has discovered. There is one managed access point definition for each AP device. An access point definition can use automatic AP profile settings or select a custom AP Profile. When automatic profile settings are used, the managed AP definition also selects the SSIDs to be carried on the AP.
About SSIDs on FortiWiFi units

FortiWiFi units have a default SSID (wireless interface) named wlan. You can modify or delete this SSID as needed. As with external APs, the built-in wireless AP can be configured to carry any SSID.

The AP settings for the built-in wireless access point are located at WiFi Controller > Managed Access Points > Local WiFi Radio. The available operational settings are the same as those for external access points which are configured at WiFi Controller > Managed Access Points > Managed FortiAP.

About automatic AP profile settings

FortiOS simplifies wireless network configuration by providing an automatic setting for the access point profile. You can enable wireless AP operation and Rogue AP scanning with the radios in the AP automatically allocated as follows:

<table>
<thead>
<tr>
<th>No. of Radios</th>
<th>Wireless Access enabled</th>
<th>Rogue AP Scan enabled</th>
<th>Wireless Access and Rogue AP Scan enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Radio 1 - AP</td>
<td>Radio 1 - scan</td>
<td>Radio 1 - AP + background scan</td>
</tr>
<tr>
<td></td>
<td>Radio 2 - disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Radio 1 - AP</td>
<td>Radio 1 - disabled</td>
<td>Radio 1 - AP</td>
</tr>
<tr>
<td></td>
<td>Radio 2 - scan</td>
<td></td>
<td>Radio 2 - scan</td>
</tr>
</tbody>
</table>

You can select which SSIDs (wireless networks) will be available through the access point and adjust the wireless power level of the AP.
Process to create a wireless network

To set up your wireless network, you will need to perform the following steps.

- Make sure the FortiGate wireless controller is configured for your geographic location. This ensures that the available radio channels and radio power are in compliance with the regulations in your region.
- Optionally, if you don’t want to use automatic AP profile settings, configure a custom Access Point (AP) profile, specifying the radio settings and the SSIDs to which they apply.
- Configure one or more SSIDs for your wireless network. The SSID configuration includes DHCP and DNS settings.
- Configure the user group and users for authentication on the WLAN.
- Configure the firewall policy for the WLAN.
- Optionally, customize the captive portal.
- Configure access points.

Configuration of the built-in AP on FortiWiFi units is described in this chapter. Connection and configuration of FortiAP units is described in the next chapter, “Access point deployment”.

Setting your geographic location

The maximum allowed transmitter power and permitted radio channels for Wi-Fi networks depend on the region in which the network is located. By default, the WiFi controller is configured for the United States. If you are located in any other region, you need to set your location before you begin configuring wireless networks.

To change the location setting - CLI

To change the country to France, for example, enter

```
config wireless-controller setting
  set country FR
end
```

To see the list of country codes, enter a question mark (‘?’) instead of a country code.

Before changing the country setting, you must remove all Custom AP profiles. To do this, go to WiFi Controller > Managed Access Points > Custom AP Profile.

Creating a custom AP Profile

If the automatic AP profile settings don’t meet your needs, you can define a custom AP Profile. For information about the automatic profile settings, see “About automatic AP profile settings” on page 22.

An AP Profile configures radio settings and selects the Virtual APs to which the settings apply. FortiAP units contain two radio transceivers, making it possible, for example, to provide both 2.4GHz 802.11b/g/n and 5GHz 802.11a/n service from the same access point.

FortiAP units also provide a monitoring function for the Rogue AP feature.
To configure an AP Profile - web-based manager

1. Go to WiFi Controller > Managed Access Points > Custom AP Profile and select Create New.
2. Enter a Name for the AP Profile.
3. In Platform, select the FortiWiFi or FortiAP model to which this profile applies.
4. In Mode, select Access Point.
5. Optionally, enable Background Scan to support the Rogue AP feature.
   For more information see “Wireless network monitoring” on page 49.
   For more information see “Automatic Radio Resource Provisioning” on page 19.
7. In Band, select the 802.11 wireless protocol that you want to support.
   Note that there are two choices for 802.11n. Select 802.11n for 2.4GHz operation or 802.11n-5G for 5GHz operation. The available choices depend on the radio’s capabilities.
8. In Channel, select the channels that the AP is permitted to use. By default, all channels are selected.
9. Leave the TX Power at its default setting. You can adjust this later.
10. In SSID, use the arrow buttons to move the SSIDs (wireless LANs) to which these settings apply into the Selected list.
11. Repeat steps 4 though 10 for Radio 2, if required.
   Note that on the FortiAP-220 unit Radio 1 is 2.4GHz and Radio 2 is 5GHz.
   Radio 2 also supports 40MHz wide channels on the 5GHz band on 802.11n.
12. Select OK.

To configure an AP Profile - CLI

This example configures a FortiAP-220A to use only Radio 1 for 802.11g operation applied to SSID example_wlan.

```
config wireless-controller wtp-profile
edit guest_prof
  config platform
    set type 220A
  end
  config radio-1
    set mode ap
    set band 802.11g
    set vaps example_wlan
  end
end
```

Defining a wireless network interface (SSID)

You begin configuring your wireless network by defining one or more SSIDs to which your users will connect.
A virtual AP defines the SSID and security settings that can be applied to one or more physical APs. On the FortiGate unit, this creates a virtual network interface with the virtual AP's name. With this interface you can define the DHCP services, firewall policies, and other settings for your WiFi LAN.

To configure an SSID - web-based manager

1. Go to WiFi Controller > WiFi Network > SSID and select Create New.
2. Enter the Interface Name that will identify the wireless interface.
3. In the Addressing Mode section, enter the IP/Netmask for the interface. If IPv6 is enabled, you can also enter an IPv6 Address.
4. In Administrative Access, select Ping. Ping is useful for testing. For security it is better not to enable administrative access on wireless interfaces.
5. Enter the SSID for your WLAN and choose whether to enable SSID Broadcast or not. For more information, see “Whether to broadcast SSID” on page 12.
6. If you want to provide DHCP service to your clients, select Enable DHCP and enter the range of IP addresses to assign. For more information, see “Configuring DHCP for WiFi clients” on page 26.
7. Select the Security Mode and enter the required settings. For more information, see “Configuring security” on page 26.
8. If you want to prevent direct communication between your wireless clients, enable Block Intra-SSID Traffic.
9. Optionally, set the Maximum Clients limit. The default of 0 sets no limit on the number of clients.
10. If you want to restrict access to the wireless network by MAC address, select Enable MAC Filter. For more information, see “Adding a MAC filter” on page 29.
11. Select OK. Each Virtual AP that you create is a wireless interface that establishes a wireless LAN. Go to System > Network > Interface to configure its IP address.

To configure a virtual access point - CLI

This example creates an access point with SSID “example” and WPA2-Personal security. The wireless interface is named example_wlan.

```
config wireless-controller vap
  edit example_wlan
    set ssid "example"
    set broadcast-ssid enable
    set security wpa2-only-personal
    set passphrase "hardtoguess"
    set vdom root
  end
config system interface
  edit example_wlan
    set ip 10.10.120.1 255.255.255.0
  end
```
Configuring DHCP for WiFi clients

Wireless clients need to have IP addresses. If you use RADIUS authentication, each user’s IP address can be stored in the Framed-IP-Address attribute. Otherwise, you need to configure a DHCP server on the WLAN interface to assign IP addresses to wireless clients.

To configure a DHCP server for WiFi clients - web-based manager

1. Go to WiFi Controller > WiFi Network > SSID and edit your SSID entry.
2. In the WiFi Settings section, select Enable DHCP.
3. In the Address Start and Address End fields, enter the IP address range to assign.
   The address range needs to be in the same subnet as the wireless interface IP address, but not include that address.
4. Set the Default Gateway to the wireless interface IP address.
5. Set the Netmask to an appropriate value, such as 255.255.255.0.
6. Enter the IP address of the DNS Server that your users will access.
7. Select OK.

The DHCP server automatically configures itself to serve only FortiAP units.
You can also configure DHCP through System > Network > DHCP Server, but that page offers additional options that might not be suitable for a wireless network.

To configure a DHCP server for WiFi clients - CLI

In this example, WiFi clients on the example_wlan interface are assigned addresses in the 10.10.120.2-9 range to connect with the WiFi access point on 10.10.120.1.

```
config system dhcp server
edit 0
   set default-gateway 10.10.120.1
   set dns-service default
   set interface example_wlan
   set netmask 255.255.255.0
config ip-range
   edit 1
      set end-ip 10.10.120.9
      set start-ip 10.10.120.2
end
end
```

You cannot delete an SSID (wireless interface) that has DHCP enabled on it.

Configuring security

The FortiGate WiFi controller supports both Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) security. WPA support includes WPA2, which has additional security improvements.
WEP security uses an encryption key between the wireless device and the access point. WEP64 uses a key of ten hexadecimal digits. WEP128 keys are 26 digits long. WEP security is relatively easy to break. Wherever possible, use WPA security. WEP can be enabled only through the CLI.

WPA security offers more robust encryption that is much more difficult to break. WPA provides two methods of authentication: through RADIUS (802.1X) authentication or by pre-shared key.

WPA security with a preshared key for authentication is called WPA-Personal. This can work well for one person or a small group of trusted people. But, as the number of users increases, it is difficult to distribute new keys securely and there is increased risk that the key could fall into the wrong hands.

A more secure form of WPA security is WPA-Enterprise. Users each have their own authentication credentials, verified through an authentication server, usually RADIUS. FortiOS can also authenticate WPA-Enterprise users through its built-in user group functionality. FortiGate user groups can include RADIUS servers and can select users by RADIUS user group. This makes possible Role-Based Access Control (RBAC).

WPA security can encrypt communication with either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES). AES is the preferred encryption, but some older wireless clients do not support it. You can select the encryption during setup.

Captive Portal security connects users to an open web portal defined in replacement messages. To navigate to any location beyond the web portal, the user must pass FortiGate user authentication.

**WPA-Personal security**

WPA-Personal security setup requires only the preshared key that you will provide to your clients.

**To configure WPA-Personal security - web-based manager**

1. Go to WiFi Controller > WiFi Network > SSID and edit your SSID entry.
2. In Security Mode, select WPA/WPA2-Personal.
3. In Data Encryption, select AES.
   - If some of your wireless clients do not support AES, select TKIP.
4. In Pre-shared Key, enter a key between 8 and 63 characters long.
5. Select OK.

**To configure WPA-Personal security - CLI**

```
config wireless-controller vap
edit example_wlan
    set security wpa-personal
    set passphrase "hardtoguess"
    set encrypt AES
end
```

**WPA-Enterprise security**

If you will use FortiOS user groups for authentication, go to User > User Group and create those groups first. The groups should be Firewall groups.

If you will use a RADIUS server to authenticate wireless clients, you must first configure the FortiGate unit to access the RADIUS server.
To configure FortiGate unit access to the RADIUS server - web-based manager

1. Go to User > Remote > RADIUS and select Create New.
2. Enter a Name for the server.
3. In Primary Server Name/IP, enter the network name or IP address for the server.
4. In Primary Server Secret, enter the shared secret used to access the server.
5. Optionally, enter the information for a secondary or backup RADIUS server.
6. Select OK.

To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
  edit exampleRADIUS
    set auth-type auto
    set server 10.11.102.100
    set secret aoewmntiasf
  end
```

To configure WPA-Enterprise security - web-based manager

1. Go to WiFi Controller > WiFi Network > SSID and edit your SSID entry.
2. In Security Mode, select WPA/WPA2-Enterprise.
3. In Data Encryption, select AES.
   If some of your wireless clients do not support AES, select TKIP.
4. In Authentication, do one of the following:
   • If you will use a RADIUS server for authentication, select RADIUS Server and then select the RADIUS server.
   • If you will use a local user group for authentication, select Usergroup and then select the user group that is permitted to use the wireless network.
5. Select OK.

To configure WPA-Enterprise security - CLI

```
config wireless-controller vap
  edit example_wlan
    set security wpa-enterprise
    set encrypt AES
    set auth radius
    set radius-server exampleRADIUS
  end
```

Captive Portal security

Captive Portal security provides an access point that initially appears open. The wireless client can connect to the AP with no security credentials. The AP responds to the client’s first HTTP request with a web page requesting user name and password. Until the user enters valid credentials, no communication beyond the AP is permitted.

The wireless controller authenticates users through the FortiGate user accounts. In the SSID configuration, you select the user groups that are permitted access through the captive portal.

The captive portal contains the following web pages:

- Login page—requests user credentials
These pages are defined in replacement messages. Defaults are provided. In the web-based manager, you can modify the default messages in the SSID configuration by selecting Customize Portal Messages. Each SSID can have its own unique portal content.

To configure Captive Portal security - web-based manager
1. Configure user groups as needed in User > User Group.
2. Go to WiFi Controller > WiFi Network > SSID and edit your SSID entry.
4. Optionally, select Customize Portal Messages and modify the portal pages that users of this SSID will see.
5. In User Groups, select the group(s) that are allowed to use the wireless network and move them to the Selected list.
6. Select OK.

Adding a MAC filter

On each SSID, you can create a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.

This is actually not as secure as it appears. Someone seeking unauthorized access to your network can obtain MAC addresses from wireless traffic and use them to impersonate legitimate users. A MAC filter list should only be used in conjunction with other security measures such as encryption.

To configure a MAC filter list, you must use the CLI.

To configure a MAC filter - CLI

In this example, the MAC addresses 11:11:11:11:11:11 and 12:12:12:12:12:12 will be excluded from the example_wlan wireless interface.

```
config wireless-controller vap
edit example_wlan
  config mac-filter-list
    edit 1
      set mac 11:11:11:11:11:11
      set mac-filter-policy deny
    edit 2
      set mac 12:12:12:12:12:12
      set mac-filter-policy deny
  end
end
```
Configuring user authentication

You can perform user authentication when the wireless client joins the wireless network and when the wireless user communicates with another network through a firewall policy. WEP and WPA-Personal security rely on legitimate users knowing the correct key or passphrase for the wireless network. The more users you have, the more likely it is that the key or passphrase will become known to unauthorized people. WPA-Enterprise and captive portal security provide separate credentials for each user. User accounts can be managed through FortiGate user groups or an external RADIUS authentication server.

WPA-Enterprise authentication

If your WiFi network uses WPA-Enterprise authentication verified by a RADIUS server, you need to configure the FortiGate unit to connect to that RADIUS server.

Configuring connection to a RADIUS server - web-based manager

1. Go to User > Remote > RADIUS and select Create New.
2. Enter a Name for the server. This name is used in FortiGate configurations. It is not the actual name of the server.
3. In Primary Server Name/IP, enter the network name or IP address for the server.
4. In Primary Server Secret, enter the shared secret used to access the server.
5. Optionally, enter the information for a secondary or backup RADIUS server.
6. Select OK.

To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
edit exampleRADIUS
    set auth-type auto
    set server 10.11.102.100
    set secret aoewmntiasf
end
```

To implement WPA-Enterprise security, you select this server in the SSID security settings. See “Configuring security” on page 26.

To use the RADIUS server for authentication, you can create individual FortiGate user accounts that specify the authentication server instead of a password, and you then add those accounts to a user group. Or, you can add the authentication server to a FortiGate user group, making all accounts on that server members of the user group.

Creating a wireless user group

Most wireless networks require authenticated access. To enable creation of identity-based firewall policies, you should create at least one user group for your wireless users. You can add or remove users later. There are two types of user group to consider:

- A Firewall user group can contain user accounts stored on the FortiGate unit or external authentication servers such as RADIUS that contain and verify user credentials.
- A Directory Services user group is used for integration with Windows Active Directory or Novell eDirectory. The group can contain Windows or Novell user groups who will be permitted access to the wireless LAN. Fortinet Single Sign On (FSSO) agent must be installed on the network.
Configuring firewall policies for the SSID

For users on the WiFi LAN to communicate with other networks, firewall policies are required. Before you create firewall policies, you need to define any firewall addresses you will need. This section describes creating a WiFi network to Internet policy.

To create a firewall address for WiFi users - web-based manager

1. Go to Firewall Objects > Address > Address.
2. Select Create New, enter the following information and select OK.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Enter a name for the address, wifi_net for example.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>Enter the subnet address, 10.10.110.0/24 for example.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface where this address is used, e.g., example_wifi</td>
</tr>
</tbody>
</table>

To create a firewall address for WiFi users - CLI

```
config firewall address
  edit "wifi_net"
    set associated-interface "example_wifi"
    set subnet 10.10.110.0 255.255.255.0
  end
```

To create a firewall policy - web-based manager

1. Go to Policy > Policy and select Create New.
2. In Source Interface/Zone, select the wireless interface.
3. In Source Address, select the address of your WiFi network, wifi_net for example.
4. In Destination Interface/Zone, select the Internet interface, for example, port1.
5. In Destination Address, select All.
6. In Service, select ANY, or select the particular services that you want to allow, and then select the right arrow button to move the service to the Selected Services list.
7. In Schedule, select Always, unless you want to define a schedule for limited hours.
8. In Action, select ACCEPT.
9. Select Enable NAT.
10. Optionally, select UTM and set up UTM features for wireless users.
11. Select OK.

To create a firewall policy - CLI

```
config firewall policy
  edit 0
    set srcintf "example_wifi"
    set dstintf "port1"
    set srcaddr "wifi_net"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
```
Customizing captive portal pages

If you select Captive Portal authentication in the SSID, the wireless controller presents to the user pages defined in Captive Portal Default replacement pages.

The captive portal contains the following web pages:

- **Login page**—requests user credentials
- **Login failed page**—reports that the entered credentials were incorrect and enables the user to try again.
- **Disclaimer page**—is statement of the legal responsibilities of the user and the host organization to which the user must agree before proceeding.
- **Declined disclaimer page**—is displayed if the user does not agree to the statement on the Disclaimer page. Access is denied until the user agrees to the disclaimer.

These pages are defined in replacement messages. Defaults are provided. In the web-based manager, you can modify the default messages in the SSID configuration by selecting **Customize Portal Messages**. Each SSID can have its own unique portal content.

Modifying the login page

The login page requests the user’s credentials. Typical modifications for this page would be to change the logo and modify some of the text.

**Figure 3: Default captive portal login page**

![Login Page]

Changing the logo

You can replace the default Fortinet logo with your organization’s logo. First, import the logo file into the FortiGate unit and then modify the Login page code to reference your file.

```
set nat enable
end
```
To import a logo file
1. Go to System > Config > Replacement Message and select Manage Images.
2. Select Create New.
3. Enter a Name for the logo and select the appropriate Content Type.
   The file must not exceed 6000 bytes.
4. Select Browse, find your logo file and then select Open.
5. Select OK.

To specify the new logo in the replacement message
1. Go to WiFi Controller > WiFi Network > SSID and edit your SSID.
   The SSID Security Mode must be Captive Portal.
2. Make sure that Customize Portal Messages is selected and then select the adjacent Edit icon.
3. In the Edit Message window, select the Login page message.
4. In the Message HTML, find the %%IMAGE tag.
   By default it specifies the Fortinet logo:
   ```html
   %%IMAGE:logo_fw_auth%%
   ```
5. Change the image name to the one you provided for your logo.
   The tag should now read, for example,:
   ```html
   %%IMAGE:mylogo%%
   ```
6. Select OK.

Modifying text
You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters. There are two exceptions to this rule:

- The line “Please enter your username and password to continue” is provided by the %%QUESTION%% tag. You can replace this tag with text of your choice.
- The line “SSID ... Authentication Required” includes the name of the SSID, provided by the %%CPAUTH_SSID%% tag. You can remove or change the position of this tag.

Except for these items, you should not remove any tags because they may carry information that the FortiGate unit needs.

To modify login page text
1. Go to WiFi Controller > WiFi Network > SSID and edit your SSID.
   The SSID Security Mode must be Captive Portal.
2. Make sure that Customize Portal Messages is selected and then select the adjacent Edit icon.
3. In the Edit Message window, select the Login page message.
4. In the Message HTML box, edit the text, then select OK.
5. Select OK.

Modifying the login failed page
The Login failed page is similar to the Login page. It even contains the same login form.
You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters. There are two exceptions to this rule:

- The line “Firewall authentication failed. Please try again.” is provided by the %%FAILED_MESSAGE%% tag. You can replace this tag with text of your choice.
Configuring the built-in access point on a FortiWiFi unit

Both FortiGate and FortiWiFi units have the WiFi controller feature. If you configure a WiFi network on a FortiWiFi unit, you can also use the built-in wireless capabilities in your WiFi network as one of the access points.

If Virtual Domains are enabled, you must select the VDOM to which the built-in access point belongs. You do this in the CLI. For example:

```
config wireless-controller global
  set local-radio-vdom vdom1
end
```

To configure the FortiWiFi unit’s built-in WiFi access point

1. Go to WiFi Controller > Managed Access Points > Local WiFi Radio.
2. Make sure that AP Profile is Automatic.
3. Make sure that Enable WiFi Radio is selected.
4. In SSID, if you do not want this AP to carry all SSIDs, select Select SSIDs and then select the required SSIDs.
5. Optionally, adjust the TX Power slider.
   - If you have selected your location correctly (see “Setting your geographic location” on page 23), the 100% setting corresponds to the maximum power allowed in your region.
6. If you do not want the built-in WiFi radio to be used for rogue scanning, select Do not participate in Rogue AP scanning.
7. Select OK.

If you want to connect external APs, such as FortiAP units, see the next chapter, “Access point deployment”.

The line “SSID ... Authentication Required” includes the name of the SSID, provided by the %%CPAUTH_SSID%% tag. You can remove or change the position of this tag. Except for these items, you should not remove any tags because they may carry information that the FortiGate unit needs.

Figure 4: Default login failed page
Access point deployment

This chapter describes how to configure access points for your wireless network. The following topics are included in this section:

- Overview
- Network topology for managed APs
- Discovering and authorizing APs
- Advanced WiFi controller discovery

Overview

FortiAP units discover WiFi controllers. The administrator of the WiFi controller authorizes the FortiAP units that the controller will manage.

In most cases, FortiAP units can find WiFi controllers through the wired Ethernet without any special configuration. Review the following section, “Network topology for managed APs”, to make sure that your method of connecting the FortiAP unit to the WiFi controller is valid. Then, you are ready to follow the procedures in “Discovering and authorizing APs” on page 40.

If your FortiAP units are unable to find the WiFi controller, refer to “Advanced WiFi controller discovery” on page 45 for detailed information about the FortiAP unit’s controller discovery methods and how you can configure them.

Network topology for managed APs

The FortiAP unit can be connected to the FortiGate unit in any of the following ways:

**Direct connection**: The FortiAP unit is directly connected to the FortiGate unit with no switches between them. This configuration is common for locations where the number of FortiAP’s matches up with the number of ‘internal’ ports available on the FortiGate. In this configuration the FortiAP unit requests an IP address from the FortiGate unit, enters discovery mode and should quickly find the FortiGate WiFi controller. This is also known as a wirecloset deployment. See Figure 7, below.

**Switched Connection**: The FortiAP unit is connected to the FortiGate WiFi controller by an Ethernet switch operating in L2 switching mode or L3 routing mode. There must be a routable path between the FortiAP unit and the FortiGate unit and ports 5246 and 5247 must be open. This is also known as a gateway deployment. See Figure 7, below.

**Connection over WAN**: The FortiGate WiFi controller is off-premises and connected by a VPN tunnel to a local FortiGate. In this method of connectivity its best to configure each FortiAP with the static IP address of the WiFi controller. Each FortiAP can be configured with three WiFi controller IP addresses for redundant failover. This is also known as a datacenter remote management deployment. See Figure 8, below.
Discovering and authorizing APs

After you prepare your FortiGate unit, you can connect your APs to discover them using the discovery methods described earlier. To prepare the FortiGate unit, you need to:

- Configure the network interface to which the AP will connect.
- Configure DHCP service on the interface to which the AP will connect.
- Connect the AP units and let the FortiGate unit discover them.
- Enable each discovered AP and configure it or assign it to an AP profile.
Configuring the network interface for the AP unit

The interface to which you connect your wireless access point needs an IP address. No administrative access, DNS Query service or authentication should be enabled.

To configure the interface for the AP unit - web-based manager

1. Go to System > Network > Interface and edit the interface to which the AP unit connects.
2. Set Addressing Mode to Manual and enter the IP address and netmask to use.
3. Enable Dedicate this interface to FortiAP connection and set Reserve IP addresses for FortiAP to the range of addresses that you want to use for FortiAP units.
   - The address range needs to be in the same subnet as the interface IP address, but not include that address. This step automatically configures a DHCP server for the AP units.
4. Select OK.

To configure the interface for the AP unit - CLI

```bash
config system interface
   edit port3
       set mode static
       set ip 192.168.8.1 255.255.255.0
   end
```

To configure the DHCP server for AP unit - CLI

```bash
config system dhcp server
   edit 0
       set default-gateway 192.168.8.1
       set interface wan2
       config ip-range
           edit 1
               set end-ip 192.168.8.9
               set start-ip 192.168.8.2
           end
       set netmask 255.255.255.0
   end
```

Enabling a discovered AP

Within two minutes of connecting the AP unit to the FortiGate unit, the discovered unit should be listed on WiFi Controller > Managed Access Points > Managed FortiAP page.

Figure 9: Discovered access point unit

<table>
<thead>
<tr>
<th>Admin</th>
<th>Name</th>
<th>AP Profile</th>
<th>Clients</th>
<th>Join Time</th>
<th>Reset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FAP33ATUN6D0118</td>
<td></td>
<td>0</td>
<td>06/24/10 14:54</td>
<td></td>
</tr>
</tbody>
</table>

To add the discovered AP unit - web-based manager

1. Go to WiFi Controller > Managed Access Points > Managed FortiAP.
2. Select the FortiAP unit from the list and edit it.
3. Optionally, enter a Name. Otherwise, the unit will be identified by serial number.
4. Select Authorize.
5 Select OK.
The physical access point is now added to the system. If the rest of the configuration is complete, it should be possible to connect to the wireless network through the AP.

To add the discovered AP unit - CLI
First get a list of the discovered access point unit serial numbers:
```
get wireless-controller wtp
```
Add a discovered unit and associate it with AP-profile1, for example:
```
config wireless-controller wtp
edit FAP22A3U10600118
set admin enable
set wtp-profile AP-profile1
end
```
To use the automatic profile, leave the `wtp-profile` field unset.

To view the status of the added AP unit
```
config wireless-controller wtp
edit FAP22A3U10600118
get
```
The `join-time` field should show a time, not “N/A”. See the preceding web-based manager procedure for more information.

Configuring a managed AP
When you add a FortiAP unit, it is configured by default to
- use the Automatic profile
- operate at the maximum radio power permitted in your region
- carry all SSIDs
You can change the radio power and selection of SSIDs or assign the unit to a custom AP profile which defines the entire configuration for the AP.

To modify settings within Automatic profile - web-based manager
1 Go to WiFi Controller > Managed Access Points > Managed FortiAP.
2 Select the FortiAP unit from the list and edit it.
   `AP Profile` should be `Automatic`.
3 Make sure that `Enable WiFi Radio` is selected.
4 In `SSID`, if you do not want this AP to carry all SSIDs, select `Select SSIDs` and then select the required SSIDs.
5 Optionally, adjust the `TX Power` slider.
   If you have selected your location correctly (see “Setting your geographic location” on page 23), the 100% setting corresponds to the maximum power allowed in your region.
6 Select OK.

To modify settings within Automatic profile - CLI
When `wtp-profile` is unset (null value), the Automatic profile is in use and some of its settings can be adjusted. This example sets the AP to carry only the employee and guest SSIDs and operate at 80% of maximum power.
To select a custom AP profile - web-based manager
1. Go to WiFi Controller > Managed Access Points > Managed FortiAP.
2. Select the FortiAP unit from the list and edit it.
3. In AP Profile, select the custom AP Profile to use, and then select Apply.
   Only AP Profiles that are appropriate for this AP unit are available.
4. Select OK.

To select a custom AP profile - CLI

```
config wireless-controller wtp
  edit FAP22A3U10600118
    set radio-enable enable
    set vap-all disable
    set vaps employee guest
    set power-level 80
  end
```

To select automatic AP profile - CLI

```
config wireless-controller wtp
  edit FAP22A3U10600118
  unset wtp-profile
  end
```

Updating FortiAP unit firmware
You can update the FortiAP unit's firmware from the FortiGate unit that acts as its WiFi controller.

Updating FortiAP firmware from the FortiGate unit
You can update the FortiAP firmware using either the web-based manager or the CLI. Only the CLI method can update all FortiAP units at once.

To update FortiAP unit firmware - web-based manager
1. Go to WiFi Controller > Managed Access Points > Managed FortiAP.
2. Select the FortiAP unit from the list and edit it.
3. In FortiAP OS Version, select [Upgrade].
4. Select Browse and locate the firmware upgrade file.
5. Select OK.
6. When the upgrade process completes, select OK.
   The FortiAP unit restarts.

To update FortiAP unit firmware - CLI
1. Upload the FortiAP image to the FortiGate unit.
   For example, the Firmware file is FAP_22A_v4.3.0_b0212_fortinet.out and the server IP address is 192.168.0.100.
execute wireless-controller upload-wtp-image tftp
   FAP_22A_v4.3.0_b0212_fortinet.out 192.168.0.100
If your server is FTP, change tftp to ftp, and if necessary add your user name and password at the end of the command.

2 Verify that the image is uploaded:
   execute wireless-controller list-wtp-image

3 Upgrade the FortiAP units:
   exec wireless-controller reset-wtp all
   If you want to upgrade only one FortiAP unit, enter its serial number instead of all.

**Updating FortiAP firmware from the FortiAP unit**

You can connect to a FortiAP unit’s internal CLI to update its firmware from a TFTP server on the same network. This method does not require access to the wireless controller.

1 Place the FortiAP firmware image on a TFTP server on your computer.

2 Connect the FortiAP unit to a separate private switch or hub or directly connect to your computer via a cross-over cable.

3 Change your computer’s IP address to 192.168.1.3.

4 Telnet to IP address 192.168.1.2.
   This IP address is overwritten if the FortiAP is connected to a DHCP environment. Ensure that the FortiAP unit is in a private network with no DHCP server.

5 Login with the username “admin” and no password.

6 Enter the following command.
   For example, the FortiAP image file name is FAP_22A_v4.3.0_b0212_fortinet.out.
   restore FAP_22A_v4.3.0_b0212_fortinet.out 192.168.1.3

**Advanced WiFi controller discovery**

A FortiAP unit can use any of four methods to locate a controller. By default, FortiAP units cycle through all four of the discovery methods. In most cases there is no need to make configuration changes on the FortiAP unit.

There are exceptions. The following section describes the WiFi controller discovery methods in more detail and provides information about configuration changes you might need to make so that discovery will work.

You can also configure a FortiWiFi unit to act as an AP. But in this case you must choose which discovery method it will use. See “Configuring a FortiWiFi unit as a WiFi AP” on page 47.

**Controller discovery methods**

There are four methods that a FortiAP unit can use to discover a WiFi controller.

**Static IP configuration**

If FortiAP and the controller are not in the same subnet, broadcast and multicast packets cannot reach the controller. The admin can specify the controller’s static IP on the AP unit. The AP unit sends a discovery request message in unicast to the controller. Routing must be properly configured in both directions.
To specify the controller's IP address on a FortiAP unit

```bash
cfg -a AC_IPADDR_1="192.168.0.1"
```

By default, the FortiAP unit receives its IP address by DHCP. If you prefer, you can assign the AP unit a static IP address.

To assign a static IP address to the FortiAP unit

```bash
cfg -a ADDR_MODE=STATIC
cfg -a AP_IPADDR="192.168.0.100"
cfg -a AP_NETMASK="255.255.255.0"
```

For information about connecting to the FortiAP CLI, see “Connecting to the FortiAP CLI” on page 46.

**Broadcast request**

The AP unit broadcasts a discovery request message to the network and the controller replies. The AP and the controller must be in the same broadcast domain. No configuration adjustments are required.

**Multicast request**

The AP unit sends a multicast discovery request and the controller replies with a unicast discovery response message. The AP and the controller do not need to be in the same broadcast domain if multicast routing is properly configured.

The default multicast destination address is 224.0.1.140. It can be changed through the CLI. The address must be same on the controller and AP. For information about connecting to the FortiAP CLI, see “Connecting to the FortiAP CLI” on page 46.

To change the multicast address on the controller

```bash
config wireless-controller global
   set discovery-mc-addr 224.0.1.250
end
```

To change the multicast address on a FortiAP unit

```bash
cfg -a AC_DISCOVERY_MC_ADDR="224.0.1.250"
```

For information about connecting to the FortiAP CLI, see “Connecting to the FortiAP CLI” on page 46.

**DHCP**

If you use DHCP to assign an IP address to your FortiAP unit, you can also provide the WiFi controller IP address at the same time. This is useful if the AP is located remotely from the WiFi controller and other discovery techniques will not work.

When you configure the DHCP server, configure Option 138 to specify the WiFi controller IP address. You need to convert the address into hexadecimal. Convert each octet value separately from left to right and concatenate them. For example, 192.168.0.1 converts to C0A80001.

If Option 138 is used for some other purpose on your network, you can use a different option number if you configure the AP units to match.

To change the FortiAP DHCP option code

To use option code 139 for example, enter
Connecting to the FortiAP CLI

The FortiAP unit has a CLI through which some configuration options can be set.

To access the FortiAP unit CLI

1. Connect your computer to the FortiAP directly with a cross-over cable or through a separate switch or hub.
2. Change your computer’s IP address to 192.168.1.3
3. Telnet to IP address 192.168.1.2.
   Ensure that FortiAP is in a private network with no DHCP server for the static IP address to be accessible.
4. Login with user name admin and no password.
5. Enter commands as needed.
6. Optionally, use the `passwd` command to assign an administrative password for better security.
7. Save the configuration by entering the following command:
   `cfg -c .`
8. Unplug the FortiAP and then plug it back in, in order for the configuration to take effect.

When a WiFi controller has taken control of the FortiAP unit, Telnet access to the FortiAP unit’s CLI is no longer available.

Configuring a FortiWiFi unit as a WiFi AP

FortiWiFi units can also be deployed as managed APs controlled by a FortiGate unit wireless controller.

In the CLI, enter
```
config system global
   set wireless-mode wtp
end
```

Setting the discovery mode

Unlike FortiAP units, a FortiWiFi unit deployed as an AP does not cycle through the discovery methods. You must select one discovery method to use.

To select DHCP discovery
```
config wireless-controller global
   set ac-discovery-type dhcp
end
```

The DHCP discovery method is the simplest to use and will work when the AP is connected directly to the WiFi controller unit.
To select multicast discovery
In this example, the FortiWiFi AP is configured for multicast discovery and its multicast address is changed:

```
config wireless-controller global
  set ac-discovery-type multicast
  set discovery-mc-addr 224.0.1.250
end
```

Discovery by multicast will work even when the FortiWiFi AP is not in the same domain as the WiFi controller.

Completing configuration
The rest of the configuration is located in `config wireless-controller` and is similar to the FortiGate WiFi controller configuration.
Wireless network monitoring

You can monitor both your wireless clients and other wireless networks that are available in your coverage area.

The following topics are included in this section:

- Monitoring wireless clients
- Monitoring rogue APs
- Suppressing rogue APs

Monitoring wireless clients

To view connected clients on a FortiWiFi unit

- Go to WiFi Controller > Monitor > Client Monitor.

The following information can be displayed, depending on the Column Settings you have selected.

<table>
<thead>
<tr>
<th>Association Time</th>
<th>How long the client has been connected to this access point.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth</td>
<td>The type of authentication used.</td>
</tr>
<tr>
<td>Bandwidth Rx</td>
<td>Received bandwidth used by the client, in Kbps.</td>
</tr>
<tr>
<td>Bandwidth Tx</td>
<td>Transmit bandwidth used by the client, in Kbps.</td>
</tr>
<tr>
<td>Bandwidth Tx/Rx</td>
<td>Bandwidth Rx + Bandwidth Tx.</td>
</tr>
<tr>
<td>FortiAP</td>
<td>The serial number of the FortiAP unit to which the client connected.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>The total time this session that the client was idle.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address assigned to the wireless client.</td>
</tr>
<tr>
<td>MAC</td>
<td>The MAC address of the wireless client.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Manufacturer of the client wireless device.</td>
</tr>
<tr>
<td>Physical AP</td>
<td>The name of the physical access point with which the client is associated.</td>
</tr>
<tr>
<td>Rate</td>
<td>The data rate that the wireless connection can support.</td>
</tr>
<tr>
<td>Signal Strength / Noise</td>
<td>The signal-to-noise ratio in deciBels calculated from signal strength and noise level.</td>
</tr>
<tr>
<td>SSID</td>
<td>The SSID that the client connected to.</td>
</tr>
<tr>
<td>Virtual AP</td>
<td>The name of the virtual access point with which the client is associated.</td>
</tr>
</tbody>
</table>
Monitoring rogue APs

The access point radio equipment can scan for other available access points, either as a dedicated monitor or as a background scan performed while the access point is idle. Discovered access points are listed in the Rogue AP Monitor list. You can then mark them as either Accepted or Rogue access points. This designation helps you to track access points. It does not affect anyone’s ability to use these access points.

It is also possible to suppress rogue APs. See “Suppressing rogue APs” on page 53.

On-wire rogue AP detection technique

Other APs that are available in the same area as your own APs are not necessarily rogues. A neighboring AP that has no connection to your network might cause interference, but it is not a security threat. A rogue AP is an unauthorized AP connected to your wired network. This can enable unauthorized access. When rogue AP detection is enabled, the On-wire column in the Rogue AP Monitor list shows a green up-arrow on detected rogues.

Rogue AP monitoring of WiFi client traffic builds a table of WiFi clients and the Access Points that they are communicating through. The FortiGate unit also builds a table of MAC addresses that it sees on the LAN. The FortiGate unit’s on-wire correlation engine constantly compares the MAC addresses seen on the LAN to the MAC addresses seen on the WiFi network.

There are two methods of Rogue AP on-wire detection operating simultaneously: Exact MAC address match and MAC adjacency.

Exact MAC address match

If the same MAC address is seen on the LAN and on the WiFi network, this means that the wireless client is connected to the LAN. If the AP that the client is using is not authorized in the FortiGate unit configuration, that AP is deemed an ‘on-wire’ rogue. This scheme works for non-NAT rogue APs.

MAC adjacency

If an access point is also a router, it applies NAT to WiFi packets. This can make rogue detection more difficult. However, an AP’s WiFi interface MAC address is usually in the same range as its wired MAC address. So, the MAC adjacency rogue detection method matches LAN and WiFi network MAC addresses that are within a defined numerical distance of each other. By default, the MAC adjacency value is 7. If the AP for these matching MAC addresses is not authorized in the FortiGate unit configuration, that AP is deemed an ‘on-wire’ rogue.

Limitations

On-wire rogue detection has some limitations. There must be at least one WiFi client connected to the suspect AP and continuously sending traffic. If the suspect AP is a router, its WiFi MAC address must be very similar to its Ethernet port MAC address.

Logging

Information about detected rogue APs is logged and uploaded to your FortiAnalyzer unit, if you have one. By default, rogue APs generate an alert level log, unknown APs generate a warning level log. This log information can help you with PCI-DSS compliance requirements.
Rogue AP scanning as a background activity

Each WiFi radio can perform monitoring of radio channels in its operating band while acting as an AP. It does this by briefly switching from AP to monitoring mode. By default, a scan period starts every 300 seconds. Each second a different channel is monitored for 20ms until all channels have been checked.

During heavy AP traffic, it is possible for background scanning to cause lost packets when the radio switches to monitoring. To reduce the probability of lost packets, you can set the CLI `ap-bgscan-idle` field to delay the switch to monitoring until the AP has been idle for a specified period. This means that heavy AP traffic may slow background scanning.

The following CLI example configures default background rogue scanning operation except that it sets `ap-bgscan-idle` to require 100ms of AP inactivity before scanning the next channel.

```plaintext
config wireless-controller wtp-profile
  edit ourprofile
  config radio-1
    set ap-bgscan enable
    set rogue-scan enable
    set ap-bgscan-period 300
    set ap-bgscan-intv 1
    set ap-bgscan-duration 20
    set ap-bgscan-idle 100
  end
end
```

Configuring rogue scanning

Rogue scanning is easily enabled for all of your APs.

**To enable the rogue AP scanning feature - web-based manager**

1. Go to WiFi Controller > WiFi Network > Rogue AP Settings.
2. Select Enable Rogue AP Detection.
3. Select Enable On-wire Rogue AP Detection Technique if you want to use that method of distinguishing rogues from neighbors.
4. Select Apply.

**To enable the rogue AP scanning feature - CLI**

```plaintext
config wireless-controller setting
  set ap-scan enable
  set on-wire-scan enable
end
```

**To adjust MAC adjacency**

You can adjust the maximum WiFi to Ethernet MAC difference used when determining whether an suspect AP is a rogue. For example, to change the adjacency to 8, enter

```plaintext
config wireless-controller global
  set rogue-scan-mac-adjacency 8
end
```
Exempting an AP from rogue scanning

By default, if Rogue AP Detection is enabled, it is enabled on all managed FortiAP units. Optionally, you can exempt an AP from scanning. You should be careful about doing this if your organization must perform scanning to meet PCI-DSS requirements.

To exempt an AP from rogue scanning - web-based manager

1. Go to WiFi Controller > Managed Access Points > Managed FortiAP.
2. Select which AP to edit.
3. Select Do not participate in Rogue AP Scanning and then select OK.

To exempt an AP from rogue scanning - CLI

This example shows how to exempt access point AP1 from rogue scanning.

```
config wireless-controller wtp
  edit AP1
    set ap-scan disable
  end
```

Using the Rogue AP Monitor

Go to WiFi Controller > Monitor > Rogue AP Monitor to view the list of other wireless access points that are receivable at your location. Available information about the APs includes:

<table>
<thead>
<tr>
<th>SSID</th>
<th>channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>security type</td>
<td>signal strength</td>
</tr>
<tr>
<td>detected by which of your APs</td>
<td>MAC address</td>
</tr>
<tr>
<td>AP equipment vendor</td>
<td>on-wire status</td>
</tr>
<tr>
<td>time first seen</td>
<td>time last seen</td>
</tr>
</tbody>
</table>

The status of newly detected APs is Unclassified. You can manually change the status using the Mark menu.

- **Rogue AP.** Use this status for unauthorized APs attached to your wired networks. The On-wire detection technique determines which unknown APs are rogues.
- **Accepted AP.** Use this status for APs that are an authorized part of your network or are neighboring APs that are not a security threat.
- **Unclassified AP.** This is the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as Rogue or Accepted.
Suppressing rogue APs

In addition to monitoring rogue APs, you can actively prevent your users from connecting to them. When suppression is activated against an AP, the FortiGate WiFi controller sends deauthentication messages to the rogue AP’s clients, posing as the rogue AP, and also sends deauthentication messages to the rogue AP, posing as its clients. This is done using the monitoring radio.

To enable rogue AP suppression, you must enable monitoring of rogue APs with the on-wire detection technique. See “Monitoring rogue APs” on page 49. The monitoring radio must be in the Dedicated Monitor mode.

To activate AP suppression against a rogue AP

1. Go to WiFi Controller > Monitor > Rogue AP Monitor.
2. When you see an AP listed that is a rogue detected “on-wire”, select it and then select Mark > Mark Rogue.
3. To suppress an AP that is marked as a rogue, select it and then select Suppress AP.

To deactivate AP suppression

1. Go to WiFi Controller > Monitor > Rogue AP Monitor.
2. Select the suppressed rogue AP and then select Suppress AP > Unsuppress AP.
Configuring wireless network clients

This chapter shows how to configure typical wireless network clients to connect to a wireless network with WPA-Enterprise security. The following topics are included in this section:

- Windows XP client
- Windows 7 client
- Mac OS client
- Linux client
- Troubleshooting
Windows XP client

To configure the WPA-Enterprise network connection

1. In the Windows Start menu, go to Control Panel > Network Connections > Wireless Network Connection or select the wireless network icon in the Notification area of the Taskbar. A list of available networks is displayed.

![Wireless Network Connection](image)

If you are already connected to another wireless network, the Connection Status window displays. Select View Wireless Networks on the General tab to view the list.

If the network broadcasts its SSID, it is listed. But do not try to connect until you have completed the configuration step below. Because the network doesn’t use the Windows XP default security configuration, configure the client’s network settings manually before trying to connect.

2. You can configure the WPA-Enterprise network to be accessible from the View Wireless Networks window even if it does not broadcast its SSID.
3 Select Change Advanced Settings and then select the Wireless Networks tab.

![Image of Wireless Network Connection Properties]

Any existing networks that you have already configured are listed in the Preferred Networks list.

4 Select Add and enter the following information:

![Image of Wireless Network Properties]

<table>
<thead>
<tr>
<th>Network Name (SSID)</th>
<th>The SSID for your wireless network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Authentication</td>
<td>WPA2</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>AES</td>
</tr>
</tbody>
</table>

5 If this wireless network does not broadcast its SSID, select Connect even if this network is not broadcasting so that the network will appear in the View Wireless Networks list.
6 Select the Authentication tab.

7 In EAP Type, select Protected EAP (PEAP).

8 Make sure that the other two authentication options are not selected.

9 Select Properties.

10 Make sure that Validate server certificate is selected.

11 Select the server certificate UTN-USERFirst-Hardware.

12 In Select Authentication Method, select Secured Password (EAP-MSCHAPv2).

13 Ensure that the remaining options are not selected.
14 Select Configure.

15 If your wireless network credentials are the same as your Windows logon credentials, select Automatically use my Windows logon name and password. Otherwise, make sure that this option is not selected.

16 Select OK. Repeat until you have closed all of the Wireless Network Connection Properties windows.

To connect to the WPA-Enterprise wireless network
1 Select the wireless network icon in the Notification area of the Taskbar.
2 In the View Wireless Networks list, select the network you just added and then select Connect.
   You might need to log off of your current wireless network and refresh the list.
3 When the following popup displays, click on it.

4 In the Enter Credentials window, enter your wireless network User name, Password, and Logon domain (if applicable). Then, select OK.

In future, Windows will automatically send your credentials when you log on to this network.
Windows 7 client

1. In the Windows Start menu, go to Control Panel > Network and Internet > Network and Sharing Center > Manage Wireless Networks or select the wireless network icon in the Notification area of the Taskbar. A list of available networks is displayed.

2. Do one of the following:
   - If the wireless network is listed (it broadcasts its SSID), select it from the list.
   - Select Add > Manually create a network profile.

3. Enter the following information and select Next.

   | Network name | Enter the SSID of the wireless network. (Required only if you selected Add.) |
   | Security type | WPA2-Enterprise |
   | Encryption type | AES |
   | Start this connection automatically | Select |
   | Connect even if the network is not broadcasting | Select |

   The Wireless Network icon will display a popup requesting that you click to enter credentials for the network. Click on the popup notification.

4. In the Enter Credentials window, enter your wireless network User name, Password, and Logon domain (if applicable). Then, select OK.

5. Select Change connection settings.
6 On the Connection tab, select Connect automatically when this network is in range.
7 On the Security tab, select the Microsoft PEAP authentication method and then select Settings.
8 Make sure that Validate server_certificate is selected.
9 Select the server certificate UTN-USERFirst-Hardware.
10 In Select Authentication Method, select Secured Password (EAP-MSCHAPv2).
11 Select Configure.
12 If your wireless network credentials are the same as your Windows logon credentials, select Automatically use my Windows logon name and password. Otherwise, make sure that this option is not selected.
13 Ensure that the remaining options are not selected.
14 Select OK. Repeat until you have closed all of the Wireless Network Properties windows.

Mac OS client

To configure network preferences
1 Right-click the AirPort icon in the toolbar and select Open Network Preferences.
2 Select Advanced and then select the 802.1X tab.
3 If there are no Login Window Profiles in the left column, select the + button and then select Add Login Window Profile.

4 Select the Login Window Profile and then make sure that both TTLS and PEAP are selected in Authentication.

**To configure the WPA-Enterprise network connection**

1 Select the AirPort icon in the toolbar.

2 Do one of the following:
   - If the network is listed, select the network from the list.
   - Select Connect to Other Network.

One of the following windows opens, depending on your selection.

3 Enter the following information and select OK or Join:

<table>
<thead>
<tr>
<th>Network name</th>
<th>Enter the SSID of your wireless network. (Other network only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Security</td>
<td>WPA Enterprise</td>
</tr>
<tr>
<td>802.1X</td>
<td>Automatic</td>
</tr>
<tr>
<td>Username Password</td>
<td>Enter your logon credentials for the wireless network.</td>
</tr>
<tr>
<td>Remember this network</td>
<td>Select.</td>
</tr>
</tbody>
</table>

You are connected to the wireless network.

Mac OS supports only PEAP with MSCHAPv2 authentication and therefore can authenticate only to a RADIUS server, not an LDAP or TACACS+ server.
Linux client

This example is based on the Ubuntu 10.04 Linux wireless client.

To connect to a WPA-Enterprise network

1. Select the Network Manager icon to view the Wireless Networks menu.

Wireless networks that broadcast their SSID are listed in the Available section of the menu. If the list is long, it is continued in the More Networks submenu.

2. Do one of the following:
   - Select the network from the list (also check More Networks).
   - Select Connect to Hidden Wireless Network.

One of the following windows opens, depending on your selection.
3 Enter the following information:

<table>
<thead>
<tr>
<th><strong>Connection</strong></th>
<th>Leave as New. (Hidden network only)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network name</strong></td>
<td>Enter the SSID of your wireless network. (Hidden network only)</td>
</tr>
<tr>
<td><strong>Wireless Security</strong></td>
<td>WPA &amp; WPA2 Enterprise</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Protected EAP (PEAP) for RADIUS-based authentication</td>
</tr>
<tr>
<td></td>
<td>Tunneled TLS for TACACS+ or LDAP-based authentication</td>
</tr>
<tr>
<td><strong>Anonymous identity</strong></td>
<td>This is not required.</td>
</tr>
<tr>
<td><strong>CA Certificate</strong></td>
<td>If you want to validate the AP’s certificate, select the UTN-USERFirst-Hardware root certificate. The default location for the certificate is /usr/share/ca-certificates/mozilla/.</td>
</tr>
<tr>
<td><strong>PEAP version</strong></td>
<td>Automatic (applies only to PEAP)</td>
</tr>
<tr>
<td><strong>Inner authentication</strong></td>
<td>MSCHAPv2 for RADIUS-based authentication</td>
</tr>
<tr>
<td></td>
<td>PAP or CHAP for TACACS+ or LDAP-based authentication</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter your logon credentials for the wireless network.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td></td>
</tr>
</tbody>
</table>

4 If you did not select a CA Certificate above, you are asked to do so. Select Ignore.

5 Select Connect. You are connected to the wireless network.

To connect to a WPA-Enterprise network

1 Select the Network Manager icon to view the Wireless Networks menu.
2 Select the network from the list (also check More Networks).

If your network is not listed (but was configured), select Connect to Hidden Wireless Network, select your network from the Connection drop-down list, and then select Connect.
Troubleshooting

Using tools provided in your operating system, you can find the source of common wireless networking problems.

Checking that the client has received IP address and DNS server information

Windows XP

1 Double-click the network icon in the taskbar to display the Wireless Network Connection Status window. Check that the correct network is listed in the Connection section.

2 Select the Support tab.
   Check that the Address Type is Assigned by DHCP. Check that the IP Address, Subnet Mask, and Default Gateway values are valid.

3 Select Details to view the DNS server addresses.
   The listed address should be the DNS serves that were assigned to the WAP. Usually a wireless network that provides access to the private LAN is assigned the same DNS servers as the wired private LAN. A wireless network that provides guest or customer users access to the Internet is usually assigned public DNS servers.

4 If any of the addresses are missing, select Repair.
   If the repair procedure doesn’t correct the problem, check your network settings.

Mac OS

1 From the Apple menu, open System Preferences > Network.

2 Select AirPort and then select Configure.

3 On the Network page, select the TCP/IP tab.

4 If there is no IP address or the IP address starts with 169, select Renew DHCP Lease.

5 To check DNS server addresses, open a terminal window and enter the following command:
   ```bash
cat /etc/resolv.conf
   ```
   Check the listed nameserver addresses. A network for employees should us the wired private LAN DNS server. A network for guests should specify a public DNS server.
Linux

This example is based on the Ubuntu 10.04 Linux wireless client.

1. Right-click the Network Manager icon and select Connection Information.

2. Check the IP address, and DNS settings. If they are incorrect, check your network settings.
Wireless network examples

This chapter provides an example wireless network configuration. The following topics are included in this section:

- Basic wireless network
- A more complex example

Basic wireless network

This example uses automatic configuration to set up a basic wireless network. To configure this wireless network, you must:

- Configure authentication for wireless users
- Configure the SSID (WiFi network interface)
- Configure the firewall policy
- Configure and connect FortiAP units

Configuring authentication for wireless users

You need to configure user accounts and add the users to a user group. This example shows only one account, but multiple accounts can be added as user group members.

To configure a WiFi user - web-based manager
1. Go to User > User and select Create New.
2. Enter a User Name and Password and then select OK.

To configure the WiFi user group - web-based manager
1. Go to User > User Group and select Create New.
2. Enter the following information and then select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>wlan_users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
<tr>
<td>Allow SSL-VPN Access</td>
<td>Not selected.</td>
</tr>
<tr>
<td>Available Users/Groups / Members</td>
<td>Move users to the Members list.</td>
</tr>
</tbody>
</table>

To configure a WiFi user and the WiFi user group - CLI

```
config user user
  edit "user01"
    set type password
    set passwd "asdf12ghjk"
  end
```
Configuring the SSID

First, establish the SSID (network interface) for the network. This is independent of the number of physical access points that will be deployed. The network assigns IP addresses using DHCP.

To configure the SSID - web-based manager

1. Go to WiFi Controller > WiFi Network > SSID and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>example_wifi</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Netmask</td>
<td>10.10.110.1/24</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>Ping (to assist with testing)</td>
</tr>
<tr>
<td>SSID</td>
<td>example_wifi</td>
</tr>
<tr>
<td>Enable DHCP</td>
<td>Enable</td>
</tr>
<tr>
<td>Address Range</td>
<td>10.10.110.2 - 10.10.110.199</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Same As Interface IP</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Same As System DNS</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA/WPA2-Enterprise</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>AES</td>
</tr>
<tr>
<td>Authentication</td>
<td>Usergroup, select wlan_users.</td>
</tr>
</tbody>
</table>

Leave other settings at their default values.

To configure the SSID - CLI

```bash
config wireless-controller vap
edit example_wifi
    set ssid "example_wifi"
    set broadcast-ssid enable
    set security wpa-enterprise
    set auth usergroup wlan_users
end
config system interface
edit example_wifi
    set ip 10.10.110.1 255.255.255.0
end
config system dhcp server
edit 0
    set default-gateway 10.10.110.1
    set dns-service default
    set interface "example_wifi"
```
config ip-range
   edit 1
       set end-ip 10.10.110.199
       set start-ip 10.10.110.2
   end
       set netmask 255.255.255.0
end

Configuring firewall policies

A firewall policy is needed to enable WiFi users to access the Internet on port1. First you create firewall address for the WiFi network, then you create the example_wifi to port1 policy.

To create a firewall address for WiFi users - web-based manager
1 Go to Firewall Objects > Address > Address.
2 Select Create New, enter the following information and select OK.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>wlan_user_net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.10.110.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>example_wifi</td>
</tr>
</tbody>
</table>

To create a firewall address for WiFi users - CLI

config firewall address
   edit "wlan_user_net"
       set associated-interface "example_wifi"
       set subnet 10.10.110.0 255.255.255.0
   end

To create a firewall policy for WiFi users - web-based manager
1 Go to Firewall Objects > Policy and select Create New.
2 Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>example_wifi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>wlan_user_net</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>All</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Enable NAT. Select Use Destination Interface Address (default).</td>
</tr>
</tbody>
</table>

Leave other settings at their default values.
To create a firewall policy for WiFi users - CLI

```
config firewall policy
edit 0
  set srcintf "example_wifi"
  set dstintf "port1"
  set srcaddr "wlan_user_net"
  set dstaddr "all"
  set action accept
  set nat enable
end
```

Connecting the FortiAP units

You need to connect each FortiAP unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port 3 and are controlled through IP addresses on the 192.168.8.0/24 network.

To configure the interface for the AP unit - web-based manager

1. Go to System > Network > Interface and edit the port3 interface.
2. Set the Addressing mode to Manual and set the IP/Netmask to 192.168.8.1.
3. Enable Connect FortiAP to this interface and set Reserve IP addresses for FortiAP to 192.168.8.2 – 192.168.8.9.

   This step automatically configures a DHCP server for the AP units. You can see this configuration in System > Network > DHCP Server.
4. Select OK.

To configure the interface for the AP unit - CLI

```
config system interface
edit port3
  set mode static
  set ip 192.168.8.1 255.255.255.0
end
```

To configure the DHCP server for AP units - CLI

```
config system dhcp server
edit 0
  set interface port3
  config ip-range
    edit 1
      set end-ip 192.168.8.9
      set start-ip 192.168.8.2
    end
  set netmask 255.255.255.0
  set vci-match enable
  set vci-string "FortiAP"
end
```
To connect a FortiAP unit - web-based manager

1. Go to WiFi Controller > Managed Access Points > Managed FortiAP.
2. Connect the FortiAP unit to port 3.
3. Periodically select Refresh while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If FortiAP units are connected but cannot be recognized, try disabling VCI-Match in
   the DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.
   The Edit Managed Access Point window opens.
5. In State, select Authorize.
6. Make sure that AP Profile is set to Automatic.
7. In SSID, select Automatically Inherit all SSIDs.
8. Select OK.
9. Repeat Steps 2 through 8 for each FortiAP unit.

To connect a FortiAP unit - CLI

1. Connect the FortiAP unit to port 3.
2. Enter config wireless-controller wtp
3. Wait 30 seconds, then enter get.
   Retry the get command every 15 seconds or so until the unit is listed, like this:
   == [ FAP22A3U10600118 ]
   wtp-id: FAP22A3U10600118
4. Edit the discovered FortiAP unit like this:
   edit FAP22A3U10600118
   set admin enable
   end
5. Repeat Steps 2 through 4 for each FortiAP unit.

A more complex example

This example creates multiple networks and uses custom AP profiles.

Scenario

In this example, Example Co. provides two wireless networks, one for its employees and
the other for customers or other guests of its business. Guest users have access only to
the Internet, not to the company’s private network. The equipment for these WiFi
networks consists of FortiAP-220A units controlled by a FortiGate unit.

The employee network operates in 802.11n mode on both the 2.4GHz and 5GHz bands.
Client IP addresses are in the 10.10.120.0/24 subnet, with 10.10.120.1 the IP address of
the WAP. The guest network also operates in 802.11n mode, but only on the 2.4GHz
band. Client IP addresses are on the 10.10.115.0/24 subnet, with 10.10.115.1 the IP
address of the WAP.

On FortiAP-220A units, the 802.11n mode also supports 802.11g and 802.11b clients on
the 2.4GHz band and 802.11a clients on the 5GHz band.
The guest network WAP broadcasts its SSID, the employee network WAP does not. The employees network uses WPA-Enterprise authentication through a FortiGate user group. The guest network features a captive portal. When a guest first tries to connect to the Internet, a login page requests logon credentials. Guests use numbered guest accounts authenticated by RADIUS. The captive portal for the guests includes a disclaimer page.

In this example, the FortiAP units connect to port 3 and are assigned addresses on the 192.168.8.0/24 subnet.

Configuration

To configure these wireless networks, you must:
- Configure authentication for wireless users
- Configure the SSIDs (network interfaces)
- Configure the AP profile
- Configure the WiFi LAN interface and a DHCP server
- Configure firewall policies

Configuring authentication for employee wireless users

Employees have user accounts on the FortiGate unit. This example shows creation of one user account, but you can create multiple accounts and add them as members to the user group.

To configure the user group for employee access - web-based manager
1. Go to User > User Group and select Create New.
2. Enter the following information and then select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>employee-group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
<tr>
<td>Allow SSL-VPN Access</td>
<td>Disabled</td>
</tr>
<tr>
<td>Available Users/Groups / Members</td>
<td>Move appropriate user accounts to the Members list.</td>
</tr>
</tbody>
</table>

To configure the user group for employee access - CLI

```
config user group
edit "employee-group"
    set member "user01"
end
```

The user authentication setup will be complete when you select the employee-group in the SSID configuration.

Configuring authentication for guest wireless users

Guests are assigned temporary user accounts created on a RADIUS server. The RADIUS server stores each user’s group name in the Fortinet-Group-Name attribute. Wireless users are in the group named “wireless”.

The FortiGate unit must be configured to access the RADIUS server.
To configure the FortiGate unit to access the guest RADIUS server - web-based manager

1. Go to User > Remote > RADIUS and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>guestRADIUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Server Name / IP</td>
<td>10.11.102.100</td>
</tr>
<tr>
<td>Primary Server Secret</td>
<td>grikfwpfdfg</td>
</tr>
<tr>
<td>Secondary Server Name / IP</td>
<td>Optional</td>
</tr>
<tr>
<td>Secondary Server Secret</td>
<td>Optional</td>
</tr>
<tr>
<td>Authentication Scheme</td>
<td>Use default, unless server requires otherwise.</td>
</tr>
</tbody>
</table>

Leave other settings at their default values.

To configure the FortiGate unit to access the guest RADIUS server - CLI

```
config user radius
  edit guestRADIUS
    set auth-type auto
    set server 10.11.102.100
    set secret grikfwpfdfg
  end
```

To configure the user group for guest access - web-based manager

1. Go to User > User Group and select Create New.
2. Enter the following information and then select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>guest-group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
<tr>
<td>Allow SSL-VPN Access</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Available Users/Groups / Members

Match one of these group names

<table>
<thead>
<tr>
<th>Remote Server</th>
<th>Select guestRADIUS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Enter wireless</td>
</tr>
</tbody>
</table>

To configure the user group for guest access - CLI

```
config user group
  edit "guest-group"
    set member "guestRADIUS"
  config match
    edit 0
      set server-name "guestRADIUS"
      set group-name "wireless"
  end
end
```
The user authentication setup will be complete when you select the guest-group user group in the SSID configuration.

### Configuring the SSIDs

First, establish the SSIDs (network interfaces) for the employee and guest networks. This is independent of the number of physical access points that will be deployed. Both networks assign IP addresses using DHCP.

**To configure the employee SSID - web-based manager**

1. Go to WiFi Controller > WiFi Network > SSID and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>example_inc</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Netmask</td>
<td>10.10.120.1/24</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>Ping (to assist with testing)</td>
</tr>
<tr>
<td>SSID</td>
<td>example_inc</td>
</tr>
<tr>
<td>Enable DHCP</td>
<td>Enable</td>
</tr>
<tr>
<td>Address Range</td>
<td>10.10.120.2 - 10.10.120.199</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Same As Interface IP</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Same as System DNS</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA/WPA2-Enterprise</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>AES</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select Usergroup, then select employee-group.</td>
</tr>
</tbody>
</table>

Leave other settings at their default values.

**To configure the employee SSID - CLI**

```bash
cfg wireless-controller vap
  edit example_inc
    set ssid "example_inc"
    set security wpa-enterprise
    set auth usergroup
    set usergroup employee-group
  end

cfg system interface
  edit example_inc
    set ip 10.10.120.1 255.255.255.0
  end

cfg system dhcp server
  edit 0
    set default-gateway 10.10.120.1
    set dns-service default
    set interface example_inc
    config ip-range
      edit 1
        set end-ip 10.10.120.199
        set start-ip 10.10.120.2
```
end
set lease-time 7200
set netmask 255.255.255.0
end

To configure the example_guest SSID - web-based manager

1. Go to WiFi Controller > WiFi Network > SSID and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>example_guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Netmask</td>
<td>10.10.115.1/24</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>Ping (to assist with testing)</td>
</tr>
<tr>
<td>SSID</td>
<td>example_guest</td>
</tr>
<tr>
<td>Enable DHCP</td>
<td>Enable</td>
</tr>
<tr>
<td>Address Range</td>
<td>10.10.115.2 - 10.115.50</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Same as Interface IP</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Same as System DNS</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Captive Portal</td>
</tr>
<tr>
<td>Customize Portal Messages</td>
<td>Select</td>
</tr>
<tr>
<td>User Groups</td>
<td>Select guest-group</td>
</tr>
<tr>
<td>Leave other settings at their default values.</td>
<td></td>
</tr>
</tbody>
</table>

To configure the example_guest SSID - CLI

```
config wireless-controller vap
edit example_guest
    set ssid "example_guest"
    set security captive-portal
    set selected-usergroups guest-group
end
config system interface
edit example_guest
    set ip 10.10.115.1 255.255.255.0
end
config system dhcp server
edit 0
    set default-gateway 10.10.115.1
    set dns-service default
    set interface "example_guest"
    config ip-range
        edit 1
            set end-ip 10.115.50
            set start-ip 10.115.2
        end
    set lease-time 7200
    set netmask 255.255.255.0
end
```
Configuring the custom AP profile

The custom AP Profile defines the radio settings for the networks. The profile provides access to both Radio 1 (2.4GHz) and Radio 2 (5GHz) for the employee virtual AP, but provides access only to Radio 1 for the guest virtual AP.

To configure the AP Profile - web-based manager

1. Go to WiFi Controller > Managed Access Points> Custom AP Profile and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>example_AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>FAP220A</td>
</tr>
<tr>
<td>Radio 1</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Access Point</td>
</tr>
<tr>
<td>Background Scan</td>
<td>Enable</td>
</tr>
<tr>
<td>Rogue AP On-wire Scan</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Radio Resource Provision</td>
<td>Not enabled.</td>
</tr>
<tr>
<td>Band</td>
<td>802.11n</td>
</tr>
<tr>
<td>Short Guard Interval</td>
<td>Not enabled.</td>
</tr>
<tr>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>Tx Power</td>
<td>100%</td>
</tr>
<tr>
<td>SSID</td>
<td>Select example_inc and example_guest.</td>
</tr>
<tr>
<td>Radio 2</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Access Point</td>
</tr>
<tr>
<td>Background Scan</td>
<td>Enable</td>
</tr>
<tr>
<td>Rogue AP On-wire Scan</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Band</td>
<td>802.11n_5G</td>
</tr>
<tr>
<td>Short Guard Interval</td>
<td>Not enabled.</td>
</tr>
<tr>
<td>20/40 MHz Channel Width</td>
<td>Not enabled.</td>
</tr>
<tr>
<td>Channel</td>
<td>Select all.</td>
</tr>
<tr>
<td>Tx Power</td>
<td>100%</td>
</tr>
<tr>
<td>SSID</td>
<td>Select example_inc.</td>
</tr>
</tbody>
</table>

To configure the AP Profile - CLI

```
config wireless-controller wtp-profile
edit "example_AP"
  config platform
    config platform
      set type 220A
    end
  config radio-1
    set ap-bgscan enable
    set band 802.11n
```
Wireless network examples

set channel "1" "6" "11"
set rogue-scan enable
set vaps "example_inc" "example_guest"
end
config radio-2
set ap-bgscan enable
set band 802.11n-5G
set channel "36" "40" "44" "48" "149" "153" "157" "161"
 "165"
set rogue-scan enable
set vaps "example_inc"
end

Configuring firewall policies

Identity-based firewall policies are needed to enable the WLAN users to access the Internet on Port1. First you create firewall addresses for employee and guest users, then you create the firewall policies.

To create firewall addresses for employee and guest WiFi users

1. Go to Firewall Objects > Address > Address.
2. Select Create New, enter the following information and select OK.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>employee-wifi-net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.10.120.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>example_inc</td>
</tr>
</tbody>
</table>

3. Select Create New, enter the following information and select OK.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>guest-wifi-net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.10.115.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>example_guest</td>
</tr>
</tbody>
</table>

To create firewall policies for employee WiFi users - web-based manager

1. Go to Policy > Policy and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>example_inc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>employee-wifi-net</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>All</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>Any</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Enable NAT</td>
</tr>
</tbody>
</table>
3 Optionally, select UTM and set up UTM features for wireless users.

4 Select OK.

5 Repeat steps 1 through 4 but select Internal as the Destination Interface/Zone to provide access to the ExampleCo private network.

To create firewall policies for employee WiFi users - CLI

```
cfg firewall policy
edit 0
  set srcintf "employee_inc"
  set dstintf "port1"
  set srcaddr "employee-wifi-net"
  set dstaddr "all"
  set action accept
  set schedule "always"
  set service "ANY"
  set nat enable
  set schedule "always"
  set service "ANY"
next
edit 0
  set srcintf "employee_inc"
  set dstintf "internal"
  set srcaddr "employee-wifi-net"
  set dstaddr "all"
  set action accept
  set schedule "always"
  set service "ANY"
  set nat enable
  set schedule "always"
  set service "ANY"
end
```

To create a firewall policy for guest WiFi users - web-based manager

1 Go to Policy > Policy and select Create New.

2 Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>example_guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>guest-wifi-net</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>All</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>Any</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Enable NAT</td>
</tr>
</tbody>
</table>

3 Optionally, select UTM and set up UTM features for wireless users.

4 Select OK.
To create a firewall policy for guest WiFi users - CLI

```plaintext
config firewall policy
edit 0
  set srcintf "example_guest"
  set dstintf "port1"
  set srcaddr "guest-wifi-net"
  set dstaddr "all"
  set action accept
  set schedule "always"
  set service "ANY"
  set nat enable
end
```

Connecting the FortiAP units

You need to connect each FortiAP-220A unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port 3 and are controlled through IP addresses on the 192.168.8.0/24 network.

To configure the interface for the AP unit - web-based manager

1. Go to System > Network > Interface and edit the port3 interface.
2. Set the Addressing mode to Manual and set the IP/Netmask to 192.168.8.1.
3. Enable Connect FortiAP to this interface and set Reserve IP addresses for FortiAP to 192.168.8.2 – 192.168.8.9.
   This step automatically configures a DHCP server for the AP units.
4. Select OK.

To configure the interface for the AP unit - CLI

```plaintext
config system interface
edit port3
  set mode static
  set ip 192.168.8.1 255.255.255.0
end
```

To configure the DHCP server for AP units - CLI

```plaintext
config system dhcp server
edit 0
  set interface port3
config ip-range
  edit 1
    set end-ip 192.168.8.9
    set start-ip 192.168.8.2
  end
  set netmask 255.255.255.0
  set vci-match enable
  set vci-string "FortiAP"
end
```
To connect a FortiAP-220A unit - web-based manager
1. Go to WiFi Controller > Managed Access Points > Managed FortiAP.
2. Connect the FortiAP unit to port 3.
3. Periodically select Refresh while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If there is persistent difficulty recognizing FortiAP units, try disabling VCI-Match in the
   DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.
   The Edit Managed Access Point window opens.
5. In State, select Authorize.
6. In the AP Profile, select [Change] and then select the example_AP profile.
7. Select OK.
8. Repeat Steps 2 through 8 for each FortiAP unit.

To connect a FortiAP-220A unit - CLI
1. Connect the FortiAP unit to port 3.
2. Enter
   config wireless-controller wtp
3. Wait 30 seconds, then enter get.
   Retry the get command every 15 seconds or so until the unit is listed, like this:
   == [ FAP22A3U10600118 ]
   wtp-id: FAP22A3U10600118
4. Edit the discovered FortiAP unit like this:
   edit FAP22A3U10600118
   set admin enable
   set wtp-profile example_AP
   end
5. Repeat Steps 2 through 4 for each FortiAP unit.
Using a FortiWiFi unit as a client

A FortiWiFi unit by default operates as a wireless access point. But a FortiWiFi unit can also operate as a wireless client, connecting the FortiGate unit to another wireless network.

This section includes the following topics:

- Use of client mode
- Configuring client mode

Use of client mode

In client mode, the FortiWiFi unit connects to a remote WiFi access point to access other networks or the Internet. This is most useful when the FortiWiFi unit is in a location that does not have a wired infrastructure.

For example, in a warehouse where shipping and receiving are on opposite sides of the building, running cables might not be an option due to the warehouse environment. The FortiWiFi unit can support wired users using its Ethernet ports and can connect to another access point wirelessly as a client. This connects the wired users to the network using the 802.11 WiFi standard as a backbone.

Note that in client mode the FortiWiFi unit cannot operate as an AP. WiFi clients cannot see or connect to the FortiWiFi unit in Client mode.

Figure 10: Fortinet unit in Client mode
Configuring client mode

To set up the FortiAP unit as a WiFi client, you must use the CLI. Before you do this, be sure to remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and so on.

To configure wireless client mode

1. Change the WiFi mode to client.
   In the CLI, enter the following commands:
   ```
   config system global
   set wireless-mode client
   end
   ```
   Respond “y” when asked if you want to continue. The FortiWiFi unit will reboot.

2. Create a WiFi interface and configure the appropriate WiFi client settings.
   For example, to configure the client for WPA-Personal authentication on the `our_wifi` SSID with passphrase `justforus`, enter the following in the CLI:
   ```
   config system interface
   edit client_wifi
   set type wireless
   set mode dhcp
   set wifi-ssid our_wifi
   set wifi-security wpa-personal
   set wifi-passphrase "justforus"
   end
   ```
   The WiFi interface `client_wifi` will receive an IP address using DHCP.

3. Configure a `client_wifi` to `port1` policy.
   You can use either CLI or web-based manager to do this. The important settings are:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Destination Interface/Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>client_wifi</code></td>
<td><code>port1</code></td>
</tr>
<tr>
<td><code>All</code></td>
<td><code>All</code></td>
</tr>
<tr>
<td><code>ACCEPT</code></td>
<td><code>ENABLE</code></td>
</tr>
<tr>
<td><code>Enable NAT. Select Use Destination Interface Address (default).</code></td>
<td></td>
</tr>
</tbody>
</table>

   Leave other settings at their default values.
WiFi Reference

This chapter provides some reference information pertaining to wireless networks. The following topics are included in this section:

- Wireless radio channels

Wireless radio channels

IEEE 802.11a/n channels

Table 4 lists the channels supported on FortiWiFi products that support the IEEE 802.11a and 802.11n wireless standards. 802.11a is available on FortiWiFi models 60B and higher. 802.11n is available on FortiWiFi models 80CM and higher.

All channels are restricted to indoor usage except in the Americas, where both indoor and outdoor use is permitted on channels 52 through 64 in the United States.

Table 4: IEEE 802.11a/n (5-GHz Band) channel numbers

<table>
<thead>
<tr>
<th>Channel number</th>
<th>Frequency (MHz)</th>
<th>Regulatory Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Americas</td>
</tr>
<tr>
<td>34</td>
<td>5170</td>
<td>•</td>
</tr>
<tr>
<td>36</td>
<td>5180</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>5190</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>5200</td>
<td>•</td>
</tr>
<tr>
<td>42</td>
<td>5210</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>5220</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>5230</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>5240</td>
<td>•</td>
</tr>
<tr>
<td>149</td>
<td>5745</td>
<td>•</td>
</tr>
<tr>
<td>153</td>
<td>5765</td>
<td>•</td>
</tr>
<tr>
<td>157</td>
<td>5785</td>
<td>•</td>
</tr>
<tr>
<td>161</td>
<td>5805</td>
<td>•</td>
</tr>
<tr>
<td>165</td>
<td>5825</td>
<td></td>
</tr>
</tbody>
</table>

IEEE 802.11b/g/n channel numbers

Table 5 lists IEEE 802.11b/g/n channels. All FortiWiFi units support 802.11b and 802.11g. Newer models also support 802.11n.

Mexico is included in the Americas regulatory domain. Channels 1 through 8 are for indoor use only. Channels 9 through 11 can be used indoors and outdoors. You must make sure that the channel number complies with the regulatory standards of Mexico.
<table>
<thead>
<tr>
<th>Channel number</th>
<th>Frequency (MHz)</th>
<th>Regulatory Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Americas</td>
</tr>
<tr>
<td>1</td>
<td>2412</td>
<td>•</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
<td>•</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
<td>•</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
<td>•</td>
</tr>
<tr>
<td>5</td>
<td>2432</td>
<td>•</td>
</tr>
<tr>
<td>6</td>
<td>2437</td>
<td>•</td>
</tr>
<tr>
<td>7</td>
<td>2442</td>
<td>•</td>
</tr>
<tr>
<td>8</td>
<td>2447</td>
<td>•</td>
</tr>
<tr>
<td>9</td>
<td>2452</td>
<td>•</td>
</tr>
<tr>
<td>10</td>
<td>2457</td>
<td>•</td>
</tr>
<tr>
<td>11</td>
<td>2462</td>
<td>•</td>
</tr>
<tr>
<td>12</td>
<td>2467</td>
<td>•</td>
</tr>
<tr>
<td>13</td>
<td>2472</td>
<td>•</td>
</tr>
<tr>
<td>14</td>
<td>2484</td>
<td>•</td>
</tr>
</tbody>
</table>
WiFi Controller Reference

This section introduces you to the web-based manager WiFi Controller menu. The following topics are included in this section:

- WiFi Controller overview
- WiFi Network
- Managed access points
- Monitor

The word “unit” refers to the FortiGate unit. The words “FortiGate unit” are used when talking about different Fortinet products in one sentence. For example, “The Central Management menu provides the option of remotely managing your FortiGate unit by a FortiManager unit.”

WiFi Controller overview

The WiFi Controller menu configures WiFi networks on your FortiWiFi or FortiGate unit. Your WiFi networks can use any of the following WiFi networking equipment:

- your FortiWiFi unit’s built-in wireless access point/client (see “FortiWiFi units” on page 14)
- FortiAP units—wireless access points compliant with the CAPWAP standard (see “FortiAP units” on page 16)
- the built-in wireless access point/client of a FortiWiFi unit connected to your unit (see “Using a FortiWiFi unit as a managed AP” on page 15)

Each of these pieces of WiFi networking equipment is an access point. Each access point can carry multiple networks to which clients can connect.

The WiFi Controller feature is available on all models running FortiOS or FortiOS Carrier, except model 30B.

The wireless controller feature can also:

- monitor activity on your WiFi networks
- monitor neighboring access points that might cause interference
- detect rogue (unauthorized) access points connected to your wired networks
- suppress access points that you have designated as rogues
WiFi Network

In the WiFi Network menu, you can configure SSID and rogue AP detection settings.

An SSID defines the security settings for a wireless LAN. For each SSID, the Fortinet unit creates a virtual network interface. You create firewall policies to control traffic between the SSID interface and other networks. Users need the correct security settings to connect to the access point, and they can also be required to authenticate to use a firewall policy.

A Rogue AP is an unauthorized AP connected to your network. This can be a security issue. Other APs may be receivable in your area. These APs belong to neighboring businesses or homes. They can cause interference but are not a security threat. The on-wire detection technique can distinguish between neighbors and rogues.

This topic includes the following:
- SSID list
- SSID configuration settings
- Rogue AP Settings

SSID list

The list of SSIDs (WiFi networks) at WiFi Controller > WiFi Network > SSID contains the following columns:

<table>
<thead>
<tr>
<th>Create New</th>
<th>Creates a new SSID. When you select Create New, you are automatically redirected to the New SSID page. See SSID configuration settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Modifies an SSID’s settings. When you select Edit, you are automatically redirected to the Edit SSID page. See SSID configuration settings.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes an SSID from the list on the SSID page. To remove multiple SSIDs from within the list, on the SSID page, in each of the rows of the SSIDs you want removed, select the check box and then select Delete. To remove all SSIDs from the list, on the SSID page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>SSID</td>
<td>The SSID or network name for the wireless interface.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Indicates whether the SSID’s administrative status is up or down. A green up arrow indicates that it is up; a red down arrow indicates that it is not.</td>
</tr>
</tbody>
</table>
| Security mode | The type of security for the wireless interface:  
- **WPA/WPA2 Personal** — user must know pre-shared key value to connect.  
- **WPA/WPA2 Enterprise** — user must know user name and password to connect.  
- **Captive Portal** — user connects to the open access point and then must authenticate to use the network |
### SSID configuration settings

When you edit an SSID or create a new one in WiFi Controller > WiFi Network > SSID, the following configuration settings are available:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Enter a name for the SSID.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Select to have the SSID’s status either up or down. If the SSID’s status is down, the SSID is not being used. If the SSID’s status is up, the SSID is being used.</td>
</tr>
<tr>
<td>Addressing Mode</td>
<td></td>
</tr>
<tr>
<td>IP/Netmask</td>
<td>Enter the IP address and netmask for the SSID.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Enter the IPv6 address. This is available only when IPv6 has been enabled on the unit.</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>Select the administrative access for the SSID.</td>
</tr>
<tr>
<td>IPv6 Administrative Access</td>
<td>If you have IPv6 addresses, select the administrative access for IPv6 for SSID.</td>
</tr>
<tr>
<td>Enable Explicit Web Proxy</td>
<td>Select to enable explicit web proxy for the SSID.</td>
</tr>
</tbody>
</table>

---

**Data Encryption**

The type of encryption for the wireless interface in WPA/WPA2 modes.

AES is the most secure, but some older clients support only TKIP.

**Clients**

The maximum number of clients permitted to connect simultaneously.

**Ref.**

Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (UTM > Antivirus > Profile), 1 appears in Ref.

To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object.

To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:

- **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at.
- **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when this icon is selected, the user is redirected to the Edit Policy page.
- **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting than the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy’s settings appear within the table.
## WiFi Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSID</strong></td>
<td>Enter the SSID. By default, this field contains fortinet.</td>
</tr>
<tr>
<td><strong>Enable DHCP</strong></td>
<td>Select to enable a DHCP server and configure basic DHCP server settings.</td>
</tr>
<tr>
<td></td>
<td>The Address Start and Address End settings are used to create an appropriate</td>
</tr>
<tr>
<td></td>
<td>DHCP server in the DHCP server list. If the unit is in transparent mode,</td>
</tr>
<tr>
<td></td>
<td>the DHCP server settings will be unavailable.</td>
</tr>
<tr>
<td><strong>Address Range</strong></td>
<td>Enter the starting IP address of the DHCP server.</td>
</tr>
<tr>
<td><strong>Netmask</strong></td>
<td>Enter the netmask of the DHCP server.</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>Enter the default gateway for the DHCP server.</td>
</tr>
<tr>
<td><strong>DNS Server</strong></td>
<td>Enter the DNS server.</td>
</tr>
<tr>
<td><strong>Security Mode</strong></td>
<td>Select the security mode for the wireless interface. Wireless users must</td>
</tr>
<tr>
<td></td>
<td>use the same security mode to be able to connect to this wireless interface.</td>
</tr>
<tr>
<td></td>
<td>Additional security mode options are available in the CLI.</td>
</tr>
<tr>
<td><strong>WPA/WPA2-Personal</strong></td>
<td>WPA or WPA2 security. WPA is WiFi protected access. WPA2 is WPA with</td>
</tr>
<tr>
<td></td>
<td>additional security features. There is one shared key (password) that all</td>
</tr>
<tr>
<td></td>
<td>users use.</td>
</tr>
<tr>
<td><strong>WPA/WPA2-Enterprise</strong></td>
<td>similar to WPA/WPA2-Personal, but is best used for enterprise networks.</td>
</tr>
<tr>
<td></td>
<td>Each user is separately authenticated by user name and password.</td>
</tr>
<tr>
<td><strong>Captive Portal</strong></td>
<td>Captive Portal – authenticates users through a customizable web page.</td>
</tr>
<tr>
<td><strong>Customize Portal</strong></td>
<td>Available only when Security Mode is Captive Portal. Select to customize</td>
</tr>
<tr>
<td><strong>Messages</strong></td>
<td>the endpoint replacement messages. When you select Edit, the Edit Message</td>
</tr>
<tr>
<td></td>
<td>window appears. Within the window, you can modify each one of the endpoint</td>
</tr>
<tr>
<td></td>
<td>replacement messages.</td>
</tr>
<tr>
<td><strong>User Groups</strong></td>
<td>Available only when Security Mode is Captive Portal. Select the user groups</td>
</tr>
<tr>
<td></td>
<td>that can authenticate.</td>
</tr>
<tr>
<td></td>
<td>To select a user group, select the group in Available and then use the -&gt;</td>
</tr>
<tr>
<td></td>
<td>arrow to move that group to Selected. To remove a user group from Selected,</td>
</tr>
<tr>
<td></td>
<td>select the group and then use the &lt;- arrow to move the group back to</td>
</tr>
<tr>
<td></td>
<td>Available.</td>
</tr>
<tr>
<td><strong>Data Encryption</strong></td>
<td>Available only when Security Mode is WPA/WPA2-Enterprise. Select TKIP or</td>
</tr>
<tr>
<td></td>
<td>AES encryption as appropriate for the capabilities of your wireless clients.</td>
</tr>
<tr>
<td></td>
<td>This is available for WPA/WPA2 security modes.</td>
</tr>
<tr>
<td><strong>Pre-shared Key</strong></td>
<td>Available only when Security Mode is WPA/WPA2-Personal. Enter the encryption</td>
</tr>
<tr>
<td></td>
<td>key that the clients must use.</td>
</tr>
</tbody>
</table>
Rogue AP Settings

From the Rogue AP Settings page, you can enable rogue AP detection and the on-wire rogue AP detection technique. Rogue APs are APs that are not known to the WiFi controller and these unknown APs can be monitored by using these two features.

The feature, *Enable On-Wire Rogue AP Detection Technique*, determines which unknown APs are actually connected to your network. The unknown APs are considered rogues.

You can enable or disable these settings in *WiFi Controller > WiFi Network > Rogue AP Settings*.

Managed access points

The WiFi controller needs to be configured to manage each physical access point and configure its radio settings for the wireless LAN.

From the Managed Access Points menu, you can configure managed FortiAP and local WiFi radio settings and create custom AP profiles.

This topic contains the following:

- Local WiFi Radio configuration settings
- Managed FortiAP list
- Managed FortiAP configuration settings
- Custom AP Profiles
- Custom AP Profile Settings

The Local WiFi Radio submenu is available only on FortiWiFi units.
Local WiFi Radio configuration settings

Go to WiFi Controller > Managed Access Points > Local WiFi Radio to configure the WiFi radio facility of your FortiWiFi unit. FortiGate units do not have this page.

**Local WiFi Radio page**

Displays the local WiFi radio settings. From this page you can change the local WiFi settings, such as changing the AP profile. You must select Apply to save the changes.

<table>
<thead>
<tr>
<th>AP Profile</th>
<th>Select Change to change the profile. A drop-down list appears when you select Change; select the profile from the list and then select Apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Wireless Radio</td>
<td>Select to enable the wireless radio settings on the unit.</td>
</tr>
<tr>
<td>Automatically Inherit All SSIDs</td>
<td>Select to have the unit automatically inherit all SSID broadcasts.</td>
</tr>
<tr>
<td>Select SSIDs</td>
<td>Select to manually choose which SSID broadcasts.</td>
</tr>
<tr>
<td>TX Power</td>
<td>Displays the transmission power in percent. Use the slider to change the power.</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel that the unit is broadcasting on. For example, channel 2.</td>
</tr>
<tr>
<td>Band</td>
<td>The IEEE wireless protocol that the unit is using.</td>
</tr>
</tbody>
</table>

**Managed FortiAP list**

Go to WiFi Controller > Managed Access Points > Managed FortiAP to view the list of managed APs that have discovered the WiFi Controller. On this page, you can edit, delete, authorize, ignore or restart access points.

<table>
<thead>
<tr>
<th>Edit</th>
<th>Modifies a managed physical AP’s settings. When you select Edit, you are automatically redirected to the Managed FortiAP configuration settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Removes a managed physical AP in the list on the Managed Physical AP page.</td>
</tr>
<tr>
<td></td>
<td>To remove multiple managed APs from within the list, on the Managed Physical AP page, in each of the rows of the APs you want removed, select the check box and then select Delete.</td>
</tr>
<tr>
<td></td>
<td>To remove all APs in the list, on the Managed Physical AP page, select the check box in the check box column, and then select Delete.</td>
</tr>
<tr>
<td>Column Settings</td>
<td>Not all columns are shown by default. Select Column Settings to choose which columns to display.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Select to refresh the current information on the page.</td>
</tr>
<tr>
<td>Restart</td>
<td>Select to restart an AP.</td>
</tr>
<tr>
<td>Show Ignored</td>
<td>Select to show the FortiAP units that the unit currently ignores.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the FortiAP unit. The state is indicated by an icon, for example, if there is a blue question mark, this indicates that the unit is connecting.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the FortiAP unit.</td>
</tr>
</tbody>
</table>
### Managed FortiAP configuration settings

You can select a managed AP on the WiFi Controller > Managed Access Points > Managed FortiAP page and modify the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>The name or serial number of the physical AP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients</td>
<td>The maximum number of clients that are permitted to connect simultaneously. When you click on the number, you are automatically redirected to WiFi Controller &gt; Monitor &gt; Client Monitor.</td>
</tr>
<tr>
<td>SSIDs</td>
<td>The SSIDs of the FortiAP unit.</td>
</tr>
<tr>
<td>Connecting From</td>
<td>The wired IP address of the FortiAP unit.</td>
</tr>
</tbody>
</table>

**Serial Number**

The serial number of the unit (read-only).

**Name**
Enter a name for the access point. Otherwise, the serial number is displayed as the AP name.

**Description**
Select Change to change the existing description. If there is no description, “N/A” displays.

**Managed AP status section**

**Status**
Indicates the connection status of the access point. For example, if the access point is connecting, Connecting displays.

**Connecting From**
The IP address of the unit.

**State**
The type of state the unit is in. Select Authorize to authorize the managed access point. If you want to deauthorize the managed access point, select Deauthorize.

**Wireless Settings**

**AP Profile**
The name of the AP Profile or Automatic if a custom profile is not used. Select Change to select a different profile or Automatic settings, then select Apply.

**Enable WiFi Radio**
Select to enable operation of this AP.

**SSID**
Automatically Inherit all SSIDs — AP will carry all WiFi networks. Select SSIDs — selects individual SSIDs for this AP to carry.

**Tx Power**
Adjust AP transmitter power. The 100% setting is the maximum permitted in your country.

**Band**
The WiFi radio band to be used. 802.11n, for example.

**Channel**
The radio channel currently in use.

**Do not participate in Rogue AP Scanning**
Select if AP performance is poor due to heavy traffic. The scanning function can affect performance.

**Wireless Settings with Custom AP Profile**

**Radio 1**
Specific information about the AP’s first radio.

**Radio 2**
Specific information about the AP’s second radio.
Custom AP Profiles

The following are profile configuration settings in WiFi Controller > Managed Access Points > Custom AP Profile.

<table>
<thead>
<tr>
<th>Custom AP Profile page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual physical FortiAP that are currently on your network. On this page, you can edit, delete, authorize, ignore or restart.</td>
<td></td>
</tr>
</tbody>
</table>

| Create New | Creates a new AP profile. When you select Create New, you are automatically redirected to the Custom AP Profile Settings page. |
| Edit | Modifies a managed physical AP settings. When you select Edit, you are automatically redirected to the Custom AP Profile Settings page. |
| Delete | Removes a managed physical AP in the list on the Managed Physical AP page. To remove multiple managed APs from within the list, on the Managed Physical AP page, in each of the rows of the APs you want removed, select the check box and then select Delete. To remove all APs in the list, on the Managed Physical AP page, select the check box in the check box column, and then select Delete. |

| Name | The name of the AP profile. |
| Comments | A description or comment about the AP profile. |
| Platform | The type of model that is associated with the AP profile. |
| Radio 1 | The selected radio band and channels for the first (or only) radio in the managed access point. |
| Radio 2 | The selected radio band and channels for the second radio in the managed access point. This is for FortiAP units only. |
| Ref. | Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a firewall policy; on the Profile page (UTM > Antivirus > Profile), 1 appears in Ref.. To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window: |
| - **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at. |
| - **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy and so, when the icon is selected, the user is redirected to the Edit Policy page. |
| - **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a firewall policy, and that firewall policy’s settings appear within the table. |
### Custom AP Profile Settings

You can edit or create new custom AP profiles on the WiFi Controller > Managed Access Points > Custom AP Profile page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the AP profile.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter a description or comment about the AP profile. This is optional.</td>
</tr>
<tr>
<td>Platform</td>
<td>Select the type of Fortinet platform that will be using the AP profile. For example, FortiWiFi-60C.</td>
</tr>
</tbody>
</table>
| Radio 1 settings / Radio 2 settings | Radio 1 settings are the same as Radio 2 settings except for the options for Channel.  
**Note:** Radio 2 settings are available only for FortiAP models with dual radios. |
| Mode               | Select the type of mode.  
- **Disable** – no mode is set.  
- **Access Point** – allows for the platform to be an access point  
- **Dedicated Monitor** – allows for the platform to be a dedicated monitor |
| Background Scan    | Select to enable a background scan, which monitors for rogue APs. This is for the Rogue AP feature. By default, a background scan is disabled.     |
| Radio Resource Provision | Select to enable the radio resource provision feature.                                                                                      |
| Band               | Select the IEEE wireless protocol that is available to the region.                                                                         |
| Short Guard Interval | Select to enable the short guard interval feature for 802.11n.                                                                           |
| 20/40 Mhz Channel Width | Select to enable the channel width to have 20/40 megahertz for 802.11n-5G.                                                              |
| Channel            | Select the channel or channels to include. These channels change with regards to what IEEE wireless protocol you selected in **Band**.          |
| TX Power           | By default, the TX power is set to 100% of the maximum power permitted in your region. To change the level, drag the slider.                   |
| SSID               | Choose the SSIDs (WiFi networks) that APs using this profile will carry.  
Select the required SSIDs in the **Available** list and use the -> arrow to move them to the **Selected** list. To remove an SSID from the **Selected** list, select the SSID and then use the <- arrow to move it back to the **Available** list. |
Monitor

The Monitor menu allows you to view monitored wireless activity.

This topic contains the following:

- Client Monitor
- Rogue AP Monitor

Client Monitor

In WiFi Controller > Monitor > Client Monitor, you can view information about wireless clients of your managed access points.

<table>
<thead>
<tr>
<th>Refresh</th>
<th>Update the information in the table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Settings</td>
<td>Select to filter the information on the page. Filters appears automatically after selecting Filter Settings, below the column headings. Use to configure filter settings.</td>
</tr>
<tr>
<td></td>
<td>- To apply a filter setting, select the plus sign beside Add new filter and then select and enter the information required. Repeat to add other filter settings.</td>
</tr>
<tr>
<td></td>
<td>- To modify settings, select Change beside the setting and edit the settings.</td>
</tr>
<tr>
<td></td>
<td>- To clear all filter settings, select the icon beside Clear all filters.</td>
</tr>
<tr>
<td></td>
<td>- To use a filter icon to filter settings within a column, select the filter icon in the column; Filters appears. Within Filters, configure the settings for that column.</td>
</tr>
<tr>
<td>Note: Filter Settings configures all filter settings. Filter icons are used to configure filter settings within that column.</td>
<td></td>
</tr>
<tr>
<td>Column Settings</td>
<td>Select the columns to display in the list. You can also determine the order in which they appear.</td>
</tr>
<tr>
<td>Page Controls</td>
<td>Use to navigate through the list.</td>
</tr>
</tbody>
</table>

Information columns

Actual columns displayed depends on Column Settings.

- **MAC** The MAC address of the wireless client.
- **Auth** The authentication type.
- **IP** The IP address assigned to the wireless client.
- **FortiAP** The name of the physical access point with which the client is associated.
- **SSID** The SSID for the managed access point.
- **Bandwidth Tx/Rx** The current bandwidth.
- **Signal Strength/Noise** The signal-to-noise ratio in deciBels calculated from signal strength and noise level.
- **Association Time** The time period that the client has been connected to this access point.
- **Bandwidth Rx** Received bandwidth used by the client, in Kbps.
**Bandwidth Tx**
Transmit bandwidth used by the client, in Kbps.

**Idle Time**
The total time this session that the client was idle.

**Rate**
The data rate of the client connection.

**Manufacturer**
The manufacturer of the client wireless device.

---

**Rogue AP Monitor**

View information about detected APs in **WiFi Controller > Monitor > Rogue AP Monitor**. You can also mark and suppress rogue APs.

<table>
<thead>
<tr>
<th>Mark</th>
<th>Select the down arrow to mark the AP as accepted, rogue or unclassified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppress AP</td>
<td>Select the down arrow to suppress the AP or unsuppress the AP. Available only if the AP is marked as a rogue AP.</td>
</tr>
<tr>
<td>Column Settings</td>
<td>Select the columns to display in the list. You can also determine the order in which they appear.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Select to update the information. <em>none</em> means no updates.</td>
</tr>
<tr>
<td>Show Accepted</td>
<td>Select to show only the accepted APs.</td>
</tr>
<tr>
<td>Total detected APs</td>
<td>Displays the total number of APs that are detected by the FortiGate unit.</td>
</tr>
</tbody>
</table>

**Information Columns**
Actual columns displayed depends on **Column Settings**.

<table>
<thead>
<tr>
<th>State</th>
<th>The state of the rogue AP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Status</td>
<td>A green check mark indicates an active access point. A grey X indicates that the access point is inactive.</td>
</tr>
<tr>
<td>SSID</td>
<td>The wireless service set identifier (SSID) or network name for the wireless interface.</td>
</tr>
<tr>
<td>Security Type</td>
<td>The type of security currently being used.</td>
</tr>
<tr>
<td>Channel</td>
<td>The wireless radio channel that the access point uses.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the Wireless interface.</td>
</tr>
<tr>
<td>Vendor Info</td>
<td>The name of the vendor.</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>The relative signal strength of the AP. Mouse over the symbol to view the signal-to-noise ratio.</td>
</tr>
<tr>
<td>Detected By</td>
<td>The name or serial number of the AP unit that detected the signal.</td>
</tr>
<tr>
<td>On-wire</td>
<td>A green up-arrow indicates a suspected rogue, based on the on-wire detection technique. A red down-arrow indicates AP is not a suspected rogue.</td>
</tr>
</tbody>
</table>
Appendix

Document conventions

Fortinet technical documentation uses the conventions described below.

IPv4 IP addresses

To avoid publication of public IPv4 IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Most of the examples in this document use the following IP addressing:

IP addresses are made up of A.B.C.D:

- A - can be one of 192, 172, or 10 - the private addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
  - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
  - Device or virtual device - allows multiple FortiGate units in this address space (VDOMs).
  - Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
  - 001 - 099 - physical address ports, and non-virtual interfaces
  - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.
- D - usage based addresses, this part is determined by what the device is doing. The following gives 16 reserved, 140 users, and 100 servers in the subnet.
  - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
  - 010 - 099 - DHCP range - users
  - 100 - 109 - FortiGate devices - typically only use 100
  - 110 - 199 - servers in general (see later for details)
  - 200 - 249 - static range - users
  - 250 - 255 - reserved (255 is broadcast, 000 not used)
- The D segment servers can be farther broken down into:
  - 110 - 119 - Email servers
  - 120 - 129 - Web servers
  - 130 - 139 - Syslog servers
  - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
  - 150 - 159 - VoIP / SIP servers / managers
  - 160 - 169 - FortiAnalyzers
  - 170 - 179 - FortiManagers
  - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
  - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
  - Fortinet products, non-FortiGate, are found from 160 - 189.
Example Network

Variations on network shown in Figure 3 are used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

Figure 3: Example network
Table 9: Example IPv4 IP addresses

<table>
<thead>
<tr>
<th>Location and device</th>
<th>Internal</th>
<th>Dmz</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Office, one FortiGate</td>
<td>10.11.101.100</td>
<td>10.11.201.100</td>
<td>172.20.120.191</td>
</tr>
<tr>
<td>Head Office, second FortiGate</td>
<td>10.12.101.100</td>
<td>10.12.201.100</td>
<td>172.20.120.192</td>
</tr>
<tr>
<td>Branch Office, one FortiGate</td>
<td>10.21.101.100</td>
<td>10.21.201.100</td>
<td>172.20.120.193</td>
</tr>
<tr>
<td>Office 7, one FortiGate with 9 VDOMs</td>
<td>10.79.101.100</td>
<td>10.79.101.100</td>
<td>172.20.120.194</td>
</tr>
<tr>
<td>Office 3, one FortiGate, web server</td>
<td>n/a</td>
<td>10.31.201.110</td>
<td>n/a</td>
</tr>
<tr>
<td>Bob in accounting on the corporate user network (DHCP) at Head Office, one FortiGate</td>
<td>10.0.11.101.200</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Router outside the FortiGate</td>
<td>n/a</td>
<td>n/a</td>
<td>172.20.120.195</td>
</tr>
</tbody>
</table>

Tips, must reads, and troubleshooting

A Tip provides shortcuts, alternative approaches, or background information about the task at hand. Ignoring a tip should have no negative consequences, but you might miss out on a trick that makes your life easier.

A Must Read item details things that should not be missed such as reminders to back up your configuration, configuration items that must be set, or information about safe handling of hardware. Ignoring a must read item may cause physical injury, component damage, data loss, irritation or frustration.

A Troubleshooting tip provides information to help you track down why your configuration is not working.

Typographical conventions

Table 10: Typographical conventions in Fortinet technical documentation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box, field, or check box label</td>
<td>From Minimum log level, select Notification.</td>
</tr>
<tr>
<td>CLI input</td>
<td>config system dns</td>
</tr>
<tr>
<td></td>
<td>set primary &lt;address_ipv4&gt;</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
<tr>
<td>CLI output</td>
<td>FGT-602803030703 # get system settings</td>
</tr>
<tr>
<td></td>
<td>comments : (null)</td>
</tr>
<tr>
<td></td>
<td>opmode : nat</td>
</tr>
</tbody>
</table>
Registering your Fortinet product

Access to Fortinet customer services, such as firmware updates, support, and FortiGuard services, requires product registration. You can register your Fortinet product at http://support.fortinet.com.

Training Services

Fortinet Training Services offers courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet training programs serve the needs of Fortinet customers and partners world-wide.

Visit Fortinet Training Services at http://campus.training.fortinet.com, or email training@fortinet.com.

Technical Documentation

Visit the Fortinet Technical Documentation web site, http://docs.fortinet.com, for the most up-to-date technical documentation.

The Fortinet Knowledge Base provides troubleshooting, how-to articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Customer service and support

Fortinet is committed to your complete satisfaction. Through our regional Technical Assistance Centers and partners worldwide, Fortinet provides remedial support during the operation phase of your Fortinet product’s development life cycle. Our Certified Support Partners provide first level technical assistance to Fortinet customers, while the regional TACs solve complex technical issues that our partners are unable to resolve.


Fortinet products End User License Agreement

See the Fortinet products End User License Agreement.
Index

Numerics
802.11 wireless protocols, 11

A
access point
   adding, 40
   enabling, 42
adding, configuring defining
   custom AP profile, 93
   local wifi radio, 90
   managed FortiAP, 91, 92
   rogue AP settings, 89
   SSID, 86
antenna, 12
AP profile
   creating, 23
   described, 21
   authentication, 14

B
band
   radio bands for wireless LANs, 11
   bandwidth, 17

C
captive portal, 13
certification, 106
channels
   for 802.11a, 83
   for 802.11b, 84
   for 802.11n 5GHz, 83
   radio channels for wireless LANs, 11
CLI syntax conventions, 102
client
   using FortiWiFi unit as a WiFi client, 81
   client mode, 81
   using FortiWiFi unit as a WiFi client, 81
comments, documentation, 106
   conventions, 98
   coverage, 16
   Cross-Site Scripting protection from, 104
custom AP profile
   configuring, 93
customer service, 106

D
Declined Disclaimer page
   modifying, 36
FortiWiFi unit, 14
  configuring as an AP unit, 47

G
glossary, 106
guest network, 13

H
how-to, 106

I
IEEE 802.11a, channels, 83
IEEE 802.11b, channels, 84
introduction
  Fortinet documentation, 106
IP address
  private network, 98

K
Knowledge Center, 106

L
local wifi radio
  configuring, 90

M
MAC filter, wireless, 29
managed access points
  FortiAP, 91, 92
managing access points
  local wifi radio, 90
mode
  operation, 9
monitoring
  rogue APs, 49, 96
  wireless clients, 49, 95

N
network topologies, 39

O
operation mode, 9

P
password
  administrator, 9
PMK caching, 19
power
  security consideration, 13
  WLAN power level, 12
pre-authentication, 19
product registration, 105

R
registering
  with Fortinet Technical Support, 105
RFC
  1918, 98
rogue AP settings, 89

S
security, 12
SSID
  configuring, 86
  described, 21
  whether to broadcast, 12

t
technical
documentation, 106
documentation conventions, 98
notes, 106
support, 106
technical support, 106
TKIP, 27
Training Services, 106

U
user group for wireless users, 30

V
virtual AP
  creating, 25
vulnerability
  Cross-Site Scripting, 104
  XSS, 104

W
WiFi controller
  discovery methods, 45
wireless
  client mode, 81
  configuring SSID, 86
  custom AP profile, 93
  managed FortiAP, 91, 92
  rogue AP settings, 89
WLAN
  firewall policies, 31

X
XSS vulnerability
  protection from, 104