FortiOS™ Handbook

Deploying Wireless Networks for FortiOS 5.0

FortiOS™ Handbook v5.0 MR0 Deploying Wireless Networks for FortiOS 5.0

Feb 20, 2014

01-506-126043-20140221

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Contents

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

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 Mesh explains how to configure a WiFi network where access points are connected to the WiFi controller wirelessly instead of by Ethernet.

WiFi-Ethernet Bridge Operation shows how to use the FortiAP WiFi-Ethernet bridge feature.

Protecting the WiFi Network explains the Wireless Intrusion Detection System (WIDS).

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.

Reference provides information about WiFi radio channels.

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

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 802.11b 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 108.

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 72.

Suppressing 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 76.

Rogue suppression is available only when there is a radio dedicated to scanning. It will not function during background scanning.

Wireless Intrusion Detection (WIDS)

You can create a WIDS profile to enable several types of intrusion detection:

- Unauthorized Device Detection
- Rogue/Interfering AP Detection
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- Weak WEP Detection
- Multi Tenancy Protection
- MAC OUI Checking

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 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.

or

- 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

Model	Radio	Simultaneous SSIDs
20C	802.11 b/g/n 2.4GHz 802.11 a/n 5GHz	7 for AP, 1 for monitoring
30B	802.11 b/g 2.4GHz	7 for AP, 1 for monitoring
40C	802.11 b/g/n 2.4GHz 802.11 a/n 5GHz	7 for AP, 1 for monitoring
50B	802.11 b/g 2.4GHz	7 for AP, 1 for monitoring
60B	802.11 b/g 2.4GHz 802.11 a 5GHz	7 for AP, 1 for monitoring
60C	802.11 b/g/n 2.4GHz 802.11 a/n 5GHz	7 for AP, 1 for monitoring
80/81CM	802.11 b/g/n 2.4GHz 802.11 a/n 5GHz	7 for AP, 1 for monitoring

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

Model	Radio 1	Radio 2	Simultaneous SSIDs
210B (indoor)	802.11 b/g/n 2.4GHz 802.11 a/n 5GHz	N/A	7 for AP, 1 for monitoring
220A (indoor)	802.11 b/g/n 2.4GHz	802.11 a/n 5GHz	14 for AP, 2 for monitoring

Table 2: FortiAP model capabilities

220B (indoor)	802.11 b/g/n 2.4GHz 802.11 a/n 5GHz	802.11 b/g/n 2.4GHz	14 for AP, 2 for monitoring
222B (outdoor)	802.11 b/g/n 2.4GHz	802.11 a/n 5GHz	14 for AP, 2 for monitoring

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.

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

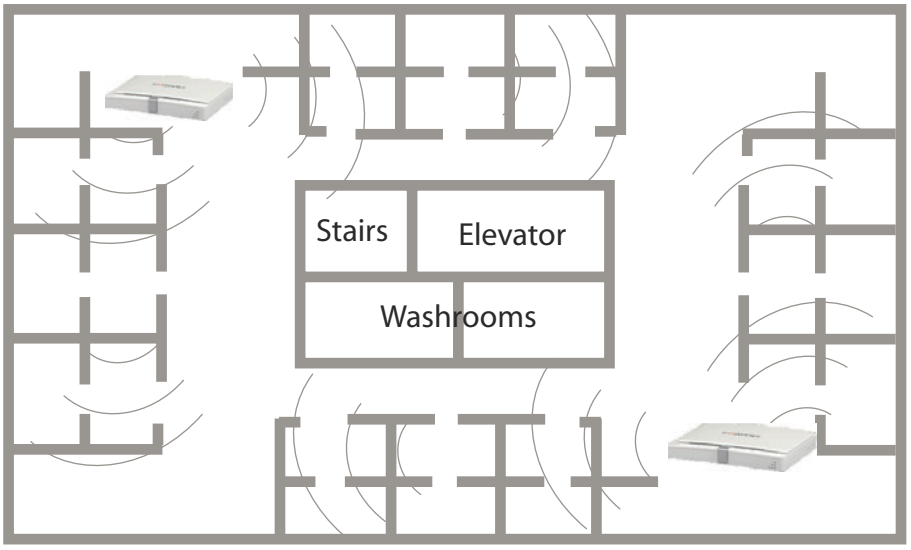
When placing the access point, your main concern is providing a strong signal to all users. A strong signal ensures a fast connection and efficient data transfer. A weaker signal means a greater chance of data transmission errors and the need to re-send information, slowing down data transfer.

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.

Figure 1: Using multiple APs to provide a constant strong signal.



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 for 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.

WiFi Mesh Network

FortiAP units can be connected to the WiFi controller by Ethernet or by WiFi. In the latter case, you configure a special backhaul network, the mesh, that carries traffic and control signals between FortiAP units and the WiFi controller. Regular WiFi clients cannot connect to the mesh network, they can connect only to non-mesh SSIDs. The mesh network is useful when running Ethernet cables is not practical. For best results, the mesh network should use a dedicated radio at both the WiFi controller and FortiAP unit. Otherwise, the client SSIDs compete for bandwidth with the mesh backhaul.

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, *Radio Resource Provision* 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:

On FortiGate model 30D, web-based manager configuration of the WiFi controller is disabled by default. To enable it, enter the following CLI commands:

```
config system global
  set gui-wireless-controller enable
end
```

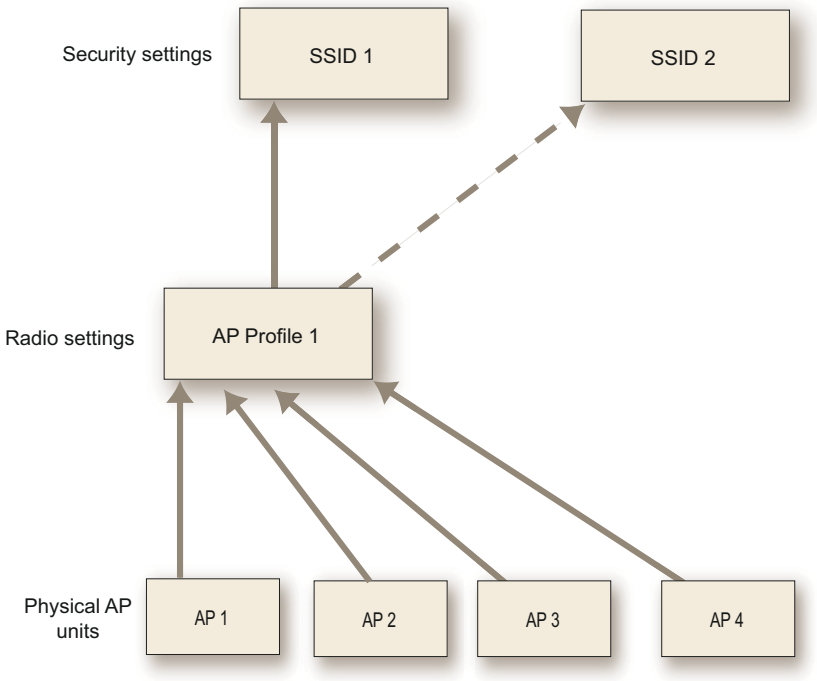
Overview of WiFi controller configuration

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.

Figure 2: Conceptual view of FortiGate WiFi controller configuration



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 3: Radio functions in automatic profile

No. of Radios	Wireless Access enabled	Rogue AP Scan enabled	Wireless Access and Rogue AP Scan enabled
1	Radio 1 - AP	Radio 1 - scan	Radio 1 - AP + background scan
2	Radio 1 - AP Radio 2 - disabled	Radio 1 - disabled Radio 2 - scan	Radio 1 - AP Radio 2 - scan

You can select which SSIDs (wireless networks) will be available through the access point and adjust the wireless power level of the AP. Also, you can configure the unit's LAN ports, if you are using a FortiAP model that has them (see "LAN port options" on page 48).

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* > *WiFi Network* > *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 19.

On FortiGate model 30D web-based manager configuration of custom AP profiles is disabled by default. To enable AP profiles, enter the following CLI commands:

```
config system global
  set gui-ap-profile enable
end
```

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* > *WiFi Network* > *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. For each radio, enter:

Mode	Select the type of mode. • *Disable* – radio disabled • *Access Point* – allows for the platform to be an access point • *Dedicated Monitor* – allows for the platform to be a dedicated monitor. See "Wireless network monitoring" on page 71.
Background Scan	Select to enable a background scan, which monitors other APs. This is needed for the Rogue AP feature. By default, background scan is disabled. See "Wireless network monitoring" on page 71.
Rogue AP On-Wire Scan	If Mode is either *Dedicated Monitor* or *Access Point* with *Background Scan* enabled, you can enable on-wire scan to distinguish rogue APs from neighbors. For more information, see "On-wire rogue AP detection technique" on page 72.
WIDS Profile	Optionally, select a Wireless Intrusion Detection (WIDS) profile. See "Wireless IDS" on page 68.
Radio Resource Provision	Select to enable the radio resource provision feature. 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.
Client Load Balancing	Select Frequency Handoff or AP Handoff as needed. See "Wireless client load balancing for high-density deployments" on page 47.

Band	Select the wireless protocols that you want to support. The available choices depend on the radio's capabilities. Where multiple protocols are supported, the letter suffixes are combined: "802.11bg" means 802.11b ***and*** 802.11g. For 802.11n, 802.11n_2.4G indicates 2.4GHz, 802.11n_5G indicates 5GHz. Note that on two-radio units such as the FortiAP-220B it is not possible to put both radios on the same band.
20/40 Mhz Channel Width	Select to enable 20/40 MHz channel width for 802.11n-5G.
Short Guard Interval	Select to enable the short guard interval for 802.11n_5G with 20/40 MHz channel width.
Channel	Select the channel or channels to include. The available channels depend on which IEEE wireless protocol you selected in *Band*. By default, all available channels are enabled.
Auto Tx Power Control	Optionally, enable automatic adjustment of transmit power, specifying minimum and maximum power levels.
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.

Radio 1 settings are the same as Radio 2 settings except for the options for *Channel*. Radio 2 settings are available only for FortiAP models with dual radios.

5. Select *OK*.

To configure an AP Profile - CLI

This example configures a FortiAP-220B to use only Radio 2 for 802.11g operation applied to SSID example_wlan.

```
config wireless-controller wtp-profile
  edit guest_prof
    config platform
      set type 220B
    end
    config radio-2
      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. When you create an SSID, a virtual network interface is also created with the *Name* you specified in the SSID configuration. You can configure the settings of an existing SSID in either *WiFi Controller* > *WiFi Network* > *SSID* or *System* > *Network* > *Interface*.

To create a new SSID

1. Go to *WiFi Controller* > *WiFi Network* > *SSID* and select *Create New*.
2. Fill in the SSID fields as described below.

To configure the settings of an existing SSID

1. Either
   - Go to *WiFi Controller* > *WiFi Network* > *SSID*.

   or
   - Go to *System* > *Network* > *Interfaces*.

     WiFi interfaces list the SSID beside the interface *Name*.
2. Edit a WiFi interface, modifying the SSID fields as needed.

SSID fields

Name	Enter a name for the SSID interface.
Type	WiFi SSID.
Traffic Mode	**Tunnel to Wireless Controller** — Data for WLAN passes through WiFi Controller. This is the default. **Local bridge with FortiAP's Interface** — FortiAP unit Ethernet and WiFi interfaces are bridged. **Mesh Downlink** — Radio receives data for WLAN from mesh backhaul SSID.
IP/Netmask	Enter the IP address and netmask for the SSID.
IPv6 Address	Enter the IPv6 address. This is available only when IPv6 has been enabled on the unit.
Administrative Access	Select which types of administrative access are permitted on this SSID.
IPv6 Administrative Access	If you have IPv6 addresses, select the permitted IPv6 administrative access types for this SSID.
DHCP Server	Select to enable a DHCP server and define IP address ranges to assign to clients or to relay DHCP requests to another server. If the unit is in transparent mode, the DHCP server settings will be unavailable. For more information, see "Configuring DHCP for WiFi clients" on page 26.

WiFi Settings	
SSID	Enter the SSID. By default, this field contains `fortinet`.
Security Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. Additional security mode options are available in the CLI. For more information, see "Configuring security" on page 26.
	WPA/WPA2-Personal – WPA or WPA2 security. WPA is WiFi protected access. WPA2 is WPA with additional security features. There is one shared key (password) that all users use.
	WPA/WPA2-Enterprise – similar to WPA/WPA2-Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password.
	Captive Portal – authenticates users through a customizable web page.
Pre-shared Key	Available only when *Security Mode* is *WPA/WPA2-Personal*. Enter the encryption key that the clients must use.
Data Encryption	Available only when *Security Mode* is *WPA/WPA2-Personal* or *WPA/WPA2-Enterprise*. Select *TKIP* or *AES* encryption as appropriate for the capabilities of your wireless clients. This is available for WPA/WPA2 security modes.
Authentication	Available only when *Security Mode* is *WPA/WPA2-Enterprise*. Select one of the following: *RADIUS Server* — Select the RADIUS server that will authenticate the clients. *Usergroup* – Select the user group(s) that can authenticate.
Customize Portal Messages	Available only when *Security Mode* is *Captive Portal*. Select to customize the endpoint replacement messages. When you select *Edit*, the Edit Message window appears. Within the window, you can modify each one of the endpoint replacement messages.
User Groups	Available only when *Security Mode* is *Captive Portal*. Select the user groups that can authenticate. To select a user group, select the group in *Available* and then use the -> arrow to move that group to *Selected*. To remove a user group from *Selected*, select the group and then use the <- arrow to move the group back to *Available*.
Block Intra-SSID Traffic	Select to enable the unit to block intra-SSID traffic.
Allow New WiFi Client Connections When Controller Is Down	This option is available for local bridge SSIDs with WPA-Personal security. See "Continued FortiAP operation when WiFi controller connection is down" on page 66.

Maximum Clients	Select to limit the number of clients permitted to connect simultaneously. Enter the limit value.
Device Management	Select *Detect and Identify Devices* if you want to monitor the device types using this interface or create device identity policies involving this interface. See “Managing “bring your own device”” on page 5. Optionally, enable *Add New Devices to Vulnerability Scan List*.
Enable Explicit Web Proxy	Select to enable explicit web proxy for the SSID.
Listen for RADIUS Accounting Messages	This is required to permit RADIUS SSO authentication on this WiFi inteface. See “SSO using RADIUS accounting records” on page 155.
Secondary IP Address	Optioanally, enable and define secondary IP addresses. Administrative access can be enabled on secondary interfaces.
Comments	Enter a description or comment for the SSID.

By default, the AP will broadcast its SSID. Optionally, you can disable SSID Broadcast in the CLI:

```
config wireless controller vap
  edit vap_name
    set broadcast-ssid disable
  end
```

For more information, see “Whether to broadcast SSID” on page 10.

Each Virtual AP that you create is a wireless interface that establishes a wireless LAN. Go to *System* > *Network* > *Interfaces* to configure its IP address.

To configure a virtual access point (SSID) - 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, enable *DHCP Server*.
3. In *Address Range*, select *Create New*.
4. In the *Starting IP* and *End IP* 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.
5. Set the *Netmask* to an appropriate value, such as 255.255.255.0.
6. Set the *Default Gateway* to *Same as Interface IP*.
7. Set the *DNS Server* to *Same as System DNS*.
8. If you want to restrict access to the wireless network by MAC address, see "Adding a MAC filter" on page 29.
9. Select *OK*.

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

Using the web-based manager, you can configure Open Portal security or Wi-Fi Protected Access (WPA) security modes WPA-Personal and WPA-Enterprise. The WPA options support both WPA and WPA2, which has additional security improvements. Using the CLI, you can also choose WPA-only and WPA2-only modes.

Using the CLI, you can also choose Wireless Equivalent Privacy (WEP) modes. WEP modes are much less secure and are provided for legacy support only. Wherever possible, use WPA security.

WPA security with a preshared key for authentication is called WPA-Personal. This can work well for one person 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 & Device* > *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 & Device* > *Authentication* > *RADIUS Server* 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
- **Login failed page**—reports that the entered credentials were incorrect and enables the user to try again.
- **Disclaimer page**—is a 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.

To configure Captive Portal security - web-based manager

1. Configure user groups as needed in *User & Device* > *User* > *User Groups*.
2. Go to *WiFi Controller* > *WiFi Network* > *SSID* and edit your SSID entry.
3. In *Security Mode*, select *Captive Portal*.
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 - web-based manager

1. Go to *WiFi Controller* > *WiFi Network* > *SSID* and edit your SSID entry.
2. In the *DHCP Server* section, expand Advanced.
3. In *MAC Address Access Control List*, select *Create New*.
4. Enter a MAC address In the *MAC* field.
5. Double-click in *IP or Action*, and do one of:
   - Select *Reserve IP* and enter the IP address to assign to this MAC address.
   - Select *Assign IP*. This MAC address will be assigned an IP address automatically.
   - Select *Block*. This MAC address will not be assigned an IP address.
6. Double-click in the Unknown MAC Addresses line and select Assign IP or Block, as needed.

   By default, unlisted MAC addresses are assigned an IP address automatically.
7. Repeat steps 3 through 6 for each additional MAC address that you want to add.
8. Select OK.

To configure a MAC filter - CLI

1. Enter

```
config system dhcp server
show
```

2. Find the entry where `interface` is your WiFi interface. Edit that entry and configure the MAC filter. In this example, the MAC address 11:11:11:11:11:11will be excluded. Unlisted MAC addresses will be assigned an IP address automatically.

```
edit 3
   config reserved-address
      edit 1
         set action block
         set mac 11:11:11:11:11:11
      end
   set mac-acl-default-action assign
end
```

Multicast enhancement

FortiOS can translate multicast traffic into unicast traffic to send to clients, maintaining its own multicast client through IGMP snooping. You can configure this in the CLI:

```
config wireless-controller vap
   edit example_wlan
      set multicast-enhance enable
      set me-disable-thresh 32
   end
```

If the number of clients on the SSID is larger than `me-disable-thresh`, multicast enhancement is disabled.

Dynamic VLAN assignment

You can assign each individual user to a VLAN based on information stored in the RADIUS authentication server. If the user's RADIUS record does not specify a VLAN ID, the user is assigned to the default VLAN for the SSID.

The RADIUS user attributes used for the VLAN ID assignment are:

IETF 64 (Tunnel Type)—Set this to VLAN.

IETF 65 (Tunnel Medium Type)—Set this to 802

IETF 81 (Tunnel Private Group ID)—Set this to the VLAN ID.

To configure dynamic VLAN assignment, you need to:

1. Configure access to the RADIUS server.
2. Create the SSID and enable dynamic VLAN assignment.
3. Create a custom AP profile and add the local bridge mode SSID to it.
4. Create the VLAN interfaces and their DHCP servers.
5. Create security policies to allow communication from the VLAN interfaces to the Internet.
6. Authorize the FortiAP unit and assign the custom profile to it.

To configure access to the RADIUS server

1. Go to *User & Device* > *Authentication* > *RADIUS Server* and select *Create New*.
2. Enter a Name, the name or IP address in Primary Server Name/IP, and the server secret in Primary Server Secret.

To create the dynamic VLAN SSID

1. Go to WiFi Controller > WiFi Network > SSID, select Create New and enter:

Name	An identifier, such as dynamic_vlan_ssid.
Traffic Mode	Local bridge or Tunnel, as needed.
SSID	An identifier, such as DYNSSID.
Security Mode	WPA/WPA2-Enterprise
Authentication	RADIUS Server. Select the RADIUS server that you configured.

2. Select OK.
3. Enable dynamic VLAN in the CLI. Optionally, you can also assign a VLAN ID to set the default VLAN for users without a VLAN assignment.

```
config wireless-controller vap
  edit dynamic_vlan_ssid
    set dynamic-vlan enable
    set vlanid 10
  end
```

To create the custom AP profile for the dynamic VLAN SSID

1. Go to *WiFi Controller* > *WiFi Network* > *Custom AP Profile*, select Create New and enter:

Name	A name for the profile, such as dyn_vlan_profile.
Platform	The FortiAP model you are using. If you use more than one model of FortiAP, you will need a custom AP profile for each model.
Radio 1 and Radio 2	
SSID	In the *Available* column, select the SSID you created (example dynamic_vlan_ssid) and move it to the *Selected* column. There should be no other SSIDs in the *Selected* column.

2. Adjust other radio settings as needed.
3. Select OK.

To create the VLAN interfaces

1. Go to *System* > *Network* > *Interfaces* and select *Create New*.
2. Enter:

Name	A name for the VLAN interface, such as VLAN100.
Interface	The physical interface associated with the VLAN interface.
VLAN ID	The numeric VLAN ID, for example 100.
Addressing mode	Select Manual and enter the IP address / Network Mask for the virtual interface.
DHCP Server	Enable and then select Create New to create an address range.

3. Select OK.
4. Repeat the preceding steps to create other VLANs as needed.

Security policies determine which VLANs can communicate with which other interfaces. These are the simple Firewall Address policy without authentication. Users are assigned to the appropriate VLAN when they authenticate.

To connect and authorize the FortiAP unit

1. Connect the FortiAP unit to the FortiGate unit.
2. Go to *WiFi Controller* > *Managed Access Points* > *Managed AP*.
3. When the FortiAP unit is listed, double-click the entry to edit it.
4. In *AP Profile*, select *Change*, then select the custom profile that you created. Select *Apply*.
5. Select Authorize.
6. Select OK.

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 & Device* > *Authentication* > *RADIUS Server* 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.

MAC-based authentication

Wireless clients can also be supplementally authenticated by MAC address. A RADIUS server stores the allowed MAC address for each client and the wireless controller checks the MAC address independently of other authentication methods.

MAC-based authentication must be configured in the CLI. In the following example, MAC-based authentication is added to an existing access point “vap1” to use a RADIUS server at 192.168.1.95:

```
config wireless-controller vap
  edit vap1
    set radius-mac-auth enable
    set radius-mac-auth-server 192.168.1.95
  end
```

Authenticating guest WiFi users

The FortiOS Guest Management feature enables you to easily add guest accounts to your FortiGate unit. These accounts are authenticate guest WiFi users for temporary access to a WiFi network managed by a FortiGate unit.

To implement guest access, you need to

1. Go to *User & Device* > *User* > *User Group* and create one or more guest user groups.
2. Go to *User & Device* > *User* > *Guest Management* to create guest accounts. You can print the guest account credentials or send them to the user as an email or SMS message.
3. Go to *WiFi Controller* > *WiFi Network* > *SSID* and configure your WiFi SSID to use captive portal authentication. Select the guest user group(s) that you created.

Guest users can log into the WiFi captive portal with their guest account credentials until the account expires. For more detailed information about creating guest accounts, see “Managing Guest Access” in the Authentication chapter of the this FortiOS Handbook.

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* > *Addresses*.
2. Select *Create New*, enter the following information and select *OK*.

Name	Enter a name for the address, wifi_net for example.
Type	Select *Subnet.*
Subnet / IP Range	Enter the subnet address, 10.10.110.0/24 for example.
Interface	Select the interface where this address is used, e.g., example_wifi

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* > *Policy* and select *Create New*.
2. In *Incoming Interface*, select the wireless interface.
3. In *Source Address*, select the address of your WiFi network, wifi_net for example.
4. In *Outgoing Interface*, select the Internet interface, for example, *port1*.
5. In *Destination Address*, select *All*.
6. In *Service*, select ALL, 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, 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"
    set nat enable
  end
```

Customizing captive portal pages

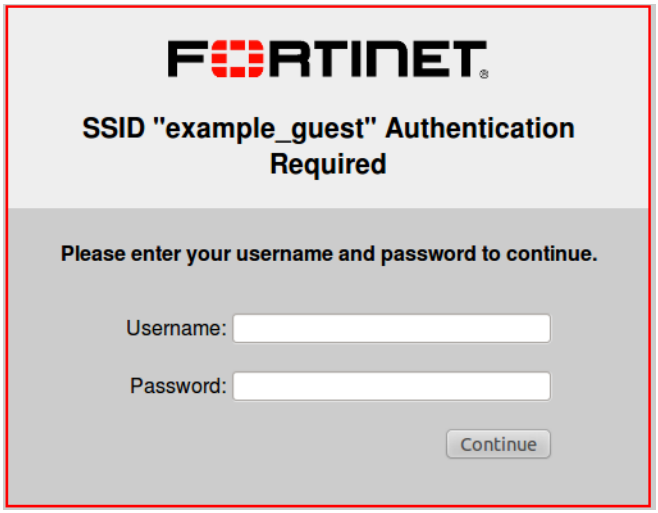
If you select Captive Portal authentication in the SSID, the wireless controller presents the user pages defined in Captive Portal Default replacement pages.

The captive portal contains the following web pages:

- **Captive Portal Login page**—requests user credentials
- **Captive Portal Login Failed page**—reports that the entered credentials were incorrect and enables the user to try again.
- **Captive Portal Disclaimer page**—is statement of the legal responsibilities of the user and the host organization to which the user must agree before proceeding.
- **Captive Portal Rejected 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.

Figure 3: Default captive portal login page



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.

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.

To import a logo file

1. Go to *System* > *Config* > *Replacement Messages* 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:%%IMAGE:logo_fw_auth%%
5. Change the image name to the one you provided for your logo.

   The tag should now read, for example, %%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*.

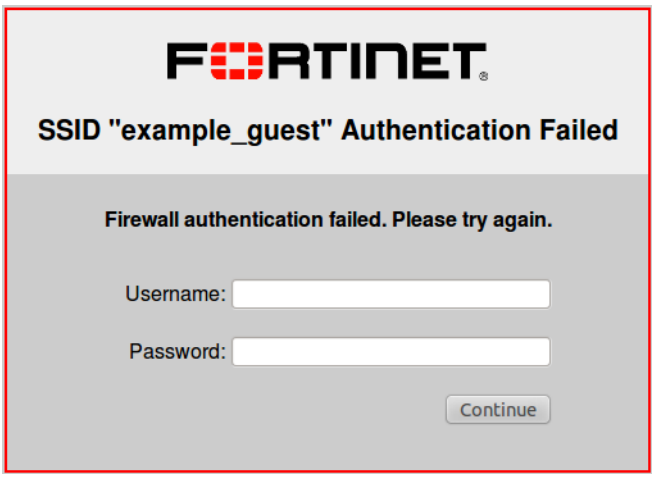
Modifying the login failed page

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.
- 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



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 20), 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".

Access point deployment

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

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 5, 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 5, 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 6, below.

Figure 5: Wirecloset and Gateway deployments

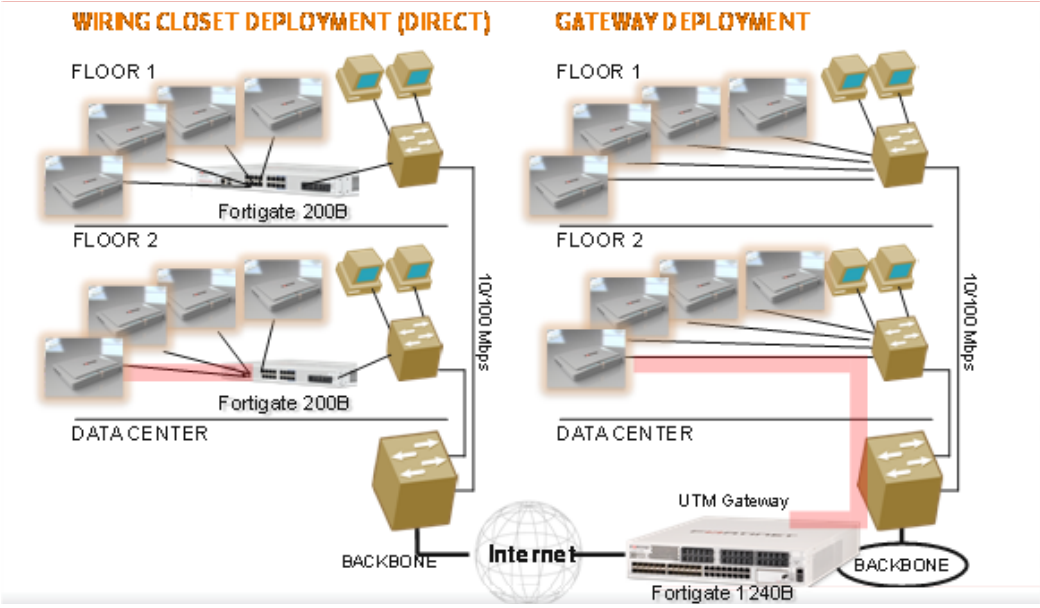
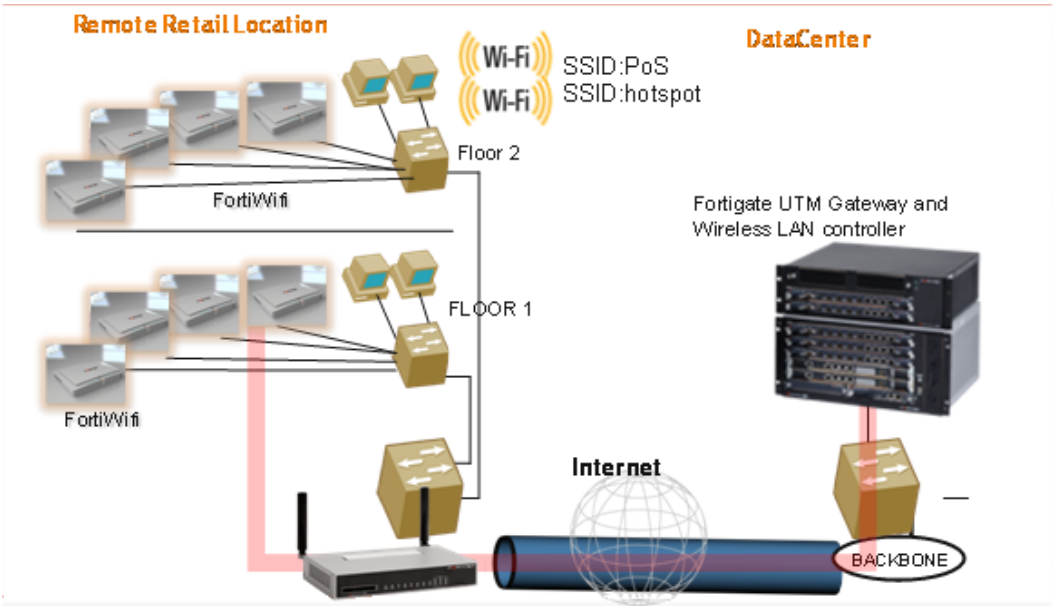


Figure 6: Remote deployment



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.
- Optionally, preauthorize FortiAP units. They will begin to function when connected.
- 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* > *Interfaces* and edit the interface to which the AP unit connects.
2. Set *Addressing Mode* to *Dedicate to FortiAP.*
3. Enter the IP address and netmask to use.

   This FortiGate unit automatically configures a DHCP server on the interface that will assign the remaining higher addresses up to .254 to FortiAP units. For example, if the IP address is 10.10.1.100, the FortiAP units will be assigned 10.10.1.101 to 10.10.1.254. To maximize the available addresses, use the .1 address for the interface: 10.10.1.1, for example.
4. Select OK.

To configure the interface for the AP unit - CLI

In the CLI, you must configure the interface IP address and DHCP server separately.

```
config system interface
  edit port3
    set mode static
    set ip 10.10.70.1 255.255.255.0
  end
config system dhcp server
  edit 0
    set interface "dmz"
    config ip-range
      edit 1
        set end-ip 10.10.70.254
        set start-ip 10.10.70.2
      end
    set netmask 255.255.255.0
    set vci-match enable
    set vci-string "FortiAP"
  end
```

The optional `vci-match` and `vci-string` fields ensure that the DHCP server will provide IP addresses only to FortiAP units.

Pre-authorizing a FortiAP unit

If you enter the FortiAP unit information in advance, it is authorized and will begin to function when it is connected.

To pre-authorize a FortiAP unit

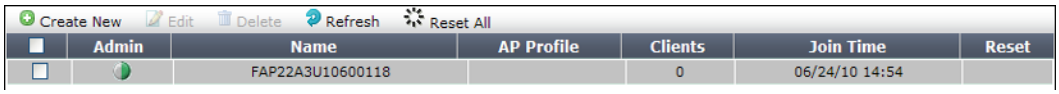
1. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAPs* and select *Create New*.

   On some models the *WiFi Controller* menu is called *WiFi & Switch Controller*.
2. Enter the *Serial Number* of the FortiAP unit.
3. Configure the *Wireless Settings* as required.
4. Select *OK*.

Enabling and configuring 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 7: Discovered access point unit



When you authorize (enable) 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 add and configure the discovered AP unit - web-based manager

1. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP*.

   This configuration also applies to local WiFi radio on FortiWiFi models.
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. If you want to use the Automatic profile, adjust its settings if needed:

Enable WiFi Radio	This must be selected to enable operation of this AP.
SSID	**Automatically Inherit all SSIDs** — AP will carry all WiFi networks. **Select SSIDs** — select individual SSIDs for this AP to carry.
Auto TX Power Control	If you enable automatic transmitter power control, adjust TX Power Low and TX Power High to set the power range.
Tx Power	If you are not using automatic power control, adjust AP transmitter power. The 100% setting is the maximum permitted in your country. See "Setting your geographic location" on page 20

6. If you want to use a custom AP profile, in *AP Profile* select *Change*, choose the AP Profile. Select *Apply*.
7. Optionally, select *Do not participate in Rogue AP scanning* if scanning adversely affects traffic.
8. 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 modify settings within the 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.

```
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 a custom AP profile - CLI

```
config wireless-controller wtp
  edit FAP22A3U10600118
    set wtp-profile AP-profile1
  end
```

To select automatic AP profile - CLI

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

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.

Assigning the same profile to multiple FortiAP units

The same profile can now be applied to multiple managed FortiAP units at the same time. To do this, do the following:

1. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAPs* to view the AP list.
2. Select all FortiAP units you wish to apply the profile to.
3. Right click on one of the selected FortiAPs and select *Assign Profile*.
4. Choose the profile you wish to apply.

Checking and updating FortiAP unit firmware

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

Checking the FortiAP unit firmware version

Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* to view the list of FortiAP units that the FortiGate unit can manage. The *OS Version* column shows the current firmware version running on each AP.

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.

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

```
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

```
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

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

To change the multicast address on a FortiAP unit

```
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

```
cfg -a AC_DISCOVERY_DHCP_OPTION_CODE=139
```

For information about connecting to the FortiAP CLI, see "Connecting to the FortiAP CLI" below.

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.

Wireless client load balancing for high-density deployments

Wireless load balancing allows your wireless network to distribute wireless traffic more efficiently among wireless access points and available frequency bands. FortiGate wireless controllers support the following types of client load balancing:

- Access Point Hand-off - the wireless controller signals a client to switch to another access point.
- Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency.

Load balancing is not applied to roaming clients.

Access point hand-off

Access point handoff wireless load balancing involves the following:

- If the load on an access point (ap1) exceeds a threshold (of for example, 30 clients) then the client with the weakest signal will be signaled by wireless controller to drop off and join another nearby access point (ap2).
- When one or more access points are overloaded (for example, more than 30 clients) and a new client attempts to join a wireless network, the wireless controller selects the least busy access point that is closest to the new client and this access point is the one that responds to the client and the one that the client joins.

Frequency hand-off or band-steering

Encouraging clients to use the 5GHz WiFi band if possible enables those clients to benefit from faster interference-free 5GHz communication. The remaining 2.4GHz clients benefit from reduced interference.

The WiFi controller probes clients to determine their WiFi band capability. It also records the RSSI (signal strength) for each client on each band.

If a new client attempts to join the network, the controller looks up that client's MAC address in its wireless device table and determines if it's a dual band device. If it is not a dual band device, then its allowed to join. If it is a dual band device, then its RSSI on 5GHz is used to determine whether the device is close enough to an access point to benefit from movement to 5GHz frequency.

If both conditions of 1) dual band device and 2) RSSI value is strong, then the wireless controller does not reply to the join request of the client. This forces the client to retry a few more times and then timeout and attempt to join the same SSID on 5GHz. Once the Controller see this new request on 5GHz, the RSSI is again measured and the client is allowed to join. If the RSSI is below threshold, then the device table is updated and the controller forces the client to timeout again. A client's second attempt to connect on 2.4GHz will be accepted.

Configuration

From the web-based manager edit a custom AP profile and select *Frequency Handoff* and *AP Handoff* as required for each radio on the AP.

From the CLI, you configure wireless client load balancing thresholds for each custom AP profile. Enable access point hand-off and frequency hand-off separately for each radio in the custom AP profile.

```
config wireless-controller wtp-profile
  edit new-ap-profile
    set handoff-rssi <rssi_int>
    set handoff-sta-thresh <clients_int>
    config radio-1
      set frequency-handoff {disable | enable}
      set ap-handoff {disable | enable}
    end
    config radio-2
      set frequency-handoff {disable | enable}
      set ap-handoff {disable | enable}
    end
  end
```

Where:

- `handoff-rssi` is the RSSI threshold. Clients with a 5 GHz RSSI threshold over this value are load balanced to the 5GHz frequency band. Default is 25. Range is 20 to 30.
- `handoff-sta-thresh` is the access point handoff threshold. If the access point has more clients than this threshold it is considered busy and clients are changed to another access point. Default is 30, range is 5 to 25.
- `frequency-handoff` enable or disable frequency handoff load balancing for this radio. Disabled by default.
- `ap-handoff` enable or disable access point handoff load balancing for this radio. Disabled by default.

Frequency handoff must be enabled on the 5GHz radio to learn client capability.

LAN port options

Some FortiAP models have one or more ethernet interfaces marked LAN. These ports can provide wired network access. LAN ports are bridged to either the wired WAN interface or to one of the WiFi SSIDs that the FortiAP unit carries.

Bridging a LAN port with a FortiAP SSID

Bridging a LAN port with a FortiAP SSID combines traffic from both sources to provide a single broadcast domain for wired and wireless users.

In this configuration

- The IP addresses for LAN clients come from the DHCP server that serves the wireless clients.
- Traffic from LAN clients is bridged to the SSID's VLAN. Dynamic VLAN assignment for hosts on the LAN port is not supported.
- Wireless and LAN clients are on the same network and can communicate locally, via the FortiAP.
- Any host connected to the LAN port will be taken as authenticated. RADIUS MAC authentication for hosts on the LAN port is not supported.

For configuration instructions, aee "Configuring FortiAP LAN ports", below.

Bridging a LAN port with the WAN port

Bridging a LAN port with the WAN port enables the FortiAP unit to be used as a hub which is also an access point.

In this configuration

- The IP addresses for LAN clients come from the WAN directly and will typically be in the same range as the AP itself.
- All LAN client traffic is bridged directly to the WAN interface.
- Communication between wireless and LAN clients can only occur if a policy on the FortiGate unit allows it.

For configuration instructions, aee "Configuring FortiAP LAN ports", below.

Configuring FortiAP LAN ports

How you configure FortiAP LAN ports depends on whether you use the automatic AP profile or create custom AP profiles. The Automatic AP profile enables APs to be individually configured. Custom AP profiles are useful if you have multiple APs that are the same model and share the same configuration.

Configuring LAN ports for an FortiAP unit - web-based manager

If your FortiAP units use the automatic AP profile, you configure each individual unit's LAN ports after you connect it to the FortiGate unit and the FortiAP discovers the WiFi controller. The AP is then listed in the Managed FortiAPs list.

To configure a FortiAP unit's LAN ports - web-based manager

1. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAPs.*

   On FortiGate models 100D, 600C, 800C, and 1000C, go to *WiFi & Switch Controller* > *Managed Devices* > *Managed FortiAPs.*
2. Select the FortiAP unit from the list and select *Edit*.
3. In the *LAN Port* section, set *Mode* to *Bridge to* and select an SSID or *WAN Port* as needed.

   On some models with multiple LAN ports, you can set *Mode* to *Custom* and configure the LAN ports individually. Enable each port that you want to use and select an SSID or *WAN Port* as needed.
4. Select *OK*.

To configure a FortiAP unit's LAN ports - CLI

In this example, a FortiAP unit's configuration is modified to bridge the LAN port to the office SSID.

```
config wireless-controller wtp
  edit FAP11C3X13000412
    config lan
      set port-mode bridge-to-ssid
      set port-ssid office
    end
  end
```

In this example, a FortiAP-28C unit's configuration is modified to bridge LAN port1 to the office SSID and to bridge the other LAN ports to the WAN port.

```
config wireless-controller wtp
  edit FAP28C3X13000412
    config lan
      set port1-mode bridge-to-ssid
      set port1-ssid office
      set port2-mode bridge-to-wan
      set port3-mode bridge-to-wan
      set port4-mode bridge-to-wan
      set port5-mode bridge-to-wan
      set port6-mode bridge-to-wan
      set port7-mode bridge-to-wan
      set port8-mode bridge-to-wan
    end
  end
```

Configuring LAN ports in a custom AP profile - web-based manager

When multiple FortiAP units will have the same LAN port configuration, you can create a custom AP profile or edit the default profile for that model.

To configure FortiAP LAN ports in a custom AP profile - web-based manager

1. Go to *WiFi Controller* > *WiFi Network* > *Custom AP Profiles*.
2. Either
   - Edit the default profile for your model,

   or
   - Select *Create New* and then in *Platform*, select your FortiAP model.
3. In the *LAN Port* section, set mode to *Bridge to* and select an SSID or *WAN Port* as needed.

   On some models with multiple LAN ports, you can select *Custom* to configure the ports individually. Enable each port that you want to use and select an SSID or *WAN Port* as needed.
4. Optionally, adjust other settings. See "Creating a custom AP Profile" on page 21.
5. Select *OK*.

To configure FortiAP LAN ports in a custom AP profile - CLI

In this example, the default FortiAP-11C profile is configured to bridge the LAN port to the office SSID.

```
config wireless-controller wtp-profile
  edit FAP11C-default
    config lan
      set port-mode bridge-to-ssid
      set port-ssid office
    end
  end
end
```

In this example, the default FortiAP-28C profile is configured to bridge LAN port1 to the office SSID and to bridge the other LAN ports to the WAN port.

```
config wireless-controller wtp-profile
  edit FAP28C-default
    config lan
      set port1-mode bridge-to-ssid
      set port1-ssid office
      set port2-mode bridge-to-wan
      set port3-mode bridge-to-wan
      set port4-mode bridge-to-wan
      set port5-mode bridge-to-wan
      set port6-mode bridge-to-wan
      set port7-mode bridge-to-wan
      set port8-mode bridge-to-wan
    end
  end
```

Preventing IP fragmentation of packets in CAPWAP tunnels

A common problem with controller-based WiFi networks is reduced performance due to IP fragmentation of the packets in the CAPWAP tunnel.

Fragmentation can occur because of CAPWAP tunnel overhead increasing packet size. If the original wireless client packets are close to the maximum transmission unit (MTU) size for the network (usually 1500 bytes for Ethernet networks unless jumbo frames are used) the resulting CAPWAP packets may be larger than the MTU, causing the packets to be ed. ing packets can result in data loss, jitter, and decreased throughput.

The FortiOS/FortiAP solution to this problem is to cause wireless clients to send smaller packets to FortiAP devices, resulting in1500-byte CAPWAP packets and no fragmentation. The following options configure CAPWAP IP fragmentation control:

```
config wireless-controller wtp
  edit new-wtp
    set ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}
    set tun-mtu-uplink {0 | 576 | 1500}
    set tun-mtu-downlink {0 | 576 | 1500}
  end
end
```

By default, `tcp-mss-adjust` is enabled, `icmp-unreachable` is disabled, and `tun-mtu-uplink` and `tun-mtu-downlink` are set to 0.

To set `tun-mtu-uplink` and `tun-mtu-downlink`, use the default TCP MTU value of 1500. This default configuration prevents packet fragmentation because the FortiAP unit limits the size of TCP packets received from wireless clients so the packets don’t have to be ed before CAPWAP encapsulation.

The `tcp-mss-adjust` option causes the FortiAP unit to limit the maximum segment size (MSS) of TCP packets sent by wireless clients. The FortiAP does this by adding a reduced MSS value to the SYN packets sent by the FortiAP unit when negotiating with a wireless client to establish a session. This results in the wireless client sending packets that are smaller than the `tun-mtu-uplink` setting, so that when the CAPWAP headers are added, the CAPWAP packets have an MTU that matches the `tun-mtu-uplink` size.

The `icmp-unreachable` option affects all traffic (UDP and TCP) between wireless clients and the FortiAP unit. This option causes the FortiAP unit to drop packets that have the "Don't Fragment" bit set in their IP header and that are large enough to cause fragmentation and then send an ICMP packet -- type 3 "ICMP Destination unreachable" with code 4 "Fragmentation Needed and Don't Fragment was Set" back to the wireless controller. This should cause the wireless client to send smaller TCP and UDP packets.

Wireless Mesh

The access points of a WiFi network are usually connected to the WiFi controller through Ethernet wiring. A wireless mesh eliminates the need for Ethernet wiring by connecting WiFi access points to the controller by radio. This is useful where installation of Ethernet wiring is impractical.

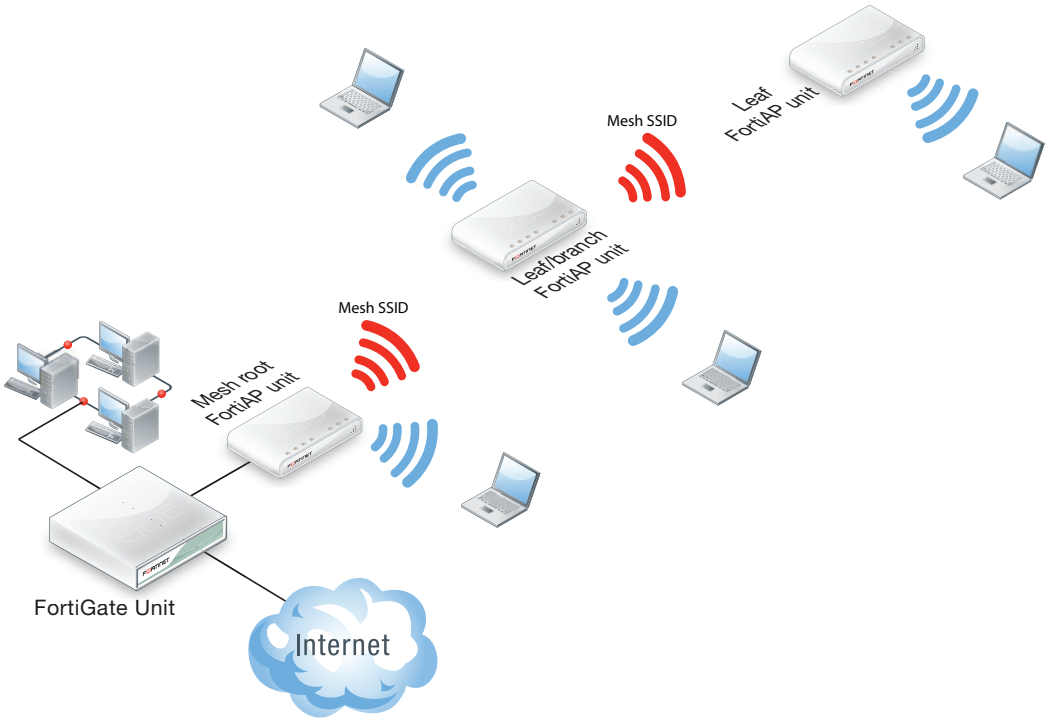
The following topics are included in this section:

- Overview of Wireless Mesh
- Configuring a meshed WiFi network
- Configuring a point-to-point bridge

Overview of Wireless Mesh

Figure 8 shows a wireless mesh topology.

Figure 8: Wireless mesh topology



The AP that is connected to the network by Ethernet is called the Mesh Root node. It is configured with an SSID (also called a virtual access point or VAP) dedicated to backhaul communication with the remote FortiAP units. The backhaul SSID carries CAPWAP discovery, configuration, and other communications that would usually be carried on an Ethernet connection. Regular WiFi clients cannot connect to the backhaul SSID. They connect to the regular SSIDs carried on the access points.

The root node can be a FortiAP unit or the built-in AP of a FortiWiFi unit. APs that serve only regular WiFi clients are called Leaf nodes. Leaf APs that also carry the mesh SSID for more distant Leaf nodes are called Leaf/branch nodes.

All access points in a wireless mesh configuration must have at least one of their radios configured to provide mesh backhaul communication. As with wired APs, when mesh APs start up they can be discovered by a FortiGate or FortiWiFi unit WiFi controller and authorized to join the network.

The backhaul SSID delivers the best performance when it is carried on a dedicated radio. On a two-radio FortiAP unit, for example, the 5GHz radio could carry only the backhaul SSID while the 2.4GHz radio carries one or more SSIDs that serve users. Background WiFi scanning is possible in this mode.

The backhaul SSID can also share the same radio with SSIDs that serve users. Performance is reduced because the backhaul and user traffic compete for the available bandwidth. Background WiFi scanning is not available in this mode. One advantage of this mode is that a two-radio AP can offer WiFi coverage on both bands.

The root mesh AP is the AP unit that has a wired Ethernet connection to the WiFi controller. The AP units that are wirelessly linked to the controller over the backhaul SSID are called branch or leaf APs.

Wireless mesh deployment modes

There are two common wireless mesh deployment modes:

Wireless Mesh	Access points are wirelessly connected to a FortiGate or FortiWiFi unit WiFi controller. WiFi users connect to wireless SSIDs in the same way as on non-mesh WiFi networks.
Wireless bridging	Two LAN segments are connected together over a wireless link (the backhaul SSID). On the leaf AP, the Ethernet connection can be used to provide a wired network. Both WiFi and wired users on the leaf AP are connected to the LAN segment to which the root AP is connected.

Firmware requirements

All FortiAP units that will be part of the wireless mesh network must be upgraded to FAP firmware version 5.0 build 003. FortiAP-222B units must have their BIOS upgraded to version 400012. The FortiWiFi or FortiGate unit used as the WiFi controller must be running FortiOS 5.0.

Types of wireless mesh

A WiFi mesh can provide access to widely-distributed clients. The root mesh AP which is directly connected to the WiFi controller can be either a FortiAP unit or the built-in AP of a FortiWiFi unit that is also the WiFi controller.

Figure 9: FortiAP units used as both mesh root AP and leaf AP

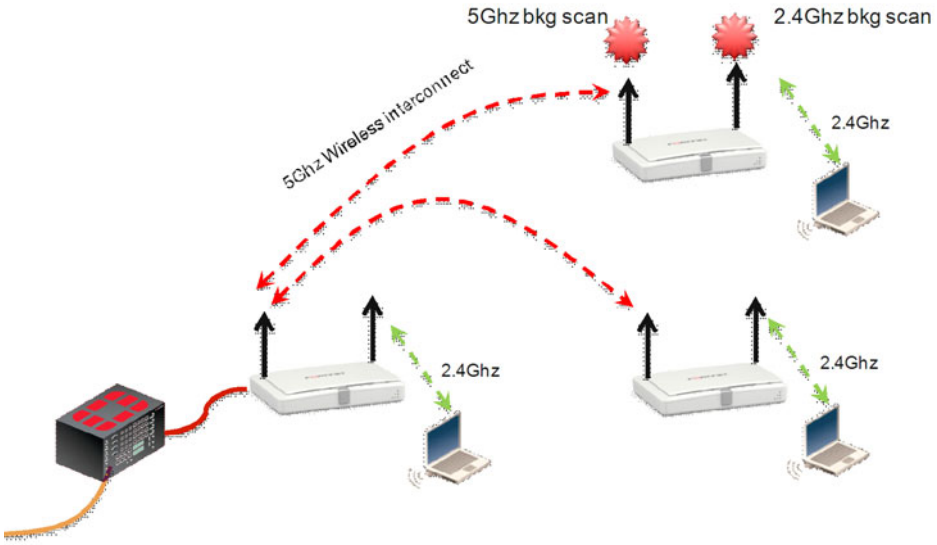
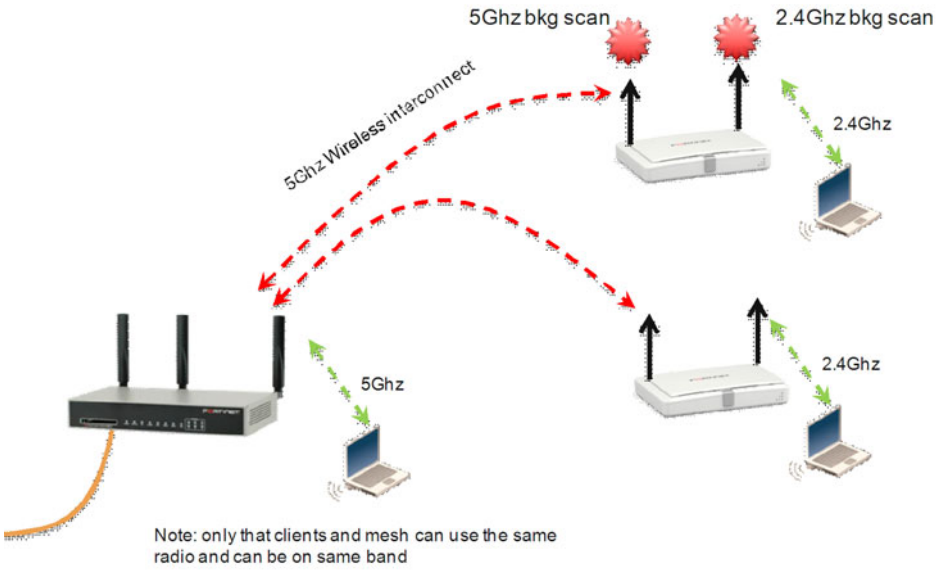
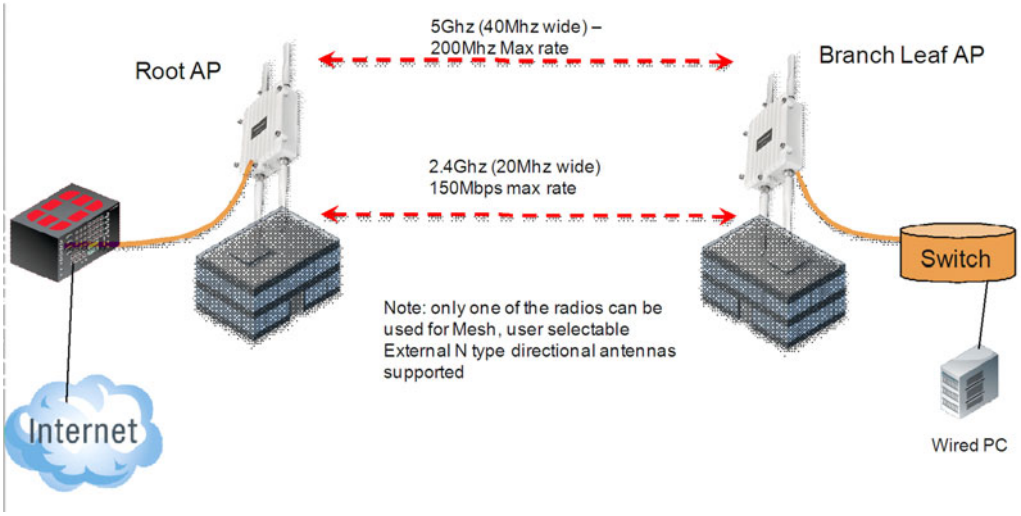


Figure 10: FortiWiFi unit as root mesh AP with FortiAP units as leaf APs



An alternate use of the wireless mesh functionality is as a point-to-point relay. Both wired and WiFi users on the leaf AP side are connected to the LAN segment on the root mesh side.

Figure 11: Point-to-point wireless mesh



Configuring a meshed WiFi network

Each VDOM on the FortiGate unit contains a predefined WiFi mesh interface named wl.mesh and a predefined SSID (which cannot be deleted) named fortinet.mesh.<vdom-name>. You can create additional mesh SSIDs. Create the SSID with *Traffic Mode* set to *Mesh Downlink*.

You need to:

- Create custom AP profiles, if you are not using the automatic AP profile.
- Configure the mesh root AP, either a FortiWiFi unit's Local Radio or a FortiAP unit.
- Configure mesh branch/leaf AP units.
- Authorize the mesh branch/leaf units when they connect to the WiFi Controller.

Creating custom AP profiles

You can apply the automatic AP profile or create one or more custom AP profiles for the mesh root and branch/leaf APs. A custom profile provides more control over which radio channels are used, intrustion protection, load balancing, background rogue AP scanning, and so on. Typically, the custom profiles are configured so that Radio 1 (5GHz) carries the mesh backhaul SSID while Radio 2 (2.4GHz) carries the SSIDs to which users connect.

For more information, see "Creating a custom AP Profile" on page 21.

Configuring the mesh root AP

The mesh root AP can be either a FortiWiFi unit's built-in AP or a FortiAP unit.

To enable a FortiWiFi unit's Local Radio as mesh root - web-based manager

1. Go to *WiFi Controller* > *Managed Access Points* > *Local WiFi Radio*.
2. Select *Enable WiFi Radio*.
3. In *SSID*, select *Select SSIDs*, then select *fortinet.mesh.root*.
4. Optionally, adjust *TX Power* or select *Auto Tx Power Control*.

5. Select *Apply*.

In a network with multiple wireless controllers, you need to change the mesh SSID so that each mesh root has a unique SSID. Other controllers using the same mesh root SSID might be detected as fake or rogue APs. Go to *WiFi Controller* > *WiFI Network* > *SSID* to change the SSID.

Fortinet also recommends that you create a new preshared key instead of using the default.

To configure a network interface for the FortiAP unit

1. On the FortiGate unit, go to *System* > *Network* > *Interfaces*.
2. Select the interface where you will connect the FortiAP unit and edit it.
3. In *Addressing mode*, select *Manual*.
4. In *IP/Network Mask*, enter an IP address and netmask for the interface.

   To maximize the number of addresses available for clients, the interface address should end with 1, for example 192.168.10.1.
5. In *DHCP Server* select *Enable*.

   An *Address Range* is entered automatically. It consists of the subnet address space above the interface address. For example, if the interface IP/mask is 192.168.10.100/24, the DHCP address range is 192.168.10.101 through 192.168.10.254.
6. Select *OK*.

To enable a FortiAP unit as mesh root - web-based manager

1. Connect the root FortiAP unit's Ethernet port to the FortiGate network interface that you configured for it. Connect the FortiAP unit to its power source.
2. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP*.

   If the root FortiAP unit is not listed, wait 15 seconds and select *Refresh*. Repeat if necessary. If the unit is still missing after a minute or two, power cycle the root FortiAP unit and try again.
3. Select the discovered FortiAP unit and edit its settings.
   - To use the Automatic profile enter:

AP Profile	Automatic
Enable WiFi Radio	Selected
SSID	Select SSID, then enable fortinet.root.mesh.
Tx Power	Optionally, adjust *TX Power* or select *Auto Tx Power Control*.

   or

   - In *AP Profile*, select *Change* and the select the custom AP profile you created for the mesh root AP.
4. In *State*, select *Authorize*.
5. Select *OK*.

You need to create firewall policies to permit traffic to flow from the network interface where the FortiAP unit is connected to the network interfaces for the Internet and other networks. Enable NAT.

Configuring the mesh branches or leaves

The FortiAP units that will serve as branch/leaf nodes must be preconfigured.

1. Connect to the FortiAP unit web-based manager on its default Ethernet interface IP address, 192.168.1.2.
2. In the *Connectivity* section enter:

Uplink	Mesh
Mesh AP SSID	fortinet.mesh.<vdom-name> For example, for the root domain, fortinet.mesh.root.
Mesh AP Password	Same as Mesh AP SSID.
Ethernet Bridge	Select

3. Select *Apply* and then select *Logout*.

Authorizing mesh branch/leaf APs

The pre-configured branch/leaf FortiAP units will connect themselves wirelessly to the WiFi Controller through the mesh network. You must authorize each unit

1. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP*. Periodically select *Refresh* until the FortiAP unit is listed.

   The *State* of the FortiAP unit should be *Waiting for Authorization*.
2. Open the FortiAP entry for editing.
   - To use the Automatic profile enter:

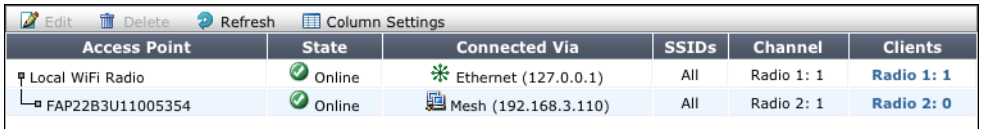
AP Profile	Automatic
Enable WiFi Radio	Selected
SSID	Optionally, select the SSIDs to make available to users.
Tx Power	Optionally, adjust *TX Power* or select *Auto Tx Power Control*.

   or

   - In *AP Profile*, select *Change* and the select the custom AP profile that you created for the branch/leaf APs and then select *[Apply]*.
3. Select *Authorize*.
4. Select *OK*.

   Initially, the *State* of the FortiAP unit is *Offline*. Periodically select *Refresh* to update the status. Within about two minutes, the state changes to *Online*.

Figure 12: FortiWiFi unit as root mesh with FortiAP unit as branch/leaf node



Viewing the status of the mesh network

Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* to view the list of APs. The *Connected Via* field shows *Mesh* for mesh-connected units and lists the IP address to which they connect.

In the FortiAP CLI, you can check the `main ip` field in the output from the command

```
cw_diag -c mesh
```

Configuring a point-to-point bridge

You can create a point-to-point bridge to connect two wired network segments using a WiFi link. The effect is the same as connecting the two network segments to the same wired switch.

You need to:

- Configure a backhaul link and root mesh AP as described in "Configuring a meshed WiFi network" on page 56. **Note:** The root mesh AP for a point-to-point bridge must be a FortiAP unit, not the internal AP of a FortiWiFi unit.
- Configure bridging on the leaf AP unit.

To configure the leaf AP unit for bridged operation - FortiAP web-based manager

1. With your browser, connect to the FortiAP unit web-based manager.

   You can temporarily connect to the unit's Ethernet port and use its default address: 192.168.1.2.

2. Enter:

Operation Mode	Mesh
Mesh AP SSID	fortinet-ap
Mesh AP Password	fortinet
Ethernet Bridge	Select

3. Select *Apply*.
4. Connect the local wired network to the Ethernet port on the FortiAP unit.

   Users are assigned IP addresses from the DHCP server on the wired network connected to the root mesh AP unit.

To configure a FortiAP unit as a leaf AP - FortiAP CLI

```
cfg -a MESH_AP_SSID=fortinet-ap
cfg -a MESH_AP_PASSWD=fortinet
cfg -a MESH_ETH_BRIDGE=1
cfg -a MESH_AP_TYPE=1
cfg -c
```

WiFi-Ethernet Bridge Operation

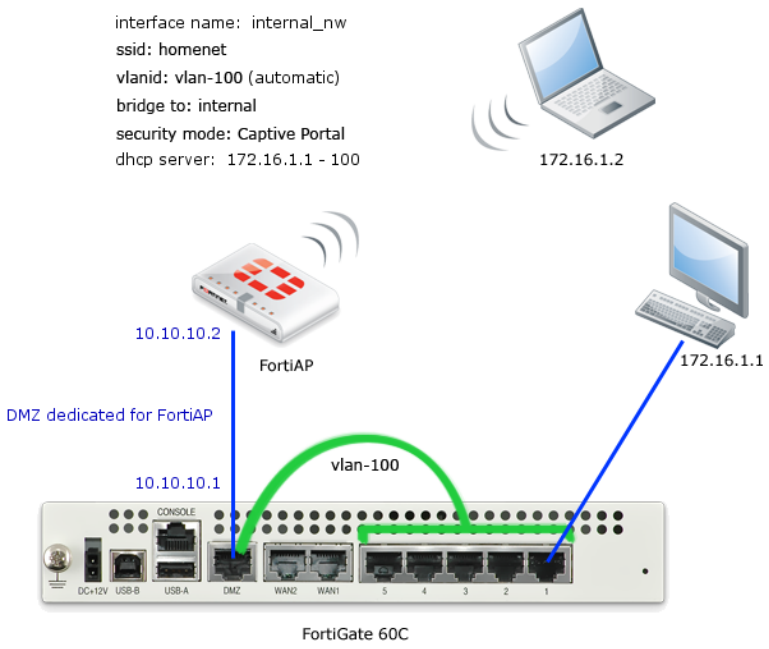
The following topics are included in this section:

- Bridge SSID to FortiGate wired network
- FortiAP local bridging (Private Cloud-Managed AP)
- Using bridged FortiAPs to increase scalability

Bridge SSID to FortiGate wired network

A WiFi network can be combined with a wired LAN so that WiFi and wired clients are on the same subnet. This is a convenient configuration for users.

Figure 13:A FortiAP unit bridged with the internal network



This configuration cannot be used in conjunction with Wireless Mesh features because it enables the FortiAP Local Bridge option.

To create the bridged WiFi and wired LAN configuration, you need to

- Configure the SSID with the Local Bridge option so that traffic is sent directly over the FortiAP unit's Ethernet interface to the FortiGate unit, instead of being tunneled to the WiFi controller.
- Configure a software switch interface on the FortiGate unit with the WiFi and Internal network interfaces as members.
- Configure Captive Portal security for the software switch interface.

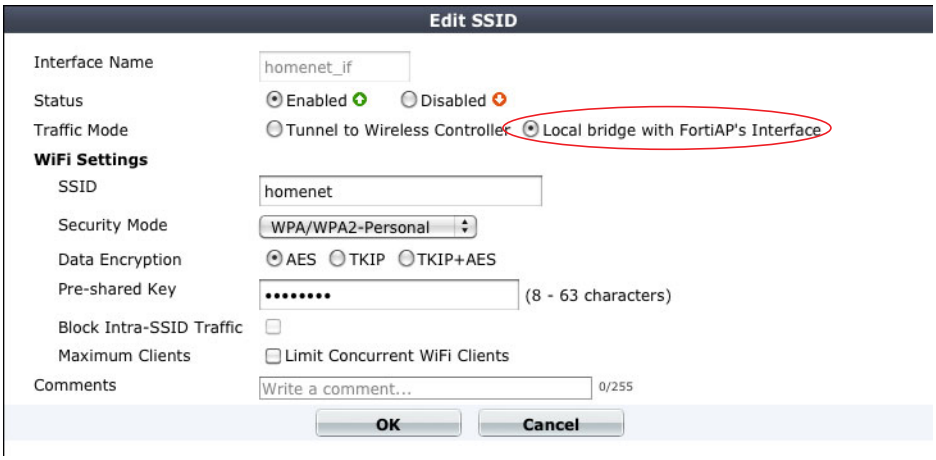
To configure the SSID - web-based manager

1. Go to *WiFi Controller* > *WiFi Network* > *SSID* and select *Create New*.
2. Enter:

Interface name	A name for the new WiFi interface, `homenet_if` for example.
Traffic Mode	Local bridge with FortiAP's Interface
SSID	The SSID visible to users, `homenet` for example.
Security Mode **Data Encryption** **Preshared Key**	Configure security as you would for a regular WiFi network.

3. Select OK.
4. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP,* select the FortiAP unit for editing.
5. Authorize the FortiAP unit.
6. The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

Figure 14:SSID configured with Local Bridge option



To configure the SSID - CLI

This example creates a WiFi interface “homenet_if” with SSID “homenet” using WPA-Personal security, passphrase “Fortinet1”.

```
config wireless-controller vap
  edit "homenet_if"
    set vdom "root"
    set ssid "homenet"
    set local-bridging enable
    set security wpa-personal
    set passphrase "Fortinet1"
  end
config wireless-controller wtp
  edit FAP22B3U11005354
    set admin enable
    set vaps "homenet_if"
  end
```

To configure the FortiGate unit - web-based manager

1. Go to *System* > *Network* > *Interfaces* and select *Create New*.
2. Enter:

Name	A name for the new interface, `homenet_nw` for example.
Type	Software Switch
Interface Members	Move internal and homenet_if into the *Selected Interfaces* list.
Addressing Mode	Select Manual and enter an address, for example `172.16.96.32/255.255.255.0`
Enable DHCP Server	Enable.
Security Mode	Select *Captive Portal*. Add the permitted *User Groups*.

3. Select OK.

To configure the FortiGate unit - CLI

```
config system interface
  edit homenet_nw
    set ip 172.16.96.32 255.255.255.0
    set type switch
    set security-mode captive-portal
    set security-groups "Guest-group"
  end
config system interface
  edit homenet_nw
    set member "homenet_if" "internal"
  end
```

VLAN configuration

If your environment uses VLAN tagging, you assign the SSID to a specific VLAN in the CLI. For example, to assign the homenet_if interface to VLAN 100, enter:

```
config wireless-controller vap
  edit "homenet_if"
    set vlanid 100
  end
```

Additional configuration

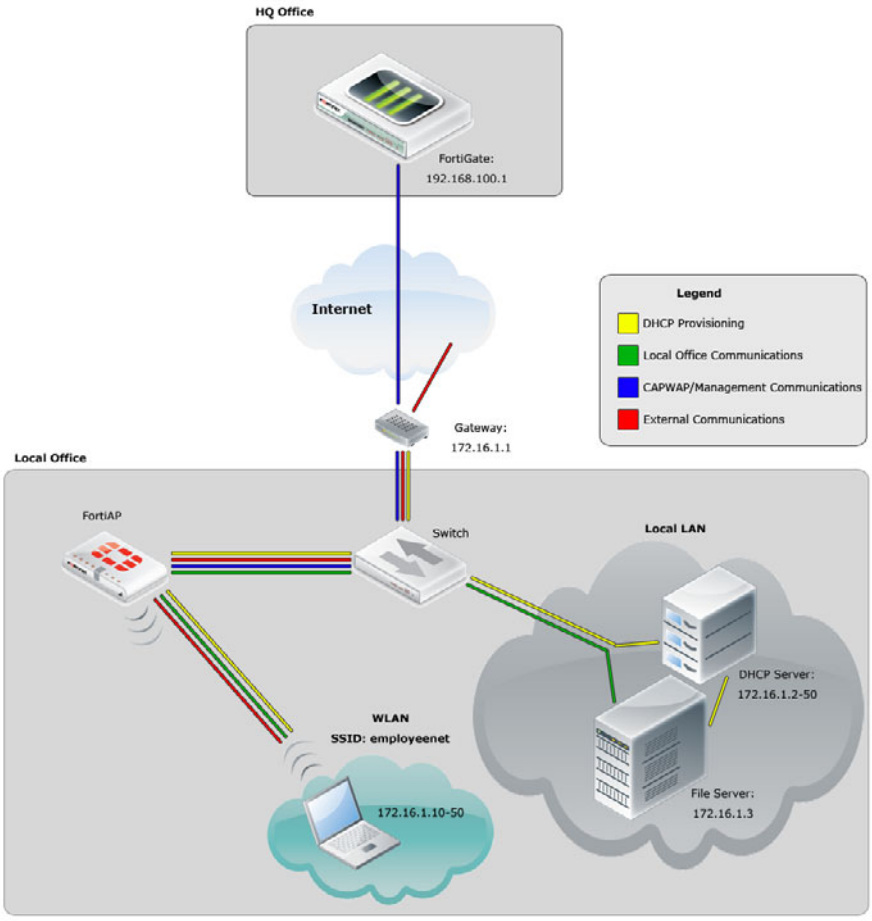
The configuration described above provides communication between WiFi and wired LAN users only. To provide access to other networks, create appropriate firewall policies between the software switch and other interfaces.

FortiAP local bridging (Private Cloud-Managed AP)

A FortiAP unit can provide WiFi access to a LAN, even when the wireless controller is located remotely. This configuration is useful for the following situations:

- Installations where the WiFI controller is remote and most of the traffic is local or uses the local Internet gateway
- Wireless-PCI compliance with remote WiFi controller
- Telecommuting, where the FortiAP unit has the WiFi controller IP address pre-configured and broadcasts the office SSID in the user's home or hotel room. In this case, data is sent in the wireless tunnel across the Internet to the office and you should enable encryption using DTLS.

Figure 15: Remotely-managed FortiAP providing WiFi access to local network



On the remote FortiGate wireless controller, the WiFi SSID is created with the *Bridge with FortiAP Interface* option selected. In this mode, no IP addresses are configured. The FortiAP unit's WiFi and Ethernet interfaces behave as a switch. WiFi client devices obtain IP addresses from the same DHCP server as wired devices on the LAN.

There can be only one Bridge mode SSID per FortiAP unit.

The Local Bridge feature cannot be used in conjunction with Wireless Mesh features.

Block-Intra-SSID Traffic is not available in Bridge mode.

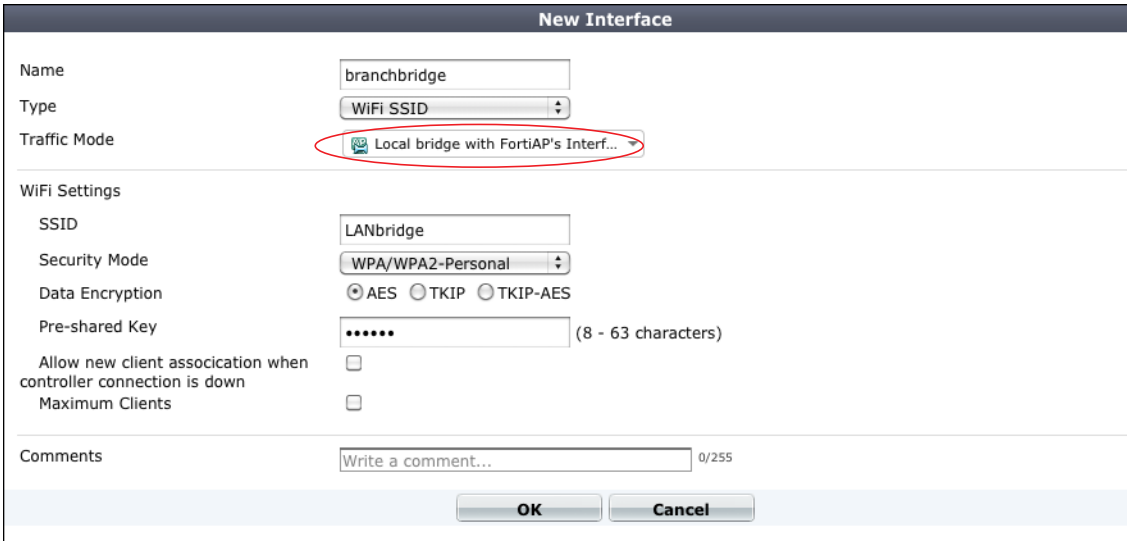
To configure a FortiAP local bridge - web-based manager

1. Go to *WiFi Controller* > *WiFi Network* > *SSID* and select *Create New*.
2. Enter:

Interface name	A name for the new WiFi interface.
Traffic Mode	Local bridge with FortiAP's Interface
SSID	The SSID visible to users.
Security Mode **Data Encryption** **Preshared Key**	Configure security as you would for a regular WiFi network.

3. Select *OK*.
4. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP,* select the FortiAP unit for editing.
5. Authorize the FortiAP unit.
6. The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

Figure 16:SSID configured for Local Bridge operation



To configure a FortiAP local bridge - CLI

This example creates a WiFi interface “branchbridge” with SSID “LANbridge” using WPA-Personal security, passphrase “Fortinet1”.

```
config wireless-controller vap
  edit "branchbridge"
    set vdom "root"
    set ssid "LANbridge"
    set local-bridging enable
    set security wpa-personal
    set passphrase "Fortinet1"
  end
config wireless-controller wtp
  edit FAP22B3U11005354
    set admin enable
    set vaps "branchbridge"
  end
```

Continued FortiAP operation when WiFi controller connection is down

The wireless controller, or the connection to it, might occasionally become unavailable. During such an outage, clients already associated with a bridge mode FortiAP unit continue to have access to the WiFi and wired networks. Optionally, the FortiAP unit can also continue to authenticate users if the SSID meets these conditions:

- *Traffic Mode* is *Local bridge with FortiAP’s Interface*.

  In this mode, the FortiAP unit does not send traffic back to the wireless controller.
- *Security Mode* is either *WPA/WPA2-Personal* or *Open*.

  These modes do not require the user database. In WPA/WPA2-Personal authentication, all clients use the same pre-shared key which is known to the FortiAP unit.
- *Allow new client assocication when controller connection is down* is enabled.

  This field is available only if the other conditions have been met.

The “LANbridge” SSID example would be configured like this in the CLI:

```
config wireless-controller vap
  edit "branchbridge"
    set vdom "root"
    set ssid "LANbridge"
    set local-bridging enable
    set security wpa-personal
    set passphrase "Fortinet1"
    set local-authentication enable
  end
```

Using bridged FortiAPs to increase scalability

The FortiGate wireless controller can support more FortiAP units in local bridge mode than in the normal mode. But this is only true if you configure some of your FortiAP units to operate in remote mode, which supports only local bridge mode SSIDs.

The Managed FortAP page (*WiFi Controller* > *Managed Devices* > *Managed FortiAP*) shows at the top right the current number of Managed FortiAPs and the maximum number that can be managed, “5/64” for example. The maximum number, however, is true only if all FortiAP units operate in remote mode. For more detailed information, consult the *Maximum Values Table.* For each FortiGate model, there are two maximum values for managed FortiAP units: the total number of FortiAPs and the number of FortiAPs that can operate in normal mode.

To configure FortiAP units for remote mode operation

1. Create at least one SSID with *Traffic Mode* set to *Local Bridge*.
2. Create a custom AP profile that includes only local bridge SSIDs.
3. Configure each managed FortiAP unit to use the custom AP profile. You also need to set the FortiAP unit’s `wtp-mode` to `remote`, which is possible only in the CLI. The following example uses the CLI both to set `wtp-mode` and select the custom AP profile:

```
config wireless-controller wtp
  edit FAP22B3U11005354
    set wtp-mode remote
    set wtp-profile 220B_bridge
  end
```

Protecting the WiFi Network

The FortiGate unit provides WiFi-specific network protection. The following topics are included in this section:

Wireless IDS

The FortiGate Wireless Intrusion Detection System (WIDS) monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected the FortiGate unit records a log message.

You can create a WIDS profile to enable the types of intrusion detection:

- Asleap Attack—ASLEAP is a tool used to perform attacks against LEAP authentication.
- Association Frame Flooding—A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
- Authentication Frame Flooding—A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
- Broadcasting De-authentication—This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-athenticate, then re-authenticate with their AP.
- EAPOL Packet Flooding—Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets are detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-Start, EAPOL-SUCC.
- Invalid MAC OUI—Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
- Long Duration Attack—To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
- Null SSID Probe Response—When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
- Spoofed De-authentication—Spoofed de-authentication frames form the basis for most denial of service attacks.
- Weak WEP IV Detection—A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
- Wireless Bridge—WiFi frames with both the fromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

You can enable wireless IDS by going to *WiFi Controller* > *WiFi Network* > *Custom AP Profile* and editing an access point profile. Inside the profile set *WIDS Profile* to the name of a wireless IDS profile to apply wireless IDS protection to the access points that uses the profile.

To create a WIDS Profile

1. Go to *WiFi Controller* > *WiFi Network* > *WIDS Profile*.
2. Select a profile to edit or select *Create New*.
3. Select the types of intrusion to protect against.

   By default, all types are selected.
4. Select *Apply*.

You can also configure a WIDS profile in the CLI using the `config wireless-controller wids-profile` command.

WiFi data channel encryption

Optionally, you can apply DTLS encryption to the data channel between the wireless controller and FortiAP units. This enhances security.

There are data channel encryption settings on both the FortiGate unit and the FortiAP units. At both ends, you can enable Clear Text, DTLS encryption, or both. The settings must agree or the FortiAP unit will not be able to join the WiFi network. By default, both Clear Text and DTLS-encrypted communication are enabled on the FortiAP unit, allowing the FortiGate setting to determine whether data channel encryption is used. If the FortiGate unit also enables both Clear Text and DTLS, Clear Text is used.

Data channel encryption settings are located in the Custom AP profile. If you use Automatic profile, only Clear Text is supported.

Data channel encryption is software-based and can affect performance. Verify that the system meets your performance requirements with encryption enabled.

Configuring encryption on the FortiGate unit

You can use the CLI to configure data channel encryption.

Enabling encryption

In the CLI, the `wireless wtp-profile` command contains a new field, `dtls-policy`, with options `clear-text` and `dtls-enabled`. To enable encryption in profile1 for example, enter:

```
config wireless-controller wtp-profile
  edit profile1
    set dtls-policy dtls-enabled
  end
```

Configuring encryption on the FortiAP unit

The FortiAP unit has its own settings for data channel encryption.

Enabling CAPWAP encryption - FortiAP web-based manager

1 On the *System Information* page, in *WTP Configuration* > *AC Data Channel Security*, select one of:

- Clear Text
- DTLS Enabled
- Clear Text or DTLS Enabled (default)

2 Select *Apply*.

Enabling encryption - FortiAP CLI

You can set the data channel encryption using the AC_DATA_CHAN_SEC variable: 0 is Clear Text, 1 is DTLS Enabled, 2 (the default) is Clear Text or DTLS Enabled.

For example, to set security to DTLS and then save the setting, enter

```
cfg -a AC_DATA_CHAN_SEC=1
cfg -c
```

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

To view connected clients on a FortiWiFi unit

- Go to *WiFi Controller* > *Monitor* > *Client Monitor.*

The following information is displayed:

SSID	The SSID that the client connected to.
FortiAP	The serial number of the FortiAP unit to which the client connected.
User	User name
IP	The IP address assigned to the wireless client.
Device	
Auth	The type of authentication used.
Channel	WiFi radio channel in use.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Signal Strength / Noise	The signal-to-noise ratio in deciBels calculated from signal strength and noise level.
Signal Strength	
Association Time	How long the client has been connected to this access point.

Results can be filtered. Select the filter icon on the column you want to filter. Enter the values to include or select NOT if you want to exclude the specified values.

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.

Rogue AP Settings (*WiFi Controller* > *WiFi Network* > *Rogue AP Settings*) control rogue AP detection for APs that use the Automatic profile. For APs that use a custom AP profile, rogue AP detection settings are contained in the custom AP profile (*WiFi Controller* > *WiFi Network* > *Custom AP Profile*).

It is also possible to suppress rogue APs. See "Suppressing rogue APs" on page 76.

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.

```
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

All APs using the Automatic profile share the same rogue scanning settings. APs using a custom AP profile follow the settings in the custom profile.

To enable rogue AP scanning for the automatic AP profile

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 for the automatic AP profile - CLI

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

To configure rogue AP scanning in a custom AP profile

1. Go to *WiFi Controller* > *WiFi Network* > *Custom AP Profiles*.

   On some models, the menu is *WiFi & Switch Controller*.
2. Select an existing AP profile and edit it, or select *Create New*.
3. For each radio, select either *Access Point* or *Dedicated Monitor*, as required.
4. If you selected *Access Point*, enable *Background Scan*.
5. Select *Rogue AP On-Wire Scan.*

6. If needed, modify other settings.
7. Select *OK*.

To enable the rogue AP scanning feature in a custom AP profile - CLI

```
config wireless-controller wtp-profile
  edit FAP220B-default
    config radio-1
      set mode ap
      set ap-bgscan enable
      set rogue-scan enable
```

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
```

MAC adjacency

You can adjust the maximum WiFi to Ethernet MAC difference used when determining whether an suspect AP is a rogue.

To adjust MAC adjacency

For example, to change the adjacency to 8, enter

```
config wireless-controller global
  set rogue-scan-mac-adjacency 8
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.

Information Columns	
Actual columns displayed depends on *Column Settings*.	
State	 Rogue AP — Use this status for unauthorized APs that *On-wire* status indicates are attached to your wired networks.  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. To see accepted APs in the list, select *Show Accepted*.  Unclassified — 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.
Online Status	 Active AP  Inactive AP  Active ad-hoc WiFi device  Inactive ad-hoc WiFi device
SSID	The wireless service set identifier (SSID) or network name for the wireless interface.
Security Type	The type of security currently being used.
Channel	The wireless radio channel that the access point uses.
MAC Address	The MAC address of the Wireless interface.
Vendor Info	The name of the vendor.
Signal Strength	The relative signal strength of the AP. Mouse over the symbol to view the signal-to-noise ratio.
Detected By	The name or serial number of the AP unit that detected the signal.
On-wire	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.
First Seen	How long ago this AP was first detected.
Last Seen	How long ago this AP was last detected.
Rate	Data rate in bps.

To change the Online Status of an AP, right-click it and select Mark Accepted or Mark Rogue.

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 72. 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*.

Monitoring wireless network health

The Wireless Health Dashboard provides a comprehensive view of the health of your network's wireless infrastructure. The dashboard includes widgets to display

- AP Status - Active, Down or missing, up for over 24 hours, rebooted in past 24 hours
- Client Count Over TIme - viewable for past hour, day, or 30 days
- Top Client Count Per-AP - separate widgets for 2.4GHz and 5GHz bands
- Top Wireless Interference - separate widgets for 2.4GHz and 5GHz bands
- Login Failures Information

To view the Wireless Health dashboard, go to *WiFi Controller* > *Monitor* > *Wireless Health*.

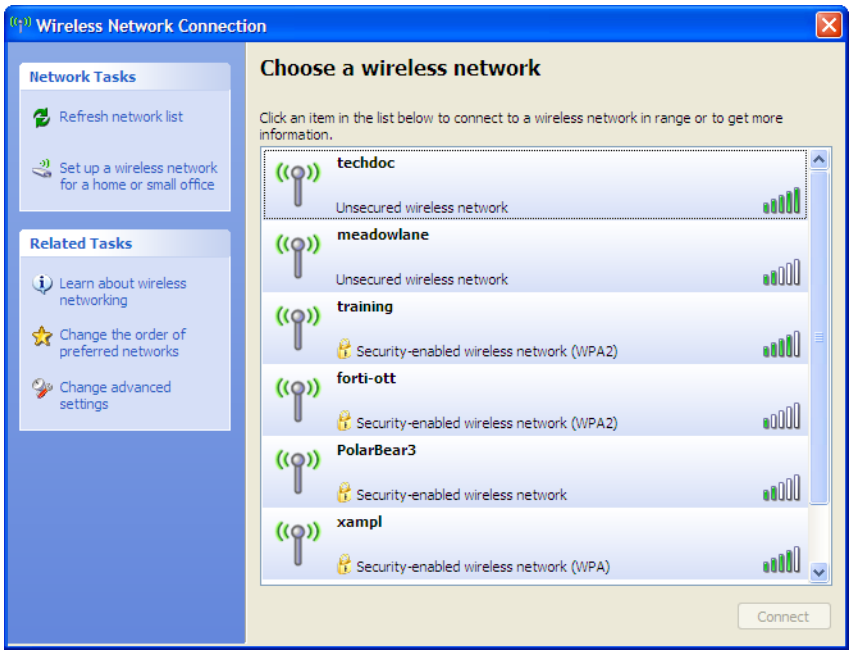
Configuring wireless network clients

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

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.

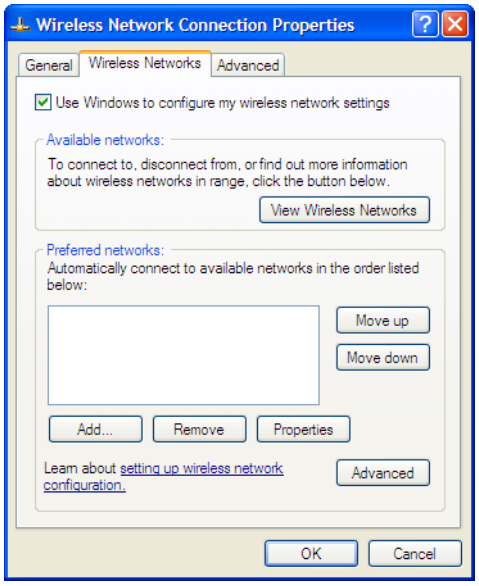


   If you are already connected to another wireless network, the Connection Status window displays. Select *View Wireless Networks* on the *General* tab to view the list.

   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.

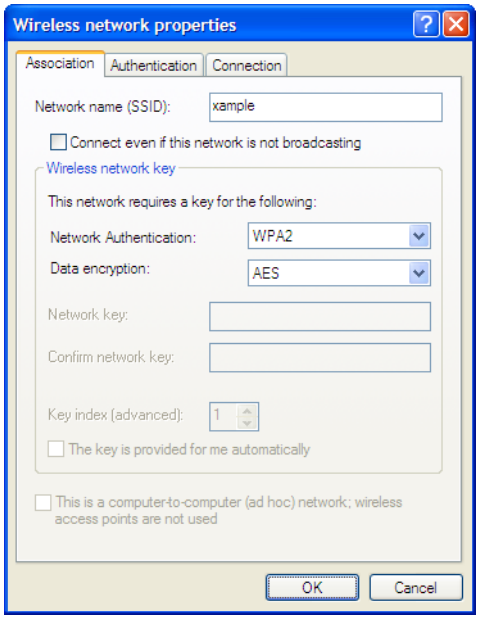
2. You can configure the WPA-Enterprise network to be accessible from the *View Wireless Networks* window even if it does not broadcast its SSID.

3. Select *Change Advanced Settings* and then select the *Wireless Networks* tab.



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

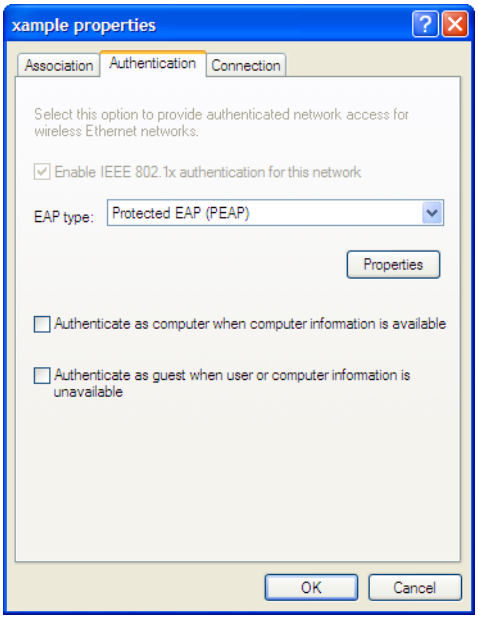
4. Select *Add* and enter the following information:



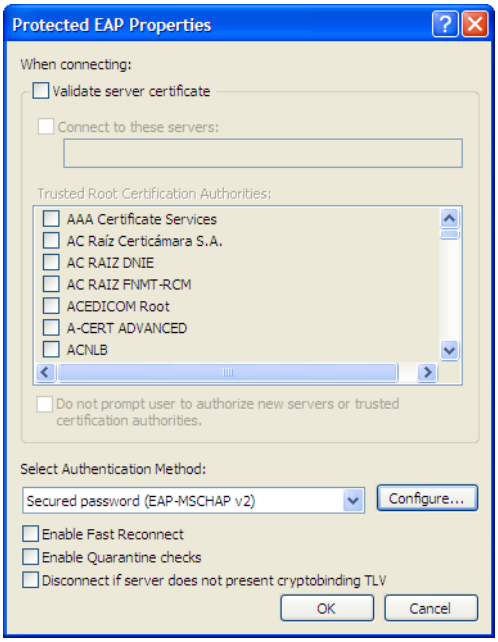
Network Name (SSID)	The SSID for your wireless network
Network Authentication	WPA2
Data Encryption	AES

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.

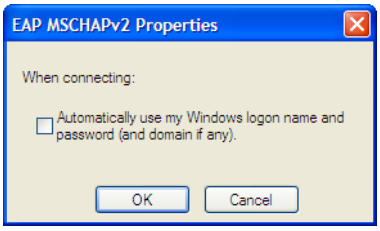


7. In *EAP Type*, select *Protected EAP (PEAP)*.
8. Make sure that the other two authentication options are not selected.
9. Select *Properties*.



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*.

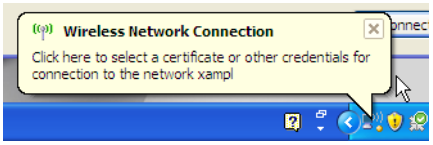


15. If your wireless network credentials are the same as your Windows logon credentials, select *Automatically use my Windows logon name and password*. Otherwise, make sure that this option is not selected.
16. Select OK. Repeat until you have closed all of the *Wireless Network Connection Properties* 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.

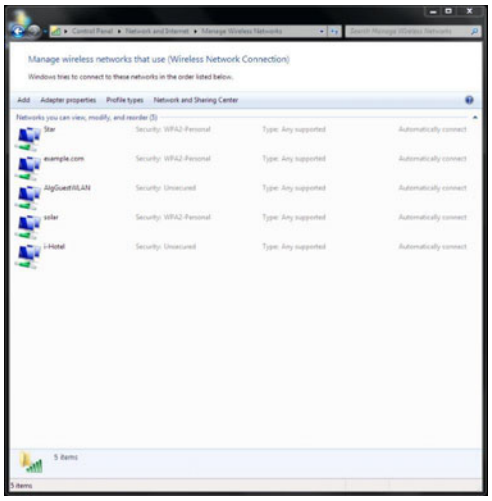


4. In the *Enter Credentials* window, enter your wireless network *User name*, *Password*, and *Logon domain* (if applicable). Then, select *OK*.

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.



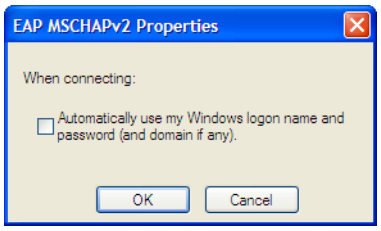
2. Do one of the following:
   - If the wireless network is listed (it broadcasts its SSID), select it from the list.
   - Select *Add* > *Manually create a network profile*.
3. Enter the following information and select *Next*.

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*.

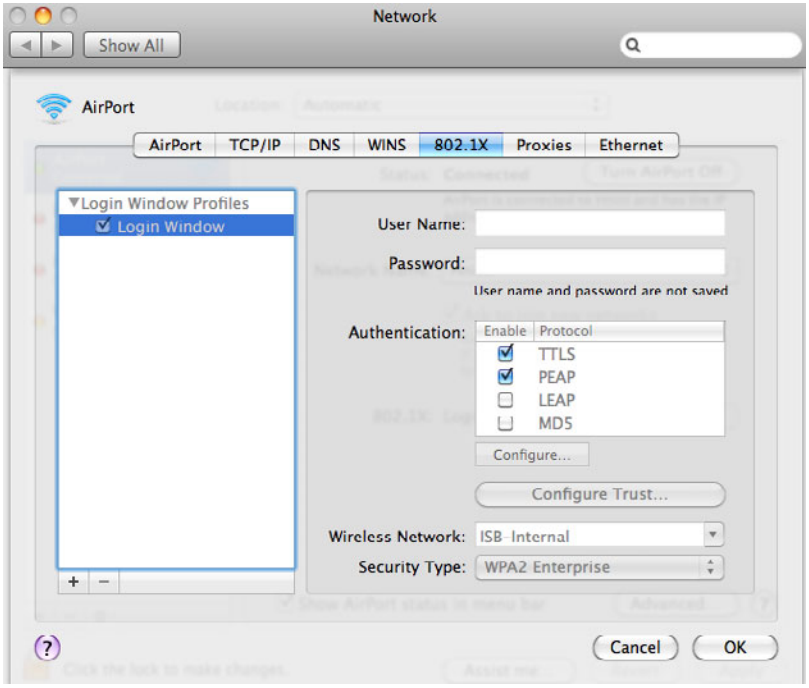


12. If your wireless network credentials are the same as your Windows logon credentials, select *Automatically use my Windows logon name and password*. Otherwise, make sure that this option is not selected.
13. Ensure that the remaining options are not selected.
14. Select OK. Repeat until you have closed 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.



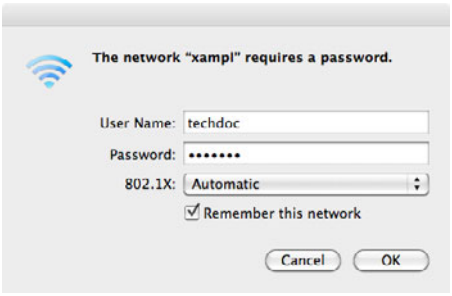
3. If there are no Login Window Profiles in the left column, select the + button and then select *Add Login Window Profile*.

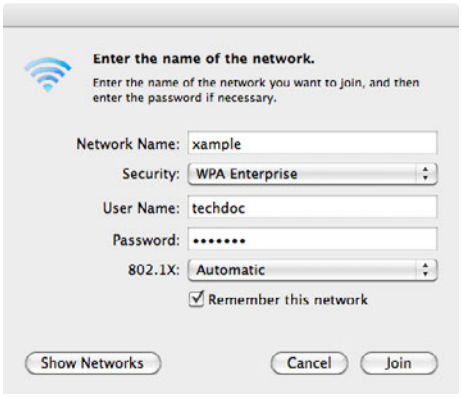
4. Select the Login Window Profile and then make sure that both TTLS and PEAP are selected in *Authentication*.

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*:

Network name	Enter the SSID of your wireless network. (Other network only)
Wireless Security	WPA Enterprise
802.1X	Automatic
Username **Password**	Enter your logon credentials for the wireless network.
Remember this network	Select.

You are connected to the wireless network.

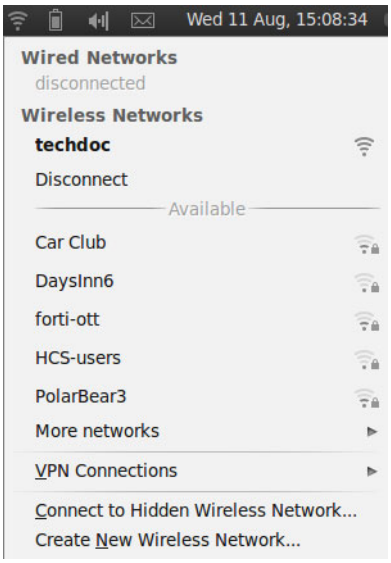
Mac OS supports only PEAP with MSCHAPv2 authentication and therefore can authenticate only to a RADIUS server, not an LDAP or TACACS+ server.

Linux client

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

To connect to a WPA-Enterprise network

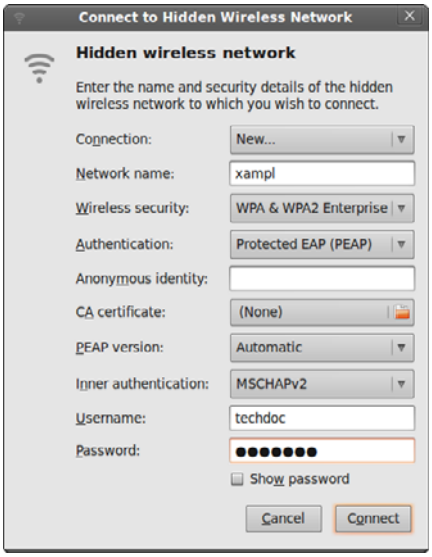
1. Select the Network Manager icon to view the Wireless Networks menu.



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:

Connection	Leave as *New*. (Hidden network only)
Network name	Enter the SSID of your wireless network. (Hidden network only)
Wireless Security	WPA & WPA2 Enterprise
Authentication	Protected EAP (PEAP) for RADIUS-based authentication Tunneled TLS for TACACS+ or LDAP-based authentication
Anonymous identity	This is not required.
CA Certificate	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/.
PEAP version	Automatic (applies only to PEAP)
Inner authentication	MSCHAPv2 for RADIUS-based authentication PAP or CHAP for TACACS+ or LDAP-based authentication
Username **Password**	Enter your logon credentials for the wireless network.

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.

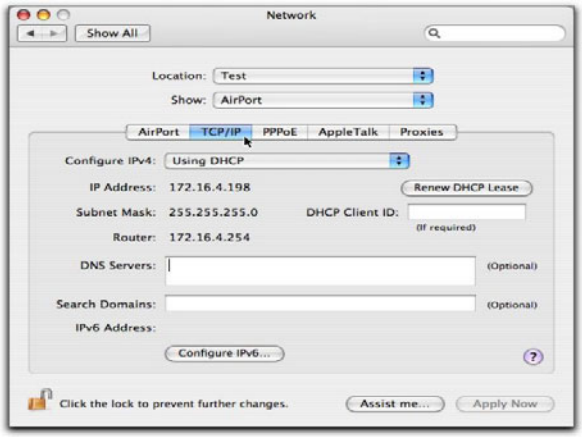
   Check that the *Address Type* is *Assigned by DHCP*. Check that the *IP Address*, *Subnet Mask*, and *Default Gateway* values are valid.
3. Select *Details* to view the DNS server addresses.

   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:

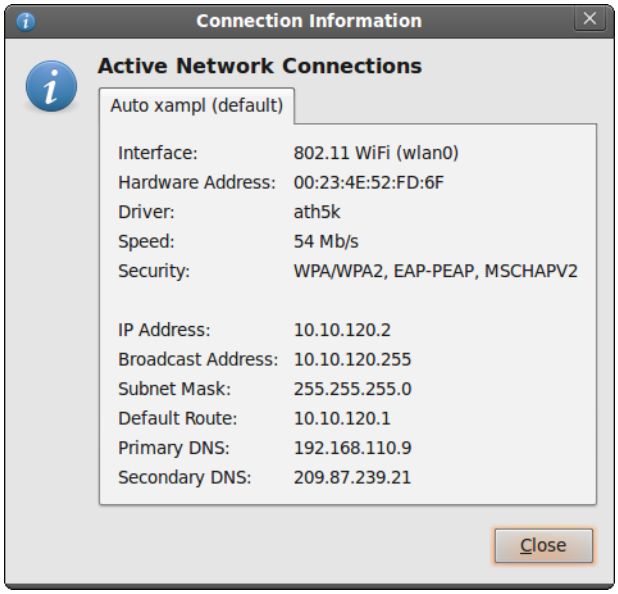
   `cat /etc/resolv.conf`

   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

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 & Device* > *User* > *User Definition* 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 & Device* > *User* > *User Group* and select *Create New*.
2. Enter the following information and then select OK:

Name	wlan_users
Type	*Firewall*
Available Users/ Members	Move users to the *Members* list.

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

```
config user user
  edit "user01"
    set type password
    set passwd "asdf12ghjk"
  end
config user group
  edit "wlan_users"
    set member "user01"
  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:

Name	example_wifi
IP/Netmask	10.10.110.1/24
Administrative Access	Ping (to assist with testing)
SSID	example_wifi
Enable DHCP Server	Enable
Address Range	10.10.110.2 - 10.10.110.199
Netmask	255.255.255.0
Default Gateway	Same As Interface IP
DNS Server	Same as System DNS
Security Mode	WPA/WPA2-Enterprise
Data Encryption	AES
Authentication	Usergroup, select *wlan_users*.
Leave other settings at their default values.	

To configure the SSID - CLI

```
config wireless-controller vap
  edit example_wifi
    set ssid "example_wifi"
    set broadcast-ssid enable
    set security wpa-enterprise
    set auth usergroup
    set 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* > *Addresses*.
2. Select *Create New*, enter the following information and select *OK*.

Address Name	wlan_user_net
Type	Subnet / IP Range
Subnet / IP Range	10.10.110.0/24
Interface	example_wifi

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*:

Incoming Interface	example_wifi
Source Address	wlan_user_net
Outgoing Interface	port1
Destination Address	All
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Selected. Select *Use Destination Interface Address* (default).
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 schedule always
    set service 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* > *Interfaces* and edit the port3 interface.
2. Set the *Addressing mode* to *Dedicate to FortiAP* and set the *IP/Network Mask* to `192.168.8.1/255.255.255.0`.
3. Select *OK*.

This procedure automatically configures a DHCP server for the AP units. You can see this configuration in *System* > *Network* > *DHCP Server*.

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 exclude-range
      edit 1
        set end-ip 192.168.8.1
        set start-ip 192.168.8.1
      end
    config ip-range
      edit 1
        set end-ip 192.168.8.254
        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 & Device* > *User* > *User Group* and select *Create New*.
2. Enter the following information and then select OK:

Name	employee-group
Type	*Firewall*
Available Users **Members**	Move appropriate user accounts to the *Members* list.

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 & Device* > *Authentication* > *RADIUS Server* and select *Create New*.
2. Enter the following information and select OK:

Name	guestRADIUS
Primary Server Name / IP	10.11.102.100
Primary Server Secret	grikfwpfdfg
Secondary Server Name / IP	Optional
Secondary Server Secret	Optional
Authentication Scheme	Use default, unless server requires otherwise.
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 & Device* > *User* > *User Group* and select *Create New*.
2. Enter the following information and then select OK:

Name	guest-group
Type	*Firewall*
Available Users / Members	Move *guestRADIUS* to the *Members* list.
Match one of these group names	Select Add and fill in the following fields:
Remote Server	Select *guestRADIUS*.
Group Name	Enter `wireless`

3. Select *Add*.
4. Enter

Remote Server	Select *guestRADIUS*.
Group Name	Select *Specify* and then enter `wireless`

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:

Interface Name	example_inc
IP/Netmask	10.10.120.1/24
Administrative Access	Ping (to assist with testing)
SSID	example_inc
Enable DHCP	Enable
Address Range	10.10.120.2 - 10.10.120.199
Netmask	255.255.255.0
Default Gateway	Same As Interface IP
DNS Server	Same as System DNS
Security Mode	WPA/WPA2-Enterprise
Data Encryption	AES
Authentication	Select *Usergroup*, then select *employee-group.*
Leave other settings at their default values.	

To configure the employee SSID - CLI

```
config wireless-controller vap
  edit example_inc
    set ssid "example_inc"
    set security wpa-enterprise
    set auth usergroup
    set usergroup employee-group
  end
config system interface
  edit example_inc
    set ip 10.10.120.1 255.255.255.0
  end
config 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:

Name	example_guest
IP/Netmask	10.10.115.1/24
Administrative Access	Ping (to assist with testing)
SSID	example_guest
Enable DHCP	Enable
Address Range	10.10.115.2 - 10.10.115.50
Netmask	255.255.255.0
Default Gateway	Same as Interface IP
DNS Server	Same as System DNS
Security Mode	Captive Portal
Customize Portal Messages	Select
User Groups	Select *guest-group*
Leave other settings at their default values.	

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 10.10.115.50
        set start-ip 10.10.115.2
      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:

Name	example_AP
Platform	FAP220A
Radio 1	
Mode	Access Point
Background Scan	Enable
Rogue AP On-wire Scan	Enabled
Radio Resource Provision	Not enabled
Band	802.11n
Short Guard Interval	Not enabled
Channel	Select 1, 6, and 11.
Tx Power	100%
SSID	Select *example_inc* and *example_guest*.
Radio 2	
Mode	Access Point
Background Scan	Enable
Rogue AP On-wire Scan	Enabled
Radio Resource Provision	Enabled
Band	802.11n_5G

Short Guard Interval	Not enabled
20/40 MHz Channel Width	Not enabled
Channel	Select all.
Tx Power	100%
SSID	Select *example_inc*.

To configure the AP Profile - CLI

```
config wireless-controller wtp-profile
  edit "example_AP"
    config platform
      set type 220A
    end
    config radio-1
      set ap-bgscan enable
      set band 802.11n
      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* > *Addresses*.
2. Select *Create New*, enter the following information and select *OK*.

Address Name	employee-wifi-net
Type	Subnet / IP Range
Subnet / IP Range	10.10.120.0/24
Interface	example_inc

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

Address Name	guest-wifi-net
Type	Subnet / IP Range
Subnet / IP Range	10.10.115.0/24
Interface	example_guest

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:

Source Interface/Zone	example_inc
Source Address	employee-wifi-net
Destination Interface/Zone	port1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable NAT

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 provides access to the ExampleCo private network.

To create firewall policies for employee WiFi users - CLI

```
config 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:

Source Interface/Zone	example_guest
Source Address	guest-wifi-net
Destination Interface/Zone	port1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable NAT

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

```
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* > *Interfaces* 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

```
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-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:

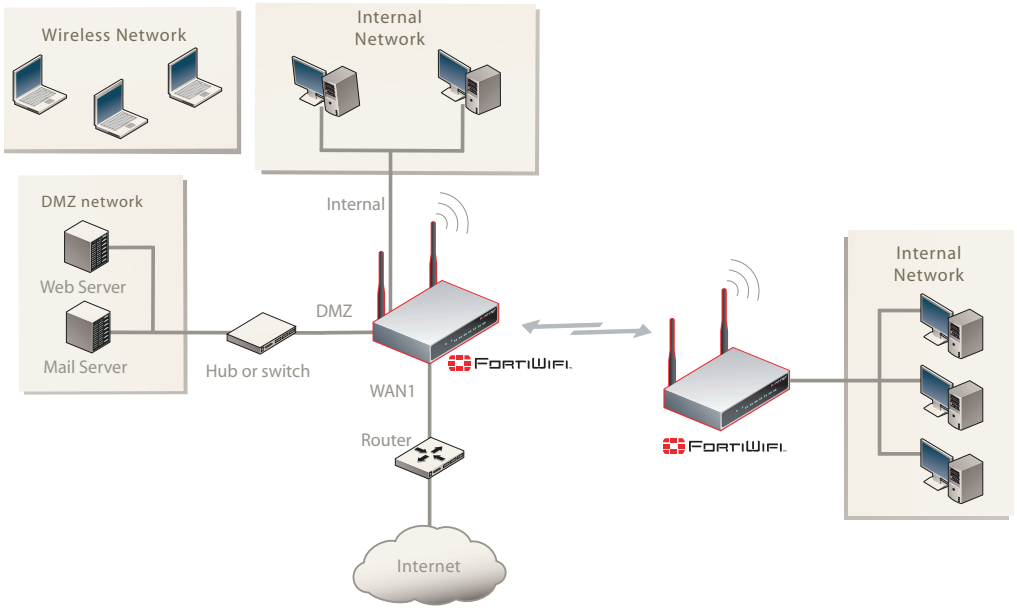
Use of client mode

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 17: 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. Configure the WiFi interface 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 wifi
       set mode dhcp
       config wifi-networks
         edit 0
           set wifi-ssid our_wifi
           set wifi-security wpa-personal
           set wifi-passphrase "justforus"
         end
   end
   ```

   The WiFi interface client_wifi will receive an IP address using DHCP.

3. Configure a wifi to port1 policy.

   You can use either CLI or web-based manager to do this. The important settings are:

Incoming Interface (srcintf)	wifi
Source Address (srcaddr)	all
Outgoing Interface (dstintf)	port1
Destination Address (dstaddr)	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Selected

Support for location-based services

FortiOS supports location-based services by collecting information about WiFi devices near FortiGate-managed access points, even if the devices don't associate with the network.

The following topics are included in this section:

Overview

WiFi devices broadcast packets as they search for available networks. The FortiGate WiFi controller can collect information about the interval, duration, and signal strength of these packets. The Euclid Analytics service uses this information to track the movements of the device owner. A typical application of this technology is to analyze shopper behavior in a shopping center. Which stores do people walk past? Which window displays do they stop to look at? Which stores do they enter and how long do they spend there? The shoppers are not personally identified, each is known only by the MAC address of their WiFi device.

After enabling location tracking on the FortiGate unit, you can confirm that the feature is working by using a specialized diagnostic command to view the raw tracking data. The Euclid Analytics service obtains the same data in its proprietary format using a JSON inquiry through the FortiGate unit's web-based manager interface.

Configuring location tracking

You can enable location tracking in any custom AP profile, using the CLI. For each radio, set the `station-locate` field to `enable`. For example:

```
config wireless-controller wtp-profile
  edit "FAP220B-locate"
    set ap-country US
    config platform
      set type 220B
    end
    config radio-1
      set station-locate enable
    end
    config radio-2
      set station-locate enable
    end
  end
```

Viewing device location data on the FortiGate unit

You can use the FortiGate CLI to list located devices. This is mainly useful to confirm that the location data feature is working, You can also reset device location data.

To list located devices

```
diag wireless-controller wlac -c sta-locate
```

To reset device location data

```
diag wireless-controller wlac -c sta-locate-reset
```

Example output

The following output shows data for three WiFi devices.

```
FWF60C3G11004319 # diagnose wireless-controller wlac -c sta-locate
sta_mac               vfid  rid base_mac          freq_lst  frm_cnt
     frm_fst frm_last     intv_sum    intv2_sum    intv3_sum intv_min
     intv_max   signal_sum  signal2_sum  signal3_sum  sig_min  sig_max
     sig_fst sig_last   ap
00:0b:6b:22:82:61       0
 FAP22B3U11005354       0    0 00:09:0f:f1:bb:e4     5745      257
     708      56         651        1836        6441       0      12
     -21832     1855438   -157758796     -88     -81     -84     -88
     0
00:db:df:24:1a:67       0
 FAP22B3U11005354       0    0 00:09:0f:f1:bb:e4     5745       42
     1666      41       1625       97210     5831613       0      60
     -3608       310072    -26658680     -90     -83     -85     -89
     0
10:68:3f:50:22:29       0
 FAP22B3U11005354       0    0 00:09:0f:f1:bb:e4     5745      102
     1623      58       1565       94136     5664566       0      60
     -8025       631703    -49751433     -84     -75     -78     -79
     0
```

The output for each device appears on two lines. The first line contains only the device MAC address and the VLAN ID. The second line begins with the ID (serial number) of the FortiWiFi or FortiAP unit that detected the device, the AP's MAC address, and then the fields that the Euclid service uses. Because of its length, this line wraps around and displays as multiple lines.

Reference

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

- Wireless radio channels
- FortiAP CLI

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

Channel number	Frequency (MHz)	Regulatory Areas				
		Americas	Europe	Taiwan	Singapore	Japan
34	5170					•
36	5180	•	•		•	
38	5190					
40	5200	•	•		•	•
42	5210					
44	5220	•	•		•	•
46	5230					
48	5240	•	•		•	•
149	5745	•		•	•	
153	5765	•		•	•	
157	5785	•		•	•	
161	5805	•		•	•	
165	5825	•			•	

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 5: IEEE 802.11b/g/n (2.4-GHz Band) channel numbers

Channel number	Frequency (MHz)	Regulatory Areas			
		Americas	EMEA	Israel	Japan
1	2412	•	•	•?	•
2	2417	•	•	•?	•
3	2422	•	•	•?	•
4	2427	•	•	•	•
5	2432	•	•	•	•
6	2437	•	•	•	•
7	2442	•	•	•	•
8	2447	•	•	•	•
9	2452	•	•	•	•
10	2457	•	•	•	•
11	2462	•	•	•?	•
12	2467		•	•?	•
13	2472		•	•?	•
14	2484				b only

FortiAP CLI

The FortiAP CLI now includes more configuration commands and a complete set of diagnose commands.

Configuration commands include the following

`cfg -h`	Display help for all commands.
`cfg -r var`	Remove variables.
`cfg -e`	Export variables.
`cfg -s`	List variables.
`cfg -x`	Reset to factory defaults.
`cfg -c`	Commit the change to flash.
`cfg -a var=value`	Add or change variables.

Diagnose commands include:

`cw_diag help`	Display help for all diagnose commands.
`cw_diag uptime`	Show daemon uptime.
`cw_diag --tlog <on|off>`	Turn on/off telnet log message.
`cw_diag --clog <on|off>`	Turn on/off console log message.
`cw_diag baudrate [9600 | 19200 | 38400 | 57600 | 115200]`	Set the console baud rate.
`cw_diag plain-ctl [0|1]`	Show or change current plain control setting.
`cw_diag sniff-cfg ip port`	Set sniff server ip and port.
`cw_diag sniff [0|1|2]`	Enable/disable sniff packet.
`cw_diag stats wl_intf`	Show wl_intf status.
`cw_diag admin-timeout [30]`	Set shell idle timeout in minutes.
`cw_diag -c wtp-cfg`	Show current wtp config parameters in control plane.
`cw_diag -c radio-cfg`	Show current radio config parameters in control plane.
`cw_diag -c vap-cfg`	Show current vaps in control plane.
`cw_diag -c ap-rogue`	Show rogue APs pushed by AC for on-wire scan.
`cw_diag -c sta-rogue`	Show rogue STAs pushed by AC for on-wire scan.
`cw_diag -c arp-req`	Show scanned arp requests.
`cw_diag -c ap-scan`	Show scanned APs.

`cw_diag -c sta-scan`	Show scanned STAs.
`cw_diag -c sta-cap`	Show scanned STA capabilities.
`cw_diag -c wids`	Show scanned WIDS detections.
`cw_diag -c darrp`	Show darrp radio channel.
`cw_diag -c mesh`	Show mesh status.
`cw_diag -c mesh-veth-acinfo`	Show mesh veth ac info, and mesh ether type.
`cw_diag -c mesh-veth-vap`	Show mesh veth vap.
`cw_diag -c mesh-veth-host`	Show mesh veth host.
`cw_diag -c mesh-ap`	Show mesh ap candidates.
`cw_diag -c scan-clr-all`	Flush all scanned AP/STA/ARPs.
`cw_diag -c ap-suppress`	Show suppressed APs.
`cw_diag -c sta-deauth`	De-authenticate an STA.

Index

W