



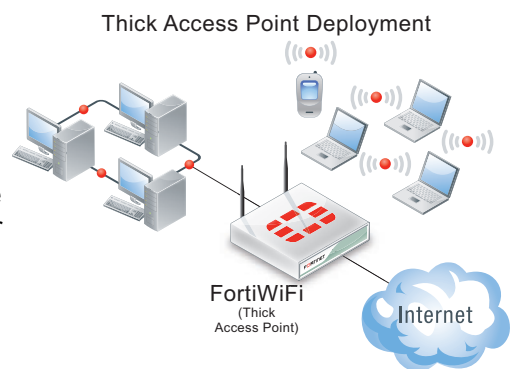
Wireless

An overview of the wireless features and options that are available when using FortiAP, FortiWiFi and FortiGate units in a wireless network

FortiOS WiFi controllers provides a wide range of capabilities for integrating wireless networks into your organization's network architecture. Each WiFi network or SSID is represented by a virtual network interface to which you apply security policies, UTM features, traffic shaping, and so on, in the same way as for wired networks.

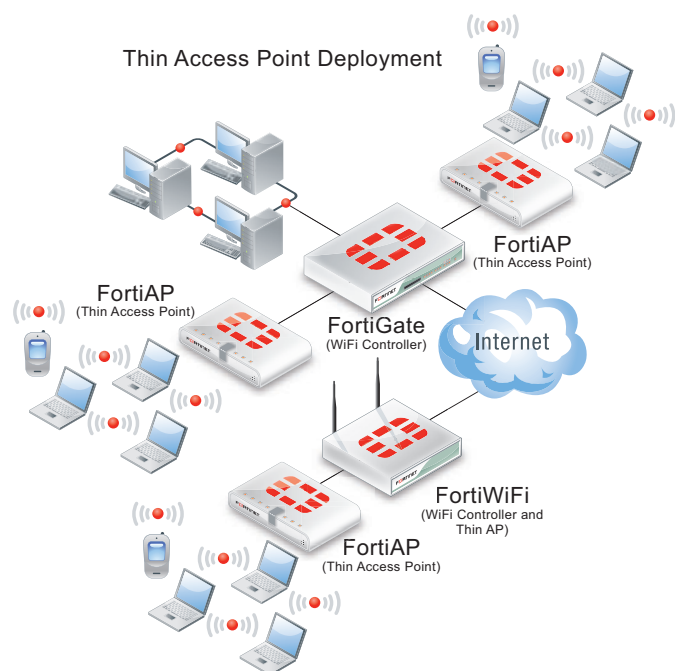
How many networks, how many access points?

You can create multiple WiFi networks to serve different groups of users. For example, you might want one network for your employees and another for guests or customers. Also, with the increase in use of smartphones, tablets and other mobile devices that use WiFi technology, wireless networks are becoming busier than ever and have to accommodate a broad range of wireless client devices each with their own strengths and limitations. You may also want to accommodate these devices and technologies on multiple overlapping wireless networks. These networks could differ greatly in the access they provide to other networks, as well as the authentication, access control, and UTM features they apply.



The number of access points you need depends on the size of the area in which radio coverage is required and the architectural features of the area. You might even need to provide coverage in several different areas, on multiple floors or in multiple buildings. The number of WiFi networks (SSIDs) you need also depends on the need to separate different kinds of users into different networks. An access point, whether a FortiWiFi or a FortiAP unit, can carry up to eight networks per radio. FortiWiFi access points include one WiFi radio. FortiAP access points include one or two WiFi radios, depending on the model. Each radio can carry up to 8 WiFi networks, seven of these can be user WiFi networks and one is reserved for monitoring.

WiFi Equipment Options



A network that requires only one WiFi access point is easily created with a FortiWiFi unit operating as a single thick AP. A thick AP such as a FortiWiFi unit contains the WiFi radio facility as well as access control and authentication functionality.

A thin AP, such as a FortiAP unit contains only the radio facility and a microcontroller that receives commands and exchanges data with a WiFi controller. If you already have a FortiGate unit, adding a FortiAP unit as a thin AP managed by the FortiGate unit operating as a WiFi controller is a cost-effective solution for adding WiFi to your network.

The FortiOS WiFi controller feature is available on both FortiGate and FortiWiFi units. A FortiWiFi unit's WiFi controller also controls the unit's internal (Local WiFi) radio facility, treating it much like a built-in thin AP.

Whenever multiple APs are required, a single FortiGate or FortiWiFi unit controlling multiple FortiAP units is best. A network of multiple thick APs would be more expensive and more complex to manage.

The FortiOS WiFi controller and FortiWiFi and FortiAP units conform to a number of Control And Provisioning of Wireless Access Points (CAPWAP) specifications, including RFC 4118, RFC 4564, RFC 5418, RFC 5417, RFC 5416, and RFC 5415 and support the 802.11 a, b, g, n and other wireless standards.

Deployment Options

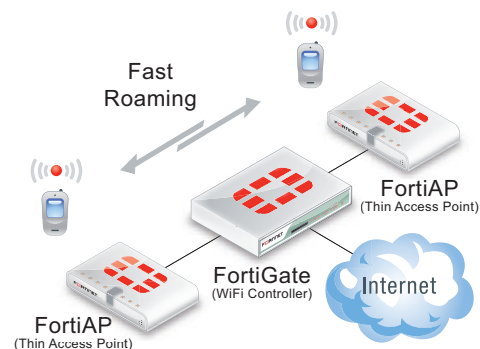
FortiAP units can discover WiFi controllers through several methods: DHCP, broadcast request, and multicast request. They can also be pre-configured with the controller's IP address. These multiple methods ensure that FortiWiFi units can communicate with the WiFi controller even through switches and routers. All such devices must, however, allow traffic on UDP ports 5246 and 5247, used by encrypted CAPWAP tunnels. Where the APs and the WiFi controller are in separate buildings with gateways on the public network, communication can occur over a gateway-to-gateway VPN.

FortiWiFi and FortiAP units provide adjustable power output of up to 17dBm or 50mW for some models and up to 27dBm or 500mW for others. The output can be optimized to meet or exceed the required power levels to close a two-way communication link with the clients on the wireless network. The actual WiFi signal depends on obstructions and interference sources, but in general for indoor deployments with obstructions a FortiWiFi or FortiAP access point can cover a radius of 50-60 feet (18 meters). To provide a signal for a larger area, FortiAP devices can be deployed every 60 feet in a hexagonal or honeycomb pattern.

To determine optimal deployment scenarios Fortinet's FortiPlanner WiFi planning tool can be used to map the buildings and outdoor locations that you want to add WiFi access to. Then using FortiPlanner you can map out optimal locations for FortiWiFi and FortiAP devices and adjust their transmitter power settings to provide optimal WiFi coverage.

Fast Roaming

Mobile device users are very likely to move from one AP's coverage area to another while communicating. After the mobile user authenticates, the FortiOS WiFi controller caches the Pairwise Master Key (PMK) to enable the user to associate quickly with other APs in the network, transferring from one AP to another without interruption. This is done in accordance with 802.11i "fast-associate-in-advance" and "fast-roam-back" features.



Distributed ARRP (Automatic Radio Resource Provisioning)

In a multi-AP network, adjacent APs need to operate on different radio channels so that they do not interfere with each other. Also, to provide the best service, APs should avoid channels with interference from neighboring APs. By enabling multiple channels when you configure managed FortiAPs or their custom profile, you enable the ARRP algorithm. With ARRP enabled, each AP will re-evaluate its choice of channel at configurable time intervals (for example, every 10 minutes) and change channels if needed to optimize WiFi performance.

WiFi Security and User Authentication

WiFi security and user authentication controls the authentication methods used by the WiFi network to identify a WiFi user before granting access and the encryption and privacy methods used to encrypt data sent over the WiFi network. WiFi security and user authentication can be customized for each WiFi network (SSID).

The FortiOS WiFi controller supports standard WPA/WPA2-Personal and WPA/WPA2-Enterprise (802.11i) wireless security modes. Both WPA and WPA2 are supported with AES encryption. TKIP encryption is provided for backward compatibility with WiFi clients that do not support AES encryption.

In addition, FortiOS offers a Captive Portal mode that applies the complete set FortiOS user authentication options available for authenticating wireless users. FortiOS user authentication features include RADIUS, LDAP, TACAS+ remote authentication, Windows AD single sign on authentication, and two-factor authentication using certificates, SMS, email or the FortiToken one-time password generator.

WPA-Enterprise mode can authenticate users with an external RADIUS server (802.1X) or through FortiOS user authentication in which the user must be a member of a specified user group. The captive portal mode uses only FortiOS user authentication, but multiple user groups can be permitted access.

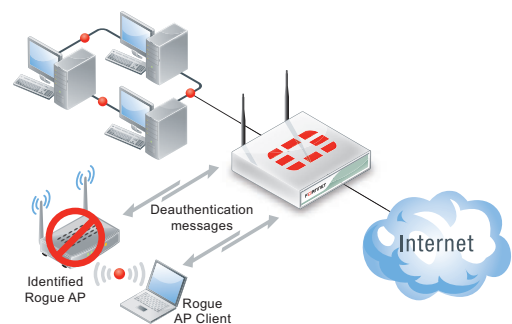
Captive portal security leaves the AP open, allowing any WiFi client to connect. Any HTTP requests are redirected and the user sees a login page. Until the user enters valid credentials, access to anything beyond the portal is not allowed. The messages displayed by the captive portal can be customized, for example to present a disclaimer (usage policy) to which the user must agree before gaining access to the network. Each WiFi network can have its own custom captive portal.

FortiOS WiFi controllers support white listing or black listing WiFi devices based on MAC address. White listed devices can be granted access without the need for further authentication. Black listed devices can be blocked from even being allowed to authenticate. MAC addresses may also be used to build a local authentication database. All devices not on the white or black lists are subject to the authentication required for the WiFi network.

If there is no reason for clients to communicate directly with each other, security can also be enhanced by enabling intra-SSID privacy that blocks individual users from communicating with each other on the same wireless network. This security enhancement prevents “man in the middle” attacks between wireless client devices.

Monitoring Neighbors and Rogues

In almost any WiFi environment, access points other than your own are active. Most of these are neighbors which might cause interference but are not a security threat. Unauthorized APs connected to your networks are rogue APs that can cause leakage of sensitive information to malicious parties. This issue is particularly important if your organization must comply with the Payment Card Industry Data Security Standard (PCI DSS). The FortiOS on-wire detection technique correlates wireless MAC addresses on other APs with those on your wired networks to differentiate neighbors from rogues. FortiOS can generate alert messages to inform system administrators when a rogue AP is identified.



Suppressing Rogues

You can activate suppression against APs that the monitor function has flagged as suspected rogues. When suppression is activated against an AP, the WiFi controller sends deauthentication frames to the rogue and its clients. This stops unwanted communication with the rogue AP until it can be found and removed from the network.

IEEE 802.11e and Application-based QoS

In addition to full support for IEEE 802.11e, FortiOS supports application-based Quality of Service control. Business-critical applications can be given preferential treatment over non-essential applications. Fortinet’s unique approach to Quality of Service by supporting both 802.11e and layer 7 application prioritization and traffic shaping provides significant value to enterprise users.