FORTINET CERTIFIED PROFESSIONAL
Network Security

Secure Wireless LAN Administrator

Study Guide

FortiOS 7.4

FORTINET
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

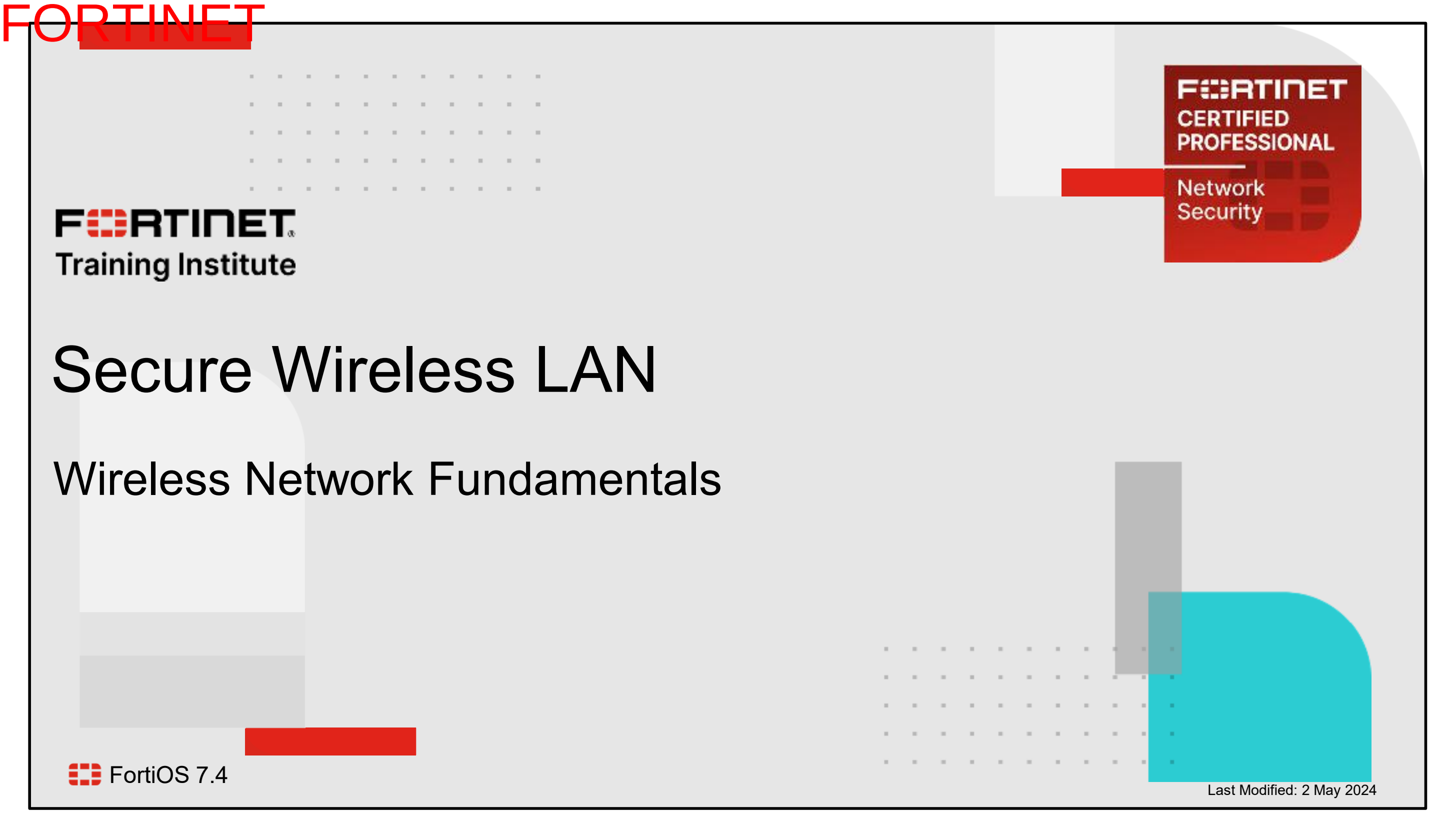
Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

FORTINET®

5/3/2024

TABLE OF CONTENTS



FORTINET CERTIFIED PROFESSIONAL
Network Security

FORTINET
Training Institute

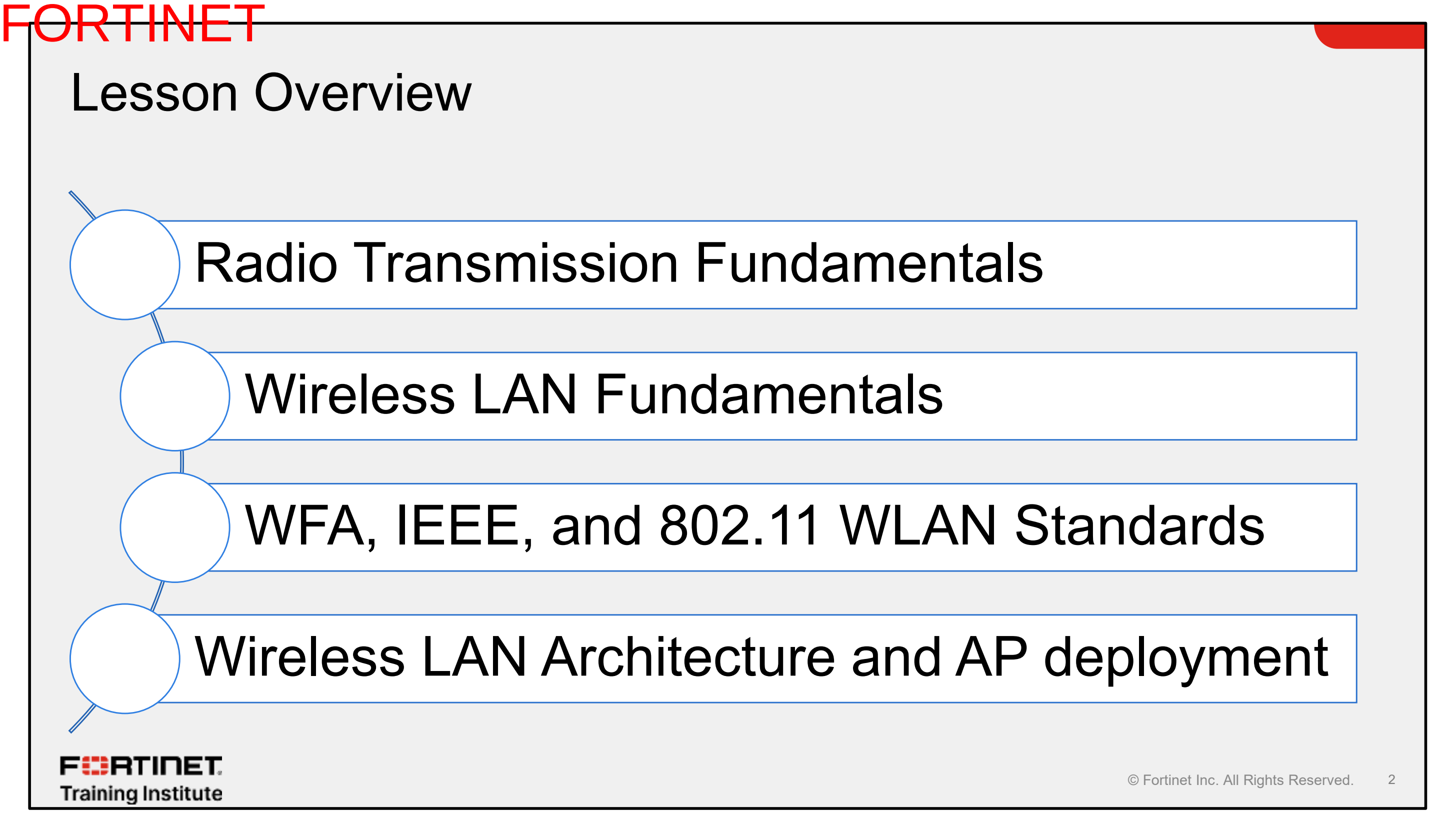
Secure Wireless LAN

Wireless Network Fundamentals

FortiOS 7.4

Last Modified: 2 May 2024

In this lesson, you will learn about wireless technology concepts.



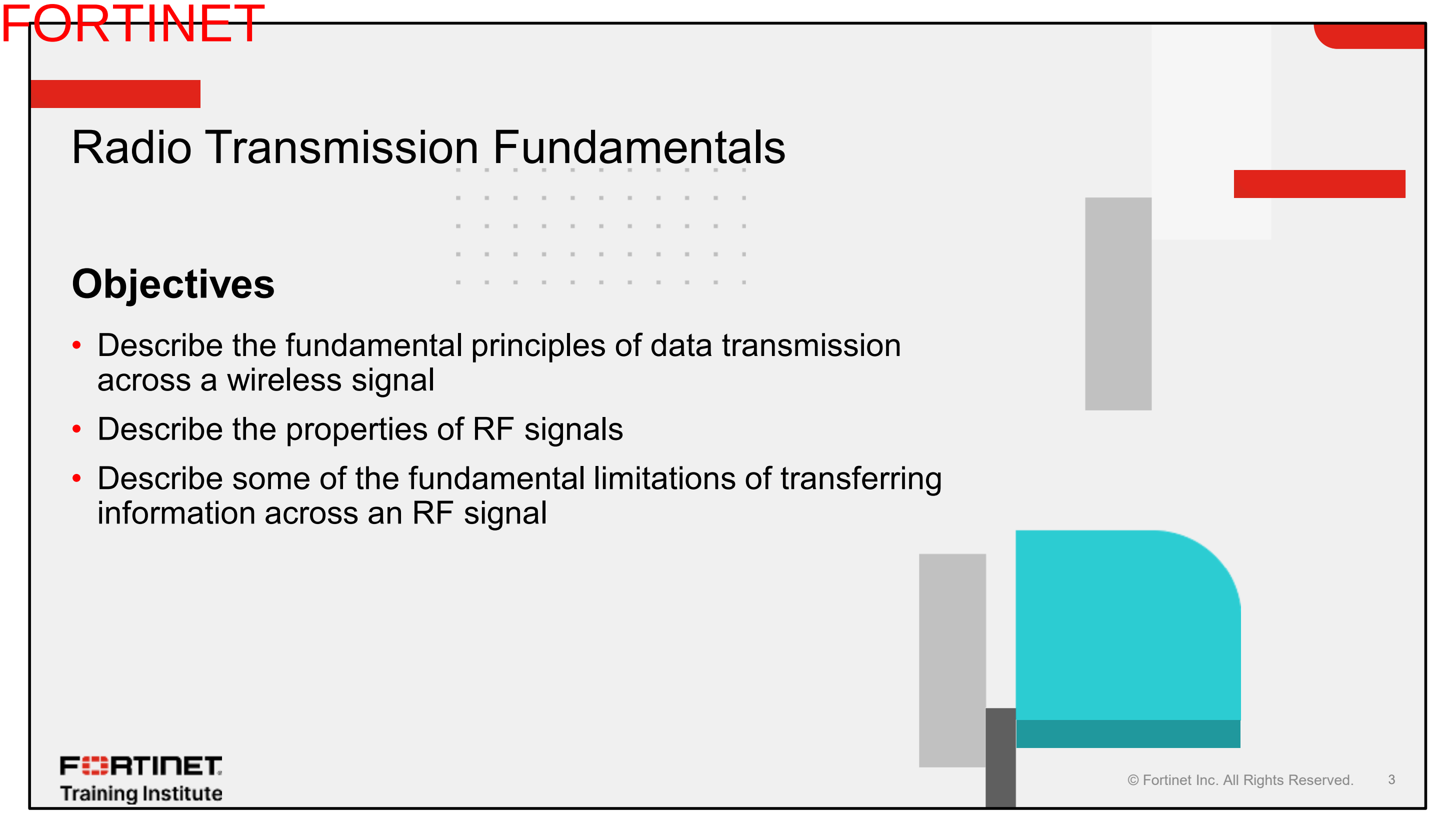
Lesson Overview

- Radio Transmission Fundamentals
- Wireless LAN Fundamentals
- WFA, IEEE, and 802.11 WLAN Standards
- Wireless LAN Architecture and AP deployment

Training Institute

2

In this lesson, you will learn about the topics shown on this slide.



Radio Transmission Fundamentals

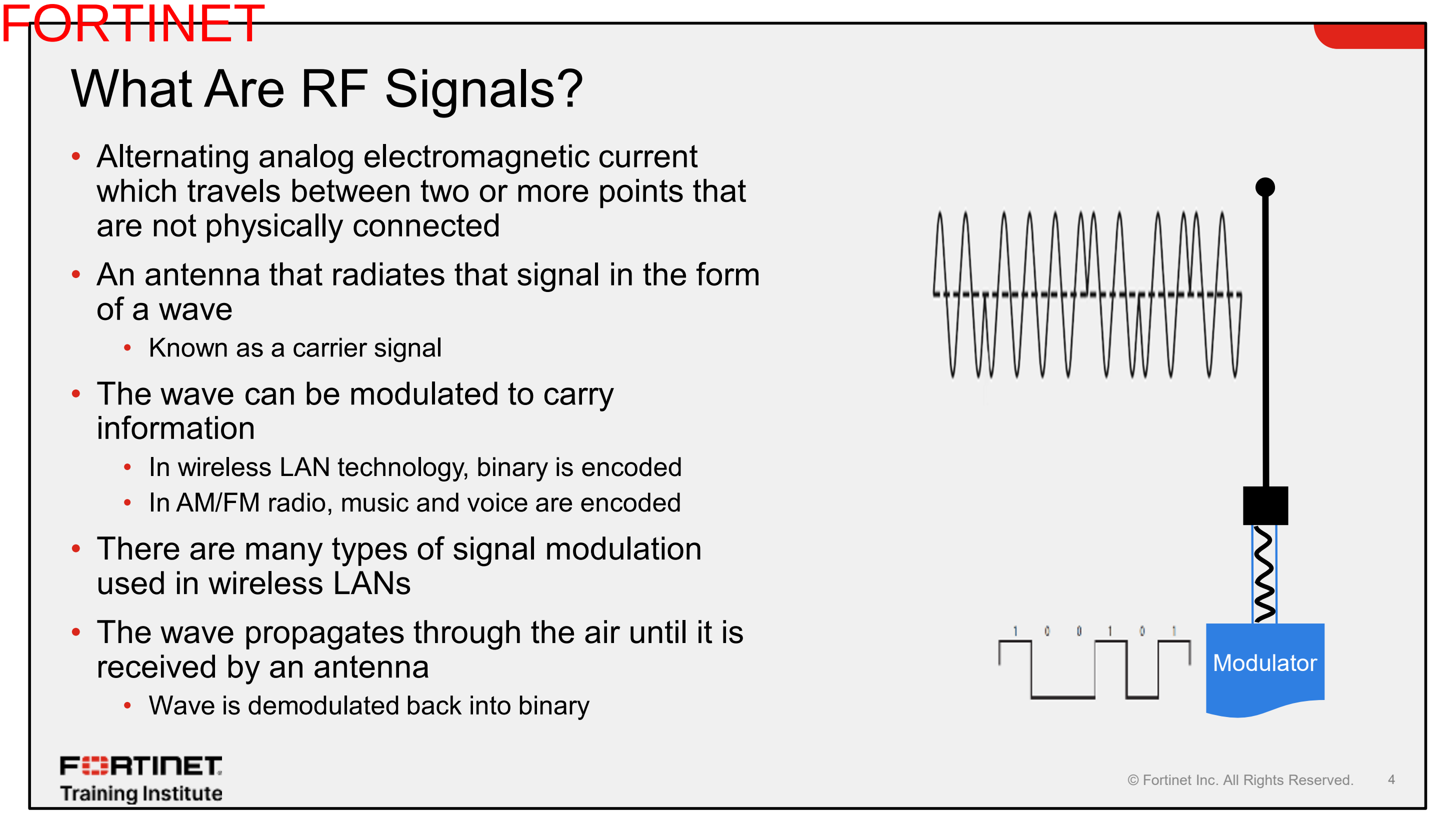
Objectives

- Describe the fundamental principles of data transmission across a wireless signal
- Describe the properties of RF signals
- Describe some of the fundamental limitations of transferring information across an RF signal

3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in radio transmission fundamentals, you will be able to plan and build an efficient wireless network.



What Are RF Signals?

- Alternating analog electromagnetic current which travels between two or more points that are not physically connected
- An antenna that radiates that signal in the form of a wave
  - Known as a carrier signal
- The wave can be modulated to carry information
  - In wireless LAN technology, binary is encoded
  - In AM/FM radio, music and voice are encoded
- There are many types of signal modulation used in wireless LANs
- The wave propagates through the air until it is received by an antenna
  - Wave is demodulated back into binary

Training Institute

As you know, when computers talk, they communicate in binary strings of ones and zeros.

Traditional wireless signals behave differently. They use alternating analogue electromagnetic waves to communicate information between two points that are not physically connected.

Typically, radio signals are transmitted or radiated in the form of a sine wave, often known as a carrier signal. This carrier signal has a constant, predictable pattern alternating between two energy levels. By itself, a signal does not carry any information, at least not until it is modulated.

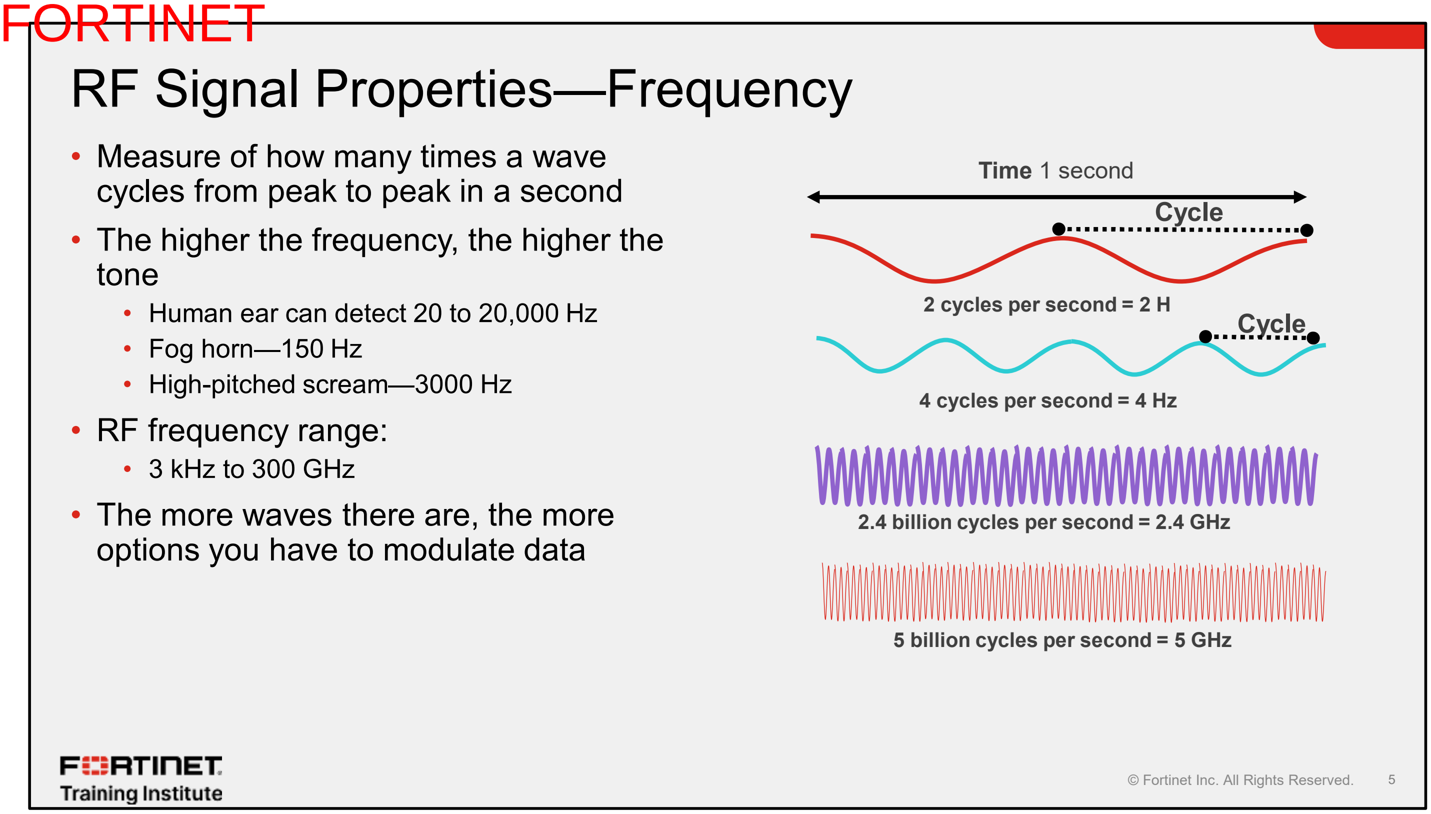
Wireless LAN technology uses encoded binary signals. Traditional radio and TV stations send encoded music, voice, or video signals.

Wireless LANs can use *many* different types of signal modulation. The type depends on the wireless standard in use, and the health of the wireless connection between radios.

Modulation changes various parameters of the signal. Those changes can be used to encode information onto the carrier signal.

Changes in wave form are transmitted across free space until they reach a receiver. During that time they are subject to various laws of physics that can change the properties of the signal, some of which can affect the quality of the signal, and, as a result, the performance of the wireless connection.

Assuming the signal reaches the receiving radio in good condition, the receiving radio compares the sine wave pattern with the encoded version to detect the changes made during modulation and then decodes the information that was sent.



RF Signal Properties—Frequency

- Measure of how many times a wave cycles from peak to peak in a second
- The higher the frequency, the higher the tone
  - Human ear can detect 20 to 20,000 Hz
  - Fog horn—150 Hz
  - High-pitched scream—3000 Hz
- RF frequency range:
  - 3 kHz to 300 GHz
- The more waves there are, the more options you have to modulate data

Time 1 second
Cycle
2 cycles per second = 2 H
Cycle
4 cycles per second = 4 Hz
2.4 billion cycles per second = 2.4 GHz
5 billion cycles per second = 5 GHz

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

The defining property of RF signals is frequency. Frequency is a measure of how many times the wave alternates from a lower energy state to a higher energy state in a second.

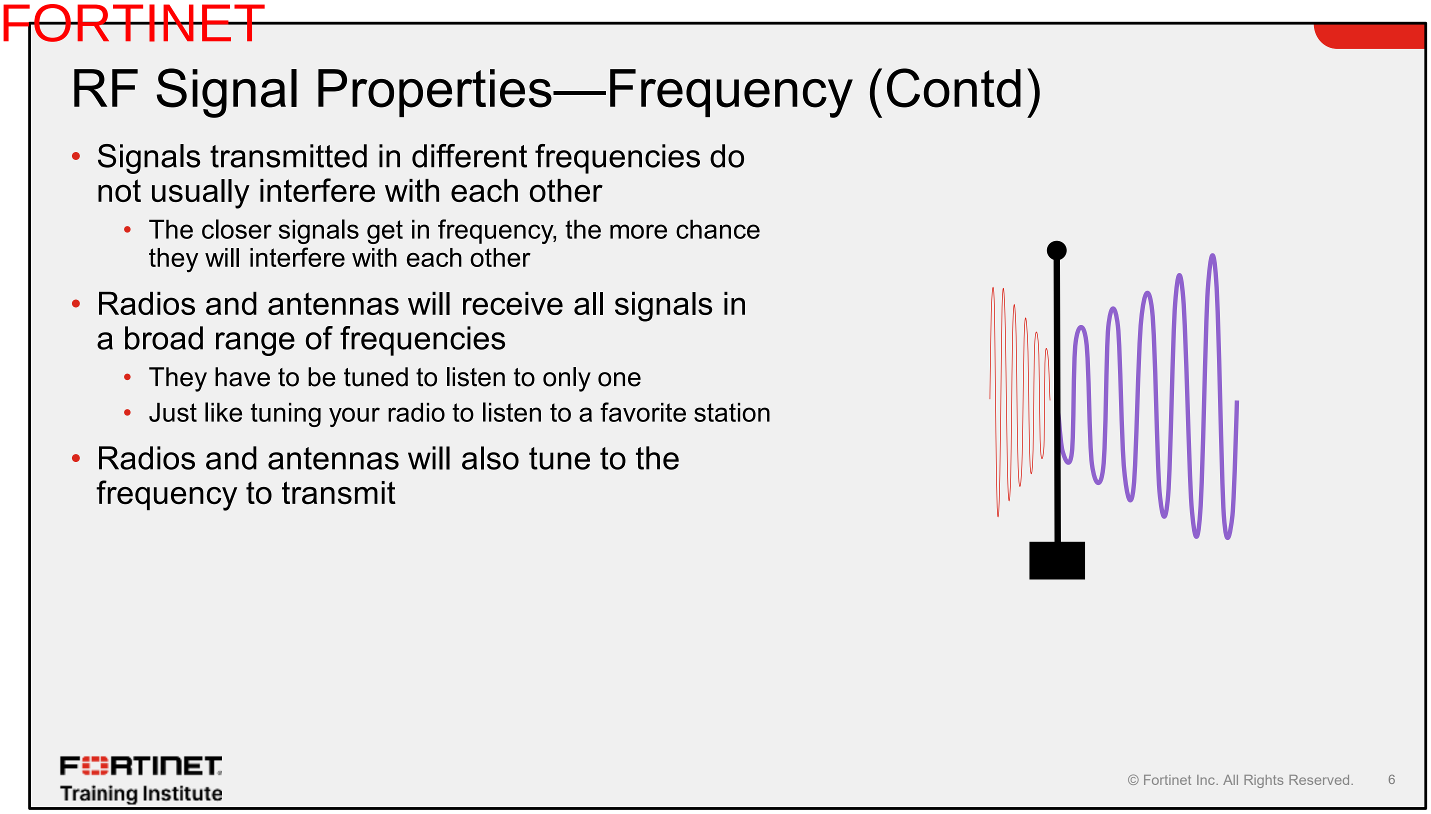
For an extremely low frequency signal of 2 Hz, the wave will cycle two times a second. The higher the frequency, the more times the signal will alternate.

A useful analogy is sound, which, although it’s not traditionally considered to be part of the electromagnetic spectrum, exhibits similar properties to radio waves. The human ear can detect a range of frequencies of sound, from the lowest at 20 Hz, to the highest at 20,000 Hz. The lower the frequency, the lower the tone. For example, a fog horn typically emits a signal at about 150 Hz, which results in a sound that can travel a long way. A high-pitch scream emits a signal at approximately 3000 Hz. This higher frequency sound wave typically requires more energy to generate. Similarly, higher frequency wireless signals will also require more energy, which can have implications for battery usage.

Radio waves adopt the same principles, but are considered to be part of the electromagnetic spectrum—a range of frequencies that includes extremely low frequency radio up to radio waves, microwaves, visible light, and finally up to ultraviolet, x-rays, and gamma radiation.

Radios typically operate in a frequency range between 3 kHz, a signal that alternates 3000 times a second, up to 300 GHz, which is a signal that alternates 300 billion times a second. Wireless LANs typically use frequencies of approximately 2.4 GHz, or 2.4 billion cycles a second, and five GHz, or five billion times a second, or approximately twice as many cycles a second.

Each cycle of a wave allows the possibility of modulation so, in theory, higher frequency waves can carry more information.



RF Signal Properties—Frequency (Contd)

- Signals transmitted in different frequencies do not usually interfere with each other
  - The closer signals get in frequency, the more chance they will interfere with each other
- Radios and antennas will receive all signals in a broad range of frequencies
  - They have to be tuned to listen to only one
  - Just like tuning your radio to listen to a favorite station
- Radios and antennas will also tune to the frequency to transmit

FORTINET Training Institute

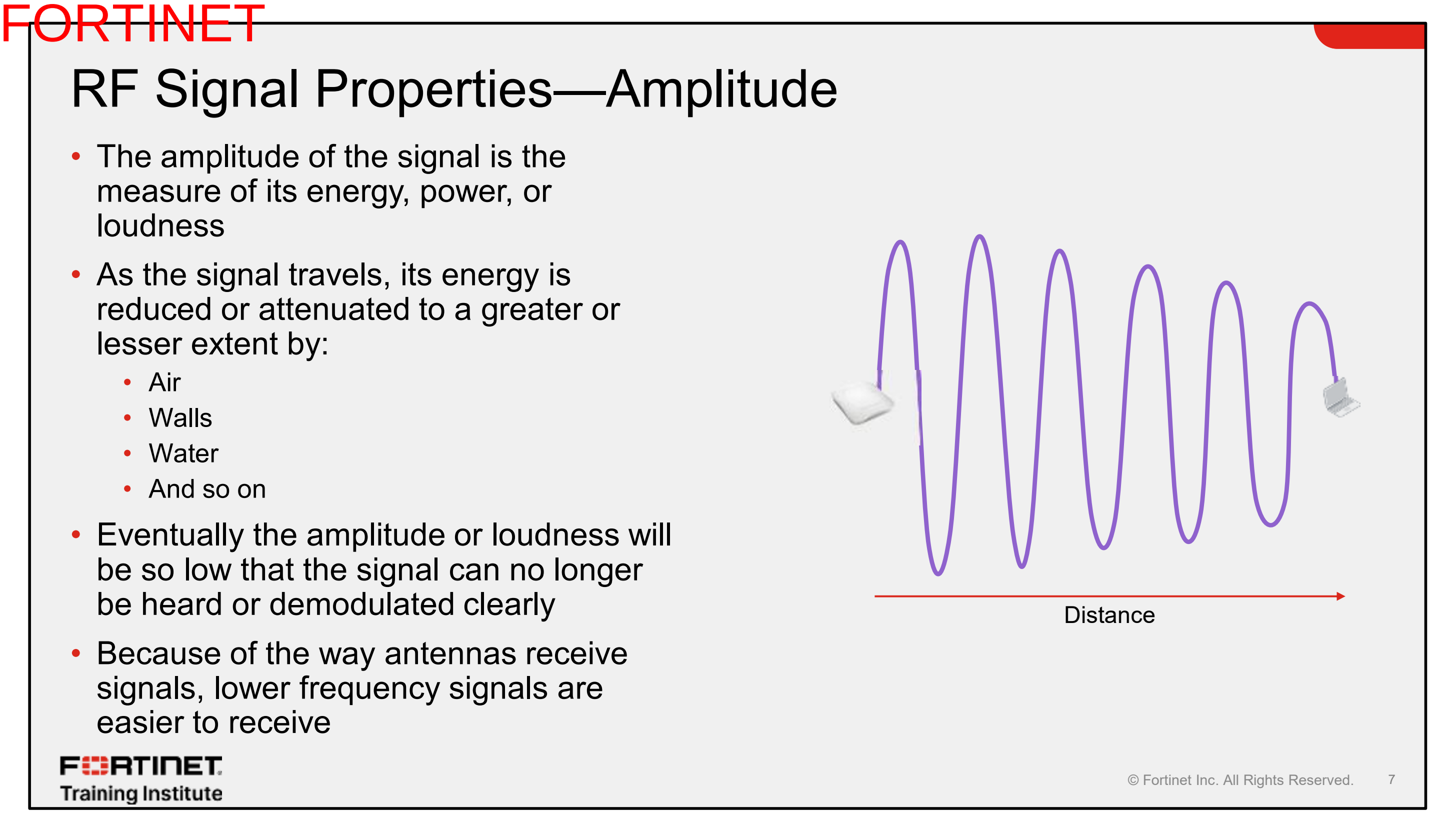
© Fortinet Inc. All Rights Reserved. 6

So, you can transmit signals in waves that cycle a different number of times a second. Each wave operates in its own precise part of the electromagnetic spectrum. If you transmit a signal at a two different frequencies, the two waves do not interact or interfere with each other. This is why some access points (AP) can transmit 2.4 and 5 GHz signals at the same time, through the same antenna.

If you transmit two signals on the same frequency, those signals can interfere with each other. The waves will interact with each other, altering the wave forms and corrupting any modulated signal.

Because radios are not perfect at transmitting in a precise frequency, the energy spills over into adjacent frequencies. The result is that two radios transmitting on adjacent frequencies can interfere with each other. The closer the radios are in frequency, the more likely that interference will occur.

In general, antennas and radios can receive signals that are in a broader range of frequencies. Like the radio receiver in your car that can be “tuned” to different radio stations, an AP radio can be tuned to only one frequency (or channel) for both receiving and transmitting wireless signals.



RF Signal Properties—Amplitude

- The amplitude of the signal is the measure of its energy, power, or loudness
- As the signal travels, its energy is reduced or attenuated to a greater or lesser extent by:
  - Air
  - Walls
  - Water
  - And so on
- Eventually the amplitude or loudness will be so low that the signal can no longer be heard or demodulated clearly
- Because of the way antennas receive signals, lower frequency signals are easier to receive

FORTINET Training Institute

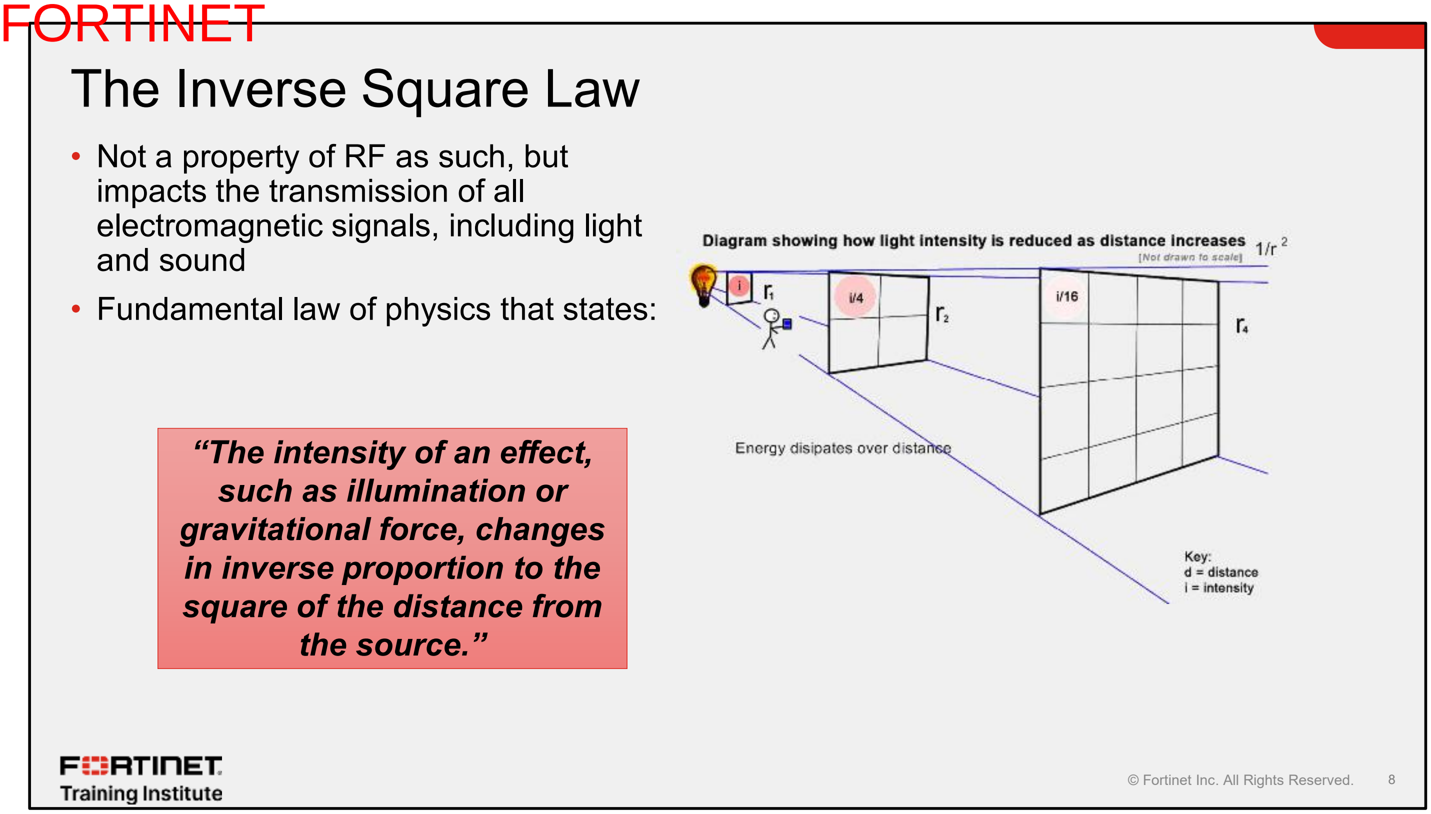
7

Another important property of radio signals is amplitude. Amplitude is a measure of the amount of energy in the signal. It is measured as the difference in energy level from a point of equilibrium and the peak signal oscillation.

If you compare amplitude with sound, amplitude is the loudness of the signal. On earth, the signal has to travel through various types of mediums. The medium will absorb energy from the radio signal and, as a result, the amplitude of the signal is reduced or attenuated. Different materials have different abilities to absorb energy. Air has very little attenuation whereas walls, water, human bodies, and so on, can attenuate much more.

As the amplitude, or loudness, of the signal is reduced, there will a point where it is difficult for the receiver to understand or decode the information in the signal. For example, if you are having a conversation with a friend at a normal volume and your friend is standing 6 feet away from you, they will easily be able to hear and understand what you're saying. However, If your friend moves 100 feet away, and you carry on the conversation at the same volume, your friend will no longer be able to hear clearly what you are saying. They may hear you talking—they can hear a signal—but they will not be able to understand or decode what you're saying. To allow your friend to hear what you're saying, you could increase the amplitude, or loudness, of your voice, otherwise known as shouting.

In theory, the frequency of a signal does not make any difference to the distance that it travels. Only the amplitude matters. However, one of the practical side effects of different frequencies is that antennas send and receive different frequencies at different efficiency rates. A feature of antenna design, called the antenna aperture, means that higher frequency signals are harder to receive successfully than lower frequency ones. This means, practically, that higher frequency signals have a shorter range.



The Inverse Square Law

- Not a property of RF as such, but impacts the transmission of all electromagnetic signals, including light and sound
- Fundamental law of physics that states:

"The intensity of an effect, such as illumination or gravitational force, changes in inverse proportion to the square of the distance from the source."

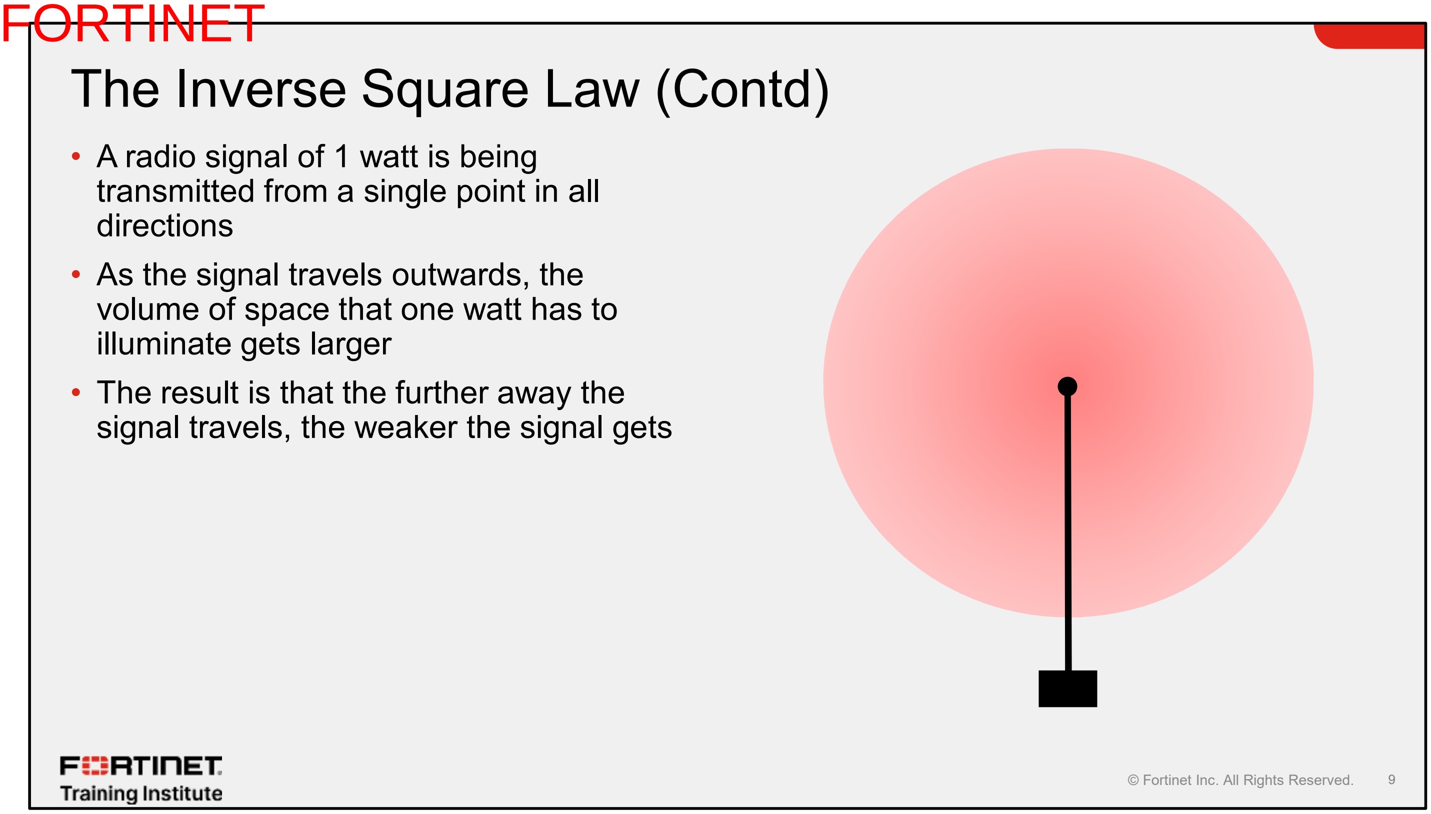
Diagram showing how light intensity is reduced as distance increases
[Not drawn to scale]
1/r 2
i
r1
i/4
r2
i/16
r4
Energy disipates over distance
Key:
d = distance
i = intensity

Training Institute

© Fortinet Inc. All Rights Reserved. 8

Another major impact on the energy level of radio signals is the inverse square law. It is not a property of the signal but it does affect the reception of all types of electromagnetic signals significantly.

The inverse square law states, "The intensity or power of a signal changes in inverse proportion to the square of the distance from the source". As the signal leaves its source, it has to cover more and more space. Because there is only a fixed amount of energy to begin with, the energy dissipates as the volume of space grows.



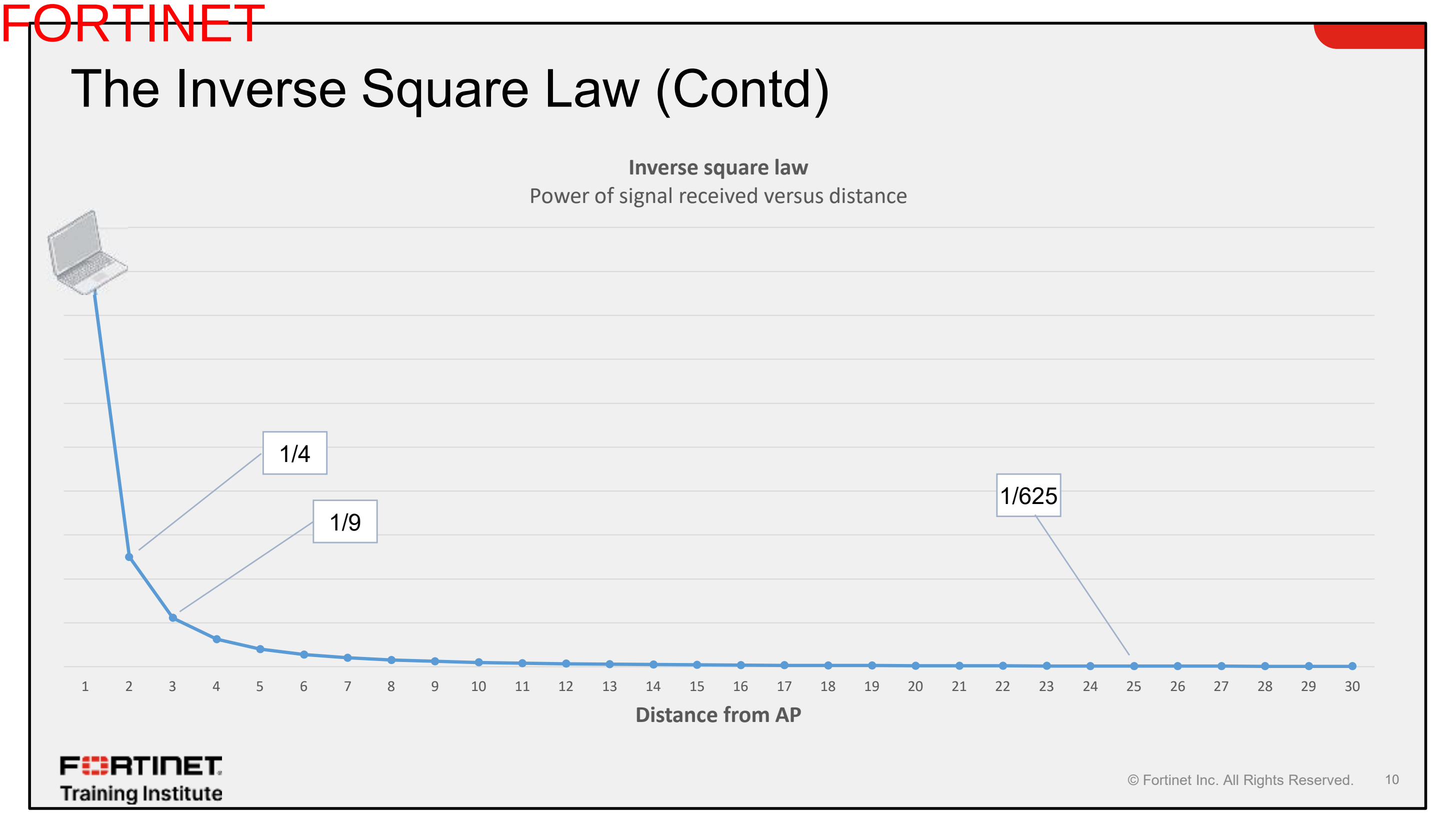
The Inverse Square Law (Contd)

- A radio signal of 1 watt is being transmitted from a single point in all directions
- As the signal travels outwards, the volume of space that one watt has to illuminate gets larger
- The result is that the further away the signal travels, the weaker the signal gets

9

If a radio signal is being transmitted from a single point, such as a signal of 1 watt being transmitted from an antenna, the signal travels in all directions at the same time.

As the signal travels out, the volume of space that that 1 watt has to illuminate increases and the quantity of signal to cover the space decreases. This happens regardless of the medium involved.



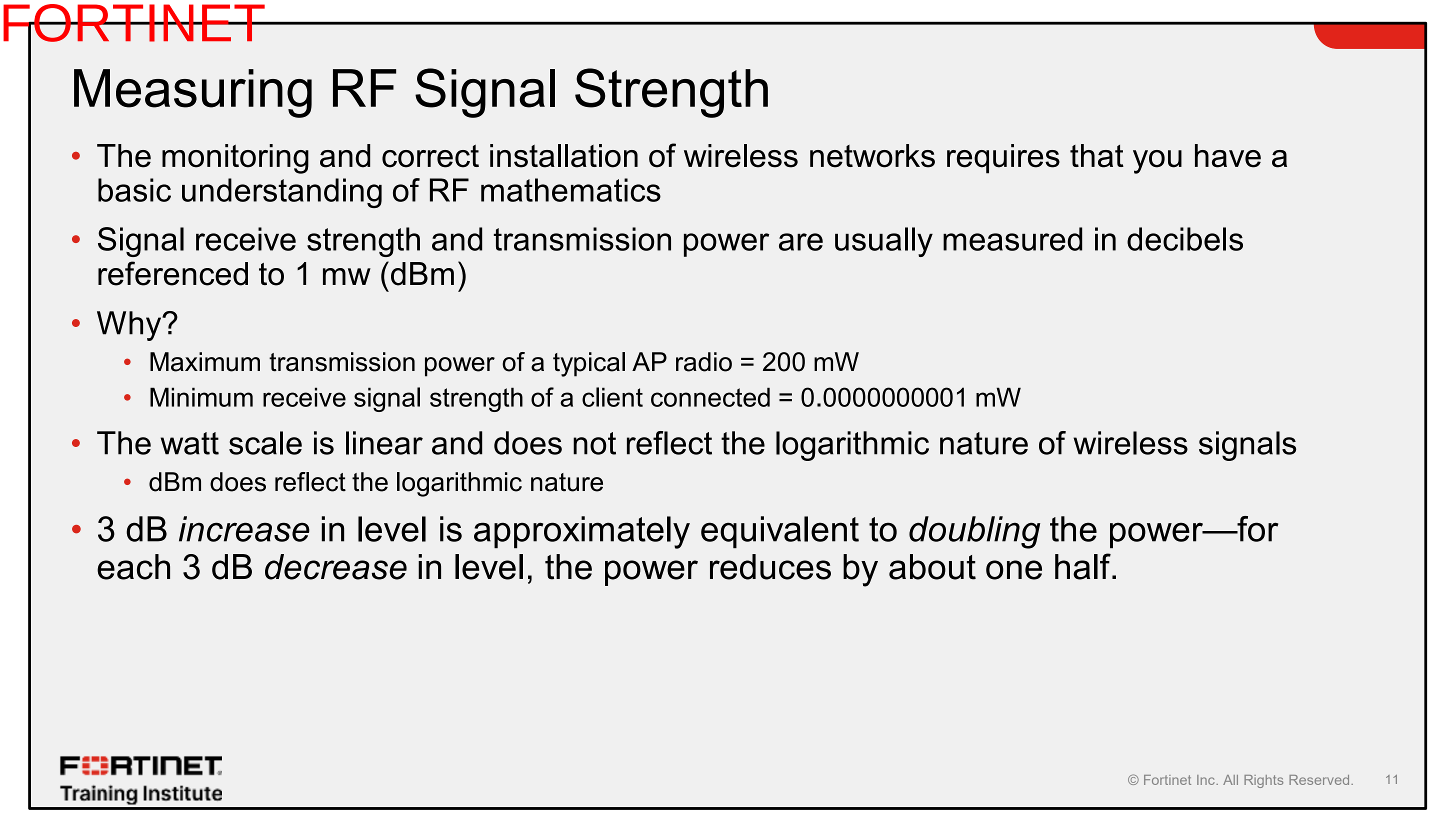
The Inverse Square Law (Contd)

10

To see how this affects energy levels for radios, the table on this slide shows the strength of the signal power plotted against the distance from the AP. The scale is 1 to 30. The unit doesn't matter—it could be inches, yards, miles, or even light years.

As the client moves away from the signal source, the signal strength rapidly drops. Even at very short distances, the signal is reduced to one-quarter or one-ninth of the power, but as the client moves farther out, the rate of reduction in power decreases. Even so, at 25 yards, the signal is approximately 1/625th of the power level emitted by the antenna. However, the signal strength never actually reaches zero. In theory, you could place the AP on the moon and some of its energy would still reach the wireless client on earth, although its energy level would be miniscule. This is why you can see stars from the other side of the galaxy, countless light years away. Some of the photons of light still manage to reach the earth because of the inverse square law.

This reduction in signal strength can have an enormous effect on the wireless signal received by your clients.



Measuring RF Signal Strength

- The monitoring and correct installation of wireless networks requires that you have a basic understanding of RF mathematics
- Signal receive strength and transmission power are usually measured in decibels referenced to 1 mw (dBm)
- Why?
  - Maximum transmission power of a typical AP radio = 200 mW
  - Minimum receive signal strength of a client connected = 0.0000000001 mW
- The watt scale is linear and does not reflect the logarithmic nature of wireless signals
  - dBm does reflect the logarithmic nature
- 3 dB *increase* in level is approximately equivalent to *doubling* the power—for each 3 dB *decrease* in level, the power reduces by about one half.

Training Institute

11

So, how do you measure amplitude or power?

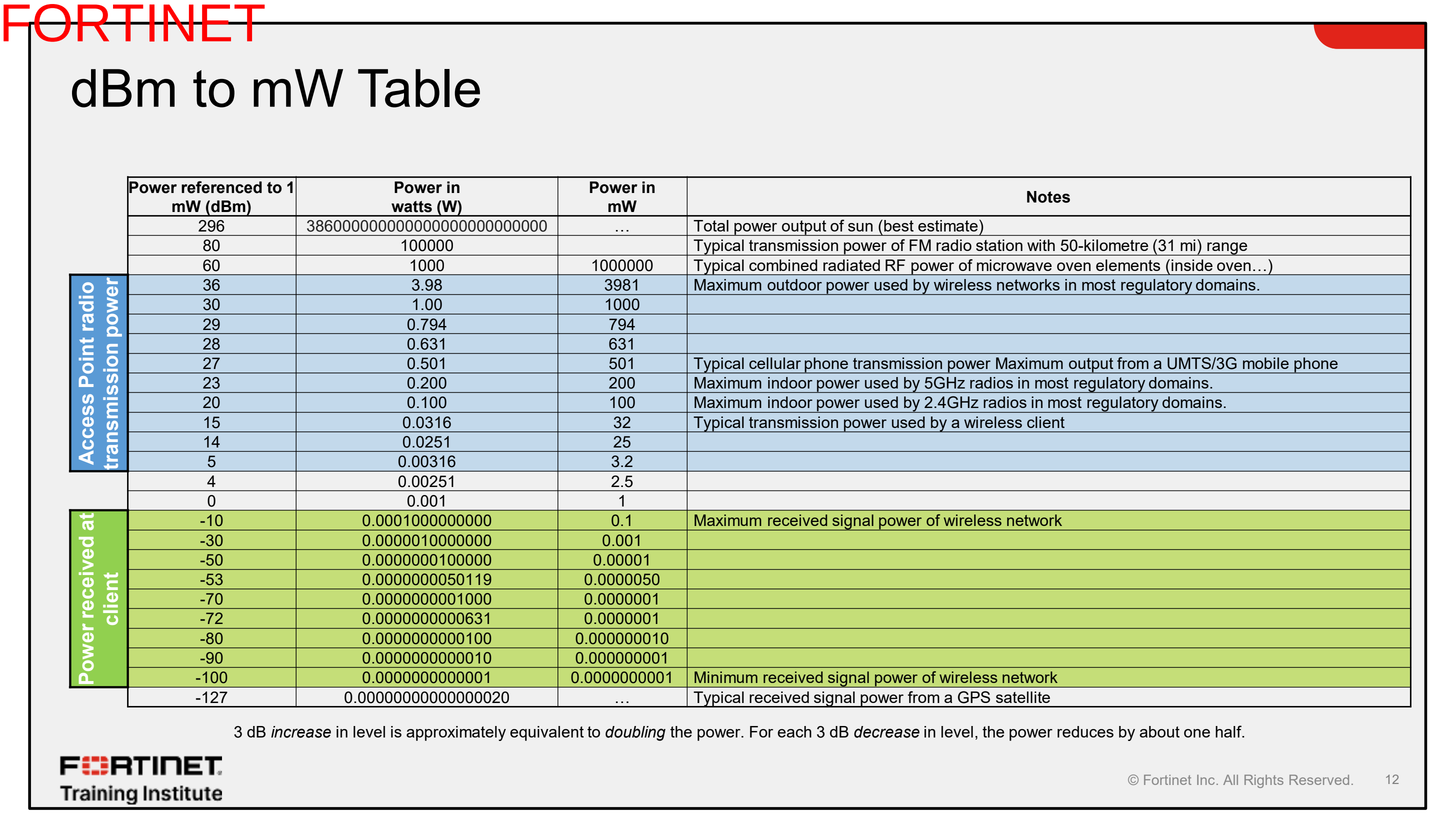
To correctly install and monitor a wireless network, it is necessary to have a basic understanding of RF mathematics. You must be able to take signal strength measurements and perform signal strength calculations to ensure that you select, for example, the right antenna and don't exceed any legal power limits.

Light is measured in the form of watts, for example, a 60w light bulb or 10w LED. But the signal strength of radio waves is measured in dBm, or decibels referenced to 1 millwatt. Most APs can transmit at up to 200 mW or 0.2 of a watt.

Consider the previous slide and the reduction in power that occurs over relatively short distances. By the time the client is any distance away, the received signal strength is very small. The actual signal strength the client can decode is the smallest number shown on the previous slide.

The watt scale is linear. It makes working with very large and very small numbers difficult and does not reflect the logarithmic nature of the inverse square law. Imagine asking an end user what their client's received signal strength is and having them read out 0.0000, and so on.

Remember decibels are logarithmic, so be aware that increasing the power of the signal by 3 dB effectively *doubles* the power, while decreasing the power of the signal by 3 *halves* the power.



dBm to mW Table

	Power referenced to 1 mW (dBm)	Power in watts (W)	Power in mW	Notes
	296	386000000000000000000000000	…	Total power output of sun (best estimate)
	80	100000		Typical transmission power of FM radio station with 50-kilometre (31 mi) range
	60	1000	1000000	Typical combined radiated RF power of microwave oven elements (inside oven…)
Access Point radio transmission power	36	3.98	3981	Maximum outdoor power used by wireless networks in most regulatory domains.
	30	1.00	1000	
	29	0.794	794	
	28	0.631	631	
	27	0.501	501	Typical cellular phone transmission power Maximum output from a UMTS/3G mobile phone
	23	0.200	200	Maximum indoor power used by 5GHz radios in most regulatory domains.
	20	0.100	100	Maximum indoor power used by 2.4GHz radios in most regulatory domains.
	15	0.0316	32	Typical transmission power used by a wireless client
	14	0.0251	25	
	5	0.00316	3.2	
	4	0.00251	2.5	
	0	0.001	1	
Power received at client	-10	0.0001000000000	0.1	Maximum received signal power of wireless network
	-30	0.0000010000000	0.001	
	-50	0.0000000100000	0.00001	
	-53	0.0000000050119	0.0000050	
	-70	0.0000000001000	0.0000001	
	-72	0.0000000000631	0.0000001	
	-80	0.0000000000100	0.000000010	
	-90	0.0000000000010	0.000000001	
	-100	0.0000000000001	0.0000000001	Minimum received signal power of wireless network
	-127	0.00000000000000020	…	Typical received signal power from a GPS satellite

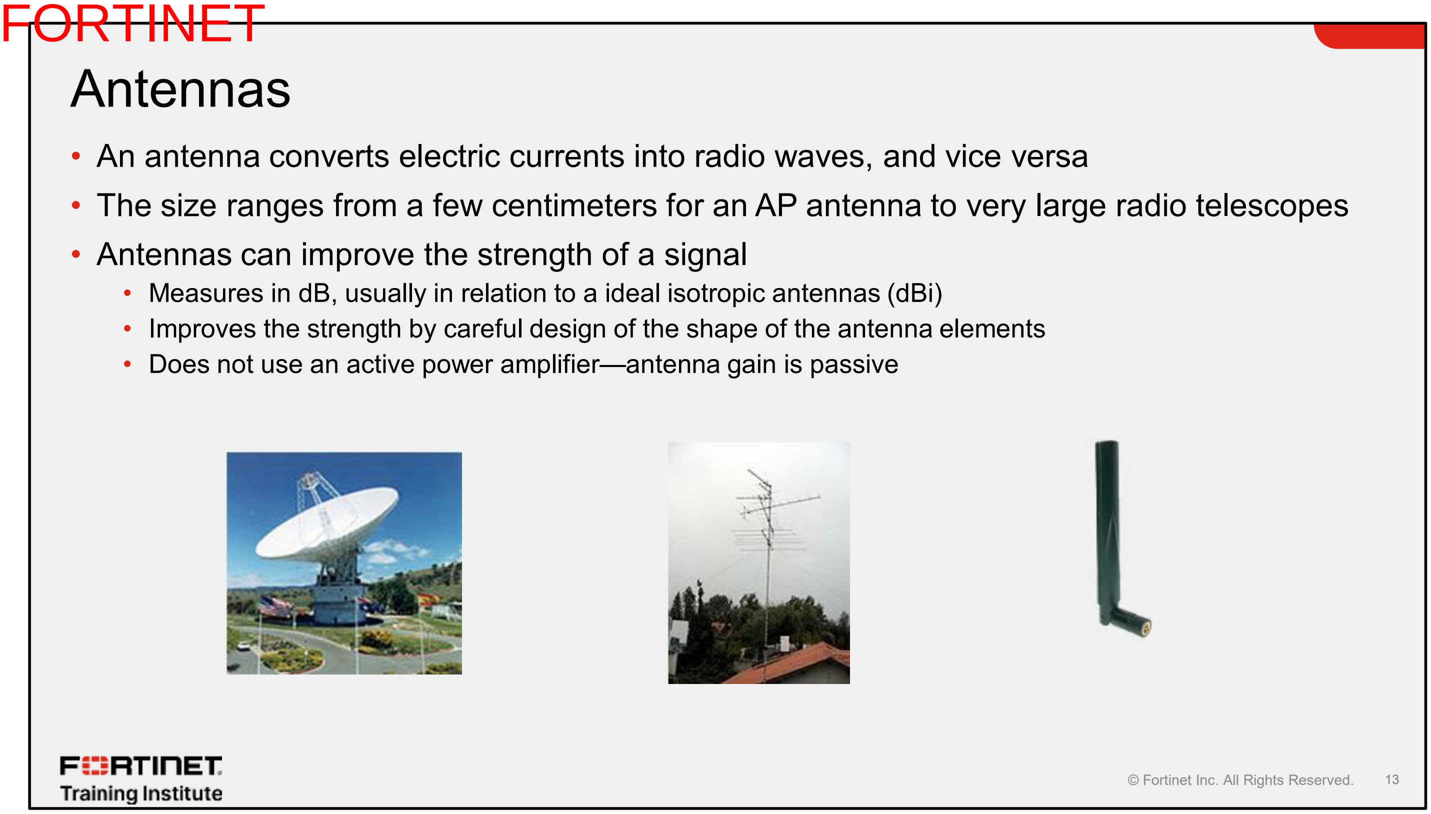
3 dB *increase* in level is approximately equivalent to *doubling* the power. For each 3 dB *decrease* in level, the power reduces by about one half.

Training Institute

The table on this slide shows some common decibel to watt/mw conversions. The blue area shows the power levels that the radios transmit in. The green area shows the power of the same signal when it arrives at the receiving radio. Remember the power of the inverse square law, and see the difference in power levels.

The power of the dBm scale is that at one end it can represent the power of the sun at 296 dBm, and at the other end it can represent the weakest wireless LAN or GPS signal, all within four characters.

Remember decibels are logarithmic, so be aware that increasing the power of the signal by 3 dB effectively *doubles* the power, while decreasing the power of the signal by 3 *halves* the power.



Antennas

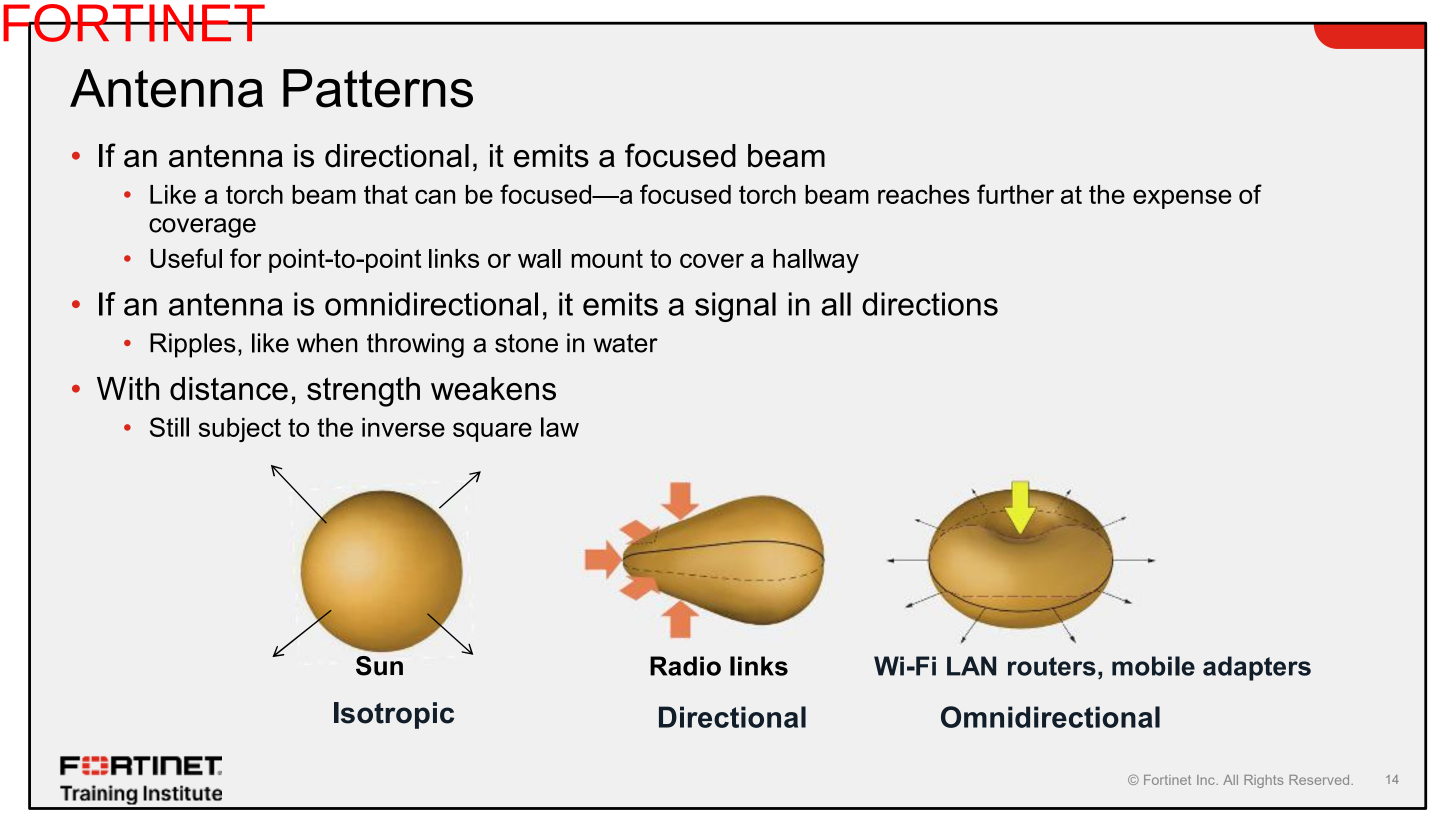
- An antenna converts electric currents into radio waves, and vice versa
- The size ranges from a few centimeters for an AP antenna to very large radio telescopes
- Antennas can improve the strength of a signal
  - Measures in dB, usually in relation to a ideal isotropic antennas (dBi)
  - Improves the strength by careful design of the shape of the antenna elements
  - Does not use an active power amplifier—antenna gain is passive

13

An antenna is an electrical device that converts electric currents into radio waves, and vice versa. Typically, an antenna consists of an arrangement of metallic conductors (elements) electrically connected to the receiver or transmitter.

In wireless APs, an antenna is sometimes visible and attached externally, and is sometimes embedded and hidden in the AP body casing.

Antennas are typically passive elements. They do not use electrical amplifiers to improve a signal, but shape its direction, which provides a gain in the transmission system.



Antenna Patterns

- If an antenna is directional, it emits a focused beam
  - Like a torch beam that can be focused—a focused torch beam reaches further at the expense of coverage
  - Useful for point-to-point links or wall mount to cover a hallway
- If an antenna is omnidirectional, it emits a signal in all directions
  - Ripples, like when throwing a stone in water
- With distance, strength weakens
  - Still subject to the inverse square law

Sun
Isotropic
Radio links
Directional
Wi-Fi LAN routers, mobile adapters
Omnidirectional
FORTINET Training Institute

14

Do antennas emit radio waves in all directions? Can a wireless client be located anywhere relative to the antenna? No.

Most obviously, the signal is best when closer to the antenna. Signals become weak over distance.

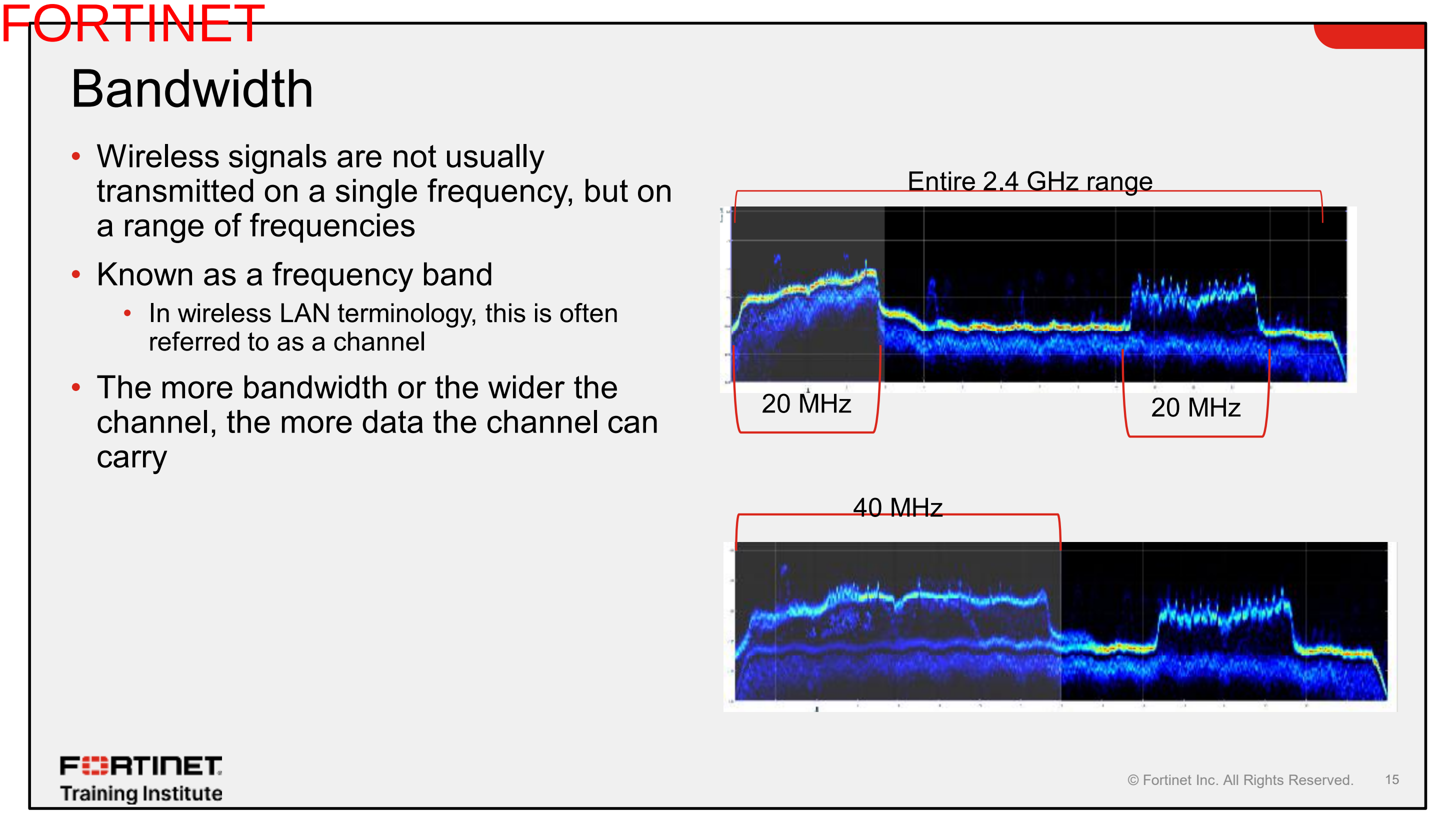
The geometry of the antenna also affects how far the signal will reach, and where. Shapes determine the radiation pattern (also known as antenna pattern or far-field pattern). Strength depends on the direction for some antennas.

The sun radiates in all directions. It's an example of an isotropic antenna shape.

Radio links usually use a directional antennal, also called a *beam antenna*, which focuses its power in transmitting in a specific direction.

Wireless LAN routers and mobile adapters often have an omnidirectional antenna . This doughnut shape radiates radio wave power uniformly, in all directions, on one plane.

Different patterns are suitable to different deployments, which is why there are many different AP models available.



Bandwidth

- Wireless signals are not usually transmitted on a single frequency, but on a range of frequencies
- Known as a frequency band
  - In wireless LAN terminology, this is often referred to as a channel
- The more bandwidth or the wider the channel, the more data the channel can carry

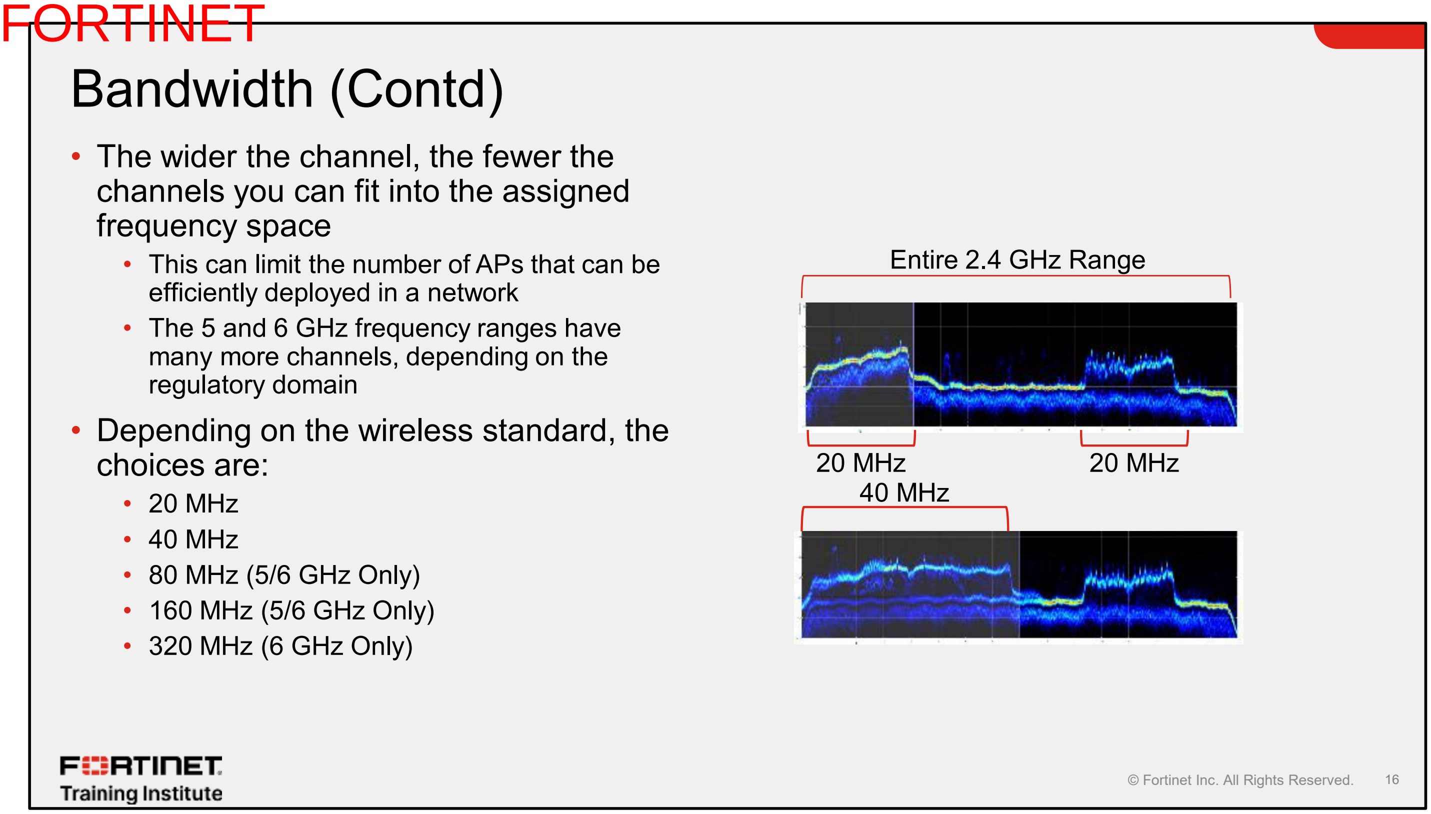
© Fortinet Inc. All Rights Reserved. 15

Along with frequency and amplitude, signals occupy bandwidth.

Often, radio signals are not transmitted on a single frequency, but on a range of frequencies, known as the frequency band, or in the wireless LAN world, a channel.

Usually, the wider the channel, the more frequency space is available for transmission. In modern wireless networks, the more frequency space that is available to transmit signals, the more data the channel can carry.

The screenshots on this slide show images taken on a spectrum analyzer. The images show different types of wireless signals being transmitted at different bandwidths. Incidentally, it is also possible to see the noise floor as well. Noise will be covered later in this lesson.



Bandwidth (Contd)

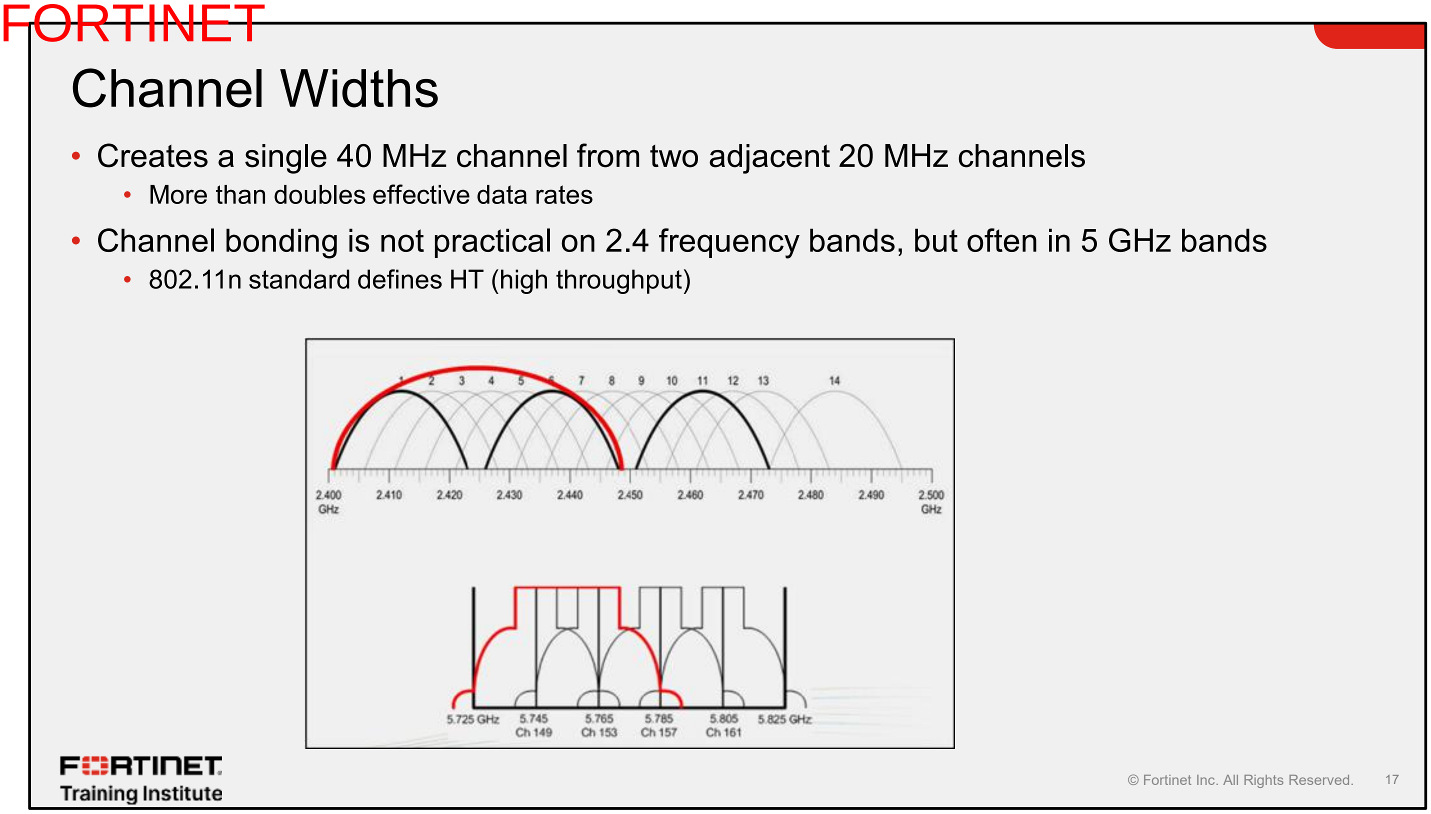
- The wider the channel, the fewer the channels you can fit into the assigned frequency space
  - This can limit the number of APs that can be efficiently deployed in a network
  - The 5 and 6 GHz frequency ranges have many more channels, depending on the regulatory domain
- Depending on the wireless standard, the choices are:
  - 20 MHz
  - 40 MHz
  - 80 MHz (5/6 GHz Only)
  - 160 MHz (5/6 GHz Only)
  - 320 MHz (6 GHz Only)

FORTINET Training Institute

16

Because the frequency range assigned for wireless LAN use is limited, the wider the channel, the fewer the channels that you can fit into the assigned frequency space. This can limit the number of APs that you can efficiently deploy in a network.

Current wireless standards allow the use of multiple channel widths, from 20 MHz up to 160 MHz. However, this depends on the standards in use. The practical applications of the wider channel widths depend on the wireless technology in use and the environment the network is operating in. It is widely acknowledged that networks will not be able to use 160 MHz channels in anything more than a single AP home environment. There simply are not enough 160 MHz channels available to accommodate the multiple channels that are required for a larger wireless network to minimise co-channel interference (CCI).



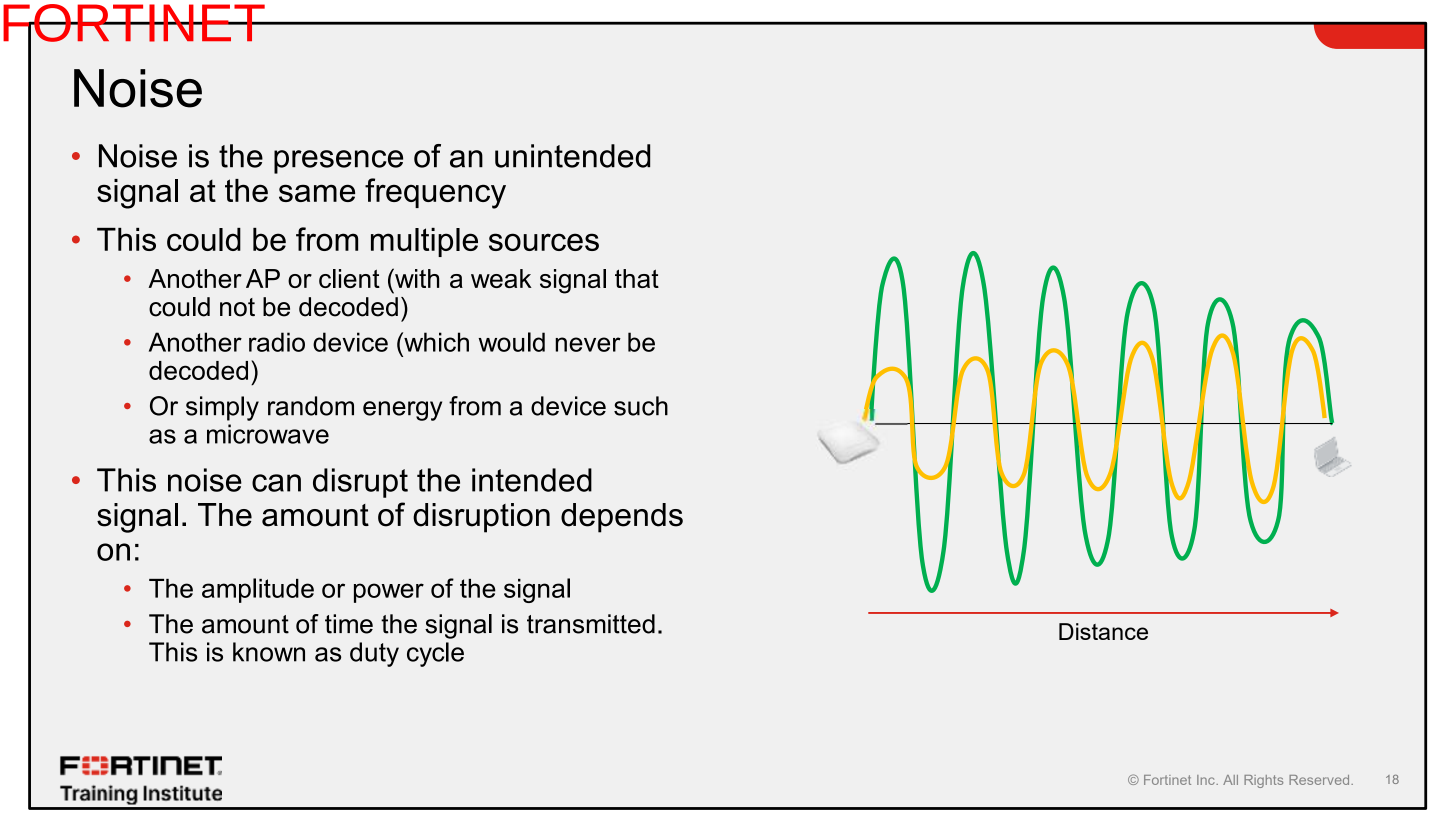
Channel Widths

- Creates a single 40 MHz channel from two adjacent 20 MHz channels
  - More than doubles effective data rates
- Channel bonding is not practical on 2.4 frequency bands, but often in 5 GHz bands
  - 802.11n standard defines HT (high throughput)

17

Channel bonding is impractical in the 2.4 GHz band because it consumes a lot of the available bandwidth—the bonded channel is 40 MHz—but it can still be used where there are few APs in the band.

It is more practical in the 5 GHz band. This is because there is a greater number of channels available. This concept was introduced in the 802.11n standard amendment, which defines high throughput (HT) on WLANs.



Noise

- Noise is the presence of an unintended signal at the same frequency
- This could be from multiple sources
  - Another AP or client (with a weak signal that could not be decoded)
  - Another radio device (which would never be decoded)
  - Or simply random energy from a device such as a microwave
- This noise can disrupt the intended signal. The amount of disruption depends on:
  - The amplitude or power of the signal
  - The amount of time the signal is transmitted. This is known as duty cycle

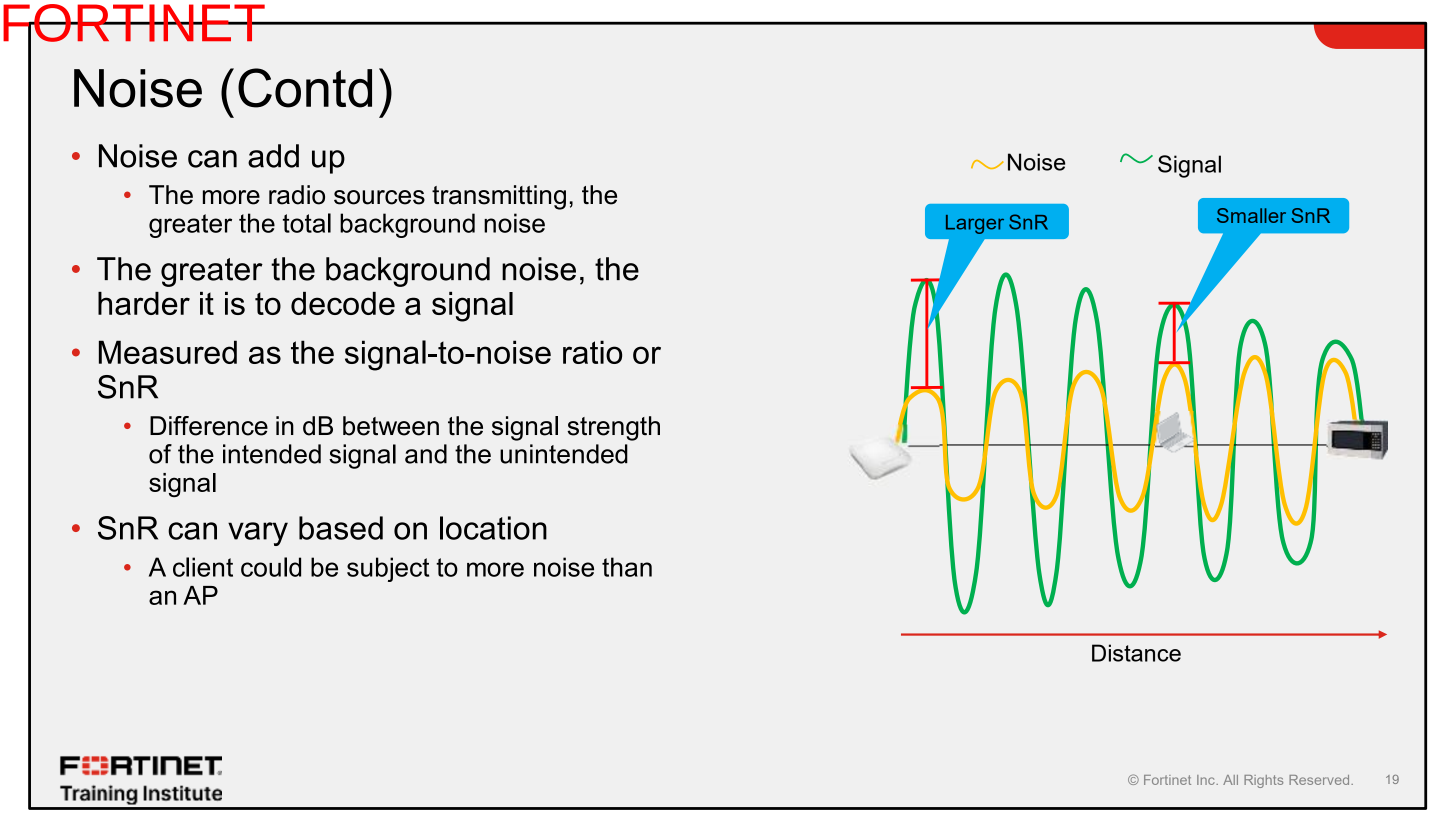
Noise is the presence of an unintended signal in the same frequency as the one that you’re trying to listen to or receive.

To listen to a radio station on longwave or AM, you must tune the radio precisely to get the best quality signal. Even then, you often hear a constant background hiss—unintended signals or background noise transmitted on the same frequency at the same time from another source. Usually, while annoying, this background noise does not stop you from listening to the radio station. You can still understand the words the radio presenter says, or in wireless terms, decode the signal

However, if someone turned on an electrical appliance, such as a vacuum cleaner, the interference on the radio could increase dramatically, possibly to the point where you could no longer hear the radio presenter clearly.

Signals could be from another radio device that can use the same frequency—for example, a baby monitor or garage door remote control. It could be random energy from a device such as a microwave, which uses the energy of microwaves to heat the water in food.

Wherever the signal comes from, it could be at a power level that drowns out the signal you are trying to hear, making it impossible to understand what is transmitted.



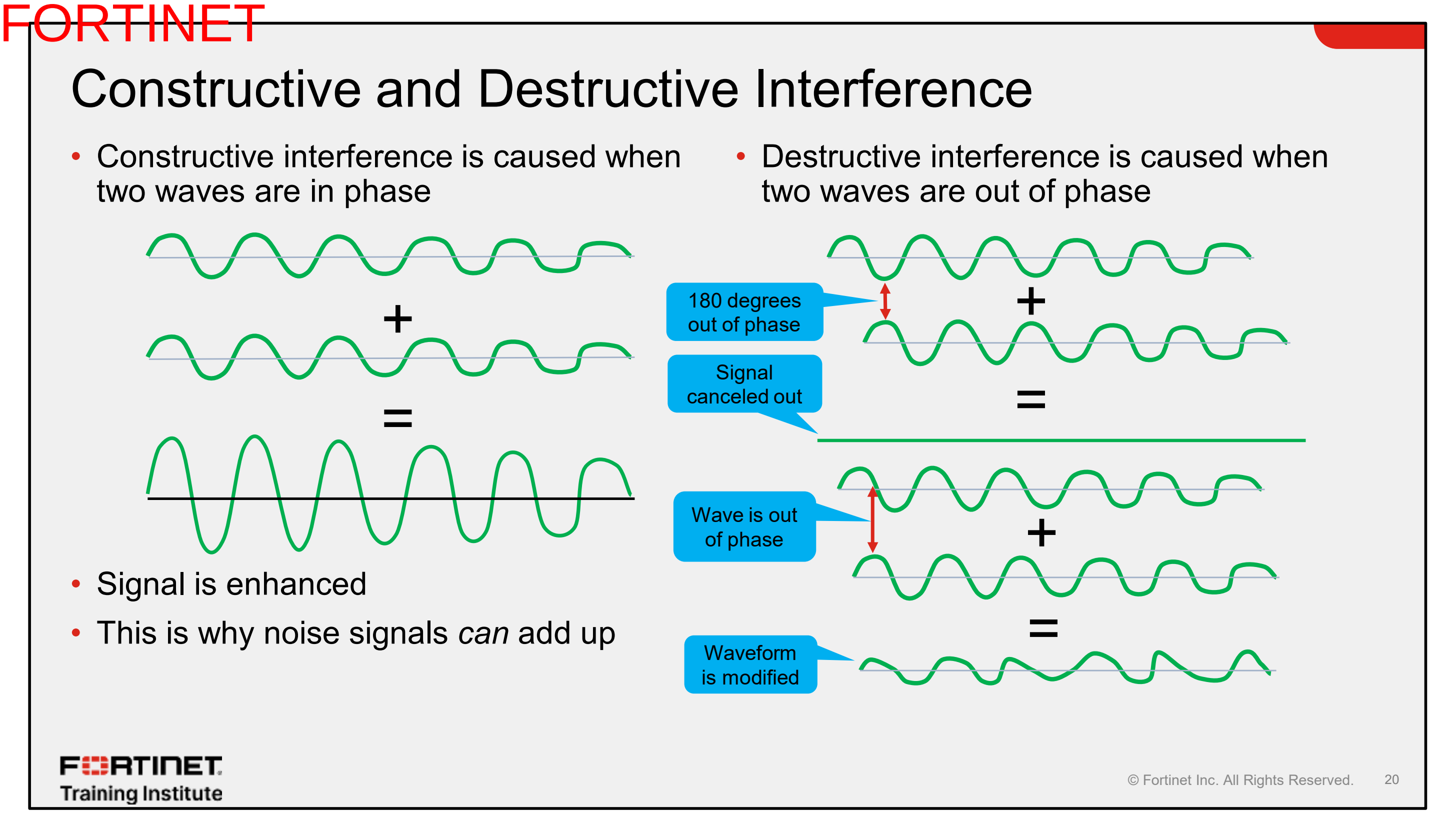
Noise (Contd)

- Noise can add up
  - The more radio sources transmitting, the greater the total background noise
- The greater the background noise, the harder it is to decode a signal
- Measured as the signal-to-noise ratio or SnR
  - Difference in dB between the signal strength of the intended signal and the unintended signal
- SnR can vary based on location
  - A client could be subject to more noise than an AP

It is important to note that multiple noise signals can add up, increasing the total noise signal. In wireless networks, the effect of noise is most often measured using SnR; this is the number of decibels *difference* in signal strength *between* the noise signal(s), sometimes called the noise floor and the signal strength of the intended signal. SnR measures the relative power of the noise signal; but equally important is how *long* the noise signal is present. The amount of time a signal is receivable is called the duty cycle. It is a measure of the percentage of air time utilized. A signal with a duty cycle of 80% is receivable for 80% of any given period.

For a wireless LAN, a noise signal with a high duty cycle but lower signal strength can be as disruptive as a powerful noise signal with a short duty cycle. While the constant low-level noise may not completely disrupt the wireless signal, it will cause high levels of retransmission or loss. The impact on the perceived performance of the wireless network can be significant—perhaps more so than the infrequent loss of connection caused by short duty cycle, high strength interference. All noise signals need to be analyzed, considering both measures.

Most enterprise wireless systems are able to measure the noise floor. It is one of the most critical measurements to monitor in a wireless environment. However, the APs take noise measurements. The amount of noise can vary depending on the location of the noise source, the clients connecting to the AP, and the location of the AP. So, even though the APs may *not* be measuring a very high noise floor, your clients could still be suffering from a noise problem if the source of noise is closer to them. Noise can be highly localized, depending on the type of source. All wireless LAN radios have to detect the noise floor to operate correctly, but reporting that measurement is another matter. Some clients can report the noise level detected, but the ability to do so depends on the client, the operating system, and whether the noise level is reported in a useful format. Often, you have to use another type of device to take precise noise measurements in different parts of the network.



Constructive and Destructive Interference

- Constructive interference is caused when two waves are in phase

- Signal is enhanced
- This is why noise signals *can* add up

- Destructive interference is caused when two waves are out of phase

180 degrees out of phase

Signal canceled out

Wave is out of phase

Waveform is modified

Training Institute

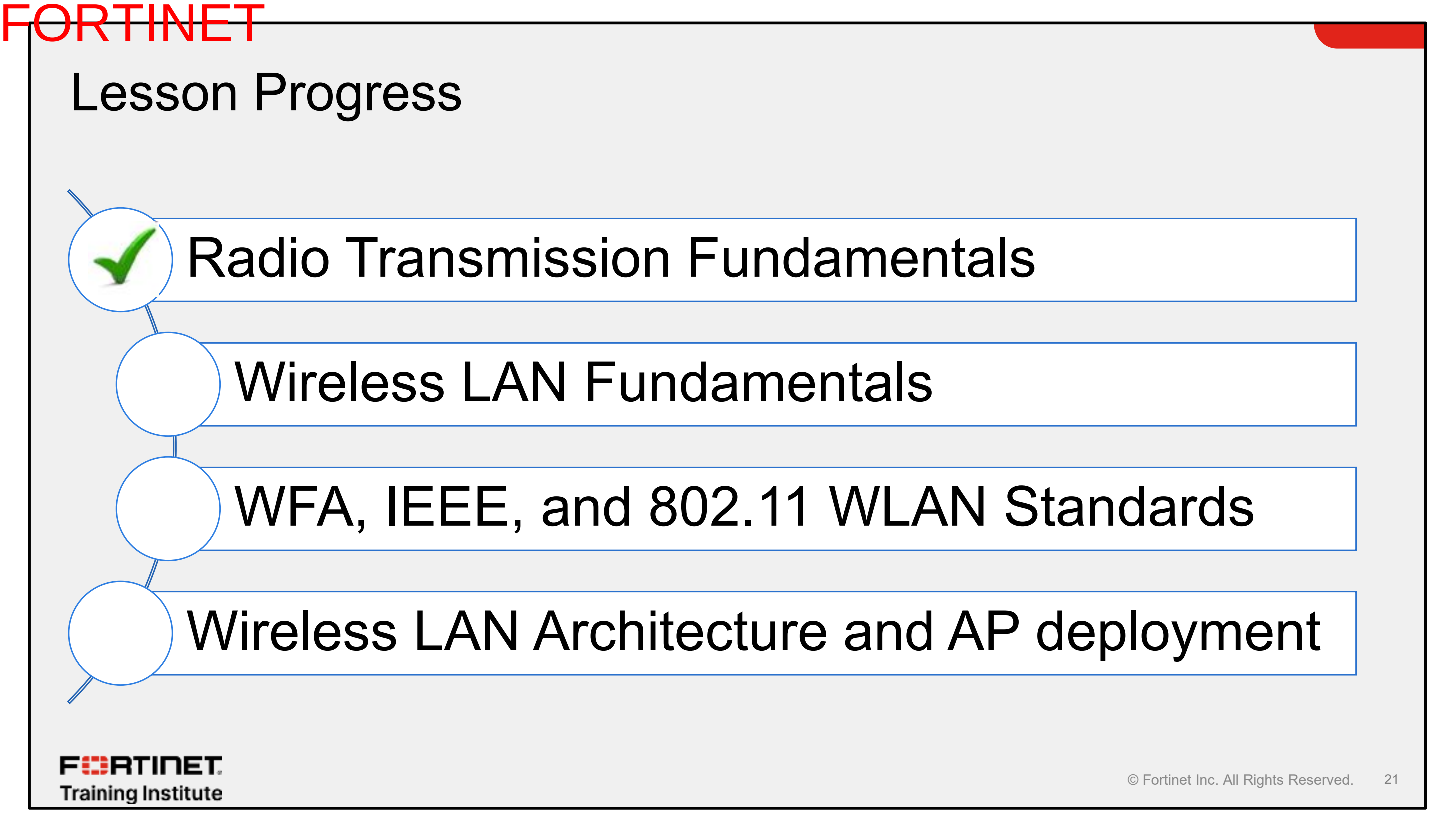
20

As you have learned, wireless LAN signals transmit in the form of waves. However, waves do not transmit in isolation. Radio waves can modify each other during transmission using the process of wave interference. Wave interference applies to all types of waves. If you drop a single pebble in a pond of water, you will see how the ripples, or waves, travel or propagate across the water. Drop two stones simultaneously and watch how the two sets of ripples interact with each other. You will see the ripples interfere with each other, generating all sorts of different effects, including constructive and destructive interference.

Wireless LAN signals behave in a very similar way, where two or more waves superpose to form a resultant wave of greater, lower, or the same amplitude. Constructive and destructive interference results from the interaction of correlated or coherent waves, either because they come from the same source or because they have the same, or nearly the same, frequency.

Theoretically, signals can cancel each other out if they are identical in form and one hundred and eighty degrees out of phase. Complete cancellation is unlikely in the real world; modulated waves are never likely to be identical and not likely to be exactly out of phase. More commonly, signals are modified by the presence of other radio waves. This is the reason noise signals can add up. Many multiple background noise signals can constructively interfere with each other causing a net increase in the noise level. Likewise, signals can have their amplitude increased through constructive interference.

Wireless LAN chipsets can decode waveforms modified to a certain point; however, if there is a lot of interference, it will soon become impossible to decode the signal correctly. Any interference is traditionally an issue for wireless LAN radios; however, the newer standards can beneficially use constructive interference, as you will see later in this module.



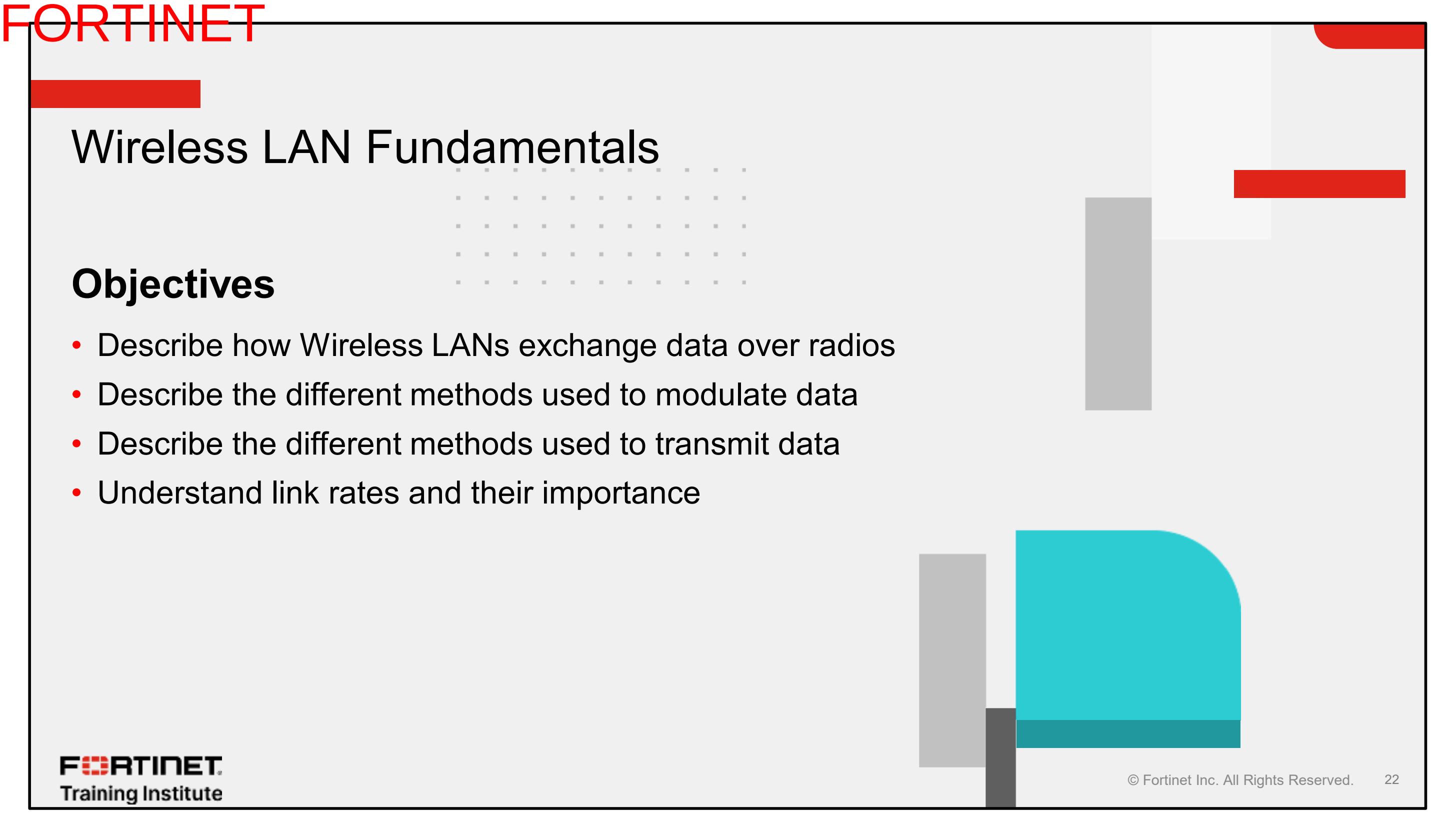
Lesson Progress

- ✓ Radio Transmission Fundamentals
- ○ Wireless LAN Fundamentals
- ○ WFA, IEEE, and 802.11 WLAN Standards
- ○ Wireless LAN Architecture and AP deployment

21

Good job! You now understand radio transmission fundamentals.

Now, you will learn about Wireless LAN fundamentals



Wireless LAN Fundamentals

Objectives

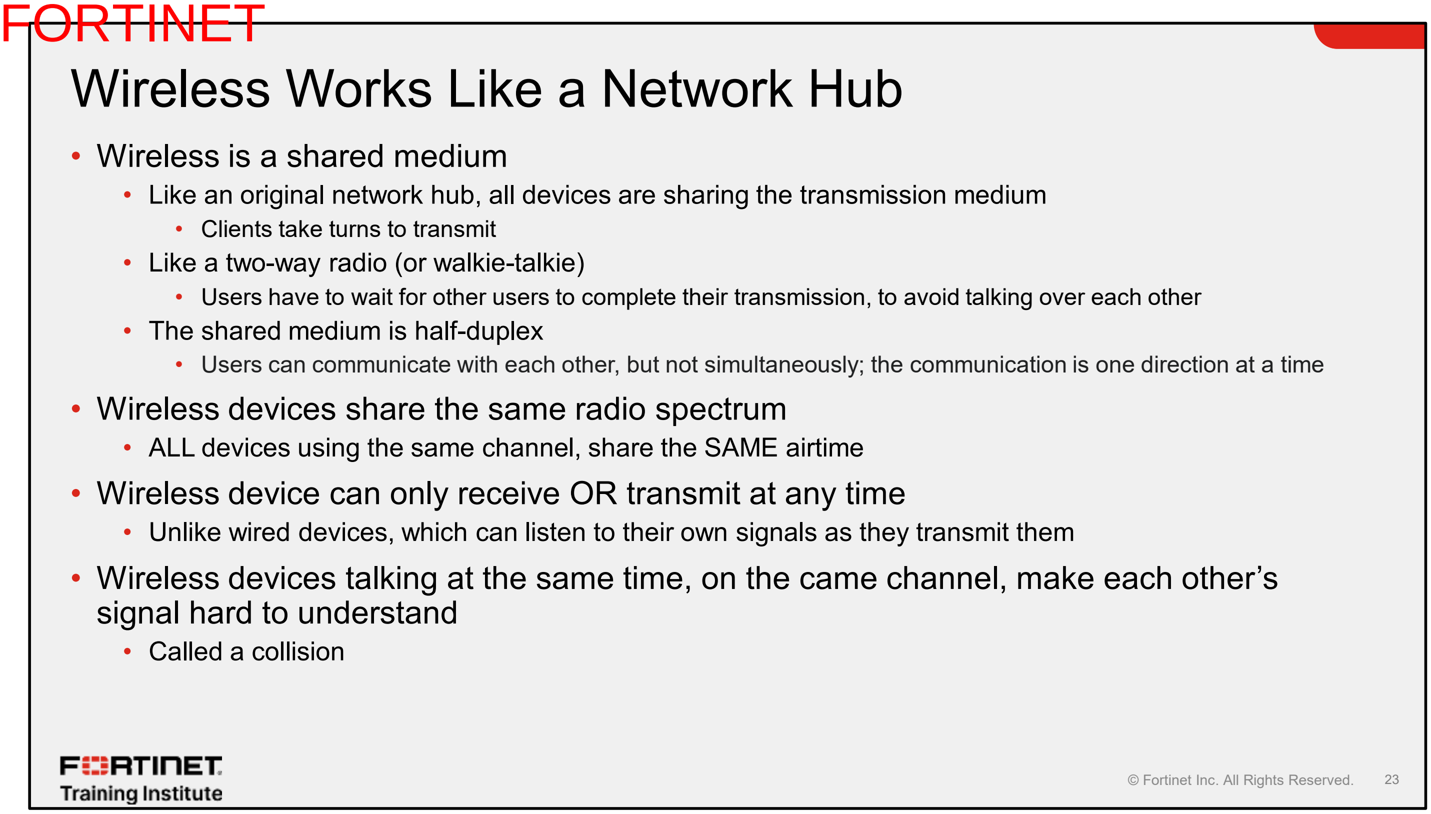
- Describe how Wireless LANs exchange data over radios
- Describe the different methods used to modulate data
- Describe the different methods used to transmit data
- Understand link rates and their importance

FORTINET Training Institute

22

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in wireless LAN fundamentals, you will be able to plan and build an efficient wireless network.



Wireless Works Like a Network Hub

- Wireless is a shared medium
  - Like an original network hub, all devices are sharing the transmission medium
    - Clients take turns to transmit
  - Like a two-way radio (or walkie-talkie)
    - Users have to wait for other users to complete their transmission, to avoid talking over each other
  - The shared medium is half-duplex
    - Users can communicate with each other, but not simultaneously; the communication is one direction at a time
- Wireless devices share the same radio spectrum
  - ALL devices using the same channel, share the SAME airtime
- Wireless device can only receive OR transmit at any time
  - Unlike wired devices, which can listen to their own signals as they transmit them
- Wireless devices talking at the same time, on the came channel, make each other's signal hard to understand
  - Called a collision

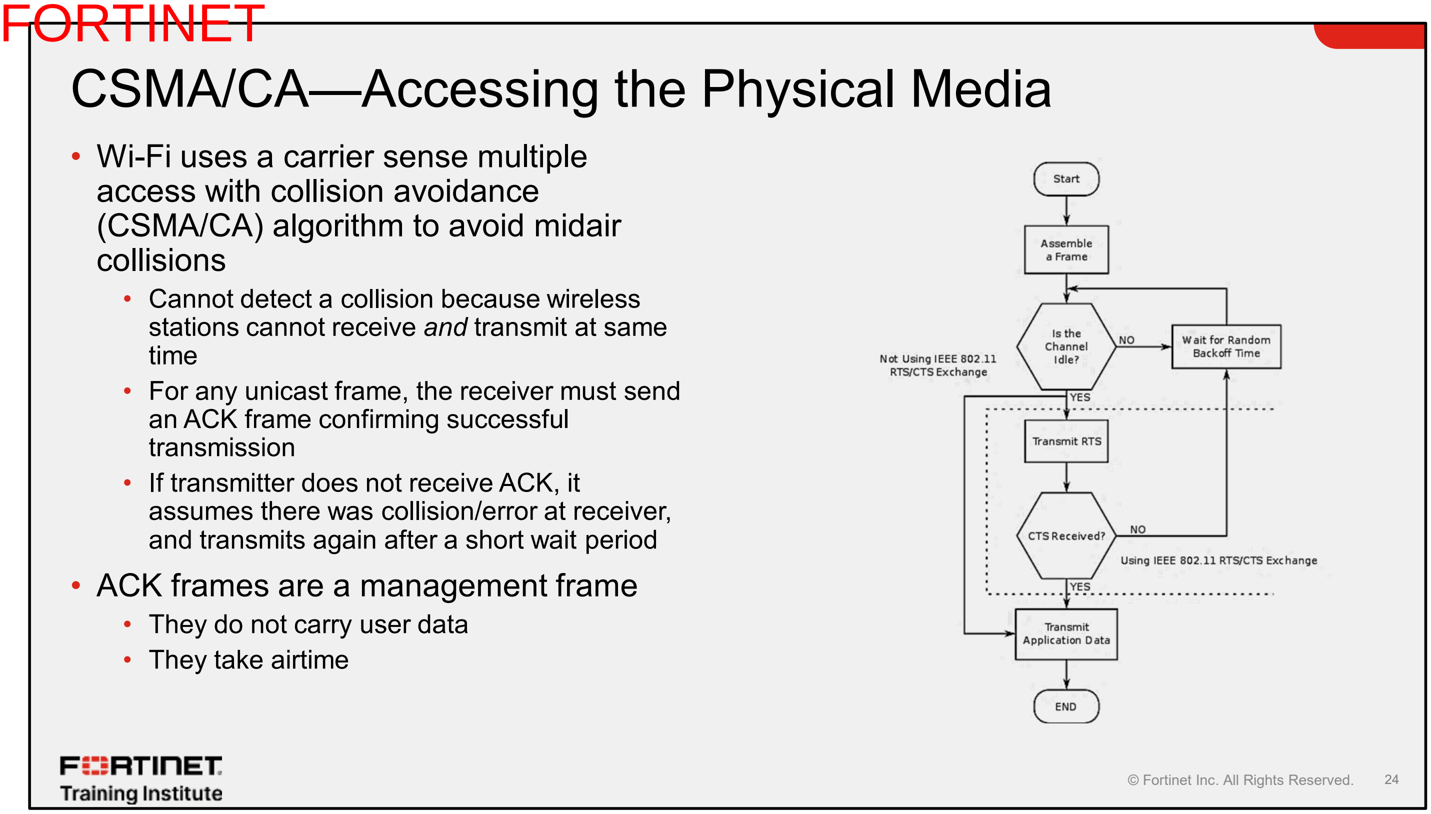
23

Wireless isn't like copper wires or optical cables, where you know only two devices might be talking: one at each end. *Space is a medium shared by all wireless devices.* So devices need a way to avoid destroying each other's signals.

Wi-Fi works like a walkie-talkie—only one party can communicate at a time. All devices running on the same channel *must* take turns and transfer data, one by one.

If two radios do transmit at the same time, this is called a collision. The data contained in the two transmissions is usually corrupted.

To prevent collisions and to achieve an acceptable throughput, Wi-Fi uses the CSMA/CA algorithm. You will explore that next.



CSMA/CA—Accessing the Physical Media

- Wi-Fi uses a carrier sense multiple access with collision avoidance (CSMA/CA) algorithm to avoid midair collisions
  - Cannot detect a collision because wireless stations cannot receive *and* transmit at same time
  - For any unicast frame, the receiver must send an ACK frame confirming successful transmission
  - If transmitter does not receive ACK, it assumes there was collision/error at receiver, and transmits again after a short wait period
- ACK frames are a management frame
  - They do not carry user data
  - They take airtime

Start
Assemble a Frame
Is the Channel Idle?
NO
Wait for Random Backoff Time
Not Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit RTS
CTS Received?
NO
Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit Application Data
END

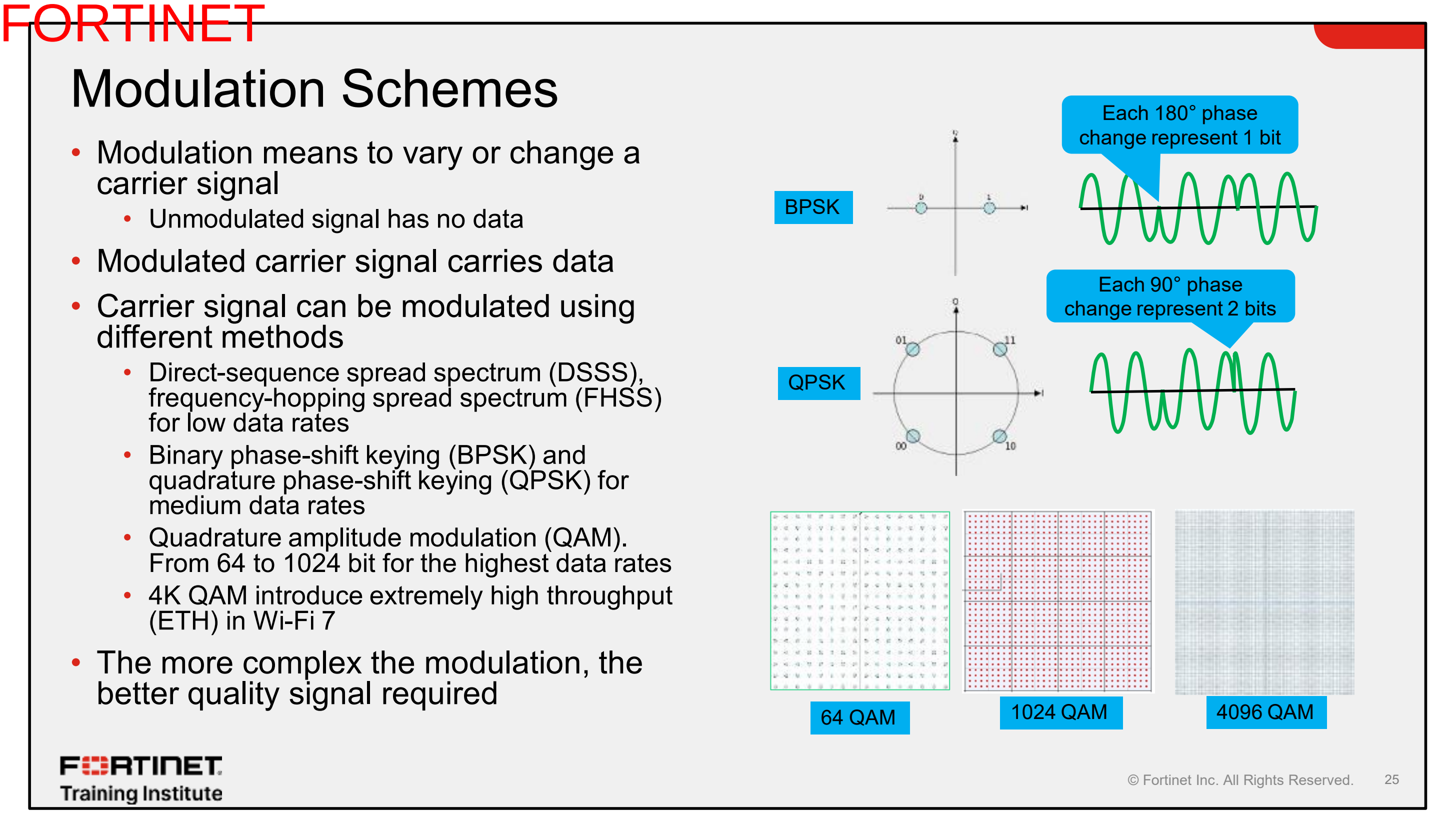
You may be wondering how wireless compares with copper wire Ethernet networks. *Carrier sense multiple access with collision detection (CSMA/CD) is used by Ethernet networks, and CSMA/CA is used by wireless networks.*

Stations using either access method must first listen to hear whether any other device is transmitting and wait until the medium is available—carrier sense (CS) and multiple access (MA).

The key difference between CSMA/CD and CSMA/CA exists at the point when a client wants to transmit and no other clients are presently transmitting.

A CSMA/CD node can immediately begin transmitting. If a collision occurs while a CSMA/CD node is transmitting, the collision will be detected and the node will temporarily stop transmitting.

Wireless devices can’t transmit and receive at the same time, so they cannot detect a collision during transmission. For this reason, wireless networks use CSMA/CA instead of CSMA/CD—they can’t *detect*, so they try to *avoid* collisions.



Modulation Schemes

- Modulation means to vary or change a carrier signal
  - Unmodulated signal has no data
- Modulated carrier signal carries data
- Carrier signal can be modulated using different methods
  - Direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS) for low data rates
  - Binary phase-shift keying (BPSK) and quadrature phase-shift keying (QPSK) for medium data rates
  - Quadrature amplitude modulation (QAM). From 64 to 1024 bit for the highest data rates
  - 4K QAM introduce extremely high throughput (ETH) in Wi-Fi 7
- The more complex the modulation, the better quality signal required

BPSK

Each 180° phase change represent 1 bit

QPSK

Each 90° phase change represent 2 bits

64 QAM

1024 QAM

4096 QAM

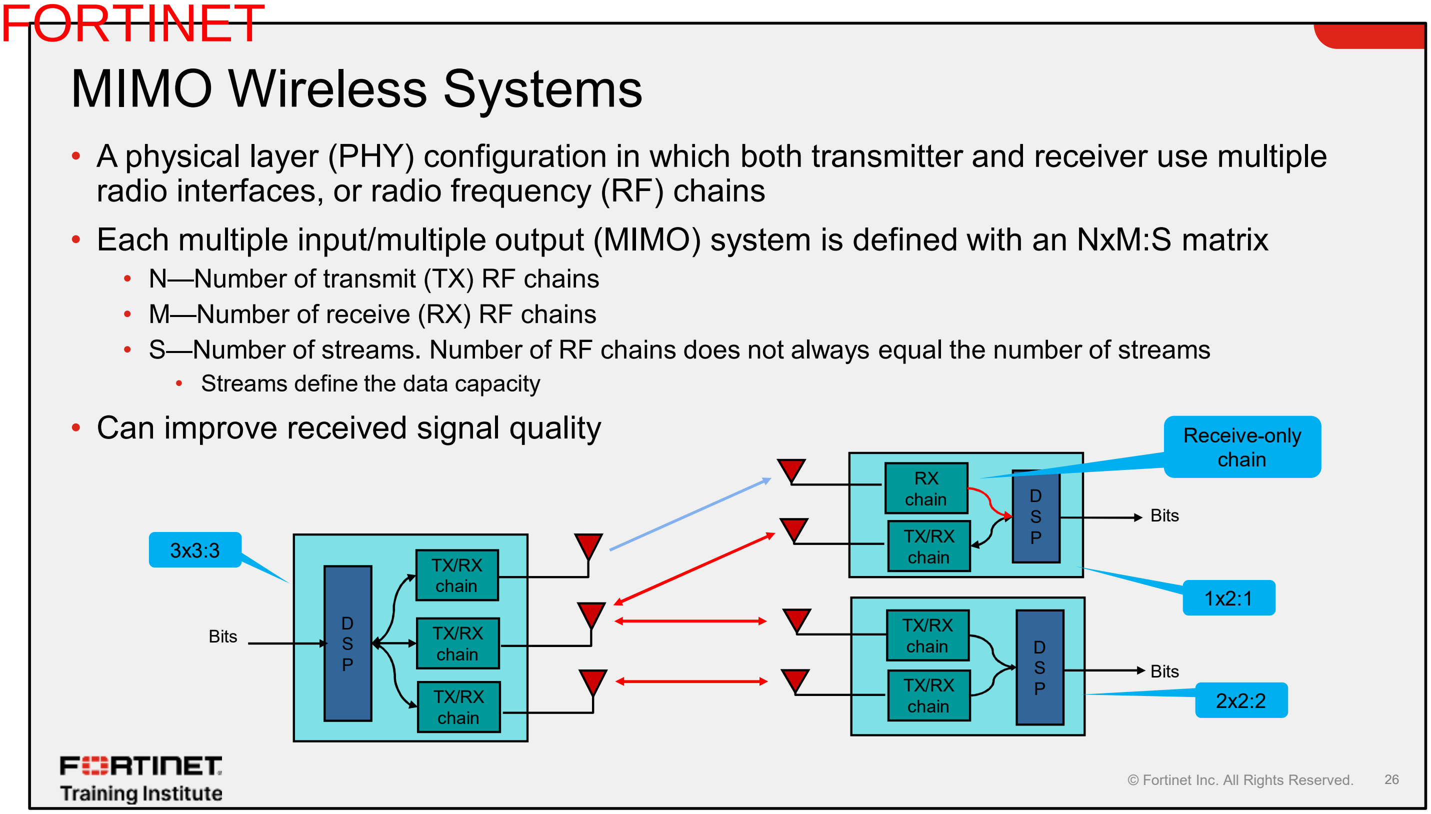
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

Modulation is the process of changing the wave (carrier) with a signal that encodes the information. It’s the radio binary equivalent of morse code. Analog messages, such as voice, can be modulated over an analog carrier using: amplitude modulation (AM) and frequency modulation (FM). These are the most basic signal modulations in use for over a hundred years in radio technology.

Wireless LAN technologies use many more complex technologies, depending on the wireless standards used and the signal quality. The first 801.11 standards use DSSS or FHSS. These methods modulate the data using GFSK, DBPSK, or DQPSK. These older standards enabled data rates of between 1 Mbps and 11 Mbps.

The later 802.11a and 802.11g standards introduced a different method of utilizing the wireless channel, and use two broadly similar modulation methods. Binary phase-shift keying (BPSK) and quadrature phase-shift keying (QPSK) allowed the coding on binary bits by changing the phase of the waveform. By offsetting/changing the wave phase by 180°, it's possible to encode a 0 or a 1 bit. By offsetting/changing the wave phase by 90°, four bits of data (or symbols) can be represented: 00,01,10,11. Later wireless standards use quadrature amplitude modulation (QAM). This adds another modification of wave amplitude, along with the phase. Each modulation of the signal is known as a symbol. Each symbol can represent a sequence of binary bits. The number of binary bits that can be represented depends on the size of QAM. 16 bit QAM is the smallest constellation supported. The constellation is a diagram that shows the number of points that wave will modulate to, a 16 bit QAM has 16 points, each representing a string of binary. The highest form for 802.11ax is 1024 bits. Each increase in QAM level requires an increase in modulation accuracy. The highest forms of QAM require a very high SnR and a strong signal. A full discussion of how modulation works is beyond the scope of this course. The key takeaway is that various modulation schemes used to enable high throughput are highly reliant on signal quality and wireless standards in use.



MIMO Wireless Systems

- A physical layer (PHY) configuration in which both transmitter and receiver use multiple radio interfaces, or radio frequency (RF) chains
- Each multiple input/multiple output (MIMO) system is defined with an NxM:S matrix
  - N—Number of transmit (TX) RF chains
  - M—Number of receive (RX) RF chains
  - S—Number of streams. Number of RF chains does not always equal the number of streams
    - Streams define the data capacity
- Can improve received signal quality

FORTINET Training Institute

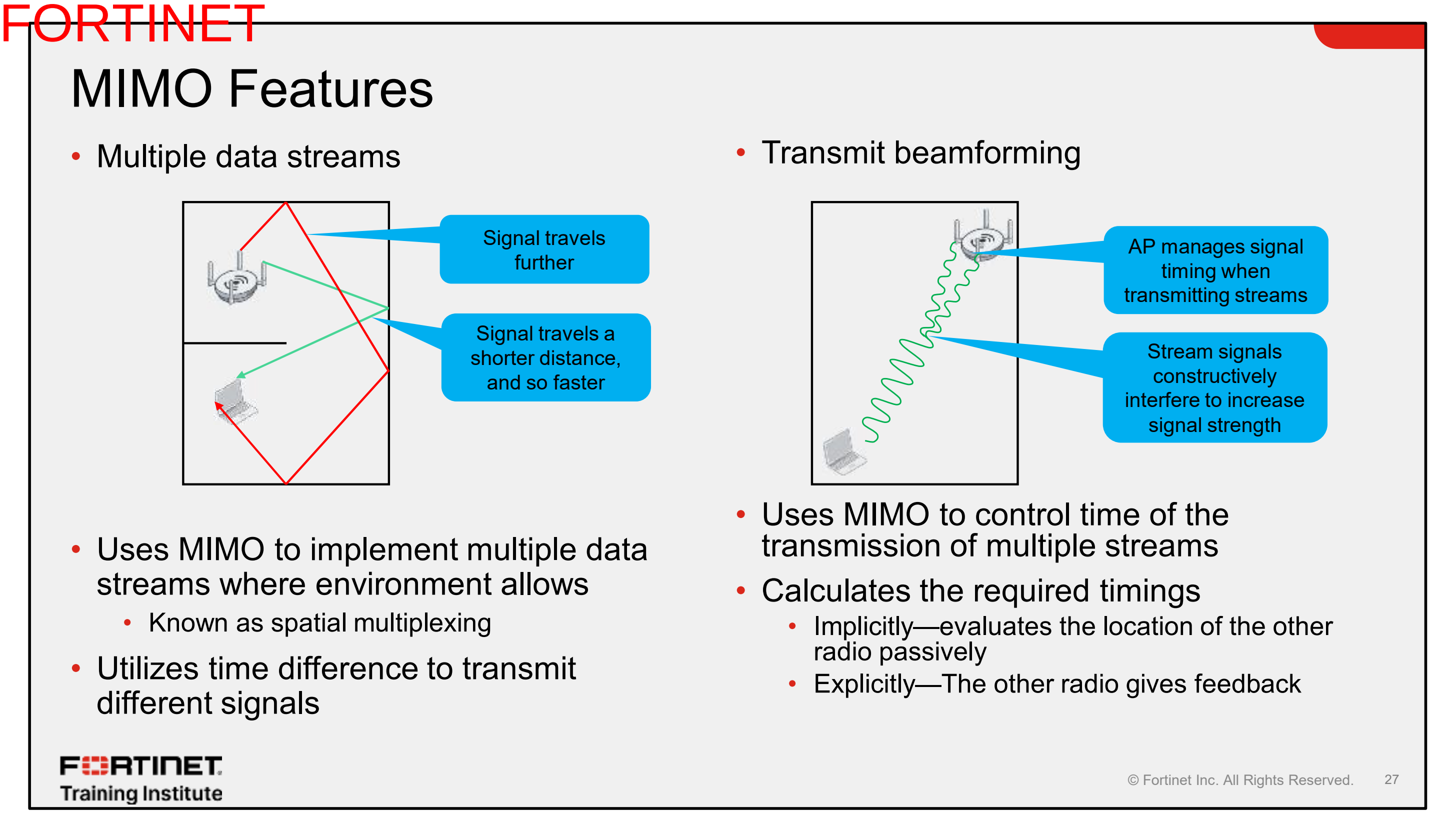
© Fortinet Inc. All Rights Reserved. 26

Older wireless LAN radios consisted of a single digital signal processor (DSP) to perform the modulation. The DSP connects to a single radio, modulating data into a radio wave transmitted through one or two antennas. The original Wi-Fi standards allowed for the use of antenna diversity. This allows the Wi-Fi chipset to use one *or* the other antennas, depending on which one is better placed to receive the signal. When receiving a signal from another radio, it would listen on both antennas. The antenna that had the strongest receive signal would be the one that would be used to transmit back to the other radio.

802.11n allows the use of multiple-input and multiple-output (MIMO) radios. MIMO allows each radio to have multiple subradios or RF chains. Each RF chain consists of a single antenna and enough supporting radio components to allow signal reception and transmission of a stream.

The number of radio chains can vary depending on the wireless standard. The most basic wireless client can have one antenna, one radio chain, and one DSP. This is known as a 1x1:1 client. These are typically used in handheld devices where power consumption is critical, and performance is not a priority, because each RF chain can consume power. 802.11ax hardware has up to eight RF chains. However, these high chain counts are usually found only in AP hardware because of power consumption. Radios with different RF chains and stream counts can communicate with each other. A single RF chain client can easily talk to an eight-RF chain AP. The number of RF chains does not always equal the number of data streams. It is common for AP radios to have three RF chains but only two data streams. It is the number of data streams that determines the quantity of data the radio can transfer. When transmitting or receiving data, the AP chooses the most suitable of the three RF chains to use, not unlike the older antenna diversity mechanism.

The first benefit of multiple RF chains is the ability to use them to receive data better. Maximal ratio combining (MRC) is a type of receive diversity technique where multiple received signals are combined, improving overall signal quality.



MIMO Features

- Multiple data streams

Signal travels further

Signal travels a shorter distance, and so faster

- Uses MIMO to implement multiple data streams where environment allows
  - Known as spatial multiplexing
- Utilizes time difference to transmit different signals

- Transmit beamforming

AP manages signal timing when transmitting streams

Stream signals constructively interfere to increase signal strength

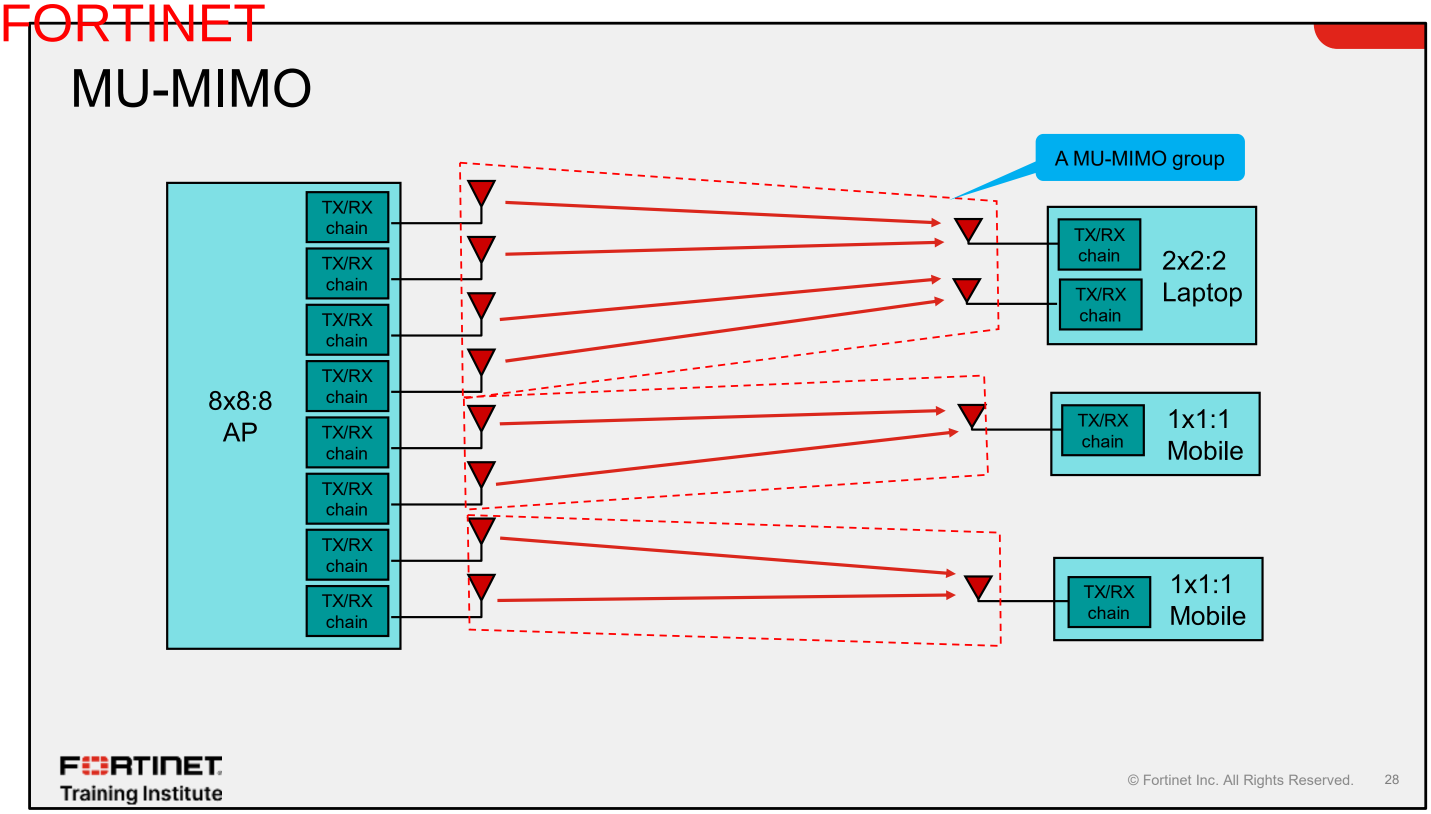
- Uses MIMO to control time of the transmission of multiple streams
- Calculates the required timings
  - Implicitly—evaluates the location of the other radio passively
  - Explicitly—The other radio gives feedback

FERTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

MIMO is utilized to provide other benefits as well. Alongside the increased radio sensitivity enabled by maximal ratio combining (MRC), it is also possible to increase data throughput using multiple streams. Radio waves can be reflected or refracted by objects. Walls, cabinets, and other solid objects commonly found in offices can cause multiple reflections. This causes the signal to bounce around and to travel further, before reaching the receive radio. Because the signal has traveled further, it takes longer. This causes the same wave form to be received at the radio, but slightly out of sync, resulting in destructive interference. For older standard wireless radios, this is a problem, but for newer MIMO standard clients, it is an opportunity. Where a MIMO radio detects multiple signals arriving at a radio, rather than send the same signal and receive multiple copies, it can choose to send different copies of data using the different signal path options. More reflections mean more path options, meaning more opportunities to send different data streams. The stream negotiation happens automatically as part of normal management traffic and is known as spatial multiplexing.

MIMO can also be used to improve the transmission signal. By controlling the timing of signals transmitted from multiple radio chains, MIMO can use the resulting constructive interference to increase a signal's amplitude for a specific client. Carefully controlling the phase of the signals transmitted from multiple antennas has the effect of emulating a directional antenna. This is known as beamforming. Transmit beamforming is part of the 802.11n standard and further enhanced in 802.11ac. Initially, the sending radio would gather information about implicitly. The beaming forming radio would take numerous measurements of the target radio when it received data. It would approximate the other client's location from the difference in timing of the received signals. It would then have an idea of where the radio is and form a beam to it. This is a passive process, not requiring the target radio to be aware of the beam. Explicit beamforming requires the other radio to be aware of the beamforming event and allows more accurate calculations. 802.11ac/ax mandates explicit beamforming, and the resultant beamform performance is better than achieved with the initial 802.11n implementation. Both spatial multiplexing and beamforming *could* be used at the same time.



MU-MIMO

A MU-MIMO group

8x8:8
AP

TX/RX chain
TX/RX chain
TX/RX chain
TX/RX chain
TX/RX chain
TX/RX chain
TX/RX chain
TX/RX chain

TX/RX chain
TX/RX chain
2x2:2
Laptop

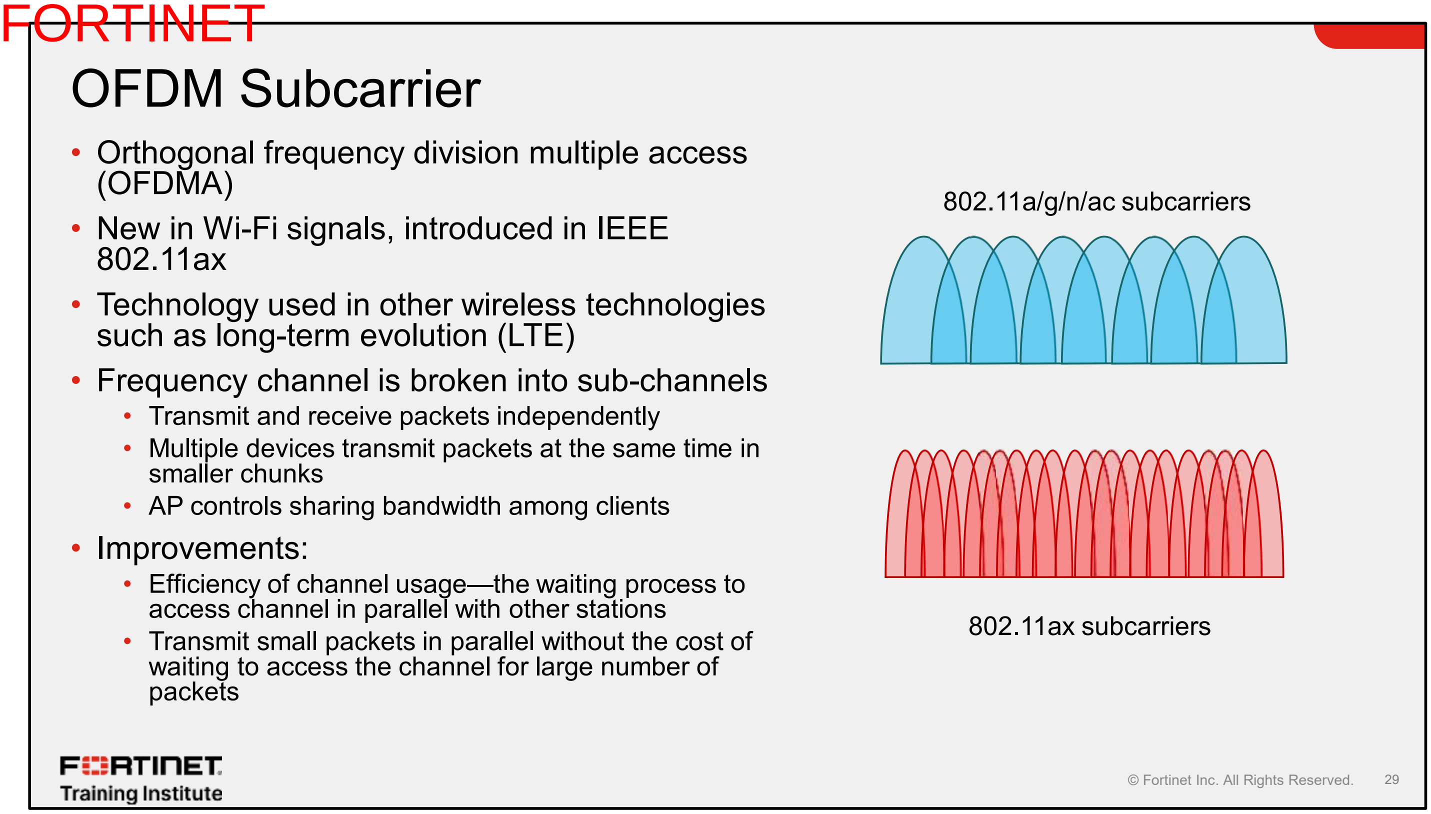
TX/RX chain
1x1:1
Mobile

TX/RX chain
1x1:1
Mobile

The second revision (wave 2) of the 802.11ac standard introduces the ability to use MIMO to transmit to multiple clients simultaneously. The enhancement is known as MU-MIMO, or multiuser MIMO. Older standards only supported radios communicating with one other radio at a time. MIMO allows the *simultaneous* use of multiple RF chains to talk to up to four other radios. The new 802.11ax is proposing to extend that number to eight. Wave 2 802.11ac restricts the multi-user ability to AP to client transmission, known as downstream or downlink MU-MIMO. The later 802.11ax standard introduces the ability for APs to *receive* simultaneous, multiple transmissions from clients, known as uplink or upstream MU-MIMO.

MU-MIMO uses explicit beamforming of *groups* of RF chains to form a signal targeted to a specific client. At the same time, the AP uses other RF chains to create beamform groups for other clients. All the clients will hear *all* the transmissions, but because its own signal group is beamformed, it receives a stronger signal. This allows the client to decode the data successfully, even though there are other, interfering signals being transmitted at the same time. Uplink MU-MIMO extends the system further to allow upstream transmissions to be received simultaneously.

APs have different MU-MIMO abilities that depend on the number of RF chains and MU-MIMO groups they can create. The AP dynamically decides how many RF chains to use and how many groups to make. It does this by exchanging sounding frames with the clients that establish the client's capability and location. The data transferred to the clients also matters. MU-MIMO transmissions are simultaneous and depend on suitable data buffered at the AP for transmission. The complex sounding and coordination mechanism make it resource-intensive and time-consuming to transmit data in this way. Clients are often located close to each other. This makes the beamforming less effective at reducing interference. Often, MU-MIMO does not result in a big uplift in performance and can decrease performance because of the increased management traffic required. As a result, in some scenarios, it may be beneficial to disable MU-MIMO.



OFDM Subcarrier

- Orthogonal frequency division multiple access (OFDMA)
- New in Wi-Fi signals, introduced in IEEE 802.11ax
- Technology used in other wireless technologies such as long-term evolution (LTE)
- Frequency channel is broken into sub-channels
  - Transmit and receive packets independently
  - Multiple devices transmit packets at the same time in smaller chunks
  - AP controls sharing bandwidth among clients
- Improvements:
  - Efficiency of channel usage—the waiting process to access channel in parallel with other stations
  - Transmit small packets in parallel without the cost of waiting to access the channel for large number of packets

802.11a/g/n/ac subcarriers

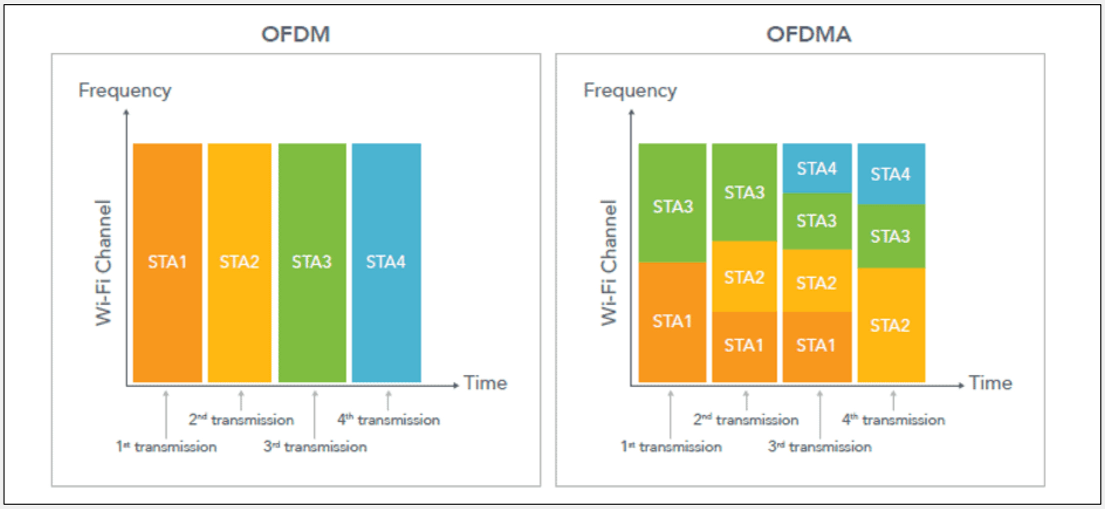
802.11ax subcarriers

FORTINET Training Institute

29

OFDMA is subcarrier technology that has been used in LTE for years now but is new to Wi-Fi. It breaks the given channel down into sub-channels which can then be used to transmit and receive packets independently. The practical upshot of this is that multiple devices can be transmitting their packets at the same time using smaller chunks of the overall available channel bandwidth. The AP is in control of who is able to use what amount of bandwidth. This can improve the overall efficiency of channel usage by allowing the process of waiting for channel access to be parallelized for multiple stations. It can be a particular benefit for large numbers of small packets, allowing lots of these small packets to be transmitted in parallel without paying large numbers of channel access wait time penalties.

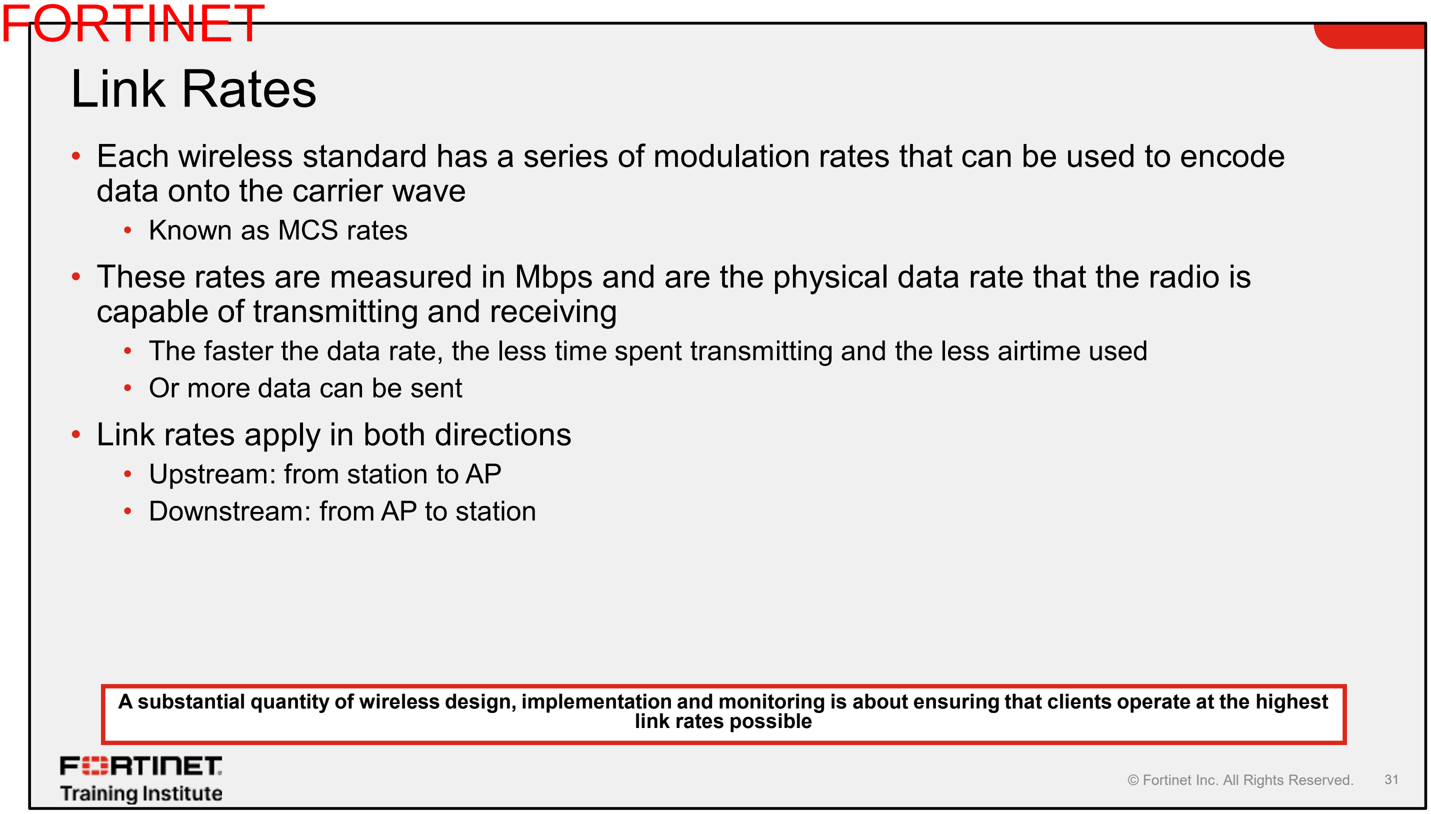
OFDM and OFDMA Subcarriers



Training Institute

30

OFDMA expands on OFDM technology by allowing transmission of small packets by multiple devices simultaneously. In OFDM, each devices must transmit packets in sequence. However, with OFDMA, devices that are transmitting smaller packets can use the subchannel to send and receive packets. As shown on this slide, OFDMA divides the available bandwidth into subchannels, which allows transmission of packets from user1 and user3 in parallel. This results in better performance because of decreased wait time and the ability to use the transmission medium more effectively.



Link Rates

- Each wireless standard has a series of modulation rates that can be used to encode data onto the carrier wave
  - Known as MCS rates
- These rates are measured in Mbps and are the physical data rate that the radio is capable of transmitting and receiving
  - The faster the data rate, the less time spent transmitting and the less airtime used
  - Or more data can be sent
- Link rates apply in both directions
  - Upstream: from station to AP
  - Downstream: from AP to station

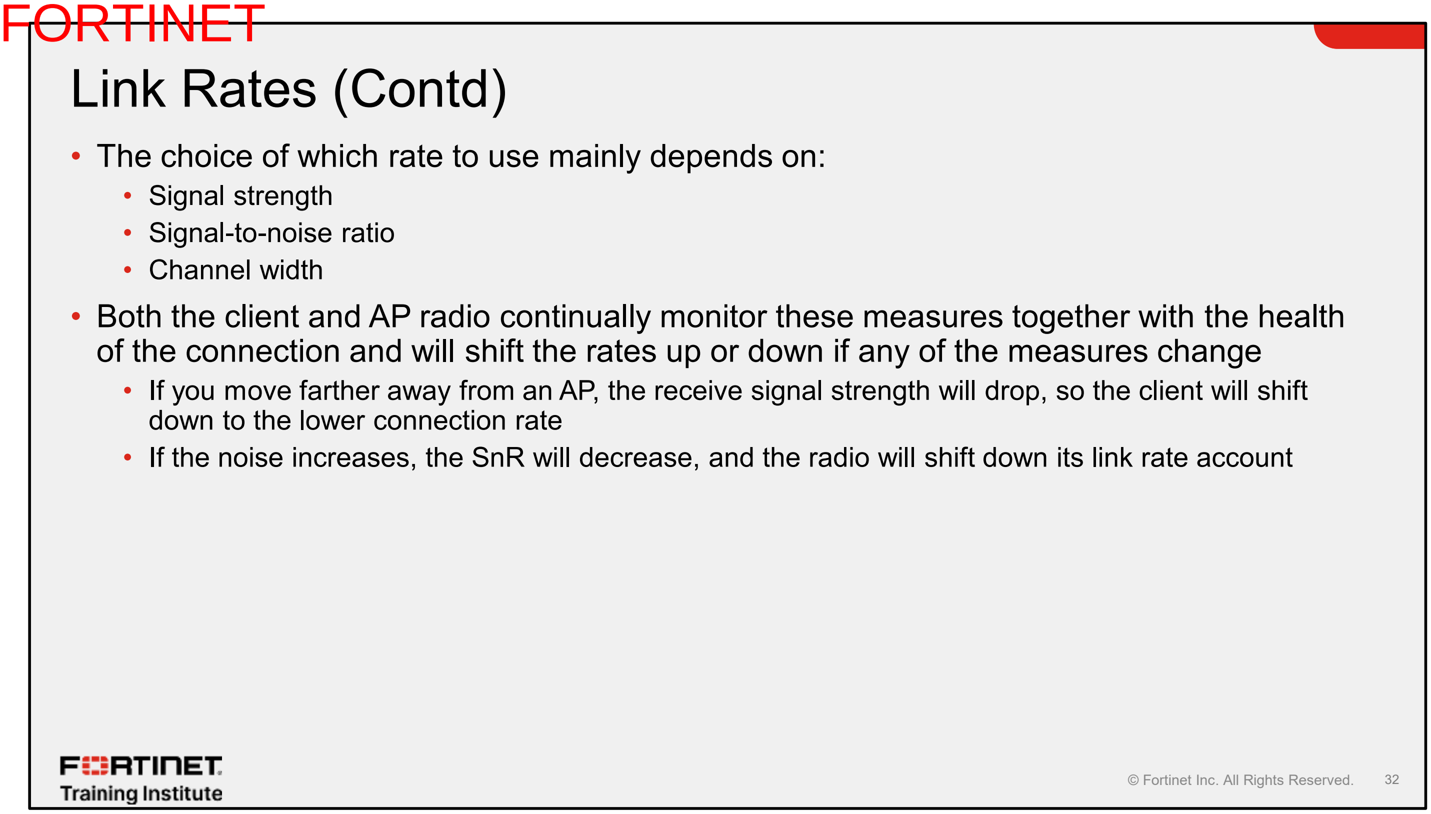
A substantial quantity of wireless design, implementation and monitoring is about ensuring that clients operate at the highest link rates possible

31

The properties of wireless signals, such as signal strength, noise, and bandwidth, affect the reliability and speed of the wireless network.

Link rates, also known as MCS rates, are used to assess this reliability and speed and are defined as part of the wireless standards. Link rates define the quantity of data that can be encoded and modulated onto a signal at any given time. The higher the link rate, the less time that is spent transmitting data and the more data that can be sent in any given time period.

Transmissions in each direction have a link rate—one link rate from the AP to the station, and one from the station to the AP. Both the station and the AP will negotiate a link rate based upon the health of the connection. The connection health is measured using the received signal strength of the other radio, the signal-to-noise ratio, and the channel width in use. There are other factors to take into account, but these are the main ones.



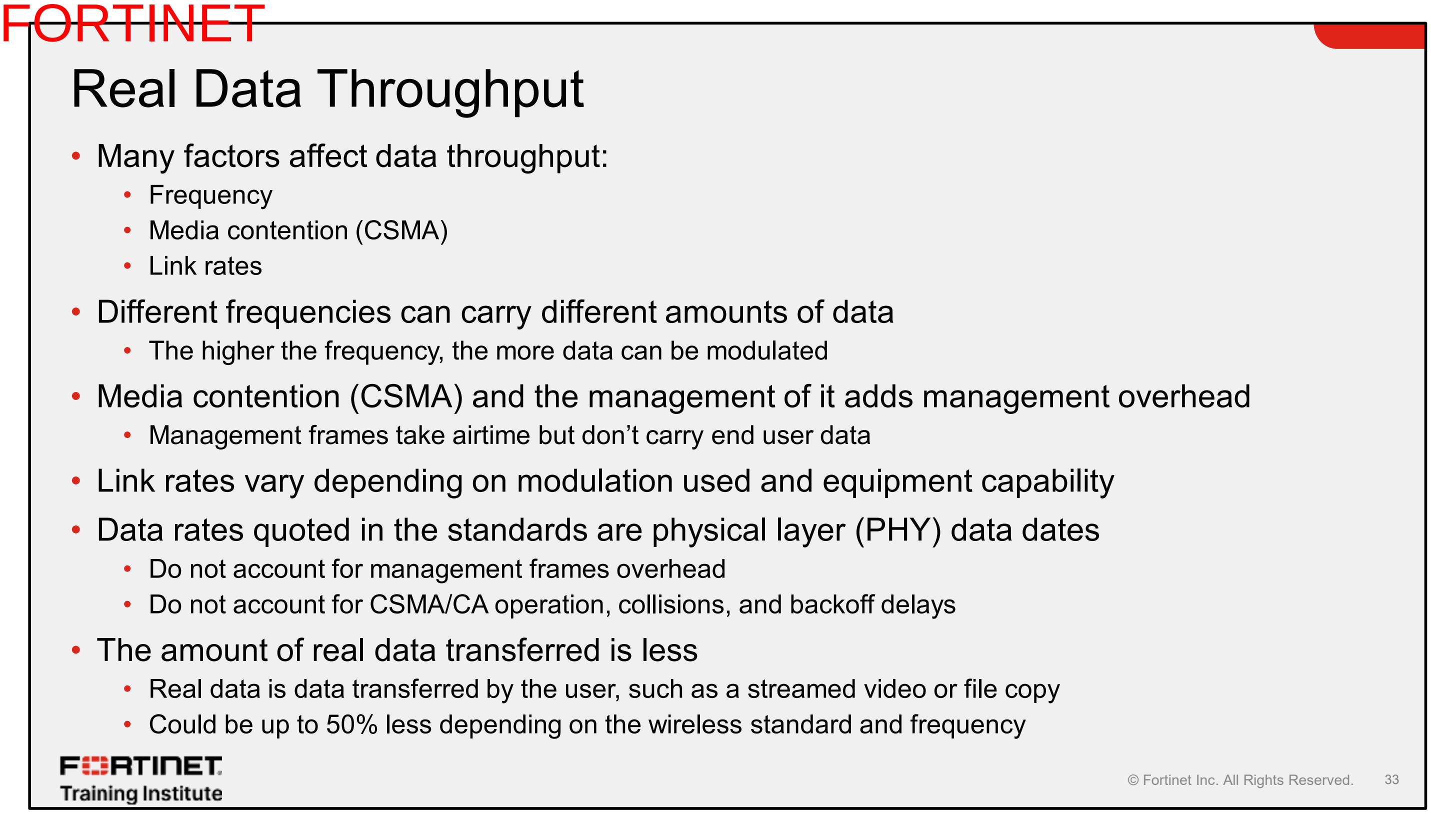
Link Rates (Contd)

- The choice of which rate to use mainly depends on:
  - Signal strength
  - Signal-to-noise ratio
  - Channel width
- Both the client and AP radio continually monitor these measures together with the health of the connection and will shift the rates up or down if any of the measures change
  - If you move farther away from an AP, the receive signal strength will drop, so the client will shift down to the lower connection rate
  - If the noise increases, the SnR will decrease, and the radio will shift down its link rate account

Each radio will attempt to use the highest link rate that conditions allow; however, both radios will continually monitor the link rates and, if the health of the connection changes, shift their link rates up or down. For example, if the station moves farther away from an AP, the client will measure the reduction in AP signal strength and reduce its link rates accordingly.

Likewise, if the noise floor increases for any reason, the signal-to-noise ratio will decrease, resulting in the radios involved reducing their link rates.

A major part of wireless design, implementation, and monitoring is ensuring that your clients achieve the highest link rates possible.



Real Data Throughput

- Many factors affect data throughput:
  - Frequency
  - Media contention (CSMA)
  - Link rates
- Different frequencies can carry different amounts of data
  - The higher the frequency, the more data can be modulated
- Media contention (CSMA) and the management of it adds management overhead
  - Management frames take airtime but don’t carry end user data
- Link rates vary depending on modulation used and equipment capability
- Data rates quoted in the standards are physical layer (PHY) data dates
  - Do not account for management frames overhead
  - Do not account for CSMA/CA operation, collisions, and backoff delays
- The amount of real data transferred is less
  - Real data is data transferred by the user, such as a streamed video or file copy
  - Could be up to 50% less depending on the wireless standard and frequency

FORTINET Training Institute

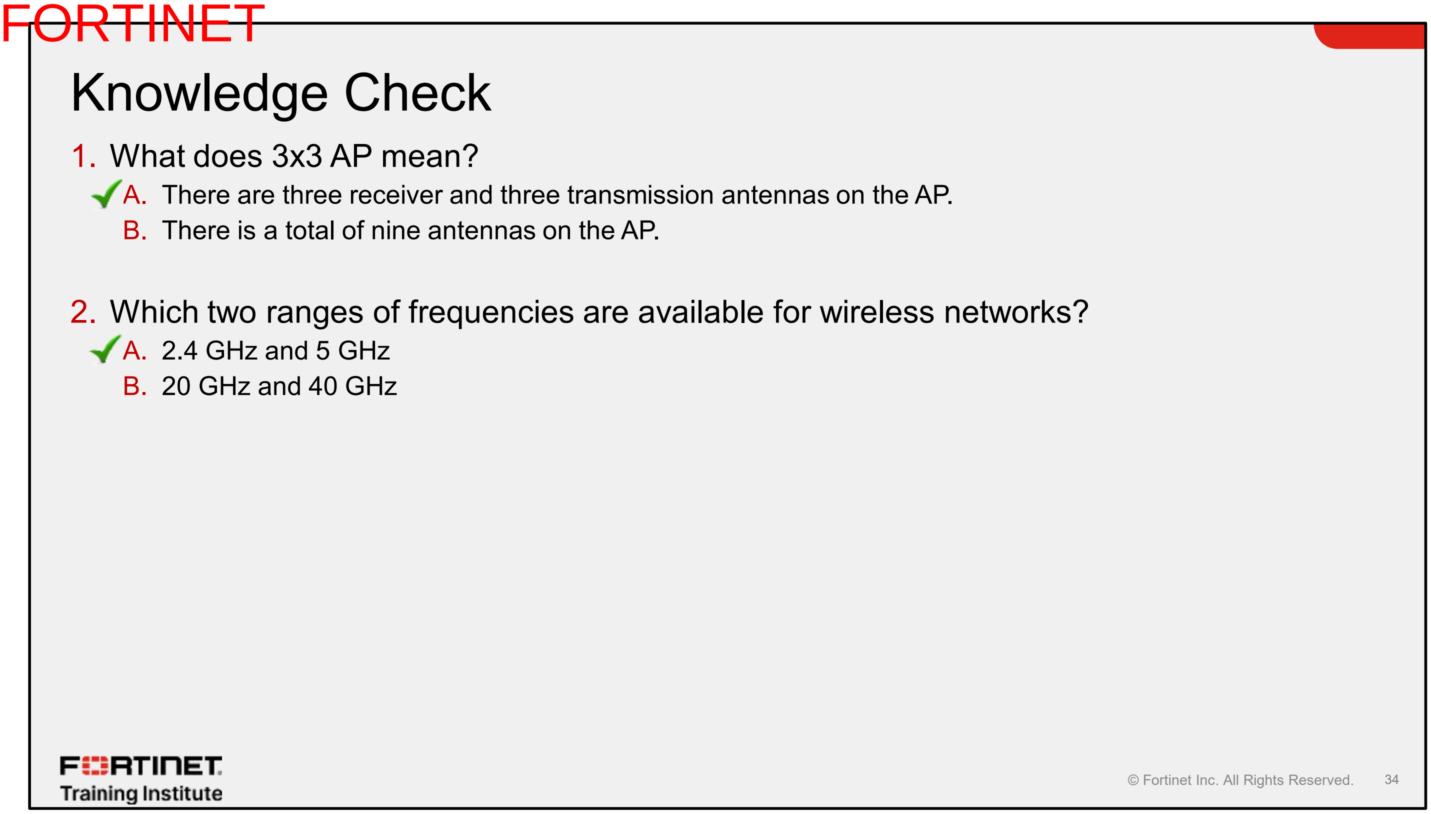
© Fortinet Inc. All Rights Reserved. 33

The frequency bandwidth, data encoding, modulation, medium contention, encryption, and many other factors play a large part in the data throughput.

Because of the half-duplex nature of the medium, the overhead generated by CSMA/CA, and the actual aggregate throughput, is typically 50 percent, or less, of the data rate.

In short, the Wi-Fi medium is a shared medium where collisions must be avoided. Because of this, throughput is an aggregate throughput.

The throughput figures quoted as part of the wireless standard do not represent the *real* data throughput, which would be the rate at which you could, for example, copy a file across a wireless link. The numbers quoted on this slide, and on the specification sheets of wireless equipment, specify the physical layer (PHY) throughput number. Wireless transmission involves a lot of administration and management traffic and processes to make the wireless link work successfully. As a result, some of the headline capacity quoted here is always used for management frames and is not available for carrying real data. These PHY numbers also vary based on the capability of the wireless equipment. Not all APs and clients are created equal in terms of radio capacity.

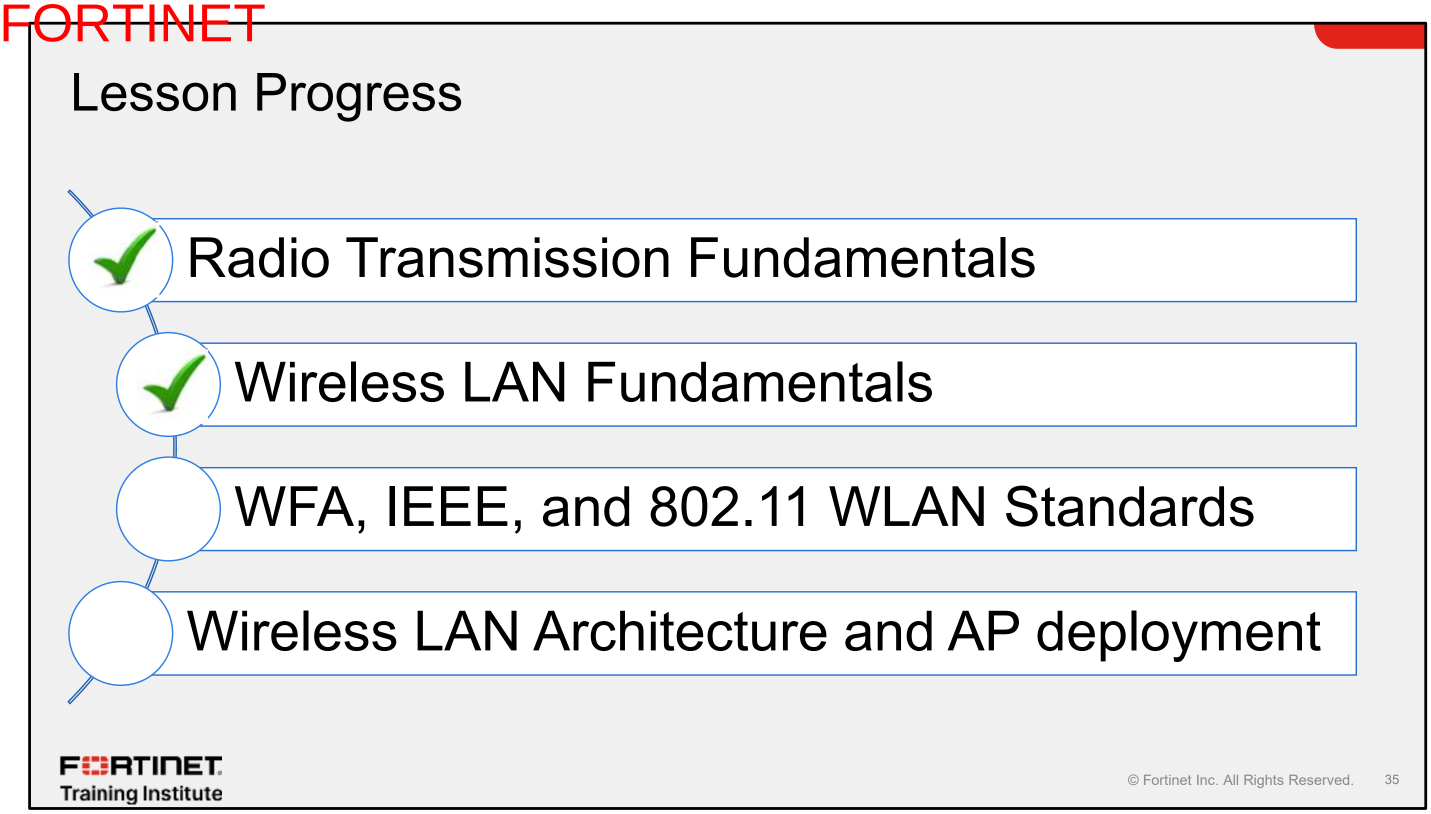


Knowledge Check

1. What does 3x3 AP mean?
   - ✓ A. There are three receiver and three transmission antennas on the AP.
   - B. There is a total of nine antennas on the AP.

2. Which two ranges of frequencies are available for wireless networks?
   - ✓ A. 2.4 GHz and 5 GHz
   - B. 20 GHz and 40 GHz

FORTINET
Training Institute

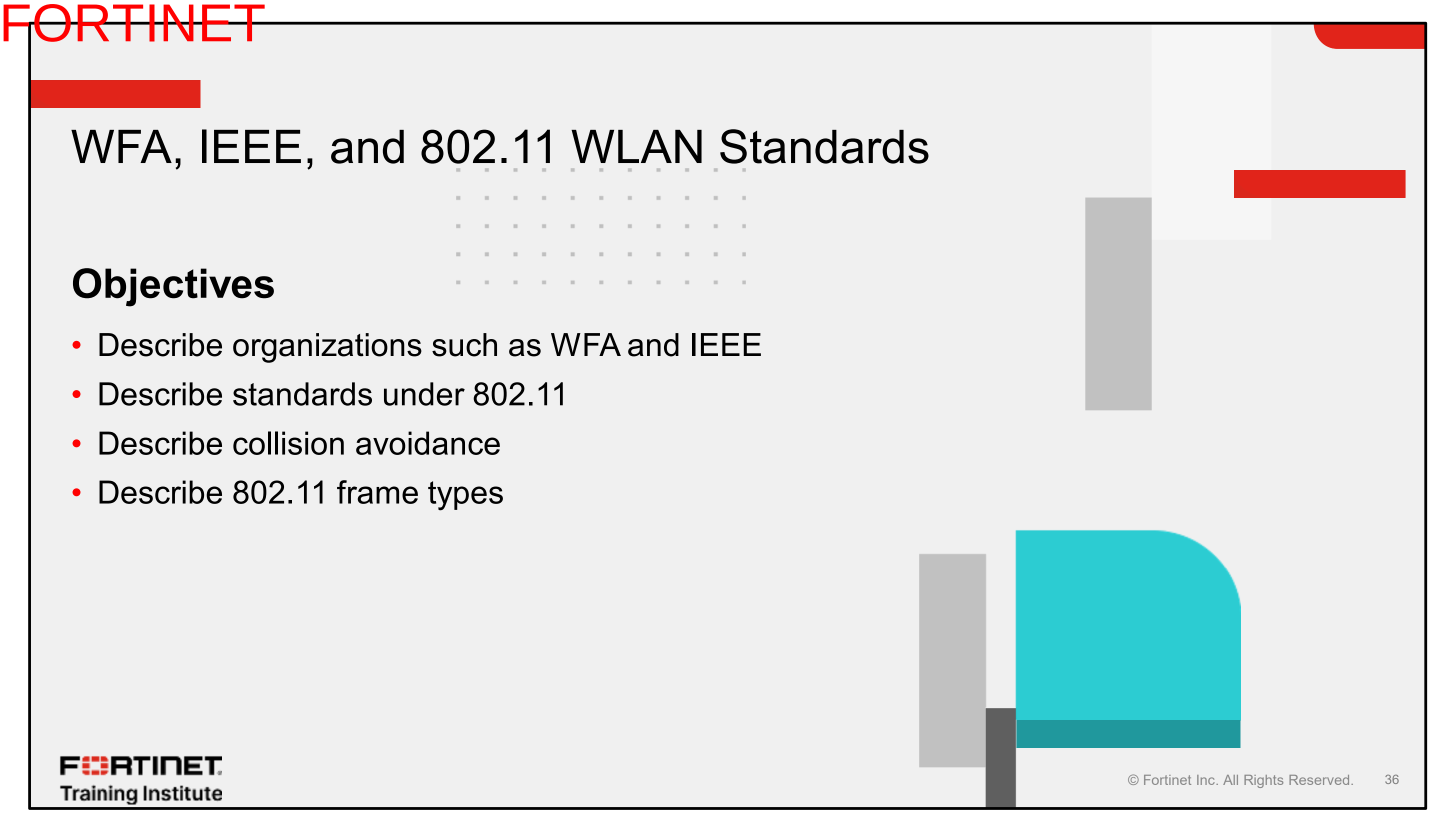


Lesson Progress

- ✓ Radio Transmission Fundamentals
- ✓ Wireless LAN Fundamentals
- WFA, IEEE, and 802.11 WLAN Standards
- Wireless LAN Architecture and AP deployment

Good job! You now understand wireless LAN fundamentals.

Now, you will learn about 802.11 Wi-Fi standards.



WFA, IEEE, and 802.11 WLAN Standards

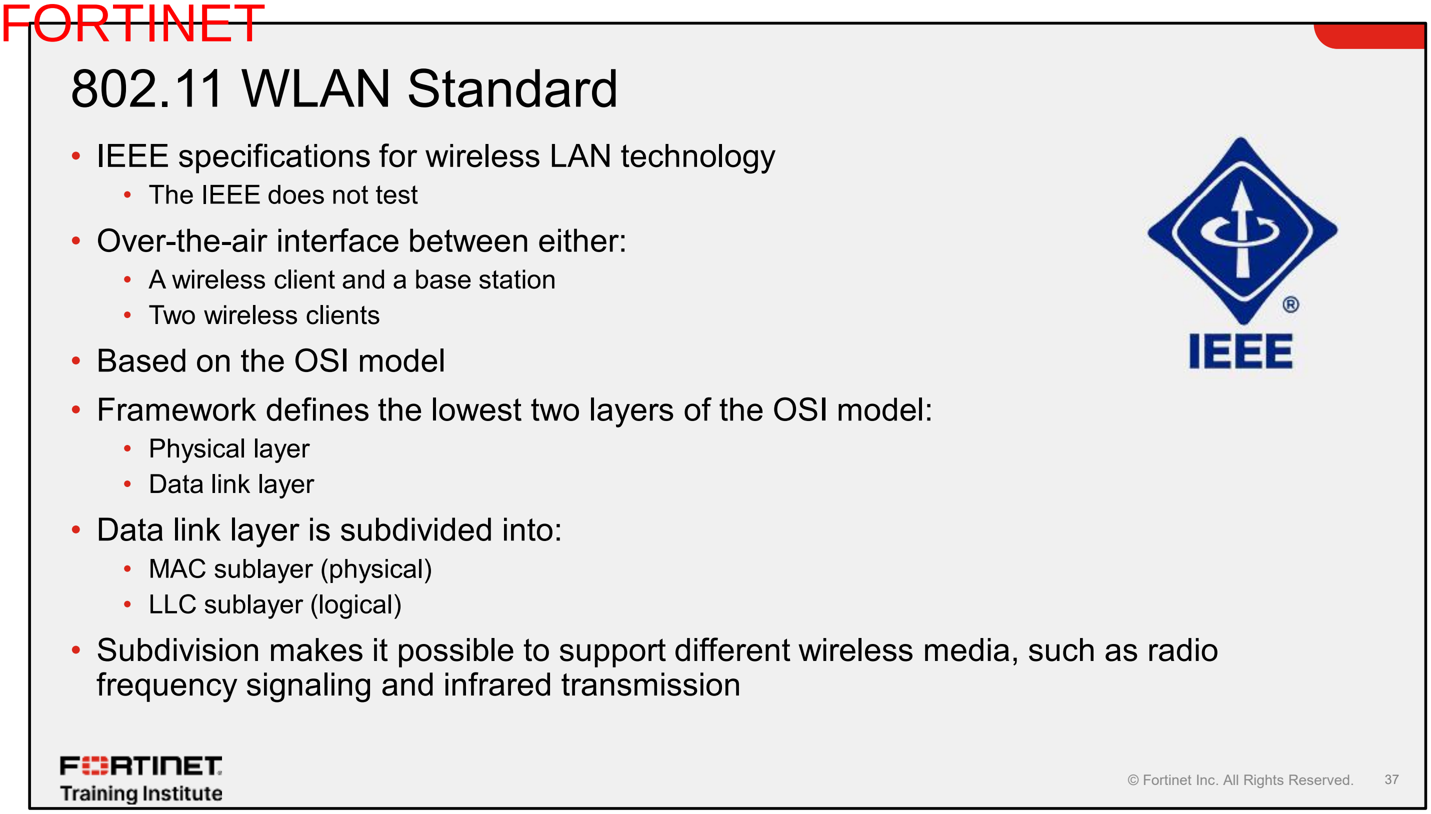
Objectives

- Describe organizations such as WFA and IEEE
- Describe standards under 802.11
- Describe collision avoidance
- Describe 802.11 frame types

36

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in WFA, IEEE, and 802.11 WLAN standards, you will be able to describe 802.11 standards.



802.11 WLAN Standard

- IEEE specifications for wireless LAN technology
  - The IEEE does not test
- Over-the-air interface between either:
  - A wireless client and a base station
  - Two wireless clients
- Based on the OSI model
- Framework defines the lowest two layers of the OSI model:
  - Physical layer
  - Data link layer
- Data link layer is subdivided into:
  - MAC sublayer (physical)
  - LLC sublayer (logical)
- Subdivision makes it possible to support different wireless media, such as radio frequency signaling and infrared transmission

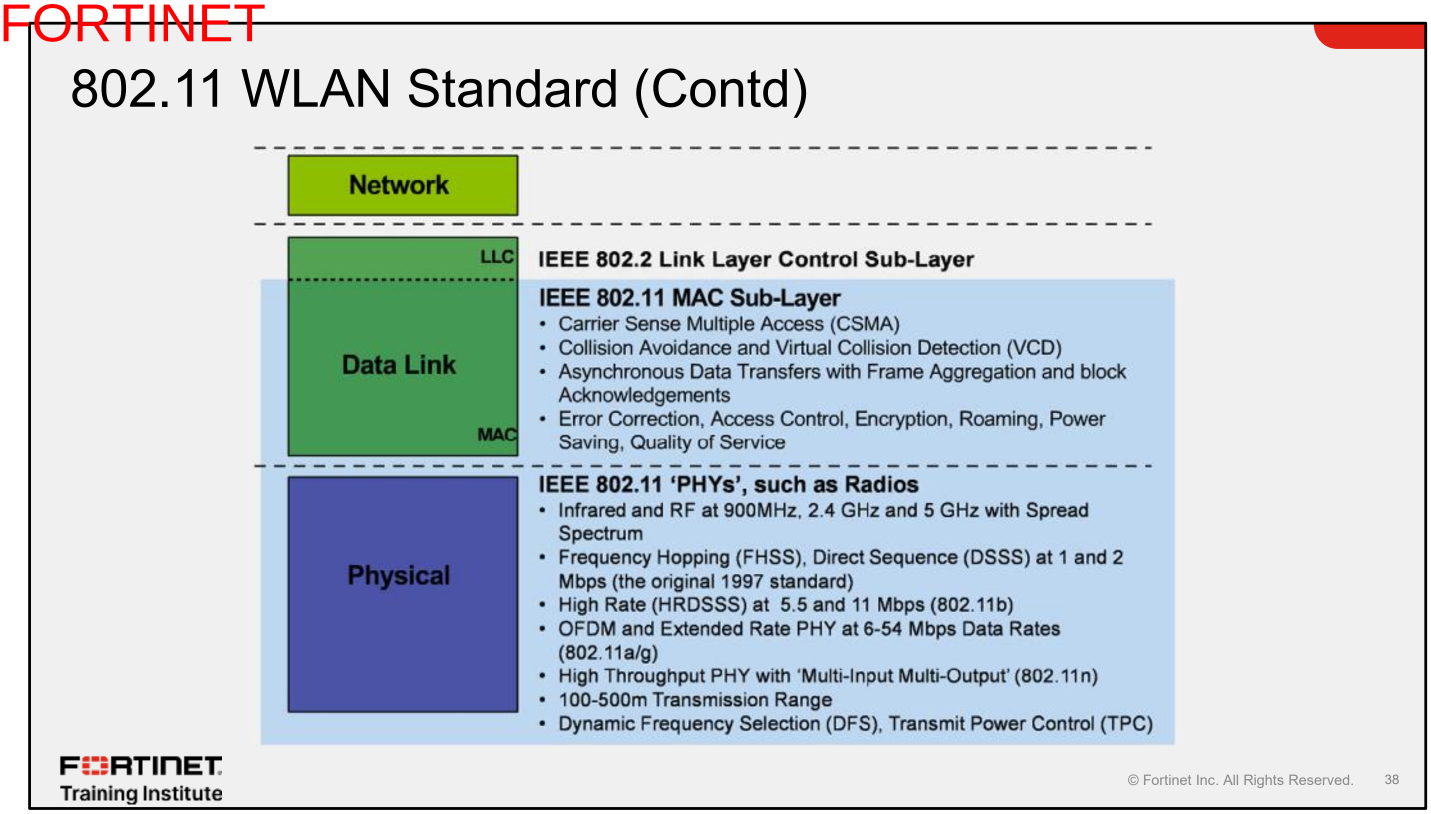
FORTINET Training Institute

37

The IEEE 802.11 standard was developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless LAN technology and describes an over-the-air interface between a wireless client and a base station, or between two wireless clients.

The 802.11 framework defines the two lowest layers of the OSI model: physical and data link. The data link layer is further subdivided to support different wireless media.

Now, you will look at the functionality of each layer.



802.11 WLAN Standard (Contd)

IEEE 802.2 Link Layer Control Sub-Layer

IEEE 802.11 MAC Sub-Layer

- Carrier Sense Multiple Access (CSMA)
- Collision Avoidance and Virtual Collision Detection (VCD)
- Asynchronous Data Transfers with Frame Aggregation and block Acknowledgements
- Error Correction, Access Control, Encryption, Roaming, Power Saving, Quality of Service

IEEE 802.11 'PHYs', such as Radios

- Infrared and RF at 900MHz, 2.4 GHz and 5 GHz with Spread Spectrum
- Frequency Hopping (FHSS), Direct Sequence (DSSS) at 1 and 2 Mbps (the original 1997 standard)
- High Rate (HRDSSS) at 5.5 and 11 Mbps (802.11b)
- OFDM and Extended Rate PHY at 6-54 Mbps Data Rates (802.11a/g)
- High Throughput PHY with 'Multi-Input Multi-Output' (802.11n)
- 100-500m Transmission Range
- Dynamic Frequency Selection (DFS), Transmit Power Control (TPC)

FORTINET Training Institute

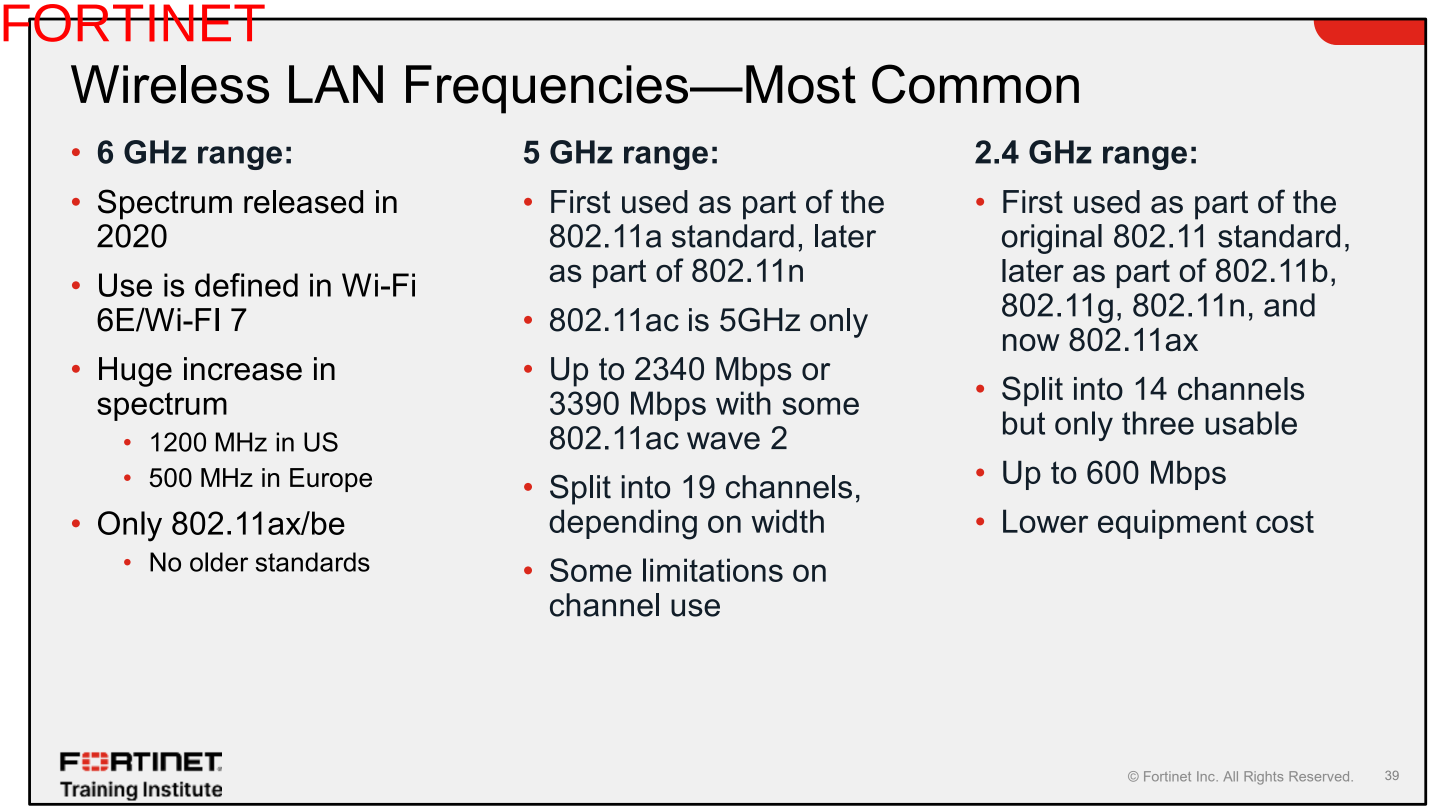
38

The data link layer is subdivided into the MAC and LLC layer in order to support different wireless media at the physical layer, such as radio frequency signaling and infrared transmission. For radio frequency signaling, frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are used. Bluetooth, which is an example of a wireless personal area network (WPAN), uses FHSS; most APs use DSSS.

- Physical layer:
    - In charge of transmission and reception; encodes and decodes signals.
    - The commonly wireless media admitted are infrared (simple and cheap but requires line of sight), radio (FHSS and DSSS), and Bluetooth.

- MAC layer:
    - Coordinates users' access to the transmission medium.
        - On transmission, assembles data into a frame for transmission.
        - On reception, disassembles frame and performs error detection.

- LLC layer:
    - Provides an interface to upper layers; allows flow and error control.



Wireless LAN Frequencies—Most Common

- **6 GHz range:**
- Spectrum released in 2020
- Use is defined in Wi-Fi 6E/Wi-FI 7
- Huge increase in spectrum
  - 1200 MHz in US
  - 500 MHz in Europe
- Only 802.11ax/be
  - No older standards

5 GHz range:

- First used as part of the 802.11a standard, later as part of 802.11n
- 802.11ac is 5GHz only
- Up to 2340 Mbps or 3390 Mbps with some 802.11ac wave 2
- Split into 19 channels, depending on width
- Some limitations on channel use

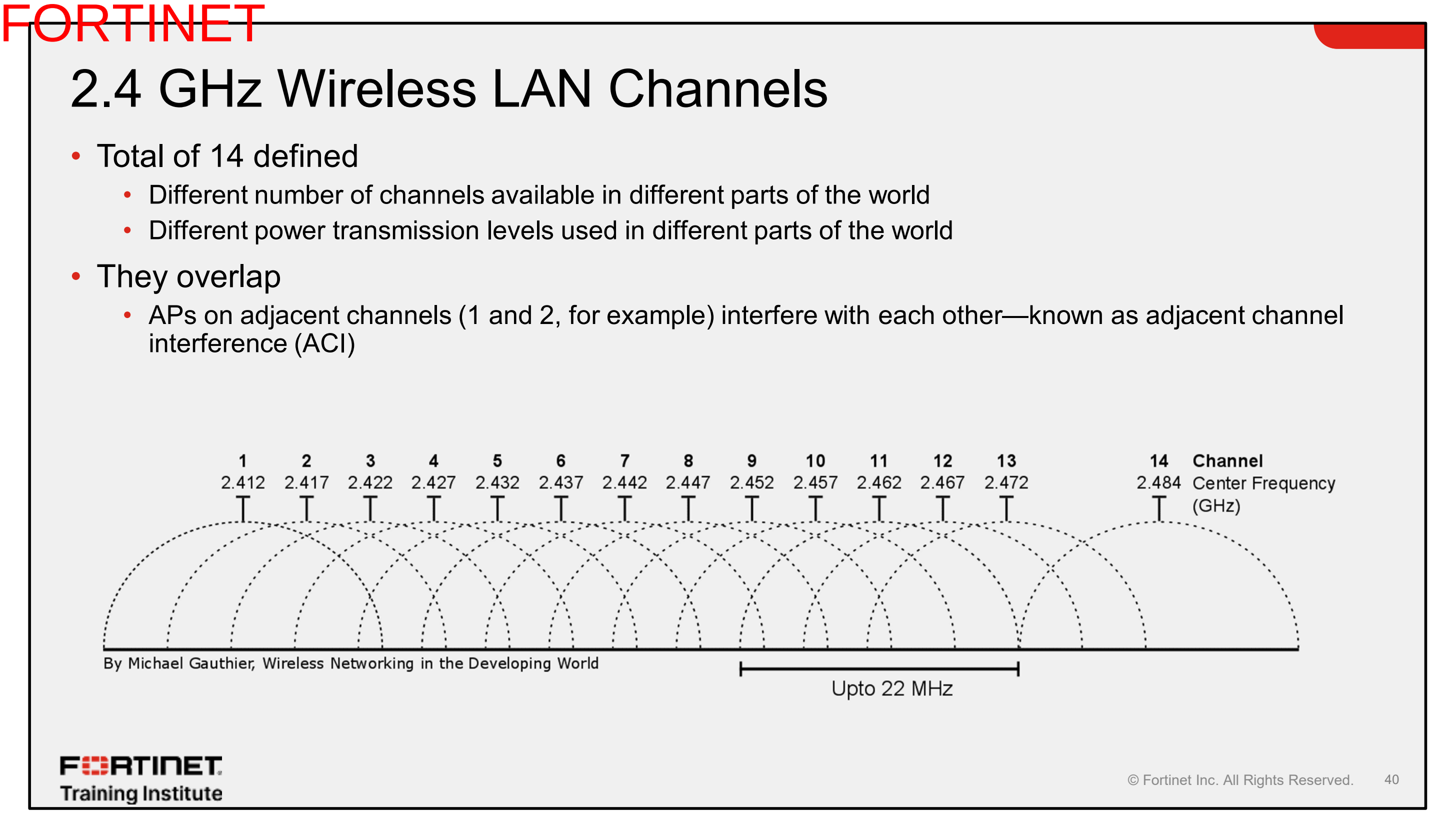
2.4 GHz range:

- First used as part of the original 802.11 standard, later as part of 802.11b, 802.11g, 802.11n, and now 802.11ax
- Split into 14 channels but only three usable
- Up to 600 Mbps
- Lower equipment cost

The most commonly used wireless LAN frequencies across the world are the 2.4 GHz range and the 5 GHz range. The 2.4 GHz range, supported in the 802.11b/g/n standards, was the first and, initially, the most commonly used frequency. It consists of 14 channels of which only three are usable. The amount of bandwidth available on 2.4 GHz is relatively small compared to 5 GHz. The lack of bandwidth combined with the lower frequency means that data rates are limited. The positive side of using 2.4 GHz was that the equipment tended to be cheaper and, as a result, it was more popular during the early days of wireless technology. However, as bandwidth requirements have increased, the lack of channels and capacity means that 2.4 GHz is much less popular today.

Initially, the 5 GHz range was less popular in some parts of the world because of local regulations and the cost of equipment. However, there is more spectrum available for the 5 GHz channels. Combined with the higher frequency, this usually means that the capacity, or throughput, of 5 GHz is much greater than 2.4 GHz. Over the years, the 5 GHz spectrum around the world has been deregulated and released from other purposes, and is increasingly being used for wireless LAN transmission. This means that it is possible to have up to 19 channels available for wireless use, depending on the channel width and global location. As it stands today, more 5 GHz frequency space will be released; however, there are some limitations over channel use, as you will explore in this lesson.

Note the numbers quoted on this slide—600 Mbps for 2.4 GHz and 3390 for 5GHz—are not real data throughput. Real data throughput would be the rate at which you could, for example, copy a file across a wireless link. The numbers quoted on this slide and on the specification sheets of wireless equipment specify the physical layer (PHY) throughput number.



2.4 GHz Wireless LAN Channels

- Total of 14 defined
  - Different number of channels available in different parts of the world
  - Different power transmission levels used in different parts of the world
- They overlap
  - APs on adjacent channels (1 and 2, for example) interfere with each other—known as adjacent channel interference (ACI)

By Michael Gauthier, Wireless Networking in the Developing World

FORTINET Training Institute

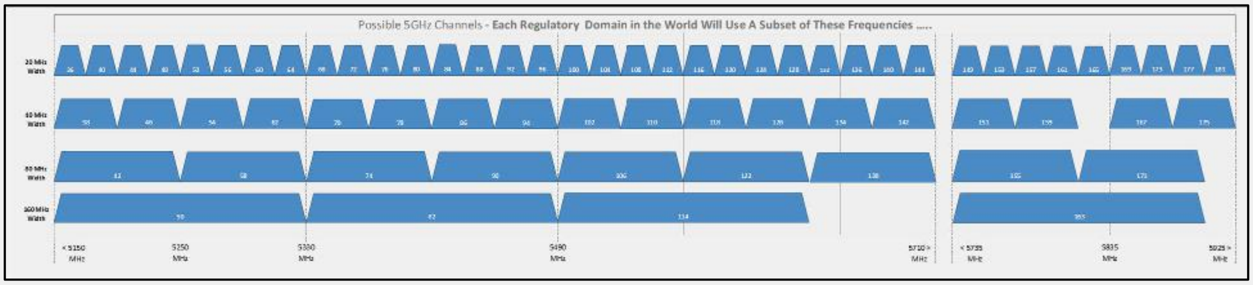
© Fortinet Inc. All Rights Reserved. 40

The International Telecommunication Union (ITU) defined the frequencies between 2.412 and 2.484 GHz for ISM use. That frequency space is split into 14 channels, approximately 20 to 22 MHz wide. However, not all of these channels are available in all parts of the world. Channel availability depends on the local regulatory requirements and the transmission power you're allowed to use.

These channels overlap, which can cause confusion. For example, if you try to use channels 1 and 2, which occupy almost the same frequency space, the signals transmitted on one channel will interfere with the other. This is typically known as ACI. This is probably one of the biggest sources of confusion when configuring requirements for 2.4 GHz. Many users do not know about the channel overlap and potential effects and, as result, might choose inappropriate channels.

5 GHz Wireless LAN Frequencies

- A total of 37 possible 20 MHz channels defined, which can be combined into larger 40/80 and 160 Mhz
- As with 2.4 GHz, there are different numbers of channels available in different parts of the world
- No overlap—each channel is distinct so it can be used

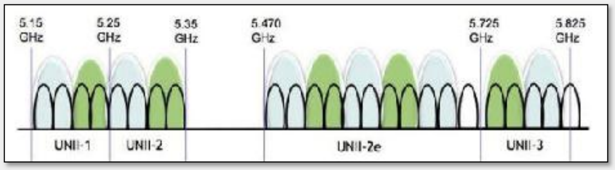


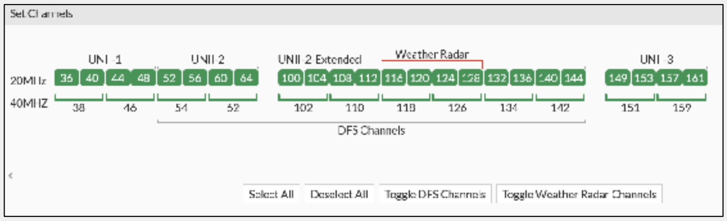
In the 5 GHz frequency range, there is far more bandwidth available. In theory, the International Telecommunication Union (ITU) has released a total of 37 possible 20 MHz channels. It should be emphasized that these are possible frequencies and have not been adopted globally.

Unlike 2.4 GHz, the channel numbers shown on this slide are distinct and do not overlap, so you can safely use channels adjacent to each other without any risk of ACI, providing the APs are spaced at least the minimum distance apart.

Dynamic Frequency Selection 5 GHz band

- Dynamic frequency selection (DFS)
  - IEEE 802.11h requires 5 GHz band (U-NII band) radios to avoid other primary-use or mission-critical radio transmissions
- Specific frequencies in the 5 GHz range are also used by airport and weather radar and satellite systems
- In order to share this spectrum, wireless APs and clients have to conform *and certify* to a set of additional wireless standards detailed in the 802.11h standard





Fortinet Training Institute

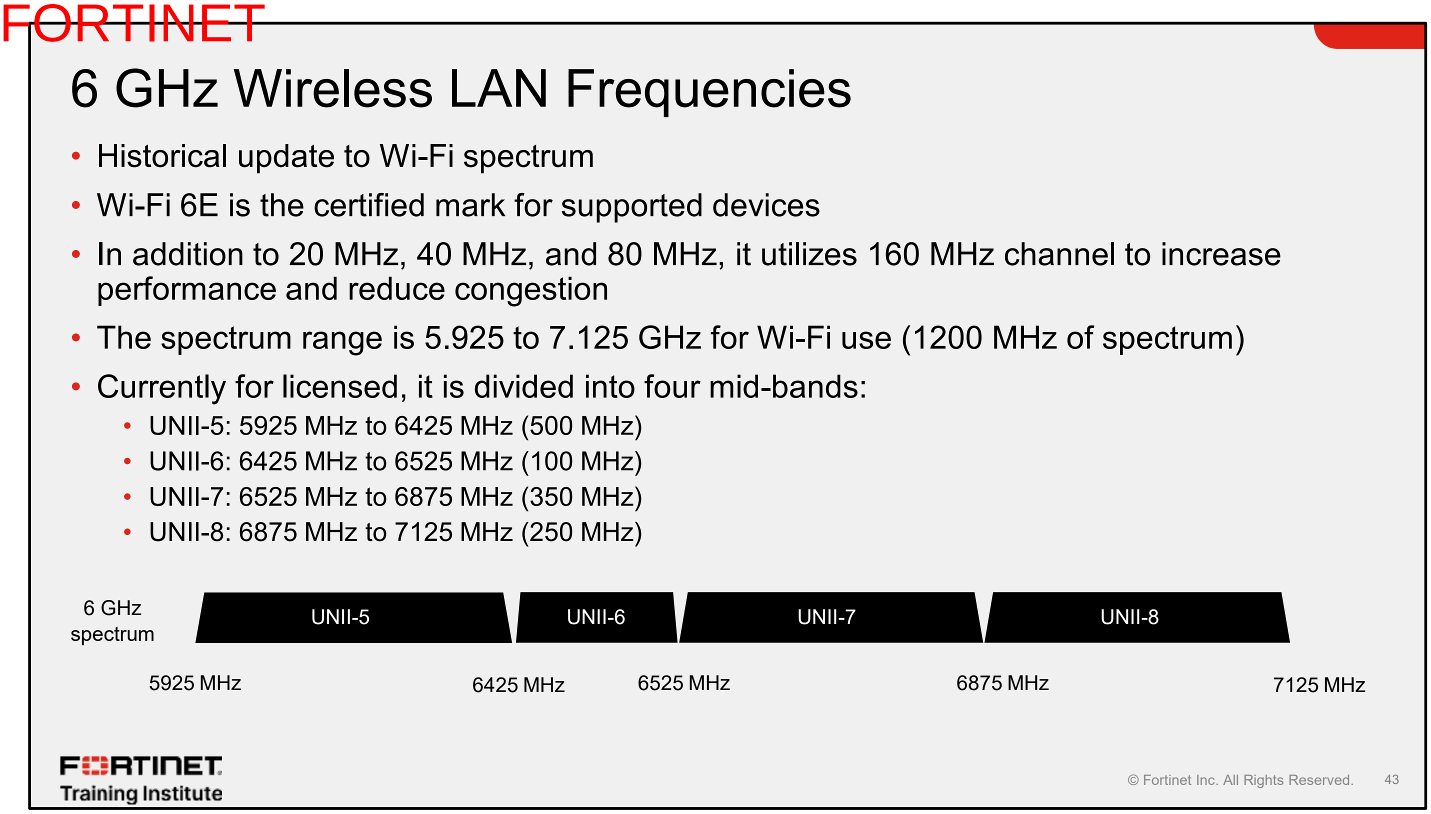
42

DFS (IEEE 802.11h) requires 5 GHz band (U-NII band) radios to avoid other primary-use or mission-critical radio transmissions. The 5 GHz frequency space is not without limitations. Because this frequency space is also used by other licenced applications, wireless LANs have to use a specific method to gain access to certain higher frequencies. This method is known as DFS.

Specific types of radar, such as an airport, weather, military, and shipping radar, operate in the 5 GHz range. Because radar depends on very weak signals returned from airplanes, ships, and so on, radar antennas must be very sensitive. This sensitivity makes it very easy for low-powered APs or wireless clients to interfere with a radar system.

So, to enable wireless LANs to share the 5 GHz spectrum, equipment has to conform and be certified to an additional set of wireless standards detailed in the 802.11h standard.

DFS is very important because 802.11 wireless APs (or any RF emitters) negatively impact radar systems.



6 GHz Wireless LAN Frequencies

- Historical update to Wi-Fi spectrum
- Wi-Fi 6E is the certified mark for supported devices
- In addition to 20 MHz, 40 MHz, and 80 MHz, it utilizes 160 MHz channel to increase performance and reduce congestion
- The spectrum range is 5.925 to 7.125 GHz for Wi-Fi use (1200 MHz of spectrum)
- Currently for licensed, it is divided into four mid-bands:
  - UNII-5: 5925 MHz to 6425 MHz (500 MHz)
  - UNII-6: 6425 MHz to 6525 MHz (100 MHz)
  - UNII-7: 6525 MHz to 6875 MHz (350 MHz)
  - UNII-8: 6875 MHz to 7125 MHz (250 MHz)

FORTINET Training Institute

43

Wi-Fi 6 was introduced using the existence of 2.4 GHz and 5 GHz bands being used for frequency spectrum available. The 6 GHz frequency is becoming a historical update to Wi-Fi technology since the time it was introduced back in 1998.

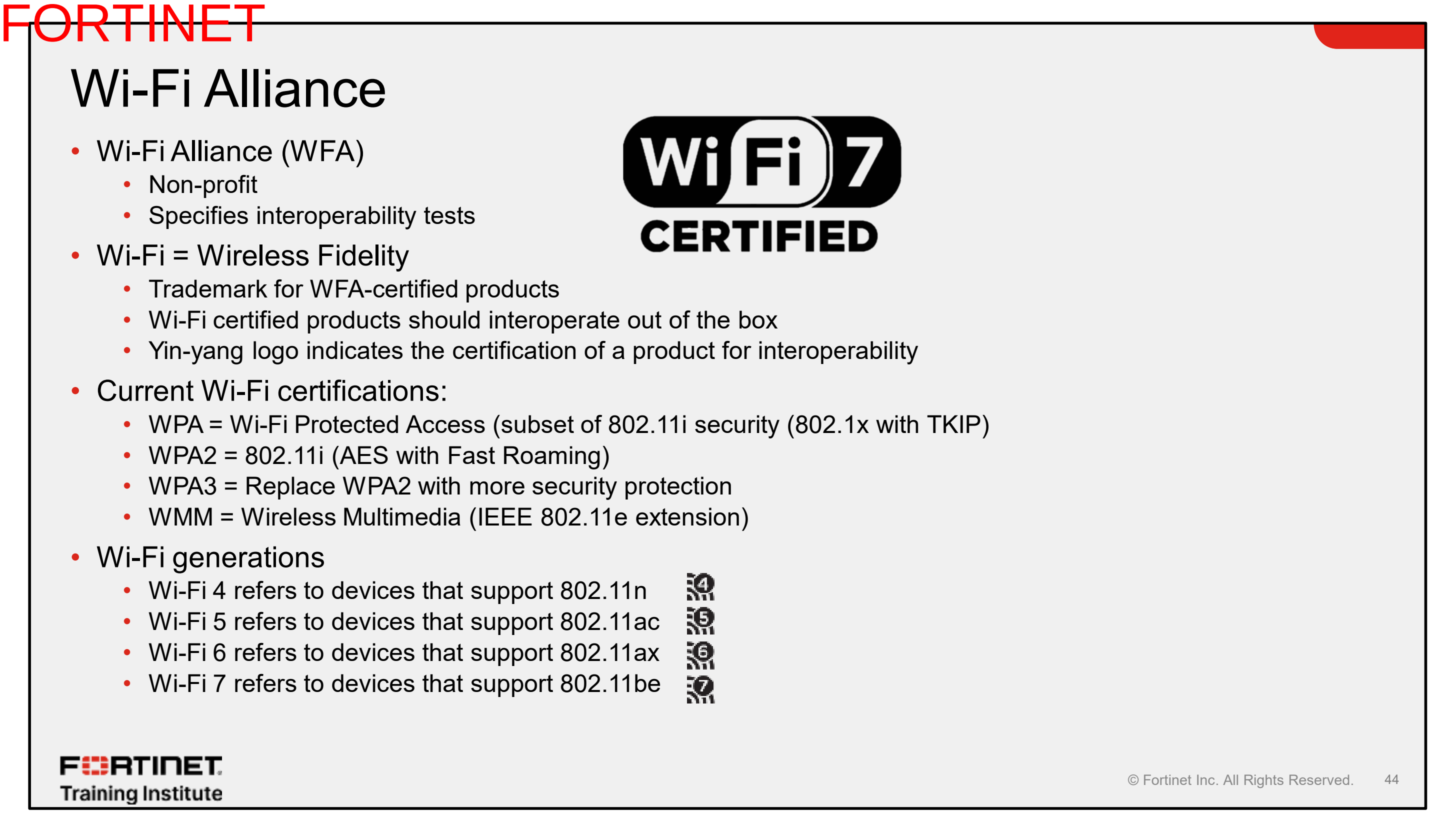
To avoid confusion, Wi-Fi 6 is not the reference to 6 GHz band support. It is referred to as Wi-Fi 6E which means that devices that can use 6 GHz are required to have Wi-Fi 6E certification. It is set to operate on an unlicensed spectrum starting from 5.925-7.125 GHz.

As Wi-Fi 6 was developed based on OFDMA, which allows multiple users to transmit simultaneously, it is said Wi-Fi 6E uses modulation to address performance and challenges wireless networks usually come across. Unlike with OFDM, OFDMA channel bandwidth (20, 40, 80, or 160 MHz) is divided to simultaneously transmit on the resource units of small channels units. Addressing congestion and performance, Wi-Fi 6E impact often gets compared to upgrading from a single-lane road (OFDM) to a multilane freeway (OFDMA).

The 6 GHz frequency band covers the 5.925 GHz to 7.125 GHz spectrum and is divided into four mid-bands for licensed users:

UNII-5: 5925-6425 MHz (500 MHz)
UNII-6: 6425-6525 MHz (100 MHz)
UNII-7: 6525-6875 MHz (350 MHz)
UNII-8: 6875-7125 MHz (250 MHz)

The mid-band spectrum is currently for licensed users who have deployed services in these frequencies. For example, users include point-to-point microwave links and mobile TV pickups at sporting events relaying signals back to a studio.



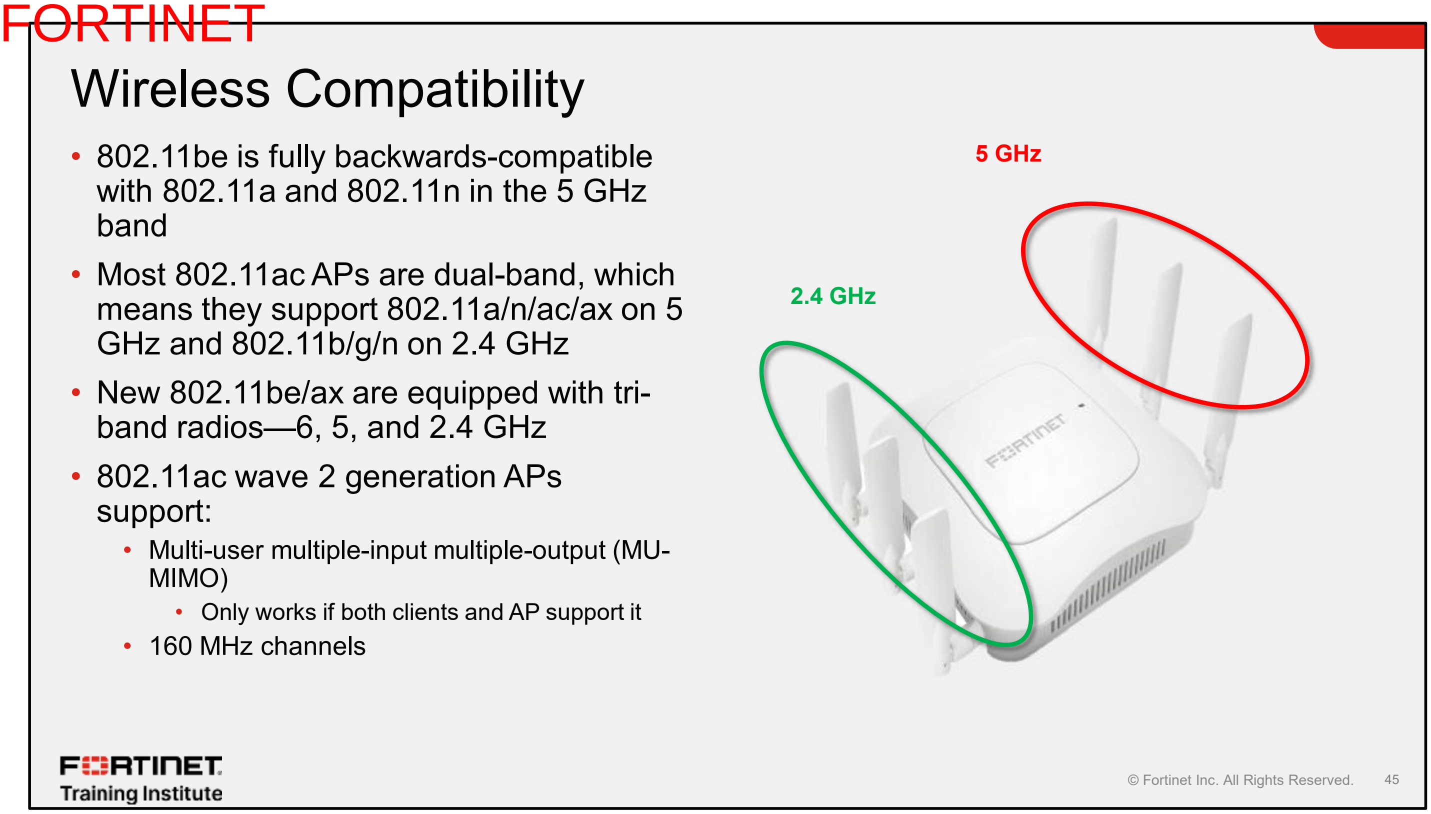
Wi-Fi Alliance

- Wi-Fi Alliance (WFA)
  - Non-profit
  - Specifies interoperability tests
- Wi-Fi = Wireless Fidelity
  - Trademark for WFA-certified products
  - Wi-Fi certified products should interoperate out of the box
  - Yin-yang logo indicates the certification of a product for interoperability
- Current Wi-Fi certifications:
  - WPA = Wi-Fi Protected Access (subset of 802.11i security (802.1x with TKIP)
  - WPA2 = 802.11i (AES with Fast Roaming)
  - WPA3 = Replace WPA2 with more security protection
  - WMM = Wireless Multimedia (IEEE 802.11e extension)
- Wi-Fi generations
  - Wi-Fi 4 refers to devices that support 802.11n
  - Wi-Fi 5 refers to devices that support 802.11ac
  - Wi-Fi 6 refers to devices that support 802.11ax
  - Wi-Fi 7 refers to devices that support 802.11be

44

The Wi-Fi Alliance is a non-profit organization that promotes Wi-Fi technology. They certify Wi-Fi products that conform to standards of interoperability and define standards for security.

This organization was founded to solve interoperability issues among products using the IEEE 802.11 standards. For further information on the alliance, go to: `http://www.wi-fi.org/`



Wireless Compatibility

- 802.11be is fully backwards-compatible with 802.11a and 802.11n in the 5 GHz band
- Most 802.11ac APs are dual-band, which means they support 802.11a/n/ac/ax on 5 GHz and 802.11b/g/n on 2.4 GHz
- New 802.11be/ax are equipped with tri-band radios—6, 5, and 2.4 GHz
- 802.11ac wave 2 generation APs support:
  - Multi-user multiple-input multiple-output (MU-MIMO)
    - Only works if both clients and AP support it
  - 160 MHz channels

FORTINET Training Institute

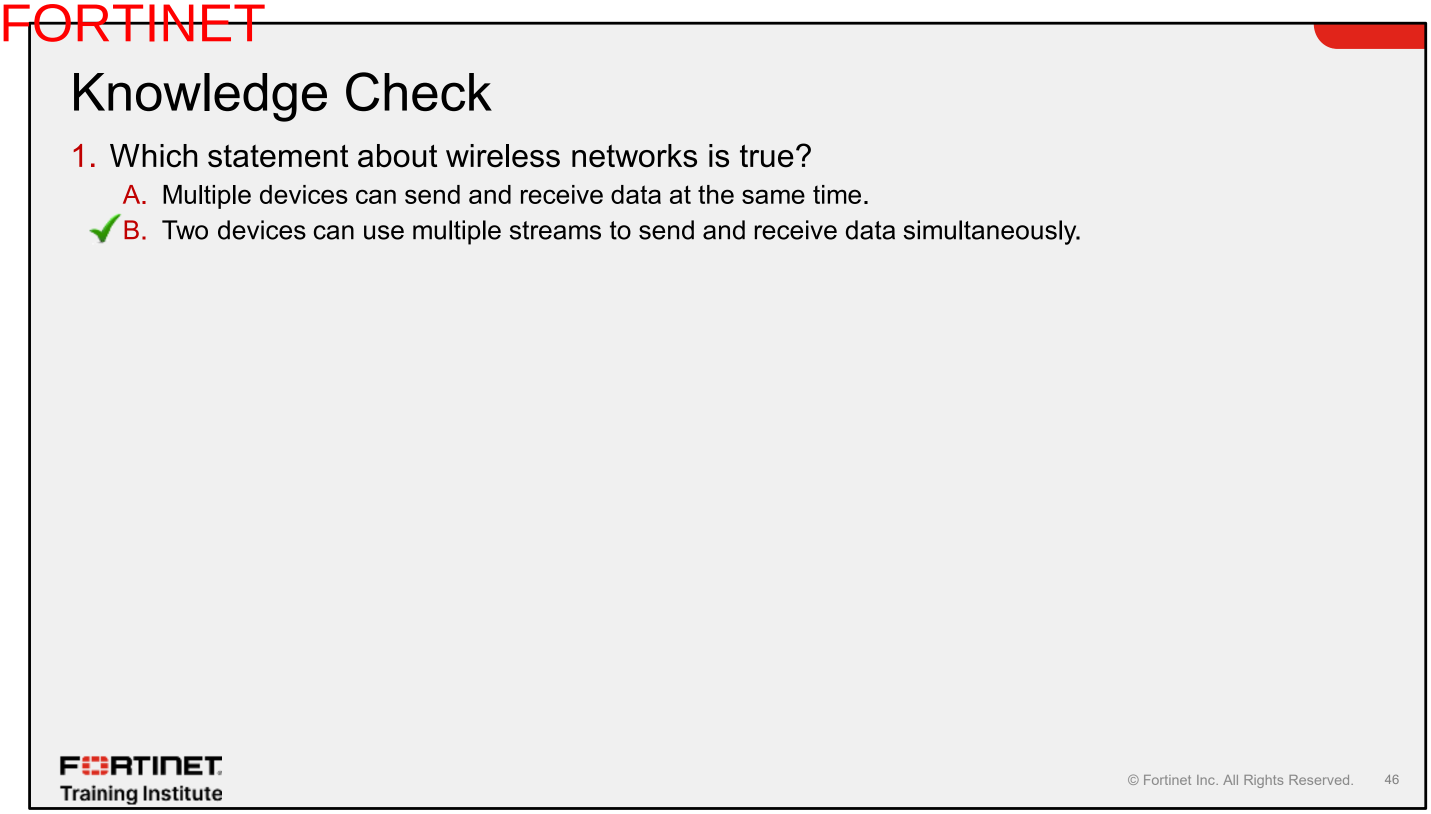
45

The IEEE 802.11ac standard is fully backwards compatible with 802.11a and 802.11n in the 5 GHz band. Most 802.11ac APs are dual-band, which means they do 802.11a/n/ac on 5 GHz and 802.11b/g/n on 2.4 GHz. However, to get good throughput, both the client and AP should support the 802.11ac standard.

The IEEE 802.11ac standard uses three main improvements to achieve the throughput:

- More spatial streams (more antennas)
- More spectrum (wider channels)
- Denser modulation (more bits per symbol)

IEEE 802.11ac wave 2 has improved throughput using MU-MIMO.

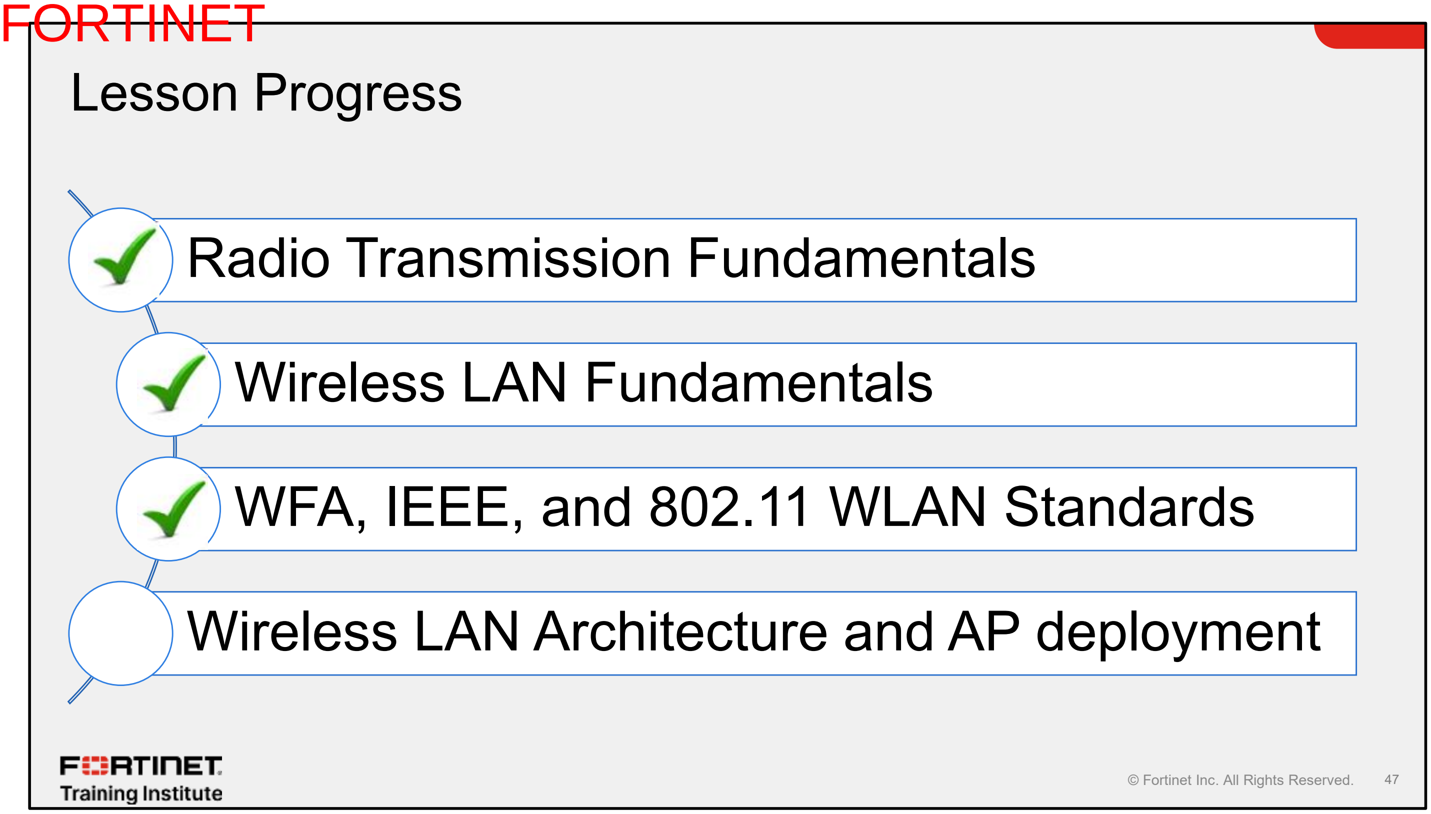


Knowledge Check

1. Which statement about wireless networks is true?
   - A. Multiple devices can send and receive data at the same time.
   - ✓ B. Two devices can use multiple streams to send and receive data simultaneously.

FORTINET Training Institute

46



Lesson Progress

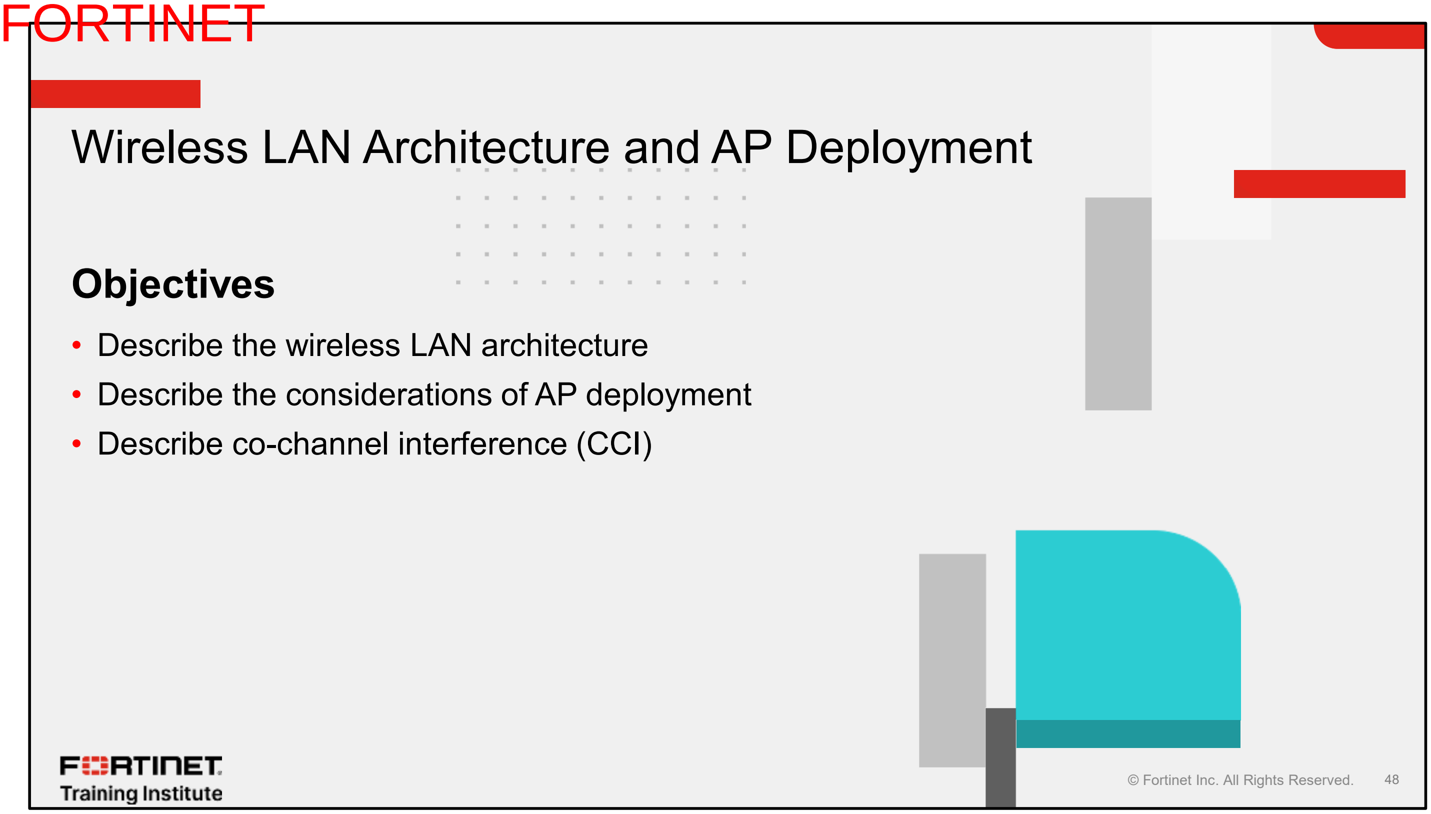
- ✓ Radio Transmission Fundamentals
- ✓ Wireless LAN Fundamentals
- ✓ WFA, IEEE, and 802.11 WLAN Standards
- ○ Wireless LAN Architecture and AP deployment

FORTINET Training Institute

47

Good job! You now understand 802.11 Wi-Fi standards.

Now, you will learn about wireless LAN architecture and AP deployment.



Wireless LAN Architecture and AP Deployment

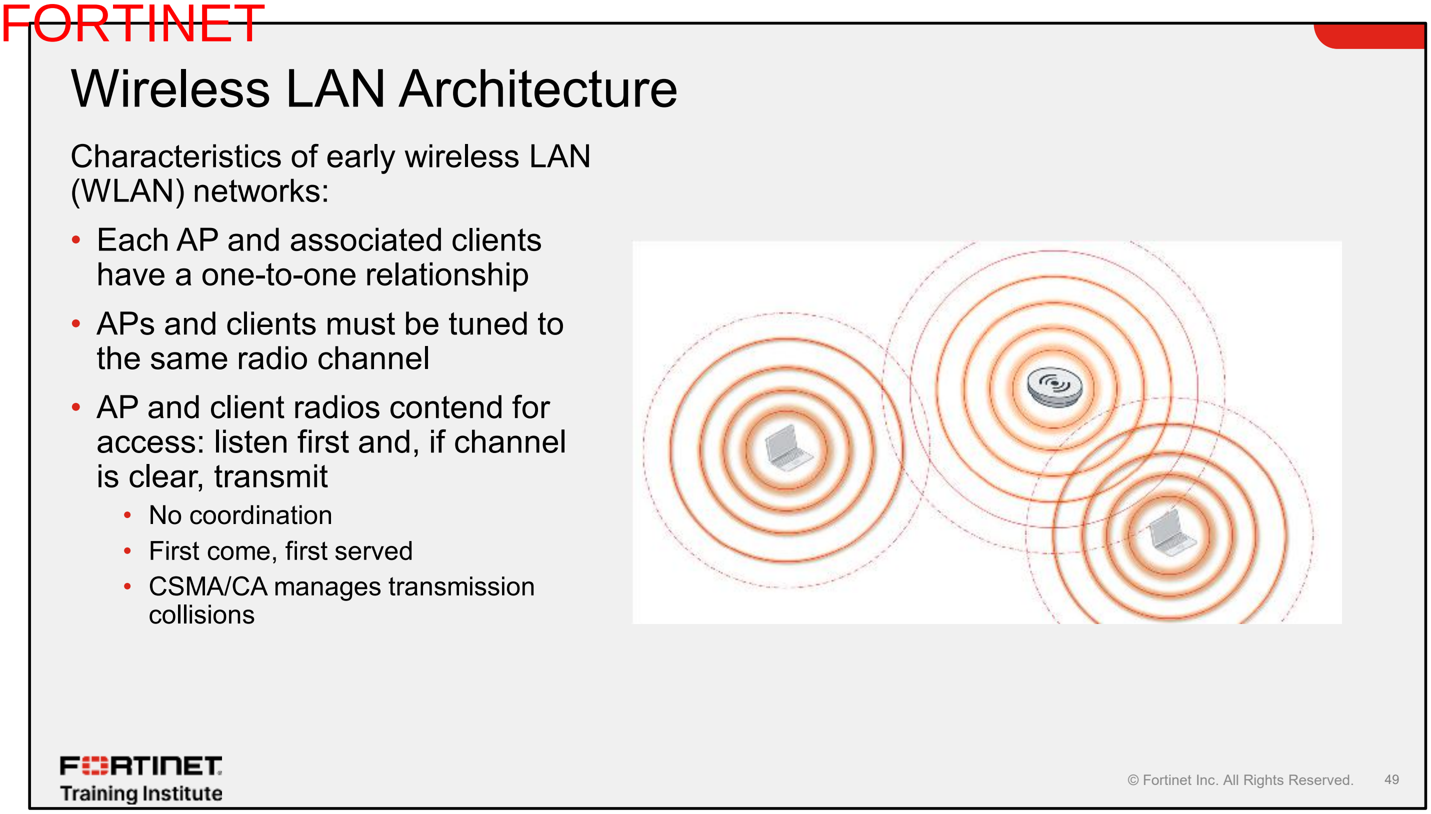
Objectives

- Describe the wireless LAN architecture
- Describe the considerations of AP deployment
- Describe co-channel interference (CCI)

48

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in wireless LAN architecture and AP deployment, you will be able to design and deploy wireless network more effectively.



Wireless LAN Architecture

Characteristics of early wireless LAN (WLAN) networks:

- Each AP and associated clients have a one-to-one relationship
- APs and clients must be tuned to the same radio channel
- AP and client radios contend for access: listen first and, if channel is clear, transmit
  - No coordination
  - First come, first served
  - CSMA/CA manages transmission collisions

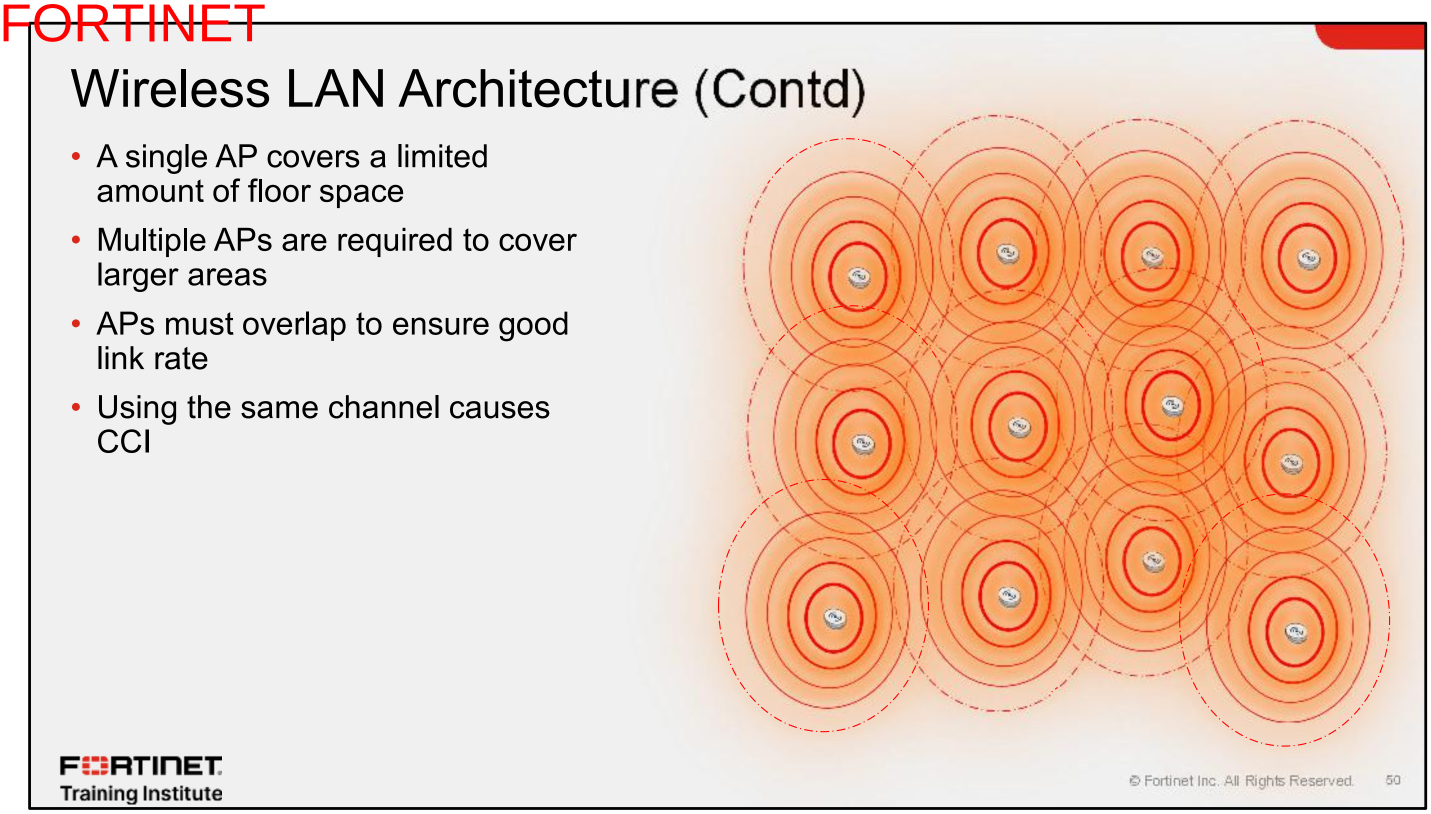
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 49

Since being standardized in the late 1990s, WLAN technology has grown and evolved; however, the fundamental operating principles have not changed. This has caused challenges, because wireless networks have grown bigger.

Early wireless networks consisted of one AP. Clients associated with this single AP to gain network access. In order to communicate, the client and the AP needed to be tuned to the same radio channel. Similar to a two-way radio system, the client and AP radios could only transmit *or* receive communications. In networking terms, this is referred to as half duplex.

A radio has to listen to its assigned channel to hear if any other radio is talking before it can transmit. It listens for and decodes the wireless LAN frames it hears, which is known as clear channel assessment (CCA). CCA allows the radio to determine if the channel is being used by another wireless LAN radio. It can also work out how long the channel is going to be used for because it can read specific fields in the frame header that set how long that transmission is expected to last (in microseconds). This is set by the sending radio.



Wireless LAN Architecture (Contd)

- A single AP covers a limited amount of floor space
- Multiple APs are required to cover larger areas
- APs must overlap to ensure good link rate
- Using the same channel causes CCI

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 50

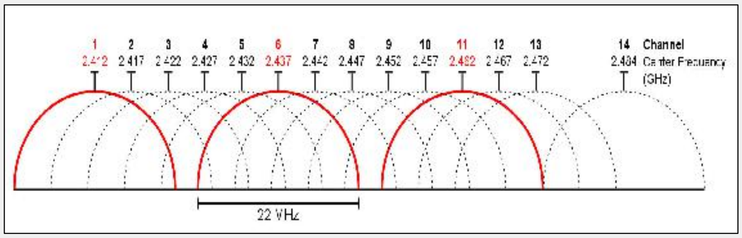
Radio transmissions in wireless networks are governed by strict transmission power regulations.

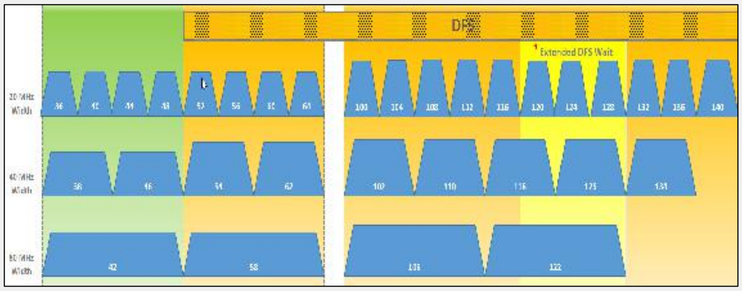
Think of each AP as an *island*; a single wireless network island covers a relatively small area. To cover a larger area, multiple islands need to be deployed, as shown on this slide. Also, to ensure that the signal remains consistent as clients moved around, some overlap is necessary.

However, if all of the APs on the neighbouring islands are trying to transmit on the same channel without any coordination, this will cause transmission interference, also known as CCI.

Wireless LAN Architecture (Contd)

- Use different channels for each island
- Limited number of channels
- Some frequencies have more channels, but with limitations





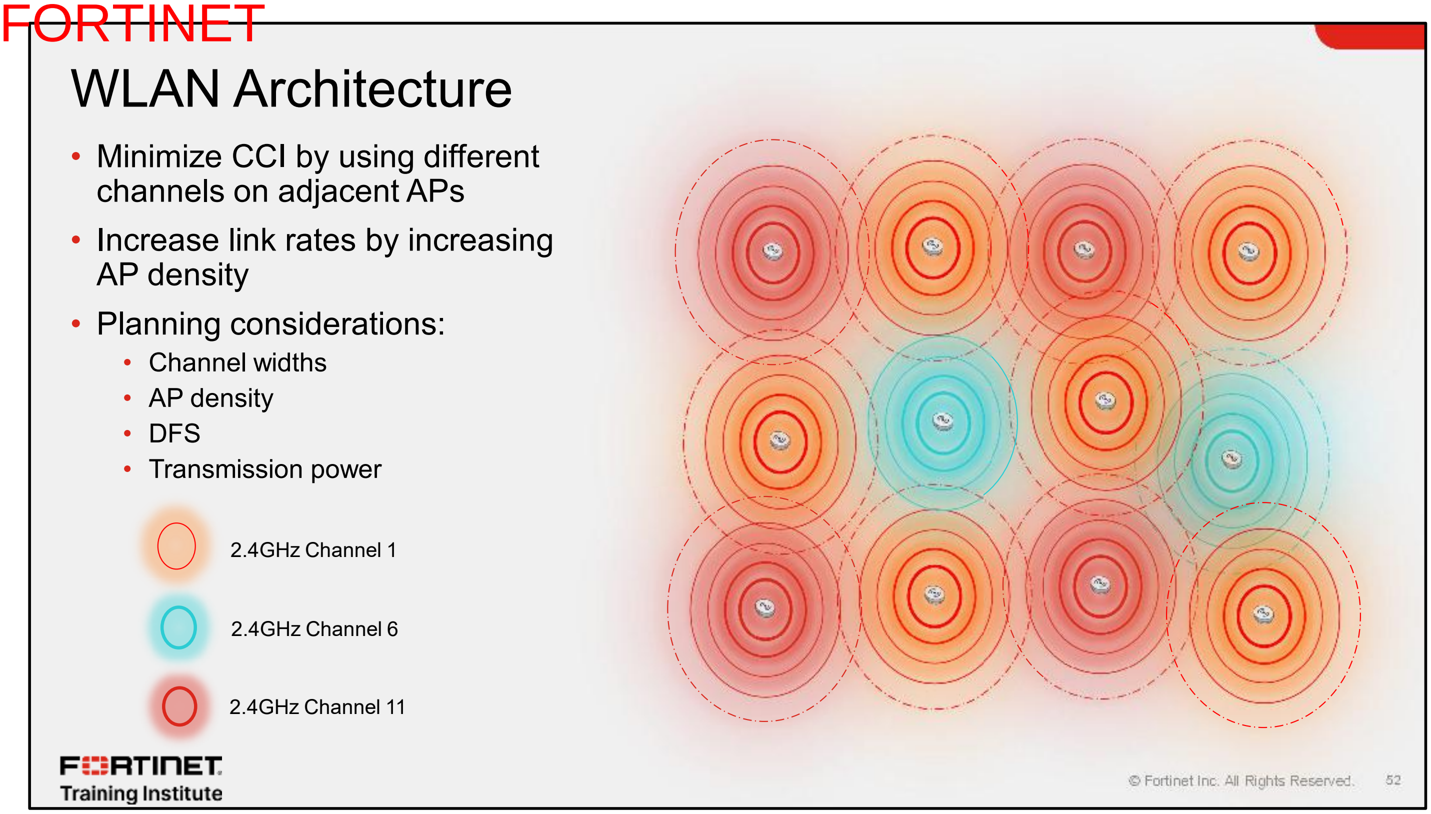
FORTINET Training Institute

51

WLANs are allowed to operate in relatively small parts of the radio spectrum.

The small part of the spectrum that WLANS are allowed to use is divided into multiple channels. One of the early methods used to accommodate multiple APs was to assign each island its own channel. This meant that conversations occurring on different islands could take place at the same time without interfering with, colliding with, or inhibiting each other.

The initial portion of the spectrum released for WLAN use was in the 2.4 GHz range. It was subdivided into 14 channels; however, some practical limitations meant that only three channels were usable. Later, more of the spectrum was released in the 5 GHz range, making more channels available. However, there were limitations around using these channels as well.



WLAN Architecture

- Minimize CCI by using different channels on adjacent APs
- Increase link rates by increasing AP density
- Planning considerations:
  - Channel widths
  - AP density
  - DFS
  - Transmission power

2.4GHz Channel 1

2.4GHz Channel 6

2.4GHz Channel 11

Training Institute

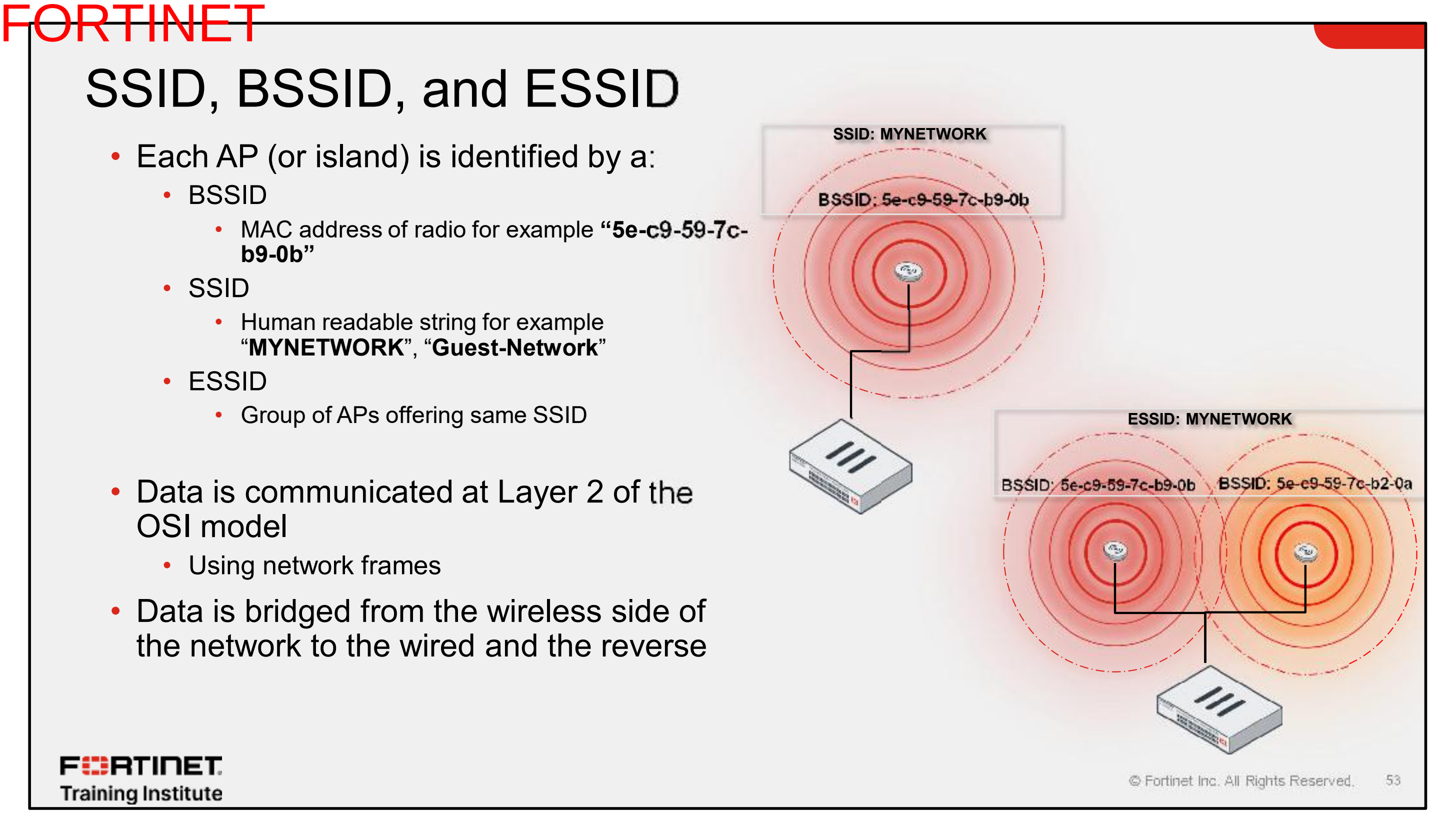
52

When different islands are assigned their own channels, the network coverage can grow. However, because there are only three usable channels in the 2.4 GHz range, in any network that has more than three APs, channels have to be reused. To prevent CCI, radios on the same channel need to be kept as far apart as possible.

Often, you have to cope with a reduced number of channels, channels being unavailable or unreliable, and, in the case of a 5 GHz space, dealing with limitations such as dynamic frequency selection (DFS).

In addition to planning channels, you also the need to ensure that the signal is strong and consistent. To achieve performance strength and consistency, APs need to be closer together than is advised from a channel planning point of view. If APs are deployed in high density, you may need to reduce transmission power to avoid CCI. Often, you must also often plan the two radio channels associated with each AP; one in 2.4 GHz and one in 5 GHz

This is known as a *microcell* architecture, and each island is referred to as a cell. Designing and implementing an efficient microcell requires careful planning.



SSID, BSSID, and ESSID

- Each AP (or island) is identified by a:
  - BSSID
    - MAC address of radio for example **“5e-c9-59-7c-b9-0b”**
  - SSID
    - Human readable string for example “**MYNETWORK**”, “**Guest-Network**”
  - ESSID
    - Group of APs offering same SSID
- Data is communicated at Layer 2 of the OSI model
  - Using network frames
- Data is bridged from the wireless side of the network to the wired and the reverse

FORTINET Training Institute

53

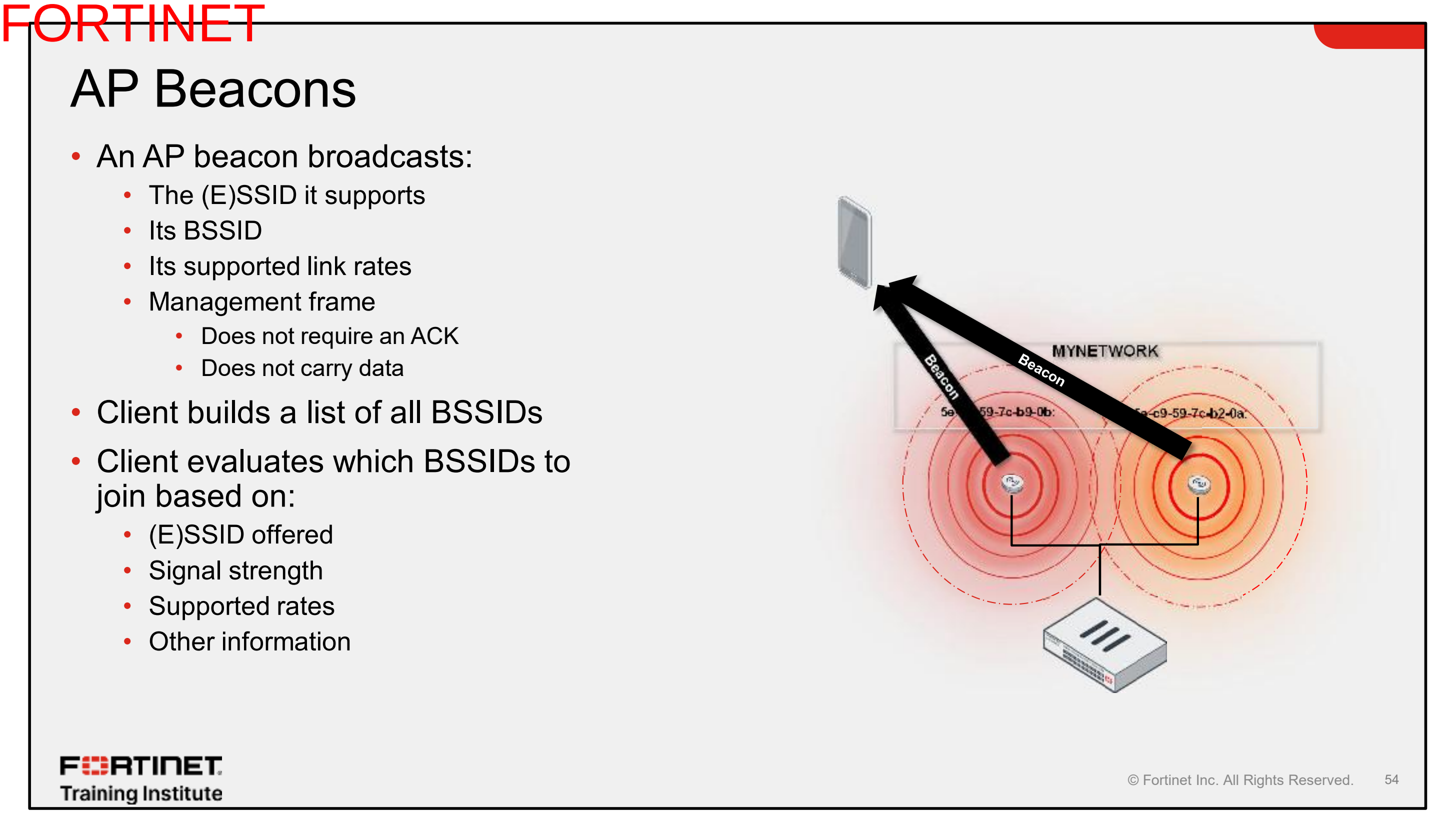
Each transmission contains a basic service set identifier (BSSID) and service set identifier (SSID) that identify the originating AP. When clients need to send data to APs, they require an address to send the data to. In WLAN standards, the address of the radio is the Ethernet MAC address assigned by the manufacturer. This is a 48-bit-long address represented in hexadecimal numbers for example, 5e-c9-59-7c-b9-0b**.**

The WLAN standards also enable the AP to broadcast a service set identifier (SSID), a human readable string that users can use to identify the network, for example MYNETWORK, or Guest-Network.

A connected group of APs offering the same SSID is called an extended SSID or ESSID. When an ESSID is used, even though each individual AP radio still has a BSSID, the entire network is represented by a single “name”. For example, if the BSSID of AP1 is 5e-c9-59-7c-b2-0a and AP2 is 5e-c9-59-7c-b2-0b, the ESSID is the same MYNETWORK**.**

Data in the wireless network is moving at layer 2 and is referred to as frames. Layer 3 protocols sit on top of layer 2 and use it as a transport.

Wireless APs bridge frames from the wireless side of the network to the wired side of the network and the reverse. The AP functions as an Ethernet bridge.



AP Beacons

- An AP beacon broadcasts:
  - The (E)SSID it supports
  - Its BSSID
  - Its supported link rates
  - Management frame
    - Does not require an ACK
    - Does not carry data
- Client builds a list of all BSSIDs
- Client evaluates which BSSIDs to join based on:
  - (E)SSID offered
  - Signal strength
  - Supported rates
  - Other information

FORTINET Training Institute

54

Each AP in the network advertises itself using beacons. A beacon is a specific type of frame that broadcasts:

- The SSID it supports
- The BSSID (unique identity) of the AP
- A selection of other configuration information, such as supported link rates

Beacons go out approximately every 100 milliseconds, or 1/10th of a second. Beacons are part of a class of frames that are used for the management and maintenance of the wireless network.

Because beacons are a type of broadcast frame, they do not require clients to acknowledge them. They carry *information* around the wireless network, but they do not carry *client data*. The more management frames are in the air, the less airtime is available to send useful data.

When a client arrives and wants to join a wireless network, it starts gathering lists of available networks, identified by BSSIDs, from the beacons that it receives.

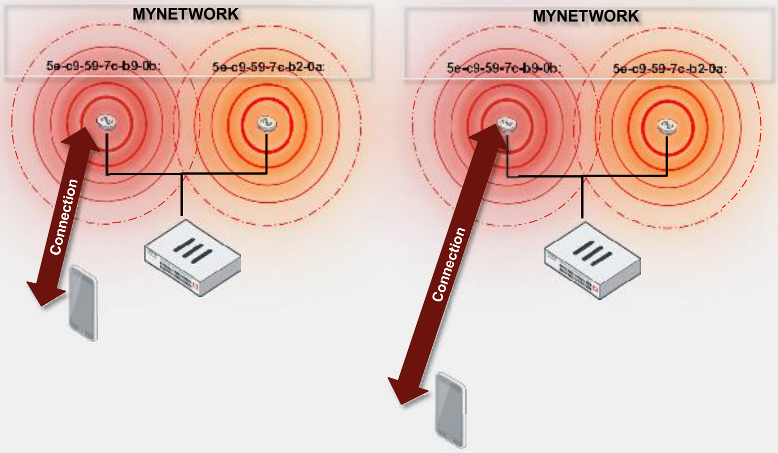
When evaluating which network to join, the client looks at:

- Signal strength
- Supported rates
- The SSID offered
- Other information

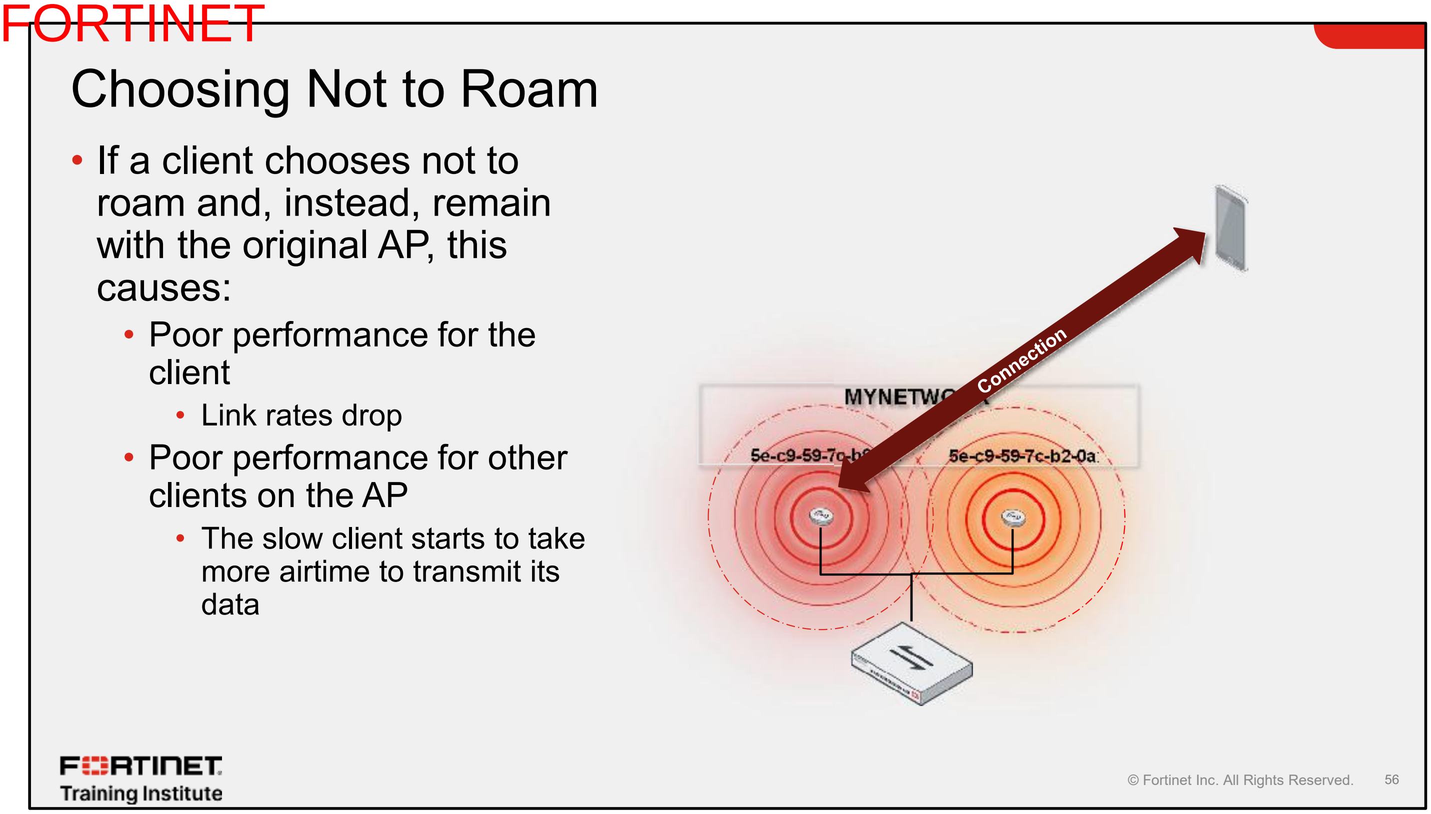
After performing the evaluation, the client makes a list of preferred candidate BSSIDs.

Roaming

- If a client moves away from the associated AP, the signal will drop
- As the signal drops, the client should look for another BSSID offering the required SSID
- At some point the client will make the decision to roam



Clients are often constantly monitoring the strength of the signal to the AP they are connected to. As the signal strength changes as the client moves, the client *should* start looking at its list of APs to see if there is a better AP to connect to. If the client does decide to disconnect from the original AP and connect to a new AP, this is called roaming.



Choosing Not to Roam

- If a client chooses not to roam and, instead, remain with the original AP, this causes:
  - Poor performance for the client
    - Link rates drop
  - Poor performance for other clients on the AP
    - The slow client starts to take more airtime to transmit its data

FORTINET Training Institute

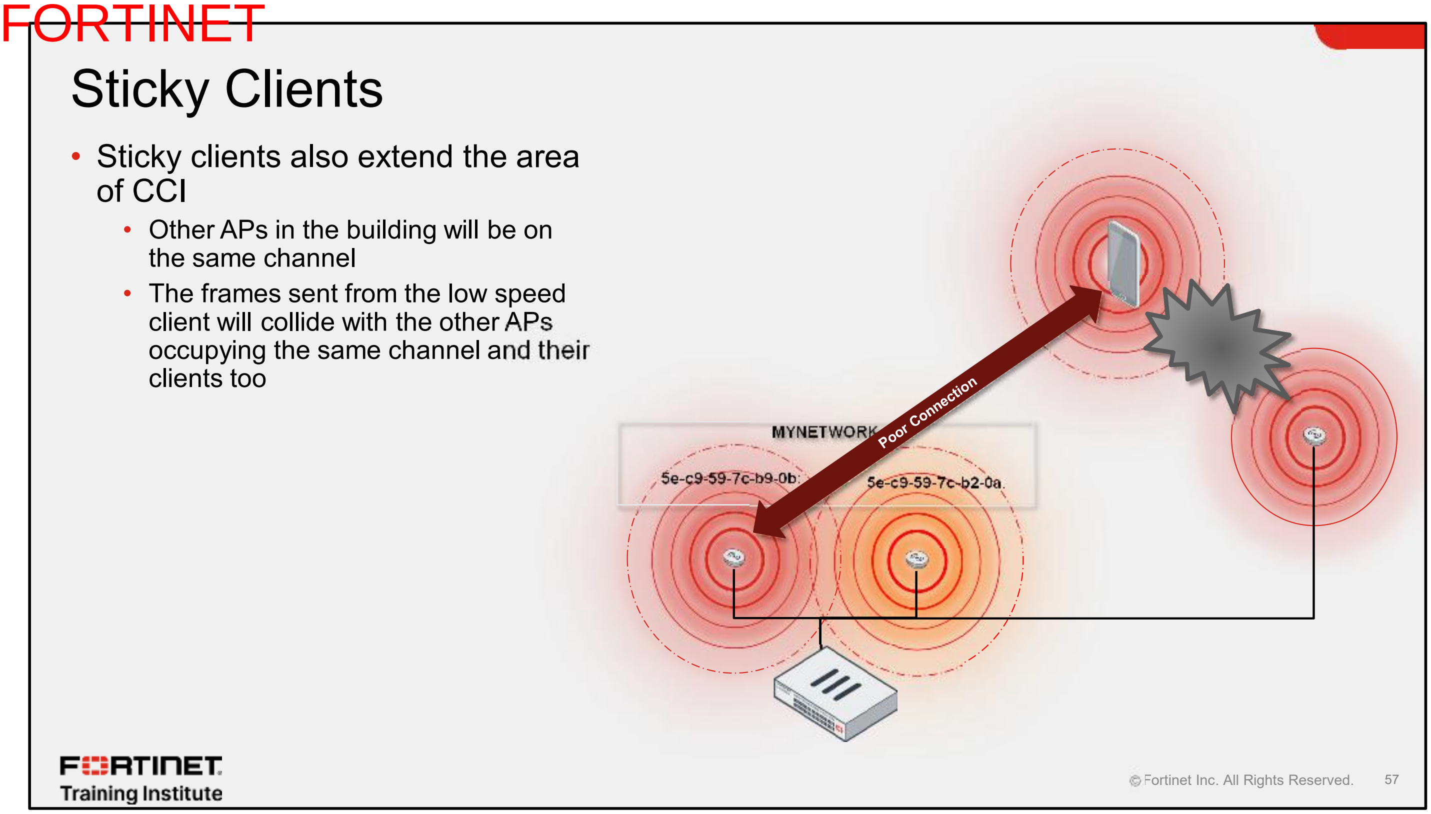
© Fortinet Inc. All Rights Reserved. 56

Clients don’t always make the best of decisions, and many of the decisions they make depend on the quality of their wireless chipset and the driver that supports that chipset.

Clients that are used mostly in the home market often choose not to roam. Instead, they choose to remain with the original AP, even when signal strength is poor or the signal drops. As the signal drops, the link rate drops, and the amount of data that the client can transfer is reduced. These types of clients are often referred to as *sticky clients*.

This not only leads to poor performance on that client, it also takes up more airtime to transfer data. This can impact other clients that are associated with the same AP.

Airtime fairness is a mechanism that can help in these types of scenarios.

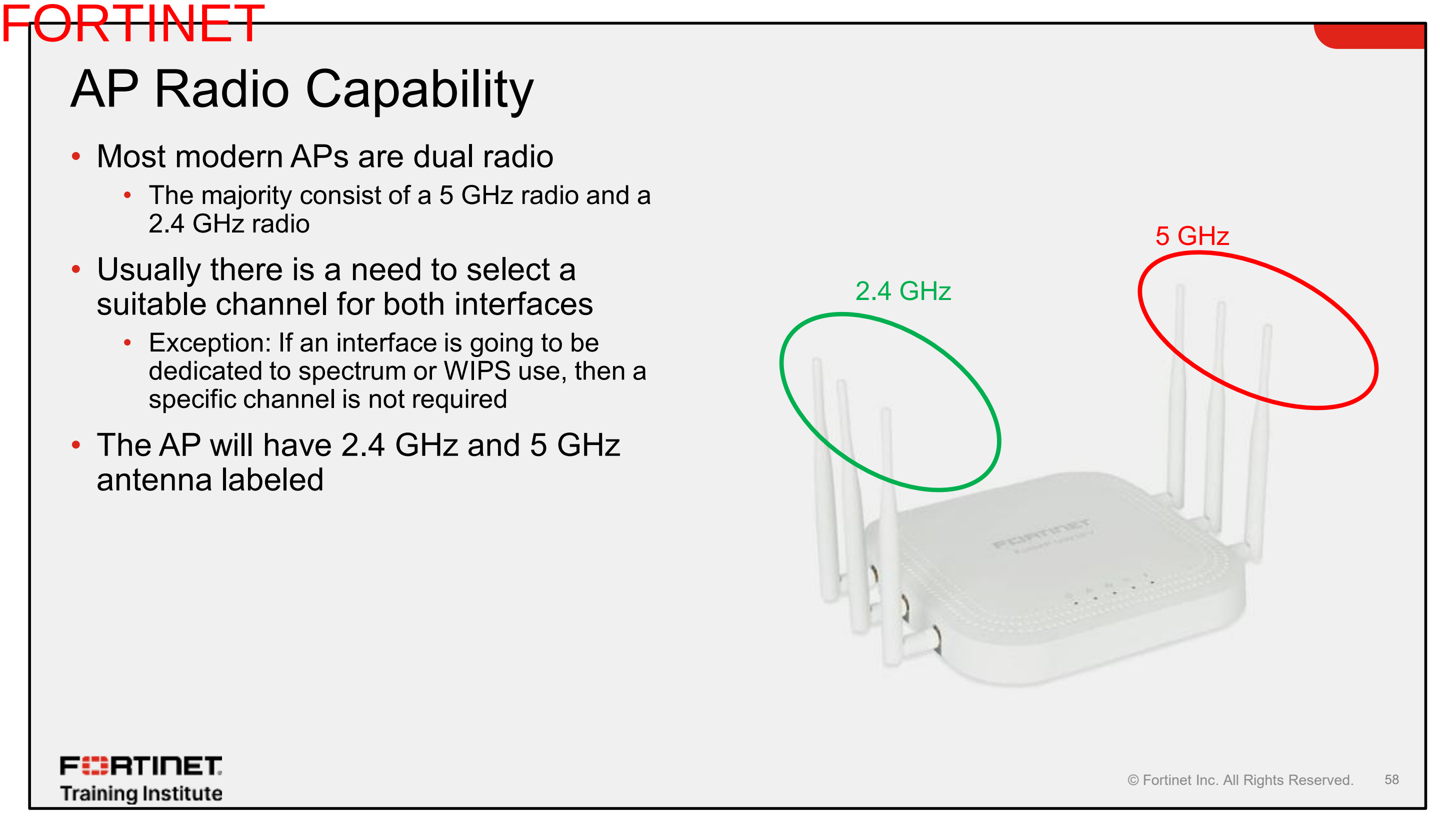


Sticky Clients

- Sticky clients also extend the area of CCI
  - Other APs in the building will be on the same channel
  - The frames sent from the low speed client will collide with the other APs occupying the same channel and their clients too

57

If a client decides not to roam and remain associated with same AP, it is called a sticky client. One side effect of sticky clients is that they extend the area of the CCI. While trying to make low-speed transmissions back to the AP they are associated with, they are also potentially colliding with transmissions from another AP in the building, impacting the performance of that AP and the clients associated with it.



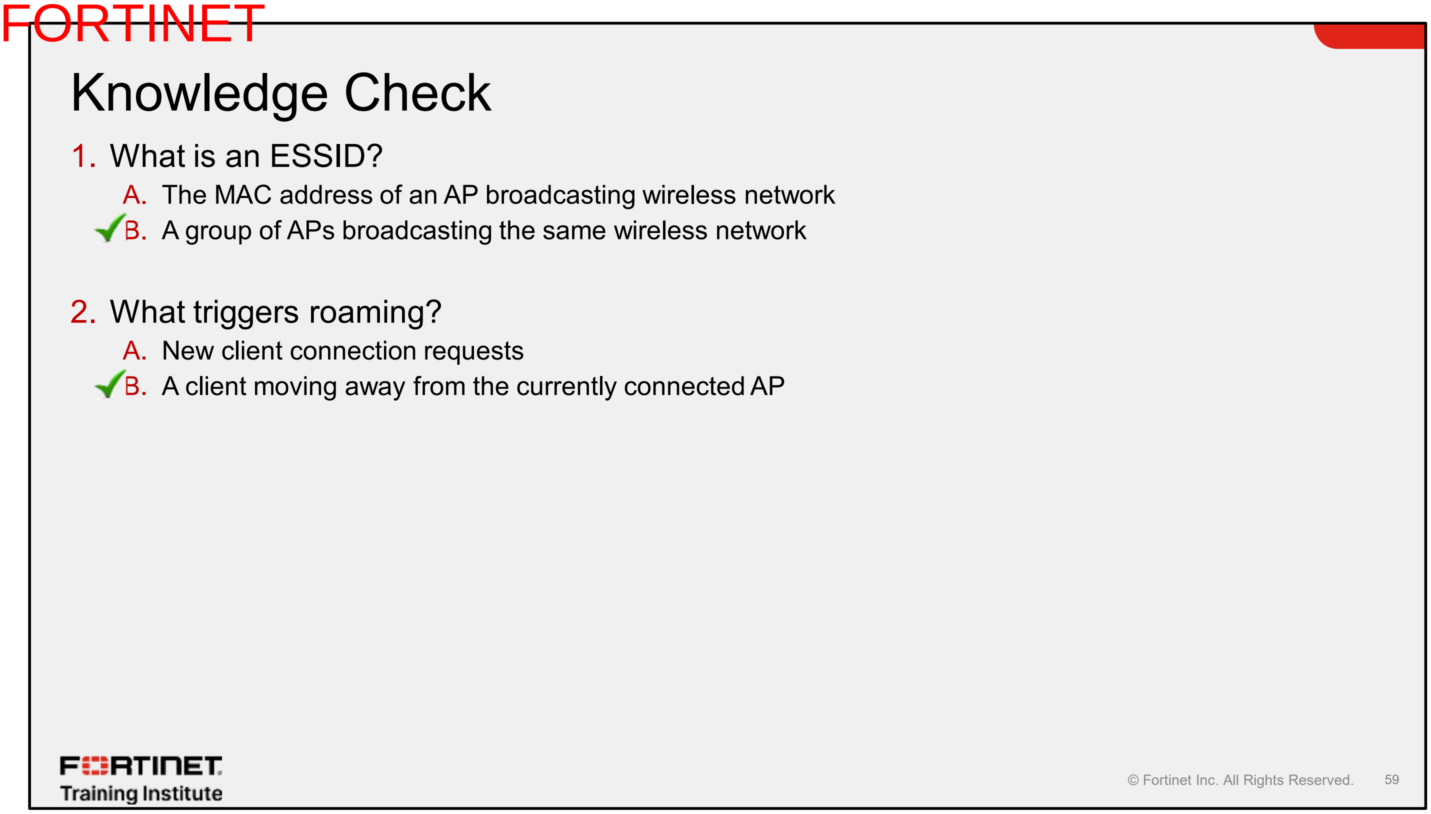
AP Radio Capability

- Most modern APs are dual radio
  - The majority consist of a 5 GHz radio and a 2.4 GHz radio
- Usually there is a need to select a suitable channel for both interfaces
  - Exception: If an interface is going to be dedicated to spectrum or WIPS use, then a specific channel is not required
- The AP will have 2.4 GHz and 5 GHz antenna labeled

Training Institute

58

Remember, the vast majority of modern APs are dual-band, which means they are equipped with two radio chips that allow simultaneous transmission. Most APs consist of a 5 GHz radio chipset and a 2.4 GHz radio chipset. Usually, but not always, you must assign a channel to both of these interfaces. Sometimes you might want to reserve a radio on an AP for a specific use, such as spectrum analysis or a wireless intrusion prevention system (WIPS). Radios used for these purposes do not need a dedicated channel—often part of their function is to scan multiple channels.

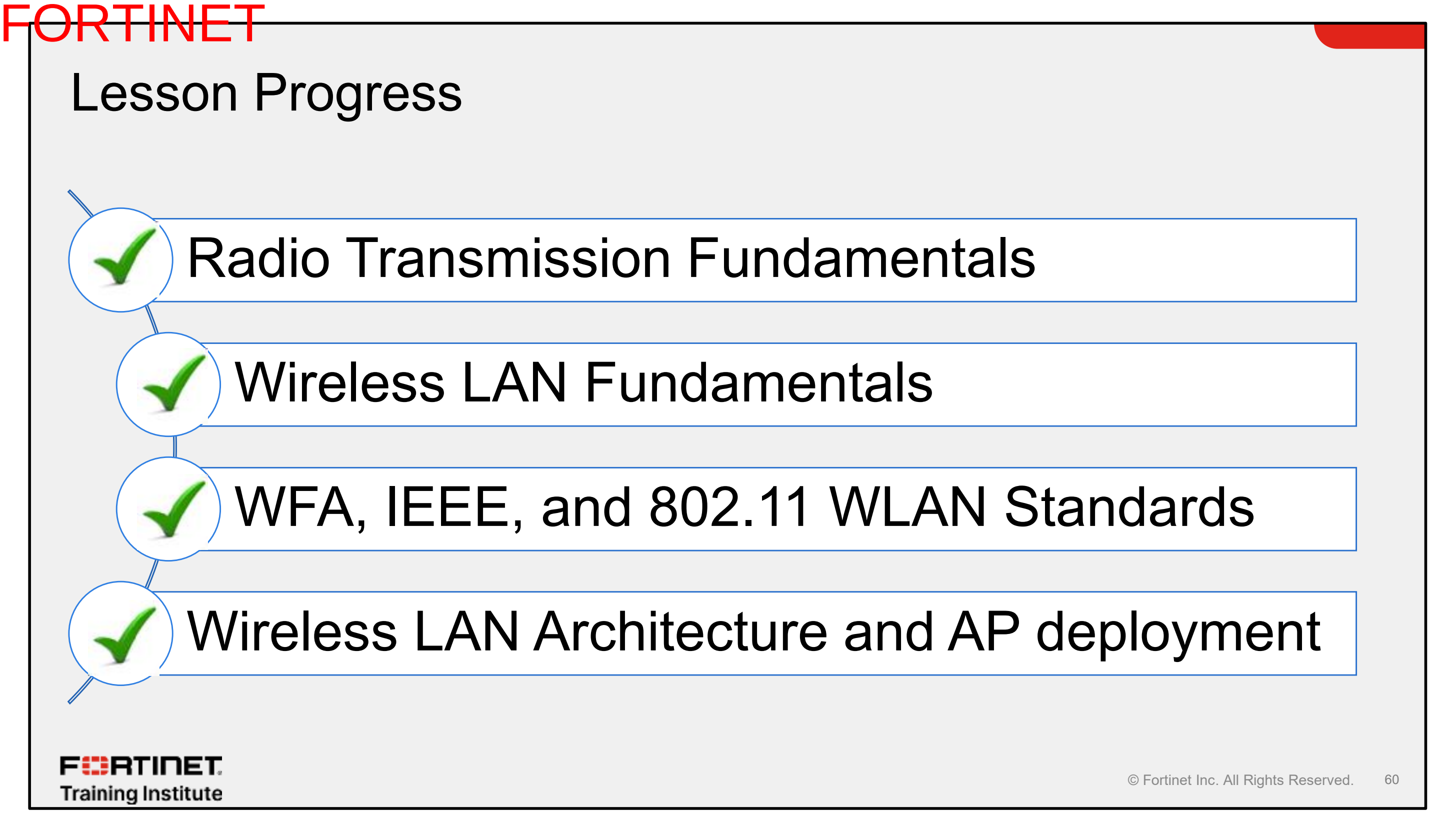


Knowledge Check

1. What is an ESSID?
   - A. The MAC address of an AP broadcasting wireless network
   - ✓ B. A group of APs broadcasting the same wireless network

2. What triggers roaming?
   - A. New client connection requests
   - ✓ B. A client moving away from the currently connected AP

FORTINET Training Institute



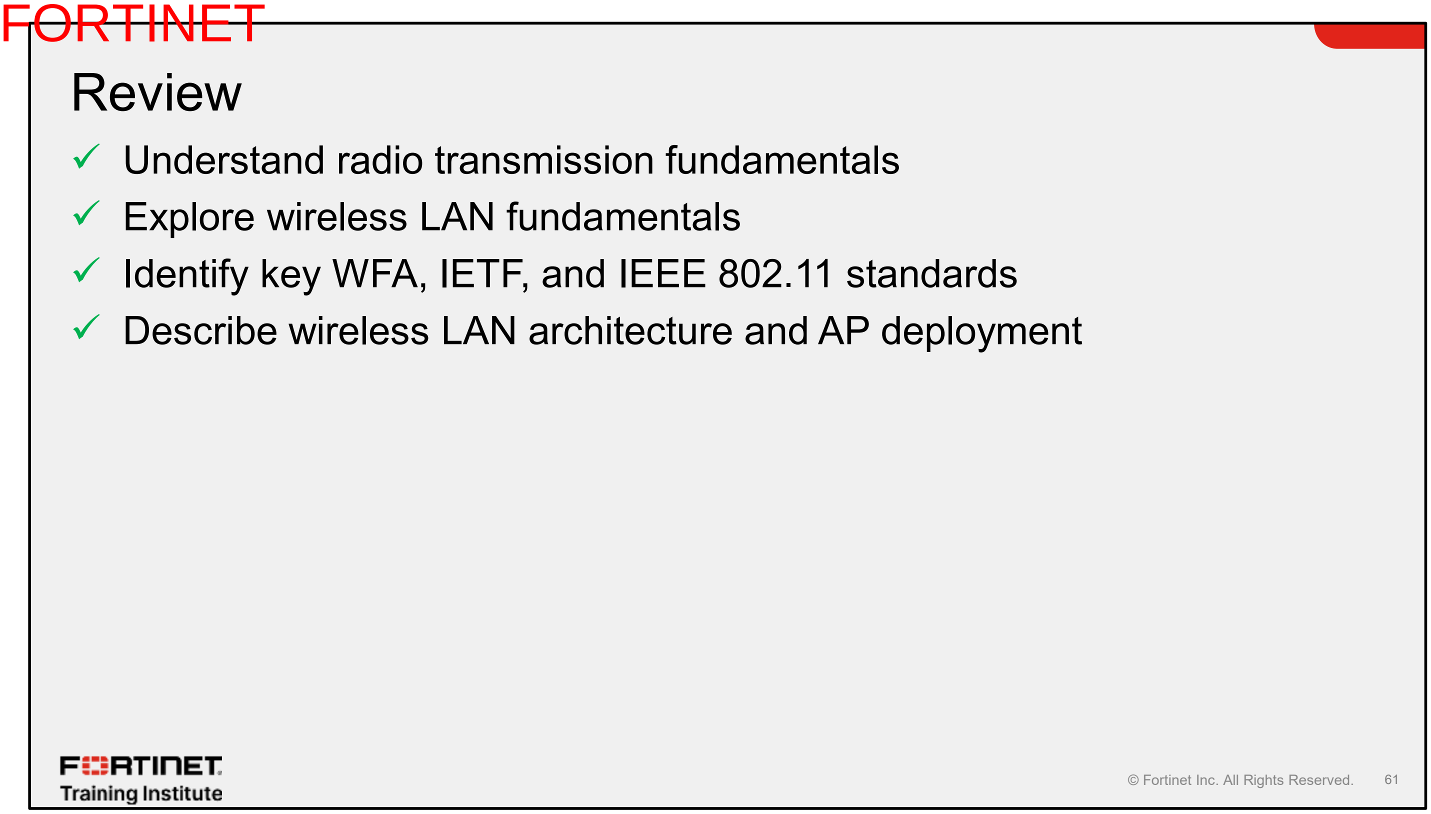
Lesson Progress

- ✓ Radio Transmission Fundamentals
- ✓ Wireless LAN Fundamentals
- ✓ WFA, IEEE, and 802.11 WLAN Standards
- ✓ Wireless LAN Architecture and AP deployment

60

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



Review

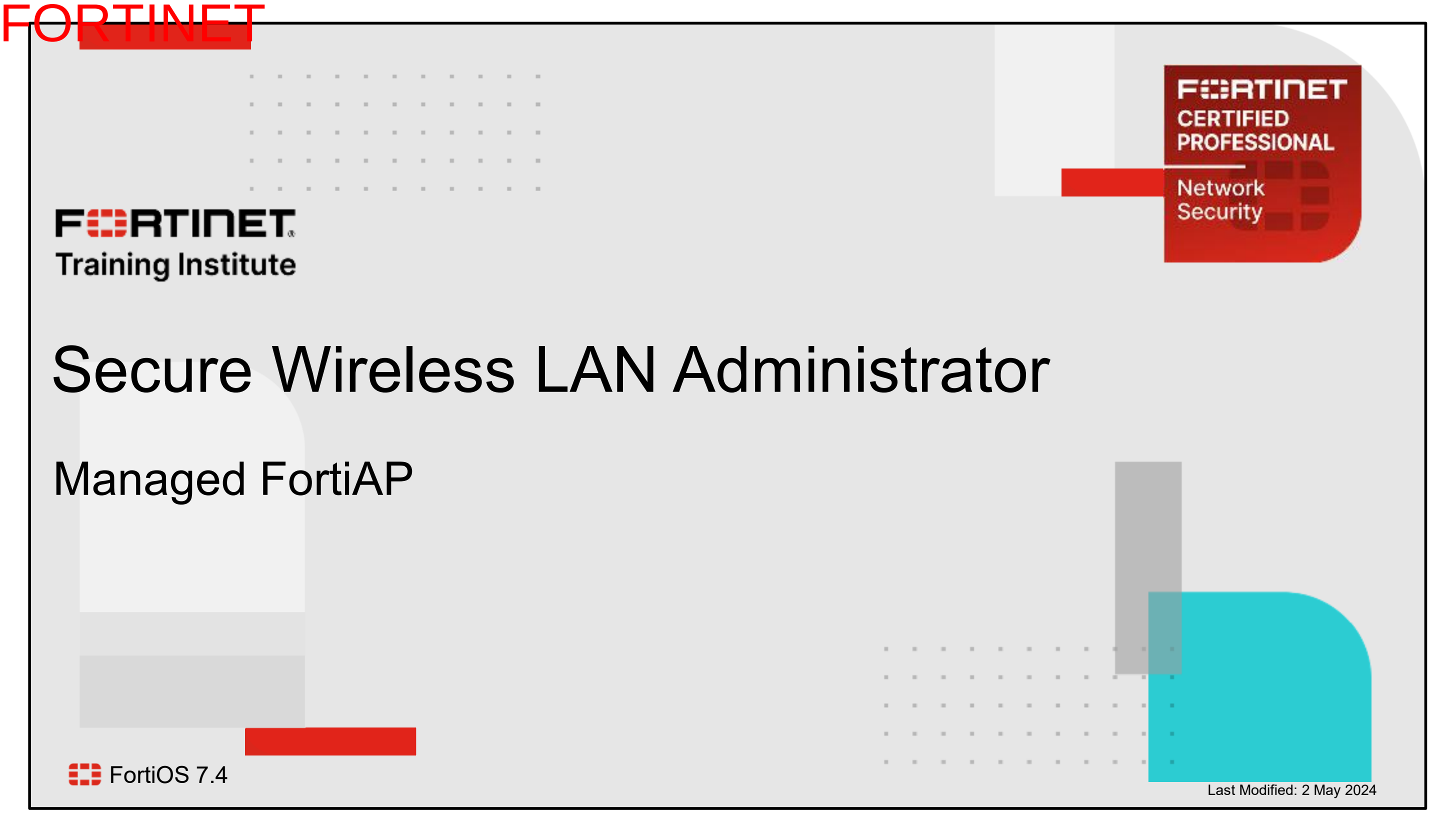
- ✓ Understand radio transmission fundamentals
- ✓ Explore wireless LAN fundamentals
- ✓ Identify key WFA, IETF, and IEEE 802.11 standards
- ✓ Describe wireless LAN architecture and AP deployment

FORTINET Training Institute

61

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about wireless technology concepts and how to apply them when deploying a wireless network using Fortinet infrastructure wireless solutions.



FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL Network Security

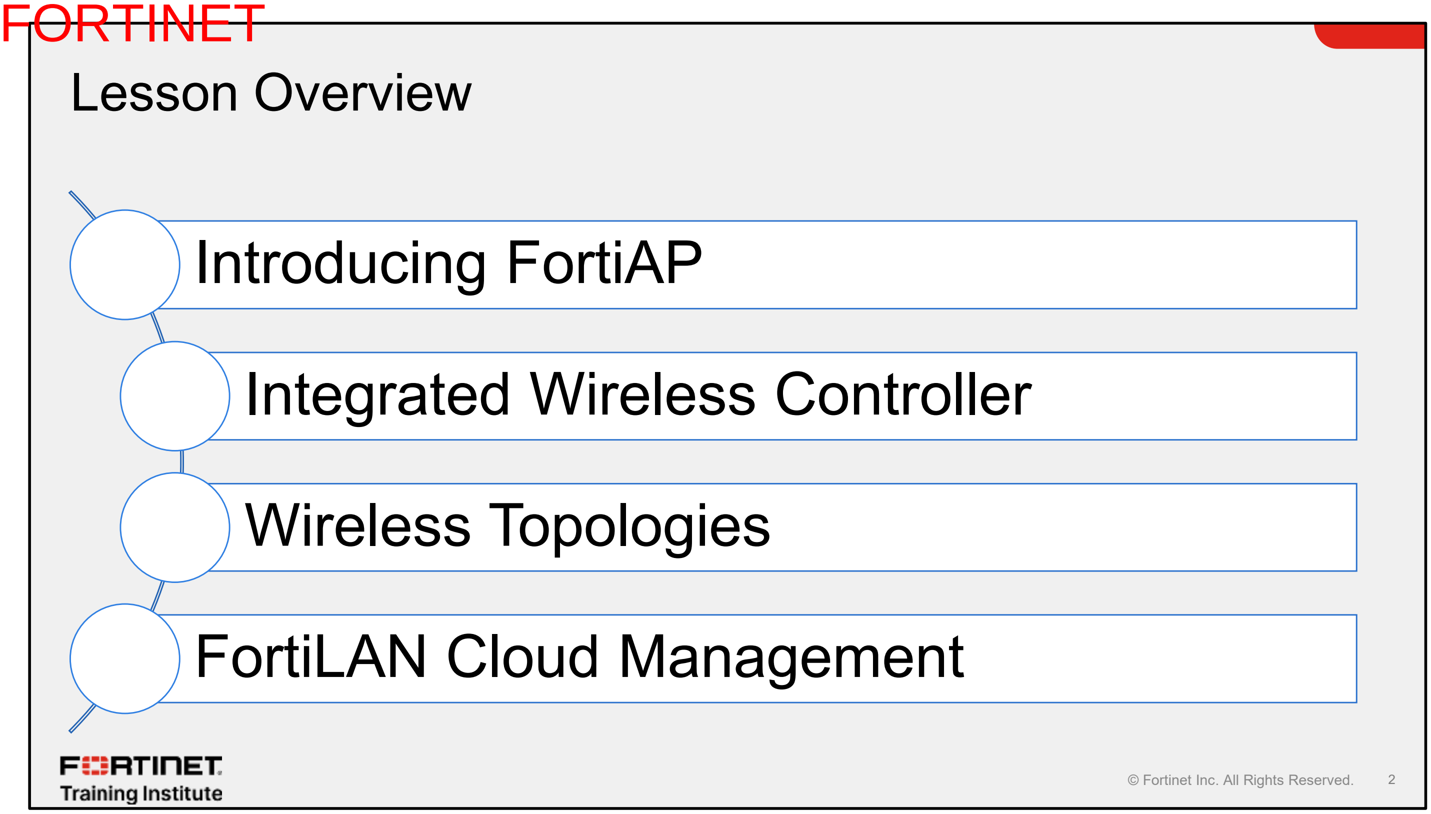
Secure Wireless LAN Administrator

Managed FortiAP

FortiOS 7.4

Last Modified: 2 May 2024

In this lesson, you will learn about FortiAP essentials, focusing on the managed FortiAP devices that use the FortiOS integrated wireless controller.



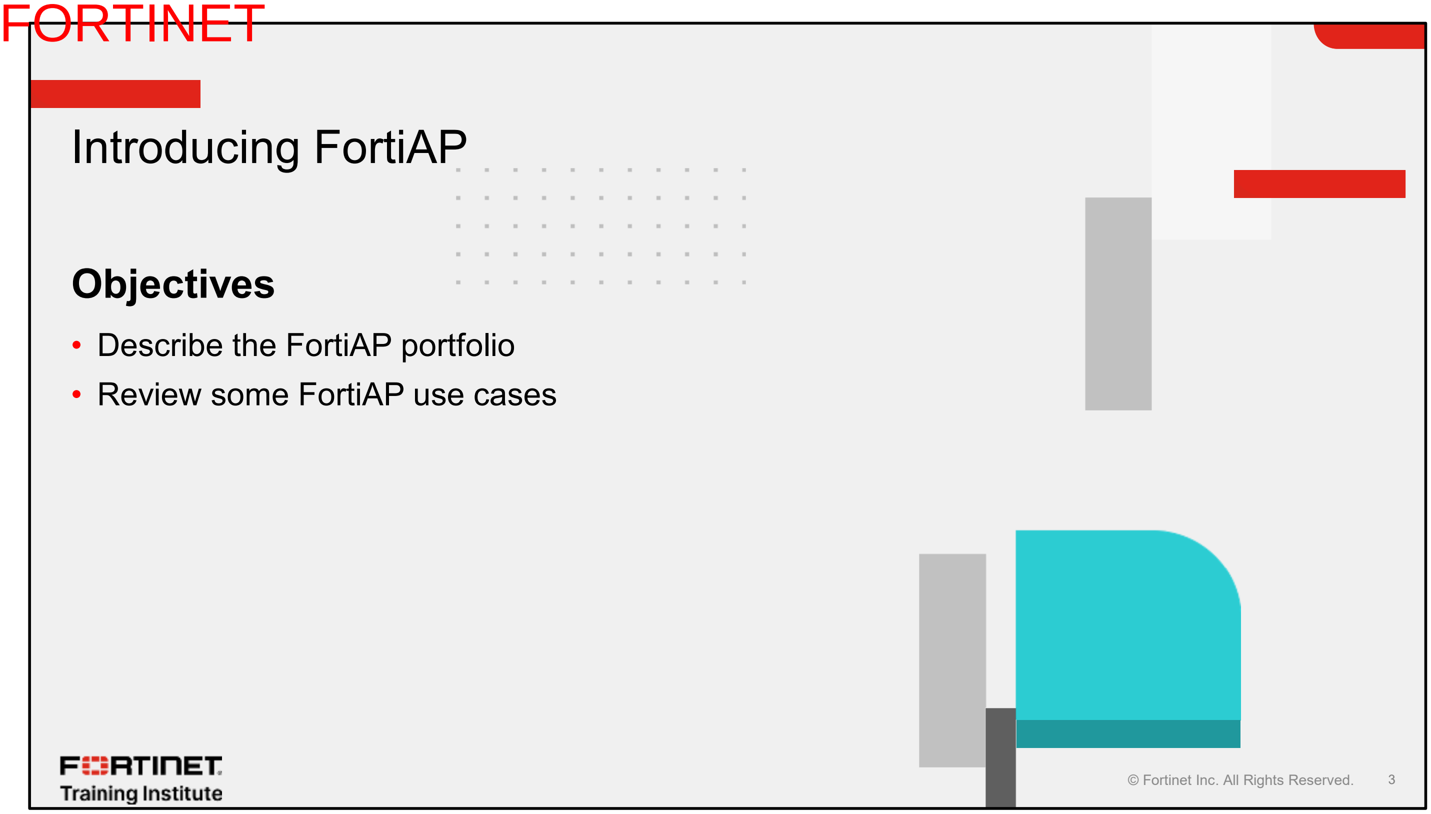
Lesson Overview

- Introducing FortiAP
- Integrated Wireless Controller
- Wireless Topologies
- FortiLAN Cloud Management

FORTINET Training Institute

2

In this lesson, you will learn about the topics shown on this slide.



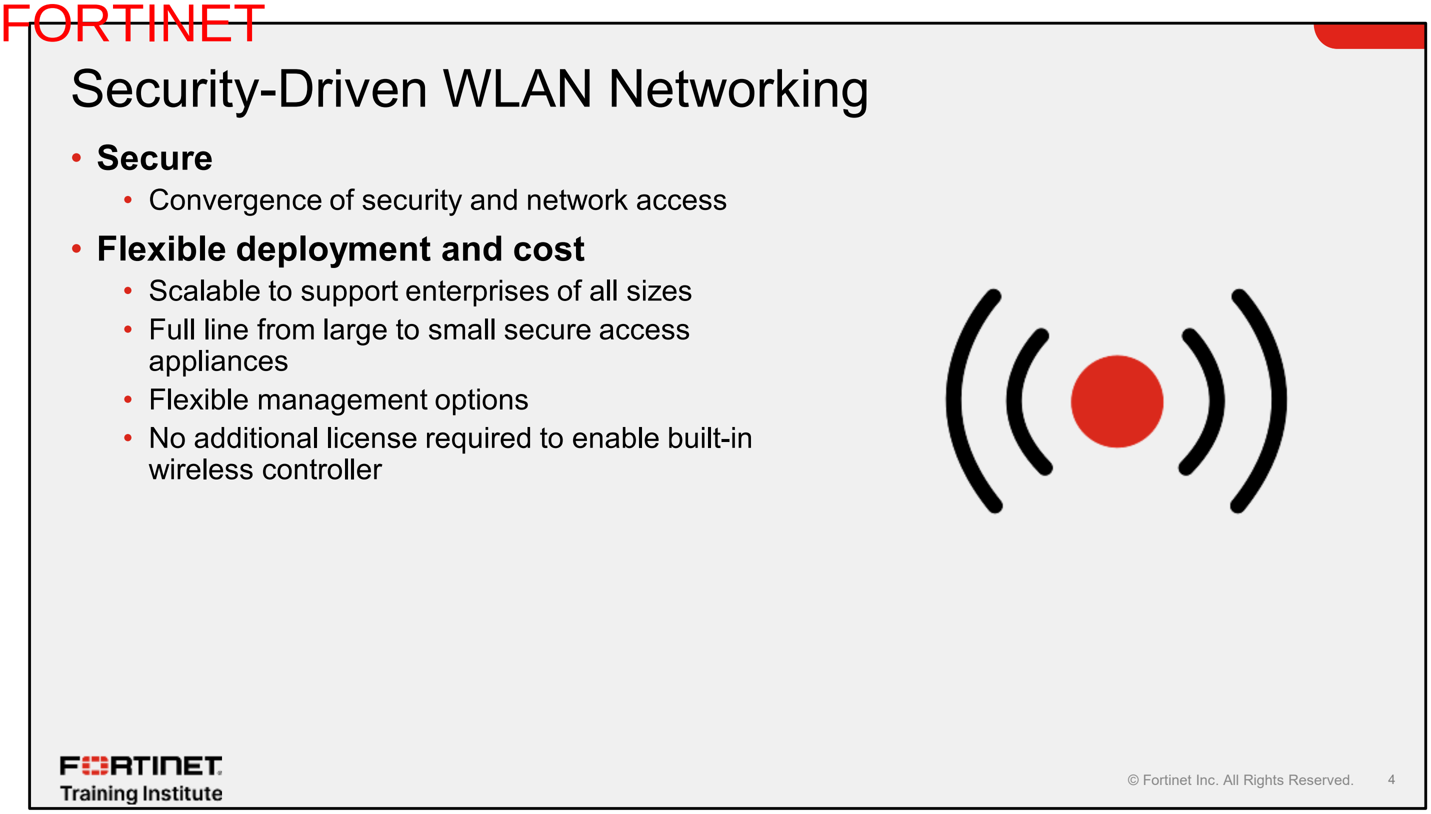
Introducing FortiAP

Objectives

- Describe the FortiAP portfolio
- Review some FortiAP use cases

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding FortiAP, you should be able to identify Fortinet wireless models and describe some use cases.



Security-Driven WLAN Networking

- **Secure**
  - Convergence of security and network access
- **Flexible deployment and cost**
  - Scalable to support enterprises of all sizes
  - Full line from large to small secure access appliances
  - Flexible management options
  - No additional license required to enable built-in wireless controller

FORTINET
Training Institute

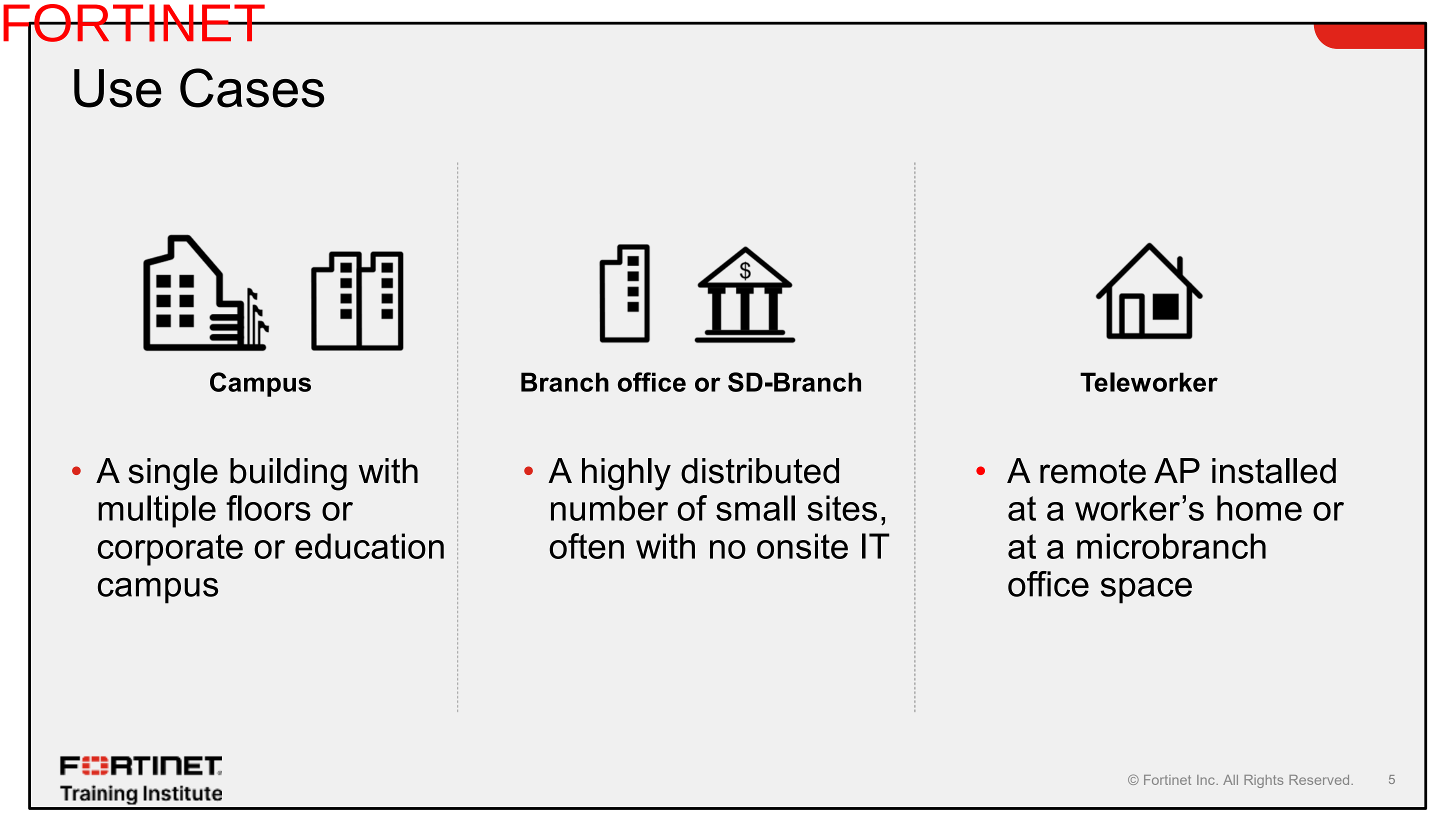
4

Wi-Fi is an important network medium in every type of business from small to medium to large enterprises, and in millions of homes.

Controller-managed wireless solutions that aren't integrated don't fit small and medium businesses (SMB), and pure cloud-managed solutions don't offer comprehensive security, which could expose users to the growing number of cyberthreats.

Fortinet secure wireless LAN (WLAN) meets the needs of these different use cases without sacrificing comprehensive security. It has several deployment models with an integrated wireless controller in FortiGate and FortiLAN Cloud.

The Fortinet integrated wireless solution provides single-pane-of-glass management for security and access. The integrated wireless solution includes the FortiGate network security platform, FortiAPs, and centralized management. FortiGate consolidates WLAN control, firewall, VPN gateway, a network intrusion prevention system (IPS), DLP, malware protection, web filtering, application control, and endpoint control on a single device. FortiGate does not require any additional licenses to enable built-in wireless controller functionality.



Use Cases

Campus

- A single building with multiple floors or corporate or education campus

Branch office or SD-Branch

- A highly distributed number of small sites, often with no onsite IT

Teleworker

- A remote AP installed at a worker's home or at a microbranch office space

FORTINET
Training Institute

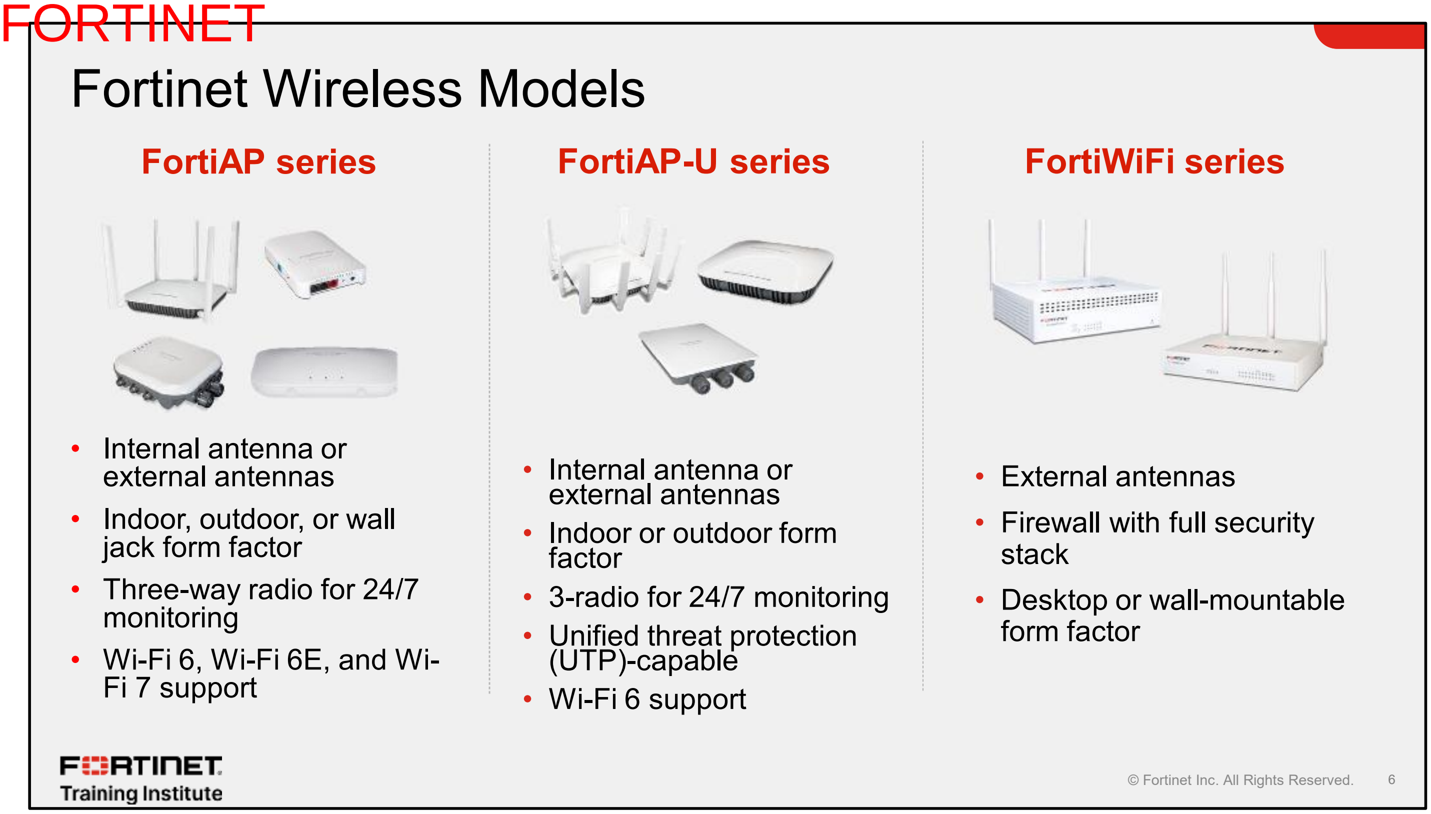
5

Fortinet offers three core use cases for secure WLAN:

- Campus: A single building with multiple floors, or a corporate or education campus with a group of large buildings. The support of designs including Dual 5GHz and tri-band with Wi-Fi 6E in FortiAPs allow a large number of client devices to attach to the network at the same time without over-air congestion.

- Branch or SD-Branch: A highly distributed number of small sites, often with no onsite IT. The built-in network access control (NAC) functionality in FortiOS allows secure onboarding of devices at remote locations where IT doesn't have reliable visibility.

- Teleworker: A remote AP installed at a worker's home or at microbranch office space. Split tunneling allows local traffic to remain local while sending other traffic to the data center for inspection when needed.



Fortinet Wireless Models

FortiAP series

- Internal antenna or external antennas
- Indoor, outdoor, or wall jack form factor
- Three-way radio for 24/7 monitoring
- Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 support

FortiAP-U series

- Internal antenna or external antennas
- Indoor or outdoor form factor
- 3-radio for 24/7 monitoring
- Unified threat protection (UTP)-capable
- Wi-Fi 6 support

FortiWiFi series

- External antennas
- Firewall with full security stack
- Desktop or wall-mountable form factor

FORTINET Training Institute

6

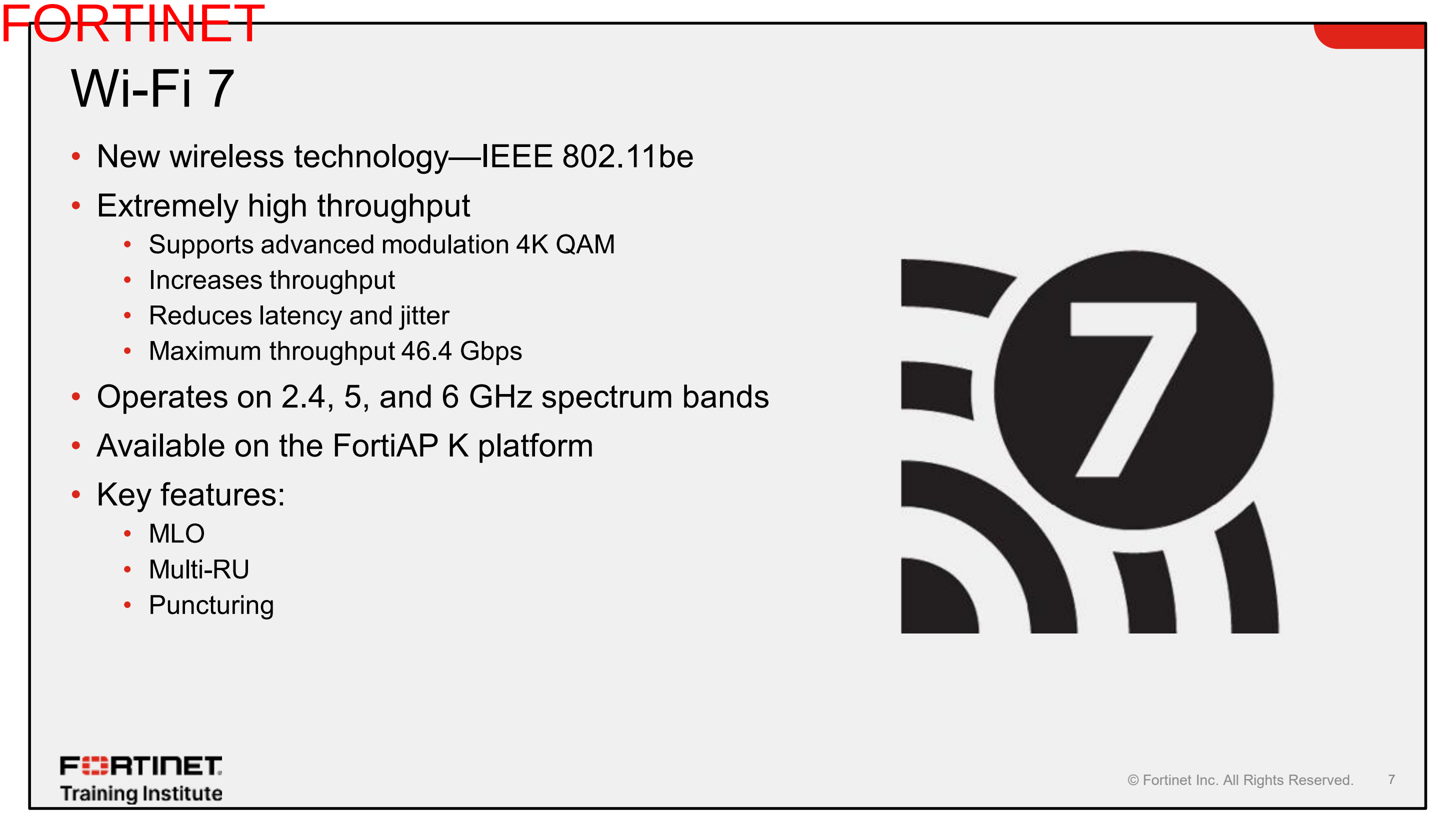
Fortinet has different Wi-Fi hardware platforms optimized for different use cases. The same security protection is available across these product families, which allows businesses to choose the topology and management model that suits them best, without giving up important security capabilities.

FortiAP devices are thin wireless access points (AP) supporting the latest Wi-Fi technologies (Wi-Fi 5, Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7), and the demand for plug-and-play deployment. FortiAP devices come in various form factors (desktop, indoor, outdoor, or wall jack). Fortinet's Security Fabric enables you to easily manage wired and wireless security from a single-pane-of-glass management console and protects your network from the latest security threats. Large deployments require multiple FortiAP devices.

The FortiAP-U series offers a wide range of models with the additional power of FortiGuard services and the flexibility of dual 5 GHz support for Wi-Fi 6 APs.

The FortiWiFi series consists of compact, standalone appliances that combine, in one platform, a full-featured wireless access point, a LAN switch, and an entry-level FortiGate device equipped with WAN features and security functionality. This is also referred to as thick AP and is suitable for a single AP to cover all areas.

Of course, Wi-Fi is not the only wireless technology. In addition to Wi-Fi devices, FortiOS also supports FortiExtender, so you can use cellular and other wireless modems as a WAN interface.



Wi-Fi 7

- New wireless technology—IEEE 802.11be
- Extremely high throughput
  - Supports advanced modulation 4K QAM
  - Increases throughput
  - Reduces latency and jitter
  - Maximum throughput 46.4 Gbps
- Operates on 2.4, 5, and 6 GHz spectrum bands
- Available on the FortiAP K platform
- Key features:
  - MLO
  - Multi-RU
  - Puncturing

FORTINET Training Institute

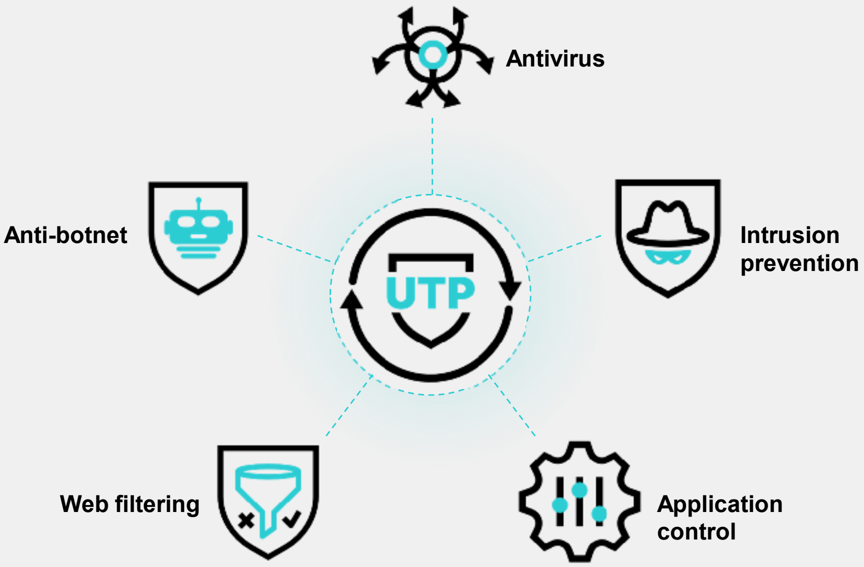
7

IEEE 802.11be is a new wireless technology (Wi-Fi 7) that introduces extremely high throughput (EHT) in wireless communication which features a boost in wireless bandwidth up to maximum of 46 Gbps. It enhances reliability and reduces latency and jitter in wireless connections and supports advanced modulation with 4K quadrature amplitude modulation (QAM)—4096 QAM..

Wi-Fi 7 is available in FortiAP K models and operates on 2.4 GHz, 5 GHz, and 6 GHz frequency bands, enhancing speed, reliability, and network performance across diverse environments.

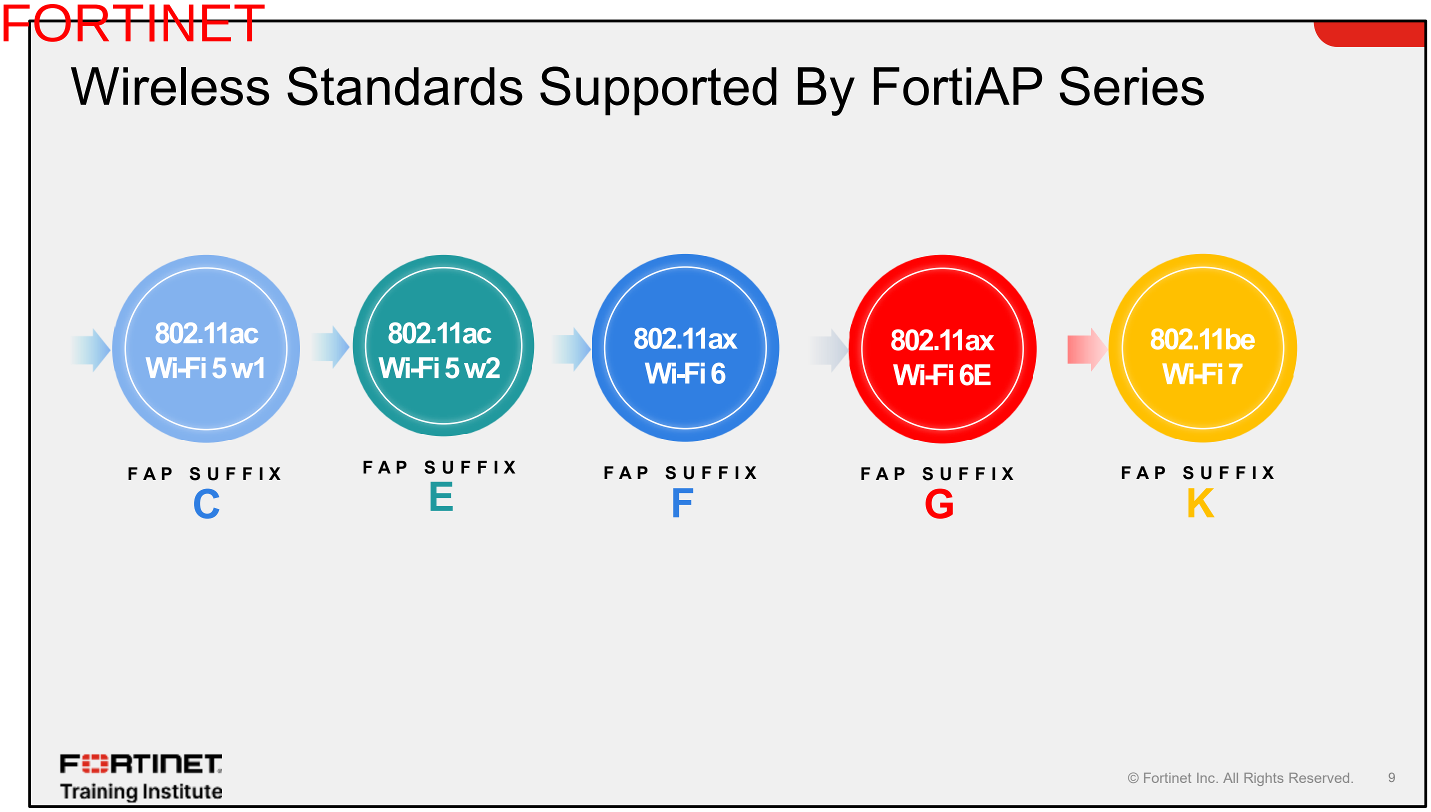
Wi-Fi 7 offers multilink operation (MLO) for simultaneous data transmission across all bands. It also offers Multi Resource Units (Multi-RU) for improved channel usage. Puncturing is another feature Wi-Fi 7 offers, to allow access points and clients to share channels if interference is present, to continue use as much of the spectrum of channels as possible.

UTP Module



8

The Unified Threat Protection (UTP) module is supported only on FortiAP-U models. An additional license is required to enable this feature. UTP is ideal for small remote branch office deployments, where the FortiAP is managed by FortiLAN Cloud and no on-premises FortiGate devices are deployed. UTP-enabled FortiAP-U models also work with bridged SSID when a FortiGate wireless controller manages FortiAP.



Wireless Standards Supported By FortiAP Series

802.11ac Wi-Fi 5 w1 — FAP SUFFIX C

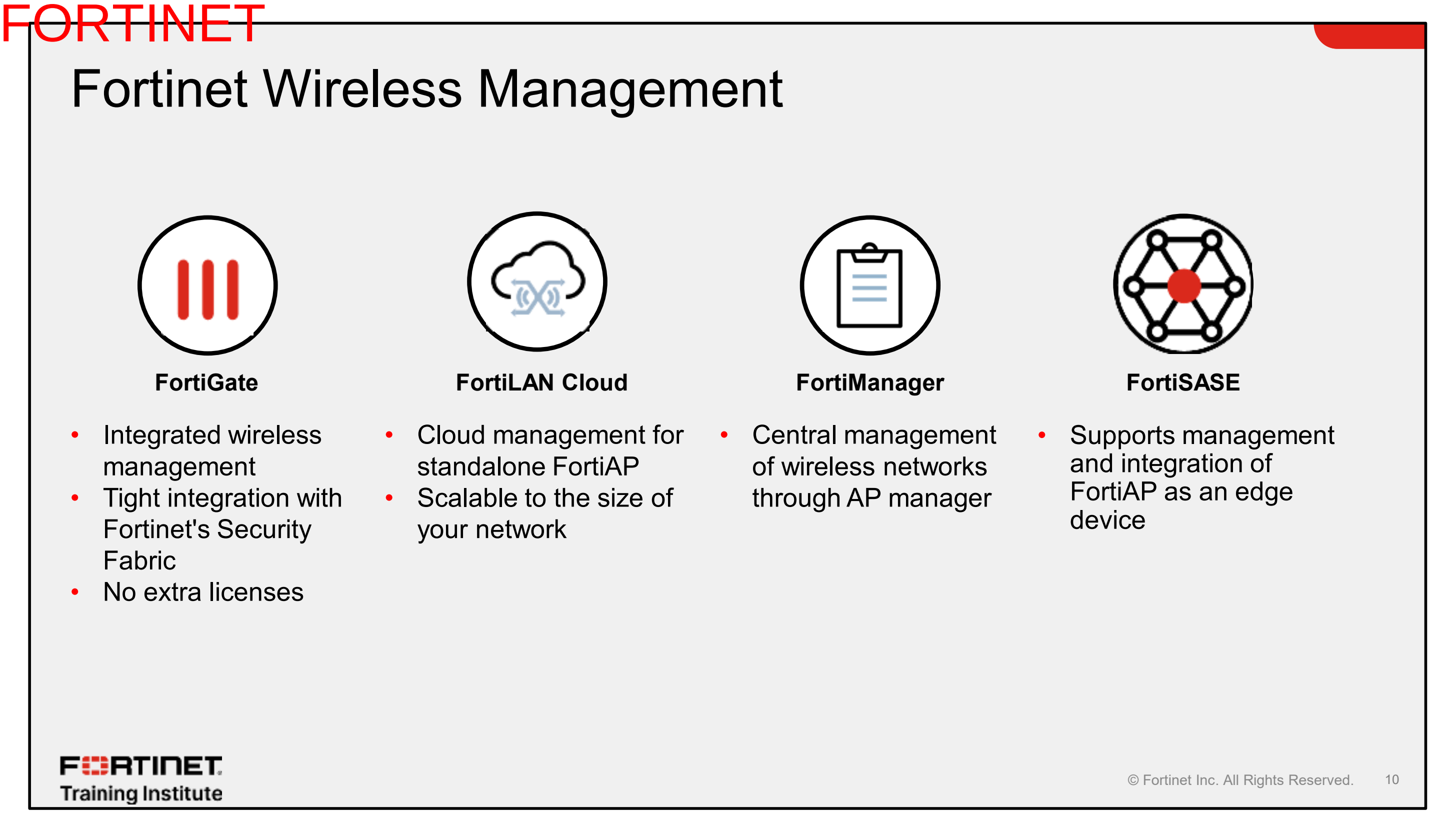
802.11ac Wi-Fi 5 w2 — FAP SUFFIX E

802.11ax Wi-Fi 6 — FAP SUFFIX F

802.11ax Wi-Fi 6E — FAP SUFFIX G

802.11be Wi-Fi 7 — FAP SUFFIX K

This slide shows the different wireless standards supported by different FortiAP models based on their suffixes. For example, FAP-443K supports Wi-Fi 7, FAP-231G supports Wi-Fi 6E, FAP-234F supports Wi-Fi 6, and so on.



Fortinet Wireless Management

FortiGate

- Integrated wireless management
- Tight integration with Fortinet's Security Fabric
- No extra licenses

FortiLAN Cloud

- Cloud management for standalone FortiAP
- Scalable to the size of your network

FortiManager

- Central management of wireless networks through AP manager

FortiSASE

- Supports management and integration of FortiAP as an edge device

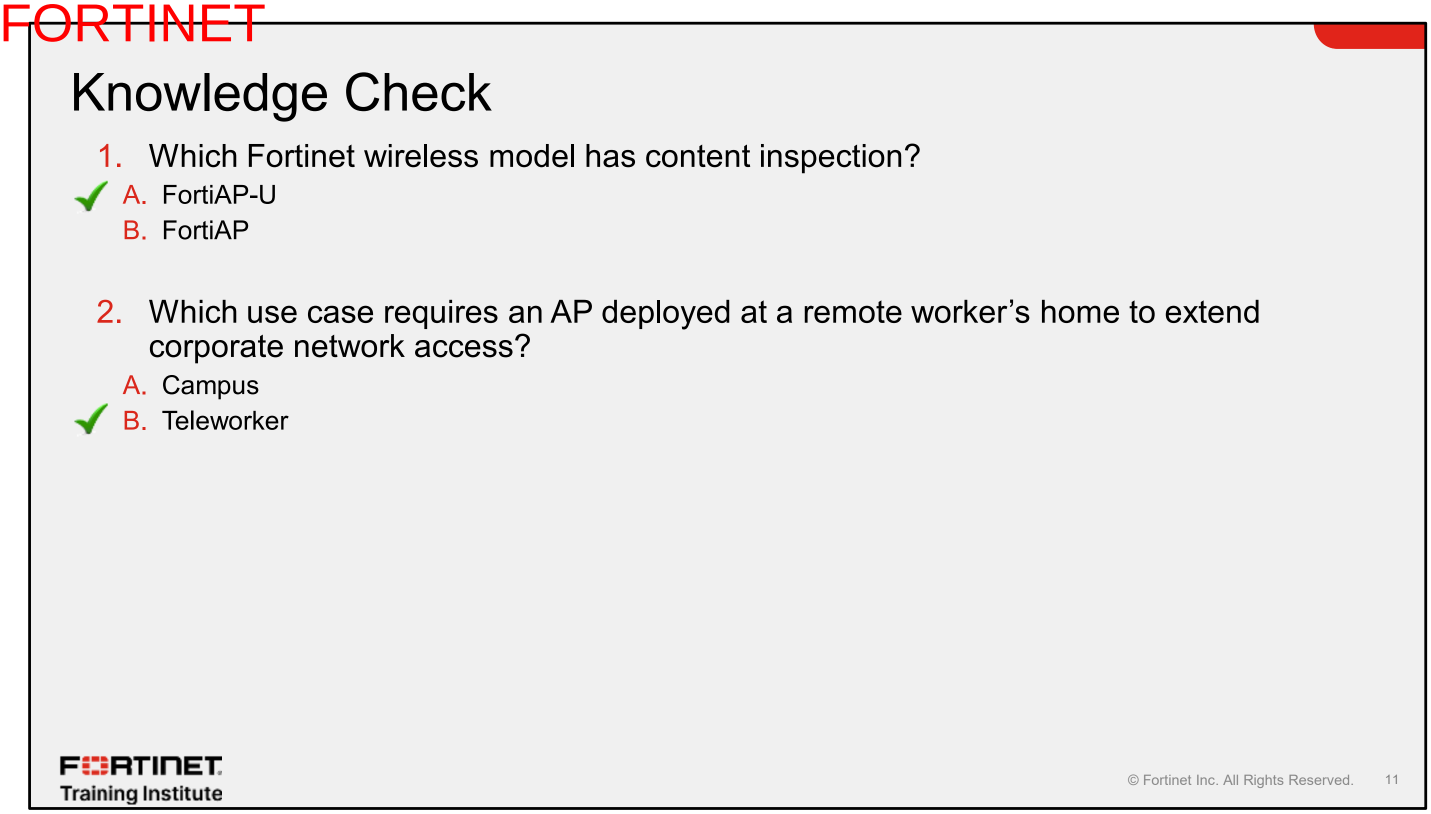
10

The FortiGate wireless controller provides a single point of management for all the APs deployed in the network. All FortiGate and FortiWiFi devices have built-in wireless controllers that are used for integrated secure wireless access. The maximum number of supported APs varies based on the FortiGate model. FortiGate does not require any additional licenses to enable built-in wireless controller functionality. This results in security-driven networking, where the network is converged with, and driven by, security. Wireless access controllers are commonly referred to as ACs.

FortiLAN Cloud management allows for centralized hosted cloud control of standalone FortiAP devices, scaling from a handful to thousands of FortiAP devices. A FortiLAN Cloud subscription enables advanced features and troubleshooting plus additional configuration options and log retention. FortiLAN Cloud management is recommended for environments where FortiGate does not manage FortiAP.

The **AP Manager** on FortiManager allows you to manage FortiAP access points that are controlled by FortiGate devices and are managed by FortiManager.

FortiSASE connects to FortiAP as an edge device for management. This allows microbranch deployment, where a branch office with FortiAP is managed over a backhaul connection to FortiSASE.



Knowledge Check

1. Which Fortinet wireless model has content inspection?

✓ A. FortiAP-U

B. FortiAP

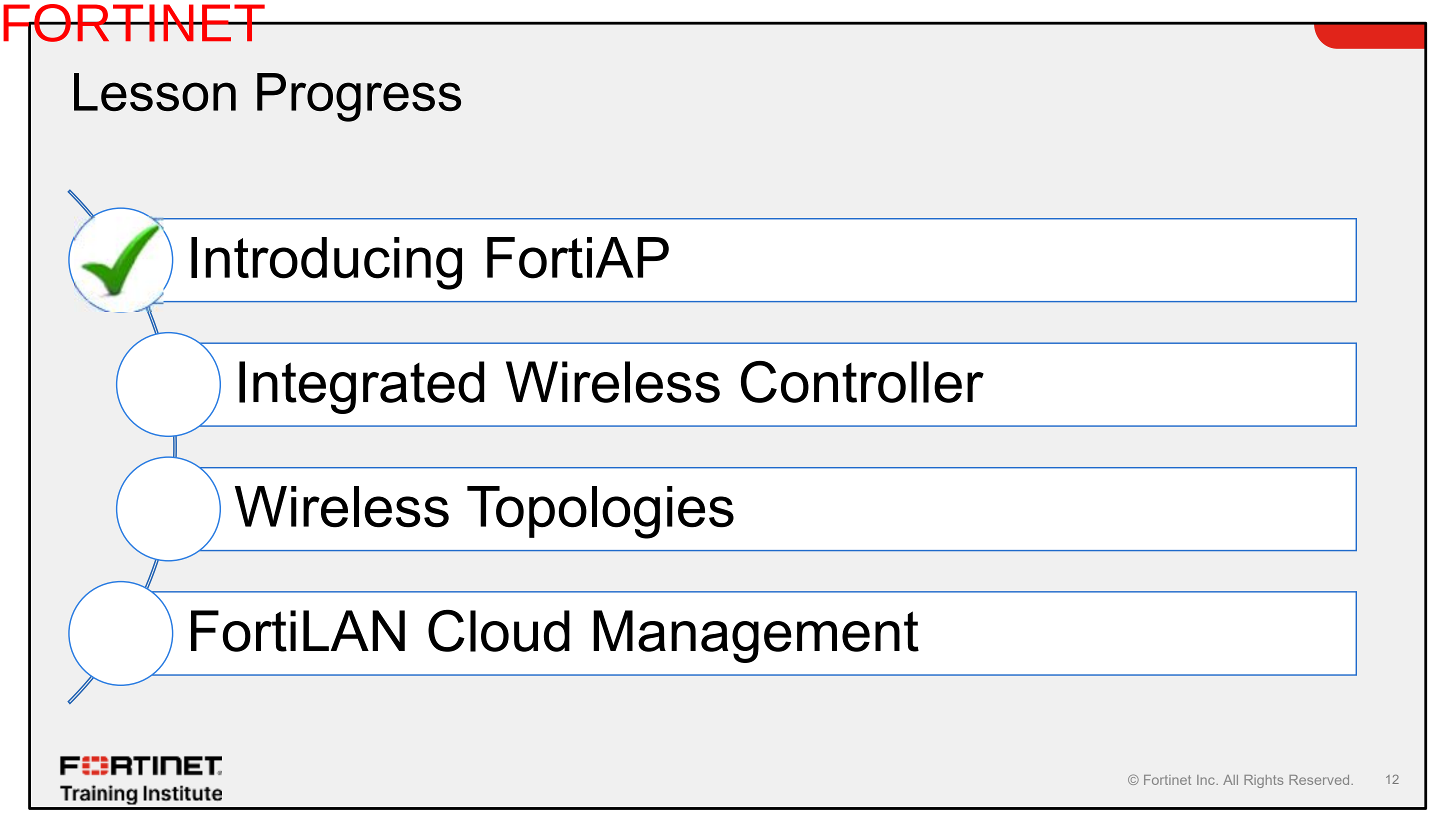
2. Which use case requires an AP deployed at a remote worker's home to extend corporate network access?

A. Campus

✓ B. Teleworker

FORTINET Training Institute

11



Lesson Progress

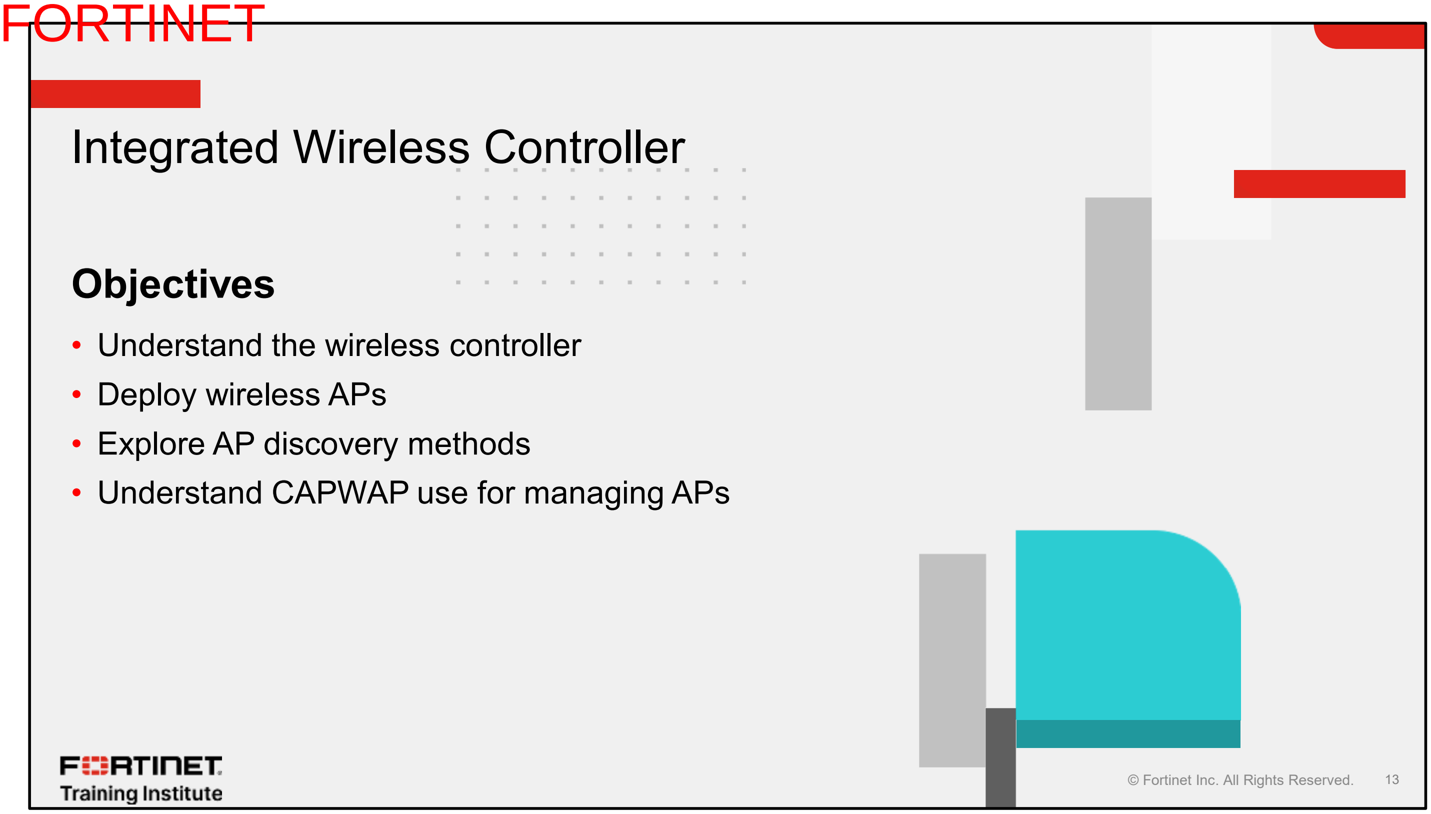
- ✓ Introducing FortiAP
- ○ Integrated Wireless Controller
- ○ Wireless Topologies
- ○ FortiLAN Cloud Management

FORTINET Training Institute

12

Good job! You now understand FortiAP basics.

Now, you will learn about the FortiGate integrated wireless controller.



Integrated Wireless Controller

Objectives

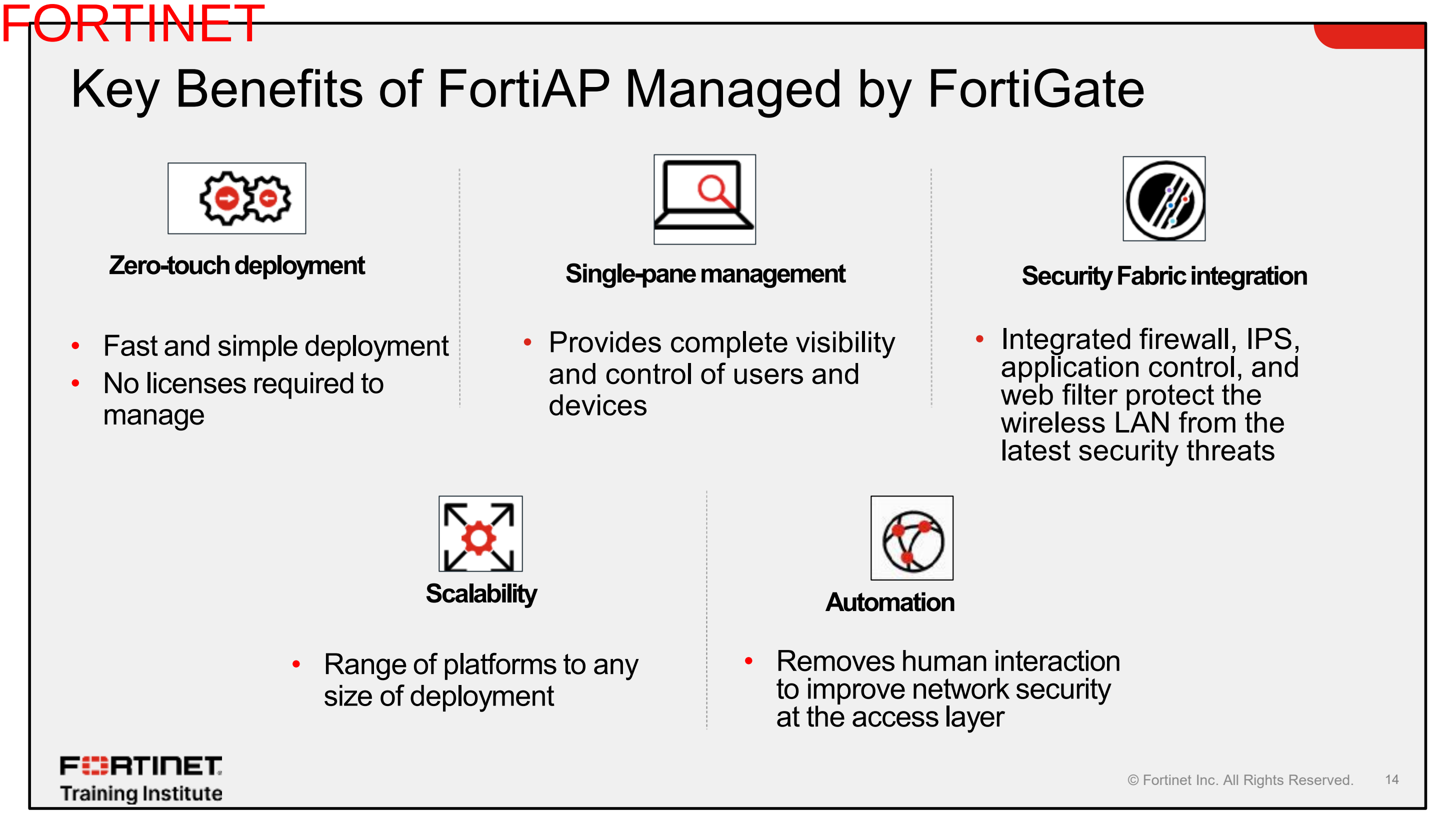
- Understand the wireless controller
- Deploy wireless APs
- Explore AP discovery methods
- Understand CAPWAP use for managing APs

FORTINET
Training Institute

13

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of the FortiGate integrated wireless controller, you will be able to deploy FortiAP.



Key Benefits of FortiAP Managed by FortiGate

Zero-touch deployment

- Fast and simple deployment
- No licenses required to manage

Single-pane management

- Provides complete visibility and control of users and devices

Security Fabric integration

- Integrated firewall, IPS, application control, and web filter protect the wireless LAN from the latest security threats

Scalability

- Range of platforms to any size of deployment

Automation

- Removes human interaction to improve network security at the access layer

FORTINET Training Institute

Managing FortiAP devices using FortiGate offers the following important key benefits:

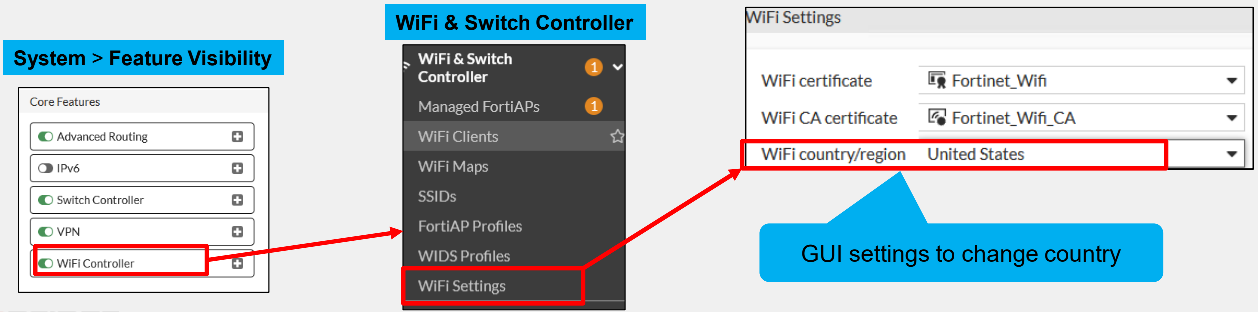
- Zero-touch deployment: FortiGate can automatically authorize FortiAP without the administrator’s manual authorization. No additional licenses are required to manage FortiAP devices with FortiGate.
- Single-pane management: You can manage FortiAP using FortiGate or FortiManager. Administrators are not required to log in to FortiAP.
- Security Fabric integration: You configure firewall policies using FortiAP SSIDs in the same way as FortiGate interfaces. FortiGate and FortiManager handle authentication and authorization.
- Scalability: FortiAP devices are available in range of platforms to support any size of deployment.
- Automation: The built-in NAC functionality on FortiOS allows secure onboarding on devices, and endpoints can be quarantined automatically using the Security Fabric automation stitch.

Enabling the Wireless Controller

- Required to discover and manage FortiAP devices on FortiGate
- To enable the wireless controller on FortiGate (enabled on most models):

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

- To display the wireless controller settings on the FortiGate GUI (enabled by default):



Core Features

- Advanced Routing
- IPv6
- Switch Controller
- VPN
- WiFi Controller

WiFi Settings

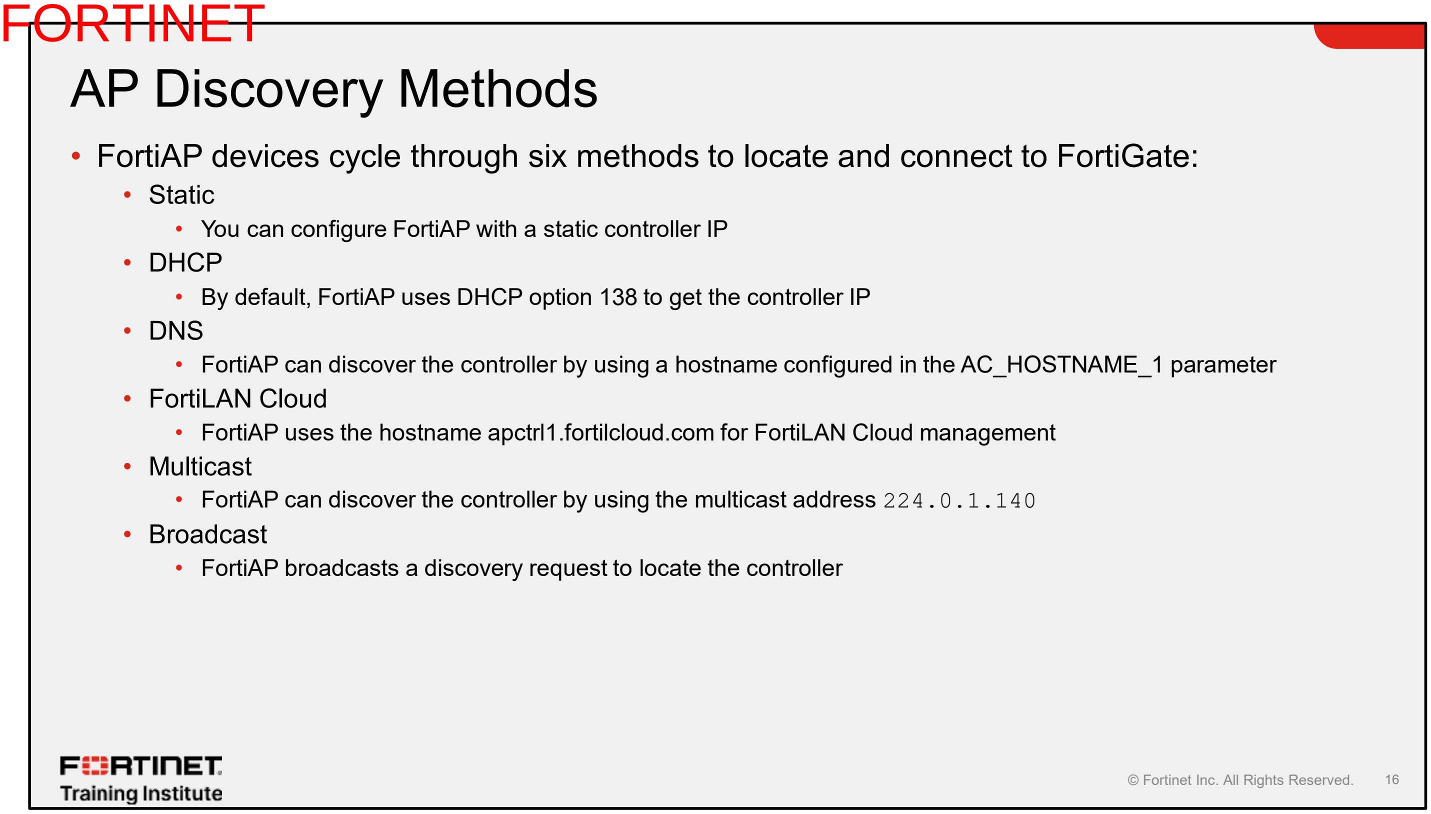
WiFi certificate: Fortinet_Wifi
WiFi CA certificate: Fortinet_Wifi_CA
WiFi country/region: United States

Training Institute

Before you can manage your FortiAP device on FortiGate, you must ensure the wireless controller feature is enabled on FortiGate, so FortiGate can discover and manage connected FortiAP devices. By default, the wireless controller feature is enabled on most FortiGate models.

After you enable the wireless controller feature, the related wireless controller settings appear on the GUI in the **WiFi & Switch Controller** section. If the GUI settings are unavailable, make sure that the **WiFi Controller** feature is enabled on the **Feature Visibility** page.

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 Wi-Fi controller is configured for the United States. If you are located in any other region, set your geographic location before you begin the wireless network configuration. You can set your geographic location by clicking **WiFi & Switch Controller** > **WiFi Settings**, and then select the country from the **WiFi country/region** menu.



AP Discovery Methods

- FortiAP devices cycle through six methods to locate and connect to FortiGate:
  - Static
    - You can configure FortiAP with a static controller IP
  - DHCP
    - By default, FortiAP uses DHCP option 138 to get the controller IP
  - DNS
    - FortiAP can discover the controller by using a hostname configured in the AC_HOSTNAME_1 parameter
  - FortiLAN Cloud
    - FortiAP uses the hostname apctrl1.fortilcloud.com for FortiLAN Cloud management
  - Multicast
    - FortiAP can discover the controller by using the multicast address `224.0.1.140`
  - Broadcast
    - FortiAP broadcasts a discovery request to locate the controller

FORTINET Training Institute

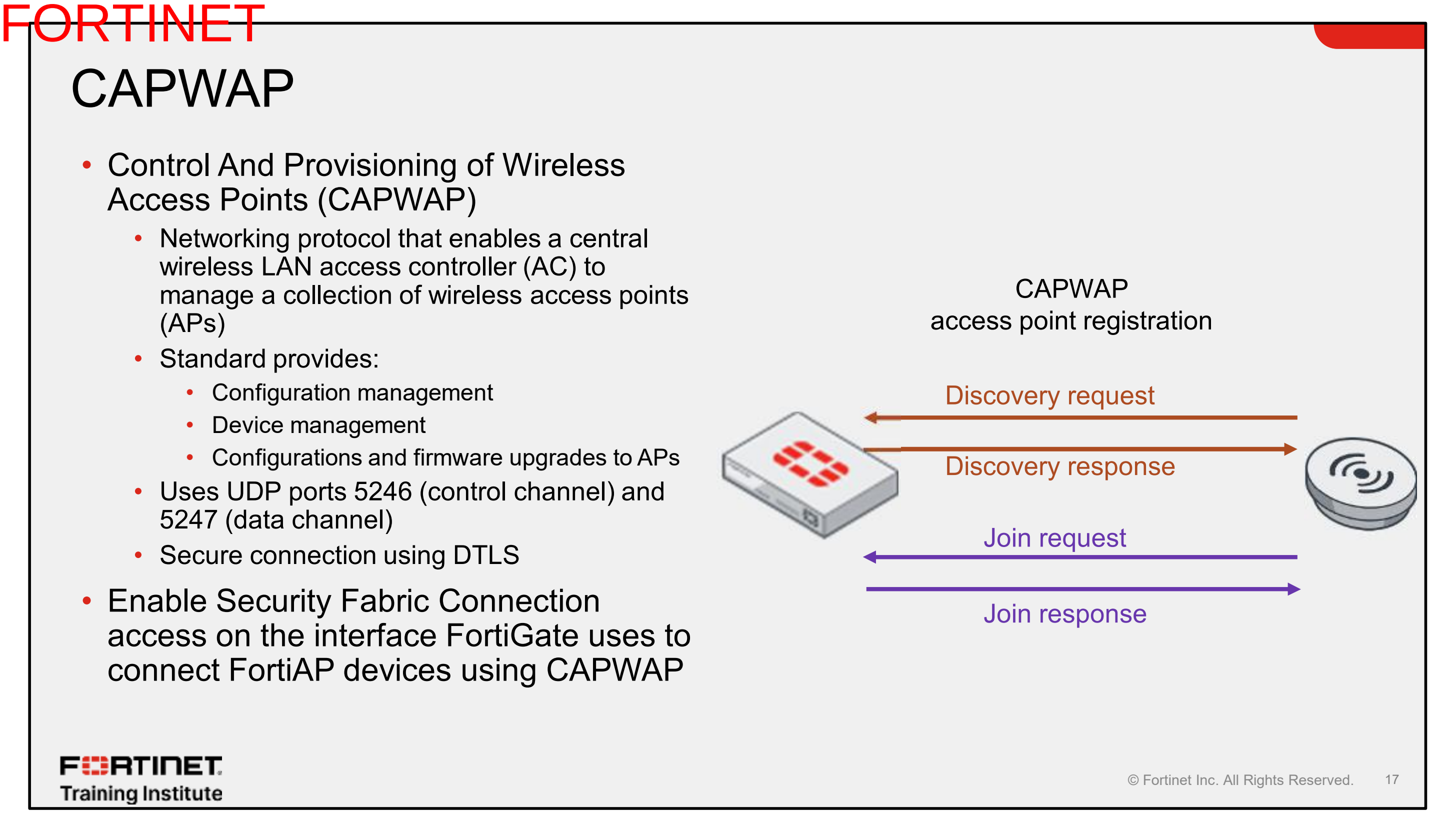
16

By default, the FortiAP discovery method is set to auto, which means the AP will cycle through the discovery methods and sequence shown on this slide to locate a wireless controller. For every discovery type, FortiAP sends out discovery requests and sets a timer for an interval of a random number of seconds—2 to 180. The default is 5 seconds. Using the FortiGate CLI, you can modify this value with the following command:

```
config wireless-controller timers
  set discovery-interval 5
end
```

After the timeout is reached, FortiAP sends out another discovery request, up to a maximum of three times. After approximately 3 to 15 seconds, if FortiAP has no AC connection, it will switch to another discovery type and repeat the process until the last broadcast fails, leading to SULKING state. After approximately 30 seconds, FortiAP will enter the AC_IP_DISCVER state. After the AC IP is found, it will enter the IDLE state, and will eventually enter the DISCOVERY state, then repeat the process.You can use static IP or DNS hostname methods when the AP is not deployed on the same subnet as the wireless controller and cannot be reached by the multicast or broadcast method. You must make this configuration change on the FortiAP devices manually, before deploying them. You can configure a static IP or DNS on a FortiAP using the GUI or CLI including the serial port on FortiAP.

By default, FortiAP uses DHCP option 138 to receive the wireless controller IP address. You need to convert the IP address of the wireless controller 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. The AP unit sends a multicast discovery request and the controller replies with a unicast discovery response message to the AP. The AP and the controller do not need to be in the same broadcast domain, if multicast routing is correctly configured. The default multicast destination address is `224.0.1.140`. You can change it using the CLI, but you must make the changes to both the controller and to the AP.



CAPWAP

- Control And Provisioning of Wireless Access Points (CAPWAP)
  - Networking protocol that enables a central wireless LAN access controller (AC) to manage a collection of wireless access points (APs)
  - Standard provides:
    - Configuration management
    - Device management
    - Configurations and firmware upgrades to APs
  - Uses UDP ports 5246 (control channel) and 5247 (data channel)
  - Secure connection using DTLS
- Enable Security Fabric Connection access on the interface FortiGate uses to connect FortiAP devices using CAPWAP

CAPWAP
access point registration

Discovery request

Discovery response

Join request

Join response

CAPWAP is a network protocol that you can use to provision and manage FortiAP devices using FortiGate. CAPWAP allows an AC to manage a collection of wireless APs. In the Fortinet integrated wireless solution, CAPWAP enables you to manage the configuration and device, and push firmware upgrades to FortiAP devices.

You must enable the **Security Fabric Connection** access on the interface FortiGate uses to connect FortiAP devices using CAPWAP. You also need to enable DHCP.

CAPWAP uses UDP port 5246 as the control channel and port 5247 as the data channel. CAPWAP-enabled devices can create a secure data channel to the AC using DTLS encryption. CAPWAP provides direct administrator access to a FortiGate interface, so it must be enabled on the interface that the FortiAP devices will be connecting to.

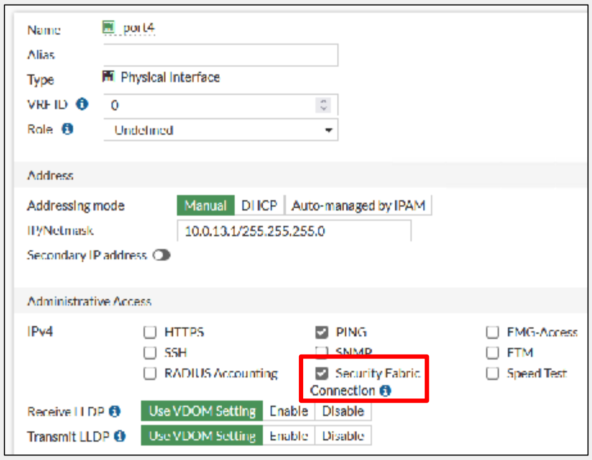
The CAPWAP discovery process is as follows:

1. FortiAP devices send a discovery request. FortiGate responds with a discovery response.
2. Both devices establish a secure DTLS session.
3. After FortiGate authorizes the FortiAP, the CAPWAP discovery and join phase takes place.
4. After the CAPWAP tunnel is established, FortiGate sends all required management and WLAN-related configuration to FortiAP.

Enabling the Security Fabric Connection

- To use CAPWAP, you must enable **Security Fabric Connection** access on the interface FortiGate uses to connect FortiAP devices
- Open ports for communication for CAPWAP on UDP ports
  - 5246 control channel
  - 5247 data channel
- Enable DHCP to automatically assign IP addresses to APs

Network > Interface



Name	port4
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask	10.0.13.1/255.255.255.0
Secondary IP address	○

Administrative Access

IPv4	□ HTTPS	☑ PING	□ FMG-Access
	□ SSH	□ SNMP	□ FTM
	□ RADIUS Accounting	☑ Security Fabric Connection	□ Speed Test
Receive LLDP	[✓ Use VDOM Setting] Enable Disable		
Transmit LLDP	[✓ Use VDOM Setting] Enable Disable		

FORTINET Training Institute

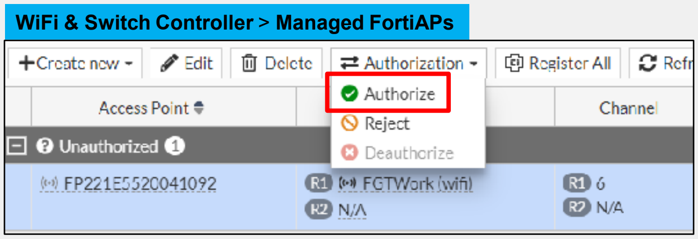
18

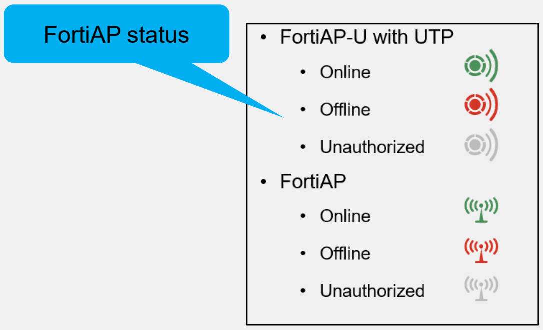
On FortiGate, choose an interface to which you will connect FortiAP devices. You must enable **Security Fabric Connection** access on the interface to use CAPWAP. Enable the DHCP server option to give IP addresses to FortiAP devices, instead of manually configuring the IP address on each AP.

Authorizing an AP

- FortiOS lists all discovered APs in the **Managed FortiAPs** window
  - Discovered APs are unavailable
- Right-click an AP, and then click **Authorization** > **Authorize** to start managing the AP
  - FortiOS will push configuration to the AP and automatically assign a default AP profile based on the model of the AP
- To allow the wireless controller to authorize new discovered FortiAP automatically:

```
config system interface
edit <interface where FortiAP is connected>
set auto-auth-extension-device enable
end
```




FortiAP status

- FortiAP-U with UTP
  - Online
  - Offline
  - Unauthorized
- FortiAP
  - Online
  - Offline
  - Unauthorized

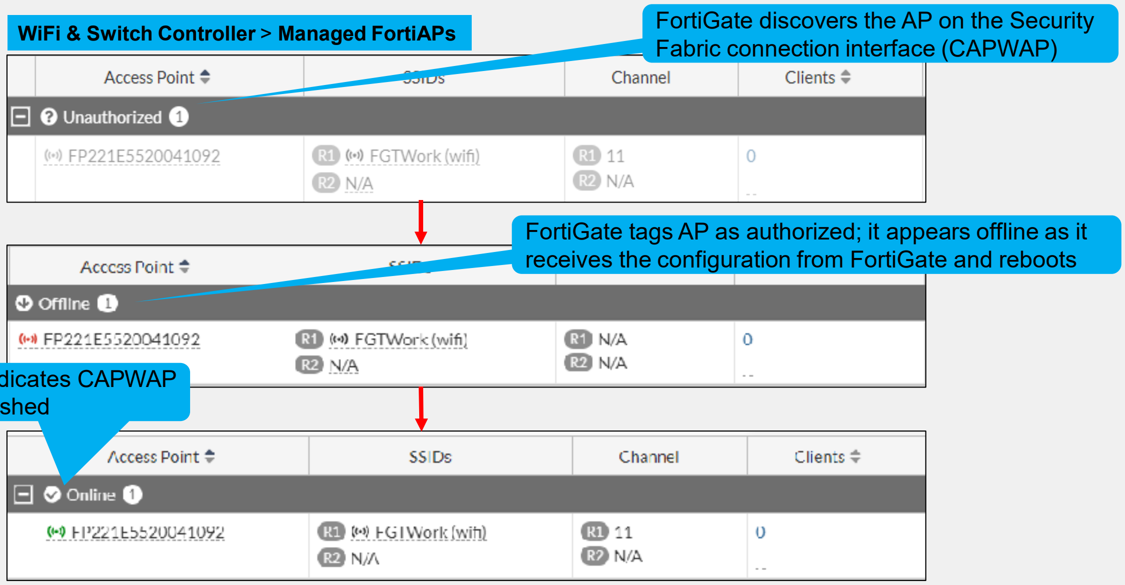
Fortinet Training Institute

19

You can connect the FortiAP to the interface. After some time, it will appear in the **Managed FortiAPs** list. At this stage, the AP is unavailable. Right-click the AP and then click **Authorization** > **Authorize** in the drop-down list, or select an AP, and then click **Authorization** > **Authorize**. This is required because the AP will not function unless it is authorized.

After an AP connects to FortiGate, FortiGate assigns a default profile for the AP model to the authorized AP.

Authorizing an AP (Contd)



WiFi & Switch Controller > Managed FortiAPs

FortiGate discovers the AP on the Security Fabric connection interface (CAPWAP)

Access Point ⬍	SSIDs	Channel	Clients ⬍
⊟ ? Unauthorized 1			
FP221E5520041092	R1 FGTWork (wifi) R2 N/A	R1 11 R2 N/A	0 --

FortiGate tags AP as authorized; it appears offline as it receives the configuration from FortiGate and reboots

Access Point ⬍			
Offline 1			
FP221E5520041092	R1 FGTWork (wifi) R2 N/A	R1 N/A R2 N/A	0 --

Green status indicates CAPWAP tunnel is established

Access Point ⬍	SSIDs	Channel	Clients ⬍
⊟ ✓ Online 1			
FP221E5520041092	R1 FGTWork (wifi) R2 N/A	R1 11 R2 N/A	0 --

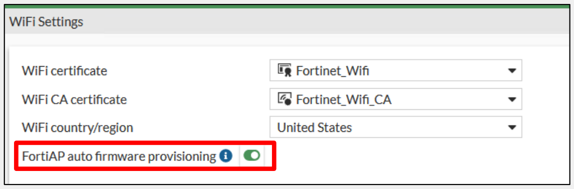
20

This slide shows the different statuses of FortiAP during authorization by FortiGate.

Firmware Upgrade—Automatic

- Multiple ways to upgrade the FortiAP firmware:
  - FortiAP auto firmware provisioning
    - Automatically upgrade newly discovered FortiAPs with the most recent compatible firmware
  - Automatic firmware updates
    - Upgrade FortiAPs at a scheduled time within the same firmware train

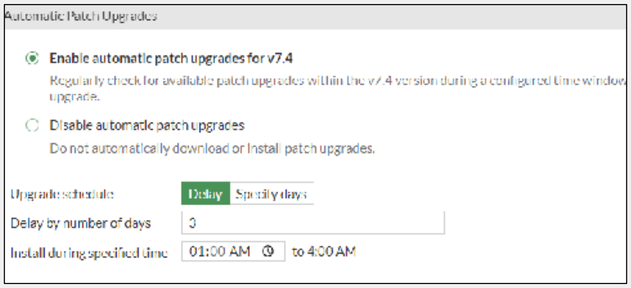
WiFi & Switch Controller > WiFi Settings



WiFi Settings

WiFi certificate	Fortinet_Wifi
WiFi CA certificate	Fortinet_Wifi_CA
WiFi country/region	United States
FortiAP auto firmware provisioning	●

System > Firmware & Registration



Automatic Patch Upgrades

● Enable automatic patch upgrades for v7.4
Regularly check for available patch upgrades within the v7.4 version during a configured time window upgrade.

○ Disable automatic patch upgrades
Do not automatically download or install patch upgrades.

Upgrade schedule: [✓ Delay] Specify days
Delay by number of days: 3
Install during specified time: 01:00 AM to 4:00 AM

FORTINET Training Institute

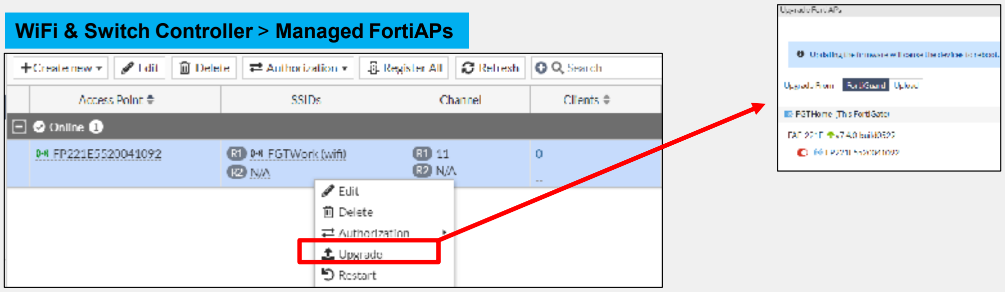
21

You can enable **FortiAP auto firmware provisioning** on the **WiFi Settings** page. When enabled, newly discovered FortiAPs are automatically upgraded to the latest compatible firmware. This happens once during authorization.

On the **Firmware & Registration** page, deselect **Disabled automatic patch upgrades**. Select **Enable automatic patch upgrades for v7.4**, and then schedule a date and time for your upgrade. This upgrades the FortiAP device directly to the target version.

Firmware Upgrade—Manual

- Use the firmware upgrade tool on the GUI



WiFi & Switch Controller > Managed FortiAPs

Updating the firmware will cause the device to reboot.

- Upload firmware image to FortiGate

```
execute wireless-controller upload-wtp-image <tftp/ftp> <filename> <IP of server>
```

- Upgrade all FortiAP devices

```
execute wireless-controller reset-wtp all
```

FORTINET Training Institute

22

You can manually upgrade the firmware on a FortiAP device using the FortiGate GUI. Go to the **Managed FortiAPs** page, right-click the target FortiAP device, and then click the **Upgrade** button. Then, you can choose to have FortiGate download the firmware upgrade file from FortiGuard or upload your local firmware image. You can upgrade only one FortiAP at a time using the GUI.

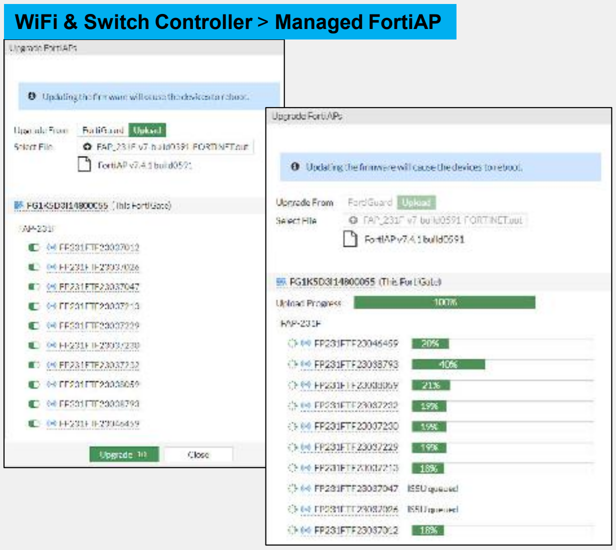
You can also upgrade the firmware of a FortiAP device using the FortiGate CLI. For this, you must first upload the target firmware image to FortiGate from an FTP or TFTP server. You can upgrade all the FortiAP devices at the same time using the CLI command `execute wireless-controller reset-wtp all`. This command pushes the firmware from the FortiOS wireless controller to the FortiAP devices. A FortiAP device reboots after the firmware is installed.

Hitless Rolling FortiAP Upgrade

- Enable hitless rolling to upgrade multiple FortiAP devices
- Hitless upgrade algorithm
  - Staggered approach
  - FortiAP devices connected to each other upgrade immediately
  - Other devices provide wireless connectivity
- Enable global hitless first on CLI

```
config wireless-controller global
  set rolling-wtp-upgrade enable
  set rolling-wtp-upgrade-threshold -70
end
config wireless-controller setting
  set rolling-wtp-upgrade enable
end
```

WiFi & Switch Controller > Managed FortiAP



Upgrade FortiAPs

Updating the firmware will cause the devices to reboot.

Upgrade From: FortiGuard | Upload
Select File: FAP_231F v7-build0591-FORTINET.out
FortiAP v7.4.1 build0591

FG1K5D3I14800055 (This FortiGate)

FAP-231F

- FP231FTF23037012
- FP231FTF23037026
- FP231FTF23037047
- FP231FTF23037213
- FP231FTF23037229
- FP231FTF23037230
- FP231FTF23037232
- FP231FTF23038059
- FP231FTF23038793
- FP231FTF23046459

Upgrade 10 | Close

Upgrade FortiAPs

Updating the firmware will cause the devices to reboot.

Upgrade From: FortiGuard | Upload
Select File: FAP_231F v7-build0591-FORTINET.out
FortiAP v7.4.1 build0591

FG1K5D3I14800055 (This FortiGate)

Upload Progress: 100%

FAP-231F

FP231FTF23046459	20%
FP231FTF23038793	40%
FP231FTF23038059	21%
FP231FTF23037232	19%
FP231FTF23037230	19%
FP231FTF23037229	19%
FP231FTF23037213	18%
FP231FTF23037047	ISSU queued
FP231FTF23037026	ISSU queued
FP231FTF23037012	18%

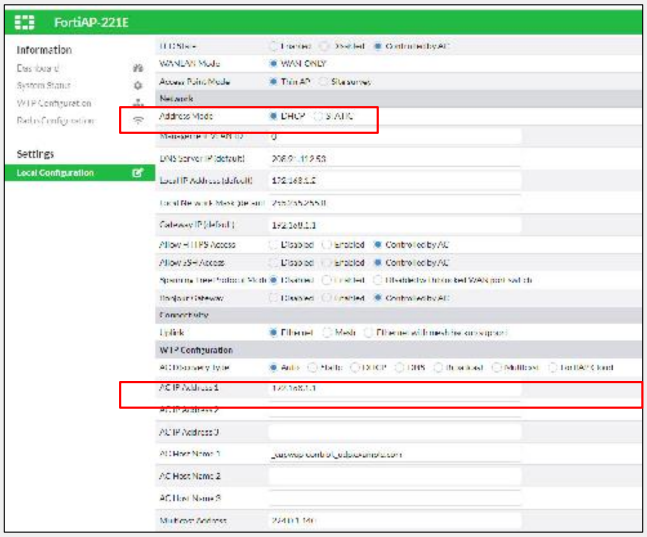
Hitless upgrade helps update FortiAP firmware in bulk without interrupting wireless services to clients. It uses an algorithm that upgrades FortiAP in a staggered process and continues to provide wireless communication. You will have to enable global hitless setting first before you can perform hitless upgrade.

FortiAP GUI Access

- IP address:
  - Assigned by DHCP server
- HTTPS access enabled by default when unmanaged
- Default login:

  User: `admin`

  Password: (blank)
  - Both are case sensitive
  - Modify the default (blank) password



FortiAP-221E

Information
- Dashboard
- System Status
- WTP Configuration
- Radio Configuration

Settings
- Local Configuration

LED State ○ Enabled ○ Disabled ● Controlled by AC
WAN-LAN Mode ● WAN ONLY
Access Point Mode ● Thin AP ○ Site survey

Network
Address Mode ● DHCP ○ STATIC
Management VLAN ID 0
DNS Server IP (default) 208.91.112.53
Local IP Address (default) 192.168.1.2
Local Network Mask (default) 255.255.255.0
Gateway IP (default) 192.168.1.1
Allow HTTPS Access ○ Disabled ○ Enabled ● Controlled by AC
Allow SSH Access ○ Disabled ○ Enabled ● Controlled by AC
Spanning Tree Protocol Mode ● Disabled ○ Enabled ○ Disabled by Untrusted WAN port switch
Bonjour Gateway ○ Disabled ○ Enabled ● Controlled by AC

Connectivity
Uplink ● Ethernet ○ Mesh ○ Ethernet with mesh backup support

WTP Configuration
AC Discovery Type ● Auto ○ Static ○ DHCP ○ DNS ○ Broadcast ○ Multicast ○ FortiAP Cloud
AC IP Address 1 192.168.1.1
AC IP Address 2
AC IP Address 3
AC Host Name 1 _capwap-control._udp.example.com
AC Host Name 2
AC Host Name 3
Multicast Address 224.0.1.140

24

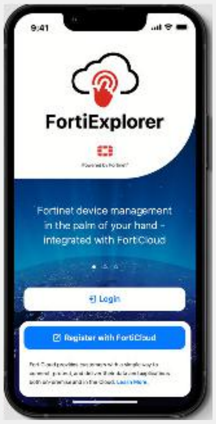
By default, FortiAP is a DHCP client, meaning it receives an IP address from a DHCP server once it is plugged into your network. HTTPS administrative access is enabled to access the FortiAP GUI for an unmanaged FortiAP device. You may be required to configure a static IP address for FortiOS wireless controller discovery before sending it out to small branch offices where there is no IT staff. After the FortiAP is managed by a FortiOS wireless controller, the administrative access is controlled by the FortiAP profile.

To access the GUI on FortiAP, open a web browser and visit `https://<IP address assigned by DHCP server>`. Note that you need a firewall policy to allow traffic to access the FortiAP management GUI.

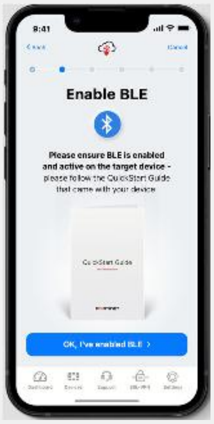
The default login information is public knowledge. Never leave the default password blank. After you log in with default login details, you'll see a message to change the default blank password for the admin user.

FortiAP BLE

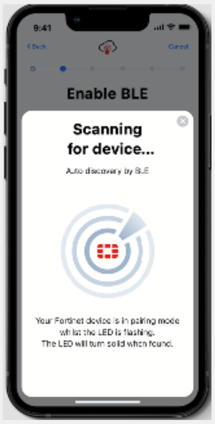
- User FortiExplorer to configure initial settings on BLE-compatible FortiAP devices
  - FortiAP G and later models
- FortiExplorer eliminates the need for a serial console and SSH
- You can use FortiExplorer to troubleshoot FortiAP



Fortinet device management in the palm of your hand - integrated with FortiCloud



Please ensure BLE is enabled and active on the target device - please follow the QuickStart Guide that came with your device



Your Fortinet device is in pairing mode whilst the LED is flashing.
The LED will turn solid when found.

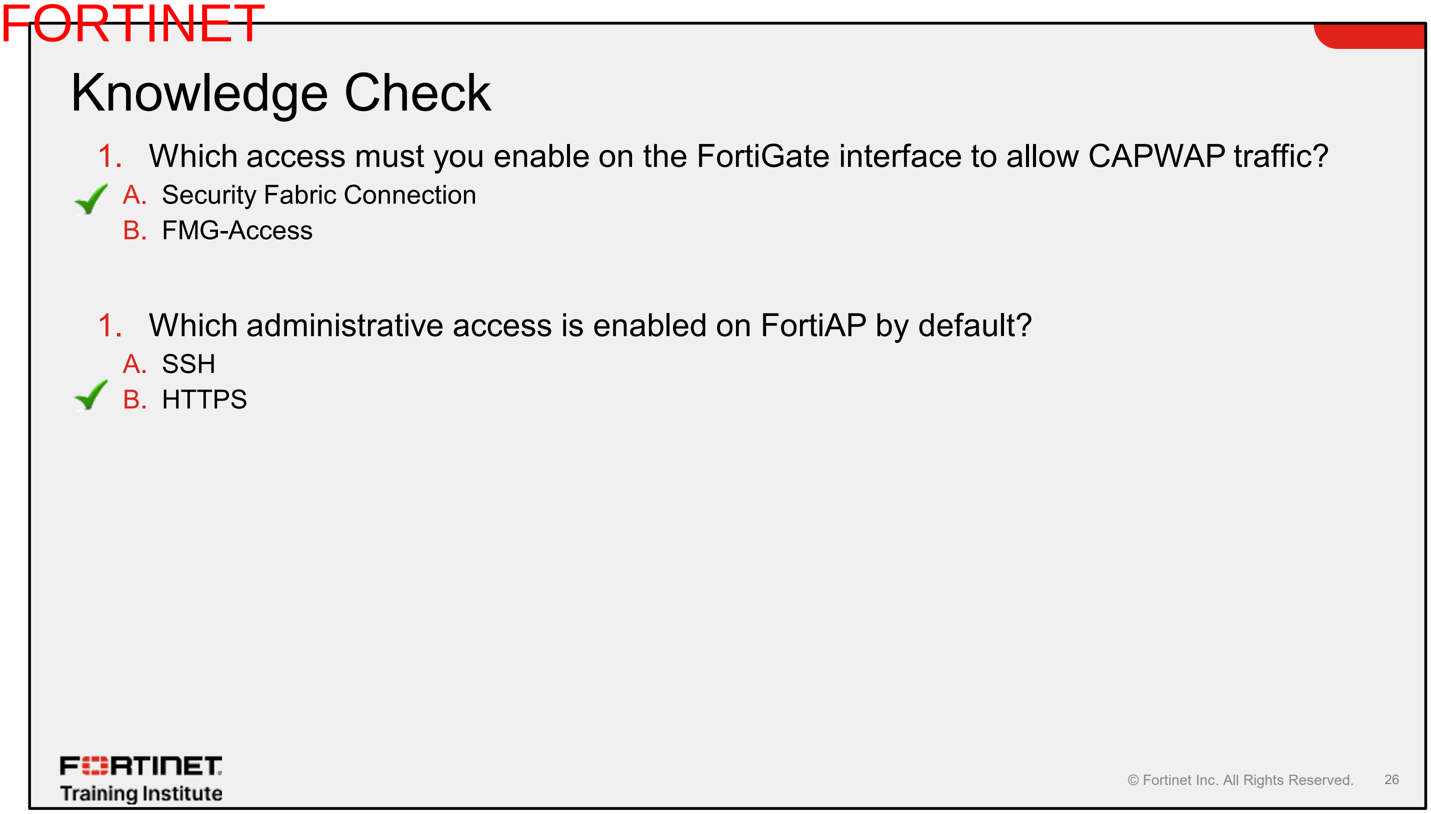
FURTINET Training Institute

25

FortiAP G and later models are compatible with FortiExplorer using Bluetooth low energy (BLE). This eliminates the need to connect a serial console or establish an SSH connection to FortiAP.

On FortiAP G and later FortiAP models, you can use FortiExplorer to:

1. Perform initial configurations on FortiAP
2. Debug and monitor FortiAP behavior when it is managed by the wireless controller



Knowledge Check

1. Which access must you enable on the FortiGate interface to allow CAPWAP traffic?

✓ A. Security Fabric Connection

B. FMG-Access

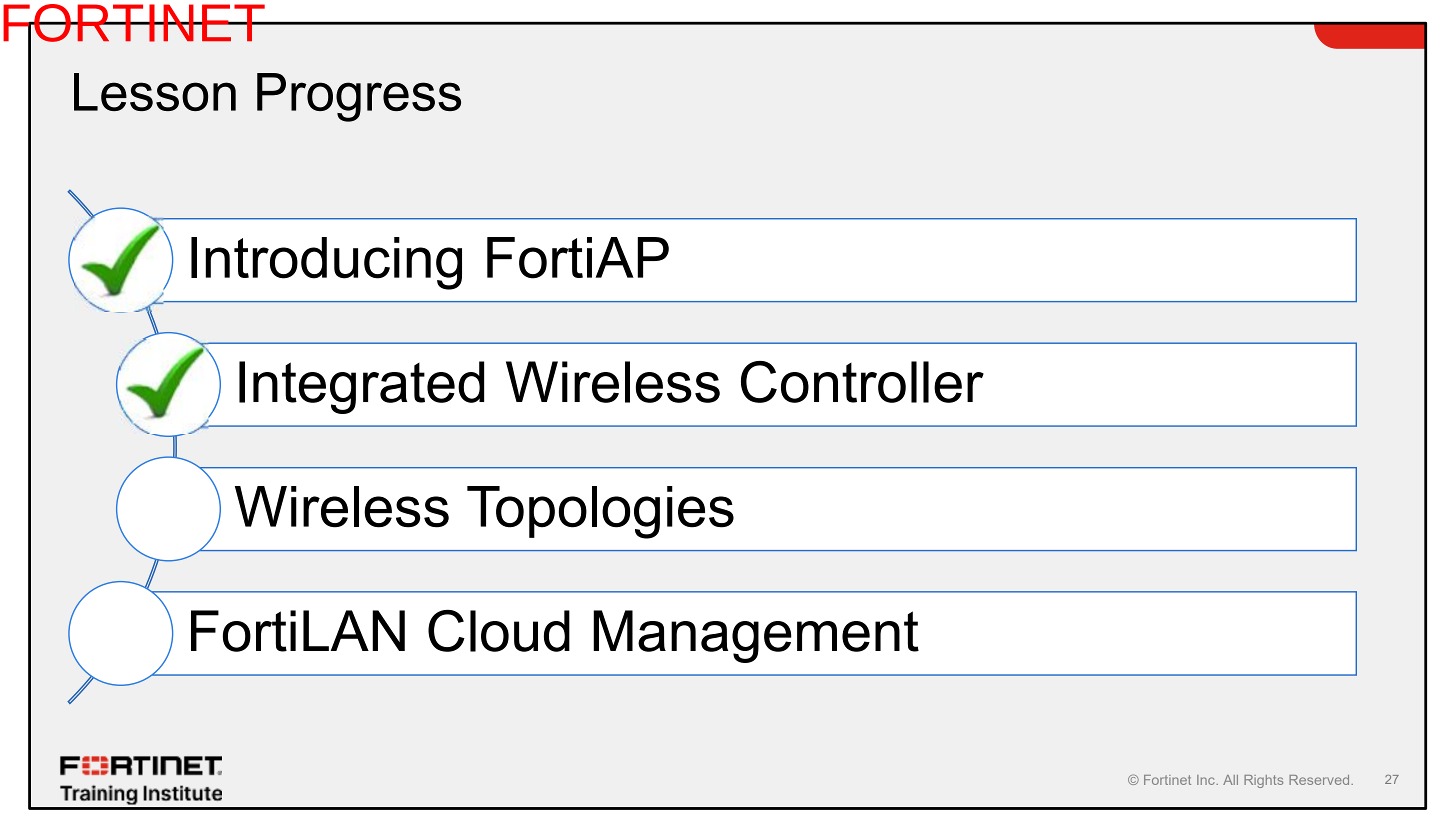
1. Which administrative access is enabled on FortiAP by default?

A. SSH

✓ B. HTTPS

Training Institute

26



Lesson Progress

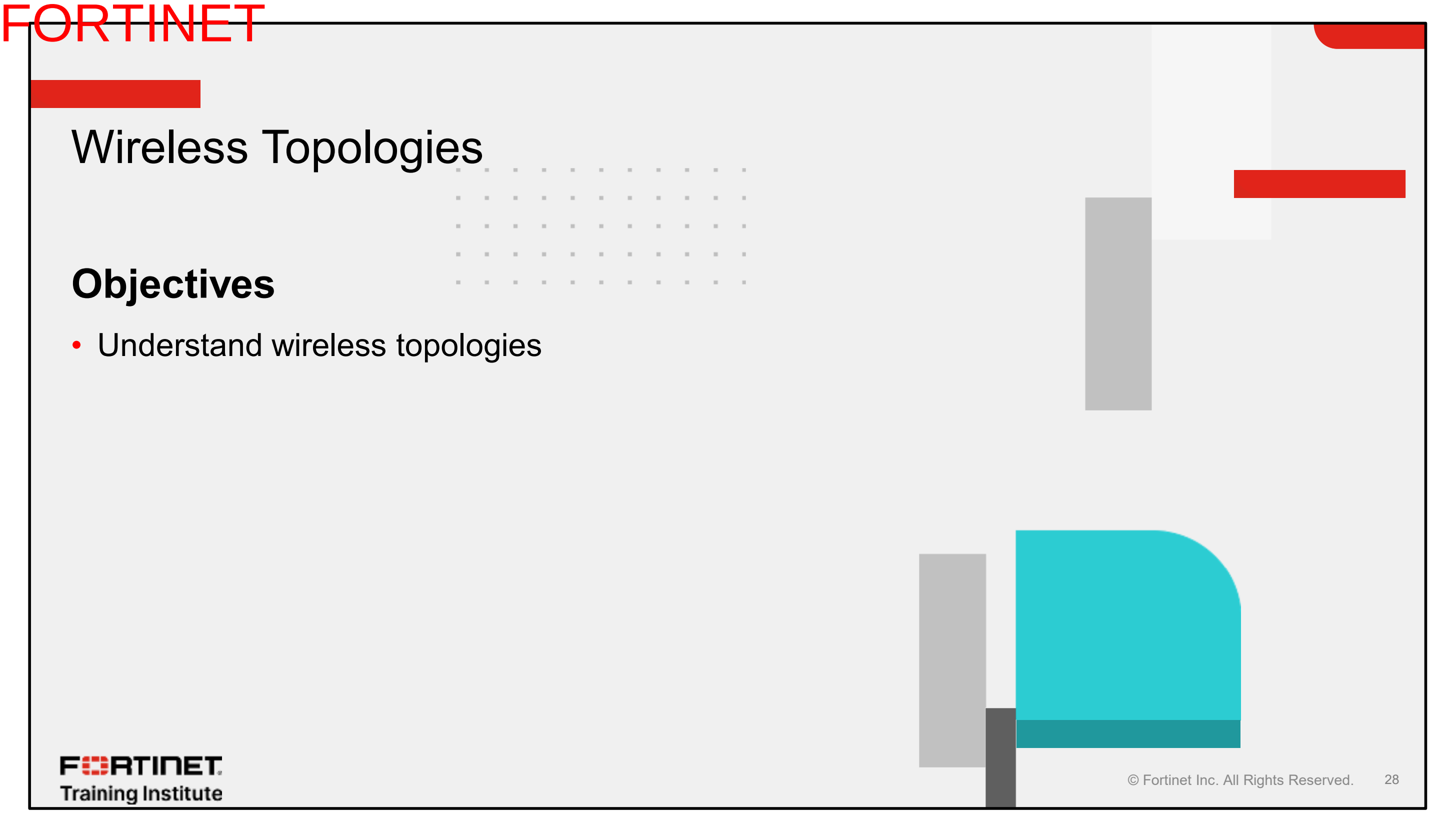
- ✓ Introducing FortiAP
- ✓ Integrated Wireless Controller
- ○ Wireless Topologies
- ○ FortiLAN Cloud Management

FORTINET Training Institute

27

Good job! You now understand the FortiGate wireless controller.

Now, you will learn about the wireless topologies.



Wireless Topologies

Objectives

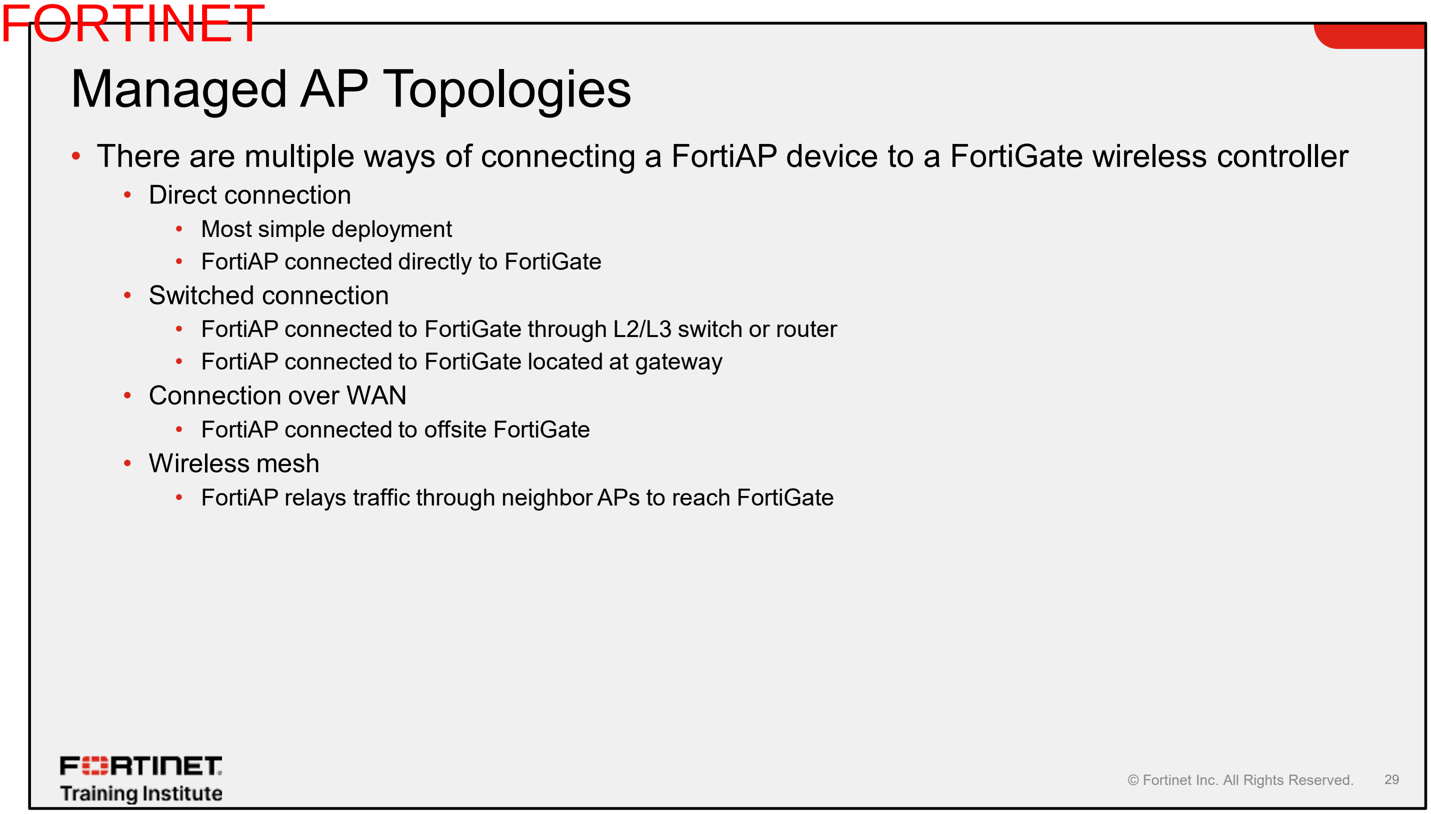
- Understand wireless topologies

FORTINET
Training Institute

28

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding wireless topologies, you will be familiar with the different ways that components connect to a wireless controller.



Managed AP Topologies

- There are multiple ways of connecting a FortiAP device to a FortiGate wireless controller
  - Direct connection
    - Most simple deployment
    - FortiAP connected directly to FortiGate
  - Switched connection
    - FortiAP connected to FortiGate through L2/L3 switch or router
    - FortiAP connected to FortiGate located at gateway
  - Connection over WAN
    - FortiAP connected to offsite FortiGate
  - Wireless mesh
    - FortiAP relays traffic through neighbor APs to reach FortiGate

29

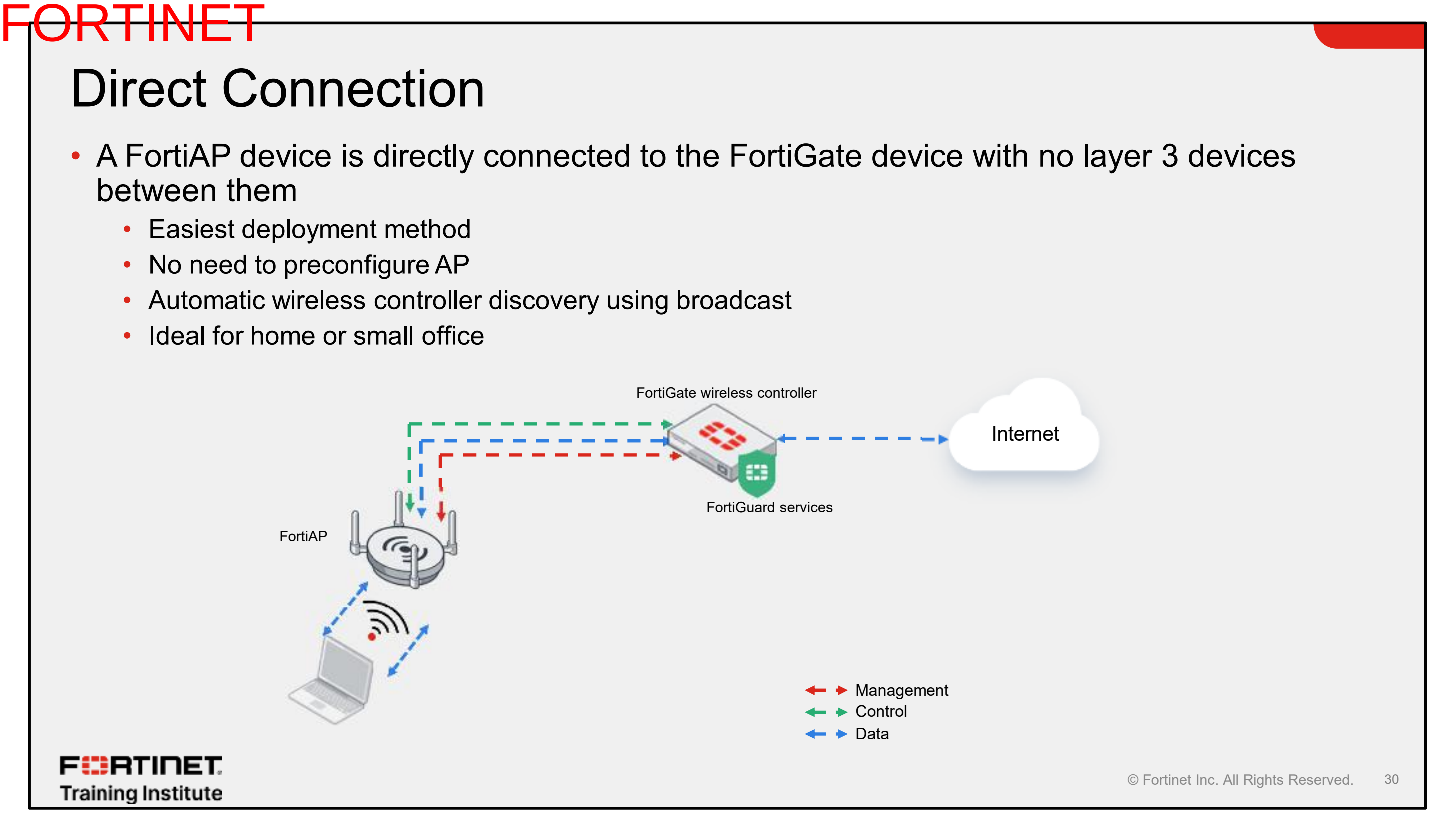
To interconnect the wireless controller and the APs, you will usually use a wired connection. The exception is when remote APs connect indirectly, through a mesh SSID running on another AP to reach the wireless controller.

FortiOS supports the following AP topologies:

- **Direct connection**: Also known as a wire closet deployment. There are no switches between FortiAP and FortiOS. Usually, this deployment type is used where the number of FortiAPs equals the number of internal ports available on FortiGate. FortiAP requests an IP address from FortiOS, enters discovery mode, and quickly finds the FortiGate wireless controller.
- **Switched connection**: Also known as gateway deployment. FortiAP is connected to FortiOS through a Layer 2 Ethernet switch/Layer 3 router/FortiGate, ports 5246 and 5247 must be open, and there must be a routable path between FortiAP and FortiOS.
- **Connection over WAN**: Also known as a datacenter remote management deployment. The FortiOS wireless controller is remote. When using this method of connectivity, it's best to configure each FortiAP device with the static IP address of the Wi-Fi controller. You can configure each FortiAP with three Wi-Fi controller IP addresses for redundant failover.
- **Distributed connection**: Also known as a wireless mesh deployment. It can provide access to widely distributed clients. The AP that is the root of the mesh is directly connected to the Wi-Fi controller. The root can be either a FortiAP device or a FortiWiFi device.

These physical topologies use two traffic modes:

- Tunnel mode
- Bridge mode

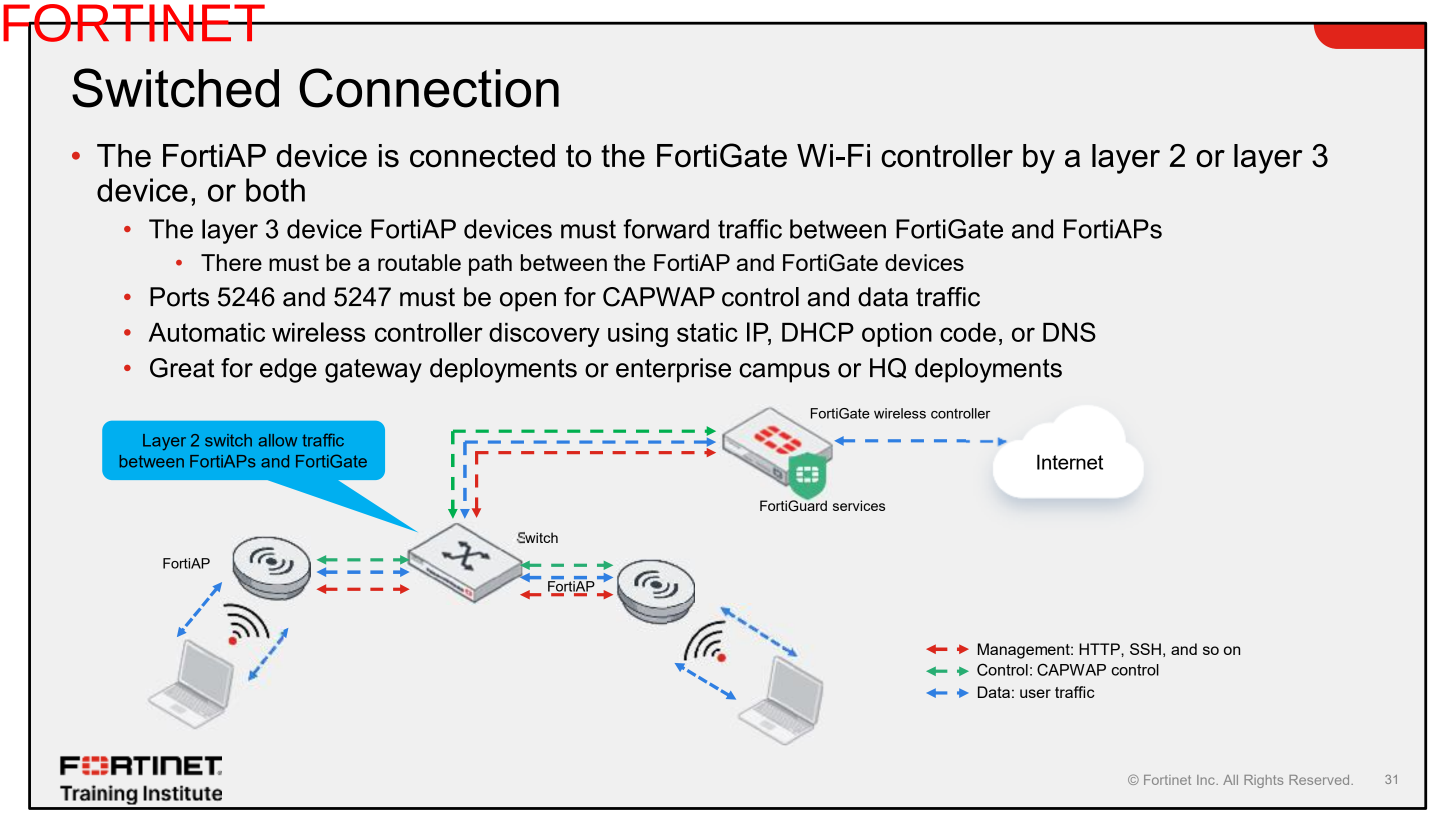


Direct Connection

- A FortiAP device is directly connected to the FortiGate device with no layer 3 devices between them
  - Easiest deployment method
  - No need to preconfigure AP
  - Automatic wireless controller discovery using broadcast
  - Ideal for home or small office

© Fortinet Inc. All Rights Reserved. 30

This configuration is commonly used in locations where the number of FortiAPs matches the number of internal ports available on FortiGate. In this configuration, the FortiAP device requests an IP address from the FortiGate device, enters discovery mode, and quickly finds the FortiGate Wi-Fi controller. This is also known as a wire closet deployment.



Switched Connection

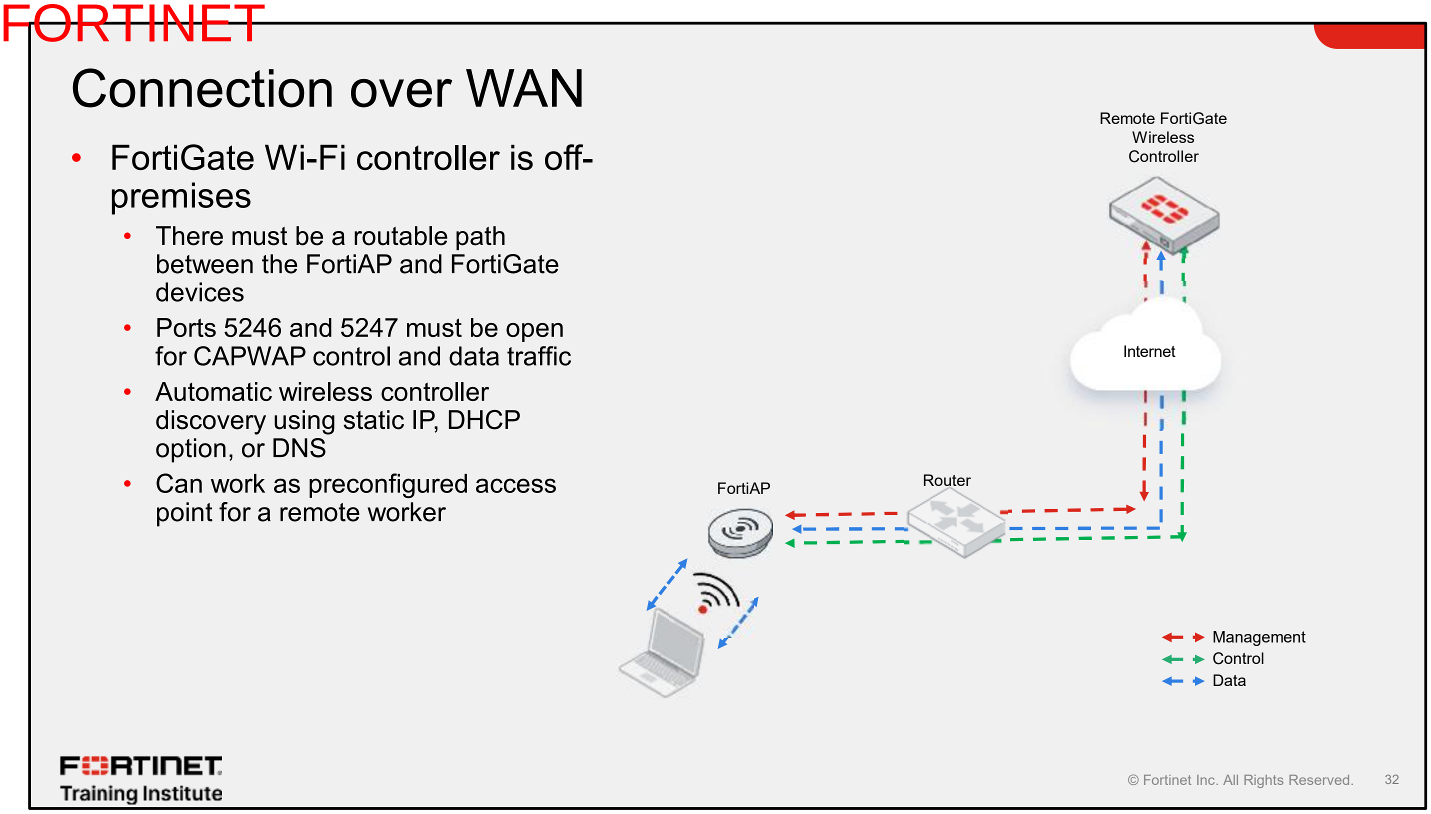
- The FortiAP device is connected to the FortiGate Wi-Fi controller by a layer 2 or layer 3 device, or both
  - The layer 3 device FortiAP devices must forward traffic between FortiGate and FortiAPs
    - There must be a routable path between the FortiAP and FortiGate devices
  - Ports 5246 and 5247 must be open for CAPWAP control and data traffic
  - Automatic wireless controller discovery using static IP, DHCP option code, or DNS
  - Great for edge gateway deployments or enterprise campus or HQ deployments

Layer 2 switch allow traffic between FortiAPs and FortiGate
FortiGate wireless controller
Internet
FortiGuard services
Switch
FortiAP
FortiAP
Management: HTTP, SSH, and so on
Control: CAPWAP control
Data: user traffic
FORTINET
Training Institute
© Fortinet Inc. All Rights Reserved.
31

This configuration is commonly used in campus environments and large offices where layer 2 and layer 3 switches are in place for core and distribution-layer connectivity. FortiAP devices could be connected to distribution-layer switches to have wireless access for users. Connecting a FortiAP device to a layer 2 switch is like a direct connection. The wireless controller is discovered either through broadcast or multicast traffic. In a deployment where FortiAP is connected to a layer 3 switch, the wireless controller discovery is performed using static, DNS, or DHCP discovery methods and there must be a routable path between the FortiAP device and the FortiOS wireless controller.

In the example shown on this slide, the FortiAP devices are connected to a power over Ethernet (PoE) FortiSwitch. That switch connects to a FortiGate firewall, using a FortiLink connection, which effectively integrates all switch management and configuration functions into the FortiGate management interface.

The traffic flow path is straightforward. The AP management traffic goes directly to FortiGate. The user or device access path goes to the switch and then to FortiGate. The AP monitors and secures user traffic through the switch, through the firewall, and out to the internet or other destination.



Connection over WAN

- FortiGate Wi-Fi controller is off-premises
  - There must be a routable path between the FortiAP and FortiGate devices
  - Ports 5246 and 5247 must be open for CAPWAP control and data traffic
  - Automatic wireless controller discovery using static IP, DHCP option, or DNS
  - Can work as preconfigured access point for a remote worker

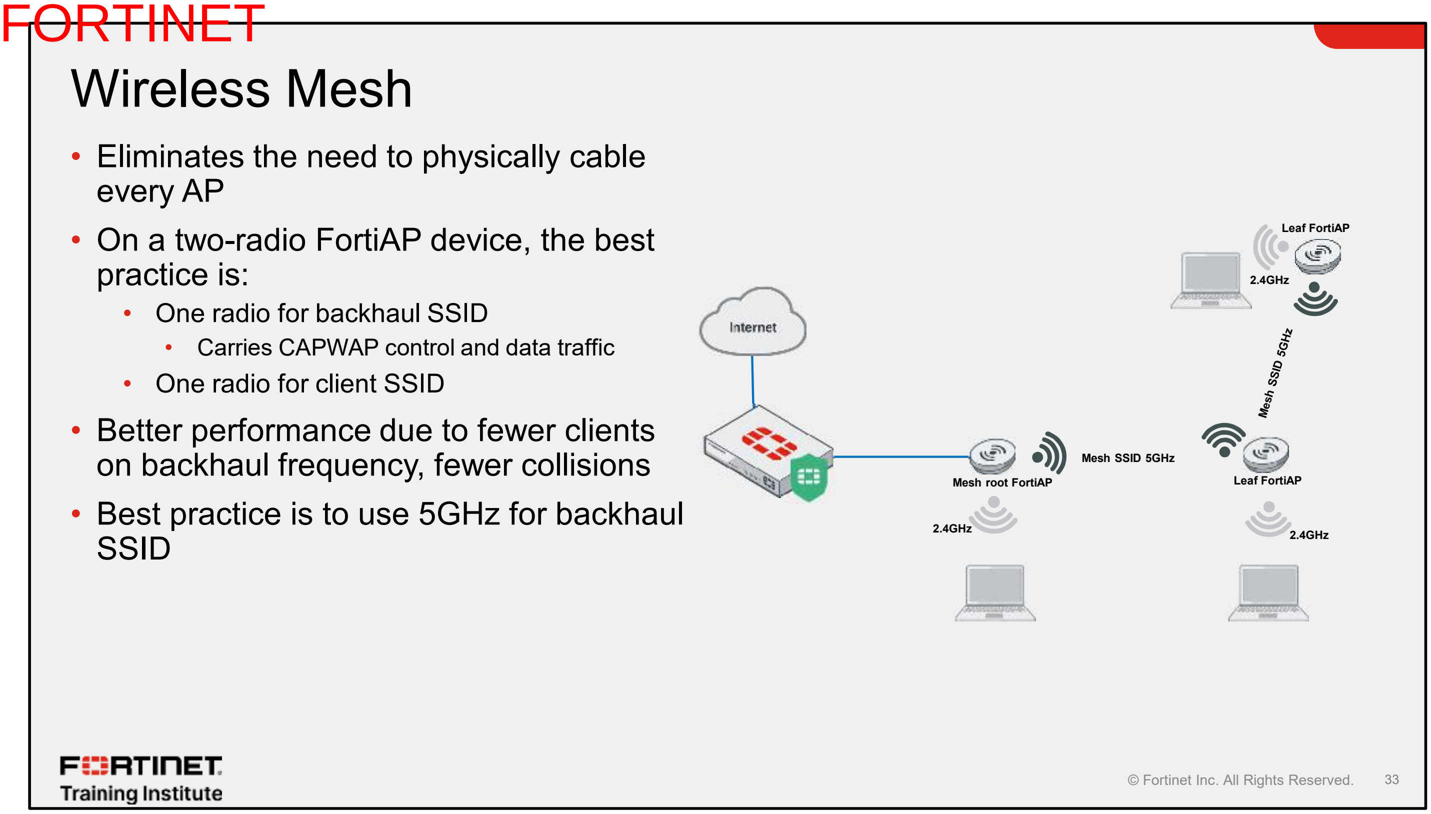
Remote FortiGate Wireless Controller
Internet
FortiAP
Router
Management
Control
Data

FORTINET Training Institute

32

The FortiGate Wi-Fi controller is off-premises. When you use this method of connectivity, it is best to configure each FortiAP device with the static IP address of the Wi-Fi controller. You can configure each FortiAP device with three Wi-Fi controller IP addresses for redundant failover.

Remote WLAN FortiAP models enable you to provide a preconfigured Wi-Fi AP to a remote or traveling employee. After it is plugged in at home or in a hotel room, FortiAP automatically discovers the enterprise FortiGate Wi-Fi controller over the internet, broadcasts the same wireless SSID used in the corporate office and provides access to corporate resources if configured. By default, the remote FortiAP device sends all traffic to the FortiGate wireless controller. FortiGate can inspect all the network traffic from the wireless clients connected to the remote FortiAP device.



Wireless Mesh

- Eliminates the need to physically cable every AP
- On a two-radio FortiAP device, the best practice is:
  - One radio for backhaul SSID
    - Carries CAPWAP control and data traffic
  - One radio for client SSID
- Better performance due to fewer clients on backhaul frequency, fewer collisions
- Best practice is to use 5GHz for backhaul SSID

FURTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

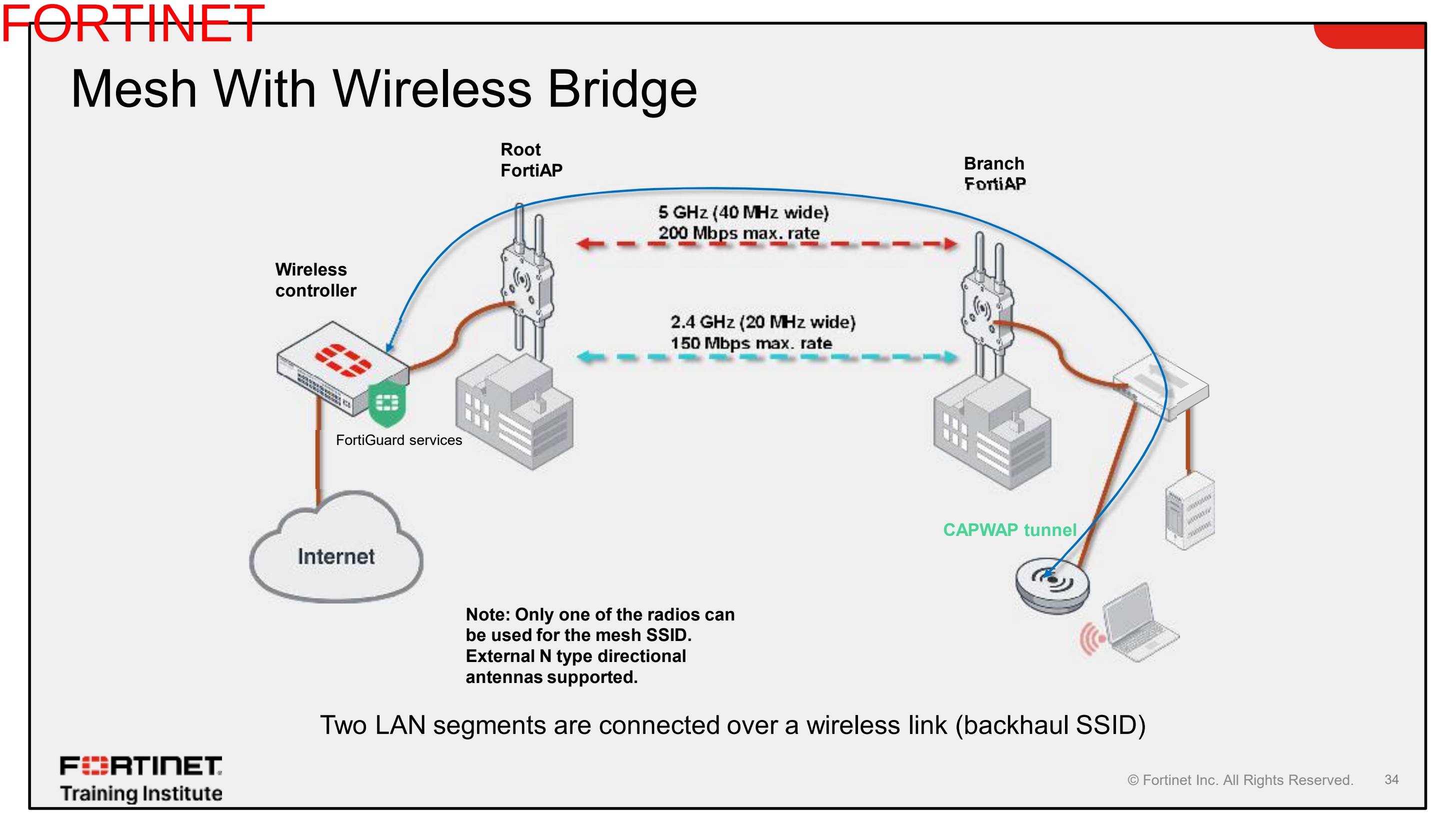
Mesh (IEEE 802.11s) topologies are useful where physical wiring is impractical. Mesh eliminates the need to *physically* cable every AP to the wireless controller. Instead, APs relay their traffic through a *wireless* connection with their neighbor APs, back to the root, which *is* physically connected to the wireless controller.

Mesh includes the devices and SSIDs shown in the diagram on this slide:

- Mesh root node APs are the only ones connected to the network by a physical cable.
- Backhaul SSIDs between APs are only for relayed connections to the wired network through the root FortiAP device. These SSIDs carry CAPWAP discovery, configuration, and other communications that are usually carried on an Ethernet connection. *Regular Wi-Fi clients such as laptops and tablets shouldn't connect to the backhaul SSID. Make sure that your backhaul SSID and user SSID on different frequencies.* This maximizes performance—the APs don't need to compete with clients for airtime.
- Branch APs are between the root and leaf APs. (Smaller meshes may not have any.) They relay packets if the leaf AP is not in range of the root.
- Leaf APs connect normal clients such as laptops, tablets, and mobile phones.

If your AP has only two radios, then you can't dedicate one of the radios to scanning for rogue APs—unless the backhaul SSID and client SSID share a radio, which decreases performance. For example, the 5GHz radio could have only the backhaul SSID; the 2.4GHz radio could have one or more SSIDs for user connections. Background Wi-Fi scanning is not available in this mode. Alternatively, the backhaul SSID could share the same radio with SSIDs for users, but performance would be reduced because backhaul and user traffic would compete for available bandwidth. Background Wi-Fi scanning is possible in this mode.

A wireless mesh topology is a good way to limit physical cabling, but a wireless medium is not considered reliable for backhaul connectivity due to interference and quality of signal issues. Site surveys are highly recommended before implementing a wireless mesh topology.



Mesh With Wireless Bridge

Note: Only one of the radios can be used for the mesh SSID. External N type directional antennas supported.

Two LAN segments are connected over a wireless link (backhaul SSID)

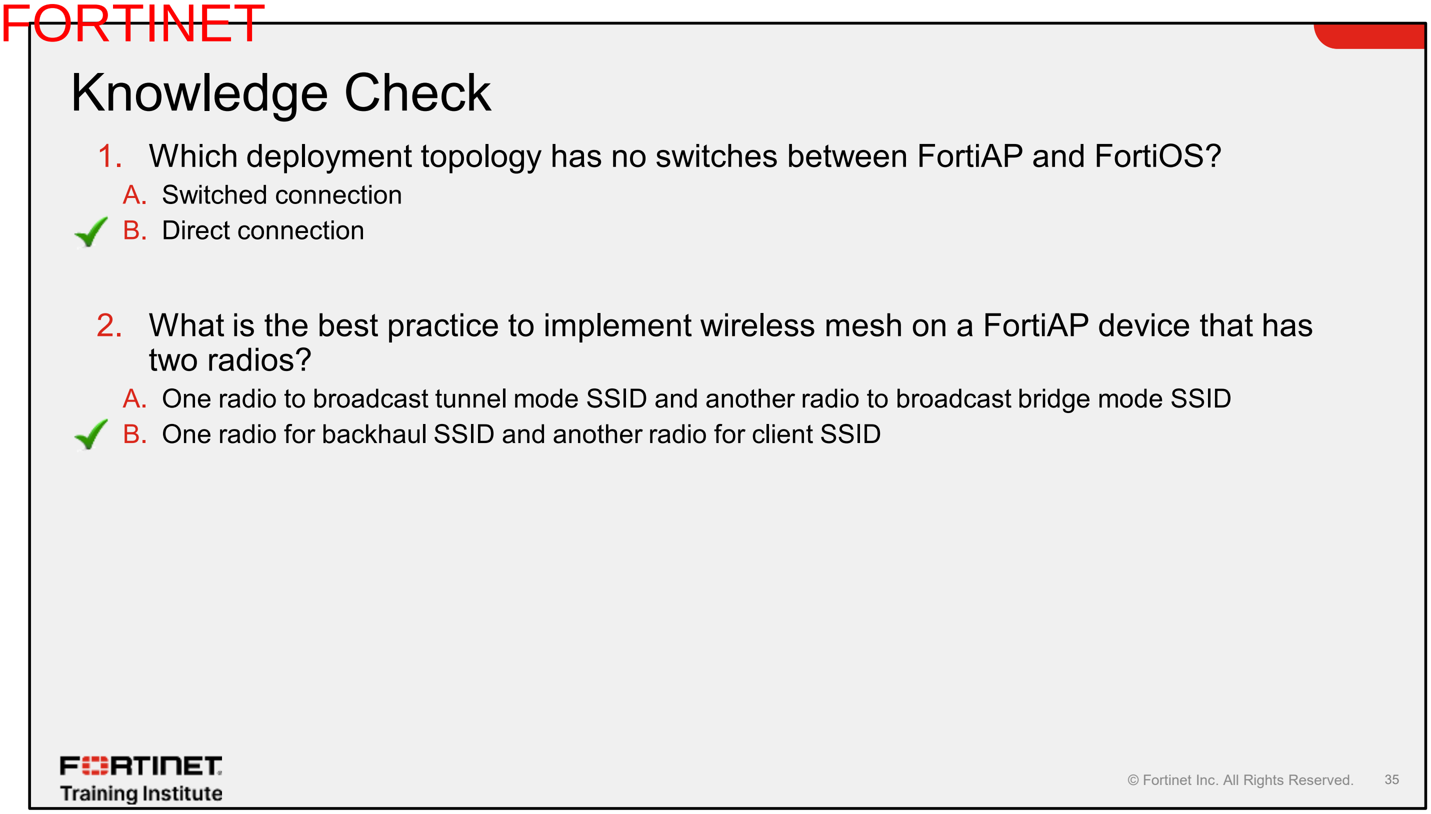
F⬚RTINET Training Institute

34

To connect two wired network segments, you can also create a wireless mesh.

To set up a full mesh:

1. Similar to the previously shown wireless mesh, configure a backhaul SSID and mesh root AP. (Note that unlike a normal mesh, the mesh root AP for a point-to-point bridge *must* be a FortiAP device, not a FortiWiFi device.)
2. Configure bridging on the branch FortiAP device.

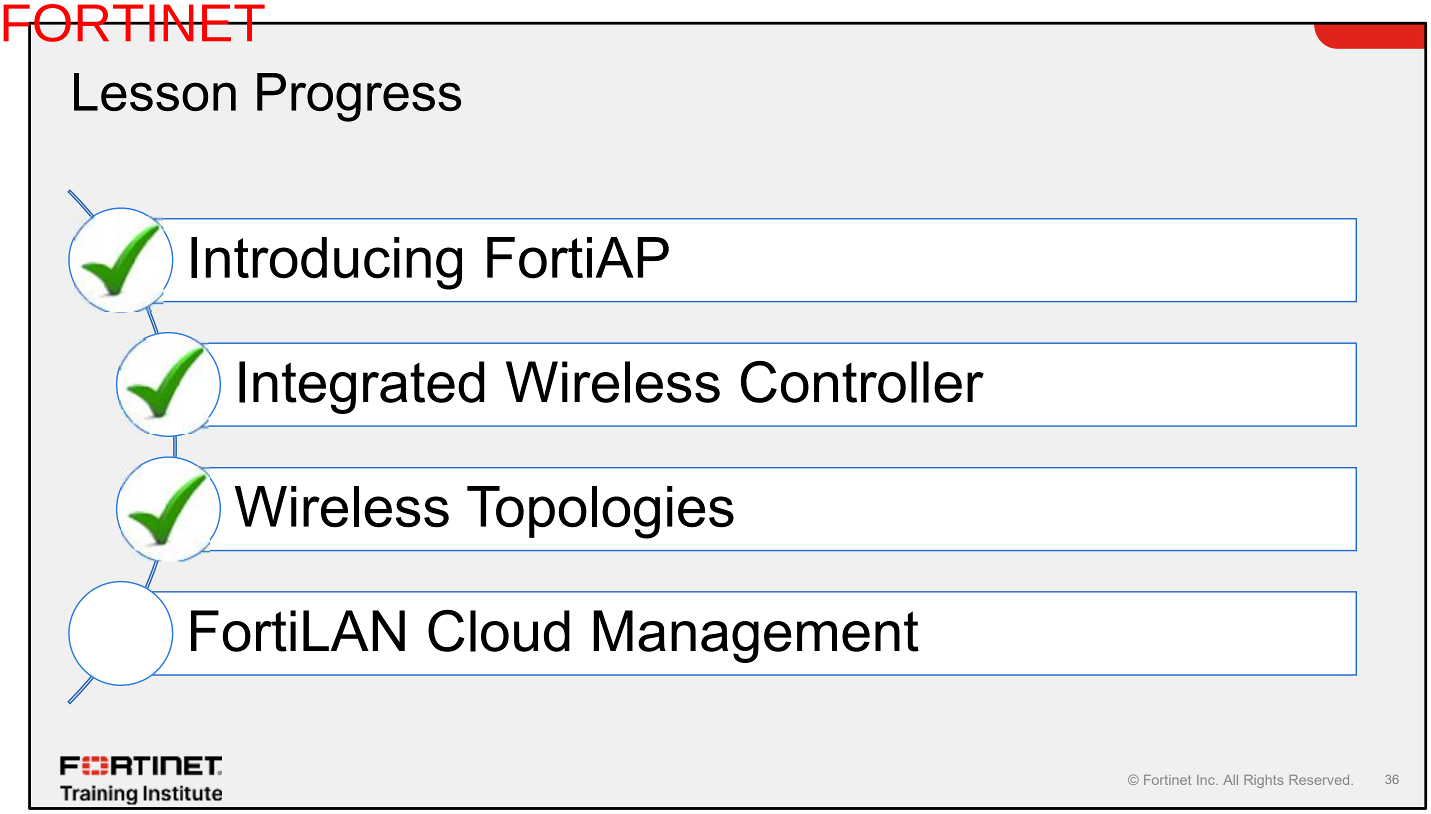


Knowledge Check

1. Which deployment topology has no switches between FortiAP and FortiOS?
   - A. Switched connection
   - ✓ B. Direct connection

2. What is the best practice to implement wireless mesh on a FortiAP device that has two radios?
   - A. One radio to broadcast tunnel mode SSID and another radio to broadcast bridge mode SSID
   - ✓ B. One radio for backhaul SSID and another radio for client SSID

35



Lesson Progress

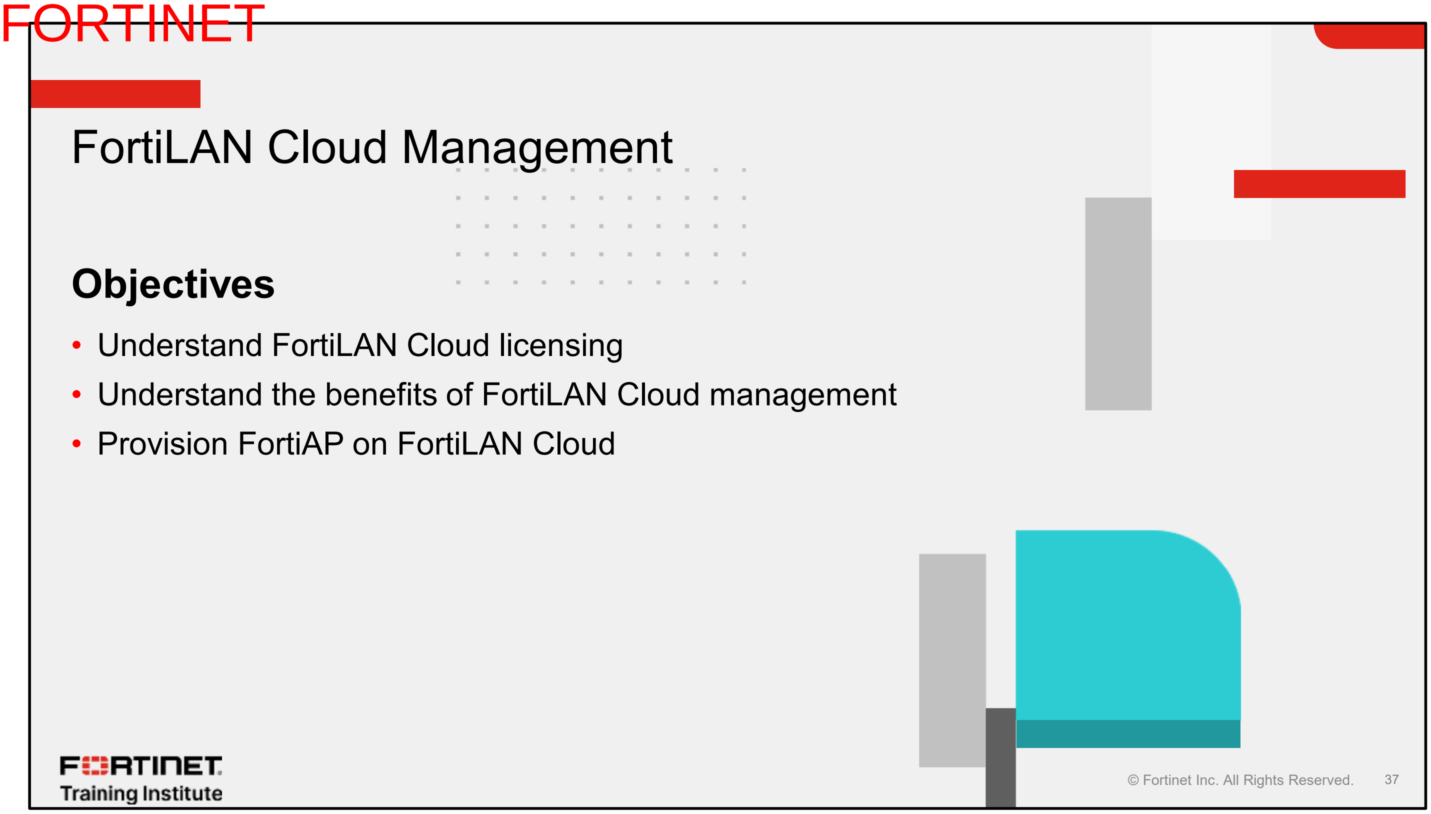
- ✓ Introducing FortiAP
- ✓ Integrated Wireless Controller
- ✓ Wireless Topologies
- ○ FortiLAN Cloud Management

FORTINET Training Institute

36

Good job! You now understand the wireless topologies.

Now, you will learn about the management of FortiLAN Cloud.



FortiLAN Cloud Management

Objectives

- Understand FortiLAN Cloud licensing
- Understand the benefits of FortiLAN Cloud management
- Provision FortiAP on FortiLAN Cloud

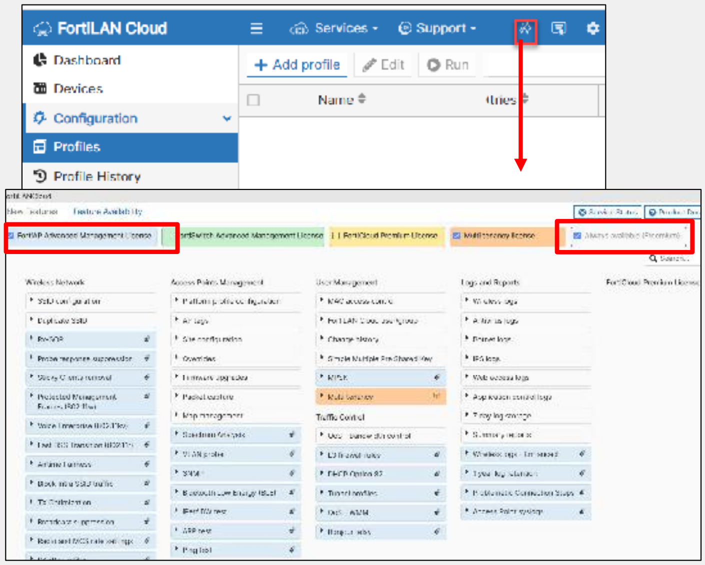
37

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding FortiLAN Cloud, you will be able to manage FortiAP devices using FortiLAN Cloud.

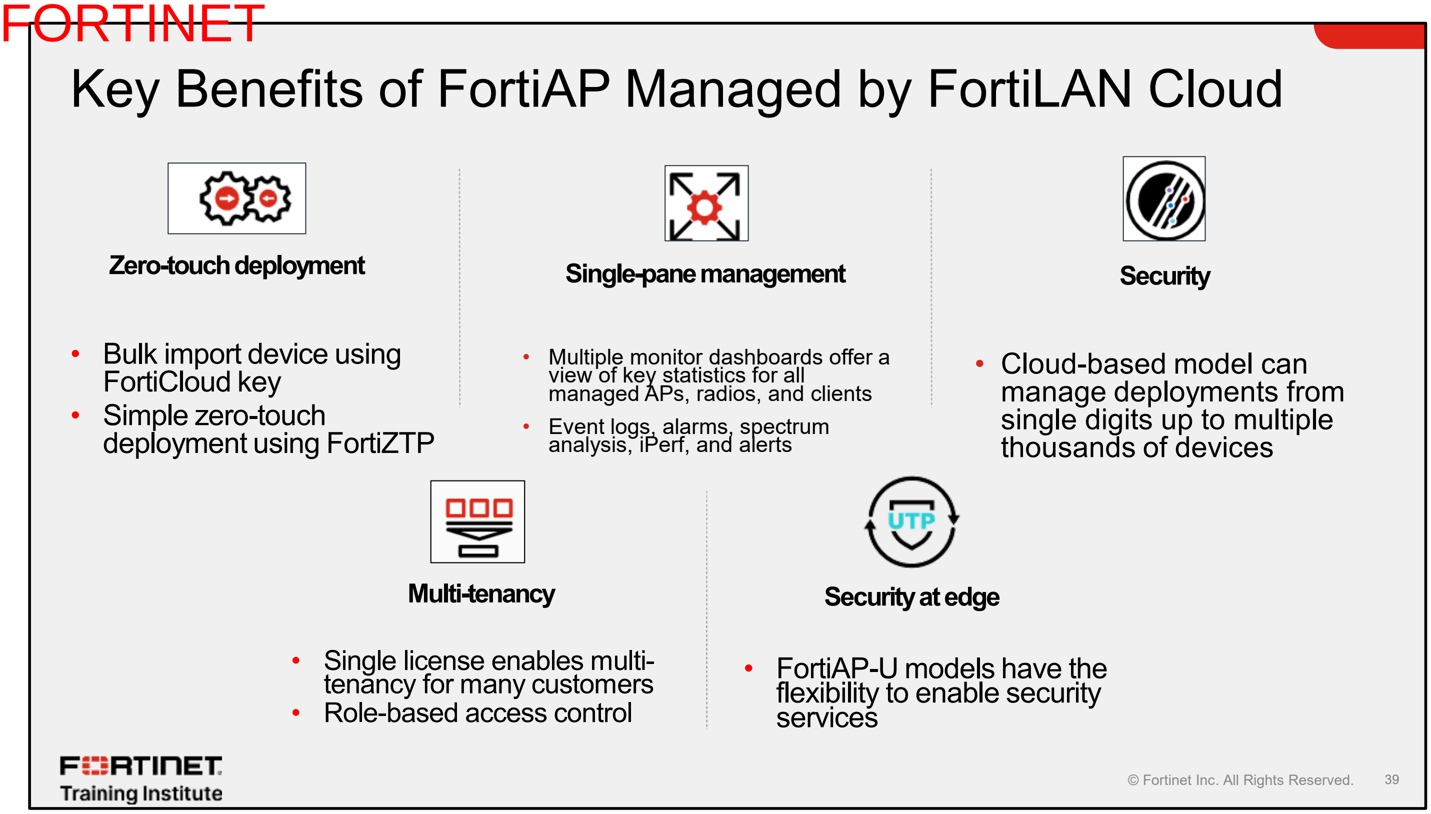
FortiLAN Cloud Licensing

- FortiLAN Cloud offers a free basic license:
  - Up to 30 FortiAP devices per account
  - Up to three FortiSwitch devices per account
  - Up to three sites
  - Log retention of 7 days
- Additional licenses are available for FortiAP advanced management, FortiSwitch advanced management, FortiCloud premium, and multi-tenancy



FortiLAN Cloud offers a free basic license that allows deployment and visibility of FortiAP and FortiSwitch devices. You can deploy up to 30 FortiAP devices and three FortiSwitch devices using the free basic license. FortiLAN Cloud retains logs for 7 days, and you can configure up to three sites.

You can access the FortiLAN Cloud portal through by going to `https://support.fortinet.com` and then clicking on **Services** > **FortiLAN Cloud** or by going to `https://fortilan.forticloud.com`. To review the different license, click on the FortiLAN Cloud feature reference icon, and then click **Feature Availability**.



Key Benefits of FortiAP Managed by FortiLAN Cloud

Zero-touch deployment

- Bulk import device using FortiCloud key
- Simple zero-touch deployment using FortiZTP

Single-pane management

- Multiple monitor dashboards offer a view of key statistics for all managed APs, radios, and clients
- Event logs, alarms, spectrum analysis, iPerf, and alerts

Security

- Cloud-based model can manage deployments from single digits up to multiple thousands of devices

Multi-tenancy

- Single license enables multi-tenancy for many customers
- Role-based access control

Security at edge

- FortiAP-U models have the flexibility to enable security services

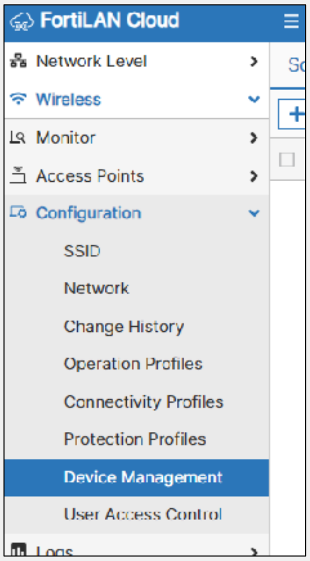
39

Managing FortiAP devices using FortiLAN Cloud offers the following important key benefits:

- Zero-touch deployment: Initial configuration of network equipment can be a difficult proposition, often requiring expert staff on site to configure each device individually. FortiLAN Cloud with FortiZTP greatly simplifies initial configuration and onboarding by providing one-touch provisioning when devices are deployed.
- Ease of management and troubleshooting: Multiple monitor dashboards offer a view of key statistics for all managed switches, ports, APs, radios, clients, and neighboring networks in your environment. Click to drill down on a particular item to see details on specific devices in a category. There is no need to change screens or hunt through the GUI to find information. You can schedule firmware updates for equipment and created update profiles for targeted devices.
- Scalability: Manage deployments from single digits up to multiple thousands of devices and easily grow with your deployment along the way.
- Multi-tenancy: Maintain multi-tenancy for many customers within a single license. Simple central visibility and access across all tenants. Enable read-only customer accounts with unique customer logos on reports.
- Security at the edge: When used with the Fortinet UTP access points (FortiAP-U models) FortiLAN Cloud has the flexibility to enable security services wherever needed in the network.

FortiLAN Cloud Features

- FortiLAN Cloud features include:
  - Ability to manage and deploy wireless networks
  - Use built-in guest management
    - Self-registration
  - Deploy protection profiles
  - Scheduled upgrades
  - Use local or remote RADIUS server
  - AP location maps
  - Real-time network visibility
- Optional premium account supports:
  - Multi-tenancy
  - Multiple customers handled from single GUI
  - Independent subaccounts
  - Assign AP networks to subaccount

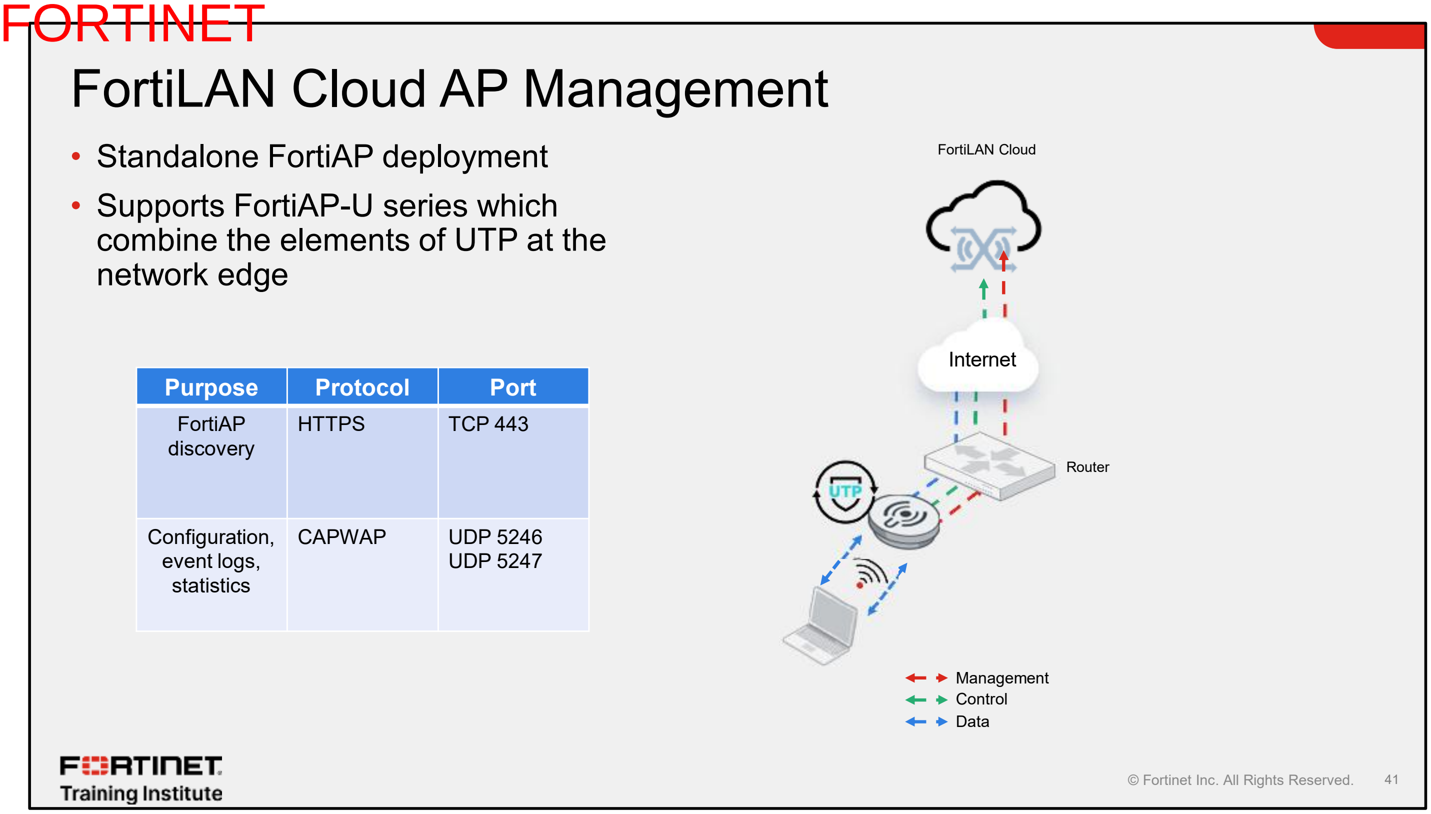


FORTINET Training Institute

40

After purchasing an AP, you can start managing it by connecting it to your FortiCloud account. The free basic version of FortiLAN Cloud provides you with the ability to manage and deploy wireless networks without the need of a premium account. It includes features such as guest management, protection profiles, local user management, RADIUS authentication, and so on.

Premium accounts are also available for enterprise customers that require multi-tenancy and more administrator access control of FortiLAN Cloud.



FortiLAN Cloud AP Management

- Standalone FortiAP deployment
- Supports FortiAP-U series which combine the elements of UTP at the network edge

Purpose	Protocol	Port
FortiAP discovery	HTTPS	TCP 443
Configuration, event logs, statistics	CAPWAP	UDP 5246 UDP 5247

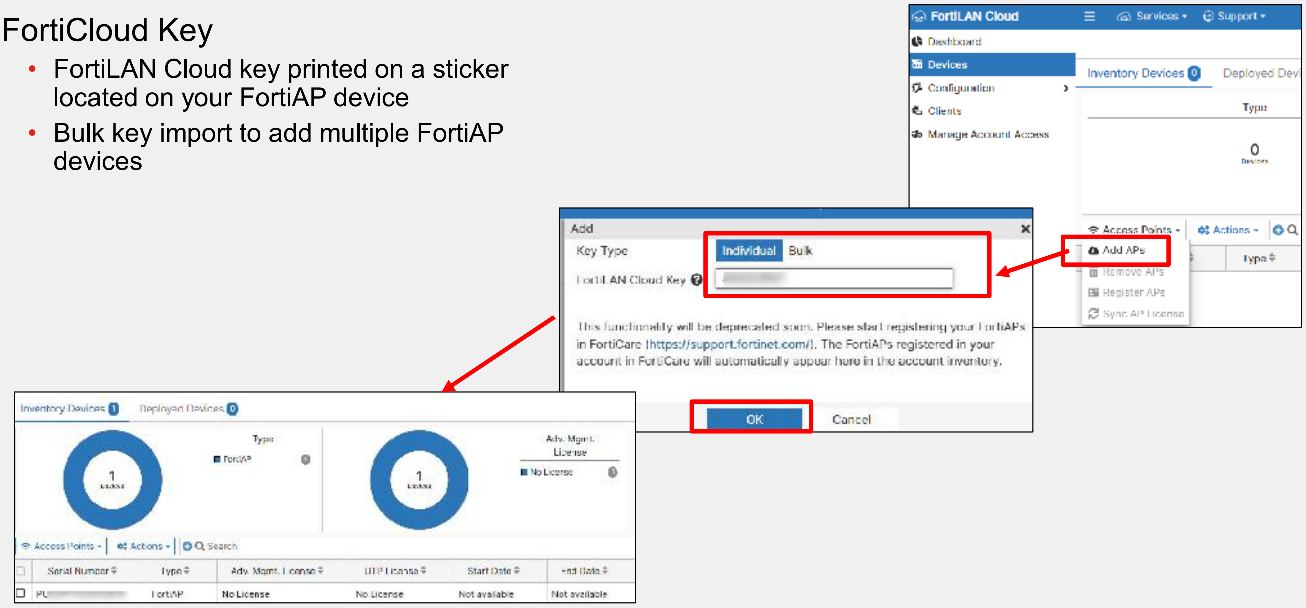
FORTINET Training Institute

41

Deploying a wireless network with FortiLAN Cloud allows management of remote APs without an onsite FortiGate device. FortiAP devices communicate with FortiLAN Cloud for management or control plane traffic. All the wireless client traffic is bridged to the FortiAP and is not tunneled back to FortiLAN Cloud. The FortiAP device initiates the connection to FortiLAN Cloud on HTTPS port 443 and makes the initial discovery. FortiAP sends all configuration, event, logs and statistics are sent on CAPWAP UDP port 5246 and UDP port 5247.

Provisioning FortiAP—FortiCloud Key

- FortiCloud Key
  - FortiLAN Cloud key printed on a sticker located on your FortiAP device
  - Bulk key import to add multiple FortiAP devices



Add

Key Type: Individual | Bulk

FortiLAN Cloud Key: [redacted]

This functionality will be deprecated soon. Please start registering your FortiAPs in FortiCare (https://support.fortinet.com/). The FortiAPs registered in your account in FortiCare will automatically appear here in the account inventory.

OK | Cancel

	Serial Number	Type	Adv. Mgmt. License	UTP License	Start Date	End Date
□	PU[redacted]	FortiAP	No License	No License	Not available	Not available

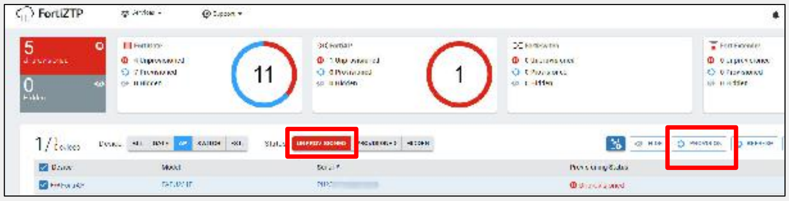
Training Institute

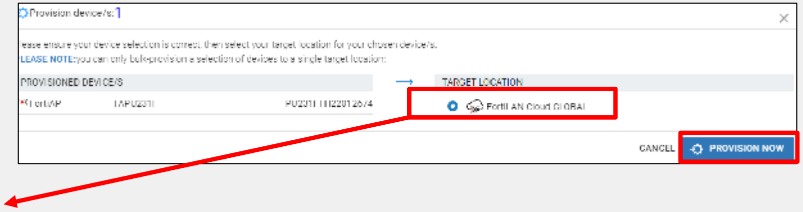
42

To provision FortiAP directly on FortiLAN Cloud click **Devices** > **Inventory Devices,** and then click **Access Points** > **Add APs**. You can add a FortiAP device using the FortiLAN Cloud key printed on a sticker located on the FortiAP device. You can also add multiple FortiAP devices in a single import, using the bulk key on the Fortinet purchase order. After you add the FortiAP devices to the inventory, you can right-click a device, and then click **Actions** > **Deploy**.

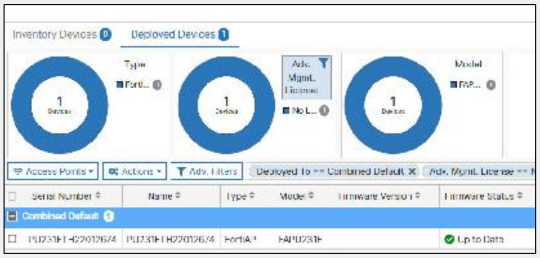
Provisioning FortiAP—FortiZTP

- FortiZTP
  - Provision FortiAP to FortiLAN Cloud using FortiZTP zero-touch provisioning portal





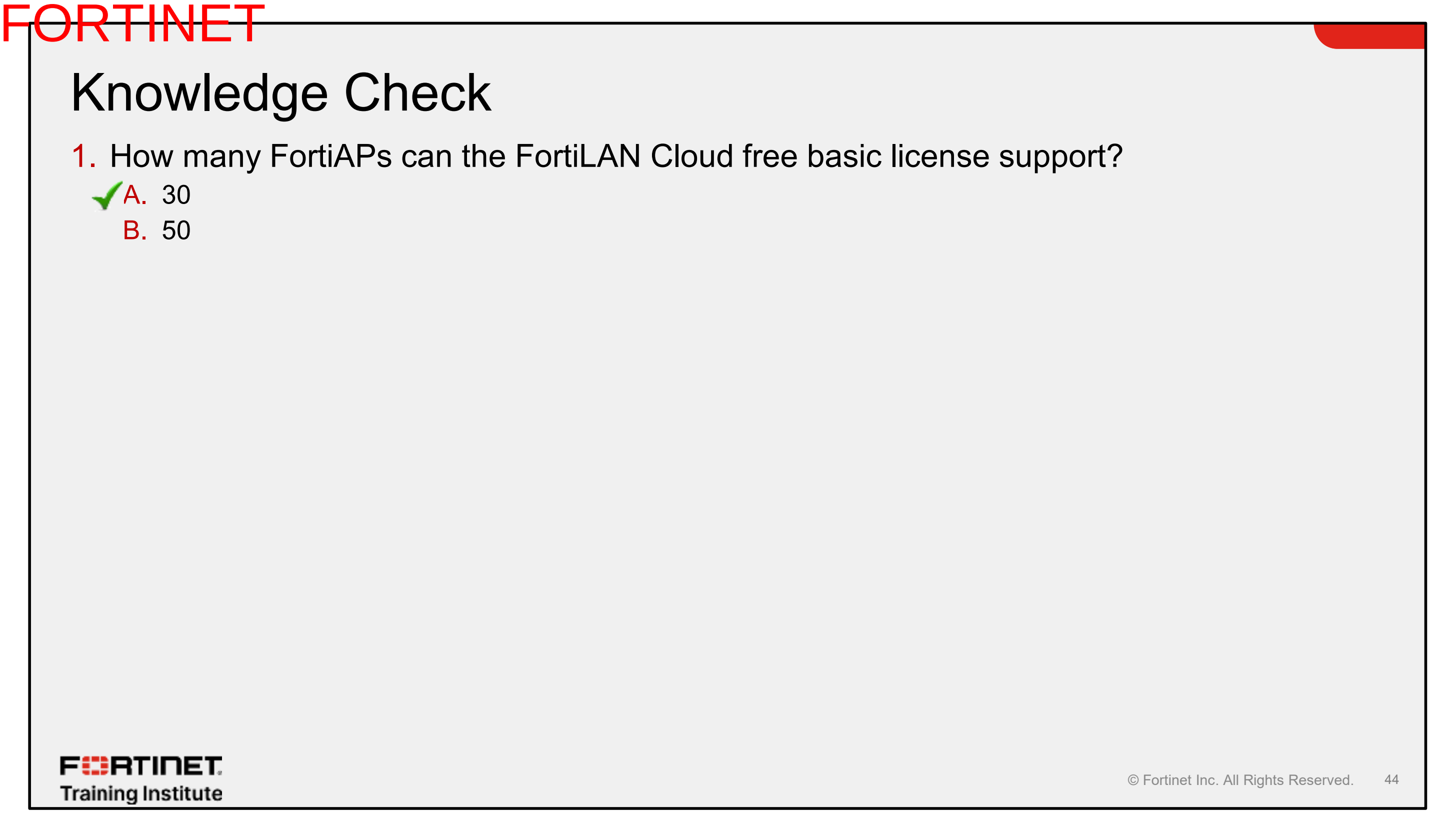
FortiLAN Cloud: Devices > Deployed Devices



Serial Number	Name	Type	Model	Firmware Version	Firmware Status
PU231FTF22012674	PU231FTF22012674	FortiAP	FAPU231F		Up to Date

43

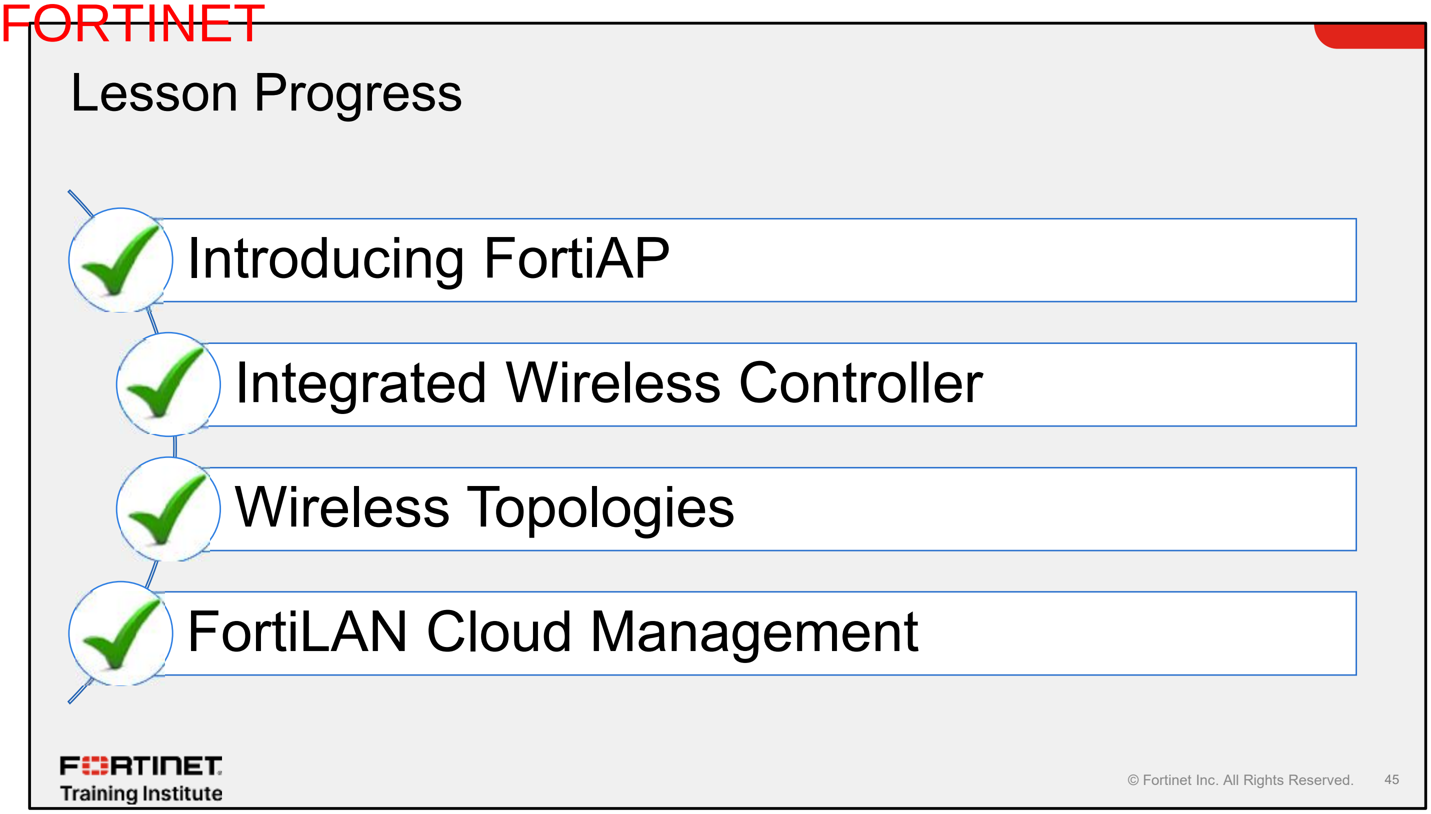
To access the FortiZTP portal, click **Services** > **FortiZTP** on `https://support.fortinet.com`. FortiZTP automatically loads devices that are registered to asset management with the same FortiCloud account on `https://support.fortinet.com`. You can view these devices on the **UNPROVISIONED** tab in FortiZTP and provision them to various Fortinet services as desired. With zero-touch deployment options, FortiLAN Cloud eliminates the need for costly onsite technical expertise. After you provision a FortiAP on FortiZTP portal, it is automatically listed on FortiLAN Cloud as a deployed device.



Knowledge Check

1. How many FortiAPs can the FortiLAN Cloud free basic license support?
   - ✓ A. 30
   - B. 50

44



Lesson Progress

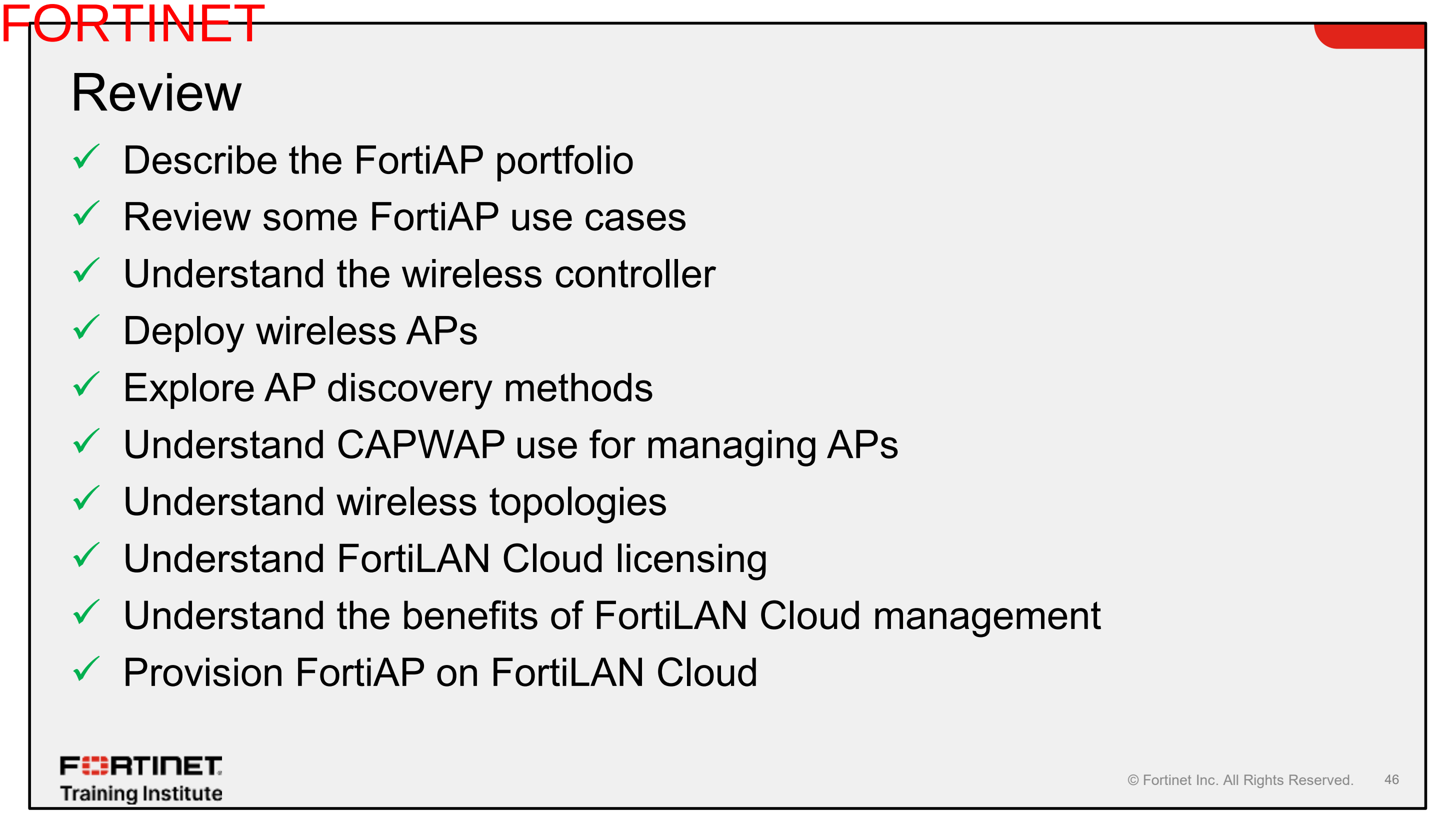
- ✓ Introducing FortiAP
- ✓ Integrated Wireless Controller
- ✓ Wireless Topologies
- ✓ FortiLAN Cloud Management

FORTINET Training Institute

45

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



Review

- ✓ Describe the FortiAP portfolio
- ✓ Review some FortiAP use cases
- ✓ Understand the wireless controller
- ✓ Deploy wireless APs
- ✓ Explore AP discovery methods
- ✓ Understand CAPWAP use for managing APs
- ✓ Understand wireless topologies
- ✓ Understand FortiLAN Cloud licensing
- ✓ Understand the benefits of FortiLAN Cloud management
- ✓ Provision FortiAP on FortiLAN Cloud

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to deploy a FortiAP using Fortinet infrastructure wireless solutions.

FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL Network Security

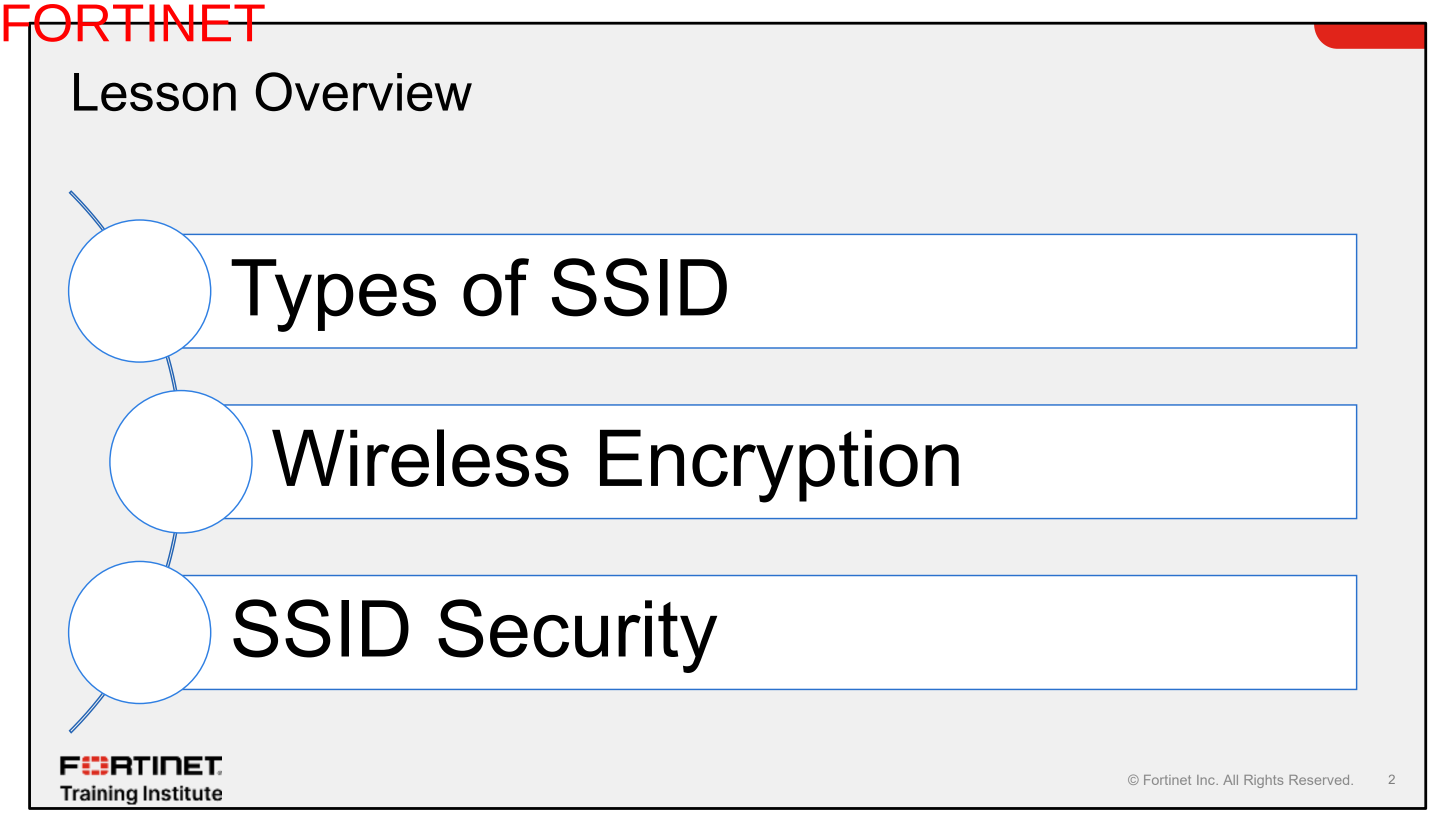
Secure Wireless LAN Administrator

Wireless Security

FortiOS 7.4

Last Modified: 2 May 2024

In this lesson, you will learn about wireless security deployment using the FortiOS integrated wireless controller.



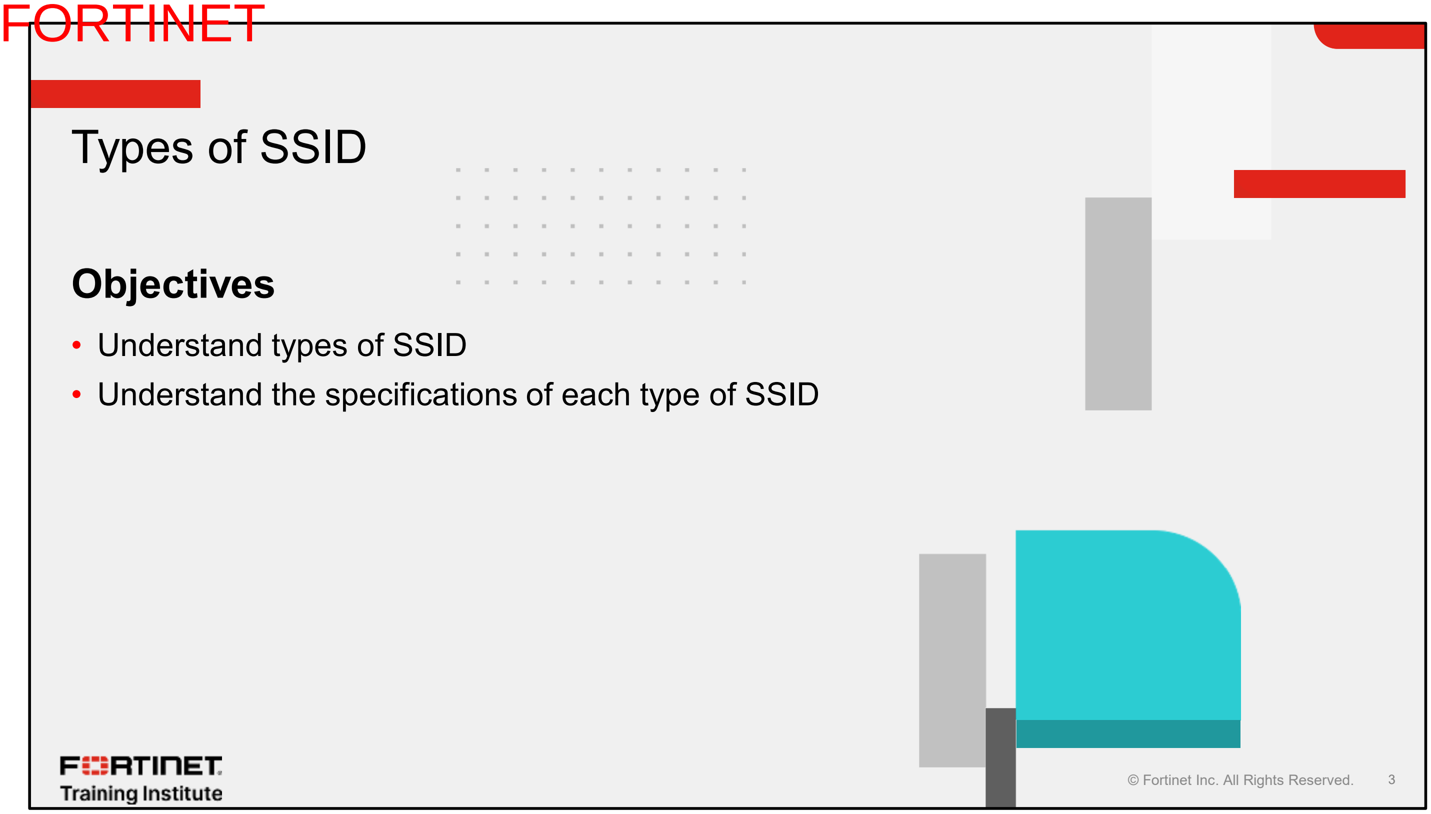
Lesson Overview

- Types of SSID
- Wireless Encryption
- SSID Security

FORTINET Training Institute

2

In this lesson, you will learn about the topics shown on this slide.



Types of SSID

Objectives

- Understand types of SSID
- Understand the specifications of each type of SSID

FORTINET Training Institute

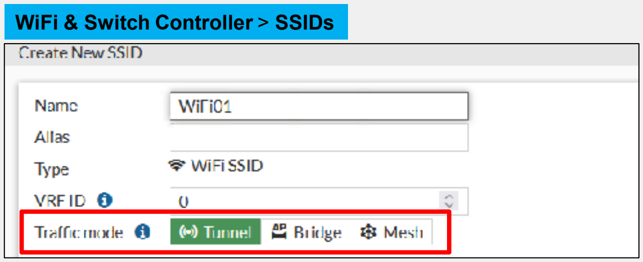
© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding SSIDs, you will be able to use them in your network.

Types of SSID

- There are three types of SSID that you can configure on FortiGate:
  - Tunnel mode—Traffic is tunneled back to wireless controller using CAPWAP data channel
  - Bridge mode—Traffic is bridged directly to the local LAN that AP is connected to
  - Wireless mesh—Used as backhaul SSID in a distributed connection



WiFi & Switch Controller > SSIDs

Create New SSID

Name: WiFi01

Alias:

Type: WiFi SSID

VRF ID: 0

Traffic mode: [✓ Tunnel] Bridge Mesh

Traffic mode must be defined at the time of initial SSID configuration

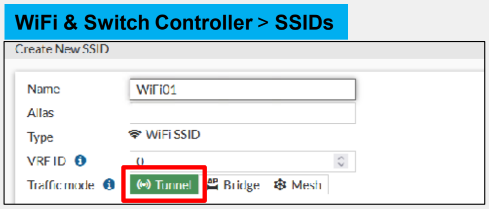
FORTINET Training Institute

4

You can configure three types of SSID on FortiGate: tunnel mode, bridge mode, and wireless mesh. It is important to choose the mode that best suits the needs and security requirements of your network.

Tunnel Mode

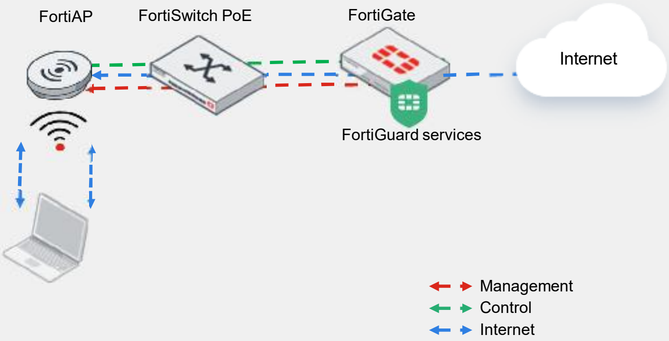
- Default SSID mode
- Wireless traffic is tunneled to FortiGate using CAPWAP data channel
- Separate interface and dedicated subnet for each SSID
- Requires separate firewall policy for SSID subnet
- **Pros**
  - Central place to enforce security
  - Layer 3 traffic segmentation
- **Cons**
  - FortiGate must be sized according to traffic
  - If controller goes down, wireless network will go down



WiFi & Switch Controller > SSIDs

Create New SSID

Name	WiFi01
Alias	
Type	WiFi SSID
VRF ID	0
Traffic mode	[✓ Tunnel] Bridge Mesh



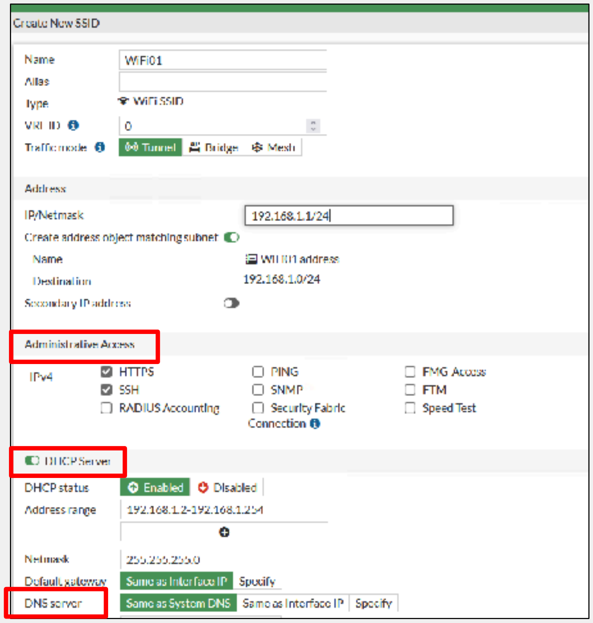
By default, tunnel mode SSID is selected when you define an SSID on FortiGate. In this mode, all traffic within CAPWAP DTLS or non-DTLS tunnels is sent to FortiGate before it is allowed on the LAN or the internet. There are two main advantages to using this mode:

- Traffic is subject to firewall policies and security threat scanning. Traffic must go through a security profile inspection and firewall policy examination before it is placed on the egress interface. This ensures that all security threats are addressed before a device is given access to internal or external resources.
- Traffic is processed at the session level. This gives FortiGate complete visibility of user and device activities on the network. FortiGate can track and log user activities and control access at the user level.

Tunnel Mode—SSID Interface

- Tunneled SSID is treated as a layer 3 interface
- Can configure required administrative access to wireless interface
- Must have separate DHCP and DNS settings

WiFi & Switch Controller > SSIDs



Create New SSID

Name: WiFi01
Alias:
Type: WiFi SSID
VRF ID: 0
Traffic mode: [✓ Tunnel] Bridge Mesh

Address

IP/Netmask: 192.168.1.1/24
Create address object matching subnet: ●
Name: WiFi01 address
Destination: 192.168.1.0/24
Secondary IP address: ○

Administrative Access

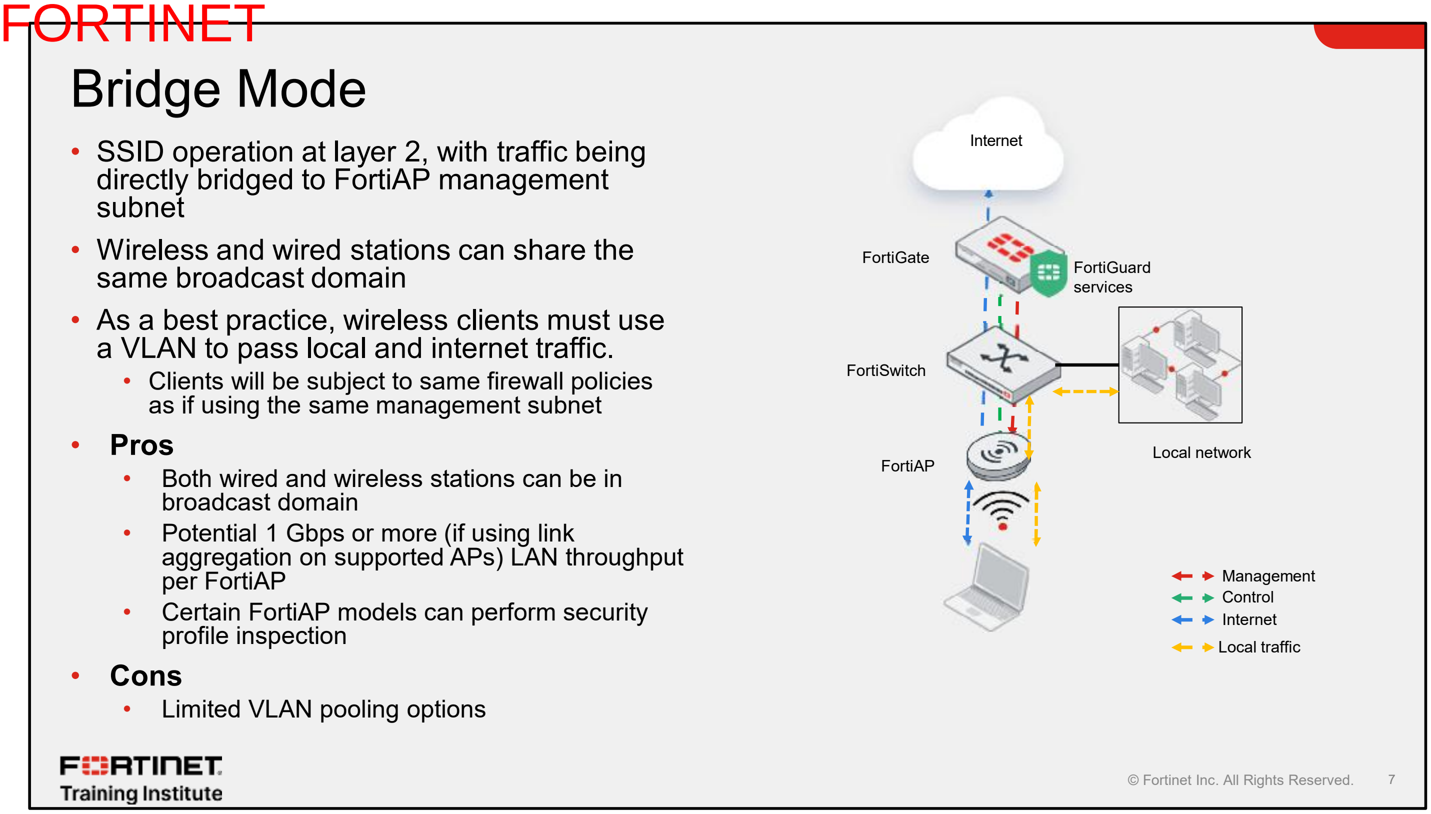
IPv4: ☑ HTTPS ☑ SSH ☐ RADIUS Accounting ☐ PING ☐ SNMP ☐ Security Fabric Connection ☐ FMG Access ☐ FTM ☐ Speed Test

● DHCP Server

DHCP status: [✓ Enabled] Disabled
Address range: 192.168.1.2-192.168.1.254
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify

6

A tunneled SSID is treated as an interface; therefore, you can configure relevant parameters as needed, including administrative access and DHCP for end stations connecting to this SSID.



Bridge Mode

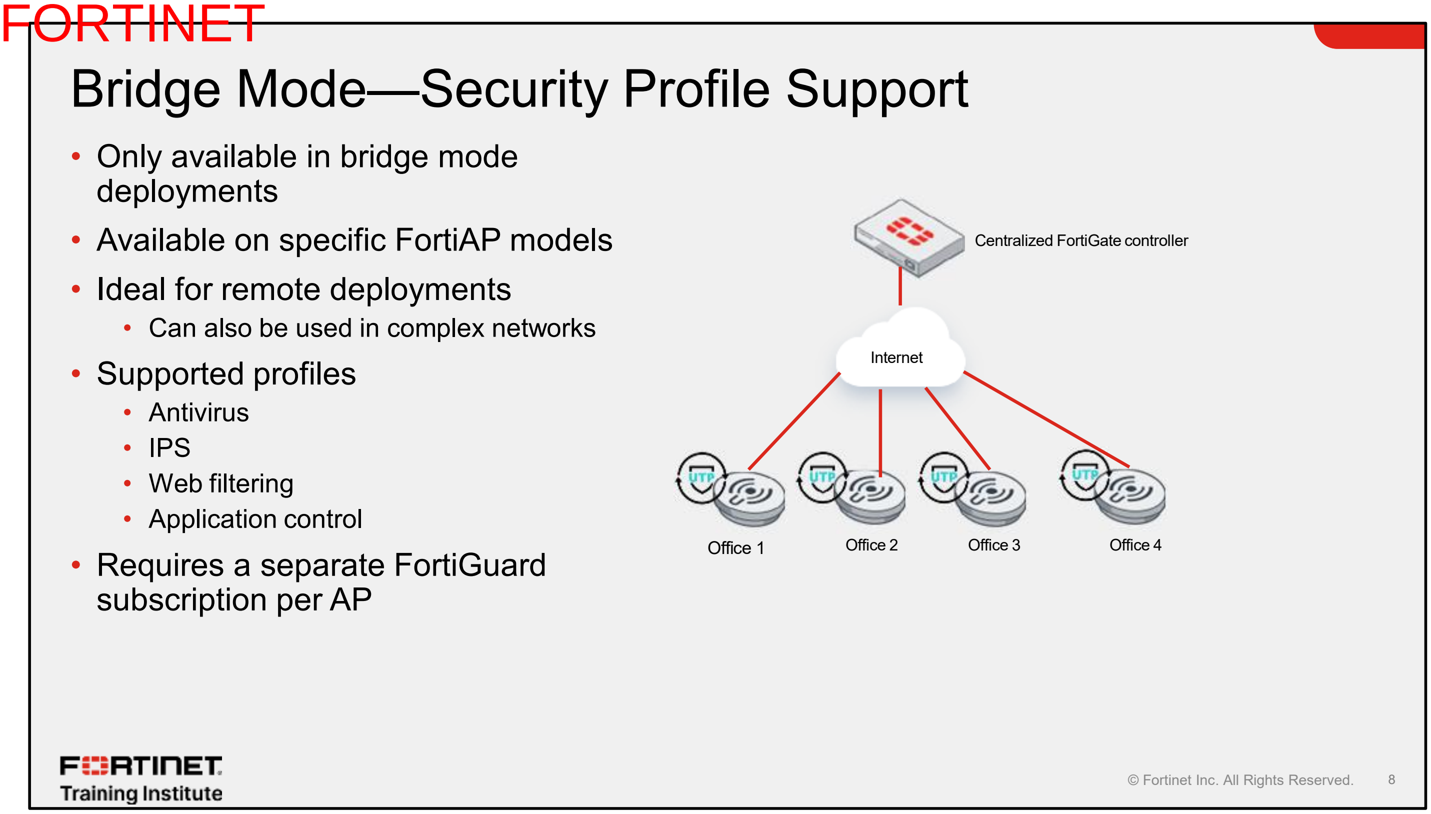
- SSID operation at layer 2, with traffic being directly bridged to FortiAP management subnet
- Wireless and wired stations can share the same broadcast domain
- As a best practice, wireless clients must use a VLAN to pass local and internet traffic.
  - Clients will be subject to same firewall policies as if using the same management subnet
- **Pros**
  - Both wired and wireless stations can be in broadcast domain
  - Potential 1 Gbps or more (if using link aggregation on supported APs) LAN throughput per FortiAP
  - Certain FortiAP models can perform security profile inspection
- **Cons**
  - Limited VLAN pooling options

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

Local bridge mode keeps the SSID operation at layer 2, with traffic being directly bridged to the FortiAP management subnet. Both wired and wireless stations can be in the same broadcast domain. As a best practice, it is important to assign a VLAN for wireless clients when connected to FortiAP. This mode is useful when deploying an AP that connects to a wireless controller over a WAN link at remote locations. As an added security measure, some FortiAP models can perform security inspection on the wireless traffic without forwarding the traffic to the wired network. This ensures that traffic put on the wired network have already been scanned for security threats.

When deployed locally, wireless traffic is subject to the same firewall policies as the FortiAP broadcasting the wireless network. Local traffic is switched at FortiSwitch and only the CAPWAP control traffic goes to the wireless controller.



Bridge Mode—Security Profile Support

- Only available in bridge mode deployments
- Available on specific FortiAP models
- Ideal for remote deployments
  - Can also be used in complex networks
- Supported profiles
  - Antivirus
  - IPS
  - Web filtering
  - Application control
- Requires a separate FortiGuard subscription per AP

8

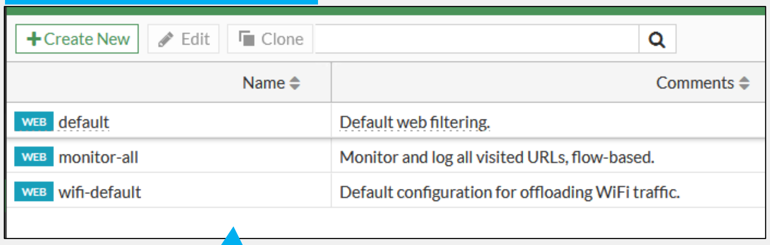
If a bridge mode SSID is configured for a managed FortiAP, you can add security profiles to the wireless controller, if the FortiAP model supports the security profile. This configuration allows you to apply the following security profile features to the traffic over the bridge SSID:

- Antivirus (including botnet protection)
- Intrusion prevention
- Application control
- Web filter

This is supported only in bridge mode. The traffic of a tunneled SSID is inspected by FortiGate, as usual.

Bridge Mode—Security Profile Support (Contd)

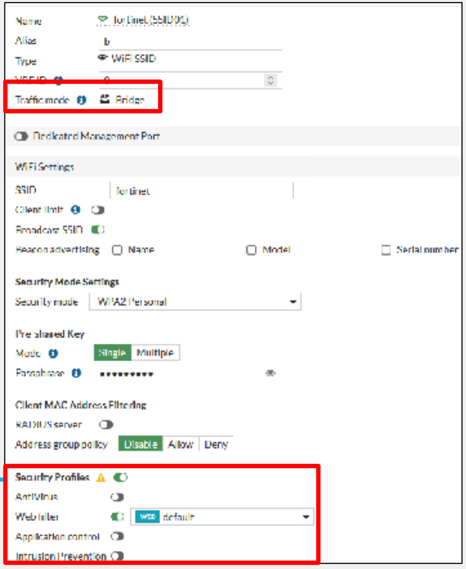
Security Profiles > Web Filter



Name	Comments
WEB default	Default web filtering.
WEB monitor-all	Monitor and log all visited URLs, flow-based.
WEB wifi-default	Default configuration for offloading WiFi traffic.

Create security profile

WiFi & Switch Controller > SSIDs



Name fortinet (SSID01)
Alias b
Type WiFi SSID
VRF ID 0
Traffic mode Bridge

Dedicated Management Port

WiFi Settings
SSID fortinet
Client limit
Broadcast SSID
Beacon advertising □ Name □ Model □ Serial number

Security Mode Settings
Security mode WPA2 Personal

Pre shared Key
Mode Single Multiple
Passphrase ••••••••••

Client MAC Address Filtering
RADIUS server
Address group policy Disable Allow Deny

Security Profiles
AntiVirus
Web filter WEB default
Application control
Intrusion Prevention

Apply security profile to an SSID

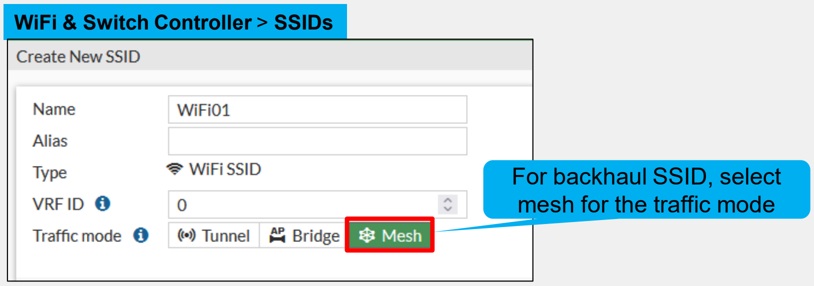
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

You can create a security profile and then apply it to an SSID. Supported FortiAPs get security profile updates from FortiGuard through a FortiGuard subscription.

Wireless Mesh

- Minimum three devices are required:
  - FortiGate as wireless controller
  - FortiAP as mesh root AP
  - FortiAP as leaf AP
- Backhaul SSID used by APs to create a mesh network



WiFi & Switch Controller > SSIDs

Create New SSID

Name: WiFi01

Alias:

Type: WiFi SSID

VRF ID: 0

Traffic mode: Tunnel | Bridge | Mesh (selected)

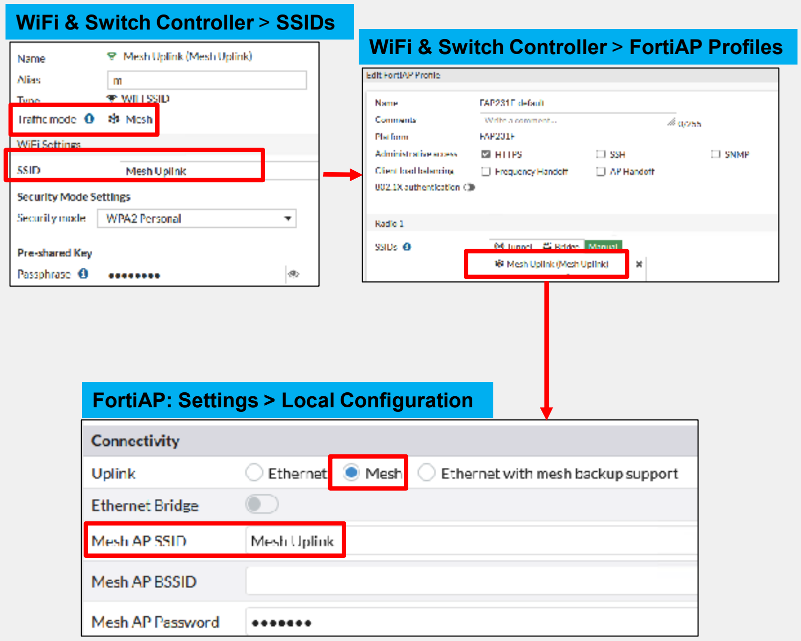
For backhaul SSID, select mesh for the traffic mode

Mesh mode SSID is deployed when Ethernet backhaul is not available. It bridges traffic from one SSID—the client service SSID—to a wireless backhaul SSID. Mesh mode is for cases where a FortiAP radio, rather than its Ethernet port, provides the backhaul to the controller. A mesh SSID is meant only for connecting FortiAPs wirelessly. For example, an outbuilding with power but no Ethernet to the main building could have a FortiAP in mesh mode connected to a root FortiAP that does have an Ethernet connection to the main network.

Wireless Mesh—Configuration

- Create a mesh SSID on the FortiGate wireless controller
- Broadcast the mesh SSID manually using the AP profile associated with the root AP
- Access the downstream AP using HTTPS or SSH
  - Change the uplink connectivity to mesh
  - Enter the mesh SSID configuration on the downstream AP
- Use these commands for configuration through SSH:

```
cfg -a MESH_AP_TYPE=1
cfg -a MESH_AP_SSID=Mesh Uplink
cfg -a MESH_AP_PASSWD=test1234
cfg -c
exit
```



WiFi & Switch Controller > SSIDs

Name: Mesh Uplink (Mesh Uplink)
Alias: m
Type: WiFi SSID
Traffic mode: Mesh

WiFi Settings
SSID: Mesh Uplink

Security Mode Settings
Security mode: WPA2 Personal

Pre-shared Key
Passphrase: ●●●●●●●●●

WiFi & Switch Controller > FortiAP Profiles

Edit FortiAP Profile

Name: FAP231F default
Comments: Write a comment... 0/255
Platform: FAP231F
Administrative access: ☑ HTTPS ☐ SSH ☐ SNMP
Client load balancing: ☐ Frequency Handoff ☐ AP Handoff
802.1X authentication

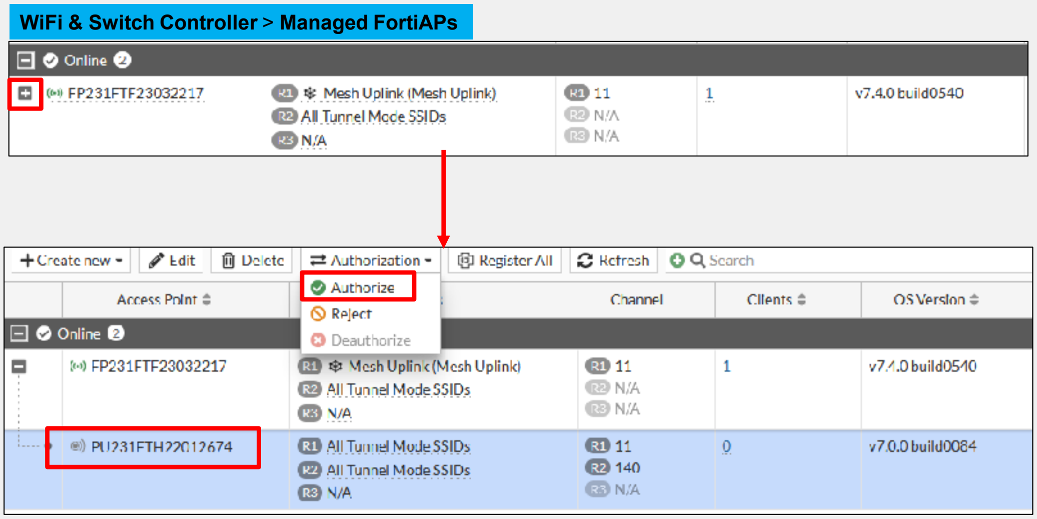
Radio 1
SSIDs: Tunnel Bridge Manual
Mesh Uplink (Mesh Uplink)

FortiAP: Settings > Local Configuration

Connectivity
Uplink: ○ Ethernet ● Mesh ○ Ethernet with mesh backup support
Ethernet Bridge
Mesh AP SSID: Mesh Uplink
Mesh AP BSSID:
Mesh AP Password: ●●●●●●●

You can configure a mesh SSID on the **SSIDs** page. You must enter all required information about the SSID, such as SSID name, security mode, and the SSID **Traffic mode** must be set to **Mesh**. You must manually broadcast the mesh SSID using the FortiAP profile associated with the root AP. You will learn more about the FortiAP profiles in another lesson. You can access the downstream AP through HTTPS or SSH, and then change the internal uplink configuration of the FortiAP device from **Ethernet** to **Mesh**. You must enter the mesh SSID configuration on the downstream FortiAP for it to connect back to the root FortiAP. You must repeat the same process for any additional downstream FortiAP.

Wireless Mesh—Configuration (Contd)



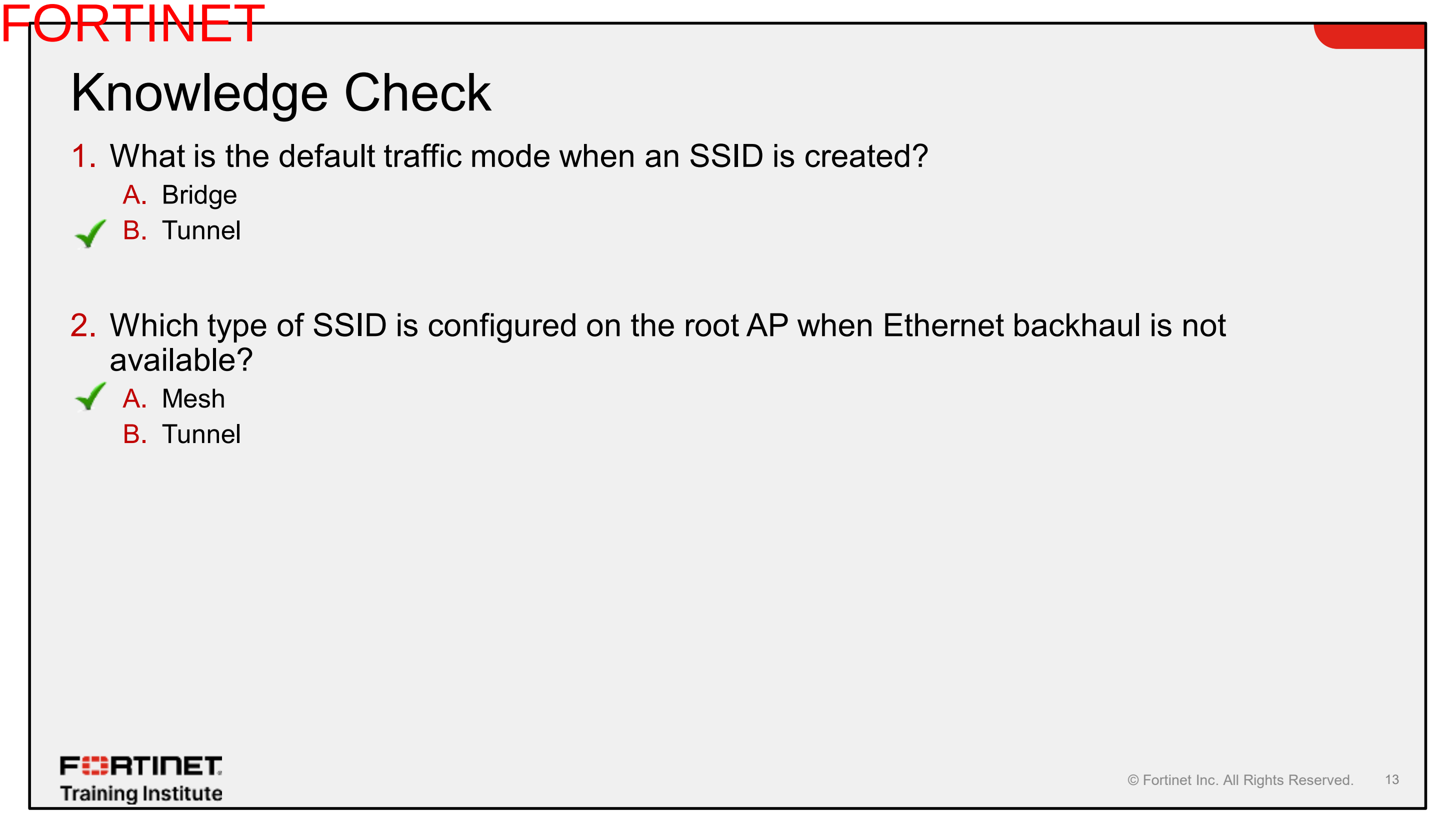
Online 2				
FP231FTF23032217	R1 Mesh Uplink (Mesh Uplink) R2 All Tunnel Mode SSIDs R3 N/A	R1 11 R2 N/A R3 N/A	1	v7.4.0 build0540

Access Point		Channel	Clients	OS Version
Online 2				
FP231FTF23032217	R1 Mesh Uplink (Mesh Uplink) R2 All Tunnel Mode SSIDs R3 N/A	R1 11 R2 N/A R3 N/A	1	v7.4.0 build0540
PU231FTH22012674	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 11 R2 140 R3 N/A	0	v7.0.0 build0084

FORTINET Training Institute

12

You must authorize the downstream FortiAP on the **Managed FortiAPs** page. You can click **+** beside the root FortiAP, to view all the downstream FortiAPs associated with it.



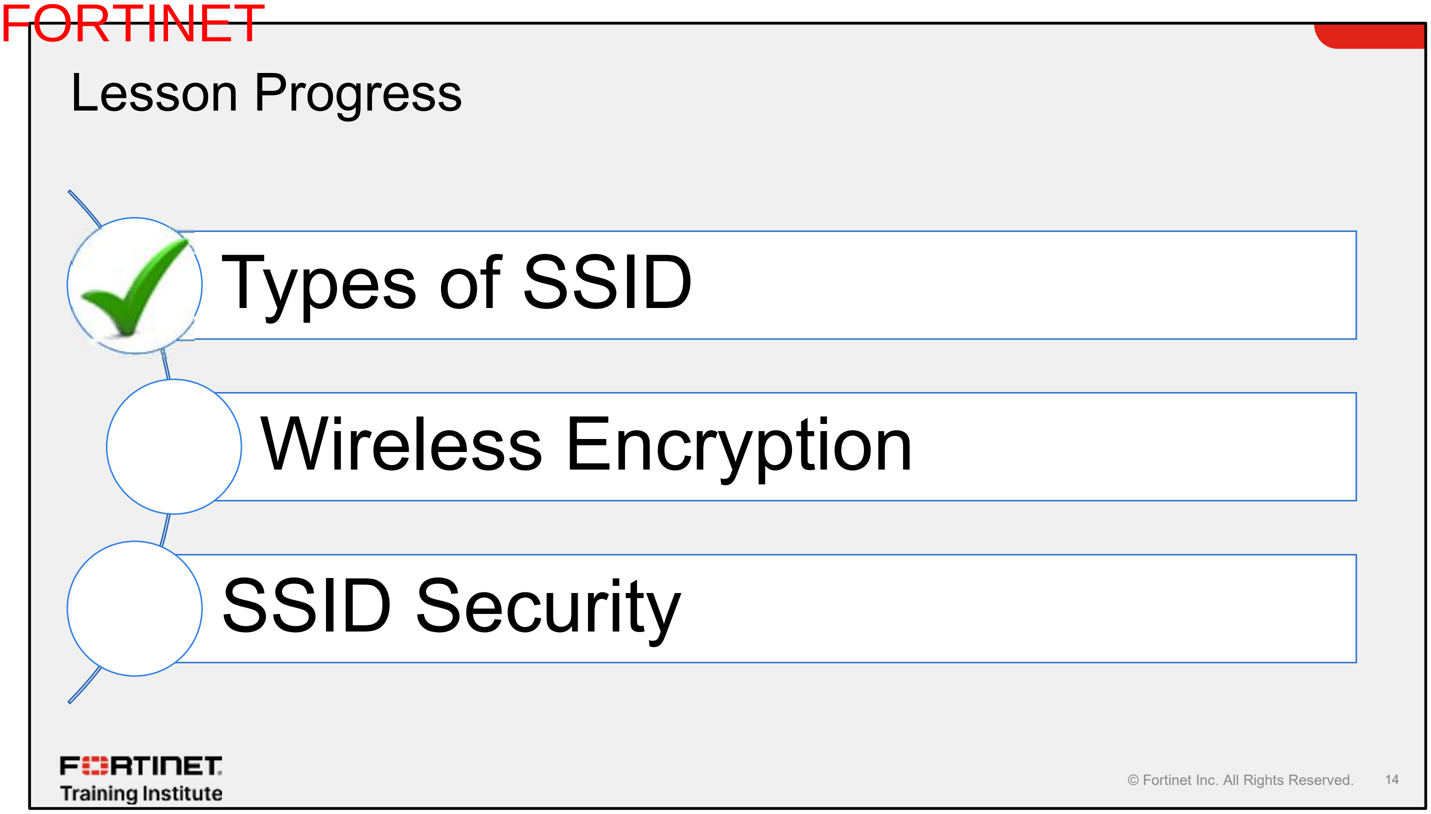
Knowledge Check

1. What is the default traffic mode when an SSID is created?
   - A. Bridge
   - ✓ B. Tunnel

2. Which type of SSID is configured on the root AP when Ethernet backhaul is not available?
   - ✓ A. Mesh
   - B. Tunnel

FORTINET Training Institute

13

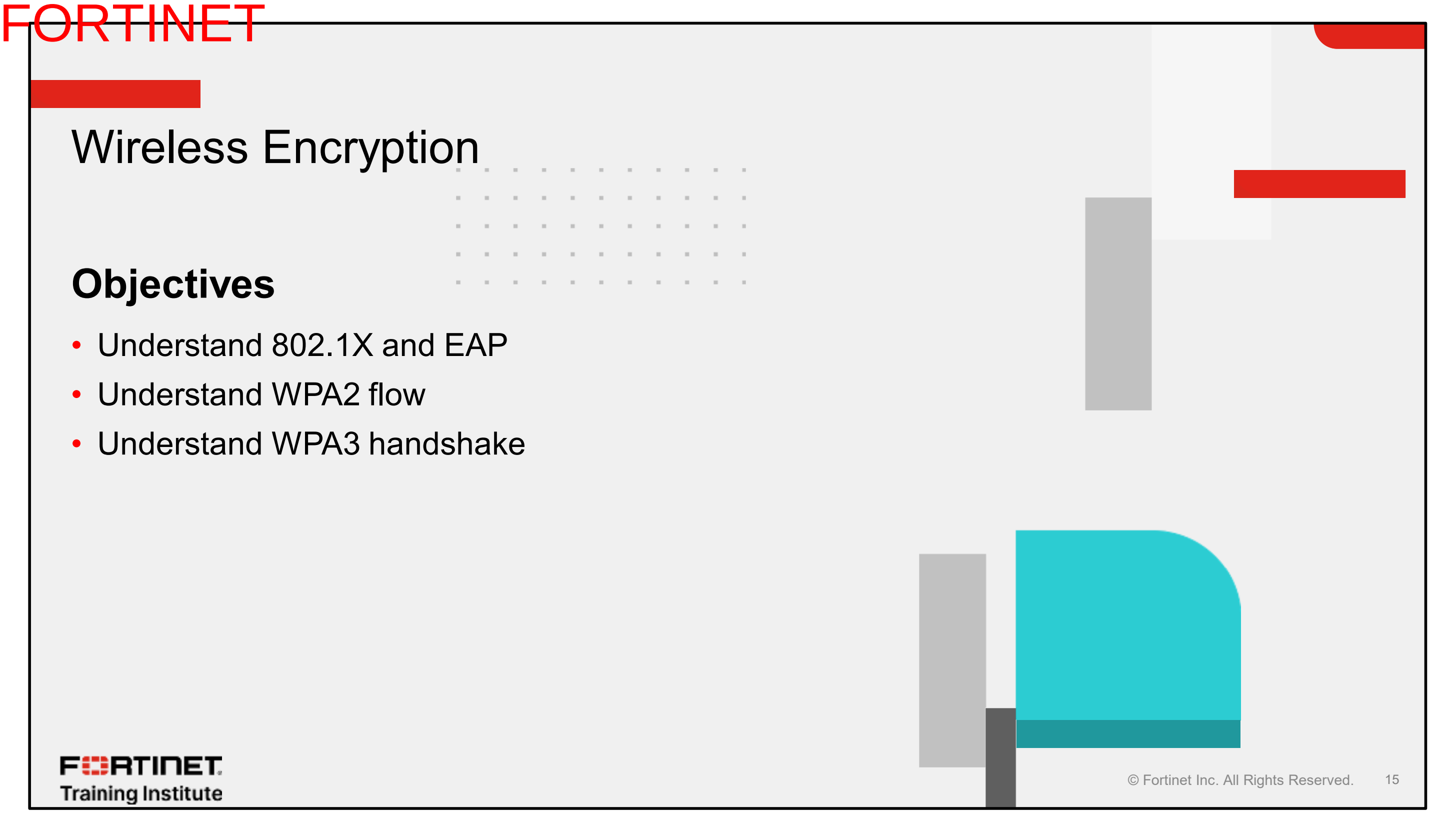


Lesson Progress

- ✓ Types of SSID
- ○ Wireless Encryption
- ○ SSID Security

14

Good job! You now understand SSID types and options. Now, you will learn about wireless encryption standards.



Wireless Encryption

Objectives

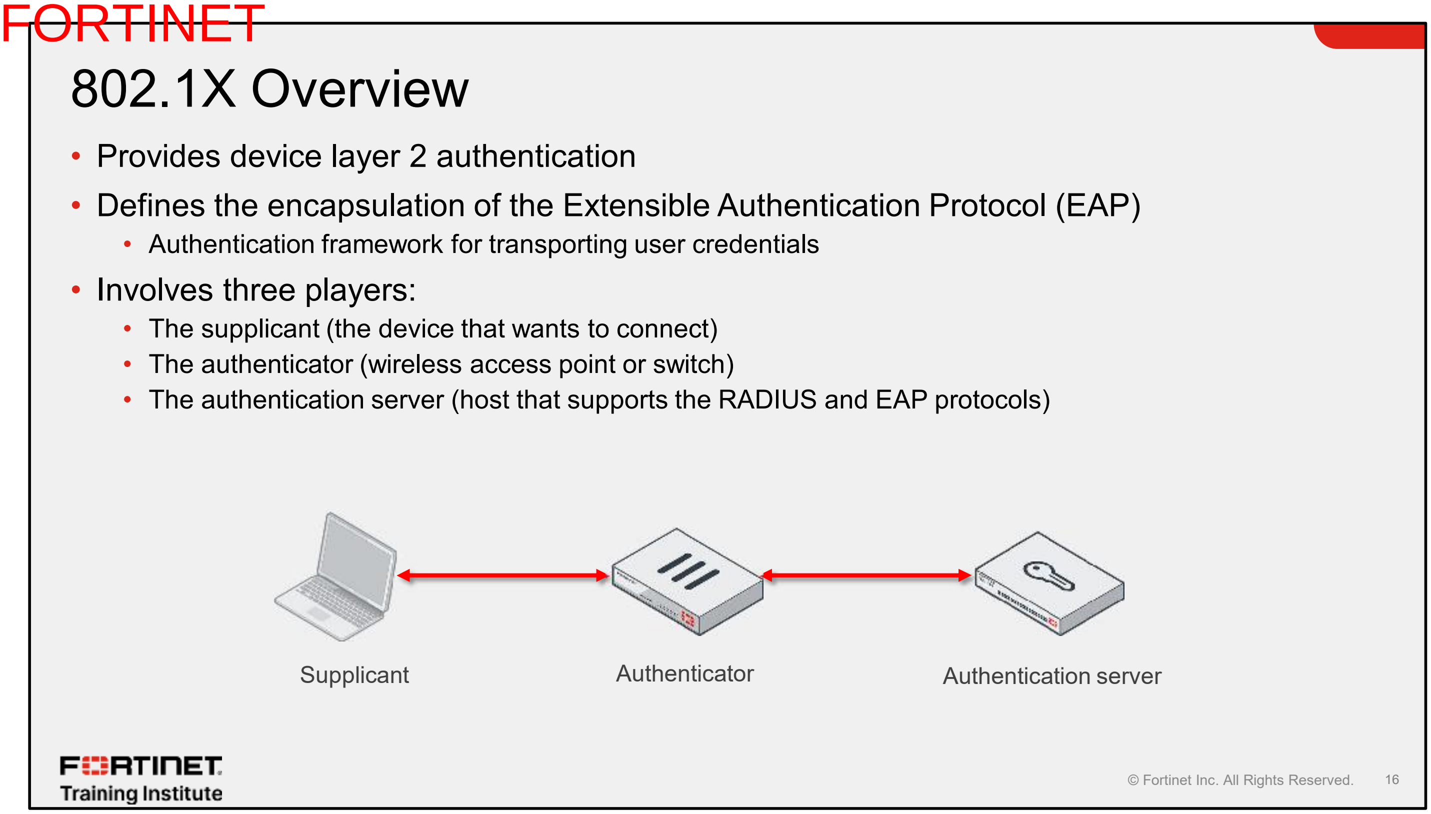
- Understand 802.1X and EAP
- Understand WPA2 flow
- Understand WPA3 handshake

Training Institute

15

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the wireless encryption standards on a wireless network, you will be able to implement them in your wireless network.



802.1X Overview

- Provides device layer 2 authentication
- Defines the encapsulation of the Extensible Authentication Protocol (EAP)
  - Authentication framework for transporting user credentials
- Involves three players:
  - The supplicant (the device that wants to connect)
  - The authenticator (wireless access point or switch)
  - The authentication server (host that supports the RADIUS and EAP protocols)

Supplicant

Authenticator

Authentication server

FORTINET Training Institute

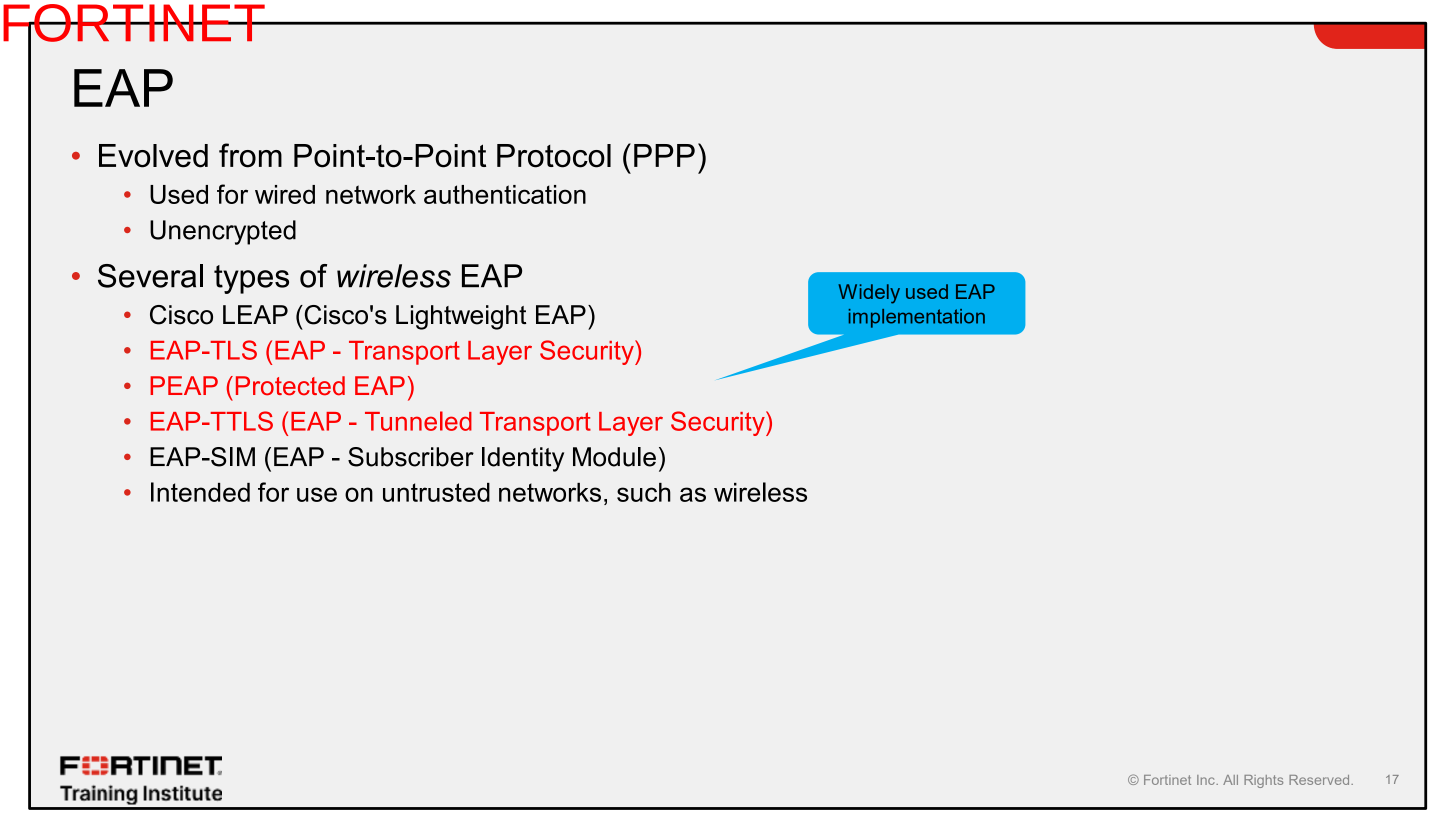
© Fortinet Inc. All Rights Reserved. 16

802.1X is a standard designed to provide authentication services to network devices that want to join a local wired or wireless network. The 802.1X standard defines an authentication protocol called EAP. It also defines how EAP is encapsulated over the LAN (the EAPOL protocol) and over RADIUS.

802.1X involves three parties: the client (also commonly known as the supplicant), which is the device that wants to join the network; the authenticator, which is a network device, such as a wireless access point or switch; and the authentication server, which is a host that supports the RADIUS and EAP protocol, such as FortiAuthenticator.

The client is allowed access to the layer 2 network until the client’s identity has been validated and authorized. Using 802.1X authentication, the client provides credentials to the authenticator, which the authenticator forwards to the authentication server for verification. If the authentication server determines that the credentials are valid, the client device is allowed access to the network.

Note that the authenticator does not need to have a certificate or have any knowledge of the authentication method (PEAP, TLS, and so on). The authentication is tunneled from the client to FortiAuthenticator over the RADIUS protocol.



EAP

- Evolved from Point-to-Point Protocol (PPP)
  - Used for wired network authentication
  - Unencrypted
- Several types of *wireless* EAP
  - Cisco LEAP (Cisco's Lightweight EAP)
  - EAP-TLS (EAP - Transport Layer Security)
  - PEAP (Protected EAP)
  - EAP-TTLS (EAP - Tunneled Transport Layer Security)
  - EAP-SIM (EAP - Subscriber Identity Module)
  - Intended for use on untrusted networks, such as wireless

Widely used EAP implementation

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

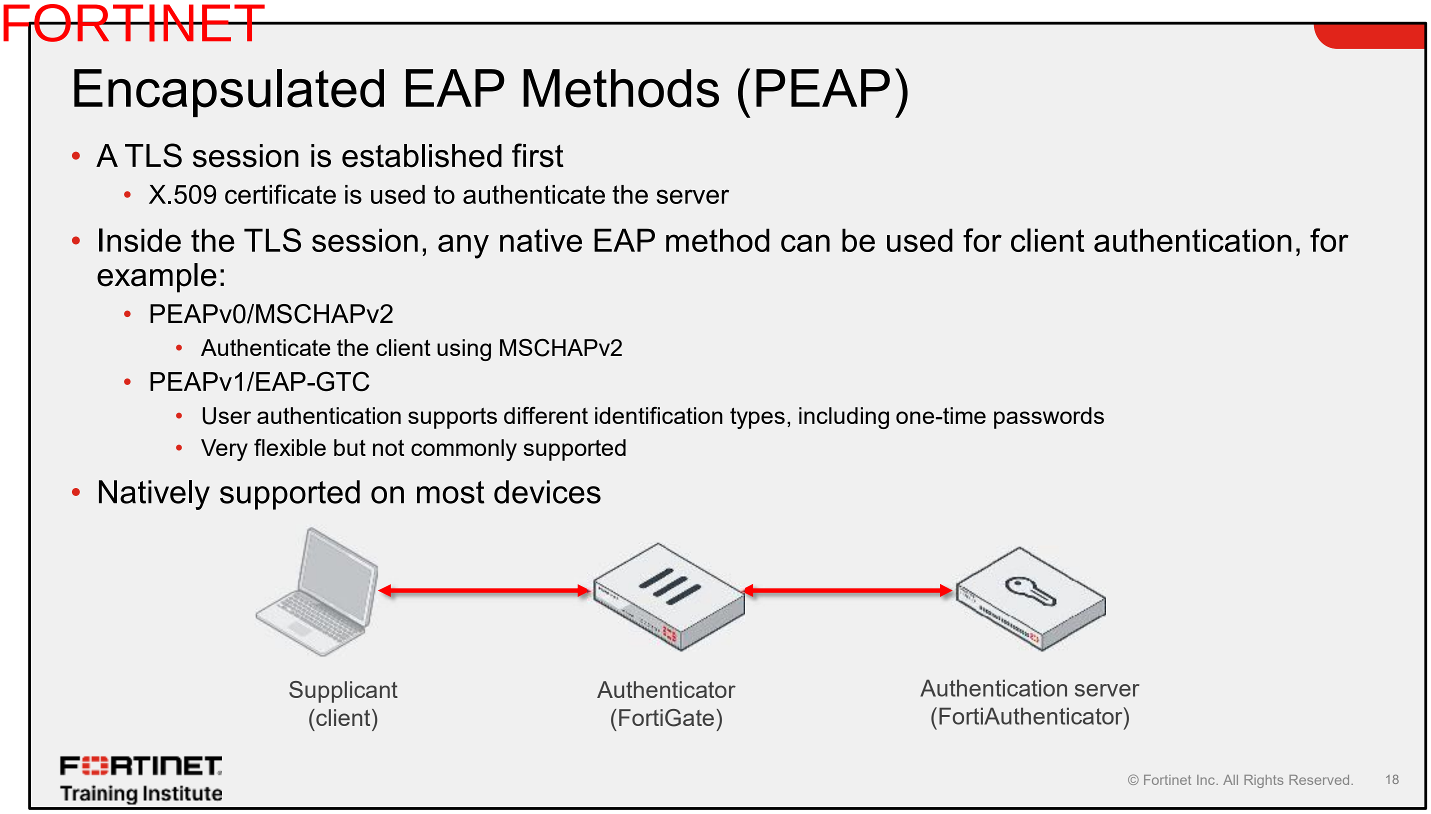
EAP is frequently used in wireless networks and point-to-point connections to authenticate users *before* they have access to the full network.

EAP is not a wire protocol; instead it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages. EAP is in wide use and has many different versions:

- Cisco LEAP (Cisco's Lightweight EAP)
- EAP-TLS (EAP - Transport Layer Security)
- PEAP (Protected EAP)
- EAP-TTLS (EAP - Tunneled Transport Layer Security)
- EAP-SIM (EAP - Subscriber Identity Module)

Some, such as Cisco LEAP, are proprietary, while others, like EAP-TLS, are considered standard. Also, some may provide only one-way authentication, while others provide two-way authentication more commonly called mutual authentication. This process involves a few elements:

- The supplicant at the client station is a piece of software running on the device that wants to be authenticated.
- The authenticator (in this case, FortiOS) controls access to the network.
- The authentication server (often a RADIUS server) decides to authorize the user or not. It can be local or remote.



Encapsulated EAP Methods (PEAP)

- A TLS session is established first
  - X.509 certificate is used to authenticate the server
- Inside the TLS session, any native EAP method can be used for client authentication, for example:
  - PEAPv0/MSCHAPv2
    - Authenticate the client using MSCHAPv2
  - PEAPv1/EAP-GTC
    - User authentication supports different identification types, including one-time passwords
    - Very flexible but not commonly supported
- Natively supported on most devices

Supplicant
(client)

Authenticator
(FortiGate)

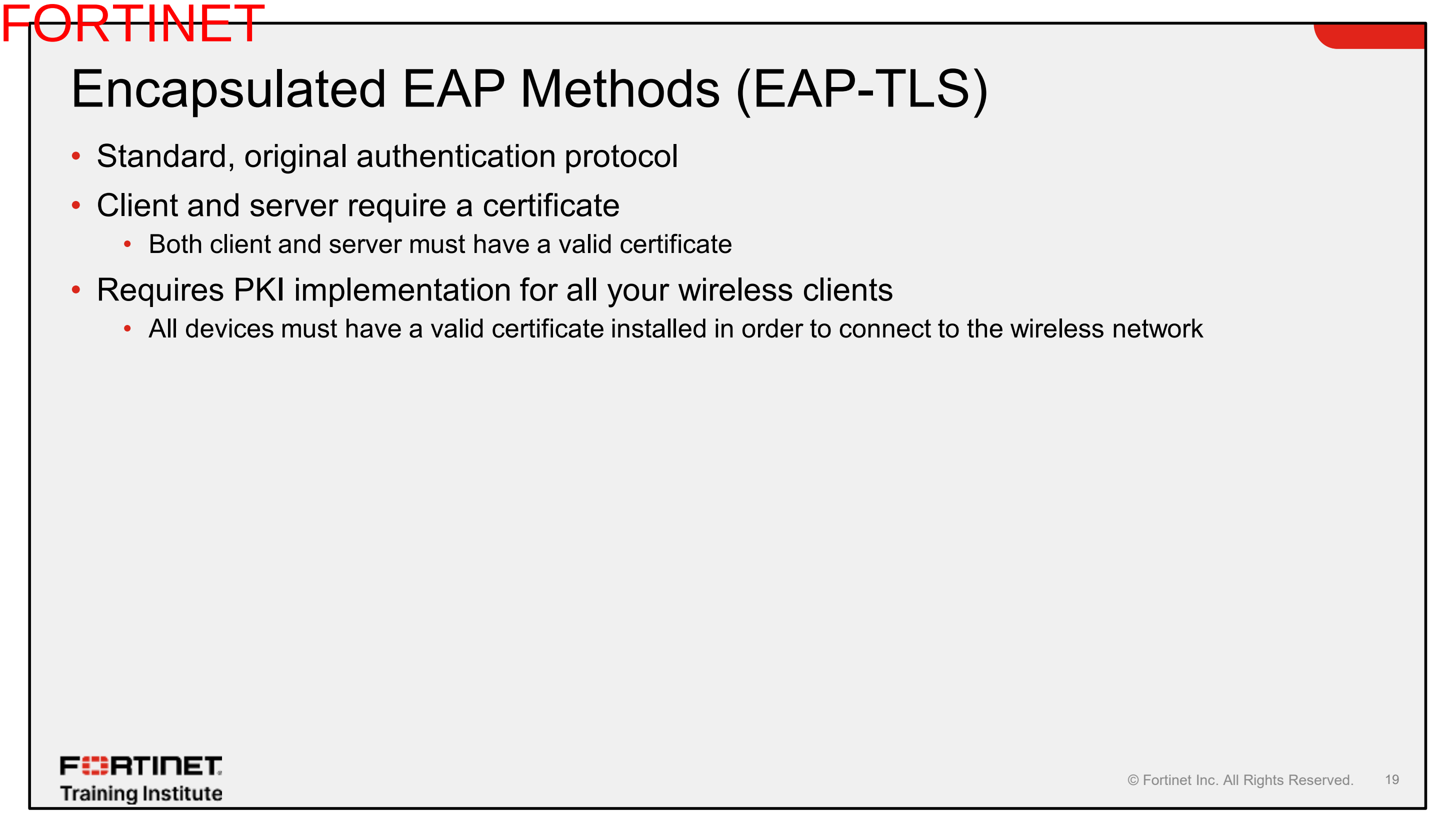
Authentication server
(FortiAuthenticator)

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 18

Using encapsulated EAP methods, the client establishes a TLS session first. At this point, the authentication server uses a digital certificate to authenticate the client. Encapsulated inside the TLS session, the client uses any native EAP method for client authentication. Two examples of encapsulated EAP methods are:

- PEAPv0/MSCHAPv2: Authenticates the client using MSCHAPv2
- PEAPv1/EAP-GTC: Uses different identification mechanisms (including one-time passwords) for authenticating clients, which makes it very flexible. FortiAuthenticator supports it, but it is not commonly supported by other vendors.



Encapsulated EAP Methods (EAP-TLS)

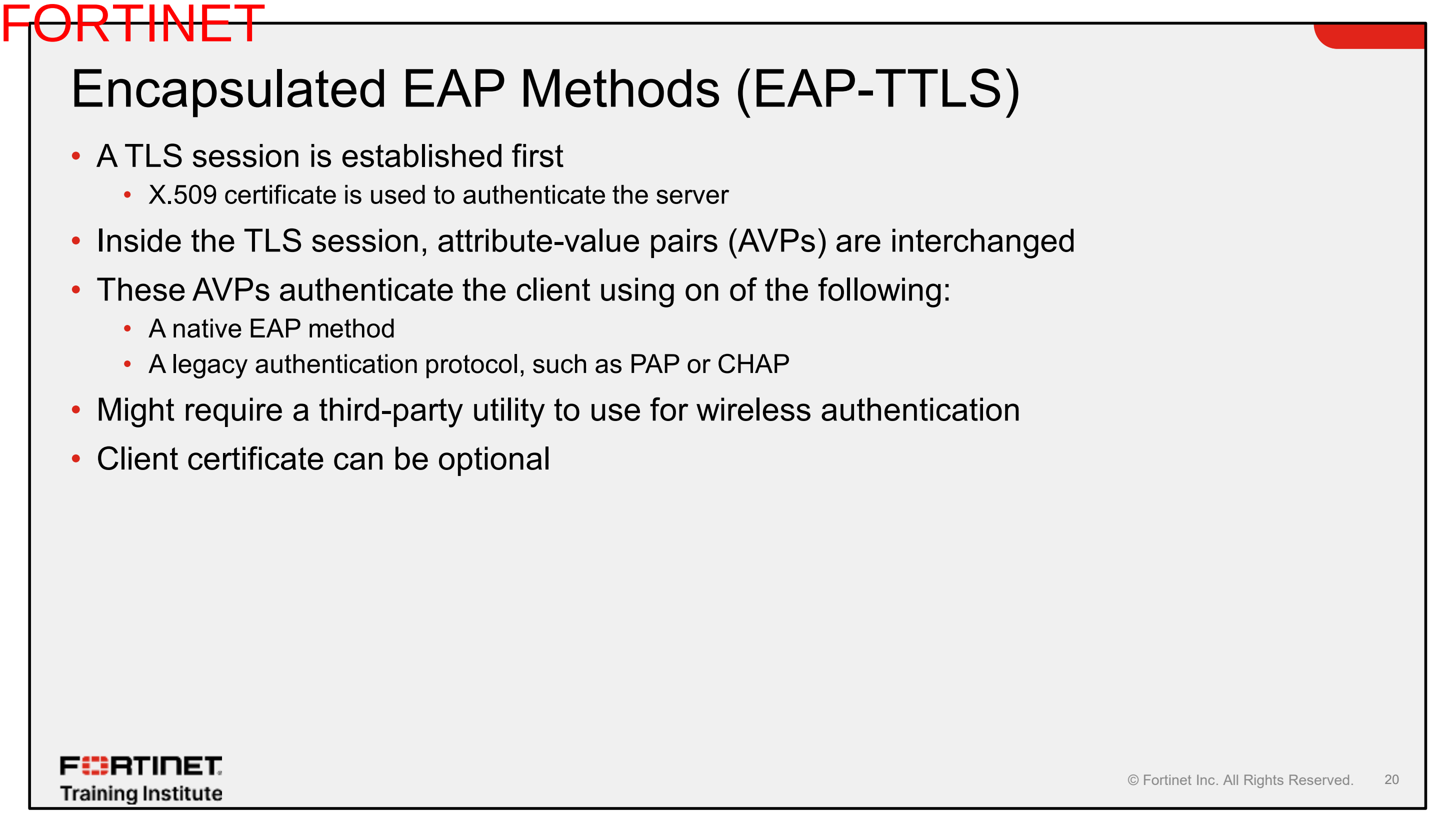
- Standard, original authentication protocol
- Client and server require a certificate
  - Both client and server must have a valid certificate
- Requires PKI implementation for all your wireless clients
  - All devices must have a valid certificate installed in order to connect to the wireless network

FORTINET Training Institute

19

EAP-TLS is one of the common native methods that uses TLS and digital certificates on both clients and server to authenticate. EAP-TLS requires PKI implementation for all your wireless clients.

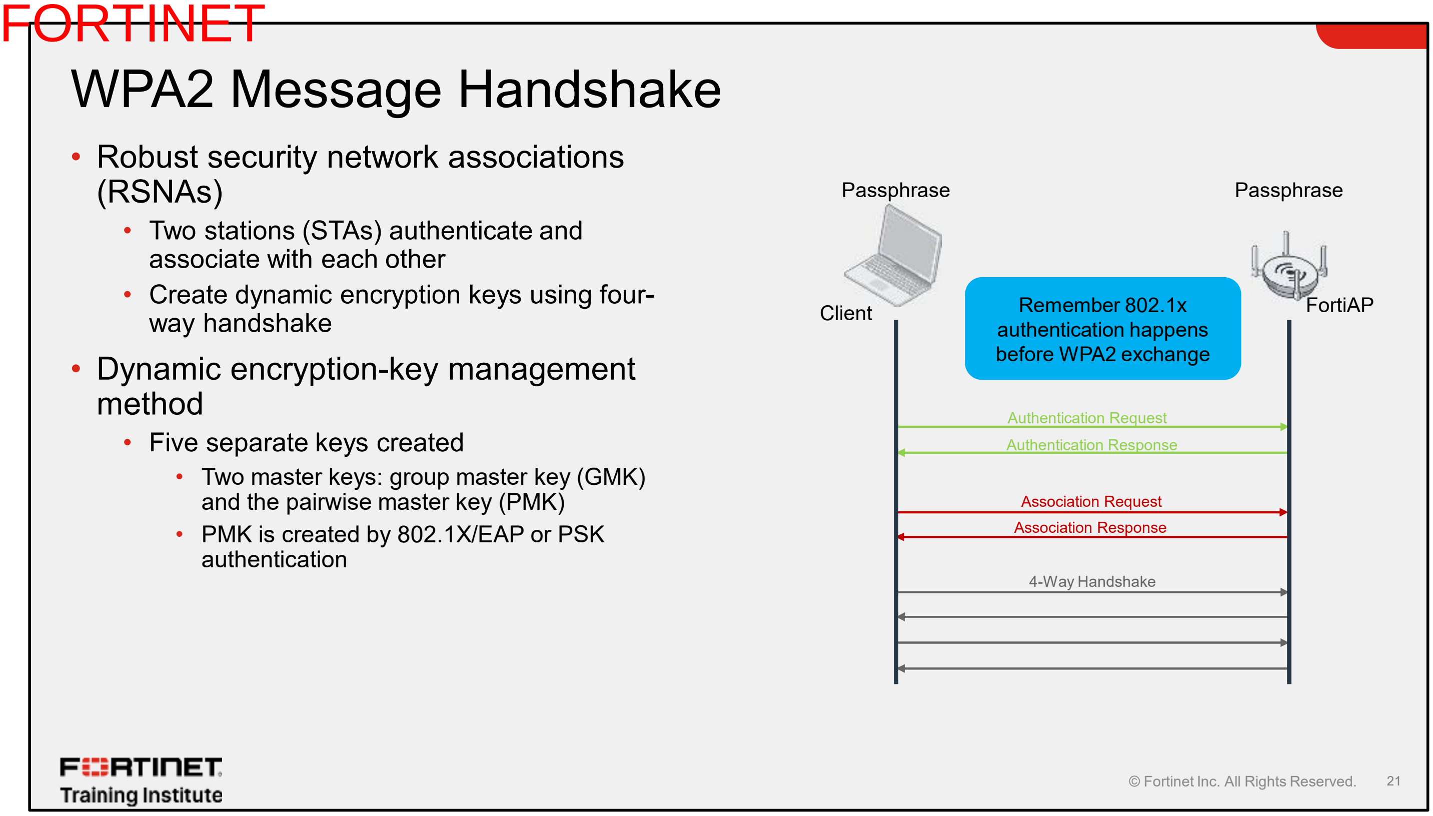
All devices will need to have a valid certificate installed in order to connect to the wireless network



Encapsulated EAP Methods (EAP-TTLS)

- A TLS session is established first
  - X.509 certificate is used to authenticate the server
- Inside the TLS session, attribute-value pairs (AVPs) are interchanged
- These AVPs authenticate the client using on of the following:
  - A native EAP method
  - A legacy authentication protocol, such as PAP or CHAP
- Might require a third-party utility to use for wireless authentication
- Client certificate can be optional

Another encapsulated method is EAP-TTLS. With this encapsulated method, AVPs authenticate the clients using either a native EAP method or a legacy authentication protocol (such as PAP or CHAP). EAP-TTLS is not natively supported on many devices. Therefore, you might need to use a third-party utility to perform authentication.



WPA2 Message Handshake

- Robust security network associations (RSNAs)
  - Two stations (STAs) authenticate and associate with each other
  - Create dynamic encryption keys using four-way handshake
- Dynamic encryption-key management method
  - Five separate keys created
    - Two master keys: group master key (GMK) and the pairwise master key (PMK)
    - PMK is created by 802.1X/EAP or PSK authentication

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

This slide provides an overview of the WPA2 message handshake. A wireless client using 802.1X authentication must be authenticated before the WPA2 message exchange. After authentication, there is association and, finally, the four-way WPA/WPA2 handshake.

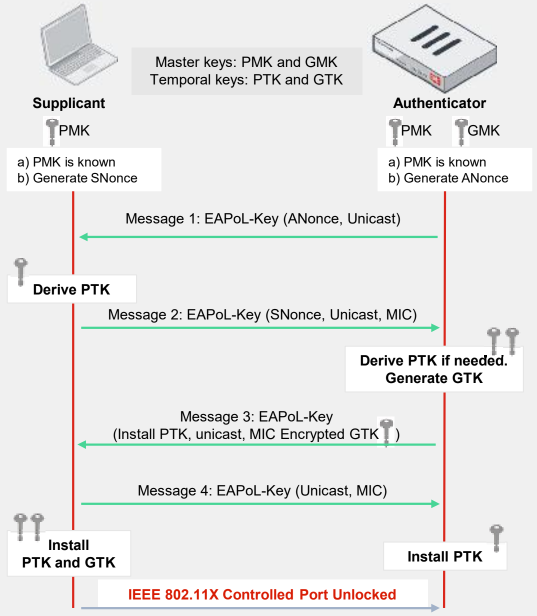
The four-way handshake occurs in the last four frames during either 802.1 X/EAP or PSK authentication. It produces what most people think of as Wi-Fi encryption. IEEE 802.11-2007 defines RSN and RSNAs. RSNAs specify that two stations must:

- Establish a procedure to authenticate and associate with each other
- Create dynamic encryption keys through a process known as the four-way handshake, which has become a major component for wireless secure communications

RSNAs utilize a dynamic encryption-key management method that involves the creation of five separate keys. Part of the RSNA process involves the creation of two master keys known as the group master key (GMK) and the pairwise master key (PMK).

The PMK is created as a result of 802.1X/EAP authentication, but can also be created from PSK authentication.

Four-Way Handshake



Supplicant

Master keys: PMK and GMK
Temporal keys: PTK and GTK

Authenticator

PMK

PMK GMK

a) PMK is known
b) Generate SNonce

a) PMK is known
b) Generate ANonce

Message 1: EAPoL-Key (ANonce, Unicast)

Derive PTK

Message 2: EAPoL-Key (SNonce, Unicast, MIC)

Derive PTK if needed.
Generate GTK

Message 3: EAPoL-Key
(Install PTK, unicast, MIC Encrypted GTK)

Message 4: EAPoL-Key (Unicast, MIC)

Install
PTK and GTK

Install PTK

IEEE 802.11X Controlled Port Unlocked

- Master keys are seeds to create final dynamic keys
- Final keys are:
  - PTK—Used to encrypt/decrypt unicast traffic
  - GTK—Used to encrypt/decrypt broadcast and multicast traffic
- Final keys are created during a four-way EAP frame exchange
  - Also known as four-way handshake
  - Always the last four frames exchanged during either 802.1 X/EAP or PSK authentication
  - Each time a client roams from one AP to another, a new four-way handshake occurs

FORTINET Training Institute

22

This slide shows the four-way handshake.

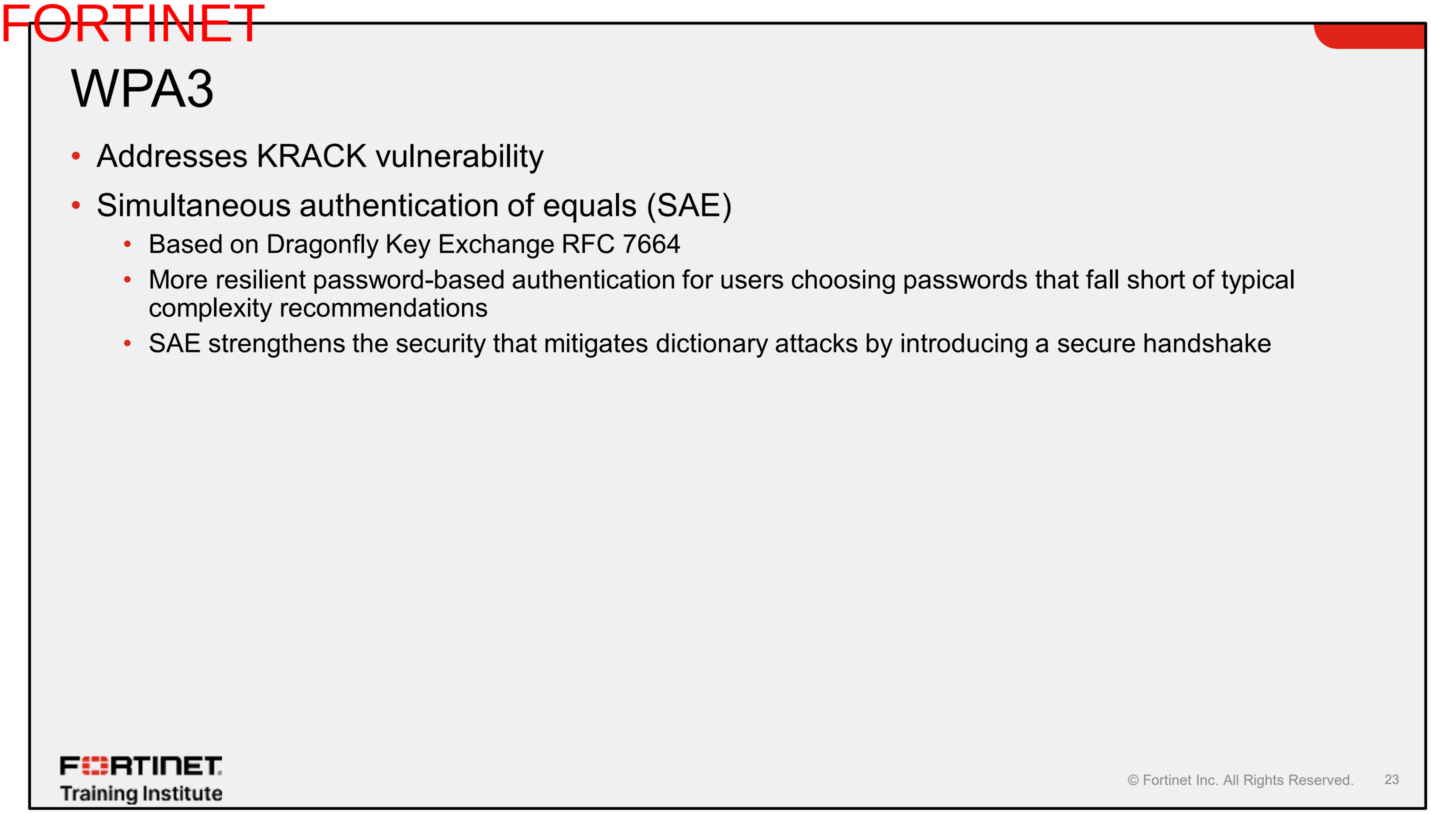
Since it occurs at the OSI layer 2 link establishment, the handshake is a frame exchange between the supplicant and the authenticator. It uses EAP key frames to generate temporary encryption keys. Those temporary keys are used to encrypt and decrypt the MAC service data unit payload of 802.11 Ethernet data frames.

These master keys are seeds used to create the final dynamic keys, which are used for encryption and decryption.

The final encryption keys are known as the PTK and the GTK.

- The PTK is used to encrypt and decrypt unicast traffic. It has no time out.
- The GTK is used to encrypt and decrypt broadcast and multicast traffic. It changes regularly and is delivered and installed on the client.

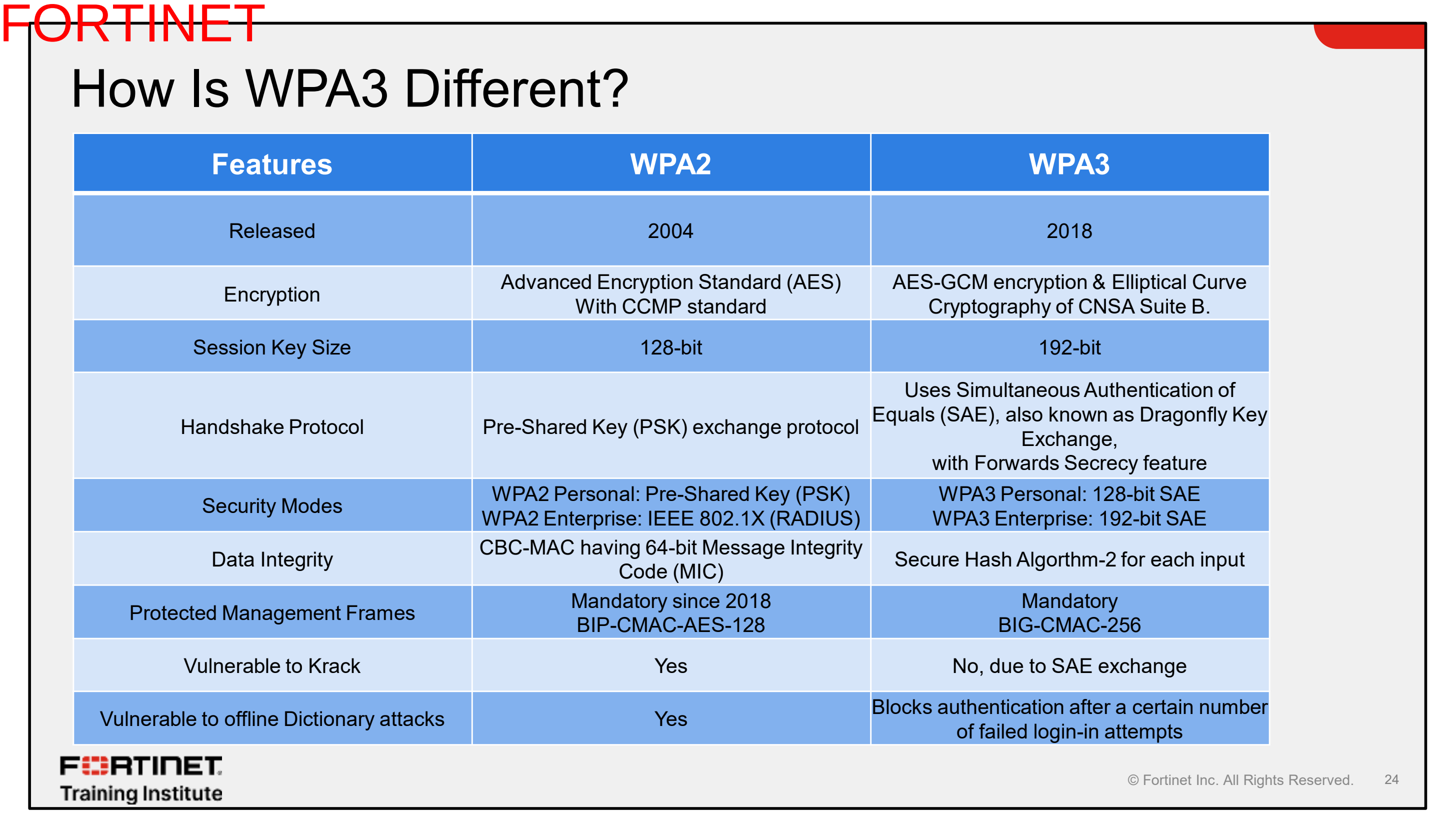
Whenever TKIP/RC4 or CCMP/AES dynamic keys are created—including when a client roams from one AP to another—the four-way handshake occurs again.



WPA3

- Addresses KRACK vulnerability
- Simultaneous authentication of equals (SAE)
  - Based on Dragonfly Key Exchange RFC 7664
  - More resilient password-based authentication for users choosing passwords that fall short of typical complexity recommendations
  - SAE strengthens the security that mitigates dictionary attacks by introducing a secure handshake

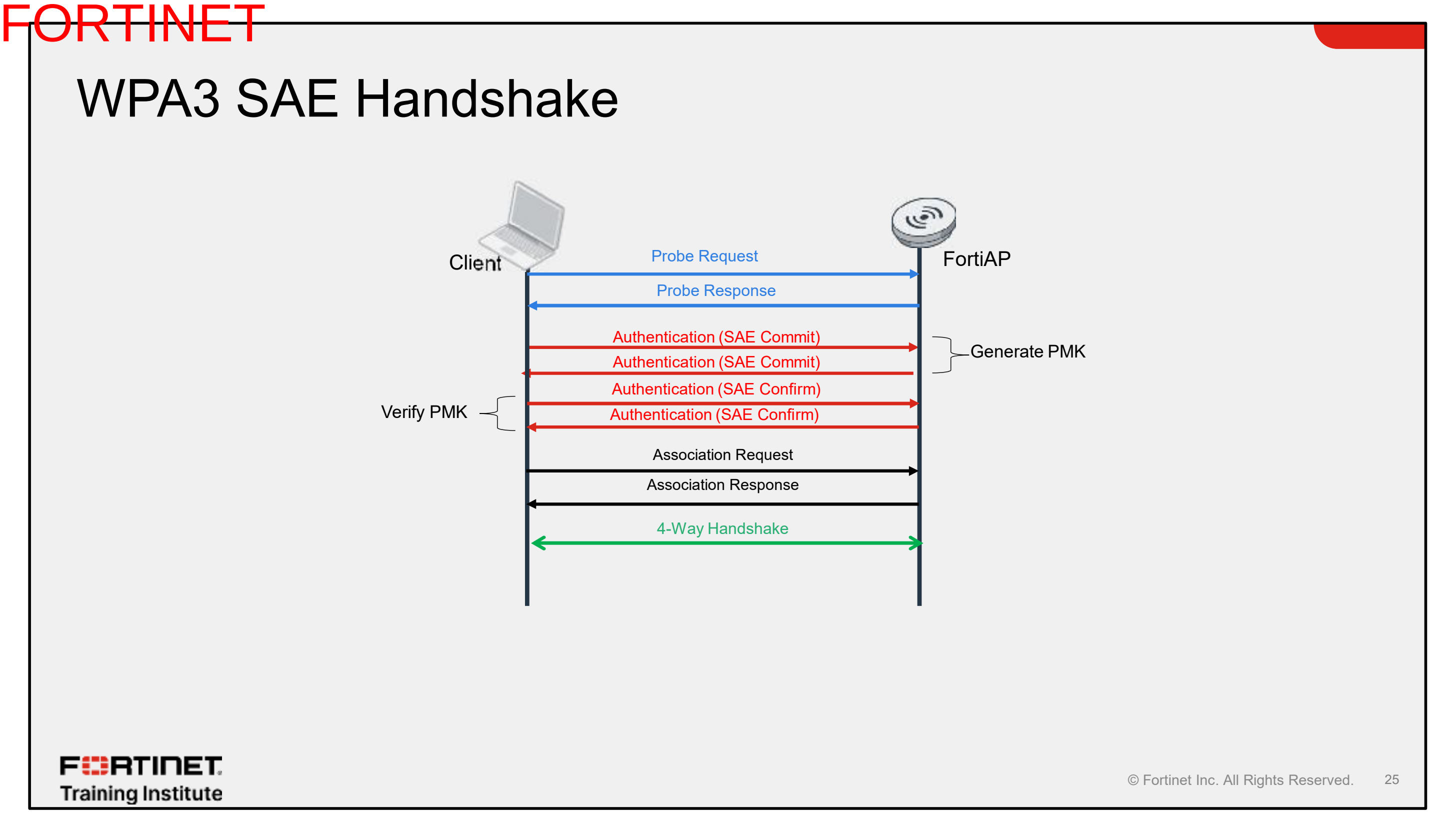
This security mode addresses the KRACK vulnerability that affected the previous version of WAP. WPA3 features SAE, which provides more resilient password-based authentication for passwords that fall short of the typical complexity recommendation. SAE strengthens the security of the wireless network against dictionary attacks because it features a secure handshake method. Unlike WPA2, WPA3 no longer uses the passphrase itself for the PMK derivation.



How Is WPA3 Different?

Features	WPA2	WPA3
Released	2004	2018
Encryption	Advanced Encryption Standard (AES) With CCMP standard	AES-GCM encryption & Elliptical Curve Cryptography of CNSA Suite B.
Session Key Size	128-bit	192-bit
Handshake Protocol	Pre-Shared Key (PSK) exchange protocol	Uses Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, with Forwards Secrecy feature
Security Modes	WPA2 Personal: Pre-Shared Key (PSK) WPA2 Enterprise: IEEE 802.1X (RADIUS)	WPA3 Personal: 128-bit SAE WPA3 Enterprise: 192-bit SAE
Data Integrity	CBC-MAC having 64-bit Message Integrity Code (MIC)	Secure Hash Algorthm-2 for each input
Protected Management Frames	Mandatory since 2018 BIP-CMAC-AES-128	Mandatory BIG-CMAC-256
Vulnerable to Krack	Yes	No, due to SAE exchange
Vulnerable to offline Dictionary attacks	Yes	Blocks authentication after a certain number of failed login-in attempts

The table on this slide shows the differences between WPA2 and WPA3 security modes.



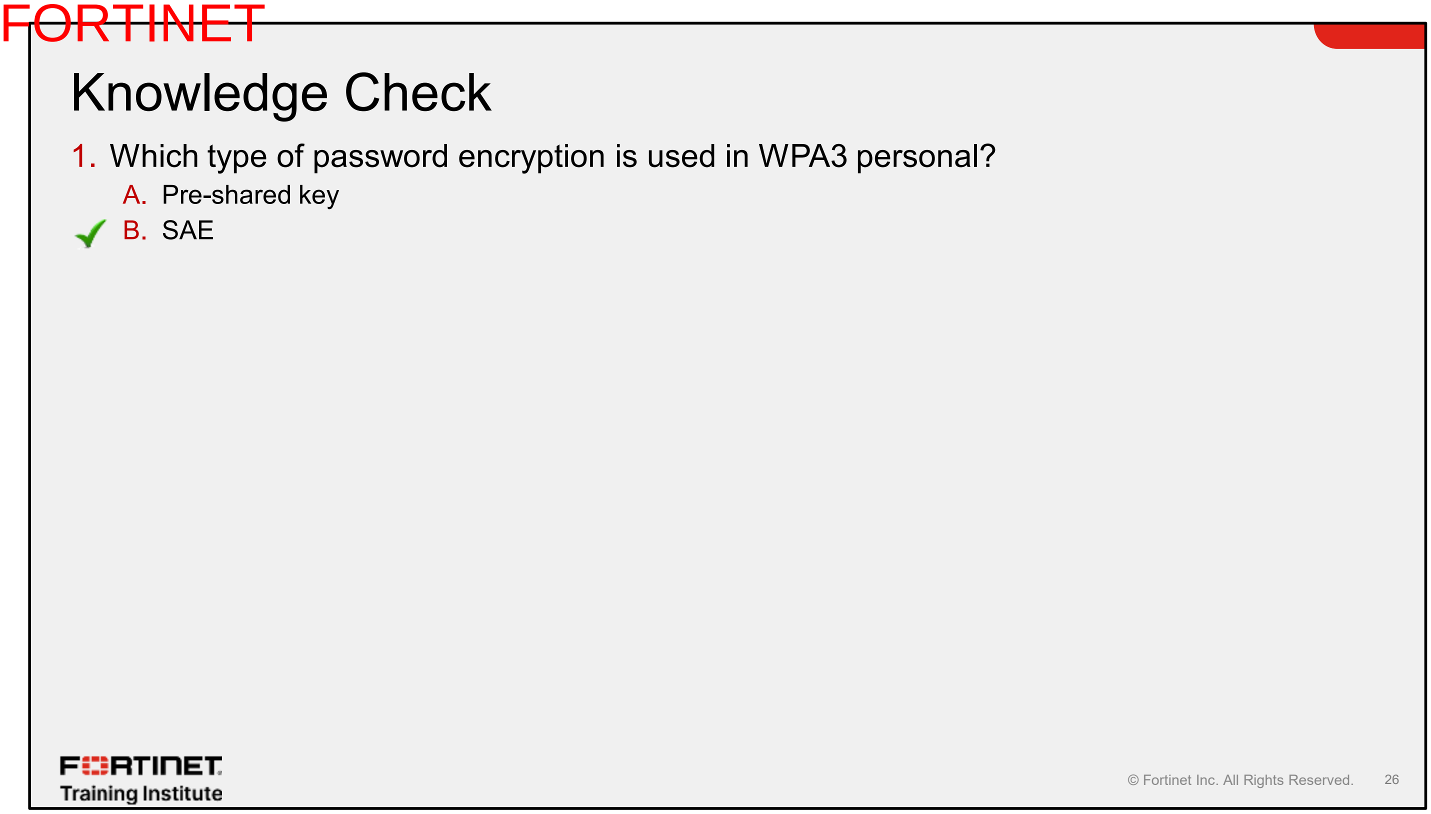
WPA3 SAE Handshake

Client
FortiAP
Probe Request
Probe Response
Authentication (SAE Commit)
Authentication (SAE Commit)
Generate PMK
Authentication (SAE Confirm)
Authentication (SAE Confirm)
Verify PMK
Association Request
Association Response
4-Way Handshake
FORTINET Training Institute

25

This slide shows the WPA3 SAE handshake.

1. The client sends a regular probe request to the AP to connect to the SSID.
2. The AP sends a probe response to the client’s request.
3. The client sends an authentication commit 802.11 frame to the AP, which contains a randomly generated scalar and element. These randomly generated values are not related to the SAE password. The authentication sequence for this frame is 1. These values are used to generate the PMK on the client based on elliptic curve cryptography (ECC). The client and AP both need each other’s scalar and element values to generate PMK.
4. The AP sends an authentication commit 802.11 frame with its own scalar and element value to the client. These values are used to generate the PMK on the AP. The authentication commit is represented with authentication sequence number 1.
5. The client sends an authentication confirmation value with a generated key based on the calculated PMK to the AP.
6. The AP sends back an authentication confirmation message, letting the client know if the authentication is successful.
7. If the authentication is successful, the client sends an association request to the AP.
8. The AP acknowledges the request and assigns an association ID to the client.
9. A four-way handshake takes place between AP and client using the PMK generated.



Knowledge Check

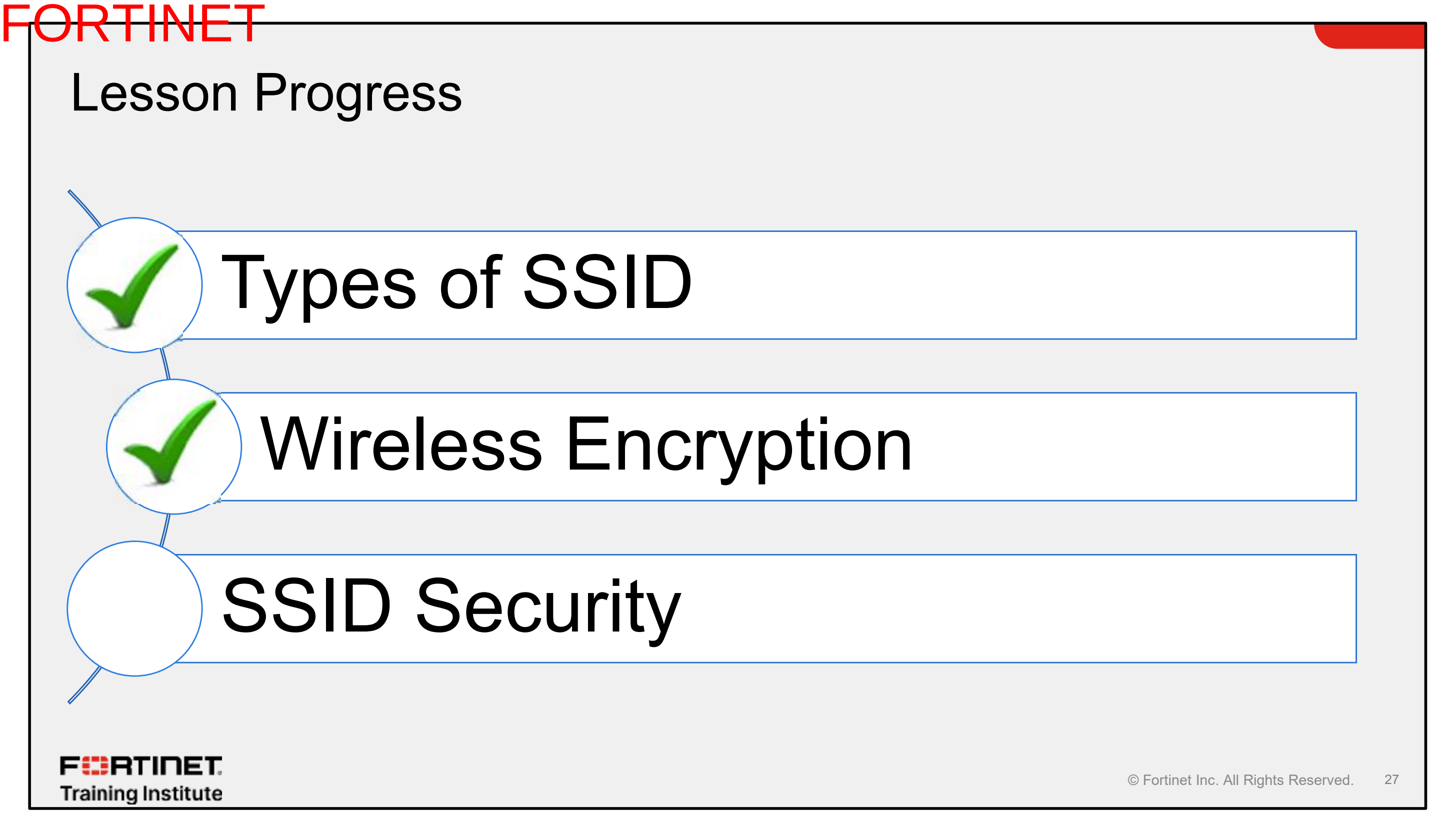
1. Which type of password encryption is used in WPA3 personal?

   A. Pre-shared key

   ✓ B. SAE

FORTINET Training Institute

26

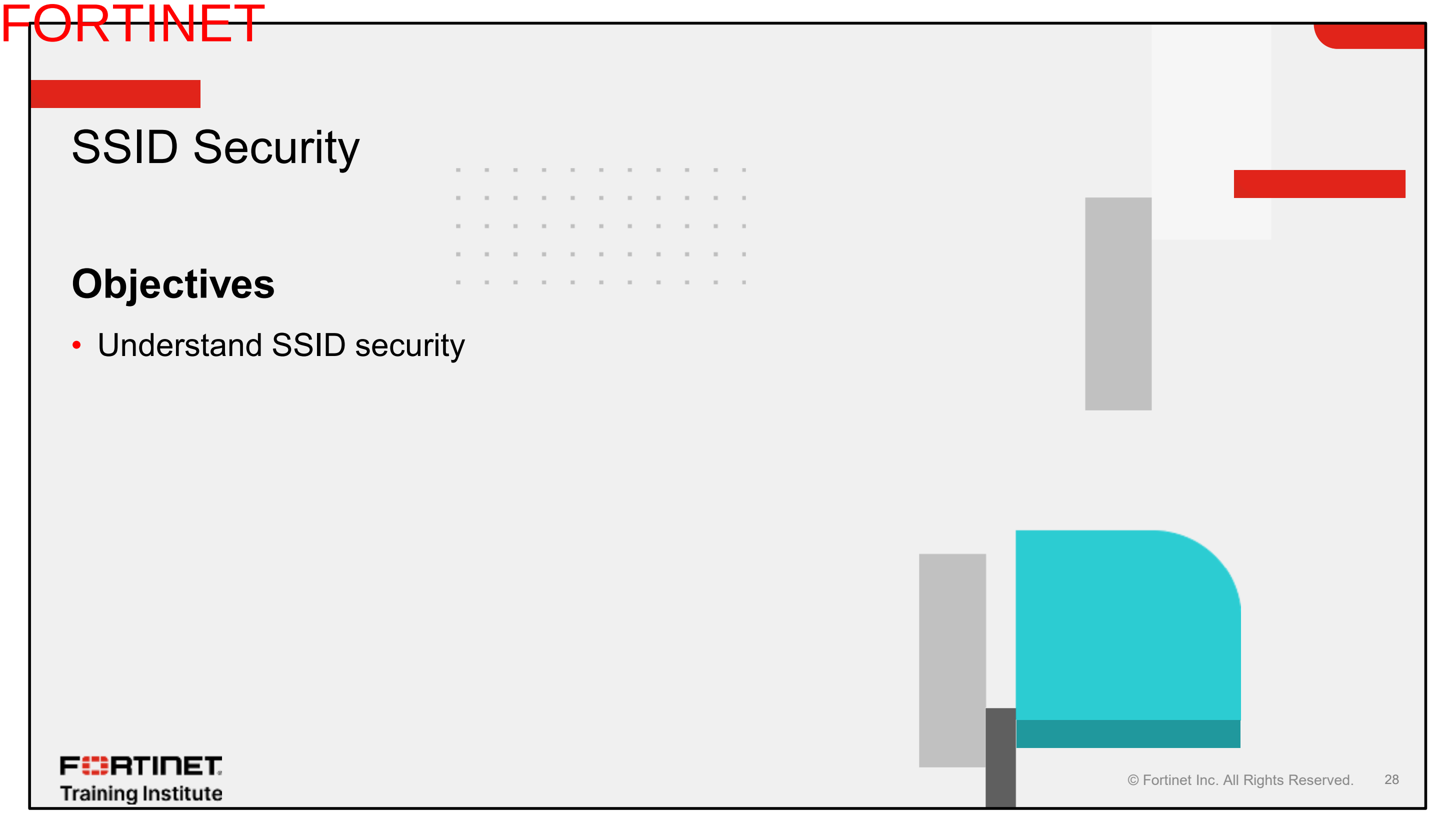


Lesson Progress

- ✓ Types of SSID
- ✓ Wireless Encryption
- SSID Security

27

Good job! You now understand wireless encryption standards. Now, you will learn about SSID security.



SSID Security

Objectives

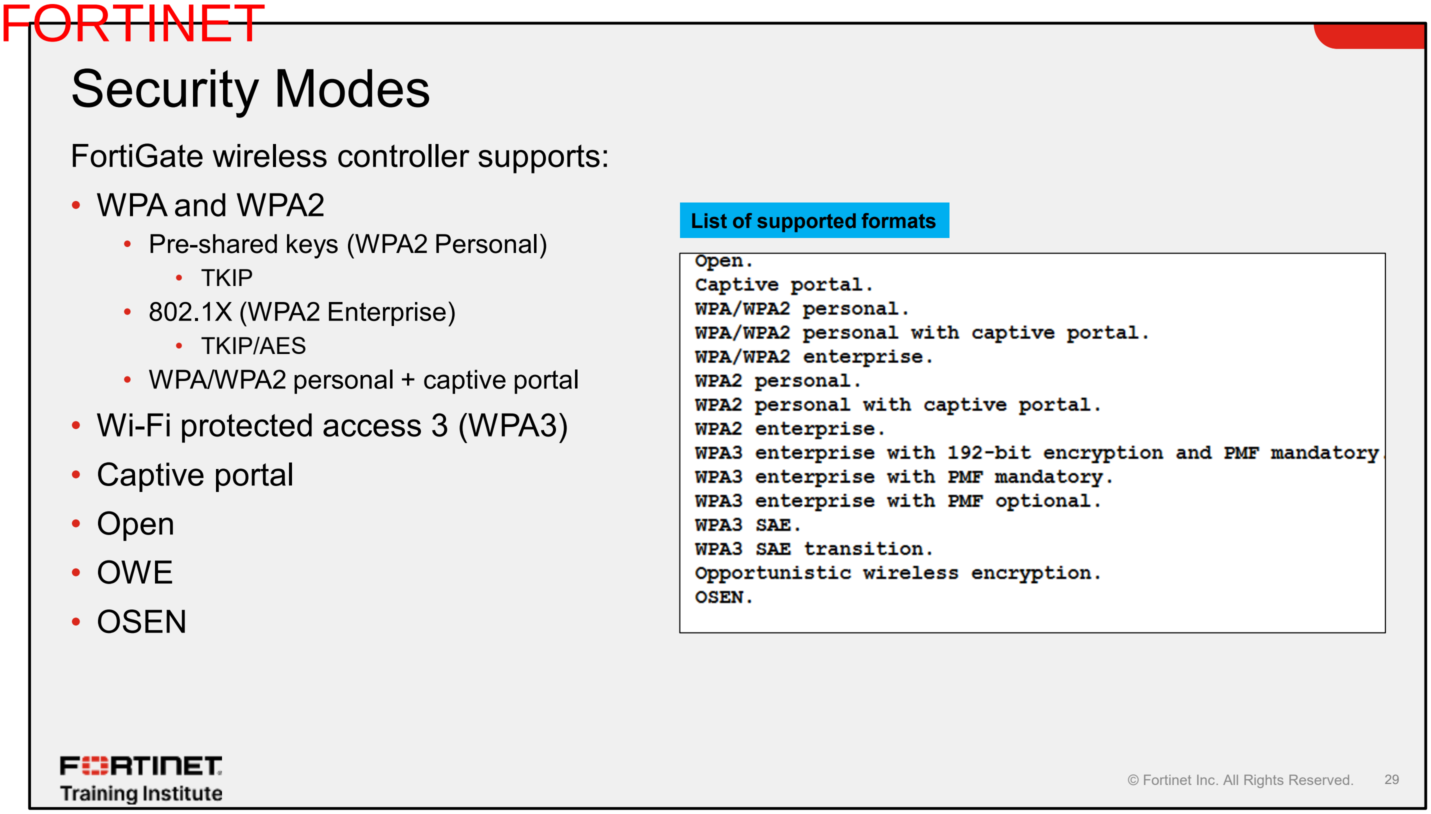
- Understand SSID security

FORTINET Training Institute

28

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding SSID security, you will be able to use it effectively in your network.



Security Modes

FortiGate wireless controller supports:

- WPA and WPA2
  - Pre-shared keys (WPA2 Personal)
    - TKIP
  - 802.1X (WPA2 Enterprise)
    - TKIP/AES
  - WPA/WPA2 personal + captive portal
- Wi-Fi protected access 3 (WPA3)
- Captive portal
- Open
- OWE
- OSEN

List of supported formats

```
Open.
Captive portal.
WPA/WPA2 personal.
WPA/WPA2 personal with captive portal.
WPA/WPA2 enterprise.
WPA2 personal.
WPA2 personal with captive portal.
WPA2 enterprise.
WPA3 enterprise with 192-bit encryption and PMF mandatory.
WPA3 enterprise with PMF mandatory.
WPA3 enterprise with PMF optional.
WPA3 SAE.
WPA3 SAE transition.
Opportunistic wireless encryption.
OSEN.
```

FERTINET
Training Institute

29

Security modes are settings for client authentication and traffic encryption between the wireless client and the AP. Remember, wireless is a shared medium; so, there are even more vectors of attack than for wired connections.

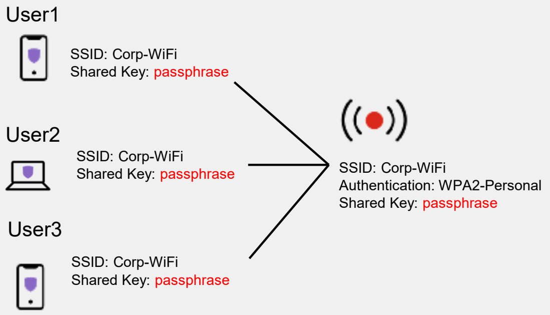
The FortiGate wireless controller supports two user authentication methods:

- Username and password (WPA2 Enterprise, WPA3, or captive portal)
- Pre-shared keys (WPA2 Personal) or SAE in WPA3

Alternatively, if you need to provide guest access without authentication, you can use captive portal as the security mode and disclaimer only as the portal type.

WPA2 Personal

- All users and devices share the same static passphrase
- If a user leaves or a device is lost, for security reasons, the shared key must be changed, and every AP and client device will need to be reconfigured
- Key length and complexity of the passphrase is extremely important from a security point of view

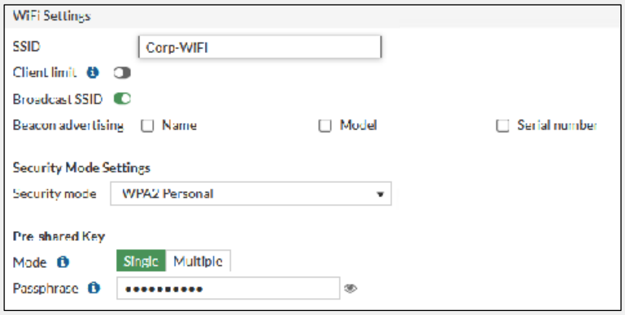

User1
SSID: Corp-WiFi
Shared Key: passphrase

User2
SSID: Corp-WiFi
Shared Key: passphrase

User3
SSID: Corp-WiFi
Shared Key: passphrase

SSID: Corp-WiFi
Authentication: WPA2-Personal
Shared Key: passphrase

WiFi & Switch Controller > SSIDs


WiFi Settings

SSID: Corp-WIFI
Client limit ⓘ ○
Broadcast SSID ●
Beacon advertising ☐ Name ☐ Model ☐ Serial numbe

Security Mode Settings

Security mode: WPA2 Personal

Pre-shared Key

Mode ⓘ: Single | Multiple
Passphrase ⓘ: ••••••••••

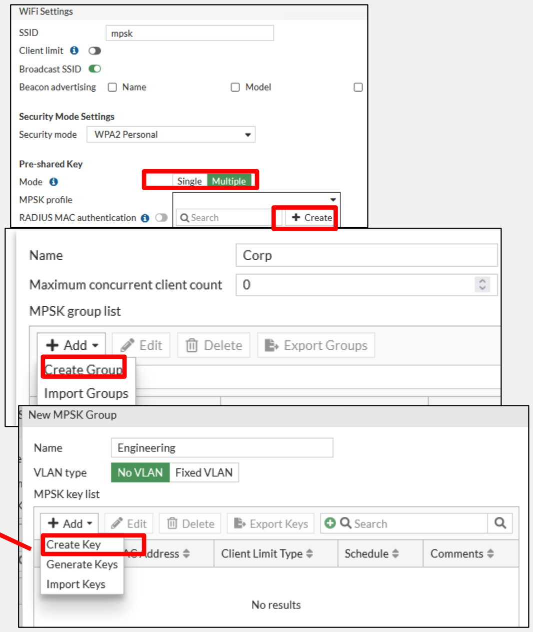
FORTINET Training Institute

WPA2 security with a pre-shared key for authentication is called WPA2 Personal. This mode can work well for one person or a small group of trusted people. But, as the number of users increases, it is difficult to distribute new keys securely and there is increased risk that the key could fall into the wrong hands.

MPSK Profile

- One MPSK profile per SSID
- Multiple MPSK groups can be linked to a MPSK profile
- Each MPSK group contains keys for a single device or group of devices
- VLANs can be assigned based on MPSK group
- Enabling MPSK will discard the single pre-shared key

WiFi & Switch Controller > SSIDs



WiFi Settings

SSID: mpsk

Client limit: off

Broadcast SSID: on

Beacon advertising: □ Name □ Model □

Security Mode Settings

Security mode: WPA2 Personal

Pre-shared Key

Mode: Single [✓ Multiple]

MPSK profile

RADIUS MAC authentication: off

Name: Corp

Maximum concurrent client count: 0

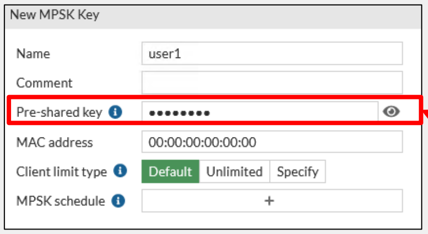
MPSK group list

New MPSK Group

Name: Engineering

VLAN type: [✓ No VLAN] Fixed VLAN

MPSK key list



New MPSK Key

Name: user1

Comment:

Pre-shared key: ••••••••

MAC address: 00:00:00:00:00:00

Client limit type: [✓ Default] Unlimited Specify

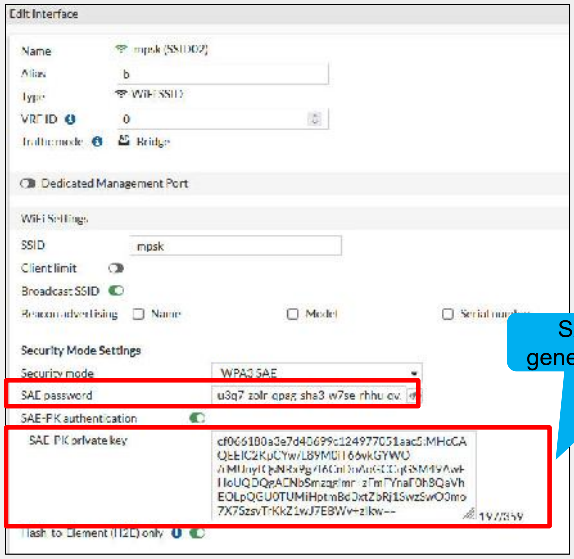
MPSK schedule: +

31

A Fortinet Wi-Fi option when creating a WPA2 Personal network is to use multiple pre-shared keys (MPSK). In this case, not every device uses the same pre-shared key, sharing the keys among groups of devices or even a unique entry for each device. You can batch generate or import MPSK keys, export MPSK keys to a CSV file, dynamically assign VLANs based on used MPSK, and apply an MPSK schedule on the GUI. On the GUI, MPSK key entries are organized in different MPSK groups. An MPSK group can be created manually or imported. The same SSID can have multiple MPSK groups, with each group assigned a specific VLAN. When MPSK is enabled, the previous single passphrase is dropped.

WPA3 SAE

WiFi & Switch Controller > SSIDs



Edit Interface

Name	mpsk (SSID02)
Alias	b
Type	WiFi SSID
VRF ID	0
Traffic mode	Bridge

Dedicated Management Port

WiFi Settings

SSID	mpsk
Client limit	
Broadcast SSID	●
Beacon advertising	□ Name □ Model □ Serial number

Security Mode Settings

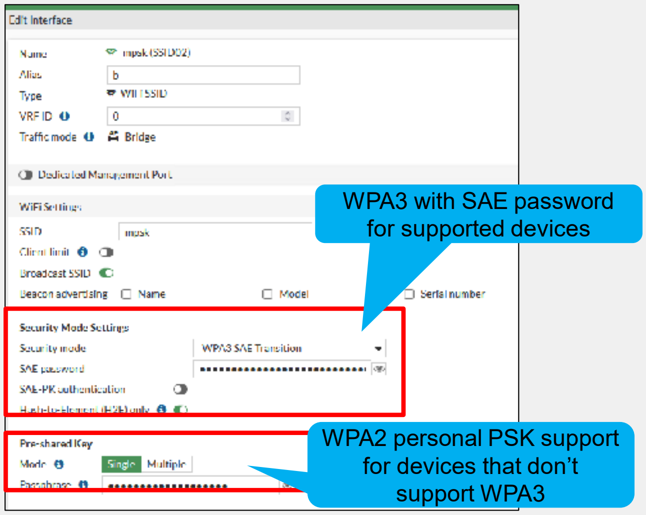
Security mode	WPA3 SAE
SAE password	u3q7 zolr opag sha3 w7se rhhu ov
SAE-PK authentication	●
SAE PK private key	cf066100a3e7d40699c124977051aac5:MHcCA QEEIC2KpCYw/L89MUiT66vkGYWO /iMUnyIQjsNRx9g/16CnI3nAnGCCCpGSM49AwE HoUQDQgAENbSmzqFmr-zFmFYnaF0h8QaVh EOLpQGU0TUMiHptmBdJxtZbRj1SwzSwO3mo 7X7SzsvTrKkZ1wJ7EBWv+zlkw-- 197/359
Hash to Element (H2E) only	●

SAE password and key generated by third-party tools

Like WPA2 personal security, you are required to enter a WPA3 SAE password, while configuring an SSID with security mode WPA3. You can also enable simultaneous authentication of equals public key (SAE-PK authentication). When SAE-PK is enabled, you are required to set an SA-PK private key. You can use third-party tools to generate the private key for encryption. You can enter the PK key and SAE password in the SSID settings. On the client side only, you should enter the SASE password for connectivity. You can also enable **Hash-to-Element (H2E) only**, which provides the cryptographic hash function to ensure a secure key exchange process to establish the Wi-Fi connection.

WPA3 SAE Transition

WiFi & Switch Controller > SSIDs



Edit Interface

Name: mpsk (SSID02)
Alias: b
Type: WiFi SSID
VRF ID: 0
Traffic mode: Bridge

Dedicated Management Port

WiFi Settings

SSID: mpsk
Client limit
Broadcast SSID
Beacon advertising: □ Name □ Model □ Serial number

Security Mode Settings

Security mode: WPA3 SAE Transition
SAE password: ••••••••••••••••••••••••••••
SAE-PK authentication
Hash-to-Element (H2E) only

Pre-shared Key

Mode: Single | Multiple
Passphrase: ••••••••••••••••••••

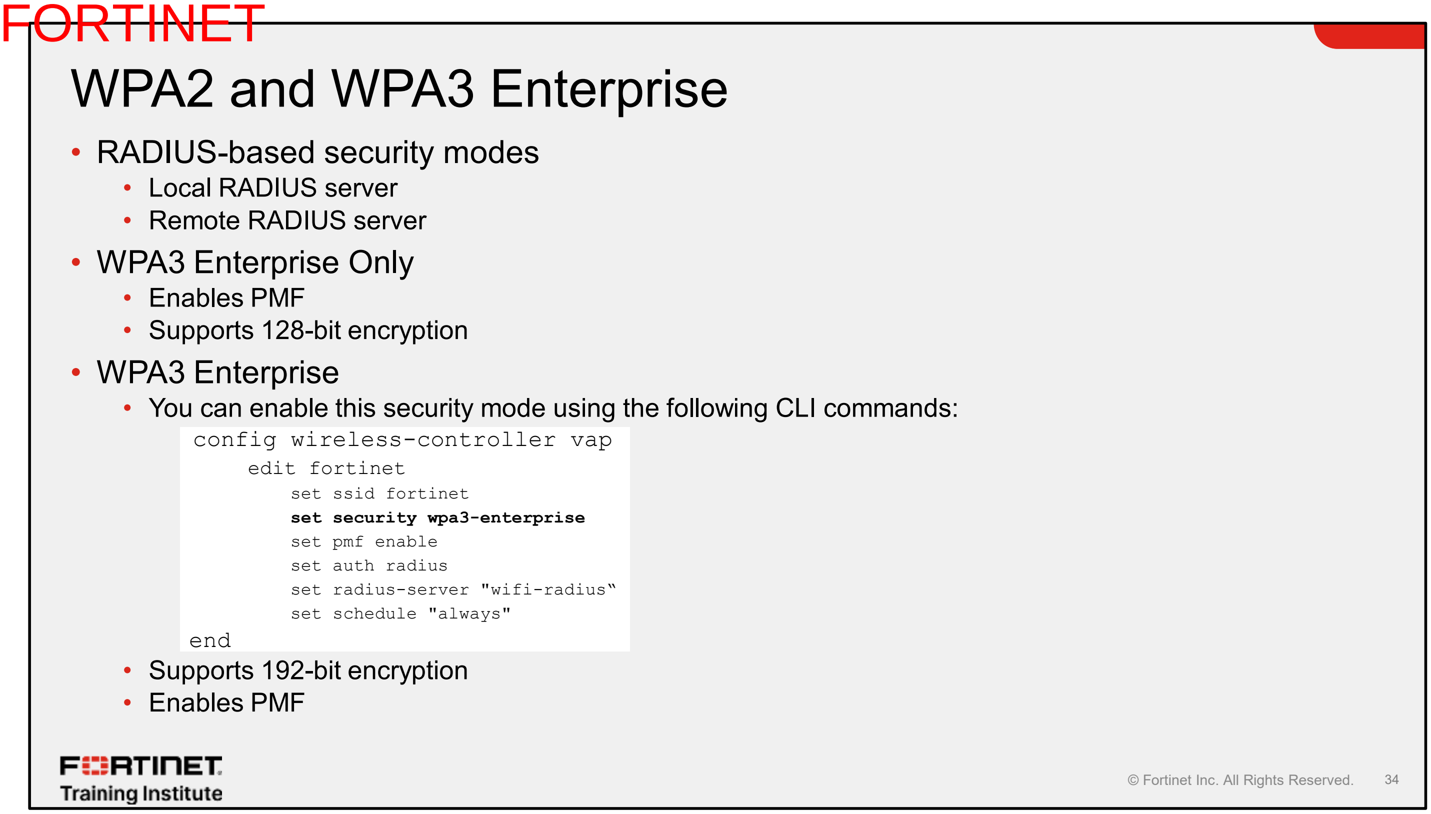
WPA3 with SAE password for supported devices

WPA2 personal PSK support for devices that don’t support WPA3

F::RTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

WPA3 SAE transition security mode is configured when there are devices in the network that are not capable of supporting the latest WPA3 SAE security, it will connect to WPA2 personal instead.



WPA2 and WPA3 Enterprise

- RADIUS-based security modes
  - Local RADIUS server
  - Remote RADIUS server
- WPA3 Enterprise Only
  - Enables PMF
  - Supports 128-bit encryption
- WPA3 Enterprise
  - You can enable this security mode using the following CLI commands:

```
config wireless-controller vap
    edit fortinet
        set ssid fortinet
        set security wpa3-enterprise
        set pmf enable
        set auth radius
        set radius-server "wifi-radius‟
        set schedule "always"
end
```

  - Supports 192-bit encryption
  - Enables PMF

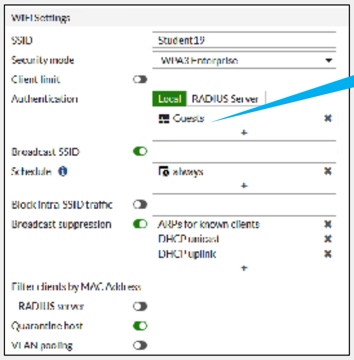
34

WPA2 Enterprise, WPA3 Enterprise Only, and WPA3 Enterprise are RADIUS-based security modes. These are the standards any enterprise class network should be using. If you have a database of users with a RADIUS front end, this is what to use. Encryption and authentication are strongest in an enterprise network. When **WPA3 Enterprise Only** or **WPA3 Enterprise** is configured as the security mode, protected management frames (PMF) are enabled automatically. PMFs are designed to prevent attacks such as disconnect, honeypot, and so on. FortiGate supports two types of RADIUS deployment: local RADIUS server and remote RADIUS server.

802.1X Local Authentication

- Local EAP, FortiGate acts as:
  - Authenticator
  - Authentication server
- Only valid for PEAP
  - Create local user(s), then create a user group to apply on an SSID

WiFi & Switch Controller > SSIDs



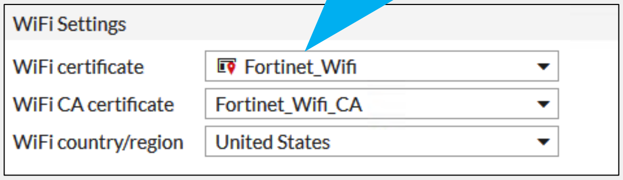
WiFi Settings

SSID		Student19
Security mode		WPA3 Enterprise
Client limit	○	
Authentication		**Local** RADIUS Server
		Guests ✖
Broadcast SSID	●	
Schedule		always ✖
Block intra SSID traffic	○	
Broadcast suppression	●	ARPs for known clients ✖ DHCP unicast ✖ DHCP uplink ✖
Filter clients by MAC Address		
RADIUS server	○	
Quarantine host	●	
VLAN pooling	○	

Select local authentication and select one or more local user groups

By default, factory default certificates are used; however, you can change them to a user-uploaded certificate

System > WiFi Settings



WiFi Settings

WiFi certificate	Fortinet_Wifi
WiFi CA certificate	Fortinet_Wifi_CA
WiFi country/region	United States

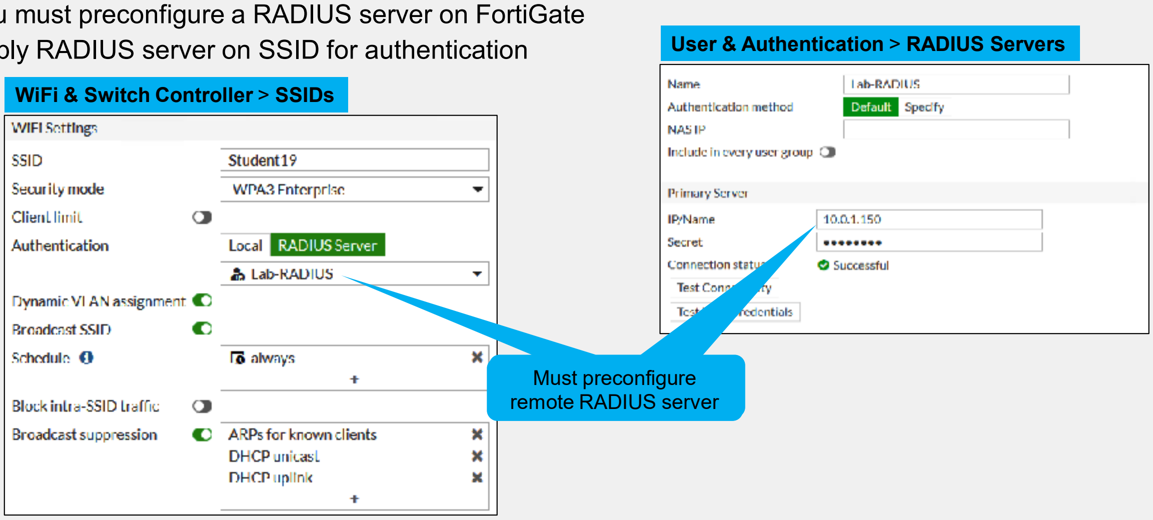
FORTINET Training Institute

35

In 802.1X local authentication mode, FortiGate plays two roles: the authenticator and the authentication server. This mode is supported only in PEAP implementation and requires a local user database. You must apply user accounts to one or more user groups that can then be used within the SSID configuration for authentication.

Remote RADIUS Authentication

- FortiGate forwards the authentication to a remote RADIUS server
  - FortiGate is an authenticator but not an authentication server
  - You must preconfigure a RADIUS server on FortiGate
  - Apply RADIUS server on SSID for authentication



WiFi & Switch Controller > SSIDs

WiFi Settings

SSID	Student19
Security mode	WPA3 Enterprise
Client limit	○
Authentication	Local **RADIUS Server**
	Lab-RADIUS
Dynamic VLAN assignment	●
Broadcast SSID	●
Schedule	always
Block intra-SSID traffic	○
Broadcast suppression	ARPs for known clients DHCP unicast DHCP uplink

User & Authentication > RADIUS Servers

Name	Lab-RADIUS
Authentication method	**Default** Specify
NAS IP	
Include in every user group	○

Primary Server

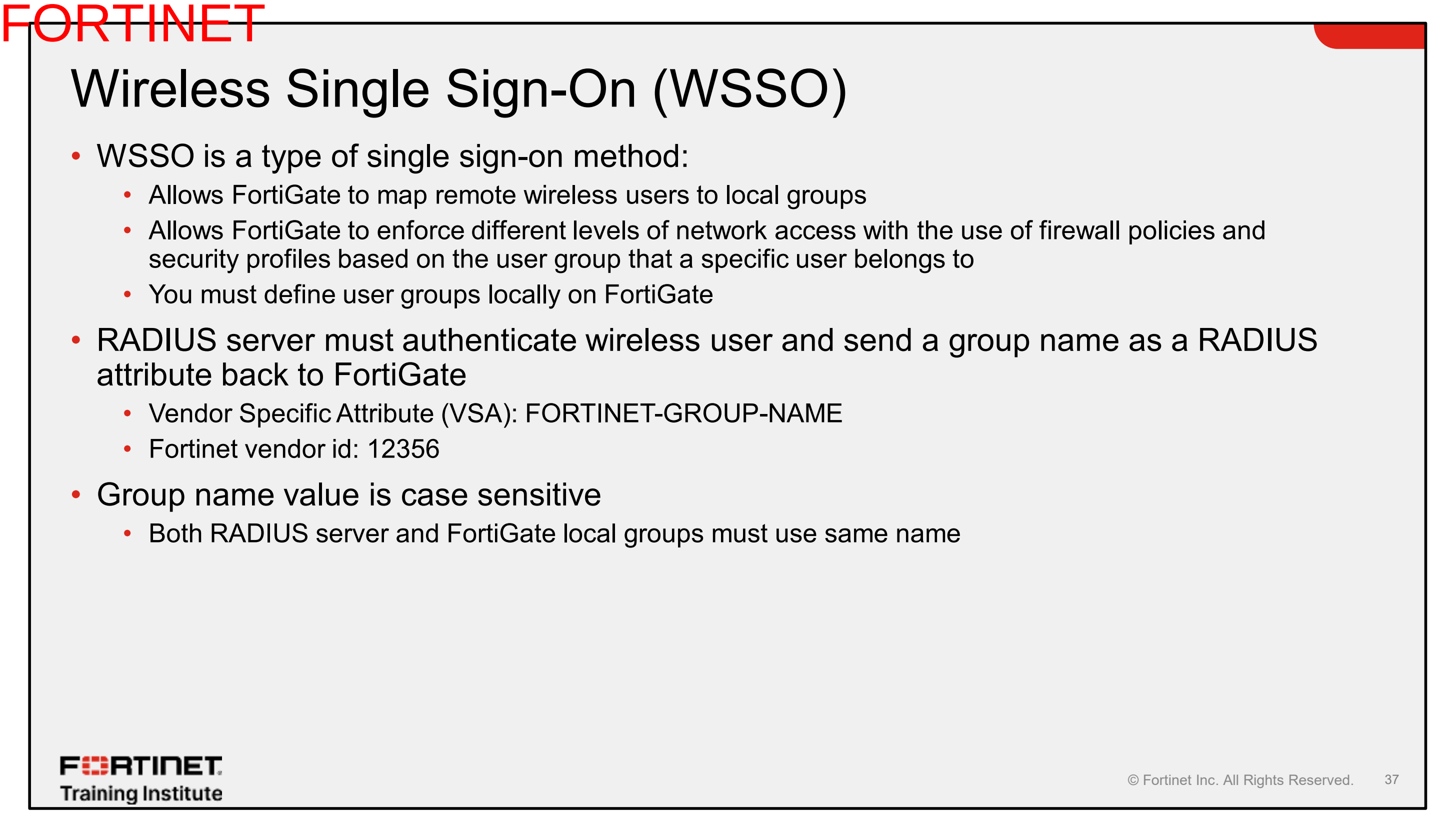
IP/Name	10.0.1.150
Secret	••••••••
Connection status	✓ Successful

Test Connectivity

Test User Credentials

Must preconfigure remote RADIUS server

Another 802.1X use case is to configure and use a remote RADIUS server on FortiGate. In this implementation, FortiGate acts as an authenticator only and forwards all authentication requests to the defined RADIUS server. Remote RADIUS server configuration is required for this mode. After you have a working RADIUS server configuration, you can apply the RADIUS server on an SSID for authentication.



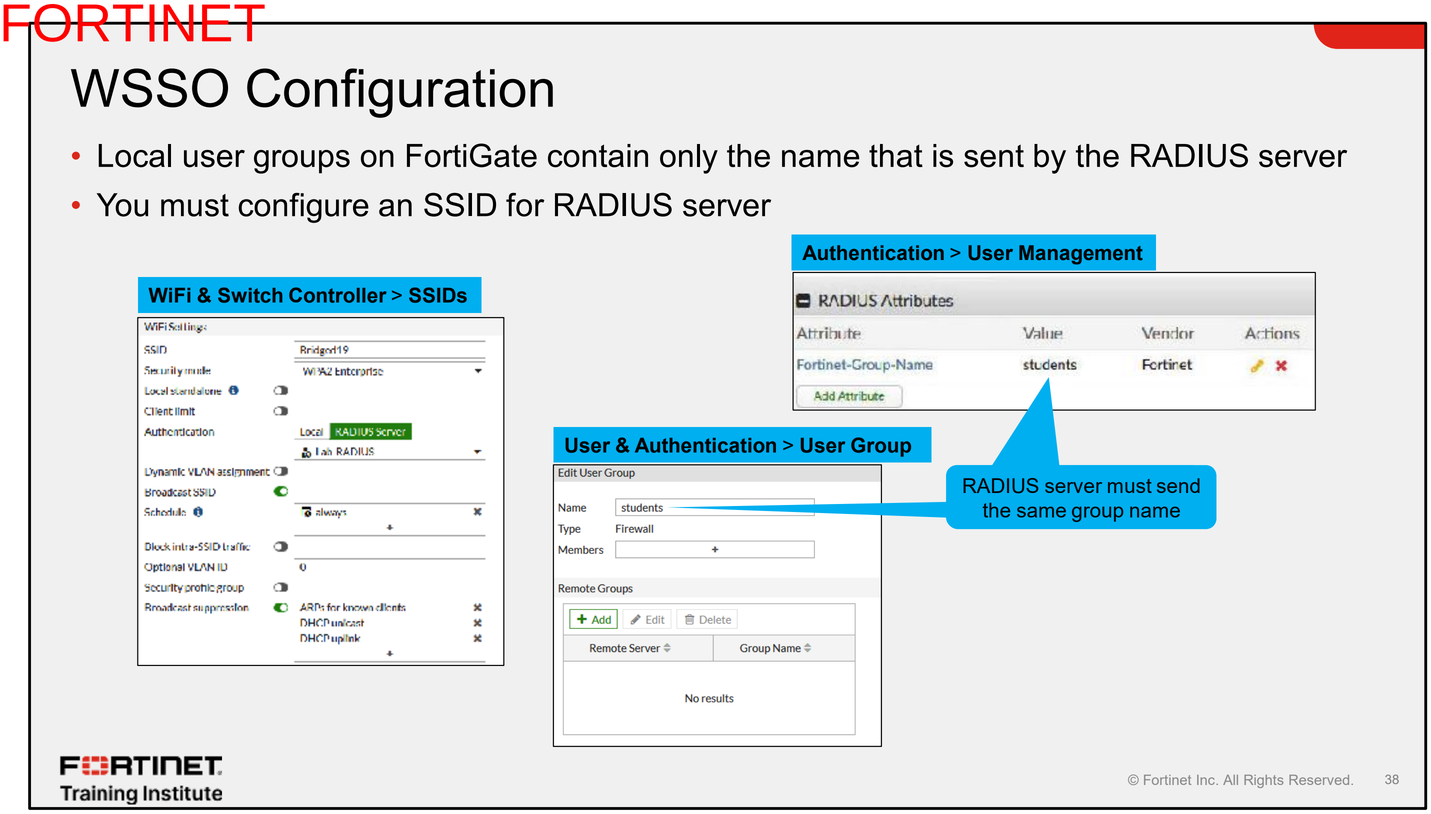
Wireless Single Sign-On (WSSO)

- WSSO is a type of single sign-on method:
  - Allows FortiGate to map remote wireless users to local groups
  - Allows FortiGate to enforce different levels of network access with the use of firewall policies and security profiles based on the user group that a specific user belongs to
  - You must define user groups locally on FortiGate
- RADIUS server must authenticate wireless user and send a group name as a RADIUS attribute back to FortiGate
  - Vendor Specific Attribute (VSA): FORTINET-GROUP-NAME
  - Fortinet vendor id: 12356
- Group name value is case sensitive
  - Both RADIUS server and FortiGate local groups must use same name

37

FortiGate uses WSSO to dynamically map remote RADIUS users to locally defined user groups. This allows FortiGate to use local user groups to apply different levels of network access, and enforce security profiles to the wireless users based on the user group they belong to. You must define user groups with the same name as that sent by the RADIUS server locally on FortiGate. A RADIUS server must authenticate the wireless user and send a group name as a RADIUS attribute back to FortiGate. The server must use the Fortinet-Group-Name attribute when it sends the group name is sent back to FortiGate.

Note that the group name is case sensitive and must match the attribute that by the RADIUS server sends back.



WSSO Configuration

- Local user groups on FortiGate contain only the name that is sent by the RADIUS server
- You must configure an SSID for RADIUS server

WiFi & Switch Controller > SSIDs

WiFi Settings

SSID	Bridged19
Security mode	WPA2 Enterprise
Local standalone	○
Client limit	○
Authentication	Local [✓ RADIUS Server] Lab RADIUS
Dynamic VLAN assignment	○
Broadcast SSID	●
Schedule	always
Block intra-SSID traffic	○
Optional VLAN ID	0
Security profile group	○
Broadcast suppression	● ARPs for known clients DHCP unicast DHCP uplink

Authentication > User Management

RADIUS Attributes

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	students	Fortinet	

Add Attribute

User & Authentication > User Group

Edit User Group

Name	students
Type	Firewall
Members	

Remote Groups

Add Edit Delete

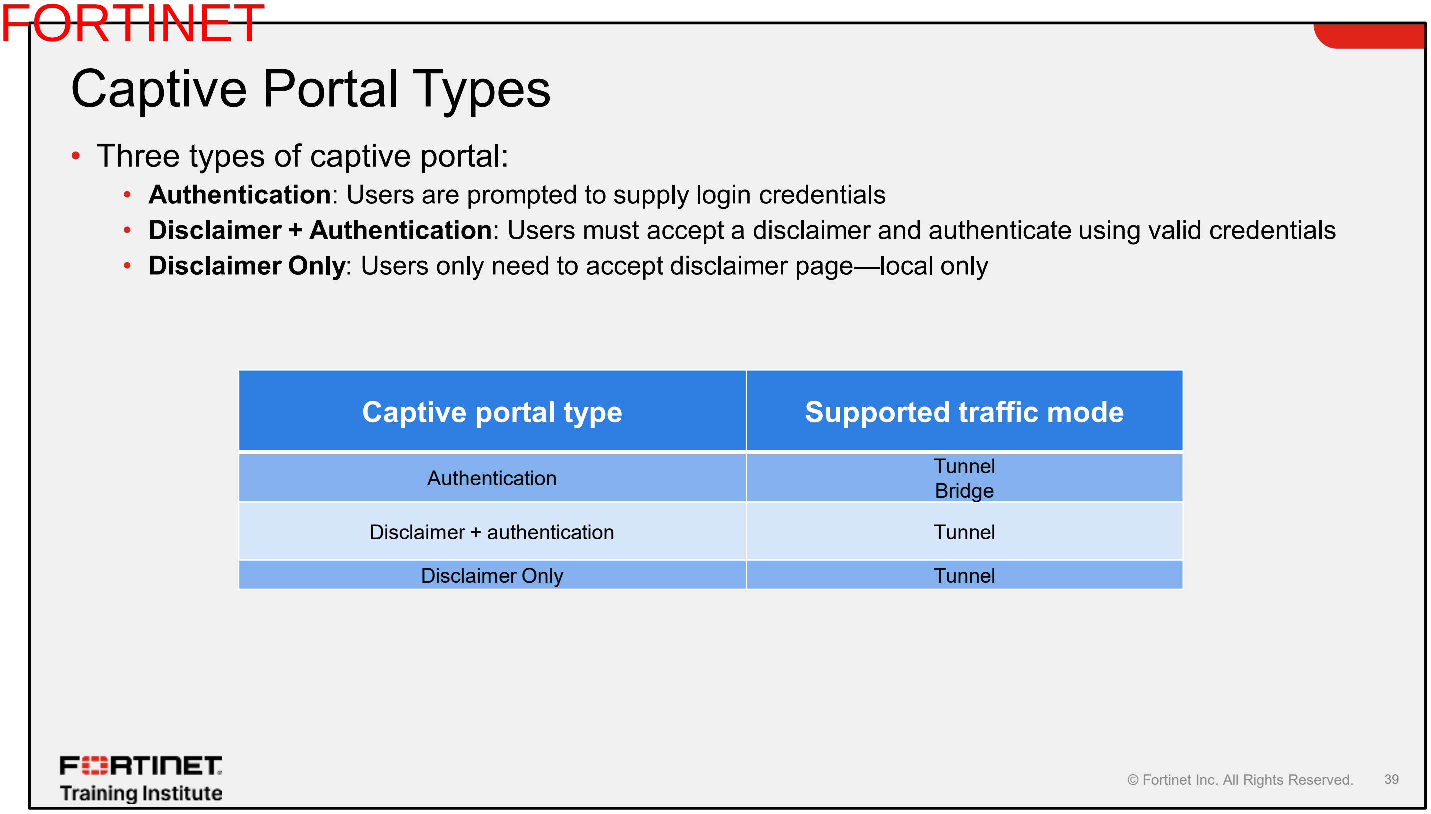
Remote Server	Group Name
No results	

RADIUS server must send the same group name

Training Institute

© Fortinet Inc. All Rights Reserved. 38

To use the WSSO method, you must first create one or more local user groups on FortiGate. Configure the RADIUS server to send back the Fortinet-Group-Name attribute after successfully authenticating a user. Make sure that the local user group name and RADIUS attribute sent by the RADIUS server match.



Captive Portal Types

- Three types of captive portal:
  - **Authentication**: Users are prompted to supply login credentials
  - **Disclaimer + Authentication**: Users must accept a disclaimer and authenticate using valid credentials
  - **Disclaimer Only**: Users only need to accept disclaimer page—local only

Captive portal type	Supported traffic mode
Authentication	Tunnel Bridge
Disclaimer + authentication	Tunnel
Disclaimer Only	Tunnel

Training Institute

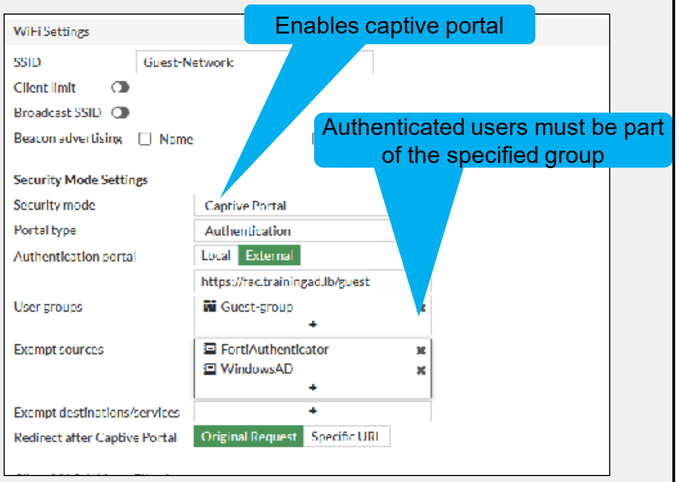
There are three types of captive portals that you can enable on an interface: authentication, disclaimer with authentication, and disclaimer only.

- **Authentication:** Requests that users authenticate before they are allowed access to the network.
- **Disclaimer with Authentication:** Presents users with a disclaimer page and an authentication page. The user must accept a disclaimer and authenticate successfully in order to get network access.
- **Disclaimer Only:** Presents users with a disclaimer page. In this case, users do not have to authenticate using a username and password. They will be allowed to access the network after they accept a disclaimer page.

Captive Portal Types (Contd)

- Authentication portal types:
  - **Local**: FortiGate presents the user with a login page and processes authentication requests
  - **External**: FortiGate redirect the users to an external URL. The external captive portal server is responsible for presenting the user with a login page and validating the authentication.

WiFi & Switch Controller > SSIDs



WiFi Settings

SSID: Guest-Network

Client limit

Broadcast SSID

Beacon advertising □ Name

Security Mode Settings

Security mode: Captive Portal

Portal type: Authentication

Authentication portal: Local [✓ External]

https://fac.trainingad.lb/guest

User groups: Guest-group

Exempt sources: FortiAuthenticator, WindowsAD

Exempt destinations/services

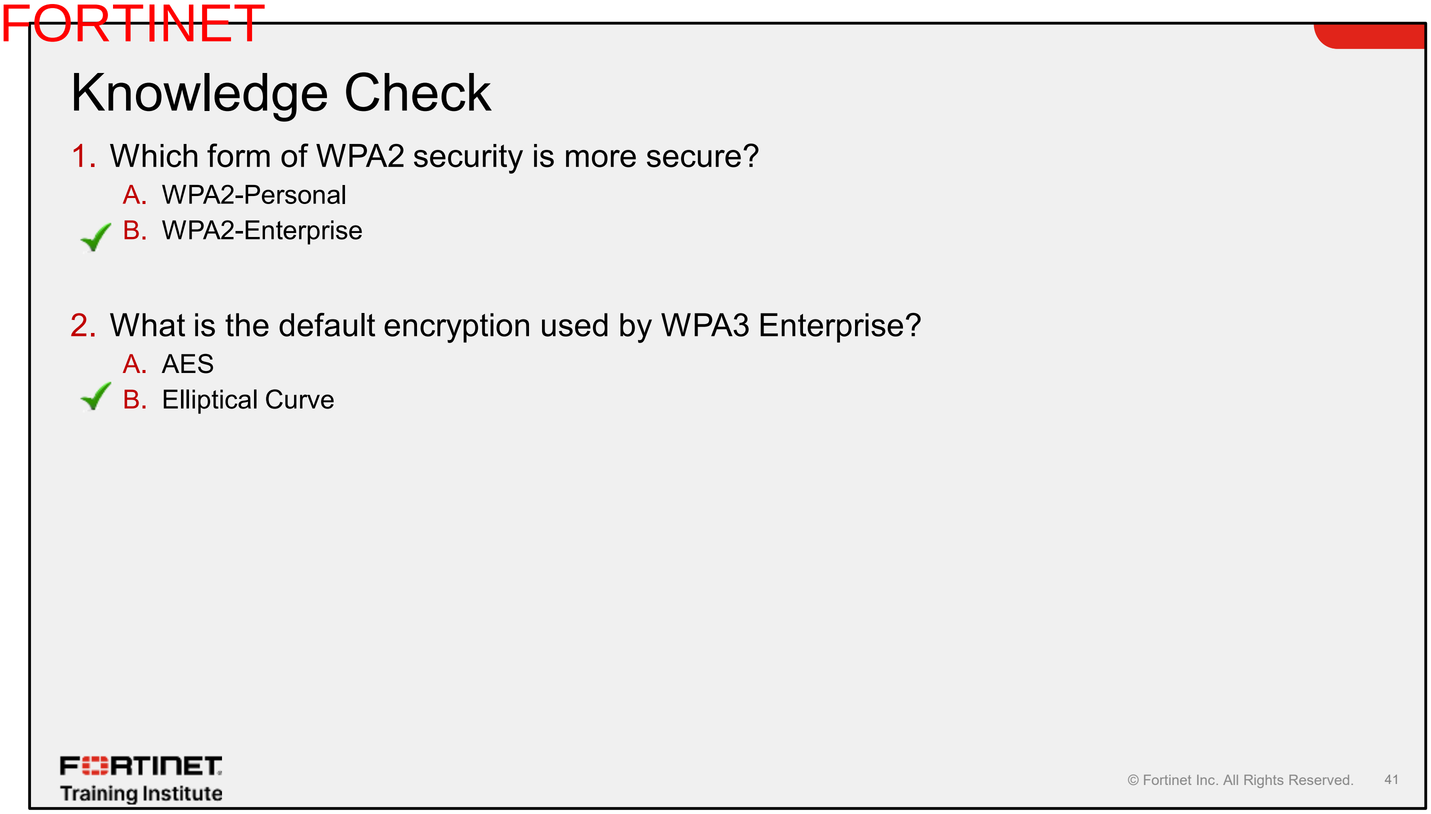
Redirect after Captive Portal: [✓ Original Request] Specific URL

Enables captive portal

Authenticated users must be part of the specified group

After you select **Authentication** for the **Portal Type** field, you can select **Local** or **External** for the **Authentication Portal**. Setting **Authentication Portal** to **Local** uses the FortiGate built-in portal page. All the portal configurations, including the web page that is presented to users as a landing page, are hosted on FortiGate.

For external captive portals, you can select **External** for the **Authentication Type** and enter the FQDN or IP of the external captive portal server. In this case, FortiGate redirects the users to the specified server address. After the user meets the requirements of the external captive portal server, FortiGate allows user access based on the firewall policy configurations.

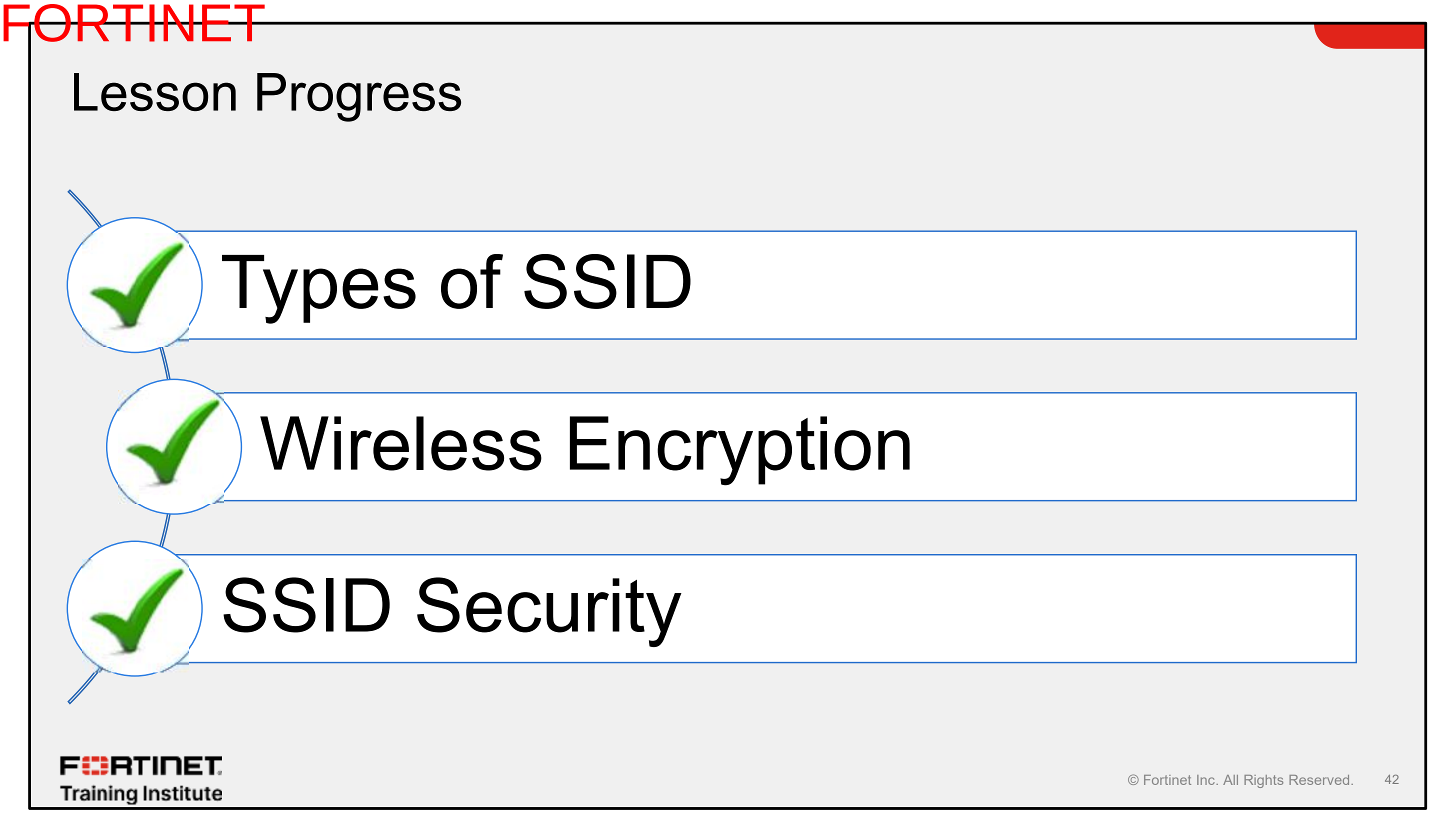


Knowledge Check

1. Which form of WPA2 security is more secure?
   - A. WPA2-Personal
   - ✓ B. WPA2-Enterprise

2. What is the default encryption used by WPA3 Enterprise?
   - A. AES
   - ✓ B. Elliptical Curve

41



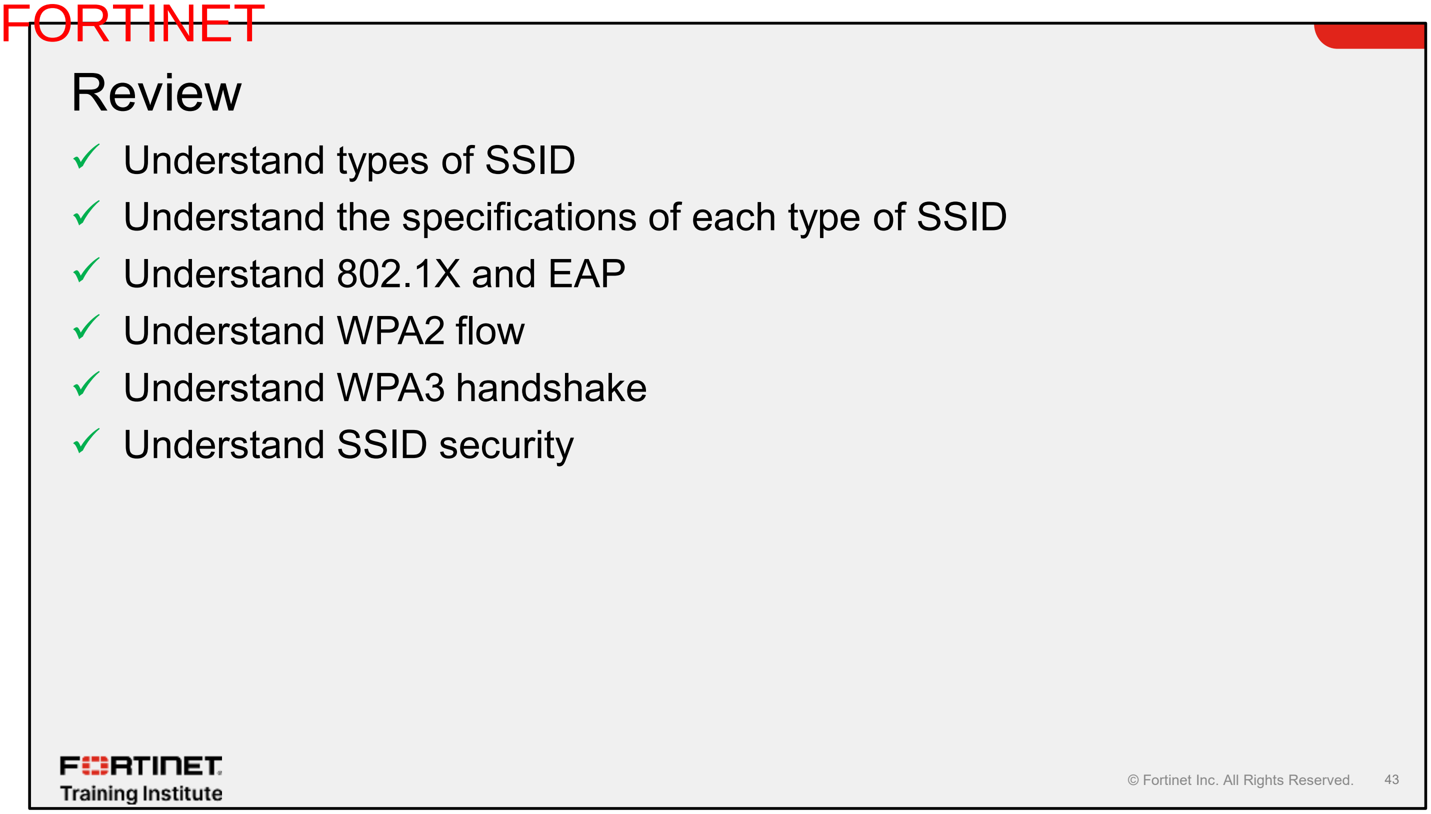
Lesson Progress

- ✓ Types of SSID
- ✓ Wireless Encryption
- ✓ SSID Security

42

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



Review

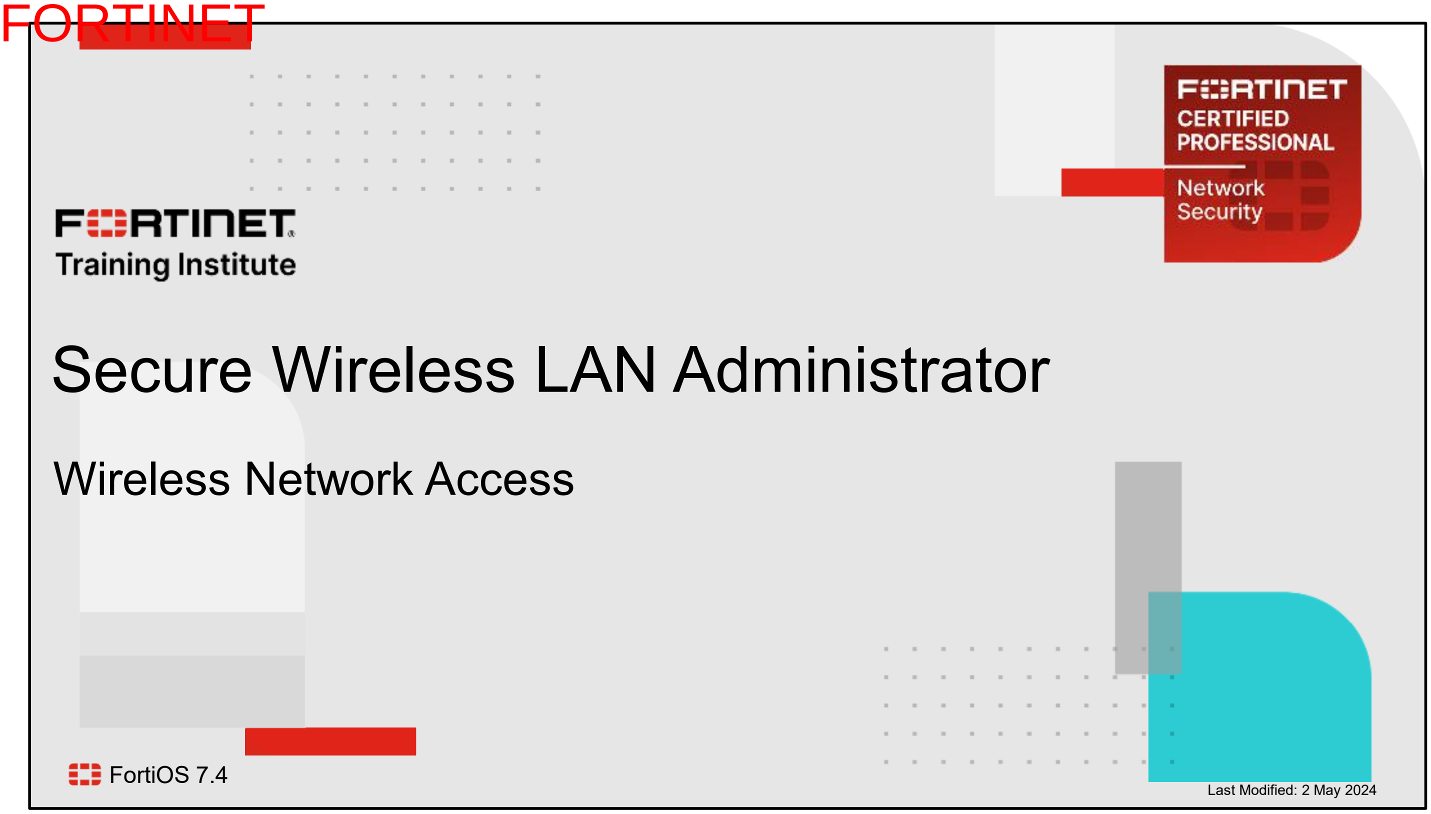
- ✓ Understand types of SSID
- ✓ Understand the specifications of each type of SSID
- ✓ Understand 802.1X and EAP
- ✓ Understand WPA2 flow
- ✓ Understand WPA3 handshake
- ✓ Understand SSID security

FORTINET Training Institute

43

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to apply wireless security using the FortiOS wireless controller.



FORTINET
Training Institute

FORTINET CERTIFIED PROFESSIONAL
Network Security

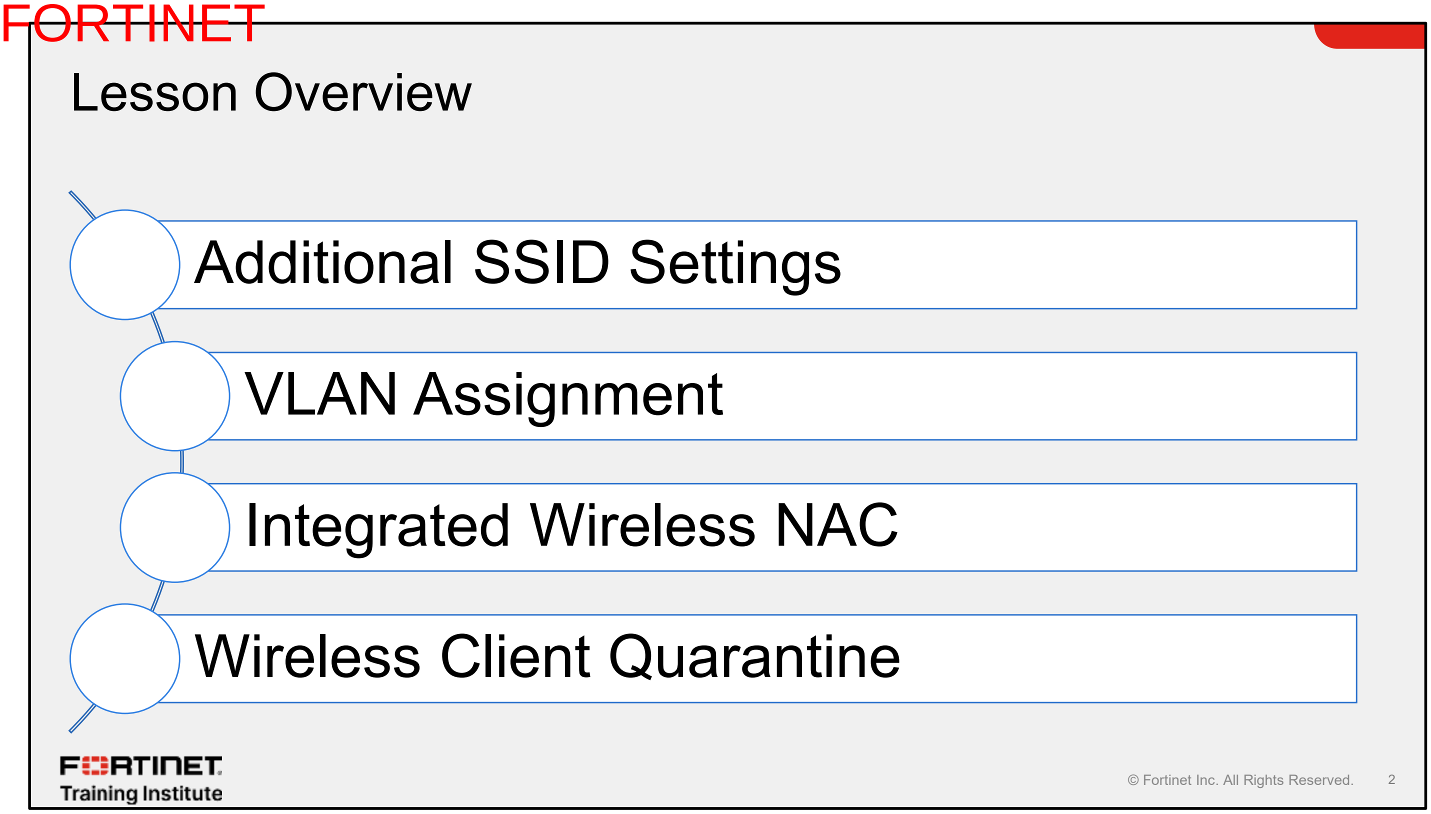
Secure Wireless LAN Administrator

Wireless Network Access

FortiOS 7.4

Last Modified: 2 May 2024

In this lesson, you will learn about wireless network access settings and options using the FortiOS integrated wireless controller.

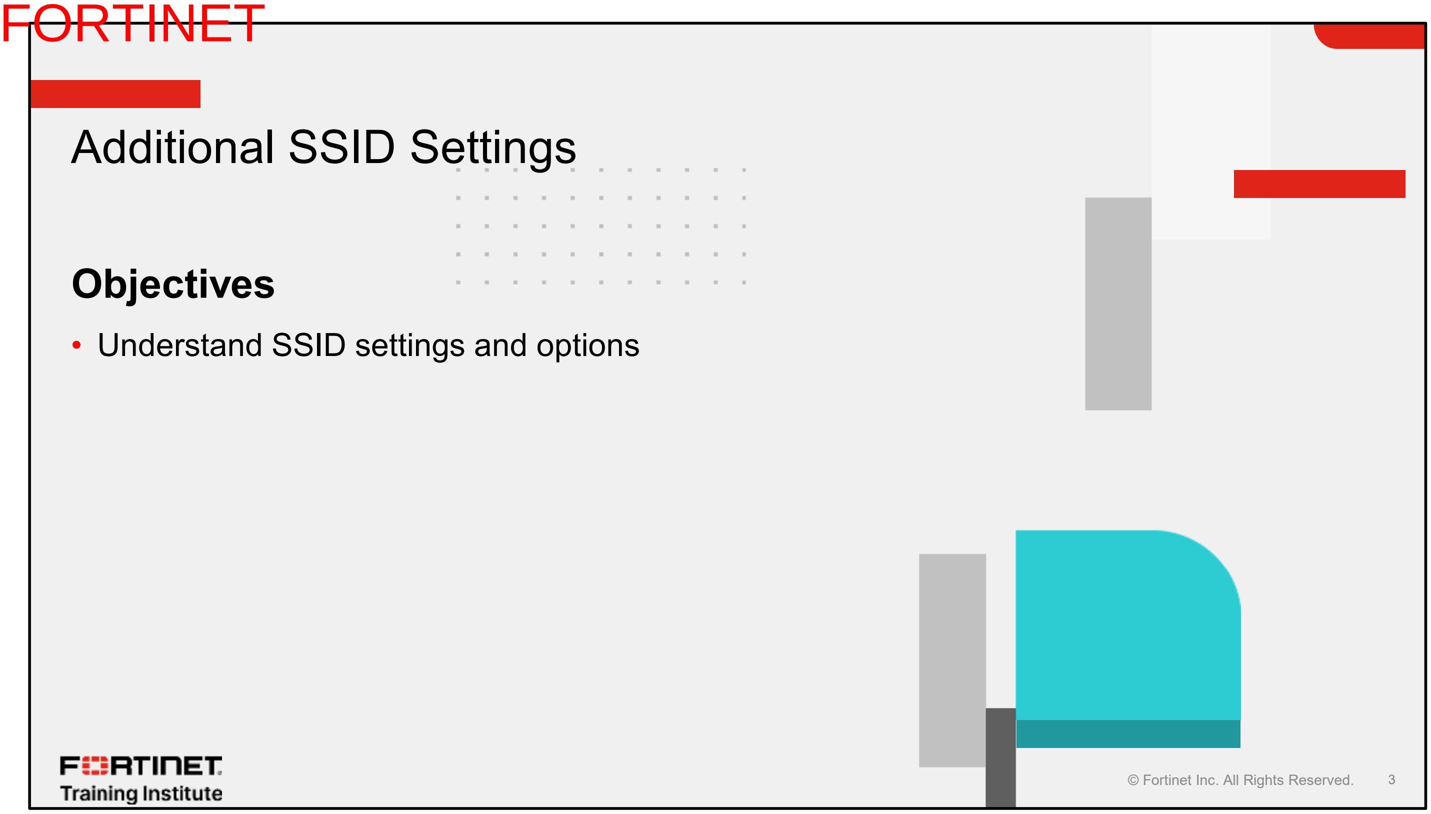


Lesson Overview

- Additional SSID Settings
- VLAN Assignment
- Integrated Wireless NAC
- Wireless Client Quarantine

FORTINET Training Institute

In this lesson, you will learn about the topics shown on this slide.



Additional SSID Settings

Objectives

- Understand SSID settings and options

Training Institute

3

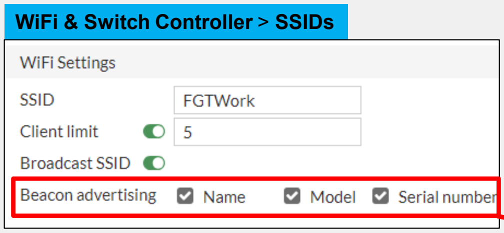
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding the additional SSID settings, you will be able to improve the wireless network options.

SSID Options

- Set maximum number of clients that can connect to an SSID
- Disable broadcast of SSID; set to broadcast by default
- Vendor-specific element over beacon frames containing information about the FortiAP name, model and serial number

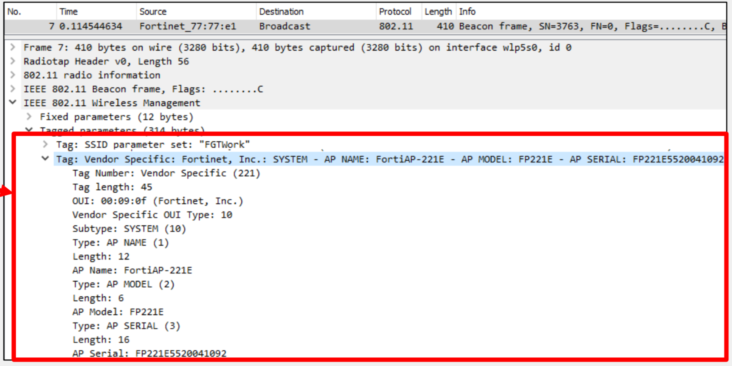
WiFi & Switch Controller > SSIDs



WiFi Settings

SSID	FGTWork
Client limit	● 5
Broadcast SSID	●
Beacon advertising	☑ Name ☑ Model ☑ Serial number

Packet capture of beacon frames



```
No.     Time          Source             Destination    Protocol  Length  Info
      7 0.114544634   Fortinet_77:77:e1  Broadcast      802.11       410  Beacon frame, SN=3763, FN=0, Flags=........C, B

> Frame 7: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits) on interface wlp5s0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (314 bytes)
    > Tag: SSID parameter set: "FGTWork"
    v Tag: Vendor Specific: Fortinet, Inc.: SYSTEM - AP NAME: FortiAP-221E - AP MODEL: FP221E - AP SERIAL: FP221E5520041092
        Tag Number: Vendor Specific (221)
        Tag length: 45
        OUI: 00:09:0f (Fortinet, Inc.)
        Vendor Specific OUI Type: 10
        Subtype: SYSTEM (10)
        Type: AP NAME (1)
        Length: 12
        AP Name: FortiAP-221E
        Type: AP MODEL (2)
        Length: 6
        AP Model: FP221E
        Type: AP SERIAL (3)
        Length: 16
        AP Serial: FP221E5520041092
```

FORTINET Training Institute

4

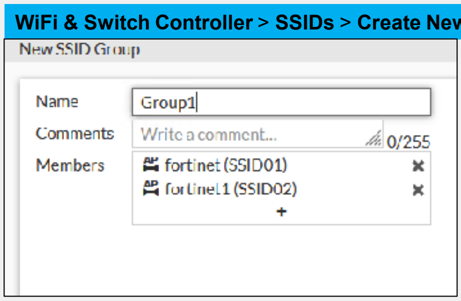
To have more control over your wireless environment, you can set a maximum number of clients that can connect to a given SSID. You can also choose to stop broadcasting the SSID so that only users who know the name of the SSID can connect to the SSID. Disabling the broadcast of the SSID increases security and can reduce management traffic.

Advertising the vendor-specific element over beacon frames containing information about the FortiAP name, model, and serial number allows wireless administrator performing site surveys to easily determine the coverage area of a FortiAP. The administrator can slowly move away from a FortiAP while continuously sniffing the beacons to determine if they can still hear from the FortiAP. Another use case is to ensure that the FortiAP can be correctly identified during post-implementation wireless site surveys. This makes troubleshooting and design improvements much easier.

SSID Groups

- Optionally, you can define SSID groups
- SSIDs are members of SSID groups
- You can specify an SSID group the same way you specify an SSID in a FortiAP profile

WiFi & Switch Controller > SSIDs > Create New > SSID Group



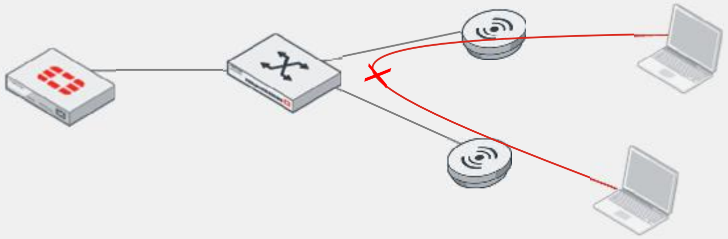
New SSID Group

Name: Group1
Comments: Write a comment... 0/255
Members: fortinet (SSID01)
fortinet1 (SSID02)
+

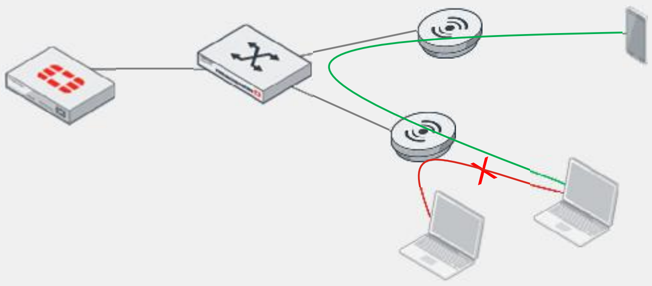
You can use SSID groups to simplify the management of multiple SSIDs. You can specify an SSID group the same way that you specify an SSID in a FortiAP profile.

Block Intra-SSID Traffic

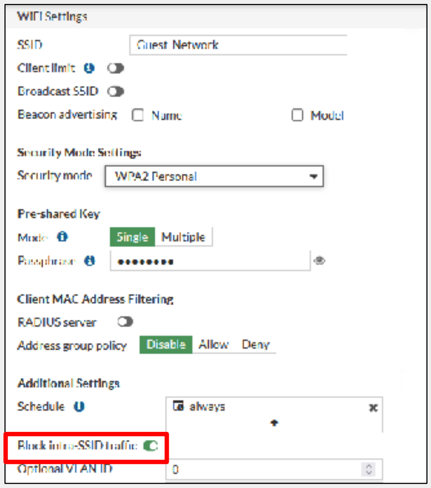
- In tunneled mode SSID, all traffic between wireless clients is blocked



- In bridge mode, traffic block works only per AP



WiFi & Switch Controller > SSIDs



WiFi Settings

SSID: Guest Network

Client limit ○

Broadcast SSID ○

Beacon advertising □ Name □ Model

Security Mode Settings

Security mode: WPA2 Personal

Pre-shared Key

Mode: [✓ Single] Multiple

Passphrase: ••••••••

Client MAC Address Filtering

RADIUS server ○

Address group policy: [✓ Disable] Allow Deny

Additional Settings

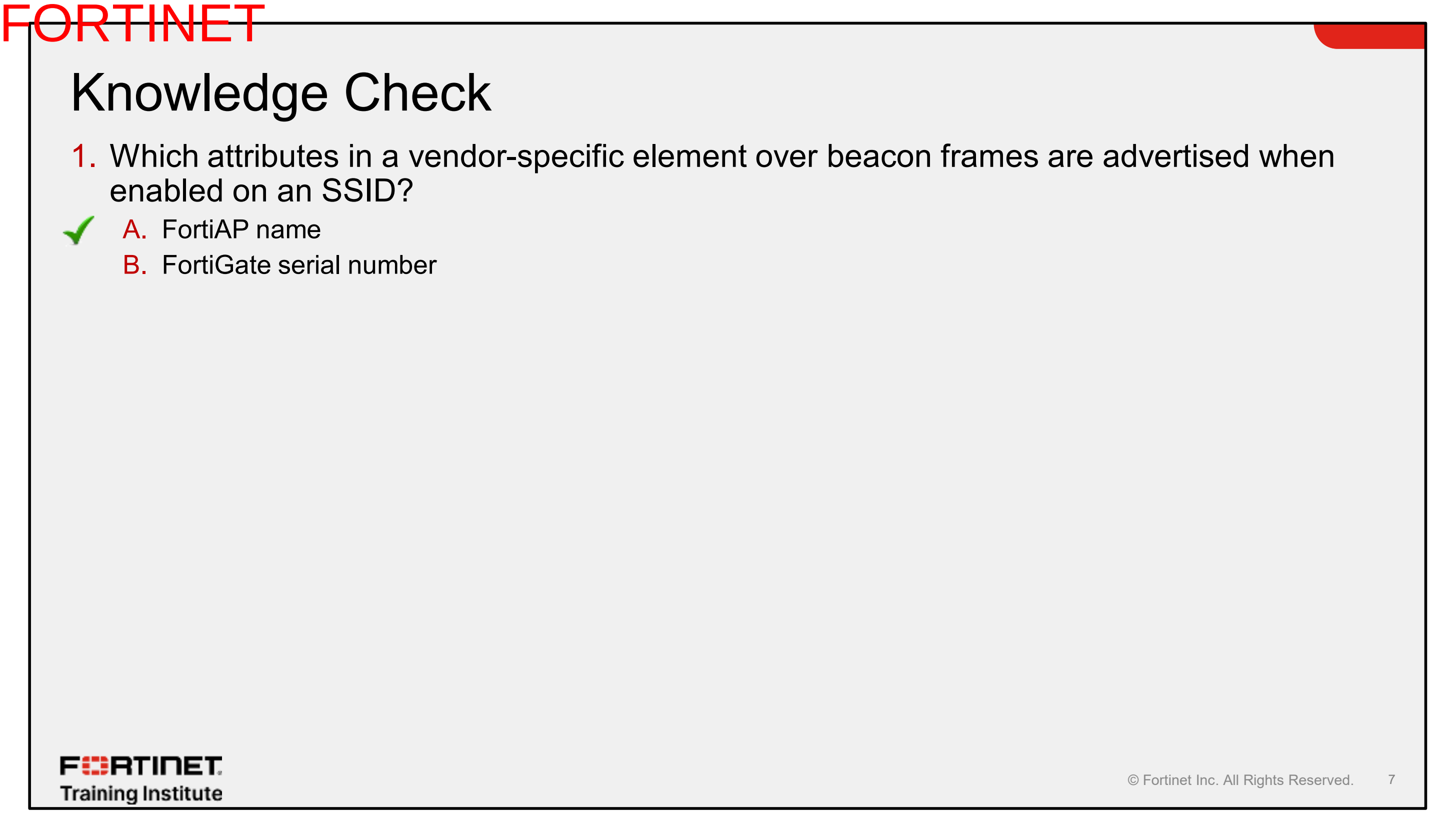
Schedule: always

Block intra-SSID traffic ●

Optional VLAN ID: 0

The **Block intra-SSID traffic** option yields different results based on the SSID mode it is enabled on. In tunneled mode, all traffic between the SSIDs is blocked. Clients can access resources based on firewall policies but are unable to communicate with other clients that are connected to the same SSID.

In bridge mode, when the **Block intra-SSID traffic** option is enabled, traffic to and from wireless clients connected to the same SSID *and* access point (AP) is blocked. However, wireless clients connected to the same SSID, but on a different AP, are still able to communicate with each other. To prevent this communication, you must have private VLAN enabled, if APs are connected to a FortiSwitch device.



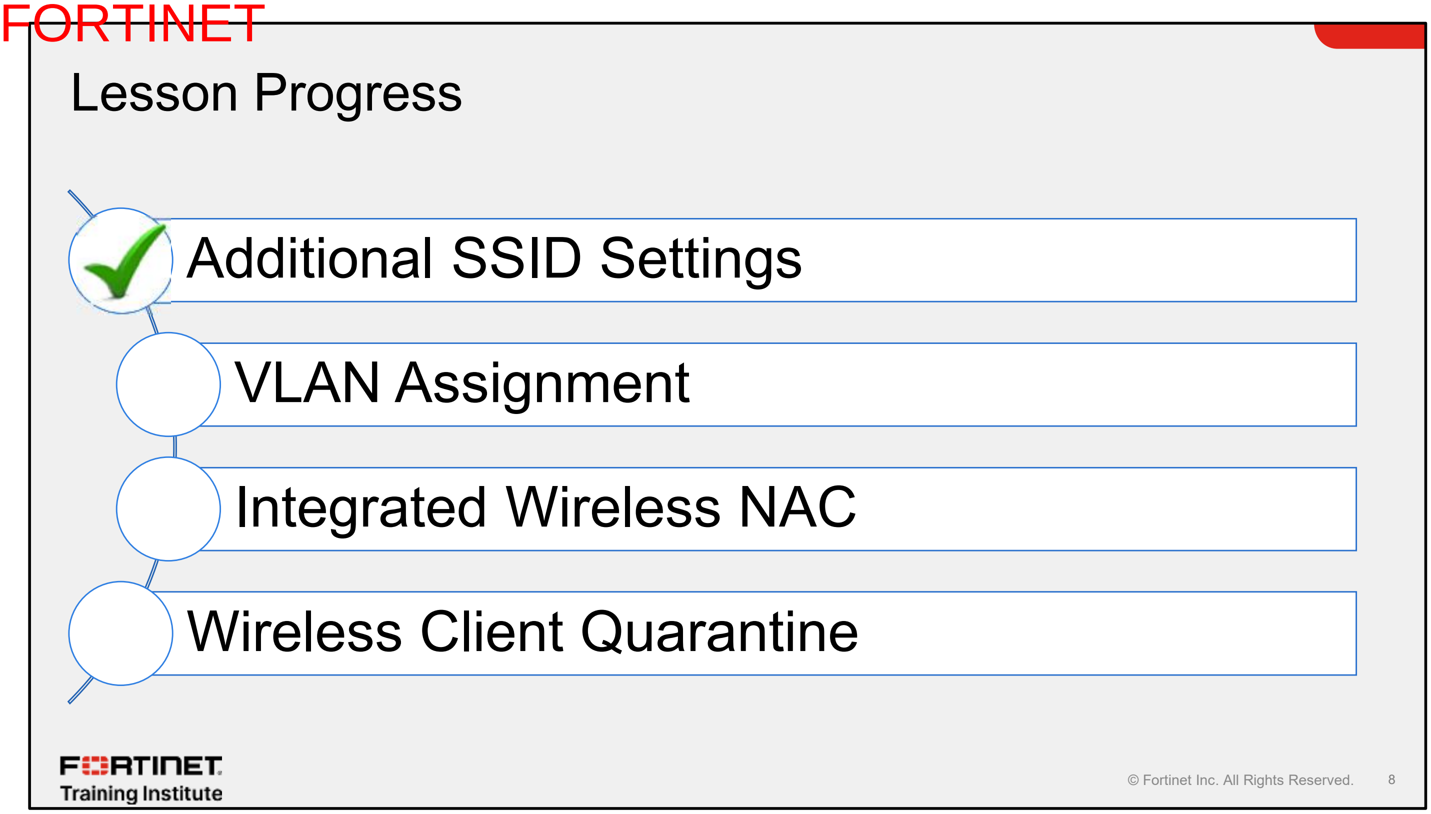
Knowledge Check

1. Which attributes in a vendor-specific element over beacon frames are advertised when enabled on an SSID?

✓ A. FortiAP name

B. FortiGate serial number

FORTINET
Training Institute
© Fortinet Inc. All Rights Reserved.
7



Lesson Progress

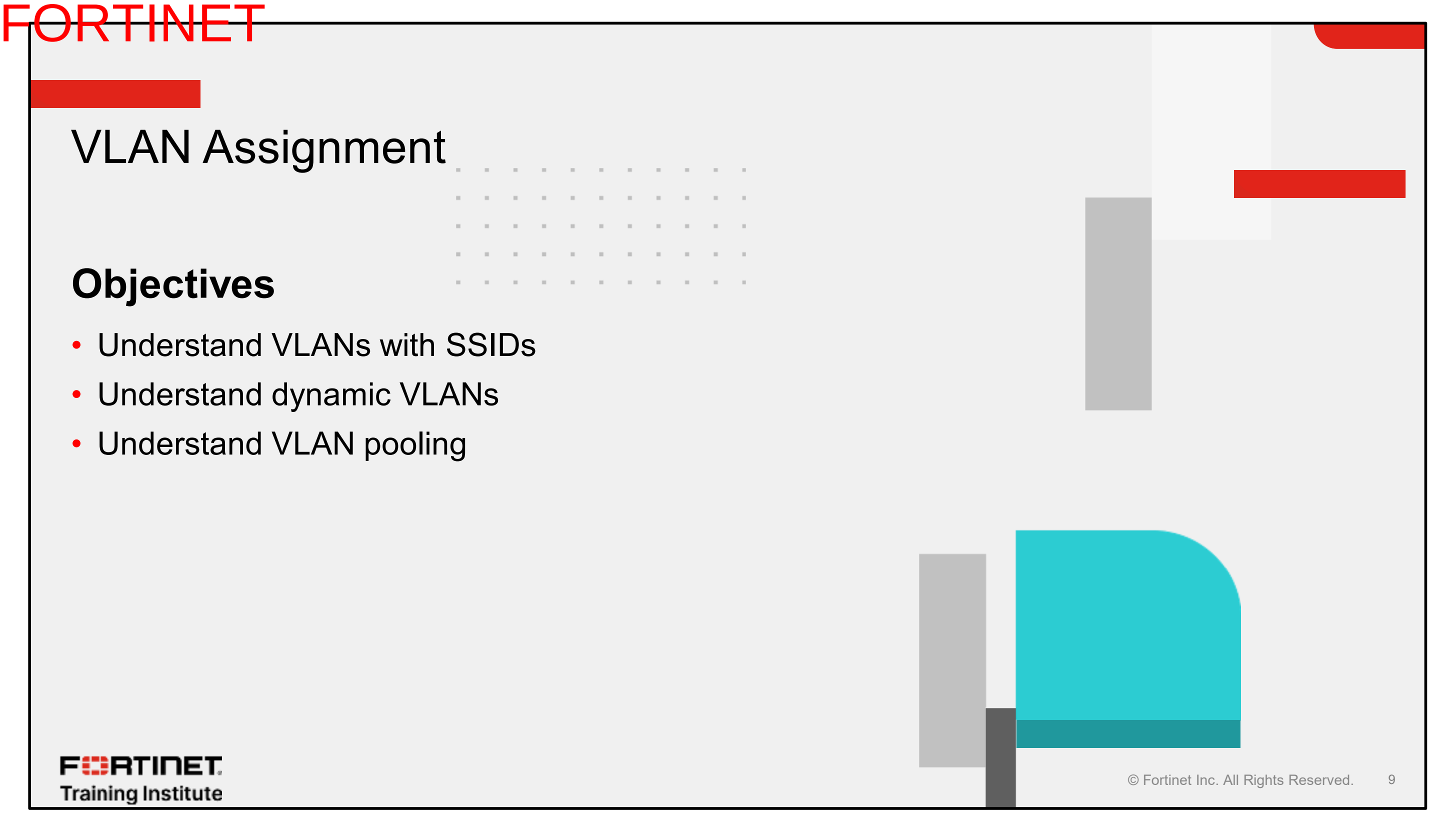
- ✓ Additional SSID Settings
- VLAN Assignment
- Integrated Wireless NAC
- Wireless Client Quarantine

FORTINET Training Institute

8

Good job! You now understand the additional SSID settings.

Now, you will learn how to dynamically configure VLAN assignments.



VLAN Assignment

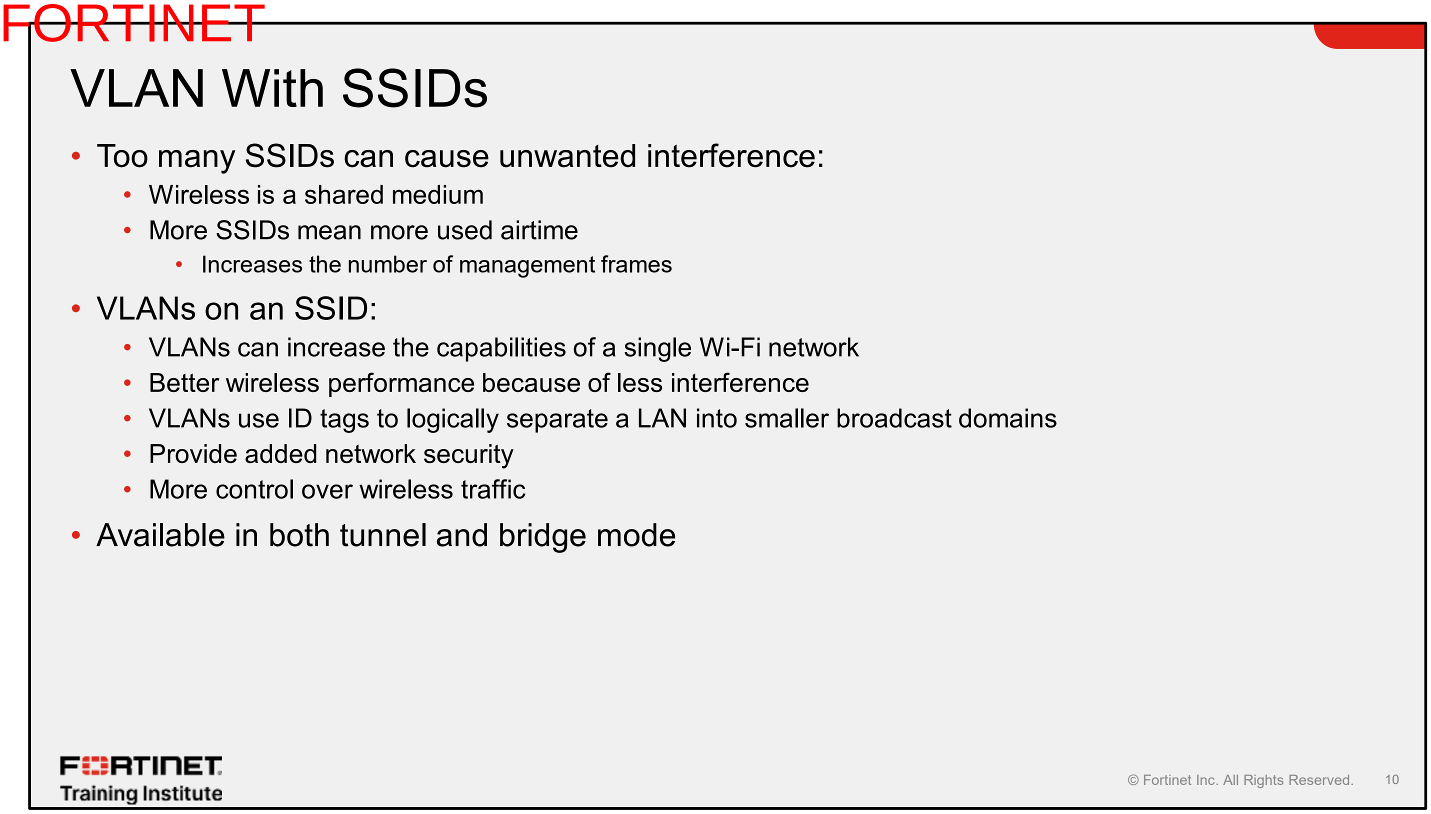
Objectives

- Understand VLANs with SSIDs
- Understand dynamic VLANs
- Understand VLAN pooling

9

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding VLANs in a wireless deployment, you will be able to use them effectively in your network.



VLAN With SSIDs

- Too many SSIDs can cause unwanted interference:
  - Wireless is a shared medium
  - More SSIDs mean more used airtime
    - Increases the number of management frames
- VLANs on an SSID:
  - VLANs can increase the capabilities of a single Wi-Fi network
  - Better wireless performance because of less interference
  - VLANs use ID tags to logically separate a LAN into smaller broadcast domains
  - Provide added network security
  - More control over wireless traffic
- Available in both tunnel and bridge mode

10

Wireless is a shared medium. Having more SSIDs means all management traffic and client data are competing for the available airtime, leading to potentially to low airtime for each client, especially with an increasing number of Wi-Fi clients.

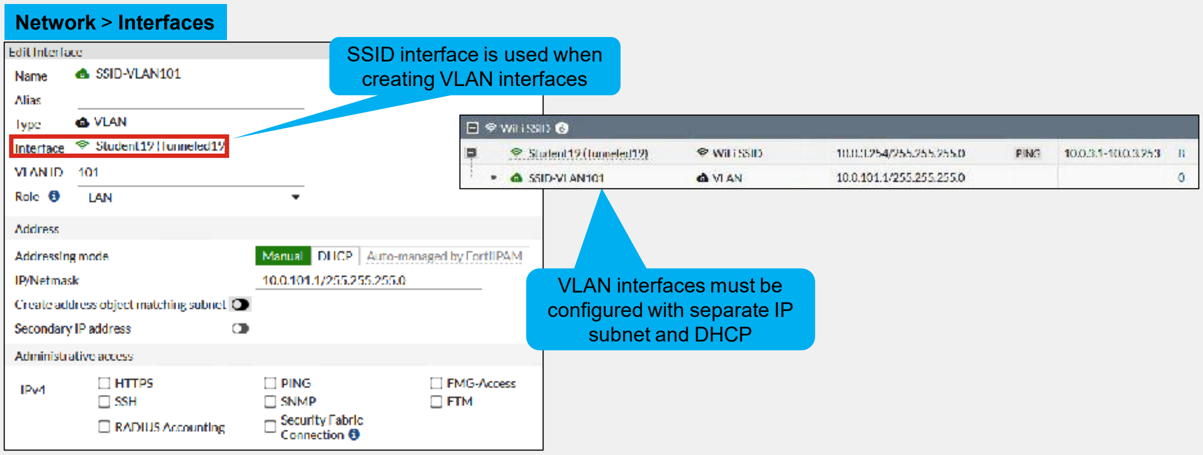
Using VLANs can enhance the capabilities of a Wi-Fi network because you can include more broadcast domains and you can control the flow of inter-VLAN traffic, which provides additional network security.

VLANs use ID tags to logically separate a LAN into smaller broadcast domains. Each VLAN is its own broadcast domain. Smaller broadcast domains reduce traffic and increase network security. The IEEE 802.1Q standard defines VLANs. All layer 2 and layer 3 devices along a route must be 802.1Q-compliant to support VLANs along that route.

Using VLANs with SSID can help you break down large broadcast domains into more manageable subnets. By reducing the need to deploy additional SSIDs, VLANs in a wireless network can help you increase wireless performance.

VLANs With Tunnel Mode

- VLANs are tied to tunneled SSID interface
  - SSID interface becomes a VLAN trunk
  - VLANs must be configured with IP address, administrative access, and so on
  - Requires separate firewall policies



Network > Interfaces

Edit Interface

Name: SSID-VLAN101
Alias:
Type: VLAN
Interface: Student19 (Tunneled19)
VLAN ID: 101
Role: LAN

Address

Addressing mode: Manual | DHCP | Auto-managed by FortiIPAM
IP/Netmask: 10.0.101.1/255.255.255.0
Create address object matching subnet
Secondary IP address

Administrative access

IPv4: □ HTTPS □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection

WiFi SSID 6					
Student19 (tunneled19)	WiFi SSID	10.0.3.254/255.255.255.0	PING	10.0.3.1-10.0.3.253	8
SSID-VLAN101	VLAN	10.0.101.1/255.255.255.0			0

SSID interface is used when creating VLAN interfaces

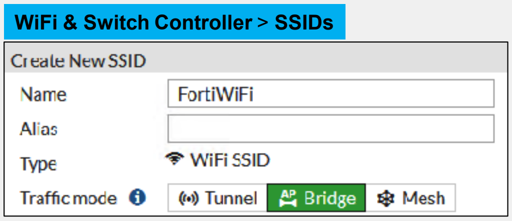
VLAN interfaces must be configured with separate IP subnet and DHCP

VLANs are treated as separate virtual interfaces that are tied to a physical or tunneled SSID interface. Therefore, you must configure all VLAN interfaces with interface settings, such as an IP address, administrative access, and so on. FortiGate also must have a DHCP server or relay configured, to ensure that all clients connecting to the SSID receive correct IP information.

Since VLANs are considered separate interfaces, you must configure firewall policies according to the level of network access you want to provide to the wireless clients.

Local Bridge With VLANs

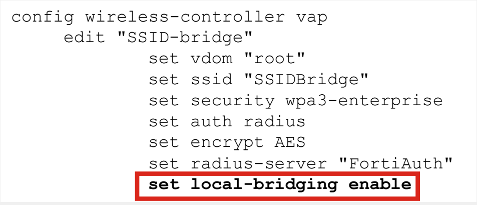
- FortiAP devices can forward tagged traffic to the bridged network
- Firewall policies on FortiGate are required only to route traffic between interfaces



WiFi & Switch Controller > SSIDs

Create New SSID

Name	FortiWiFi
Alias	
Type	WiFi SSID
Traffic mode	Tunnel [✓ Bridge] Mesh

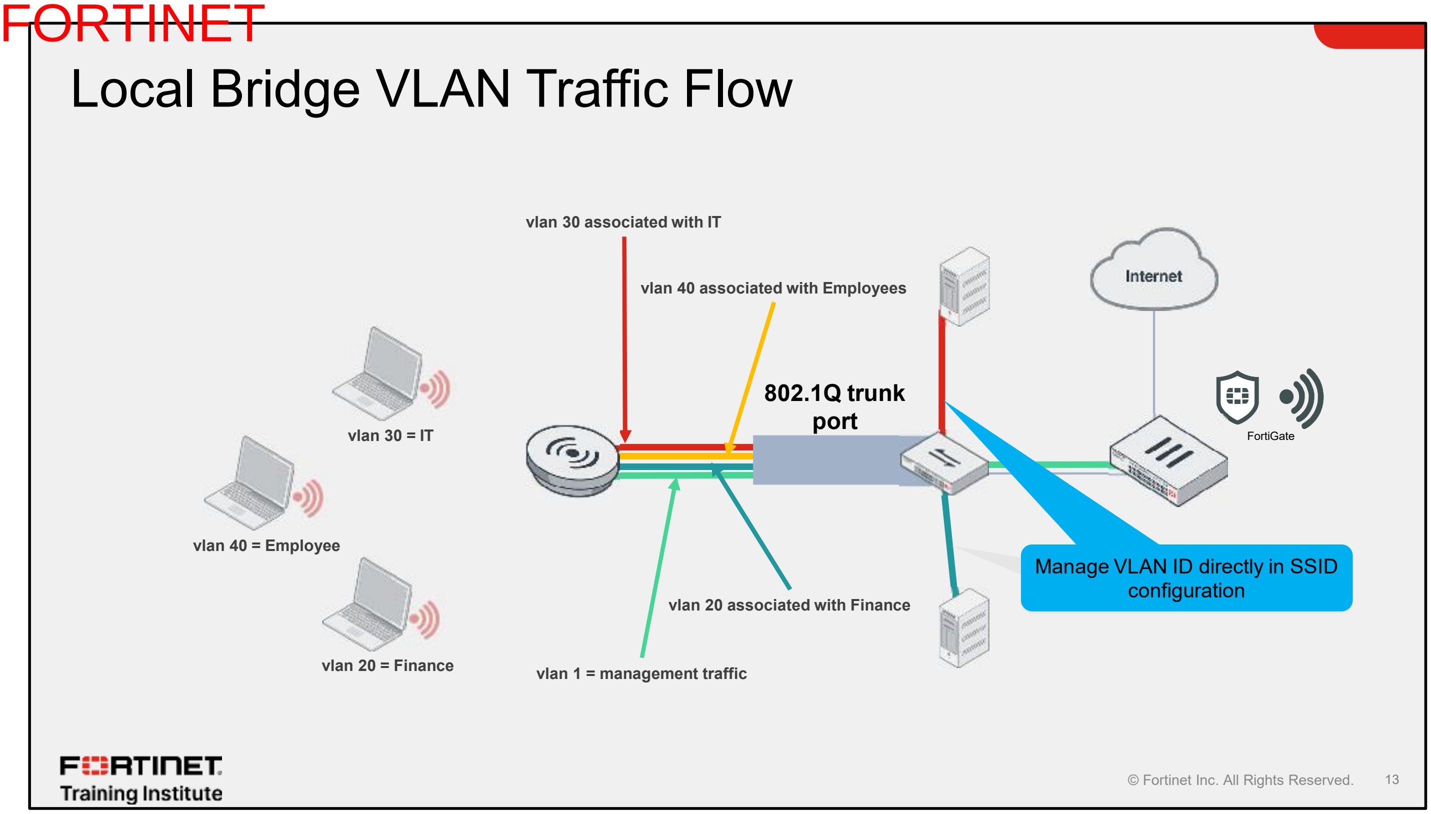


```
config wireless-controller vap
     edit "SSID-bridge"
             set vdom "root"
             set ssid "SSIDBridge"
             set security wpa3-enterprise
             set auth radius
             set encrypt AES
             set radius-server "FortiAuth"
             set local-bridging enable
```

FORTINET Training Institute

12

This slide shows the traffic flow from an AP with an SSID configured in local bridge mode. FortiAP tags the traffic coming from wireless clients with correct VLAN ID. FortiAP then places the traffic on the bridged network. Note that local traffic is switched at the FortiSwitch device, but Control and Provisioning of Wireless Access Points (CAPWAP) protocol control traffic still goes to the wireless controller.



Local Bridge VLAN Traffic Flow

vlan 30 associated with IT

vlan 40 associated with Employees

802.1Q trunk port

Internet

FortiGate

vlan 30 = IT

vlan 40 = Employee

vlan 20 = Finance

vlan 20 associated with Finance

vlan 1 = management traffic

Manage VLAN ID directly in SSID configuration

FORTINET Training Institute

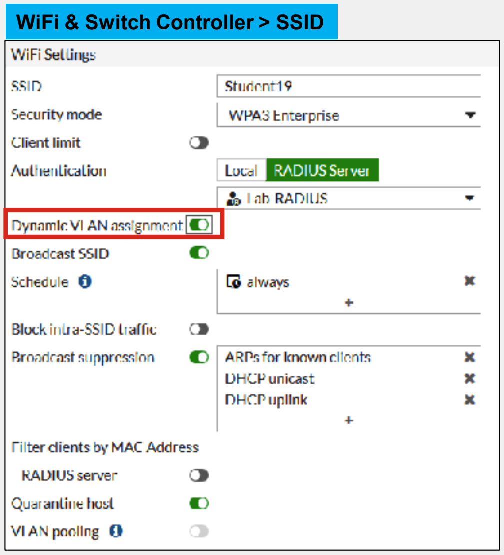
© Fortinet Inc. All Rights Reserved. 13

The diagram on this slide shows an example of traffic flow for local bridging. Note that this case has been extended to support VLAN IDs on the wired interface, which are each tagged with different VLAN IDs in local bridge mode.

Here, the FortiAP Ethernet interface functions as an 802.1Q trunk. The wireless traffic is bridged locally, and tagged with its corresponding VLAN ID.

Dynamic VLANs

- Only available using WPA2 Enterprise or WPA3 Enterprise
- The RADIUS server must provide VLAN information
  - RADIUS server must send the following attributes:
    - IETF 64 (tunnel type)—Set this to VLAN
    - IETF 65 (tunnel medium type)—Set this to IEEE 802
    - IETF 81 (tunnel private group ID)—Set this to the VLAN ID or a text string that matches a VLAN interface name
- Supported on tunneled and bridged SSID



WiFi & Switch Controller > SSID

WiFi Settings

SSID: Student19

Security mode: WPA3 Enterprise

Client limit: ○

Authentication: Local | RADIUS Server

Lab RADIUS

Dynamic VLAN assignment: ●

Broadcast SSID: ●

Schedule: always

Block intra-SSID traffic: ○

Broadcast suppression: ●
ARPs for known clients
DHCP unicast
DHCP uplink

Filter clients by MAC Address

RADIUS server: ○

Quarantine host: ●

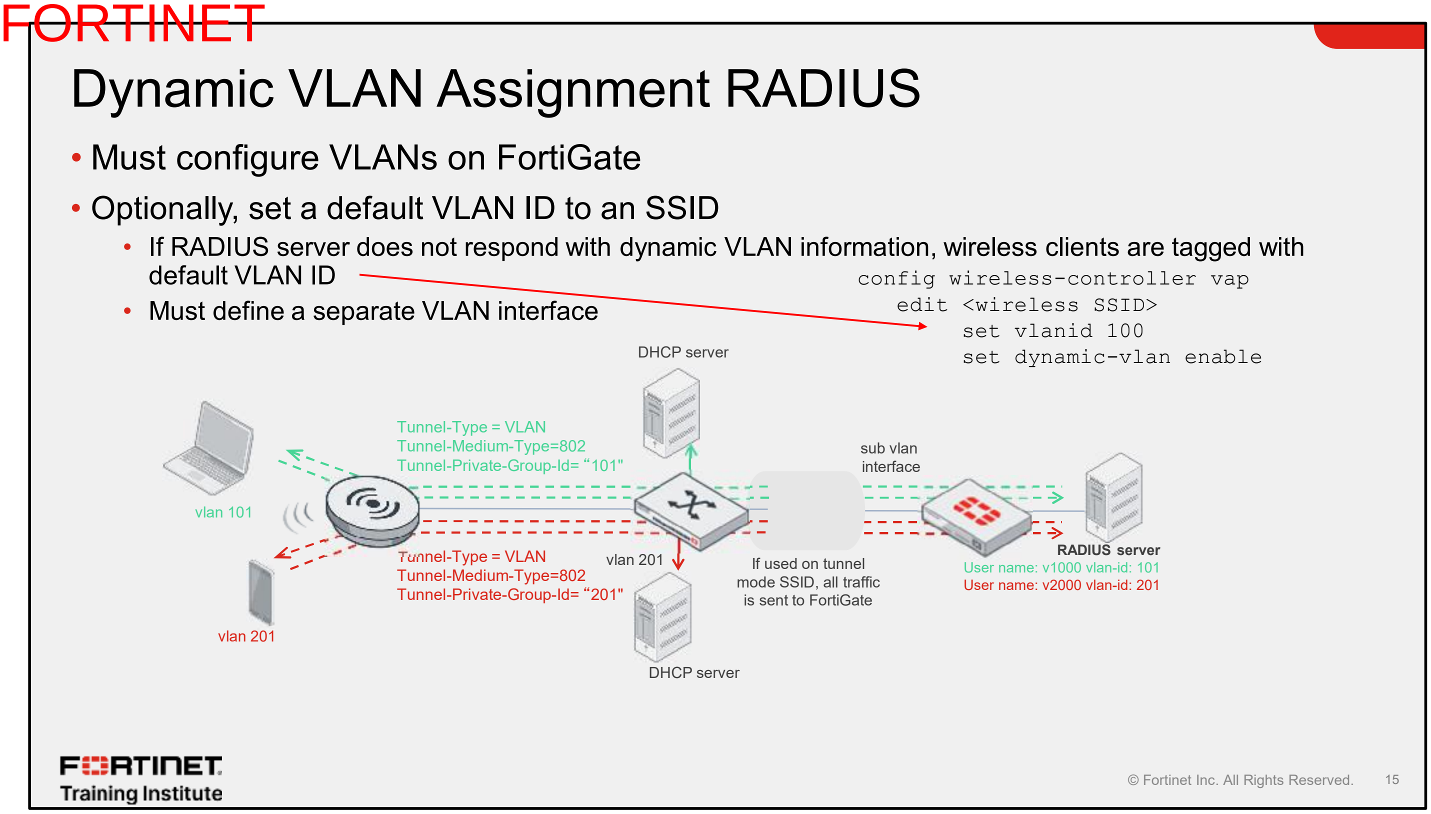
VLAN pooling: ○

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

The option to add dynamic VLANs to SSID is available on FortiGate in both tunnel and bridge modes. You can apply dynamic VLANs to SSIDs that have the security mode set to **WPA2 Enterprise** or **WPA3 Enterprise** and the authentication method set to **RADIUS Server**. The RADIUS server is responsible for sending all the required attributes after a successful authentication. The RADIUS server must send the following attributes to FortiGate:

- IETF 64 set to VLAN: This attribute tells FortiGate that VLAN information is attached to the RADIUS response.
- IETF 65 set to IEEE 802: This attribute tells FortiGate that the IEEE 802 attribute is attached to the RADIUS response.
- IETF 81 set to VLAN ID or VLAN name: This attribute tells FortiGate to attach the user to the specified VLAN ID interface.



Dynamic VLAN Assignment RADIUS

- Must configure VLANs on FortiGate
- Optionally, set a default VLAN ID to an SSID
  - If RADIUS server does not respond with dynamic VLAN information, wireless clients are tagged with default VLAN ID
  - Must define a separate VLAN interface

```
config wireless-controller vap
    edit <wireless SSID>
        set vlanid 100
        set dynamic-vlan enable
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

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

FortiGate does not dynamically create VLANs. You must configure all the VLANs on FortiGate, along with the corresponding firewall polices.

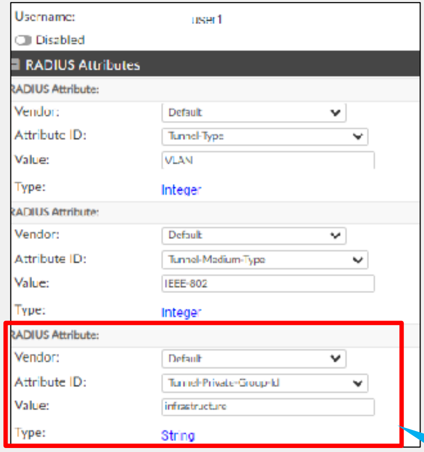
VLAN Assignment by Name Tag

- Ability to assign VLANs to wireless clients using name tags that match a VLAN ID
- The name value is returned in the Tunnel-Private-Group-Id RADIUS attribute in the Access-Accept Message

```
config wireless-controller vap
    edit " wifi_vlan"
        set ssid "wifi_vlan"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "FAC"
        set schedule "always"
        set dynamic-vlan enable
            config vlan-name
            edit "data"
                set vlan-id 100 200 300
            next
            edit "infrastructure"
                set vlan-id 213
```

VLAN table

FortiAuthenticator: Authentication > User Management > Local Users



Username: user1

Disabled

RADIUS Attributes

RADIUS Attribute:

Vendor: Default

Attribute ID: Tunnel-Type

Value: VLAN

Type: Integer

RADIUS Attribute:

Vendor: Default

Attribute ID: Tunnel-Medium-Type

Value: IEEE-802

Type: Integer

RADIUS Attribute:

Vendor: Default

Attribute ID: Tunnel-Private-Group-Id

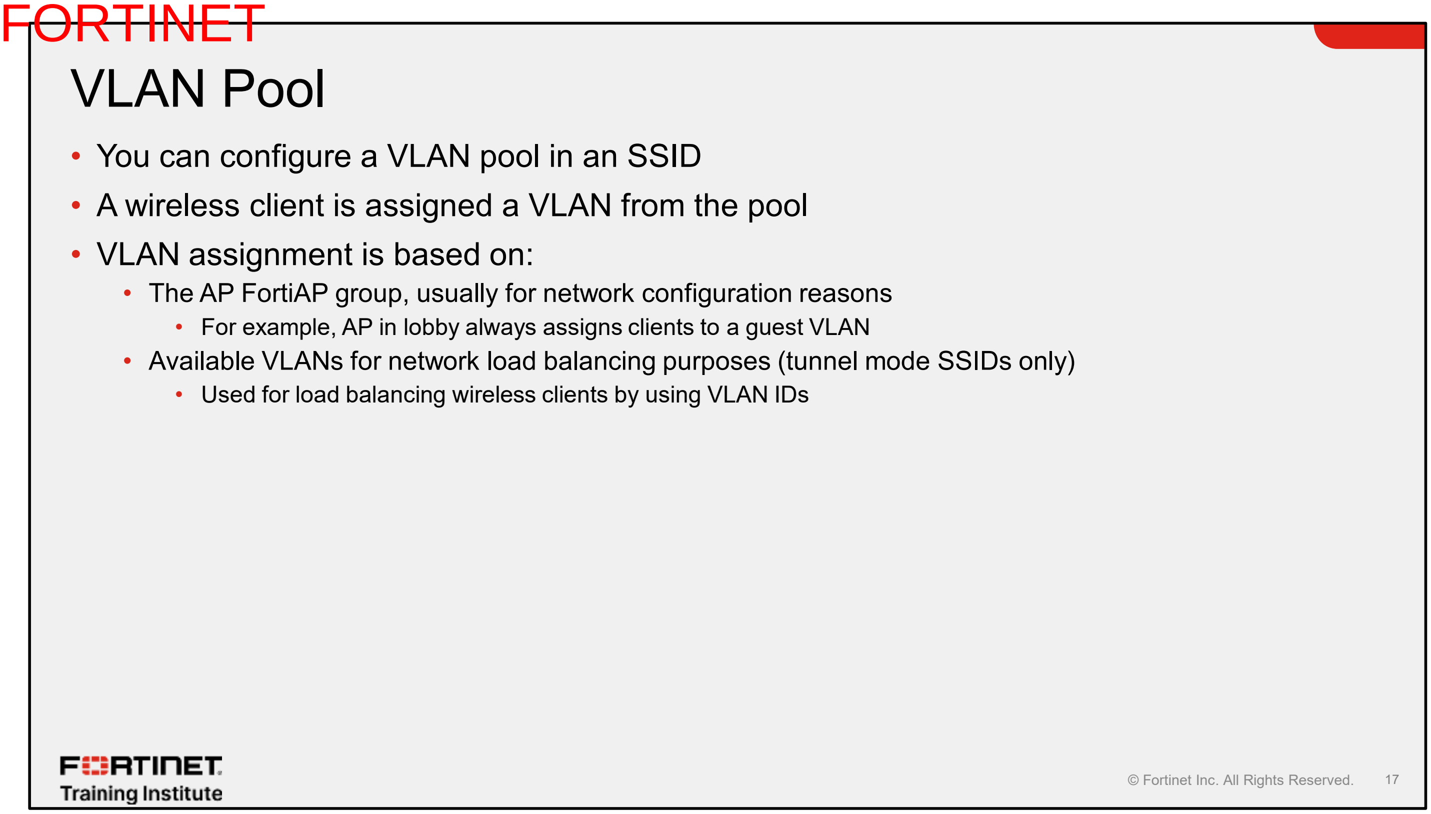
Value: infrastructure

Type: String

String sent to virtual AP for VLAN matching

16

Another option is to match based on a VLAN table defined under the virtual AP. You can assign either a single VLAN ID per name, or assign multiple VLAN IDs per name, up to a maximum of 8 VLAN IDs. When assigning multiple VLAN IDs, a round-robin method determines the ID to ensure optimal use of VLAN resources.



VLAN Pool

- You can configure a VLAN pool in an SSID
- A wireless client is assigned a VLAN from the pool
- VLAN assignment is based on:
  - The AP FortiAP group, usually for network configuration reasons
    - For example, AP in lobby always assigns clients to a guest VLAN
  - Available VLANs for network load balancing purposes (tunnel mode SSIDs only)
    - Used for load balancing wireless clients by using VLAN IDs

Training Institute

17

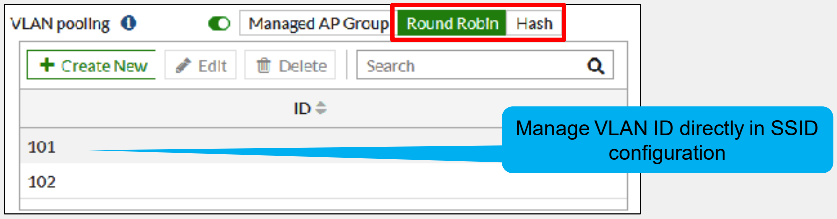
In an SSID, you can define a VLAN pool. As clients associate with an AP, they are assigned to a VLAN. A VLAN pool can assign a specific VLAN based on the AP FortiAP group, usually for network configuration reasons, or it can assign one of several available VLANs for network load balancing purposes (tunnel mode SSIDs only).

If the VLAN pool contains no valid VLAN ID, the SSID static VLAN ID setting is used.

VLAN Pooling and Load Balancing

- Two VLAN pooling methods are available for wireless client load balancing:
  - **Round Robin**
    - VLAN with least number of clients is assigned to new connections
  - **Hash**
    - FortiOS assigns a VLAN based on a hash of the current number of SSID clients and the number of entries in the VLAN pool

WiFi & Switch Controller > SSIDs



Manage VLAN ID directly in SSID configuration

- VLAN pooling load balancing is available only for SSIDs in tunnel mode

Two options available in the VLAN pooling configuration provide load balancing options for wireless clients: **Round Robin** and **Hash**. After you enable **VLAN Pooling** on SSID, you can select **Managed AP Groups**, **Round Robin**, or **Hash**.

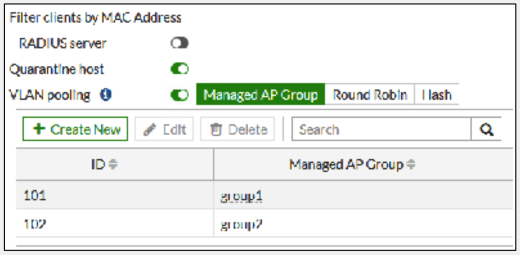
Similar to configuring managed AP groups, you can define VLANs directly on the SSID configuration page for both the **Round Robin** and **Hash** options. **Round Robin** assigns the least busy VLAN to new clients. **Hash** identifies which VLAN to use based on the hash value of the current number of clients connected to the SSID and the number of VLANs available in the pool.

VLAN pooling load balancing is available only for SSIDs operating in tunnel mode.

VLAN Pooling and FortiAP Groups

- Ability to assign wireless clients VLANs using a pool
  - Assign VLANs to clients based on AP FortiAP group
    - Groups together facilitate application of FortiAP profiles to large number of FortiAPs
    - Assign VLANs to wireless clients based on the FortiAP group

WiFi & Switch Controller > SSIDs



Filter clients by MAC Address

RADIUS server ○

Quarantine host ●

VLAN pooling ● Managed AP Group | Round Robin | Hash

ID	Managed AP Group
101	group1
102	group2

```
config wireless- controller vap
  edit wlan
    set vlan-pooling wtp-group
    config vlan- pool
       edit 101
         set wtp-group group1
       next
       edit 102
         set wtp-group group2
       next
```

- Allows assignment of VLANs to AP groups within SSID configuration page
  - FortiGate automatically creates the VLANs without any interface settings such network, administrative access, DHCP server, and so on
  - You must configure these settings manually for the VLAN interface

FORTINET Training Institute

You can put FortiAPs in a group of two or more APs, to easily manage them. For example, you can group APs based on the floor or section of the office they are installed on. You must configure managed AP groups before you can use them in the VLAN pooling configuration.

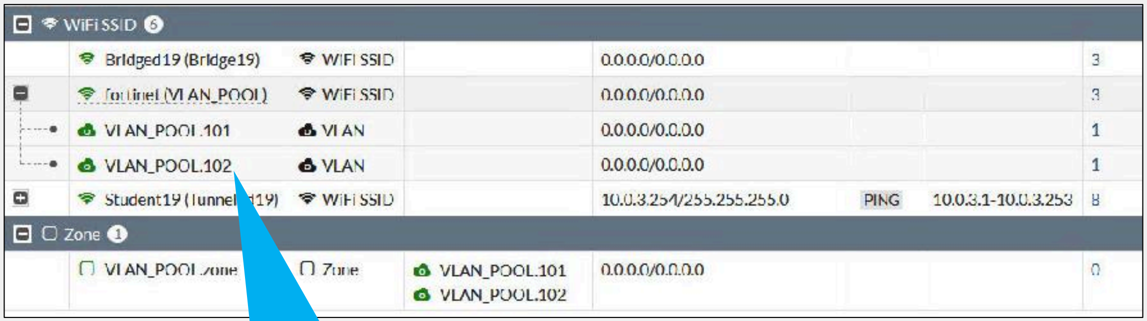
You can then use FortiAP groups to dynamically assign VLANs to wireless clients based on the APs that they connect to. This feature is useful in large deployments and can break down the broadcast domain, rather than putting all wireless clients into a single subnet. Another reason to assign VLANs based on APs is to apply security inspections and firewall rules based on the location of wireless clients. This provides you with more granular control over wireless traffic.

You can define VLANs and assign them to AP groups on the SSID configuration page on the GUI. However, you still must manually configure interface settings such as network, administrative access, DHCP server configuration, and so on.

VLAN Pooling and Load Balancing

- FortiOS automatically adds the load balancing VLANs to a zone
  - Based on the SSID
  - Ensures all load balancing VLANs are configured with identical access
  - Makes it easier for you to manage firewall policies

Network > Interfaces



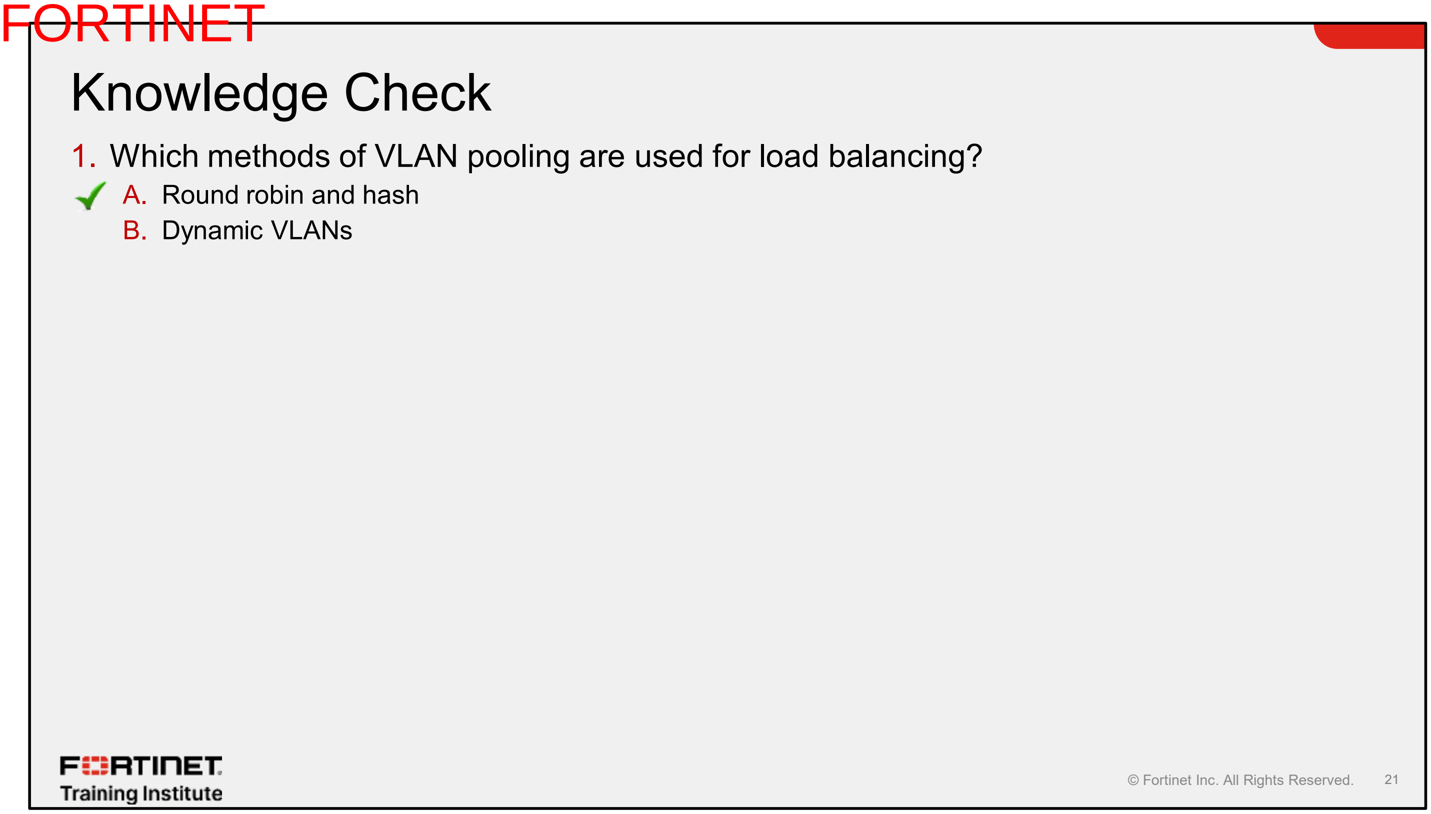
⊟	WiFi SSID 6						
	Bridged19 (Bridge19)	WiFi SSID		0.0.0.0/0.0.0.0			3
⊟	Fortinet (VLAN_POOL)	WiFi SSID		0.0.0.0/0.0.0.0			3
	VLAN_POOL.101	VLAN		0.0.0.0/0.0.0.0			1
	VLAN_POOL.102	VLAN		0.0.0.0/0.0.0.0			1
⊞	Student19 (Tunnel19)	WiFi SSID		10.0.3.254/255.255.255.0	PING	10.0.3.1-10.0.3.253	8
⊟	Zone 1						
	VLAN_POOL.zone	Zone	VLAN_POOL.101 VLAN_POOL.102	0.0.0.0/0.0.0.0			0

Configure network and DHCP options for each VLAN ID

FURTINET Training Institute

You can define VLAN pooling and load balancing VLANs on the SSID configuration page. FortiGate automatically puts all load balancing VLANs in a zone based on the SSID they were defined in. VLANs are tied to the SSID interface. The zone name includes the SSID interface name followed by `.zone`. For example, if you name your SSID interface Fortinet, then the zone will be named `Fortinet.zone`.

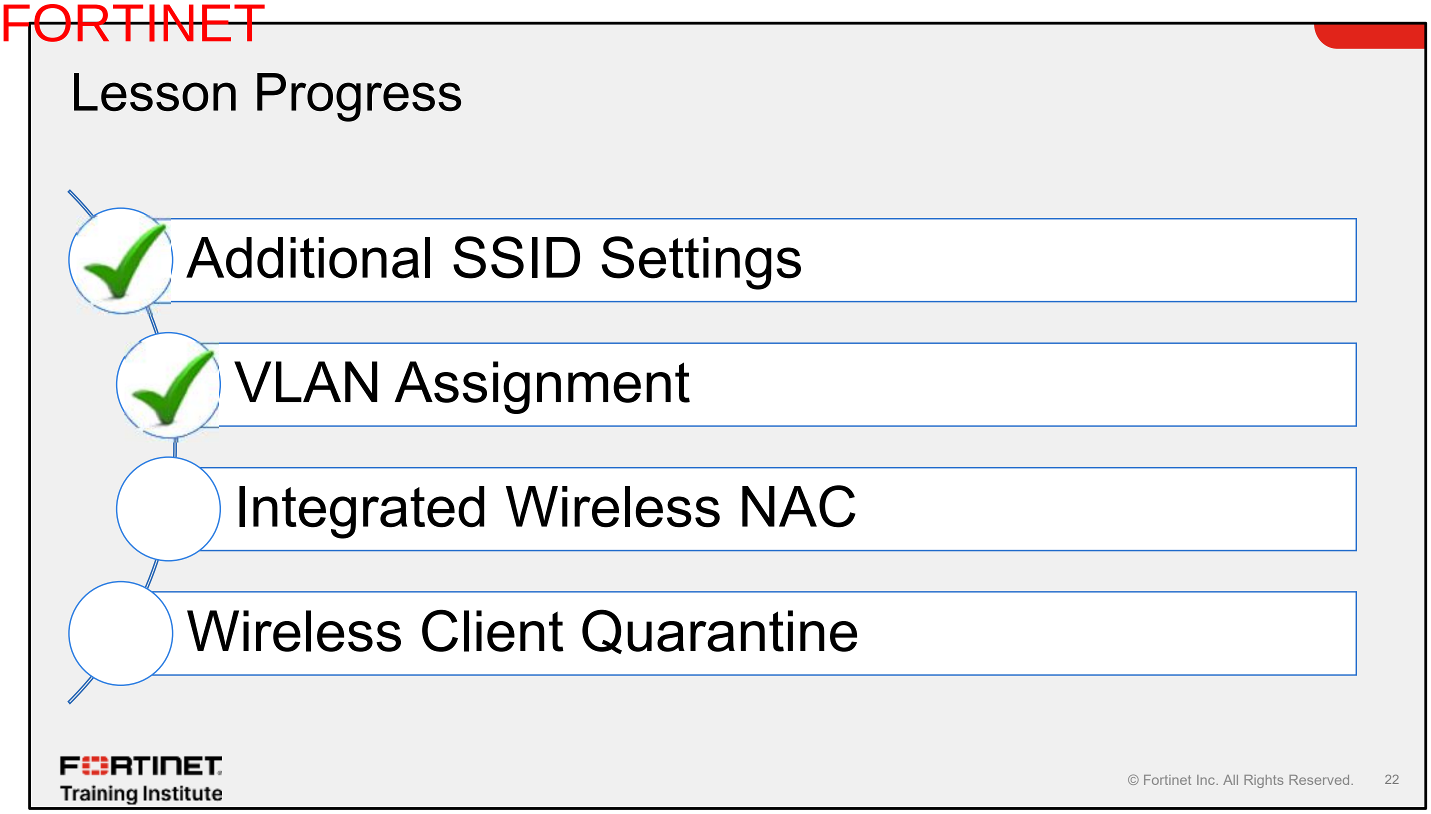
You must configure each VLAN with its own interface option, such as subnet, DHCP, and so on.



Knowledge Check

1. Which methods of VLAN pooling are used for load balancing?
   - ✓ A. Round robin and hash
   - B. Dynamic VLANs

FORTINET
Training Institute



Lesson Progress

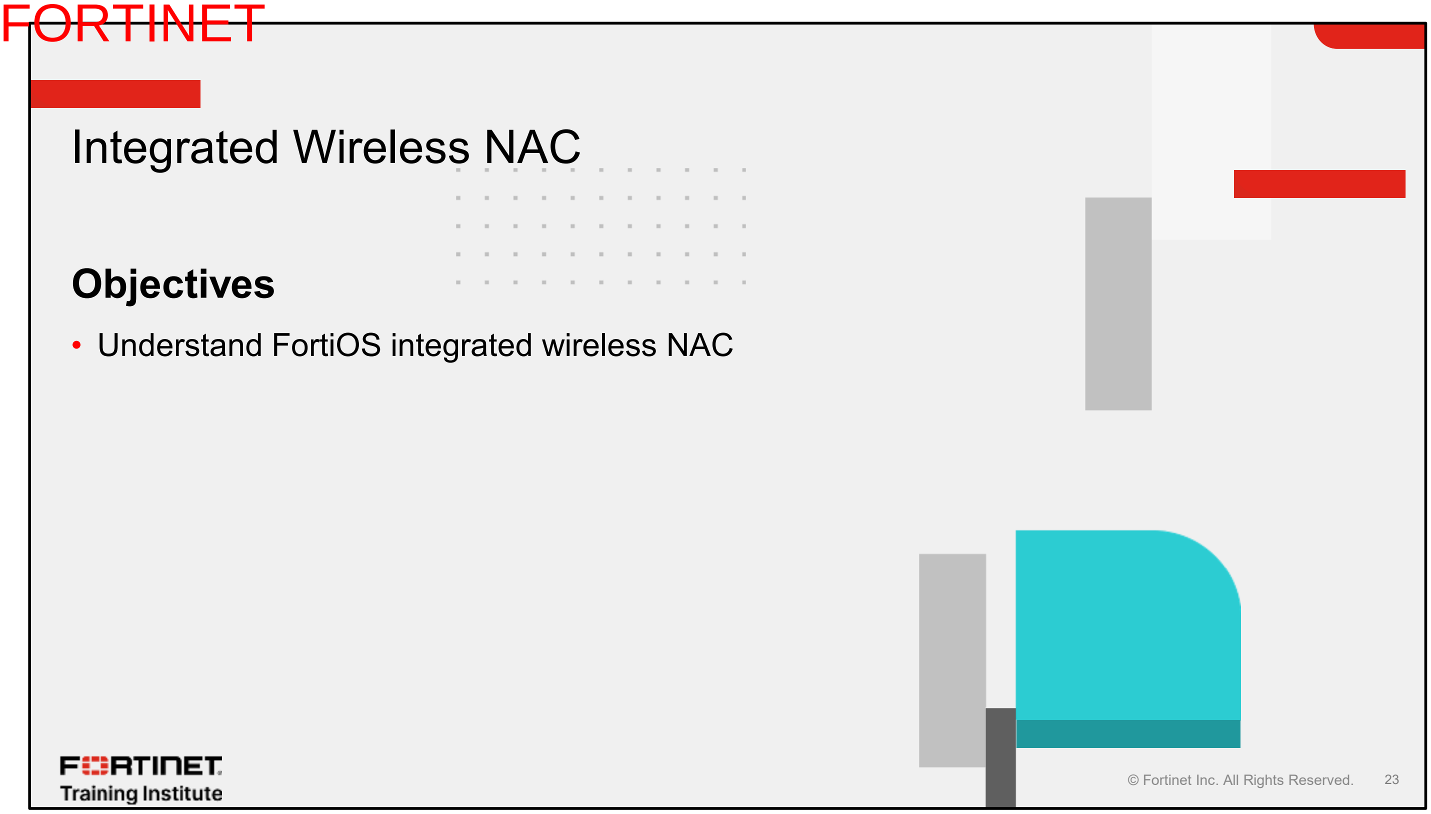
- ✓ Additional SSID Settings
- ✓ VLAN Assignment
- ○ Integrated Wireless NAC
- ○ Wireless Client Quarantine

FORTINET Training Institute

22

Good job! You now understand how VLANS are used with SSIDs.

Now, you will learn how to configure wireless network access control.



Integrated Wireless NAC

Objectives

- Understand FortiOS integrated wireless NAC

FORTINET
Training Institute

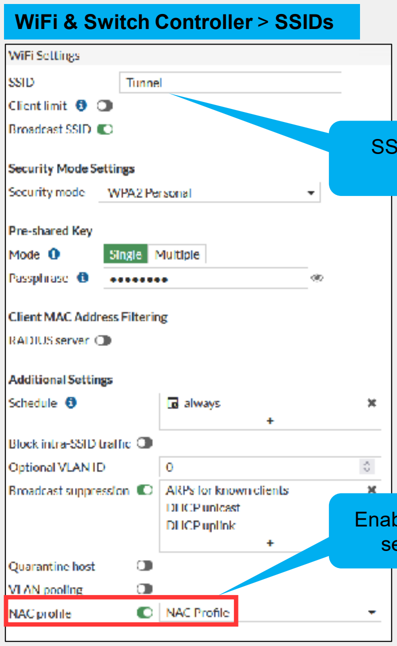
© Fortinet Inc. All Rights Reserved. 23

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding the configuration of wireless network access control (NAC), you will be able to use it effectively in your network.

Integrated Wireless NAC

- An extension to NAC functions on FortiSwitch to wireless networks
  - Shares the same set of FortiSwitch NAC policies
  - Match based on devices, user groups, devices with specified FortiClient EMS tag, and vulnerability
- Clients get assigned to an onboarding VLAN, a subinterface of the SSID
  - SSID can be bridge or tunnel
  - Onboarding VLAN requires Layer 3 settings and DHCP server
- Each SSID can use a different NAC profile
  - NAC profile has the reference to the onboarding VLAN
  - A NAC policy is required to reassign from onboarding VLAN to the appropriate VLAN



WiFi & Switch Controller > SSIDs

WiFi Settings
SSID: Tunnel
Client limit: ○
Broadcast SSID: ●

Security Mode Settings
Security mode: WPA2 Personal

Pre-shared Key
Mode: Single | Multiple
Passphrase: ••••••••

Client MAC Address Filtering
RADIUS server: ○

Additional Settings
Schedule: always
Block intra-SSID traffic: ○
Optional VLAN ID: 0
Broadcast suppression: ● ARPs for known clients, DHCP unicast, DHCP uplink
Quarantine host: ○
VLAN pooling: ○
NAC profile: ● NAC Profile

SSID can be bridge or tunnel mode

Enable NAC on SSID and select a NAC profile

NAC helps you to implement policies to control devices and users in your network. You define wireless NAC policy based on patterns users and devices can be identified with, such as user groups and device hardware information.

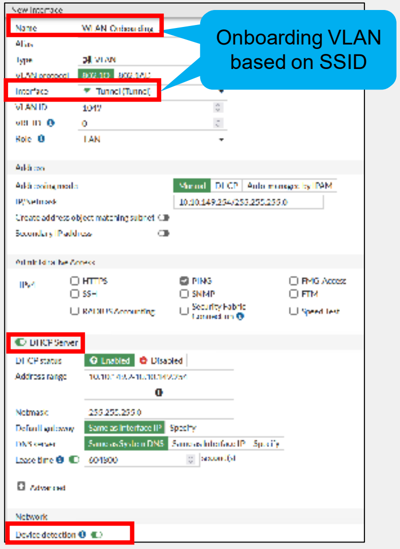
You can enable wireless NAC can be enabled on bridge or tunnel mode SSIDs. It requires at least two VLANs to configure the onboarding segment as well as the appropriate VLAN for the wireless devices. You must configure these VLANs with Layer 3 settings, including DHCP and network device detection services.

Enable the NAC profile on the SSID where you specify the onboarding VLAN. Use the NAC policy to specify the matching condition and the wireless VLAN assignment.

Integrated Wireless NAC—SSID and VLAN

- If you configure an SSID with wireless NAC, you must create at least two VLANs
- Onboarding VLAN
  - To onboard wireless clients when connected for the first time
  - Requires **DHCP Server** and **Device detection**
  - NAC profile must select this onboarding VLAN when SSID set as NAC access mode
- Another VLAN to reassign for matched device
- VLAN ID scope is only within the SSID interface broadcast domain

System > Interfaces



New Interface
Name: WLAN Onboarding
Alias:
Type: VLAN
VLAN protocol: 802.1Q | 802.1AD
Interface: Tunnel (Tunnel)
VLAN ID: 1019
VRF ID: 0
Role: LAN

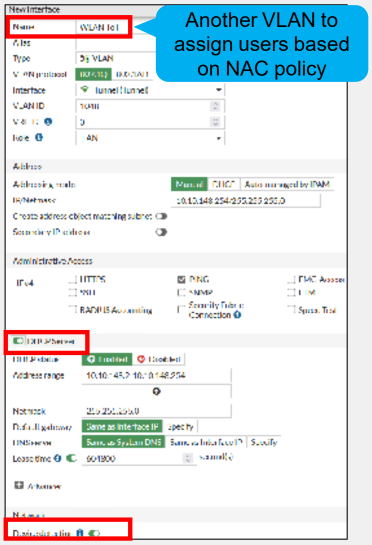
Address
Addressing mode: Manual | DHCP | Auto-managed by IPAM
IP/Netmask: 10.10.149.254/255.255.255.0
Create address object matching subnet
Secondary IP address

Administrative Access
IPv4: □ HTTPS □ SSH □ RADIUS Accounting ☑ PING □ SNMP □ Security Fabric Connection □ FMG-Access □ FTM □ Speed Test

DHCP Server
DHCP status: Enabled | Disabled
Address range: 10.10.149.1-10.10.149.254
Netmask: 255.255.255.0
Default gateway: Same as Interface IP | Specify
DNS server: Same as System DNS | Same as Interface IP | Specify
Lease time: 604800 second(s)
Advanced

Network
Device detection

Onboarding VLAN based on SSID



New Interface
Name: WLAN IoT
Alias:
Type: VLAN
VLAN protocol: 802.1Q | 802.1AD
Interface: Tunnel (Tunnel)
VLAN ID: 1018
VRF ID: 0
Role: LAN

Address
Addressing mode: Manual | DHCP | Auto-managed by IPAM
IP/Netmask: 10.10.148.254/255.255.255.0
Create address object matching subnet
Secondary IP address

Administrative Access
IPv4: □ HTTPS □ SSH □ RADIUS Accounting ☑ PING □ SNMP □ Security Fabric Connection □ FMG-Access □ FTM □ Speed Test

DHCP Server
DHCP status: Enabled | Disabled
Address range: 10.10.148.2-10.10.148.254
Netmask: 255.255.255.0
Default gateway: Same as Interface IP | Specify
DNS server: Same as System DNS | Same as Interface IP | Specify
Lease time: 604800 second(s)
Advanced

Network
Device detection

Another VLAN to assign users based on NAC policy

FORTINET Training Institute

25

If you enable wireless NAC on an SSID, you must make sure at least two VLANs are available to configure the remaining wireless NAC settings for this SSID.

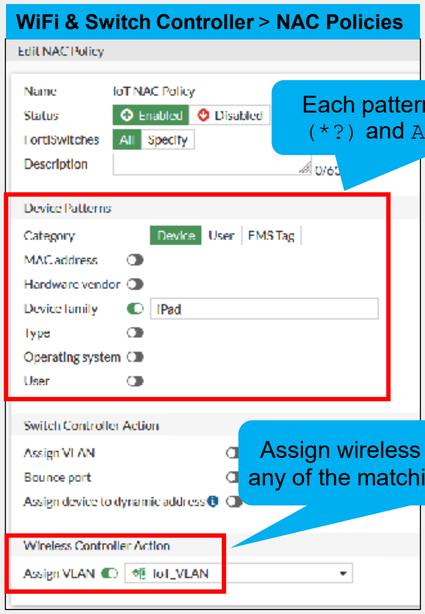
You must select the onboarding VLAN when you create the NAC profile, which enables NAC on the SSID. The onboarding VLAN must have Layer 3 settings, including DHCP and network device detection services.

Devices that match a NAC policy are assigned the VLAN configured in the NAC policy for wireless controller section. The NAC policy can still be evaluated for FortiSwitch NAC operation if its VLAN assignment is for FortiSwitch.

Integrated Wireless NAC—NAC Policies

- Define matching patterns
  - Triggers such as device, user, and EMS tag
- NAC policy patterns include scope of commands that identify where to apply policy
- Changes to existing matched NAC policies will require matched device to re-evaluate
- FortiGate checks NAC policies from top to bottom until device matches defined patterns

WiFi & Switch Controller > NAC Policies



Edit NAC Policy

Name: IoT NAC Policy
Status: Enabled | Disabled
FortiSwitches: All | Specify
Description: 0/63

Device Patterns

Category: Device | User | EMS Tag
MAC address
Hardware vendor
Device family: iPad
Type
Operating system
User

Switch Controller Action

Assign VLAN
Bounce port
Assign device to dynamic address

Wireless Controller Action

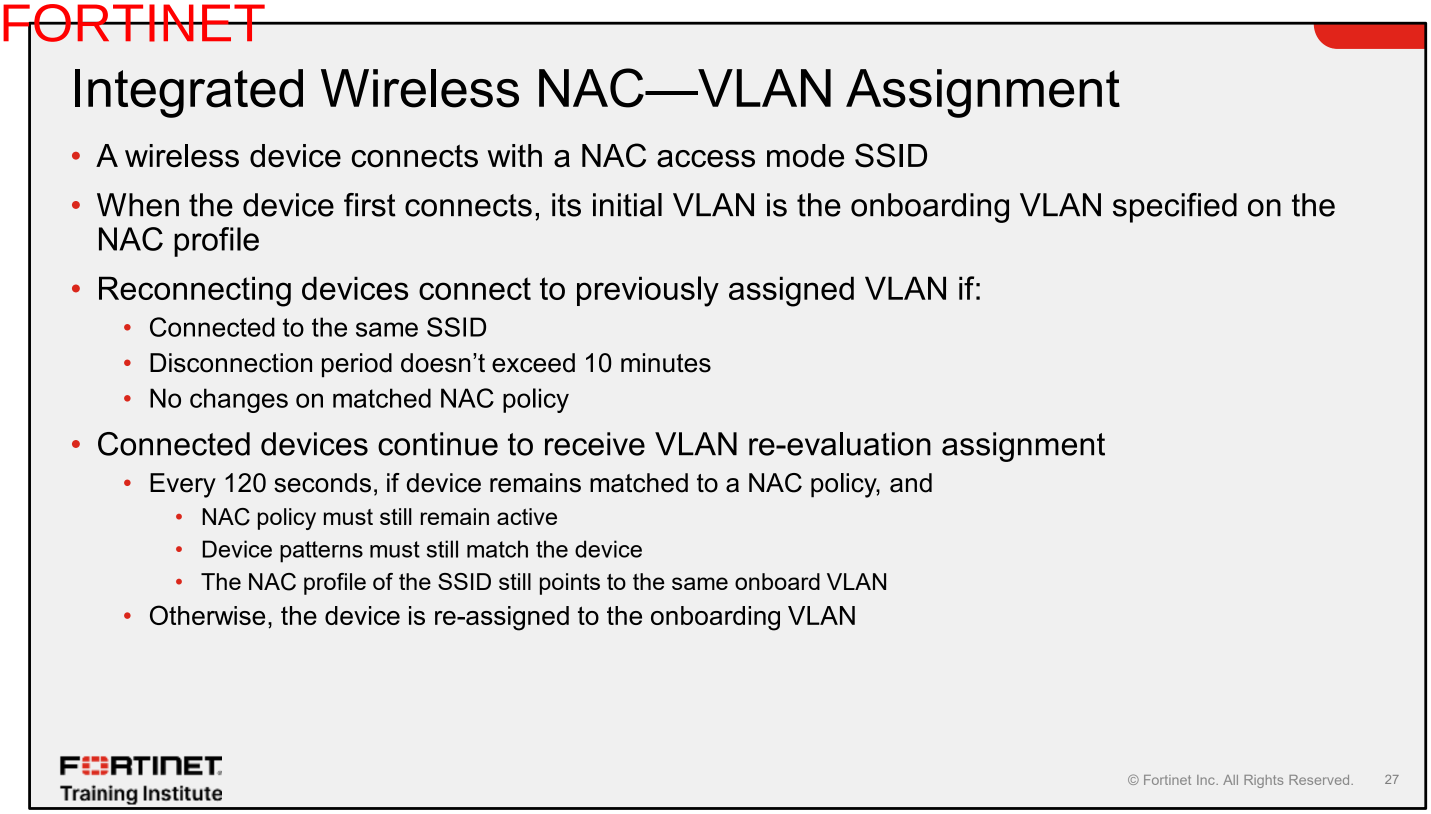
Assign VLAN: IoT_VLAN

Each pattern can use wild card (`*?`) and `AND` logical operator

Assign wireless device **IoT_VLAN** if any of the matching patterns triggered

NAC policies contain the device, user patterns, FortiClient EMS tag, and so on to check on a device, before the VLAN. Like firewall policies, FortiGate checks NAC policies from top to bottom until it finds a policy that matches *all* the defined patterns.

After FortiGate detects the device or user and it matches a NAC policy, FortiGate assigns the device the VLAN selected in the **Assign VLAN** field in the **Wireless Controller Action** section. Note that if the NAC policy changes, FortiGate deletes and re-evaluates all previously matched NAC devices using the list of NAC policies.



Integrated Wireless NAC—VLAN Assignment

- A wireless device connects with a NAC access mode SSID
- When the device first connects, its initial VLAN is the onboarding VLAN specified on the NAC profile
- Reconnecting devices connect to previously assigned VLAN if:
  - Connected to the same SSID
  - Disconnection period doesn’t exceed 10 minutes
  - No changes on matched NAC policy
- Connected devices continue to receive VLAN re-evaluation assignment
  - Every 120 seconds, if device remains matched to a NAC policy, and
    - NAC policy must still remain active
    - Device patterns must still match the device
    - The NAC profile of the SSID still points to the same onboard VLAN
  - Otherwise, the device is re-assigned to the onboarding VLAN

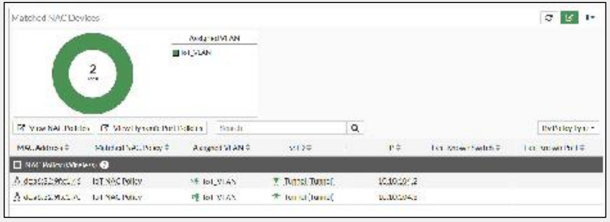
27

When a wireless device connects to a SSID that has a NAC profile enabled, the VLAN ID assigned depends on the previous status of the device. To avoid multiple DHCP servers assigning a new IP address, if the device was connected to the same SSID and was disconnected for less than 10 minutes, it is assigned the same VLAN it had prior to disconnecting, if no changes were made to the matched NAC policy.

Connected devices undergo a re-evaluation process every 120 seconds to determine the VLAN ID for each device. As long the NAC policy exists in the same VDOM, the NAC policy must remain active and device patterns must match the connected device. This is, of course, as long the SSID in question still has a NAC profile enabled and is pointing to the same onboard VLAN.

Integrated Wireless NAC—Monitor and Debug

WiFi & Switch Controller > NAC Policies > View Matched Devices



MAC Address	Matched NAC Policy	Assigned VLAN	SSID	IP	FortiSwitch	FortiSwitch Port
[illegible]	IoT NAC Policy	IoT_VLAN	Tunnel (Tunnel)	10.10.104.2		
[illegible]	IoT NAC Policy	IoT_VLAN	Tunnel (Tunnel)	[illegible]		

- To display devices on CLI connected to a NAC access mode SSID

```
FortiGate # diagnose wireless-controller wlac_hlp -c sta-nac
STA (001/002) vfid,mac: 0, dc:a6:32:9f:c1:46
    ip                      : 10.10.104.2
    wlan                    : Tunnel(tunnel)
    vlan-id(oper/dflt)      : 104/1049
    matched nac-policy      : IoT NAC Policy
```

- To list configured NAC profiles

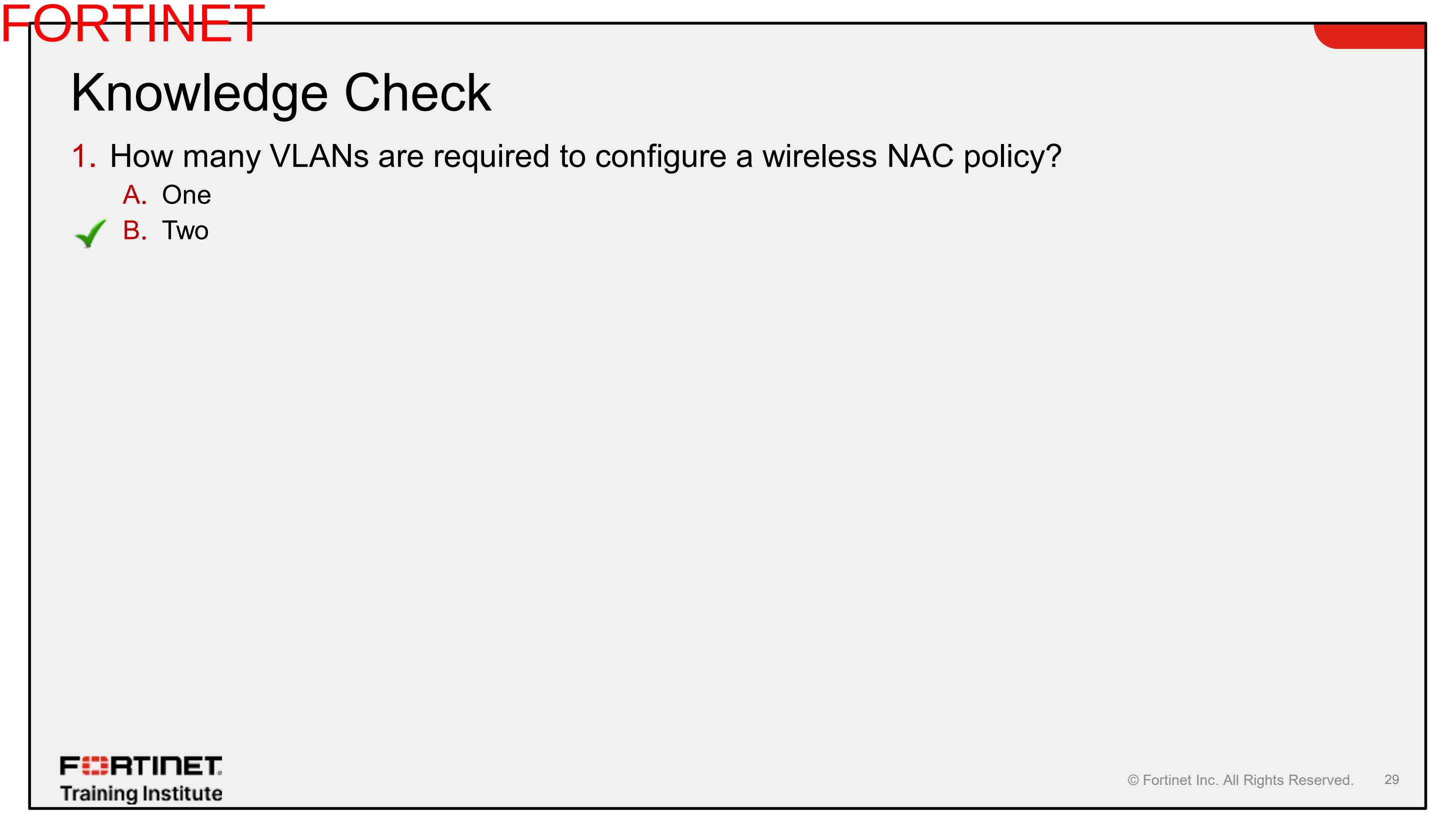
```
FortiGate # diagnose wireless-controller wlac_hlp -c nacprof
NACPROF (001/001) vdom,name: root, NAC Profile
    ob-vlan     : WLAN_Onboarding(1049)
```

FERTINET Training Institute

28

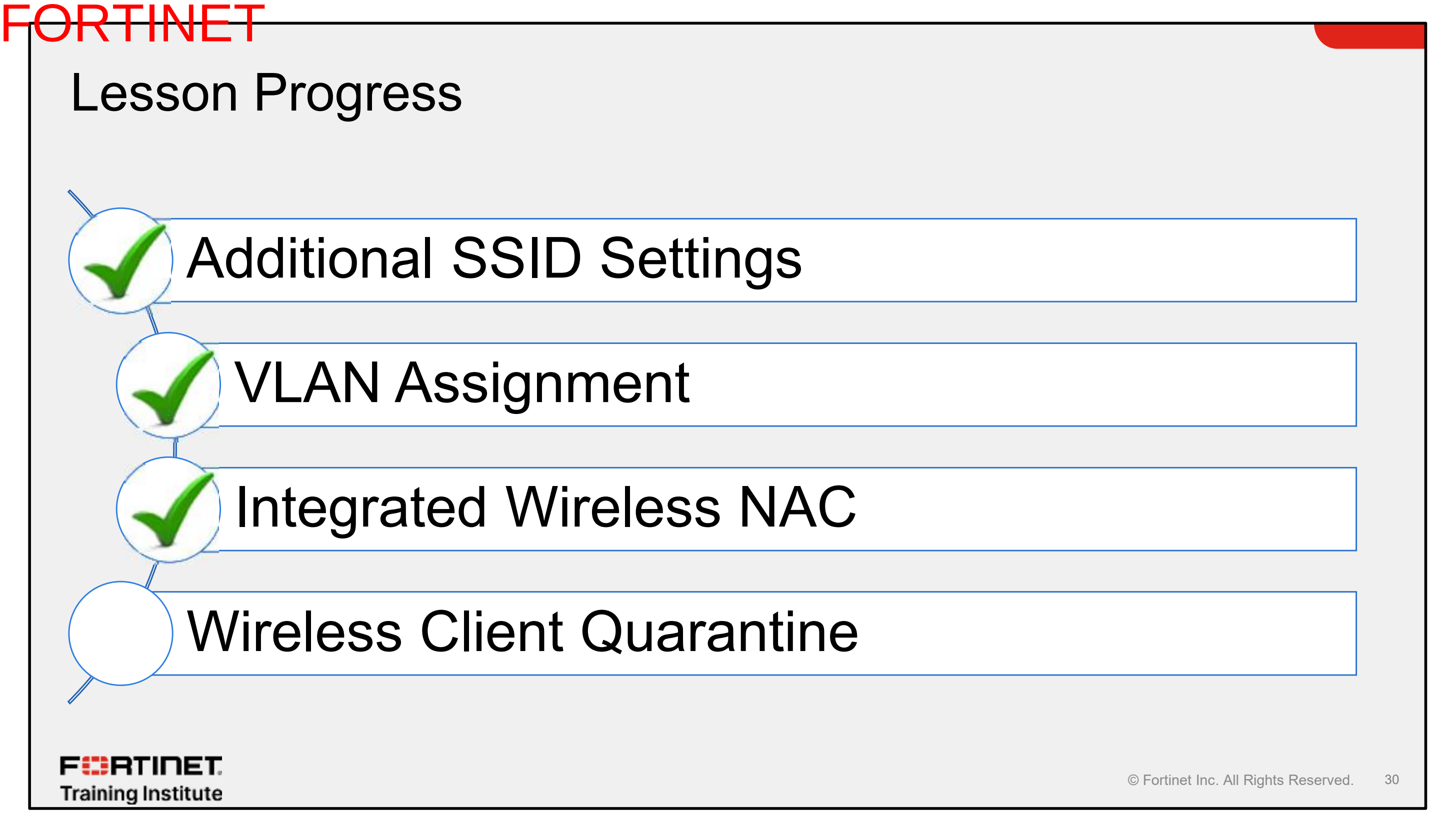
You can see the list of matched devices on the FortiGate GUI and CLI. By navigating to **NAC Policies**, you can switch the view to display devices that matched NAC policies for both FortiSwitch and FortiAP.

Other CLI commands, such as `wlac_hlp -c sta-nac`, display the information about the device that matched the wireless NAC policies in particular. You can also use `wlac_hlp -c nacprof` to display configured wireless NAC profiles, each with its onboarding VLAN reference.



Knowledge Check

1. How many VLANs are required to configure a wireless NAC policy?
   - A. One
   - ✓ B. Two



Lesson Progress

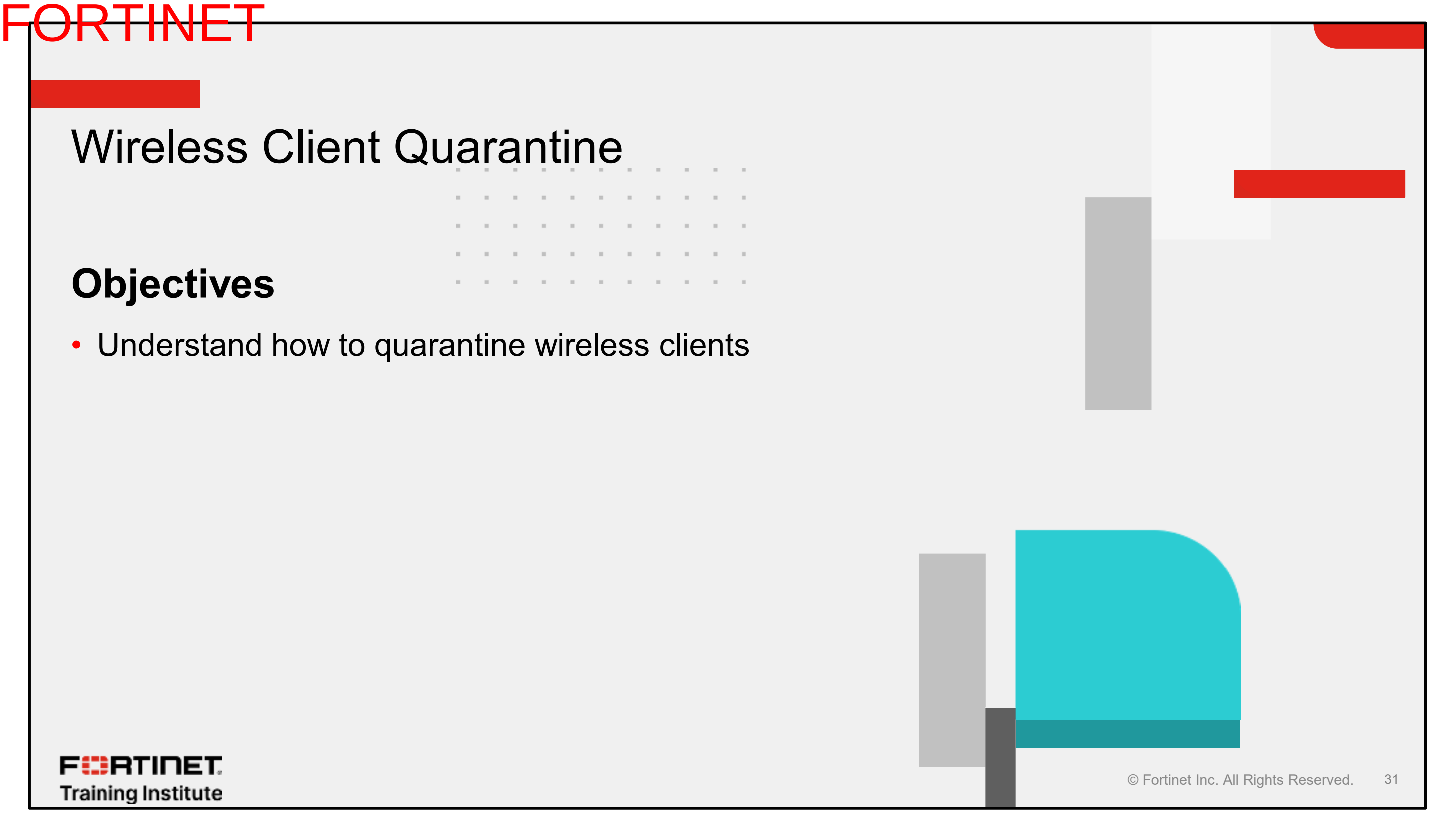
- ✓ Additional SSID Settings
- ✓ VLAN Assignment
- ✓ Integrated Wireless NAC
- ○ Wireless Client Quarantine

FORTINET Training Institute

30

Good job! You now understand how wireless NAC works.

Now, you will learn how to quarantine wireless clients automatically and manually.



Wireless Client Quarantine

Objectives

- Understand how to quarantine wireless clients

FORTINET
Training Institute

31

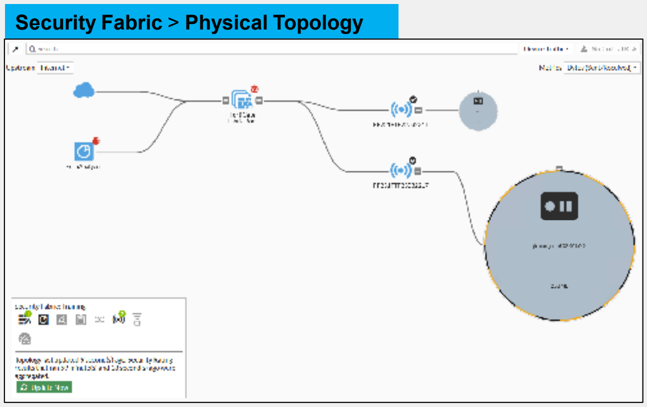
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding how to quarantine wireless clients, you can protect your network from wireless clients that are compromised.

Automated Response—Quarantine

- The Security Fabric allows multiple devices to share and leverage information
- If a device fails an IOC check, the entire fabric can react automatically
- How it works
  - A device is detected as compromised by one element of the Security Fabric
  - Switches and APs can automatically quarantine the device at the access layer
- Why it's important
  - Compromised IoT devices are no longer a threat to the wider network
  - Guest devices (if infected) will be dealt with automatically

Security Fabric > Physical Topology



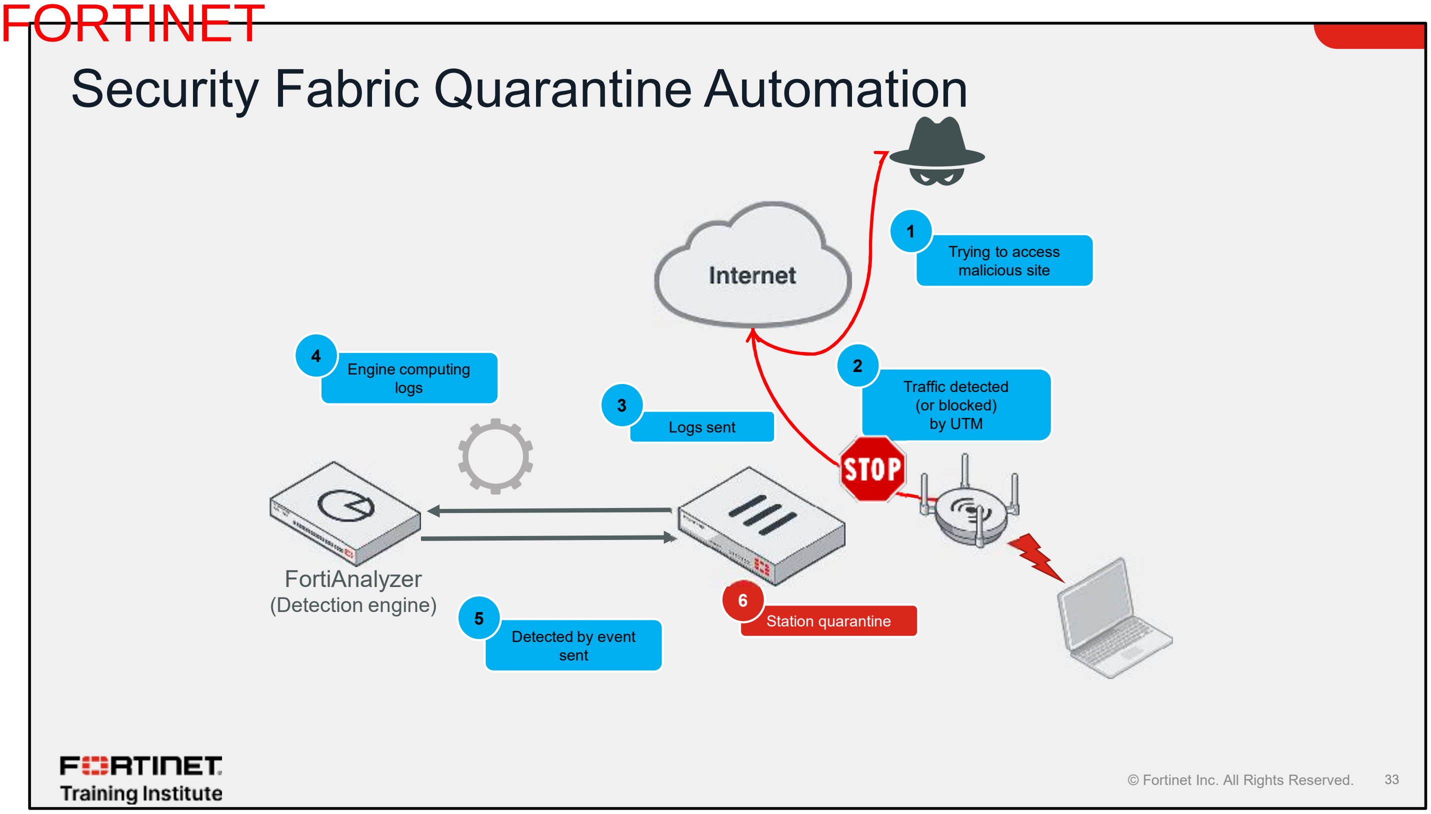
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

The Security Fabric allows you to detect and control compromised hosts, regardless of whether they are connected wirelessly or through a wired connection.

If a device fails an indicator of compromise (IOC) check, that device is considered as compromised and the entire Security Fabric can respond by placing the device in quarantine. Quarantining the device it prevents it from becoming a threat to the wider network.

Compromised Internet of Things (IoT) devices will be isolated. Any other types of devices, such as a guest device, will also be isolated when they become compromised, but these devices will have the option to remediate themselves, if required.



Security Fabric Quarantine Automation

1 Trying to access malicious site

2 Traffic detected (or blocked) by UTM

3 Logs sent

4 Engine computing logs

5 Detected by event sent

6 Station quarantine

33

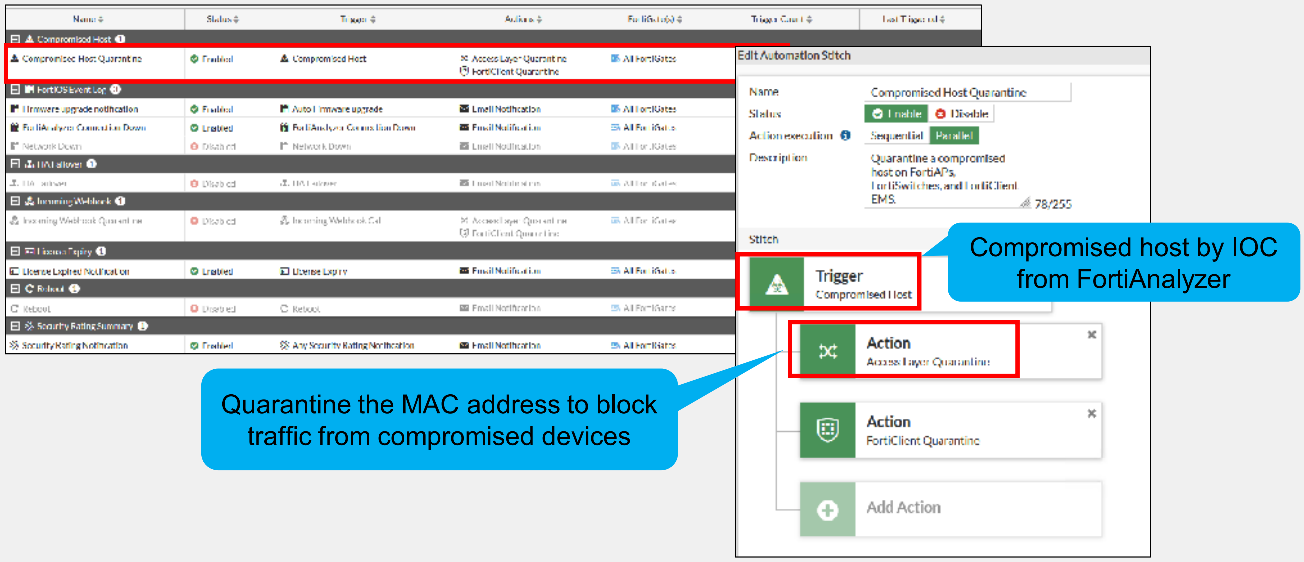
Known and unknown threat information is easily and efficiently shared among all elements and locations within the Security Fabric. User-defined automation on FortiGate can be used to quarantine compromised hosts; a process that can be strengthened by adding IOC services from FortiAnalyzer.

This slide shows the flow of events that occur when IOC and quarantine automation are combined to detect compromised workstations and place them in quarantine. The flow of events is as follows:

1. A workstation attempts to access content that is considered a security risk, such as a malicious website.
2. FortiGate blocks access to the site, based on the firewall policy defined with a web filter profile.
3. FortiGate sends a log record to FortiAnalyzer regarding the violation committed.
4. FortiAnalyzer processes the logs using information from the IOC services.
5. ForitAnalyzer determines a security risk verdict and sends that verdict back to FortiGate.
6. A user-defined automation quarantines the compromised workstation and places it in isolation.

Security Fabric Automation Stitch

Security Fabric > Automation



Name	Status	Trigger	Actions	FortiGate(s)	Trigger Count	Last Triggered
Compromised Host 1						
Compromised Host Quarantine	Enabled	Compromised Host	Access Layer Quarantine FortiClient Quarantine	All FortiGates		
FortiOS Event Log 3						
Firmware upgrade notification	Enabled	Auto Firmware upgrade	Email Notification	All FortiGates		
FortiAnalyzer Connection Down	Enabled	FortiAnalyzer Connection Down	Email Notification	All FortiGates		
Network Down	Disabled	Network Down	Email Notification	All FortiGates		
HA Failover 1						
HA Failover	Disabled	HA Failover	Email Notification	All FortiGates		
Incoming Webhook 1						
Incoming Webhook Quarantine	Disabled	Incoming Webhook Call	Access Layer Quarantine FortiClient Quarantine	All FortiGates		
License Expiry 1						
License Expired Notification	Enabled	License Expiry	Email Notification	All FortiGates		
Reboot 1						
Reboot	Disabled	Reboot	Email Notification	All FortiGates		
Security Rating Summary 1						
Security Rating Notification	Enabled	Any Security Rating Notification	Email Notification	All FortiGates		

Edit Automation Stitch

Name: Compromised Host Quarantine
Status: ● Enable ○ Disable
Action execution: Sequential [✓ Parallel]
Description: Quarantine a compromised host on FortiAPs, FortiSwitches, and FortiClient EMS. 78/255

Stitch

Trigger — Compromised Host
Action — Access Layer Quarantine
Action — FortiClient Quarantine
Add Action

Compromised host by IOC from FortiAnalyzer

Quarantine the MAC address to block traffic from compromised devices

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

Compromised wireless hosts are treated in the same way as compromised wired hosts. FortiAnalyzer identifies them using threat detection services, and then sends the IOC verdict to the root FortiGate of the Security Fabric group.

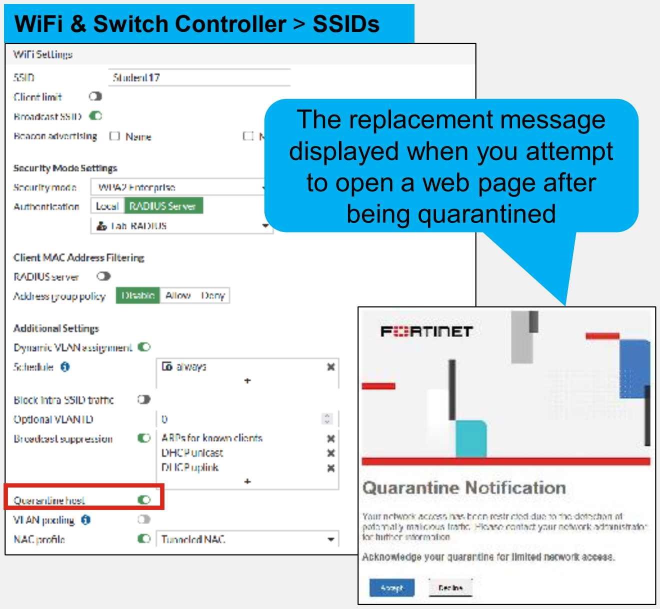
If an automation stitch is configured for compromised hosts, then that can be also be implemented.

The IOC verdict assigned to a compromised host triggers the actions specified in the automation stitch. **Access Layer Quarantine** is a layer 2 action that places the host machine in isolation.

You can configure automation stitches at each FortiGate or apply a device configuration if a FortiManager manages FortiGate. You apply the setting on a per-device basis, it cannot be applied using a template.

Integrated Wireless Quarantine

- Wireless clients can be quarantined
  - Automatically using security automation
  - Manually
- Only works with tunnel mode SSIDs
- Mandatory to be in a Security Fabric
- When quarantine is enabled on an SSID, the required resources are automatically created
  - Quarantine soft switch
  - Quarantine interface
  - Default captive portal
- No quarantine firewall policy by default
- Can filter on a FortiGate level only



WiFi & Switch Controller > SSIDs

WiFi Settings
SSID: Student17
Client limit: ○
Broadcast SSID: ●
Beacon advertising: □ Name □ N

Security Mode Settings
Security mode: WPA2 Enterprise
Authentication: Local | RADIUS Server
Lab RADIUS

Client MAC Address Filtering
RADIUS server: ○
Address group policy: Disable | Allow | Deny

Additional Settings
Dynamic VLAN assignment: ●
Schedule: always
Block Intra SSID traffic: ○
Optional VLAN ID: 0
Broadcast suppression: ● ARPs for known clients, DHCP unicast, DHCP uplink
Quarantine host: ●
VLAN pooling: ○
NAC profile: ● Tunneled NAC

The replacement message displayed when you attempt to open a web page after being quarantined

Quarantine Notification

Your network access has been restricted due to the detection of potentially malicious traffic. Please contact your network administrator for further information.

Acknowledge your quarantine for limited network access.

The quarantine process for wireless clients is very similar to wired clients; however the configuration is slightly different.

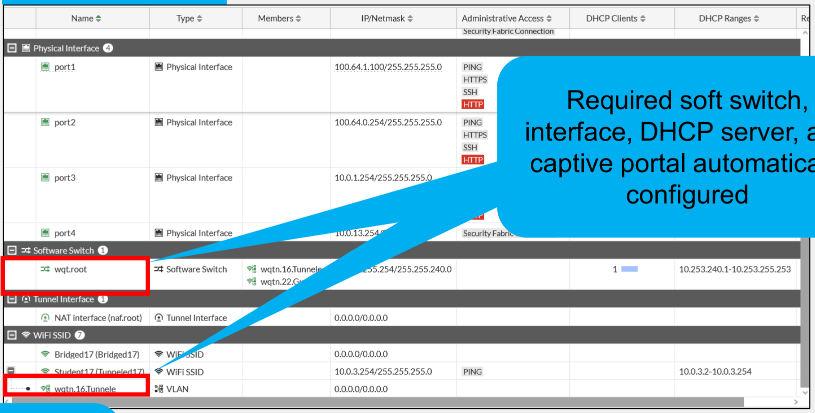
Note that it is currently possible to apply a quarantine to tunnel mode SSIDs only. For correct endpoint analysis, the APs and FortiGate have to be in the Security Fabric together with FortiAnalyzer.

You can enable quarantine on the SSID. When quarantine is enabled, FortiGate automatically creates a soft switch and interface, together with a captive portal. You create all of these features on FortiGate. FortiSwitch is not required. By default, no policies allow quarantined devices access to the internet. Note that security automation can occur only at the FortiGate level, and not at the AP level.

After they are configured, wireless clients can be automatically quarantined using the same Security Fabric automation stitches as used for wired clients. Clients that are quarantined are placed in their own isolated VLAN and then presented with a captive portal informing them that they are now isolated. You can configure this captive portal in the same way as any other captive portal, to give users information on how to remediate their device.

Integrated Wireless Quarantine (Contd)

Network > Interfaces

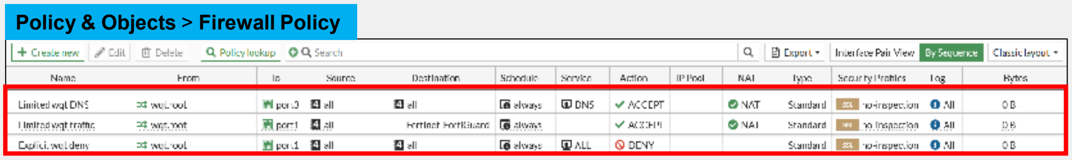


	Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
					Security Fabric Connection		
Physical Interface 4							
	port1	Physical Interface		100.64.1.100/255.255.255.0	PING HTTPS SSH HTTP		
	port2	Physical Interface		100.64.0.254/255.255.255.0	PING HTTPS SSH HTTP		
	port3	Physical Interface		10.0.1.254/255.255.255.0			
	port4	Physical Interface		10.0.13.254/	Security Fabric		
Software Switch 1							
	wqt.root	Software Switch	wqtn.16.Tunnele wqtn.22.G	55.254/255.255.240.0		1	10.253.240.1-10.253.255.253
Tunnel Interface 1							
	NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0			
WiFi SSID 7							
	Bridged17 (Bridged17)	WiFi SSID		0.0.0.0/0.0.0.0			
	Student17 (Tunneled17)	WiFi SSID		10.0.3.254/255.255.255.0	PING		10.0.3.2-10.0.3.254
	wqtn.16.Tunnele	VLAN		0.0.0.0/0.0.0.0			

Required soft switch, interface, DHCP server, and captive portal automatically configured

Example policies manually created to allow limited access to enable remediation

Policy & Objects > Firewall Policy

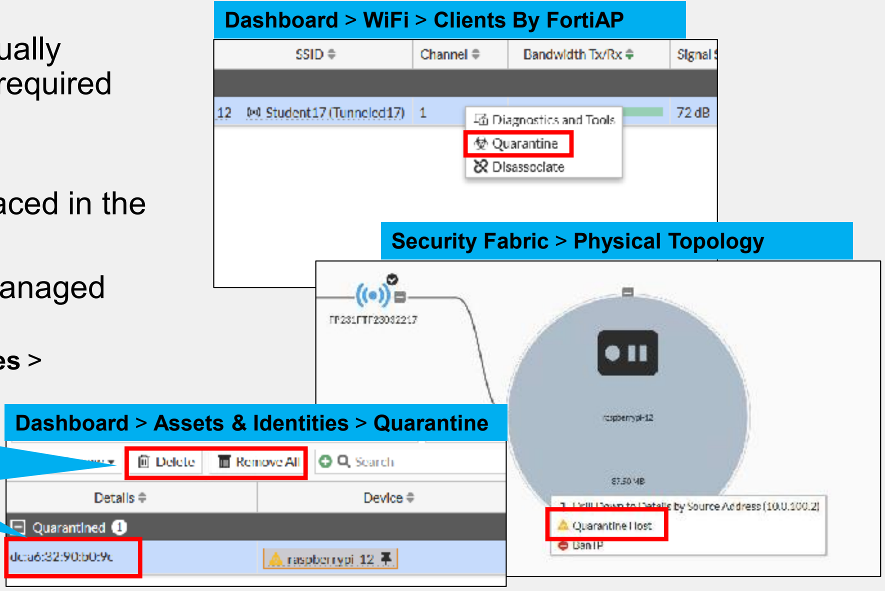


Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log	Bytes
Limited wqt DNS	wqt.root	port3	all	all	always	DNS	ACCEPT		NAT	Standard	SSL no-inspection	All	0 B
Limited wqt traffic	wqt.root	port1	all	Fortinet FortiGuard	always		ACCEPT		NAT	Standard	SSL no-inspection	All	0 B
Explicit wqt deny	wqt.root	port1	all	all	always	ALL	DENY			Standard	SSL no-inspection	All	0 B

Enabling a quarantine *automatically* creates a soft switch with a range of private IP addresses, together with a system DHCP server. It also creates a captive portal, and then creates a sub-interface under the quarantined wireless network. If you want wireless clients to have access to the internet to enable them to update themselves and/or install required software, you will need to configure a set of policies to allow limited access to the resources that are required. Typically, this requires DNS and specific HTTP/S access to resources that host the required remediation files.

Manual Client Quarantine

- Wireless clients can be manually quarantined on FortiGate, if required
    - Security Fabric
    - FortiView
- Quarantined hosts will be placed in the quarantined VLAN
- Quarantined hosts can be managed from:
    - **Dashboard** > **Users & Devices** > **Quarantine**

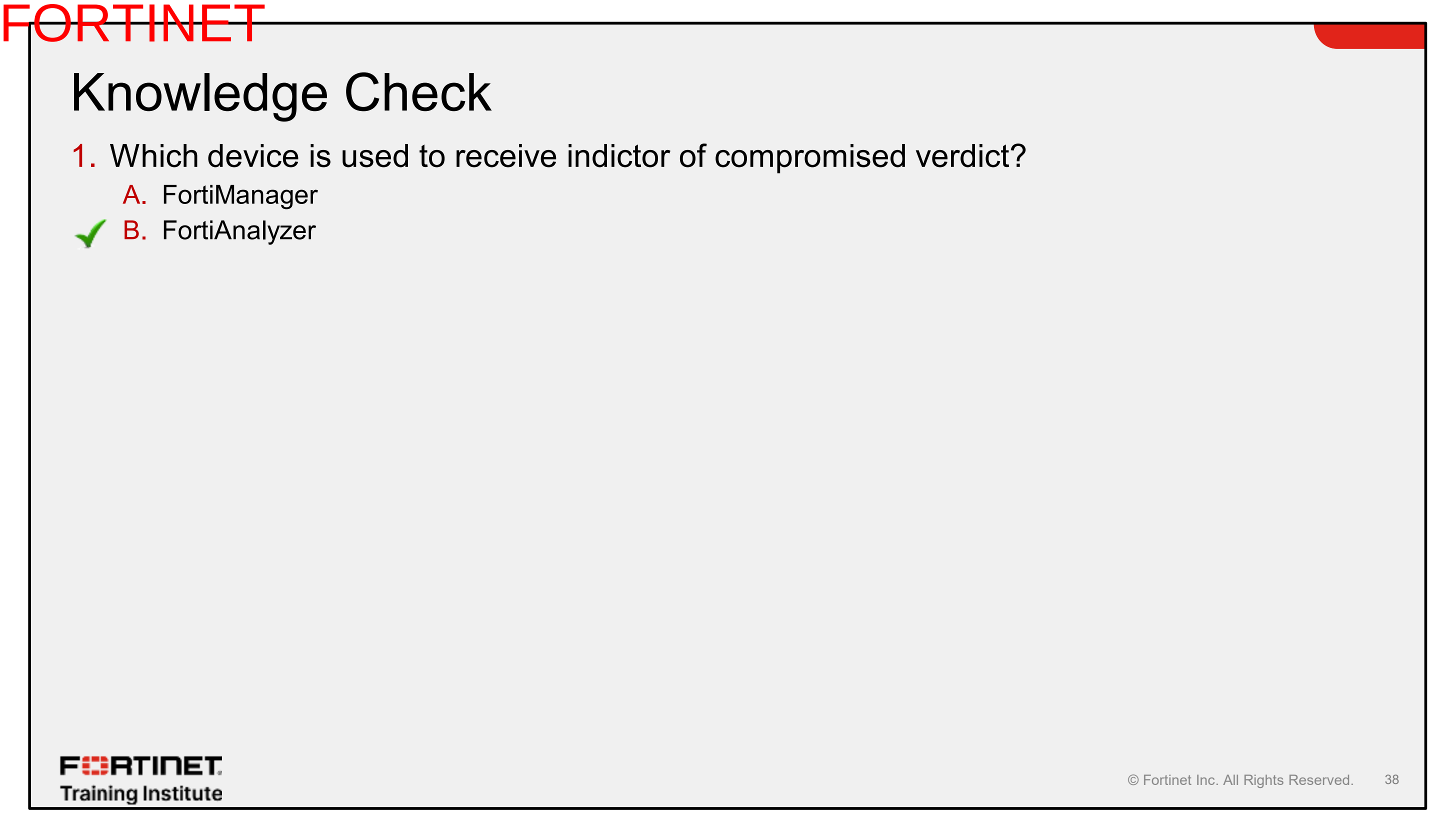


You can remove all quarantined devices or remove one device at a time

37

You can manually quarantine wireless clients on the Security Fabric or on FortiView.

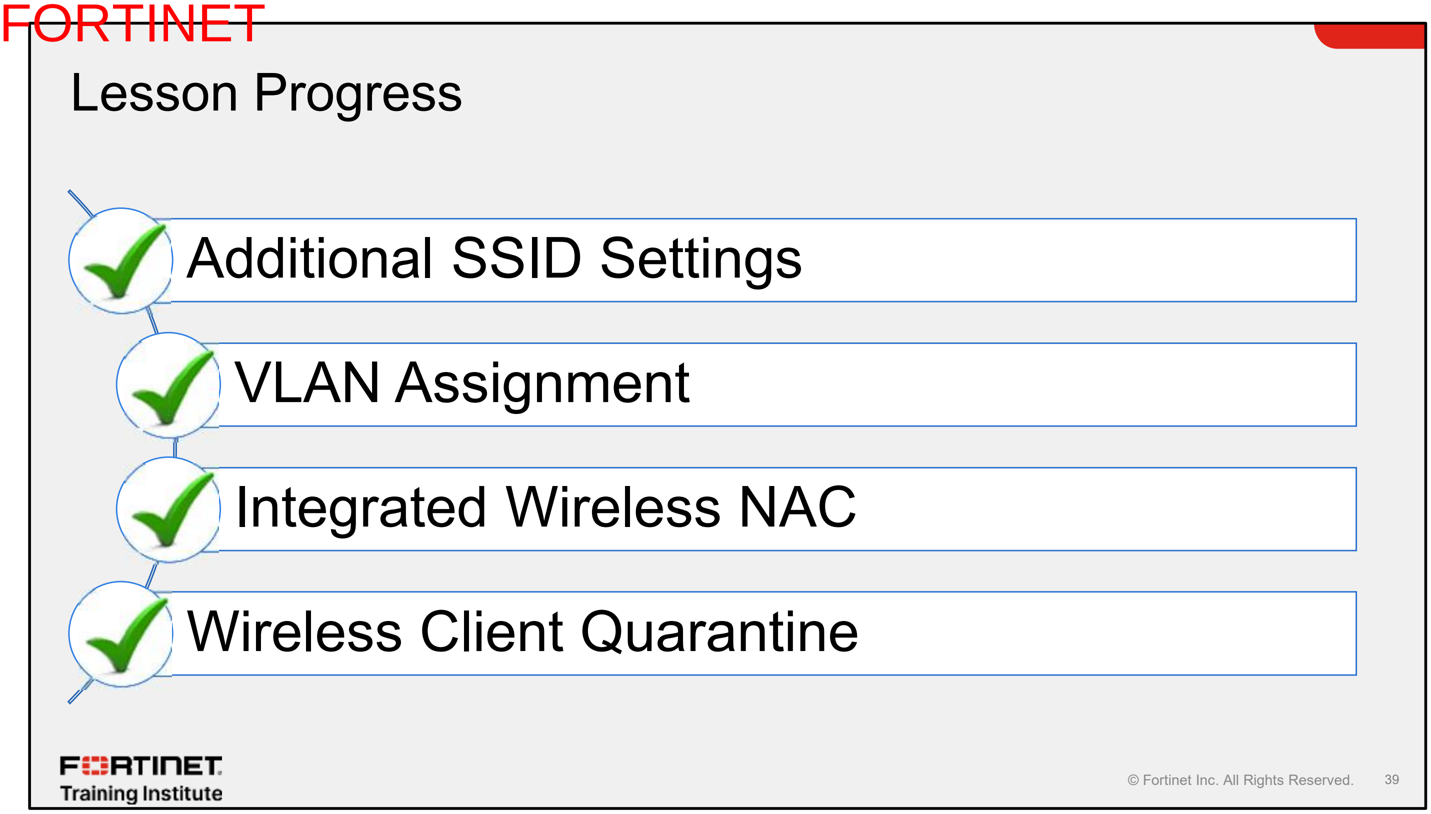
You can manage any hosts that are currently quarantined, or release hosts from quarantine using the **Quarantine** dashboard widget.



Knowledge Check

1. Which device is used to receive indictor of compromised verdict?
   - A. FortiManager
   - ✓ B. FortiAnalyzer

38



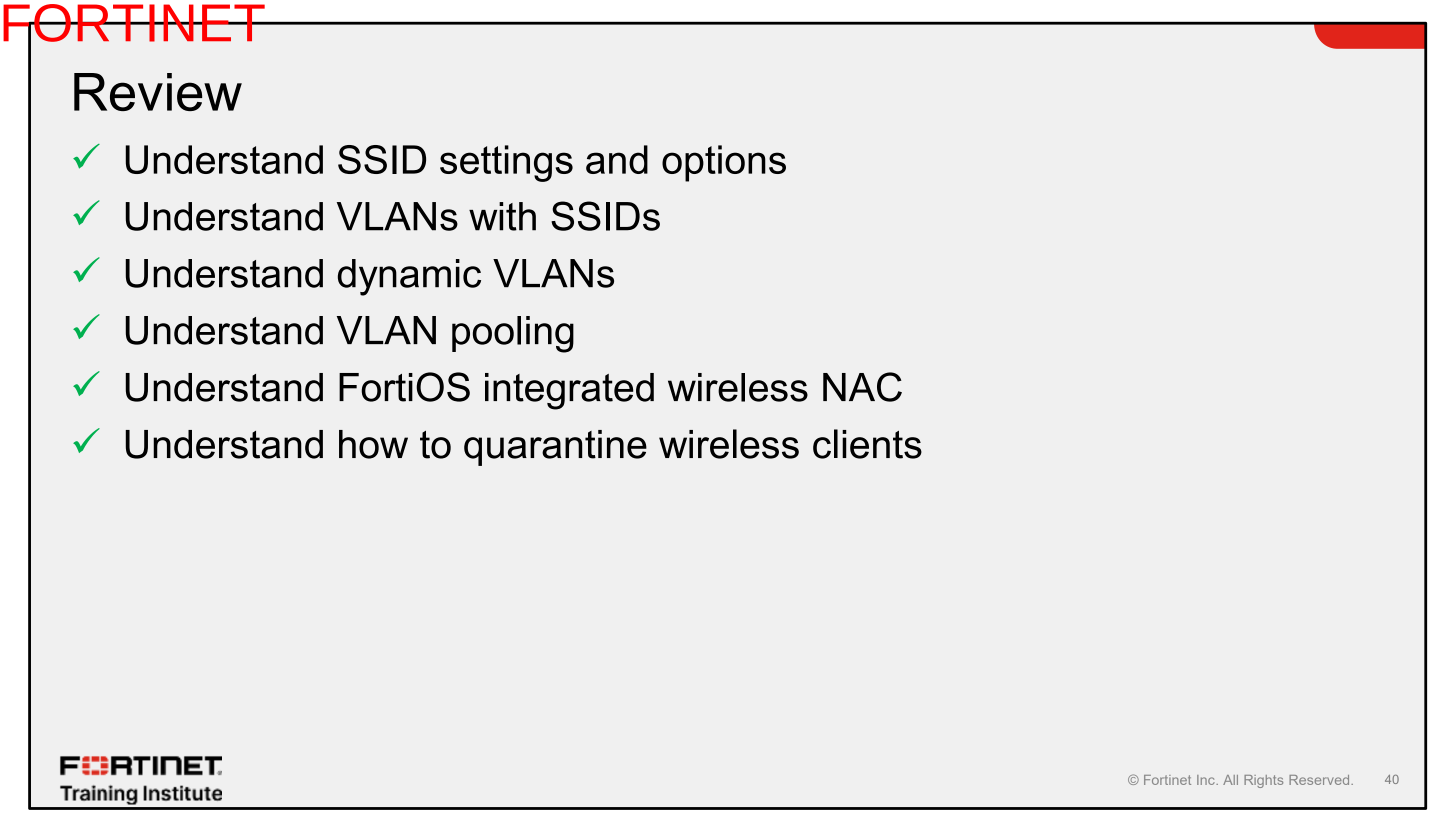
Lesson Progress

- ✓ Additional SSID Settings
- ✓ VLAN Assignment
- ✓ Integrated Wireless NAC
- ✓ Wireless Client Quarantine

FORTINET
Training Institute

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



Review

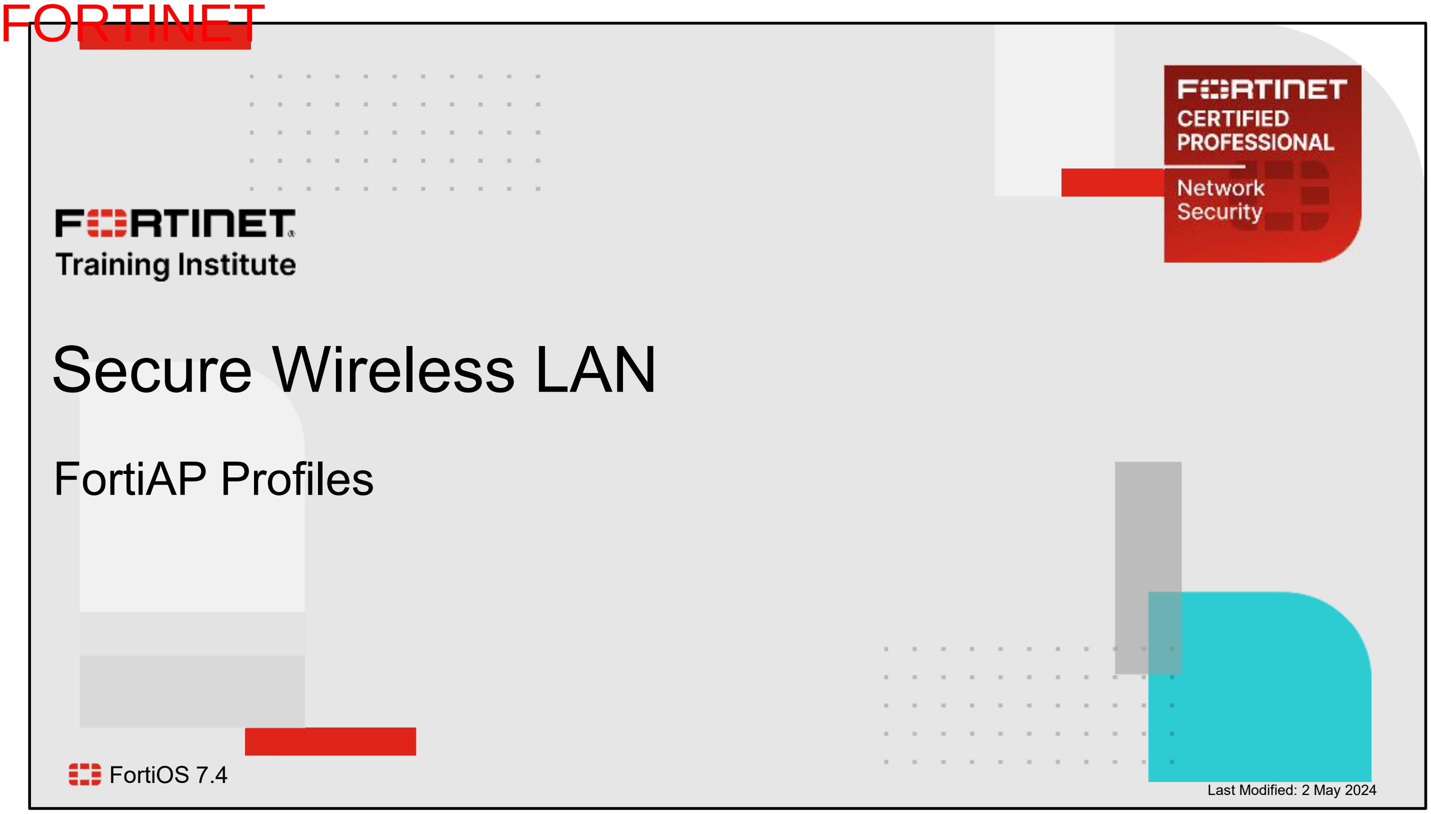
- ✓ Understand SSID settings and options
- ✓ Understand VLANs with SSIDs
- ✓ Understand dynamic VLANs
- ✓ Understand VLAN pooling
- ✓ Understand FortiOS integrated wireless NAC
- ✓ Understand how to quarantine wireless clients

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to apply wireless security using the FortiOS wireless controller.



FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL Network Security

Secure Wireless LAN

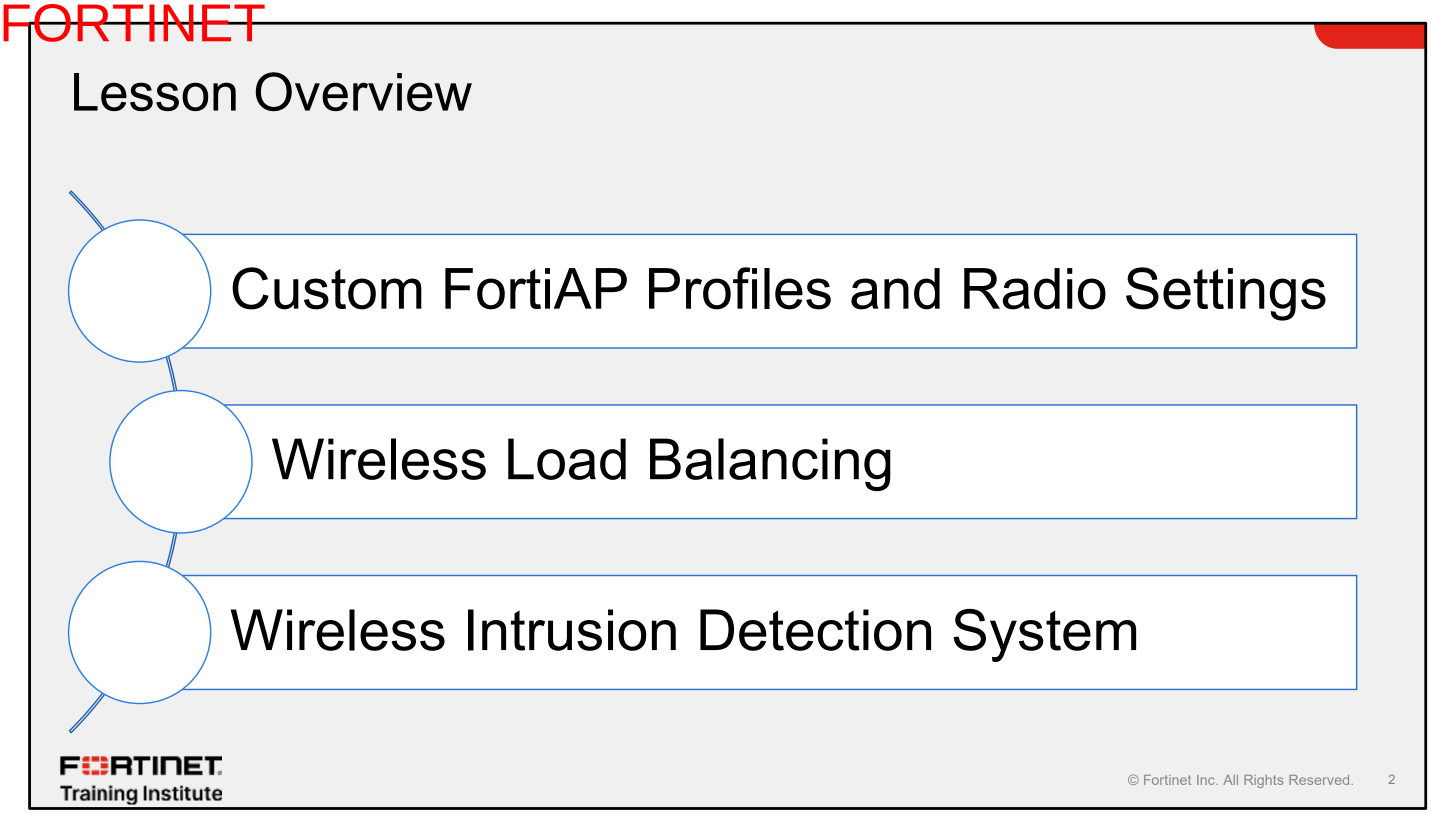
FortiAP Profiles

FortiOS 7.4

Last Modified: 2 May 2024

In this lesson, you will learn about the wireless technology concepts that you must know to understand Wi-Fi, and wireless technologies in general.

You will also learn how to plan your network for the best wireless signal coverage.



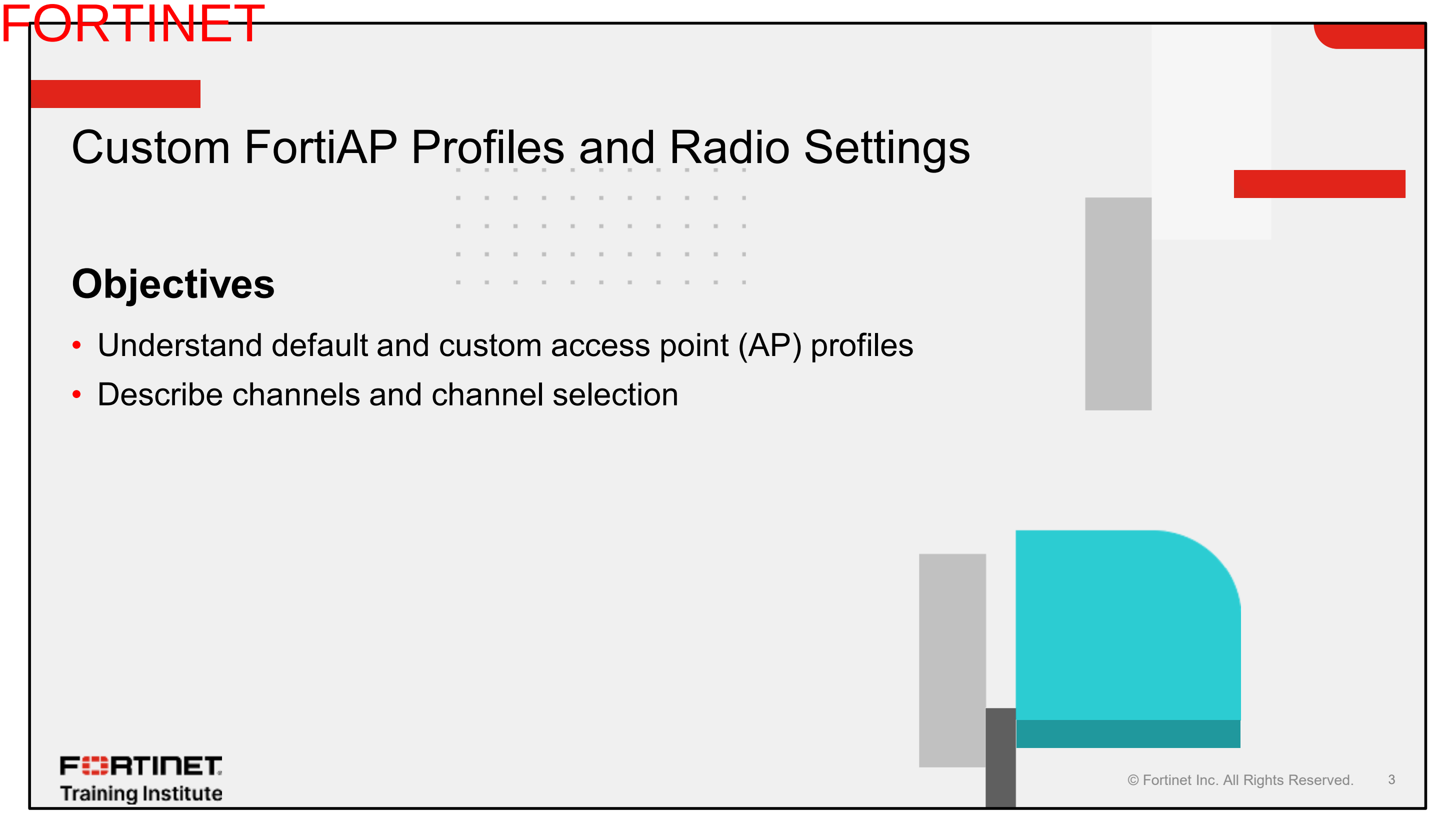
Lesson Overview

- Custom FortiAP Profiles and Radio Settings
- Wireless Load Balancing
- Wireless Intrusion Detection System

FORTINET Training Institute

2

In this lesson, you will learn about the topics shown on this slide.



Custom FortiAP Profiles and Radio Settings

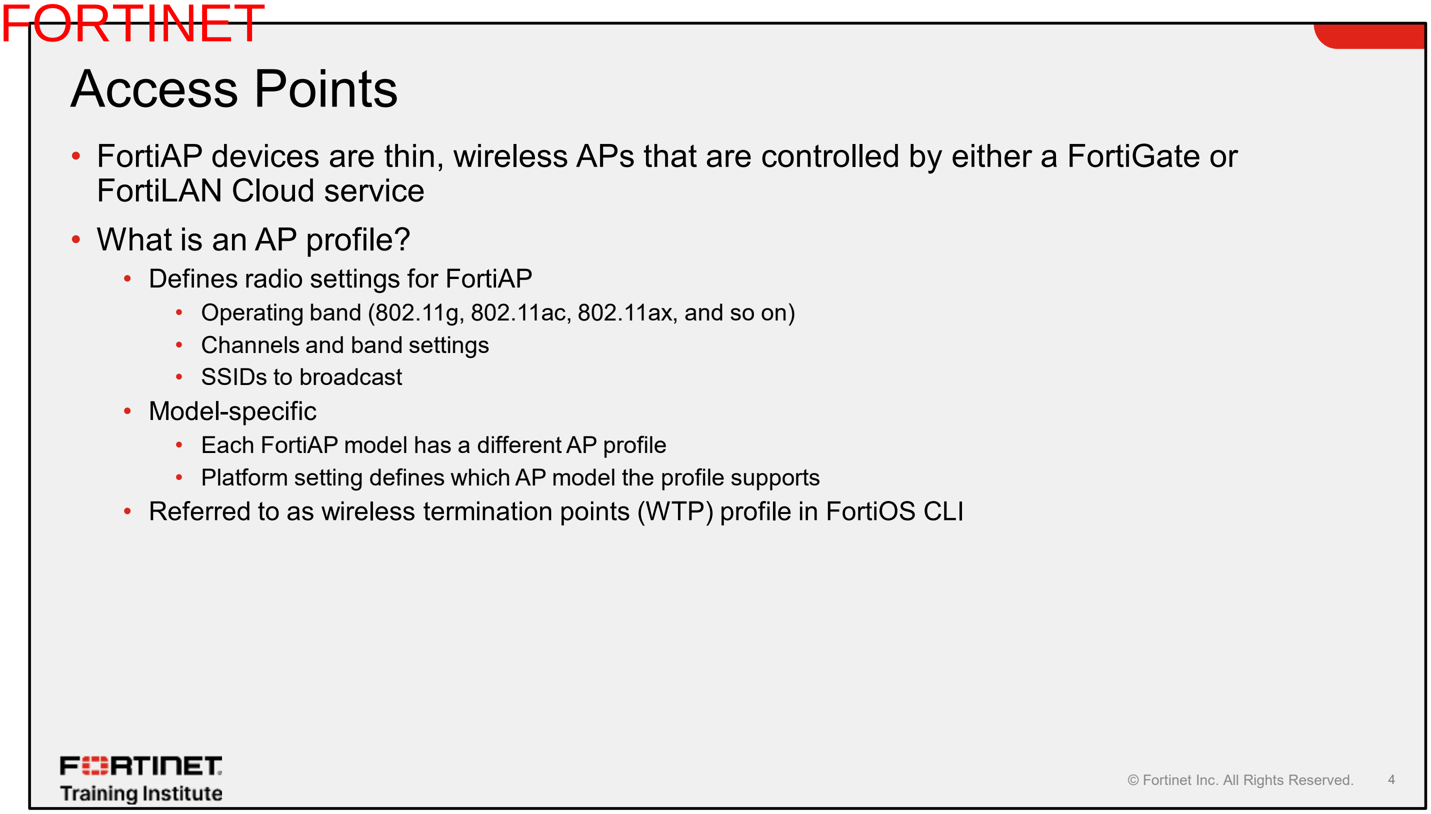
Objectives

- Understand default and custom access point (AP) profiles
- Describe channels and channel selection

FORTINET
Training Institute

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring custom FortiAP profiles and radio settings, you will be able to provision FortiAP devices more effectively.



Access Points

- FortiAP devices are thin, wireless APs that are controlled by either a FortiGate or FortiLAN Cloud service
- What is an AP profile?
  - Defines radio settings for FortiAP
    - Operating band (802.11g, 802.11ac, 802.11ax, and so on)
    - Channels and band settings
    - SSIDs to broadcast
  - Model-specific
    - Each FortiAP model has a different AP profile
    - Platform setting defines which AP model the profile supports
  - Referred to as wireless termination points (WTP) profile in FortiOS CLI

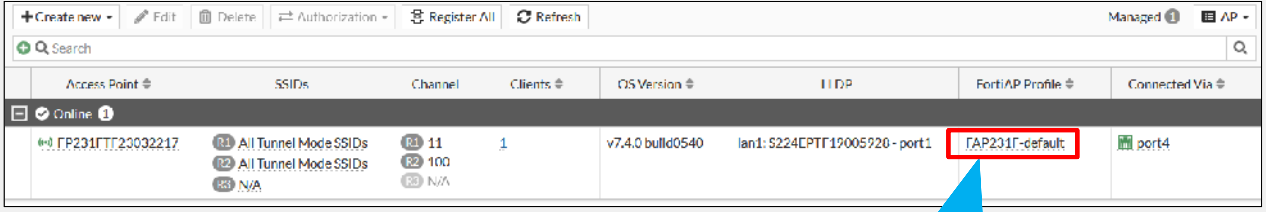
FortiAP devices are thin APs that require a wireless controller, which can be a FortiGate device or the FortiLAN Cloud service, to deploy and manage a wireless network. FortiGate uses AP profiles to push all settings that are required to manage and deploy a wireless network using FortiAP.

A FortiAP profile defines configuration settings for an AP including operating band, channels, SSID networks, and so on. The FortiAP profile specifies for the FortiGate the type of hardware that a FortiAP device uses. This information is required for FortiGate when pushing configuration parameters to the managed AP. If the hardware of the AP does not support specific settings, FortiGate removes those settings for FortiAP. For example, if a FortiAP device contains two radios, FortiGate can use the first radio to provide 802.11ac and the second radio to provide rogue AP detection from the FortiAP profile.

Access Point Profile

- FortiGate assigns a default FortiAP profile to newly discovered APs
- FortiAP profile is automatically assigned
  - Default profile is named based on the AP model, follow by '-default'
- FortiGate must authorize the FortiAP device before it pushes any configuration settings to the AP

WiFi & Switch Controller > Managed FortiAPs



Access Point	SSIDs	Channel	Clients	OS Version	LLDP	FortiAP Profile	Connected Via
FP231FTF23032217	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 11 R2 100 R3 N/A	1	v7.4.0 build0540	lan1: S224EPTF19005920 - port1	FAP231F-default	port4

The model default FortiAP profile assigned

By default, when a FortiAP device is connected to a FortiGate interface on which the Security Fabric is enabled, FortiOS tries to discover the FortiAP device. Upon discovery of the FortiAP device, FortiGate automatically assigns it a default profile, based on the FortiAP hardware model.

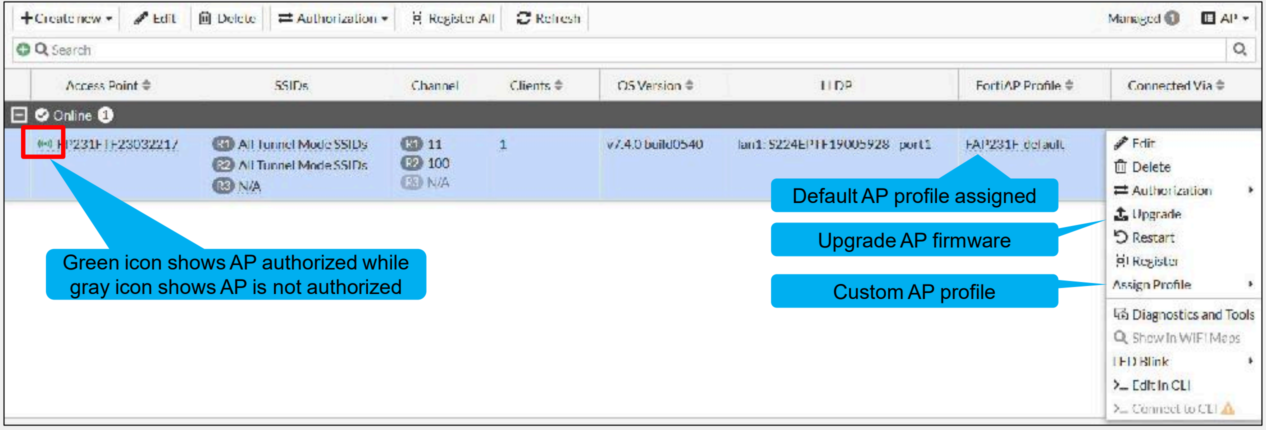
You can also create and select a different profile, if needed. As discussed, the AP profile defines all the settings that are required to manage and deploy a wireless network.

FortiAP remains unauthorized on the **Managed FortiAPs** tab and no settings are pushed to FortiAP until FortiGate authorizes it. Once authorized, the status changes to a green icon, which means that a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel is established between the controller and AP.

Authorized FortiAP Devices

- After an AP is authorized:
  - Change status of FortiAP
  - FortiAP firmware upgrade
  - Assign custom profile

WiFi & Switch Controller > Managed FortiAPs



Access Point	SSIDs	Channel	Clients	OS Version	LLDP	FortiAP Profile	Connected Via
P231FTF23032217	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 11 R2 100 R3 N/A	1	v7.4.0 build0540	lan1: S224EPTF19005928 port1	FAP231F-default	

Default AP profile assigned

Upgrade AP firmware

Custom AP profile

Green icon shows AP authorized while gray icon shows AP is not authorized

FURTINET
Training Institute

6

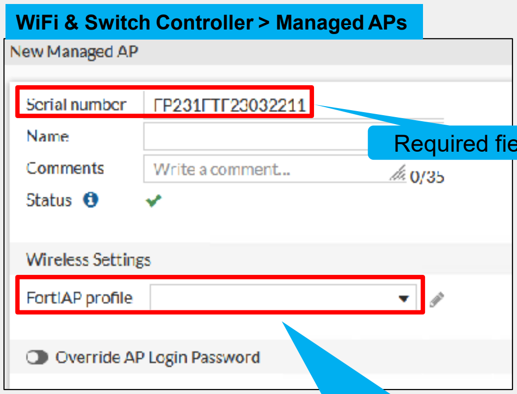
After an AP is authorized, you can perform various tasks using the FortiGate GUI. On the **Managed FortiAPs** page, you can:

- Change the status of an AP (authorized to deauthorized)
- Upgrade AP firmware
- Change assigned AP profile
- Restart FortiAP
- Telnet to FortiAP CLI to execute commands directly on the AP

You might also see the message **A new Firmware version is available**. This indicates that you can upgrade the FortiAP version. You can right-click the FortiAP device in the list and select **Upgrade**. FortiOS will automatically find the appropriate firmware for the AP and upgrade it. This option requires you to register FortiAP on the Fortinet support site and have a valid support contract.

Preauthorizing FortiAP Devices

WiFi & Switch Controller > Managed APs



New Managed AP

Serial number FP231FTF23032211

Name

Comments Write a comment... 0/35

Status ✓

Wireless Settings

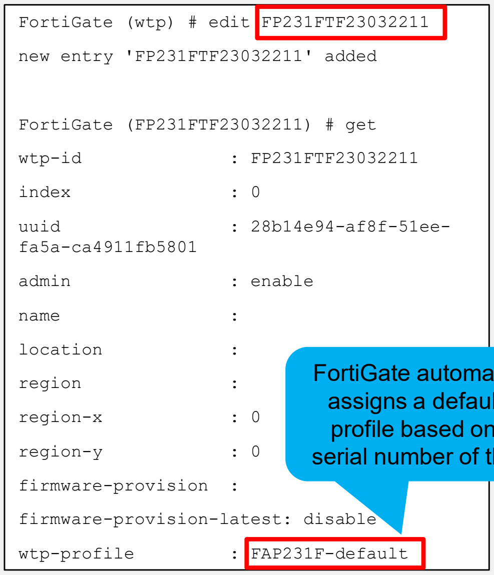
FortiAP profile

Override AP Login Password

Required field

Select the preconfigured FortiAP profile here otherwise default profile is assigned

Preauthorizing AP using CLI



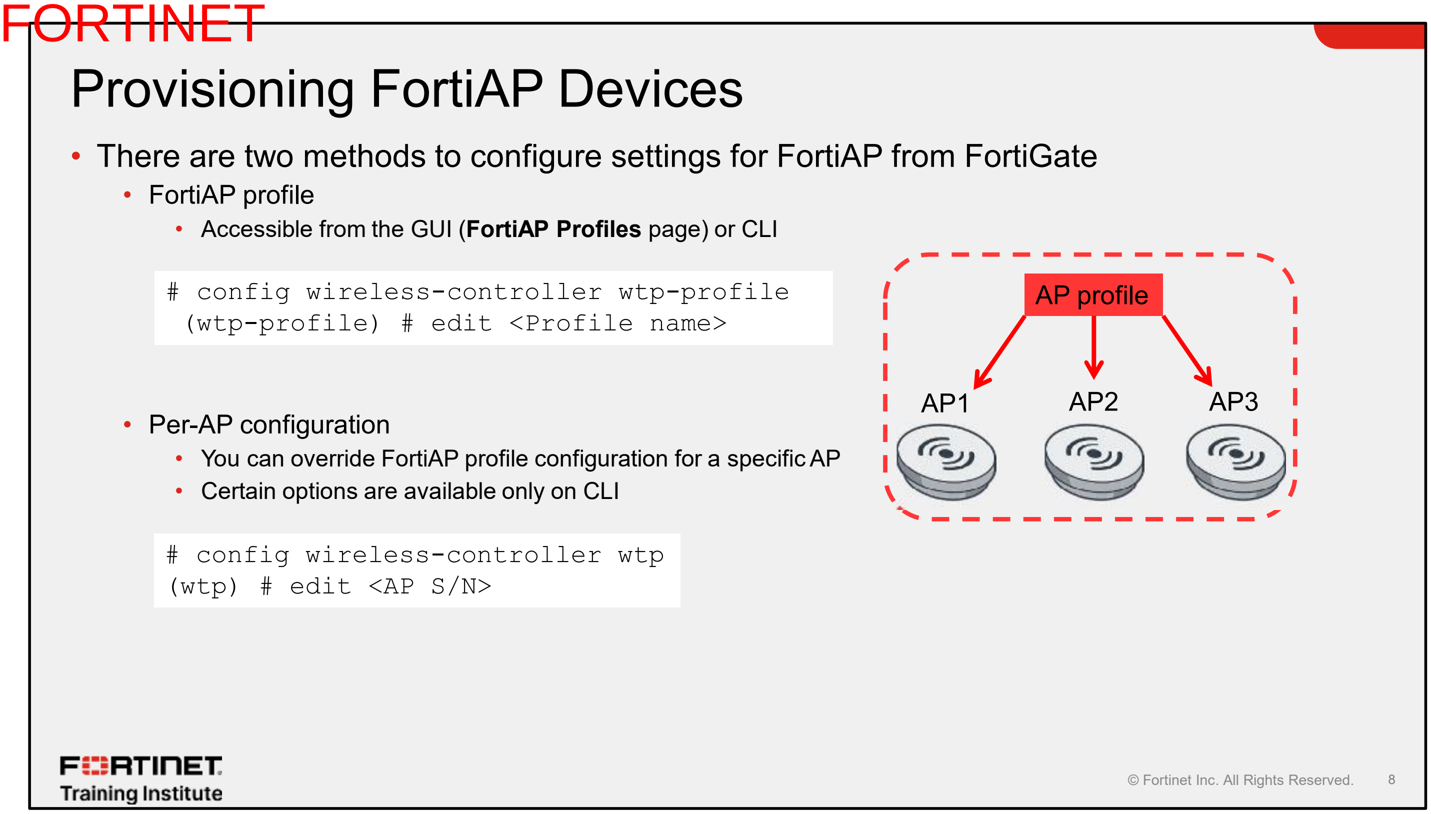
```
FortiGate (wtp) # edit FP231FTF23032211
new entry 'FP231FTF23032211' added

FortiGate (FP231FTF23032211) # get
wtp-id                  : FP231FTF23032211
index                   : 0
uuid                    : 28b14e94-af8f-51ee-
fa5a-ca4911fb5801
admin                   : enable
name                    :
location                :
region                  :
region-x                : 0
region-y                : 0
firmware-provision      :
firmware-provision-latest: disable
wtp-profile             : FAP231F-default
```

FortiGate automatically assigns a default AP profile based on the serial number of the AP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

FortiGate allows you to preauthorize FortiAP devices that will be added to your network. You must add all FortiAPs manually, one by one, to FortiGate using the AP serial number. You can also select available preconfigured FortiAP profiles that are compatible with the model of the hardware. If you don’t select a profile, the default FortiAP profile is assigned to the new device. After the preauthorized FortiAP devices come online and are discovered by FortiGate, FortiGate automatically authorizes them. FortiGate establishes a CAPWAP tunnel to the FortiAP devices and then pushes the configuration to them based on the assigned AP profile



Provisioning FortiAP Devices

- There are two methods to configure settings for FortiAP from FortiGate
  - FortiAP profile
    - Accessible from the GUI (**FortiAP Profiles** page) or CLI

```
# config wireless-controller wtp-profile
 (wtp-profile) # edit <Profile name>
```

  - Per-AP configuration
    - You can override FortiAP profile configuration for a specific AP
    - Certain options are available only on CLI

```
# config wireless-controller wtp
(wtp) # edit <AP S/N>
```

FORTINET Training Institute

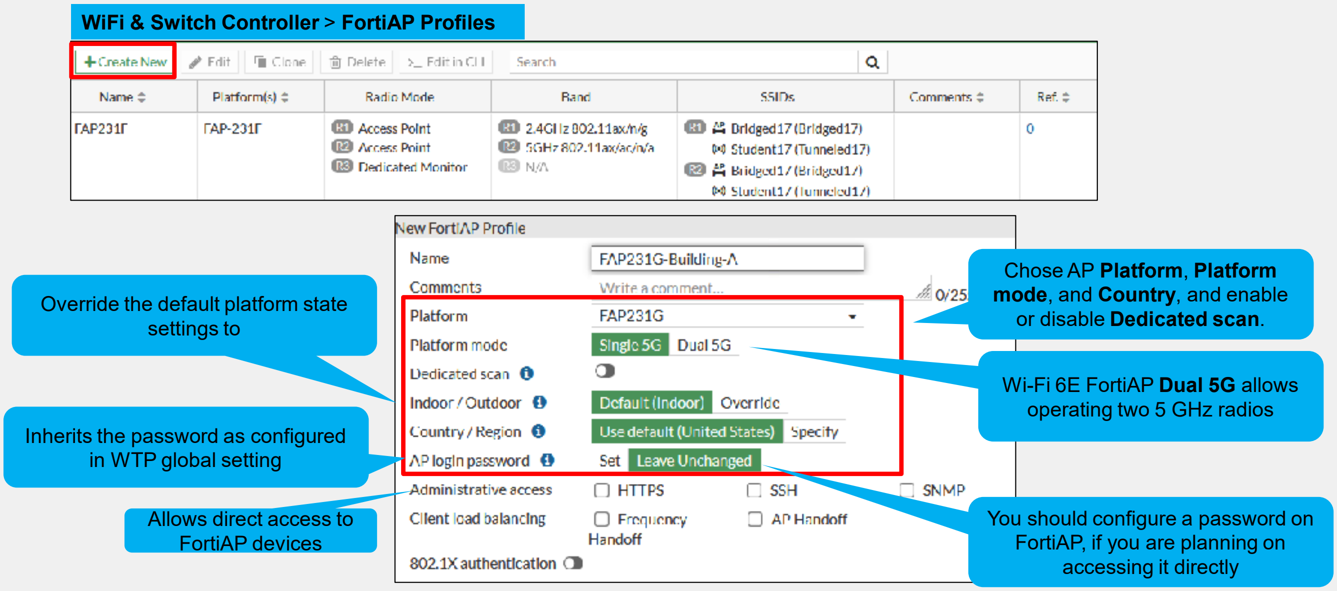
© Fortinet Inc. All Rights Reserved. 8

FortiGate automatically assigns a default AP profile to an AP when it is discovered and manually authorized. After a CAPWAP tunnel is established between FortiGate and an AP, FortiGate uses the CAPWAP control channel to push all AP profile parameters to the AP. It is important to note that you can assign an AP profile to one or multiple APs, but you cannot assign multiple profiles to one AP. All APs that use the same AP profile receive the same set of configurations from FortiGate. The AP profile includes the operating mode of the device, transmit power, and radio settings, as well as the SSID configuration that is pushed to the AP.

For more flexibility and granularity, you can override the AP profile configuration on a per-AP basis. You must still assign an AP profile to an AP but you can modify the configuration per AP. You must apply the per-AP configuration on the CLI using the following syntax:

```
# config wireless-controller wtp
# edit <AP Serial Number>
```

Custom FortiAP Profile



WiFi & Switch Controller > FortiAP Profiles

Name	Platform(s)	Radio Mode	Band	SSIDs	Comments	Ref.
FAP231F	FAP-231F	R1 Access Point R2 Access Point R3 Dedicated Monitor	R1 2.4GHz 802.11ax/n/g R2 5GHz 802.11ax/ac/n/a R3 N/A	R1 Bridged17 (Bridged17) Student17 (Tunneled17) R2 Bridged17 (Bridged17) Student17 (Tunneled17)		0

New FortiAP Profile

Name	FAP231G-Building-A
Comments	Write a comment... 0/255
Platform	FAP231G
Platform mode	[✓ Single 5G] Dual 5G
Dedicated scan	○
Indoor / Outdoor	[✓ Default (Indoor)] Override
Country / Region	[✓ Use default (United States)] Specify
AP login password	Set [✓ Leave Unchanged]
Administrative access	□ HTTPS □ SSH □ SNMP
Client load balancing	□ Frequency Handoff □ AP Handoff
802.1X authentication	○

Override the default platform state settings to

Inherits the password as configured in WTP global setting

Allows direct access to FortiAP devices

Chose AP **Platform**, **Platform mode**, and **Country**, and enable or disable **Dedicated scan**.

Wi-Fi 6E FortiAP **Dual 5G** allows operating two 5 GHz radios

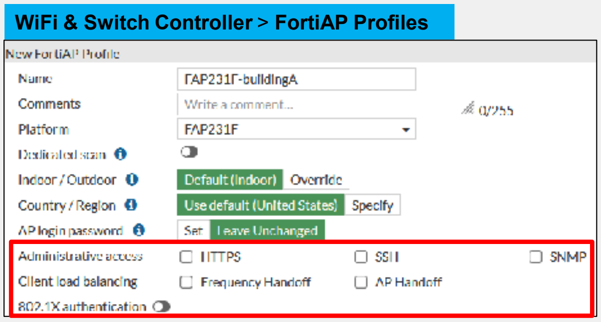
You should configure a password on FortiAP, if you are planning on accessing it directly

FortiGate allows you to configure a custom AP profile that allows you to control all the settings that are pushed to an AP. You must select the correct platform settings because these are what tell FortiGate what type of hardware the AP uses. The Wi-Fi 6 and Wi-Fi6E FortiAP platforms allow a third radio dedicated to wireless threat scanning. You can enable **Dedicated scan** to allow the third radio to collect RF analysis and wireless threat management information. You can also use background scanning using the Wireless Intrusion Detection System (WIDS) profile on either radio 1 or 2. You will learn more about WIDS later in this lesson.

Wi-Fi 6E FortiAP devices can operate two 5 GHz radios simultaneously. You can choose to operate single or dual 5 GHz radios. If you configure the **Dual 5G** operation mode, FortiAP cannot have a dedicated radio for RF and wireless scanning.

The **Country / Region** field provides RF channels available in your area. By default, the country is set to United States. Every country has different radio regulations and, to comply with these regulations, you should select the correct **Country / Region**.

Custom FortiAP Profile (Contd)



WiFi & Switch Controller > FortiAP Profiles

New FortiAP Profile

Name	FAP231F-buildingA		
Comments	Write a comment... 0/255		
Platform	FAP231F		
Dedicated scan	○		
Indoor / Outdoor	Default (Indoor) Override		
Country / Region	Use default (United States) Specify		
AP login password	Set Leave Unchanged		
Administrative access	□ HTTPS	□ SSH	□ SNMP
Client load balancing	□ Frequency Handoff	□ AP Handoff	
802.1X authentication ○			

- Can directly access FortiAP devices using HTTPS or SSH
  - Not recommended but useful in troubleshooting FortiAP issues
- FortiAP login password options:
  - **Set**: Manually configure a password
  - **Leave Unchanged**: Last configured password remains
- Can define administrator access at the FortiAP profile level or per-AP level
- Client load balancing: Frequency handoff, AP handoff
- 802.1X authentication option allows FortiAP to act as supplicant

FORTINET Training Institute

10

By default, after FortiGate authorizes and manages an AP, the AP drops all direct administrative communications on HTTPS or SSH. You can choose to enable direct access to FortiAP devices using HTTPS or SSH. You can manually push the setting to FortiAP devices, either using a FortiAP profile or by overriding the settings on a per-AP basis.

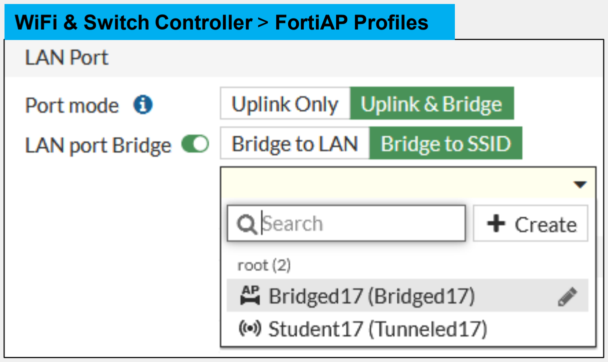
Note that if you enable administrative access using an AP profile, all APs that are using that profile inherit these settings.

Client load balancing can assist with distributing the load across APs, using either **Frequency Handoff** or **AP Handoff**.

FortiAP can act as an 802.1X supplicant to authenticate against the RADIUS server using EAP-FAST, EAP-TLS, or EAP-PEAP. This setting is for FortiAP devices connected to a switch port with 802.1X authentication enabled.

Custom FortiAP Profile (Contd)

- LAN port on some FortiAP platforms can extend wired network access
- All FortiAP models have a WAN port
  - To communicate with wireless controller
  - To communicate with FortiLAN Cloud
- FortiAP with LAN port can
  - Bridged to LAN
  - Bridged to SSID



WiFi & Switch Controller > FortiAP Profiles

LAN Port

Port mode: Uplink Only | **Uplink & Bridge**

LAN port Bridge: Bridge to LAN | **Bridge to SSID**

In the FortiAP profile, you can enable the LAN port bridge option for the desired SSID or LAN where FortiAP is connecting.

The LAN port can bridge to either a LAN or an SSID as follows:

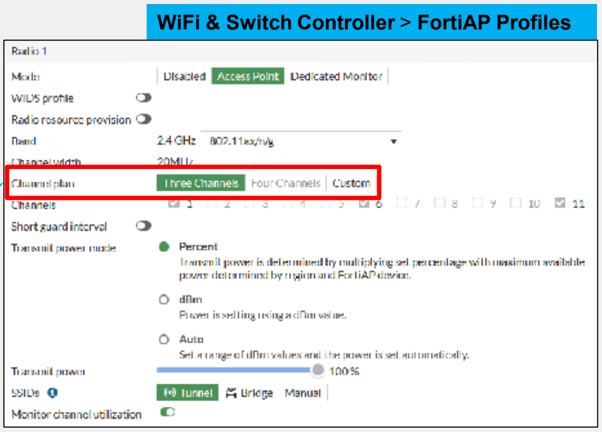
- LAN port bridge with LAN port: This option enables FortiAP to act as a hub that provides both wired and wireless network access to devices connected to the same SSID. The IP addresses for LAN clients come from the WAN directly and are typically in the same range as the AP.
- LAN port bridge with SSID: This option enables FortiAP to act as a switch that connects the wired and wireless networks on the same subnet. The IP addresses for LAN clients come from the DHCP server on the wired network connected to the wireless controller or FortiLAN Cloud.

Radio Settings in the FortiAP Profile

- Customizable settings are available for each radio, for example, Radio1, Radio2
- Wi-Fi 6 and Wi-Fi 6E FortiAP devices can operate a third radio for scanning
- Available radio settings:
  - **Mode**: **Disabled**, **Access Point**, or **Dedicated Monitor**
  - **WIDS profile**
  - **Radio resource provision**
  - **Band**:
    - 2.4 GHz: 802.11ax/n/g/b
    - 5 GHz: 802.11ax/ac/n/a
    - 6 GHz: 802.11ax
  - **Channel width**: 20, 40, 80, 160 MHz
  - **Channels**
  - **Short guard interval**
  - **Transmit power mode**
  - **Transmit power**
  - **SSIDs**
  - **Monitor channel utilization**

You can select **Three Channels** (1, 6, 11) or **Four Channels** (1, 4, 8, 11) only on the 2.4 GHz radio.

WiFi & Switch Controller > FortiAP Profiles



Radio 1

Mode: Disabled [✓ Access Point] Dedicated Monitor

WIDS profile ○

Radio resource provision ○

Band: 2.4 GHz 802.11ax/n/g ▾

Channel width: 20MHz

Channel plan: [✓ Three Channels] Four Channels Custom

Channels: ☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 □ 7 □ 8 □ 9 □ 10 ☑ 11

Short guard interval ○

Transmit power mode:
● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm
Power is setting using a dBm value.
○ Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 100%

SSIDs: [✓ Tunnel] Bridge Manual

Monitor channel utilization ●

F⁚RTINET
Training Institute

12

There are three types of radio settings on a FortiAP profile. These are predefined settings that you can set when you select a custom profile, but that you cannot modify on the GUI. The settings include:

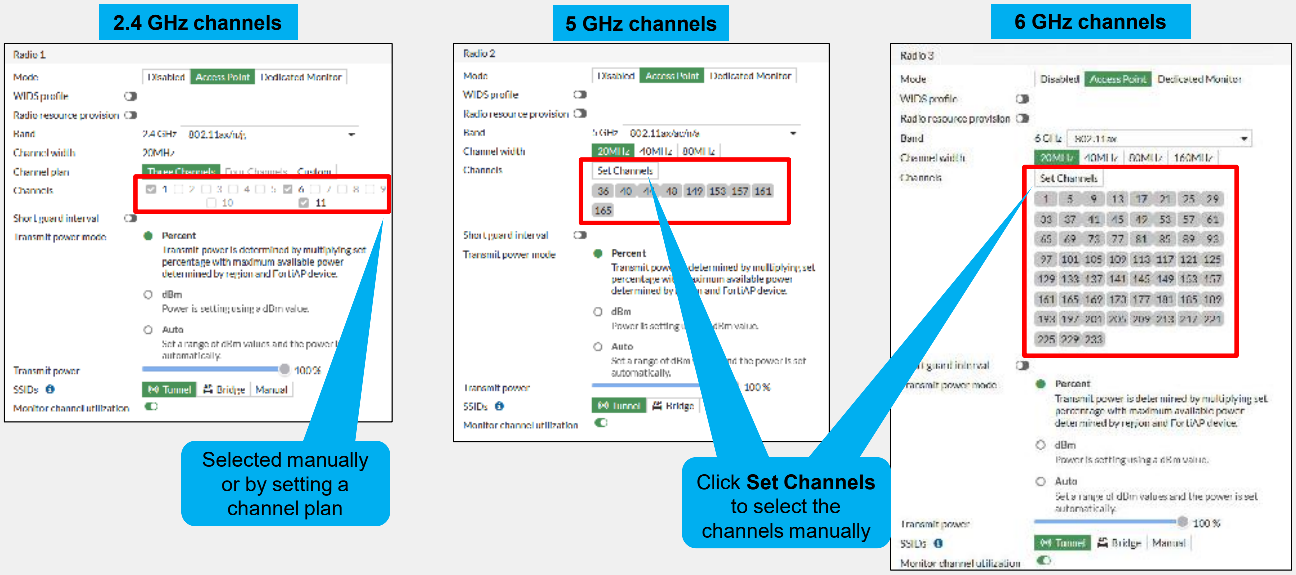
- **Platform**
- **Country / Region**

You can configure customizable settings independently for each radio, **Radio 1**, **Radio 2**, and **Radio 3**—only on Wi-Fi 6E FortiAP devices. Devices equipped with **Radio 3**, such as Wi-Fi 6 and Wi-Fi 6E FortiAP devices, with **Dedicated scan** enabled, will use the radio to scan wireless threats and RF analysis.

These settings include:

- **Mode**:
  - **Disabled**: no radio
  - **Access Point**: normal radio operation
  - **Dedicated Monitor**: radio used for monitoring only, no clients can connect
- **WIDS profile**: background radio scanning and IDS profile settings
- **Radio resource provision**: automatic channel selection on APs in the network to minimize interference
- **Band**: three bands available, 2.4 GHz, 5 GHz, and on WiFi 6E platform, 6 GHz. Choose the IEEE protocol, for example, 802.11ax/n/g.
- **Channel width**: 20, 40, 80, 160 MHz, configurable for 5 GHz and 6 GHz radios
- **Channels**: different channels are available in Country / Region setting
- **Short guard interval**: disabled (default), enable to provide marginally better throughput on 802.11ac or 802.11n on 5 GHz
- **Transmit power mode**: percent, dBm, and auto control over radio transmit power
- **SSIDs**: Tunnel, Bridge, or Manual (to add mix of SSIDs)
- **Monitor channel utilization**: monitors AP radio for channel utilization

Channels



2.4 GHz channels

Radio 1

Mode: Disabled | **Access Point** | Dedicated Monitor
WIDS profile
Radio resource provision
Band: 2.4 GHz 802.11ax/n/g
Channel width: 20MHz
Channel plan: **Three Channels** | Four Channels | Custom
Channels: ☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 □ 7 □ 8 □ 9 □ 10 ☑ 11
Short guard interval
Transmit power mode:
● Percent — Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm — Power is setting using a dBm value.
○ Auto — Set a range of dBm values and the power i automatically.
Transmit power: 100%
SSIDs: **Tunnel** | Bridge | Manual
Monitor channel utilization

Selected manually or by setting a channel plan

5 GHz channels

Radio 2

Mode: Disabled | **Access Point** | Dedicated Monitor
WIDS profile
Radio resource provision
Band: 5 GHz 802.11ax/ac/n/a
Channel width: **20MHz** | 40MHz | 80MHz
Channels: Set Channels
36 40 44 48 149 153 157 161 165
Short guard interval
Transmit power mode:
● Percent — Transmit pow determined by multiplying set percentage wi aximum available power determined by n and FortiAP device.
○ dBm — Power is setting u dBm value.
○ Auto — Set a range of dBm nd the power is set automatically.
Transmit power: 100 %
SSIDs: **Tunnel** | Bridge
Monitor channel utilization

Click **Set Channels** to select the channels manually

6 GHz channels

Radio 3

Mode: Disabled | **Access Point** | Dedicated Monitor
WIDS profile
Radio resource provision
Band: 6 GHz 802.11ax
Channel width: **20MHz** | 40MHz | 80MHz | 160MHz
Channels: Set Channels
1 5 9 13 17 21 25 29
33 37 41 45 49 53 57 61
65 69 73 77 81 85 89 93
97 101 105 109 113 117 121 125
129 133 137 141 145 149 153 157
161 165 169 173 177 181 185 189
193 197 201 205 209 213 217 221
225 229 233
t guard interval
ransmit power mode:
● Percent — Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm — Power is setting using a dBm value.
○ Auto — Set a range of dBm values and the power is set automatically.
Transmit power: 100 %
SSIDs: **Tunnel** | Bridge | Manual
Monitor channel utilization

FURTINET
Training Institute

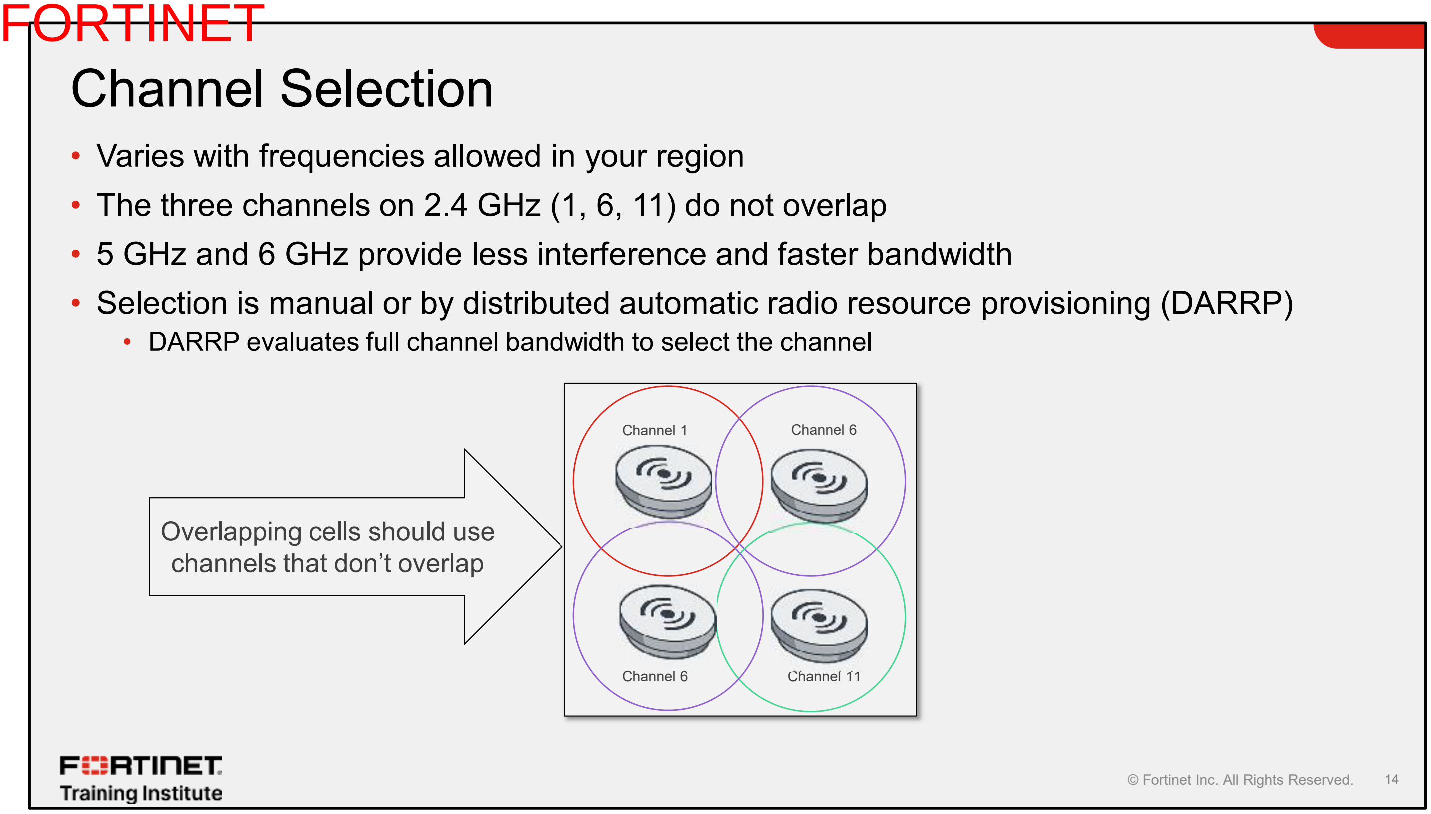
13

Related to the frequency band, you can also customize the channels.

Approved channels vary by the geographic region of your AP. For example, the 2.4 GHz band has 11 operation channels in the United States, but 13 in Europe. So, if you move the AP from one location to another, you might need to change this setting.

IEEE 802.11b and g protocols provide up to 14 channels in the 2.400–2.500 GHz industrial, scientific, and medical (ISM) band, and IEEE 802.11a and n protocols provide up to 16 channels in 5 GHz of Unlicensed National Information Infrastructure (U-NII) band (specifically portions of 5.150–5.250, 5.250–5.350, 5.725–5.875 GHz).

Note also that in the U-NII band, some channel options may be marked with an asterisk. This means that a channel is subject to the rules of dynamic frequency selection (DFS).



Channel Selection

- Varies with frequencies allowed in your region
- The three channels on 2.4 GHz (1, 6, 11) do not overlap
- 5 GHz and 6 GHz provide less interference and faster bandwidth
- Selection is manual or by distributed automatic radio resource provisioning (DARRP)
  - DARRP evaluates full channel bandwidth to select the channel

Overlapping cells should use channels that don't overlap

FORTINET Training Institute

14

Channel selection depends on the frequencies that are permitted for a particular region.

Remember that the width of channels usually exceeds the spacing between the channels, causing some overlap. Interference from adjacent channels is therefore possible. *During wireless network planning, to avoid overlapping, you must use every fourth or fifth channel.* For example, you might use ISM channels 1, 6, and 11 (2.4 GHz band).

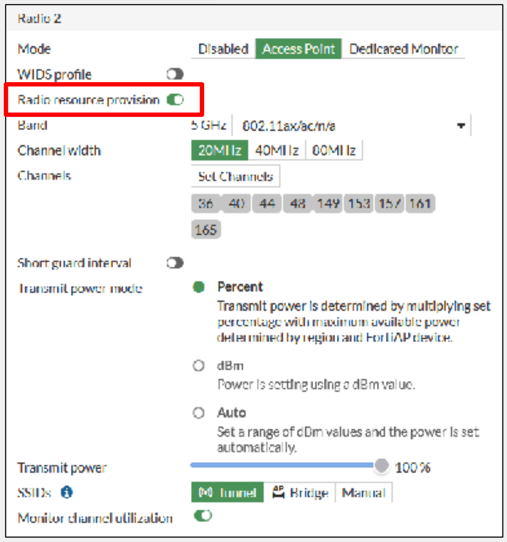
The 5 GHz band is used less than the 2.4 GHz band. Its shorter wavelengths have a shorter range and penetrate obstacles less, but it also means there is less interference from other APs, including your own. So, if your clients support this band, you can select up to 23 channels.

The new 6 GHz band offers more available spectrum and more channel options. This means faster transmission and less latency on the connection. However, it is a new technology and is not yet available in all countries.

You can manually select the channel, or use DARRP, which considers the full channel bandwidth in order to select the channel.

DARRP

- Profiles applied on each radio
- Each FortiAP device selects the best Wi-Fi channel
  - Supports evaluating channel bandwidth in full
- Helps prevent interference
- AP r-evaluates channel selection every 24 hours (84,600 seconds)
  - Override is possible via DARRP profile
- Clients automatically signaled to migrate to a new channel
- Reduces chatter between FortiAP devices
- Can cause issues when the network is being used at capacity
  - Configure schedule in DARRP profile to specify when to run DARRP scan



Radio 2

Mode: Disabled | **Access Point** | Dedicated Monitor

WIDS profile: off

Radio resource provision: on

Band: 5 GHz | 802.11ax/ac/n/a

Channel width: **20MHz** | 40MHz | 80MHz

Channels: Set Channels

36 40 44 48 149 153 157 161 165

Short guard interval: off

Transmit power mode:

● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

○ dBm
Power is setting using a dBm value.

○ Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 100 %

SSIDs: **Tunnel** | Bridge | Manual

Monitor channel utilization: on

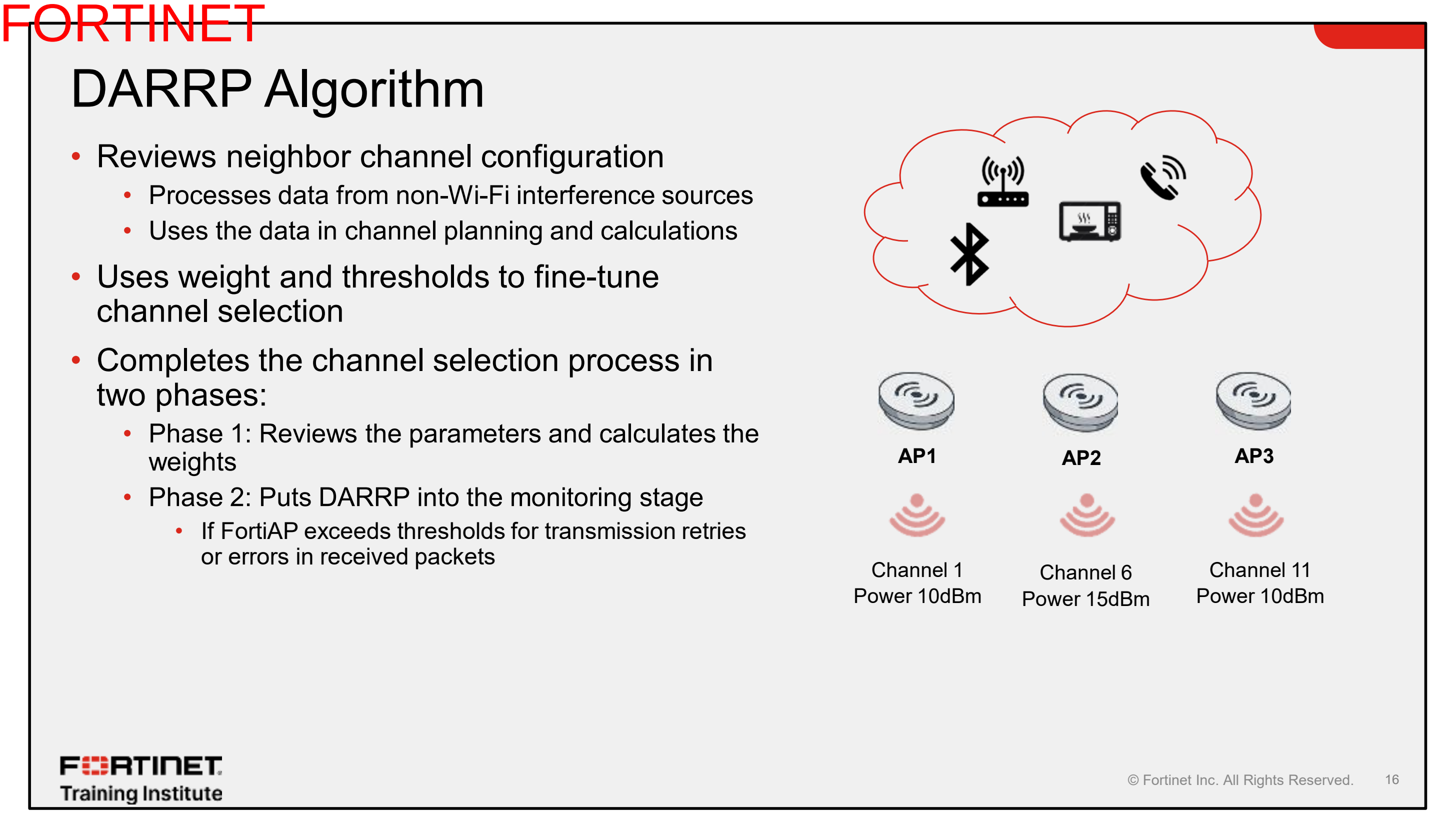
Available on each radio, using DARRP makes FortiAP select the best channel available to use based on the scan results of basic service set identifier (BSSID)/received signal strength indicator (RSSI) to AC. It supports channel bandwidth used on the radio and each FortiAP uses same FortiAP profile can has its own DARRP profile configured.

To prevent interference between APs, DARRP measures utilization and interference on the available channels and selects the clearest channel at each AP. DARRP uses AP background scan results as input.

The DARRP calculation can consume AP resources. The default running time for running DARRP optimizations is 86400 seconds and the range is 0 to 86400. To set the running time for DARRP optimizations, enter the following CLI command in the wireless controller settings: `set darrp-optimize {integer}`. You can override the global value within DARRP profile when used on FortiAP radio.

Note that DARRP doesn't perform a continuous spectrum analysis, so it may not detect intermittent interference sources such as microwave ovens.

DARRP is recommended in large deployments to reduce possible interference. In very large networks, or networks with too many radios, you can change the DARRP optimization time to reduce FortiAP load. However, in small deployments with less risk of interference, you can use the traditional static channel assignation.



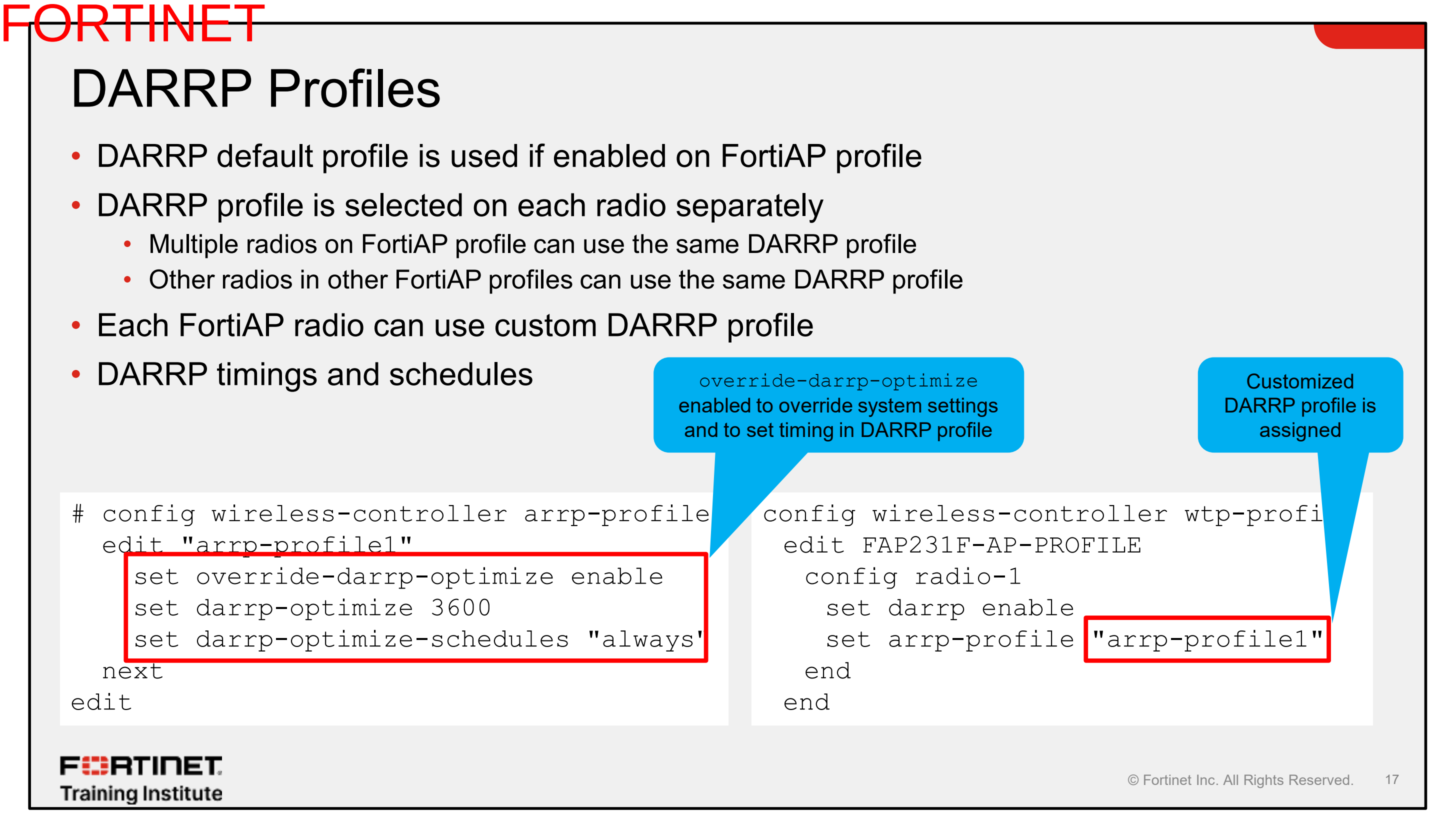
DARRP Algorithm

- Reviews neighbor channel configuration
  - Processes data from non-Wi-Fi interference sources
  - Uses the data in channel planning and calculations
- Uses weight and thresholds to fine-tune channel selection
- Completes the channel selection process in two phases:
  - Phase 1: Reviews the parameters and calculates the weights
  - Phase 2: Puts DARRP into the monitoring stage
    - If FortiAP exceeds thresholds for transmission retries or errors in received packets

16

DARRP integrates data from channel utilization into channel planning. DARRP selects channels by considering data from different sources, including neighboring channels. These channels can be Wi-Fi or non-Wi-Fi, which are both potential sources of interference.

Channel selection has two phases:
- Phase 1: DDARP calculates radio parameters including noise floor, channel load, and factors that are multiplied by a weight value that is assigned by default or customized in a DARRP profile.
- Phase 2: DARRP monitors whether FortiAP devices exceed thresholds in retries to transmit as well as errors in received packets.



DARRP Profiles

- DARRP default profile is used if enabled on FortiAP profile
- DARRP profile is selected on each radio separately
  - Multiple radios on FortiAP profile can use the same DARRP profile
  - Other radios in other FortiAP profiles can use the same DARRP profile
- Each FortiAP radio can use custom DARRP profile
- DARRP timings and schedules

`override-darrp-optimize` enabled to override system settings and to set timing in DARRP profile

Customized DARRP profile is assigned

```
# config wireless-controller arrp-profile
  edit "arrp-profile1"
    set override-darrp-optimize enable
    set darrp-optimize 3600
    set darrp-optimize-schedules "always"
  next
edit
```

```
config wireless-controller wtp-profi
  edit FAP231F-AP-PROFILE
    config radio-1
      set darrp enable
      set arrp-profile "arrp-profile1"
    end
  end
```

FORTINET Training Institute

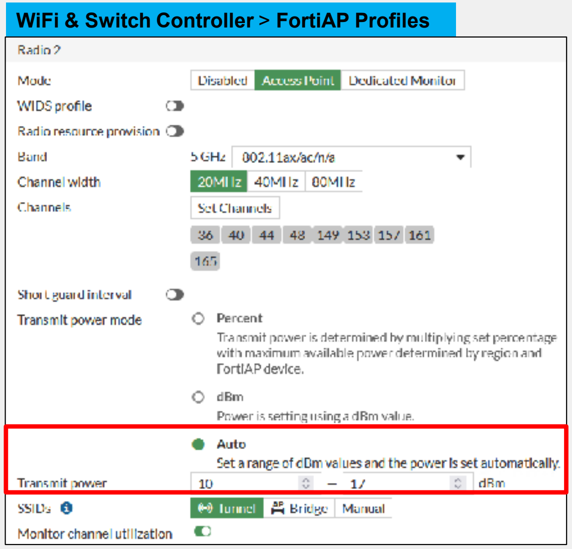
© Fortinet Inc. All Rights Reserved. 17

When DARRP is enabled on a radio, the default DARRP profile is assigned with all of the timings and thresholds defined by default. All FortiAP radios using DARRP can reference the default DARRP profile or a customized profile.

The `darrp-optimize` and `darrp-optimize-schedules` are defined in the wireless-controller setting for DARRP. By default, DARRP runs every 24 hours and it can follow the default firewall schedule “`always`” or any other customized schedule.

Auto Transmission Power

- Allowed maximum transmission (TX) power varies by region
- Percent mode allows you to use the slider bar to adjust the power
- dBm mode sets power between 1 and 33 dBm
  - Setting dBm value in decibel-milliwatt
  - Electrical power unit referenced to 1 milliwatt
- Auto mode:
  - Default range of 10 to 17 dBm
  - If interference is detected, controller reduces AP TX power until `auto-power-low threshold`
  - If interference is not detected, or is detected and removed, controller increases AP TX power until `auto-power-high threshold` value



WiFi & Switch Controller > FortiAP Profiles

Radio 2

Mode: Disabled | **Access Point** | Dedicated Monitor

WIDS profile

Radio resource provision

Band: 5 GHz 802.11ax/ac/n/a

Channel width: **20MHz** | 40MHz | 80MHz

Channels: Set Channels

36 40 44 48 149 153 157 161 165

Short guard interval

Transmit power mode:

○ Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

○ dBm
Power is setting using a dBm value.

● Auto
Set a range of dBm values and the power is set automatically.

Transmit power: 10 – 17 dBm

SSIDs: Tunnel | Bridge | Manual

Monitor channel utilization

TX power is the power FortiAP uses when broadcasting RF signals. Lowering TX power will reduce the coverage area and RF signal propagation. This is useful to control the coverage area. You can decrease the power to prevent broadcasting signals to any unwanted area that may pose as a security risk. For example, you might want to reduce the TX power so that your SSID is broadcast outside your office without compromising the coverage within the desired area.

The **Transmission power mode** has three options: **Percent**, **dBm**, and **Auto**. When you select **Percent**, a transmission slide control appears so that you can adjust the transmission power. **dBm** allows setting power using decibel-milliwatt, which is electrical power unit in decibels. dBm is referenced to 1 milliwatt and you can measure watts with a formula conversion.

FortiOS defines 100% power based on the maximum permitted in your region. But what happens if you select **Auto**?

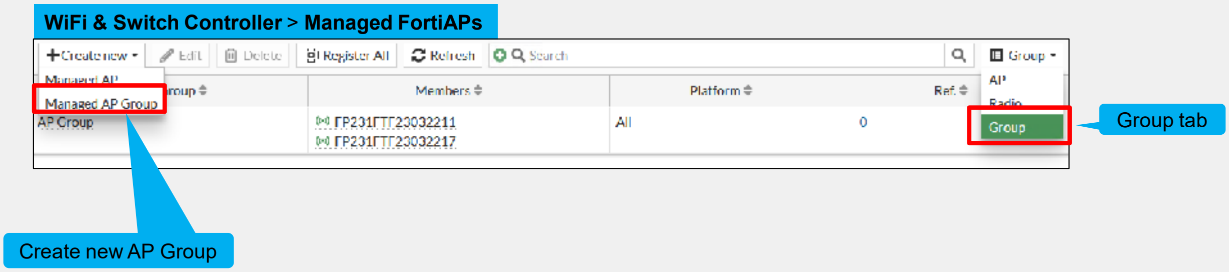
If you select **Auto**, you must then define the power range. FortiOS automatically adjusts the power within this range.

Wireless LANs operate on frequencies that do not require licenses but are limited by regulations low power. So, by default, the wireless controller reduces to the minimum power configured if interference is detected. But, if the wireless controller detects no interference, or detects and then removes interference, it increases the power until it reaches the maximum power limit.

FortiAP Group

- Can group together APs that have the same platform on the **Managed FortiAPs** tab
- Can assign all groups the same profile

WiFi & Switch Controller > Managed FortiAPs

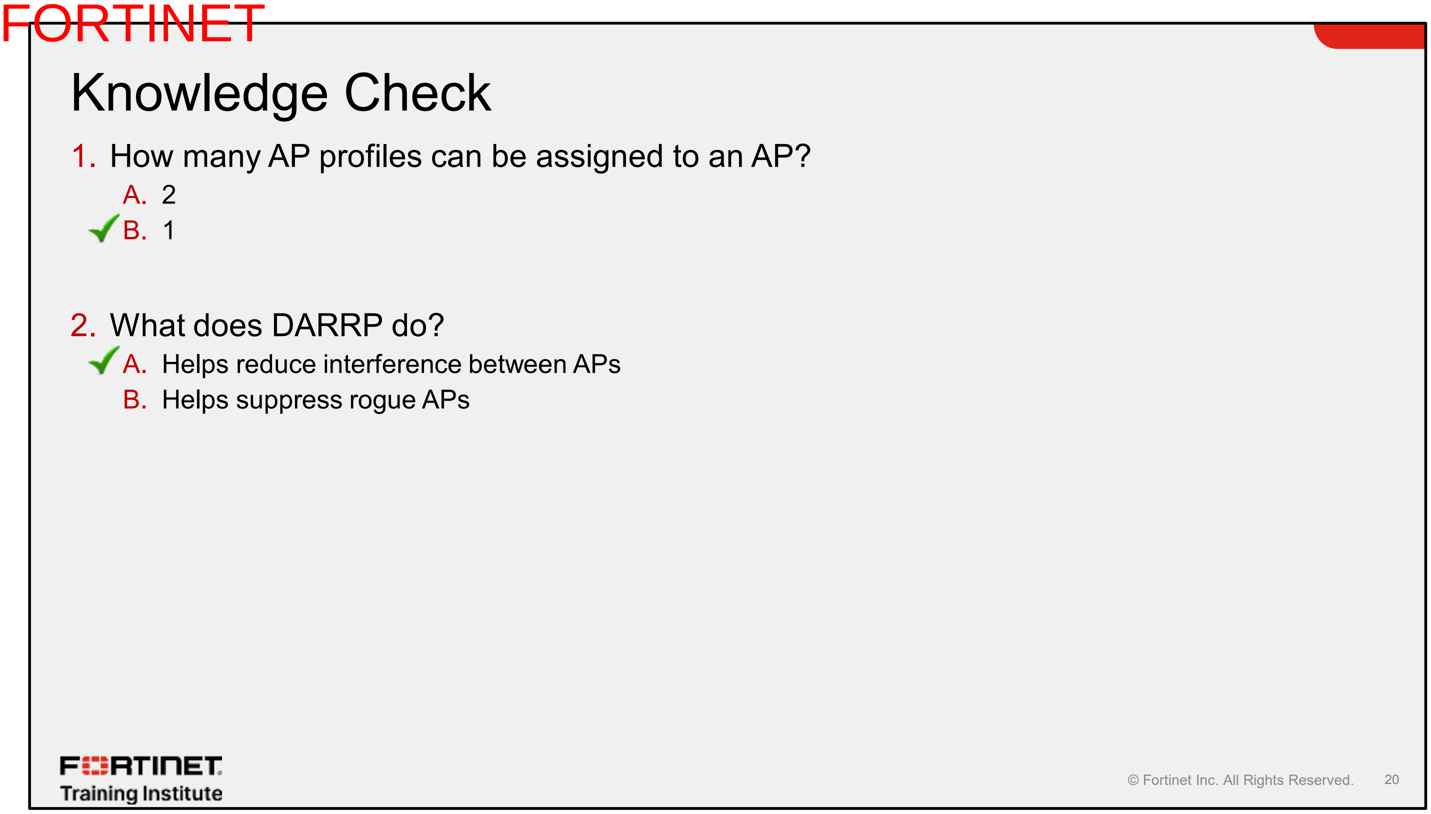


Group	Members	Platform	Ref.
AP Group	FP231FTF23032211 FP231FTF23032217	All	0

FORTINET Training Institute

19

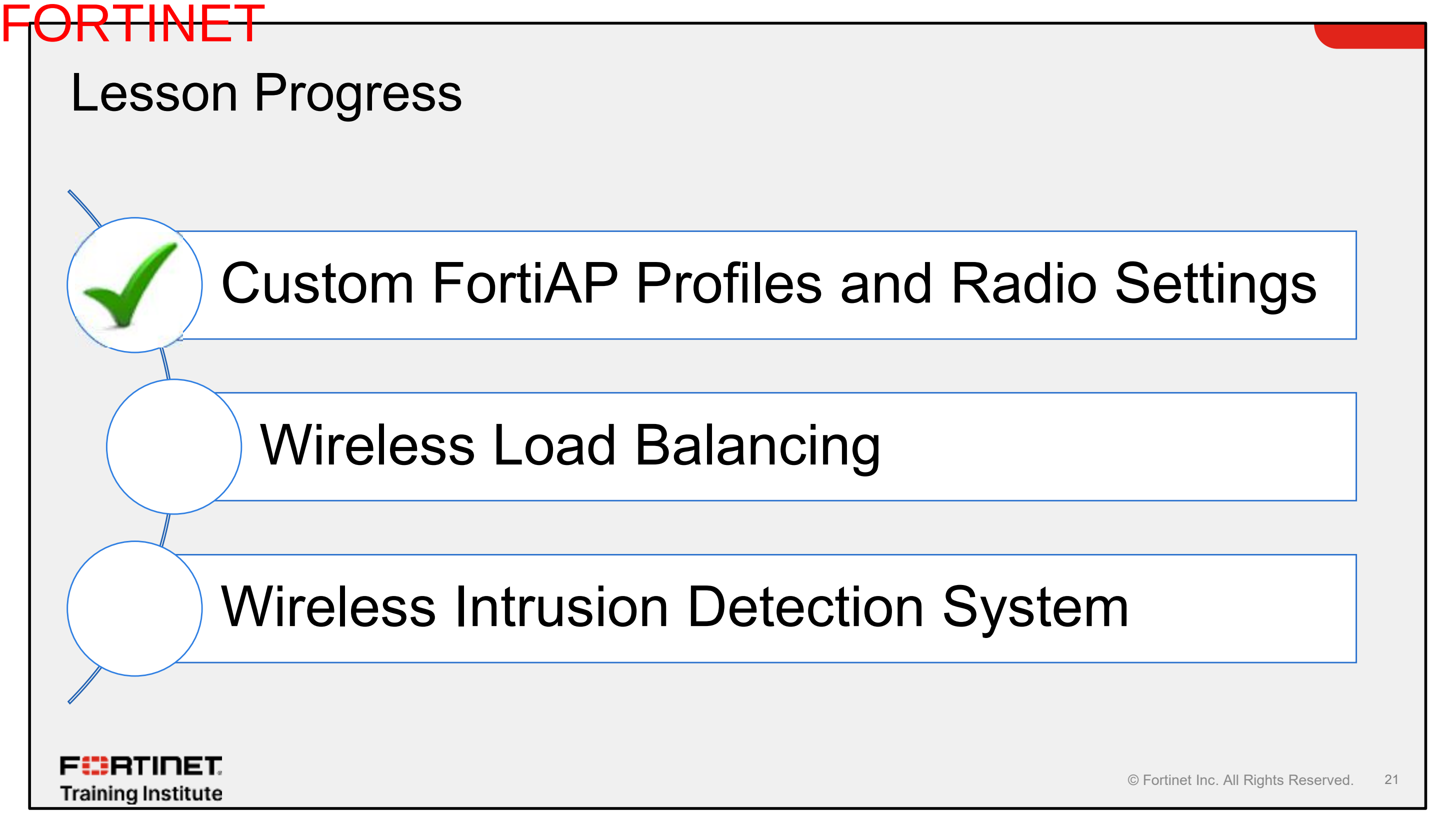
The **Group** tab allows you to create a logical grouping of APs, for example, per floor or per building, and so on. This facilitates the application of FortiAP profiles to a large number of APs. You can't assign an AP to more than one group and all must be of the same model. As a result, you are restricted to using APs that have the same platform in a group.



Knowledge Check

1. How many AP profiles can be assigned to an AP?
   - A. 2
   - ✓ B. 1

2. What does DARRP do?
   - ✓ A. Helps reduce interference between APs
   - B. Helps suppress rogue APs



Lesson Progress

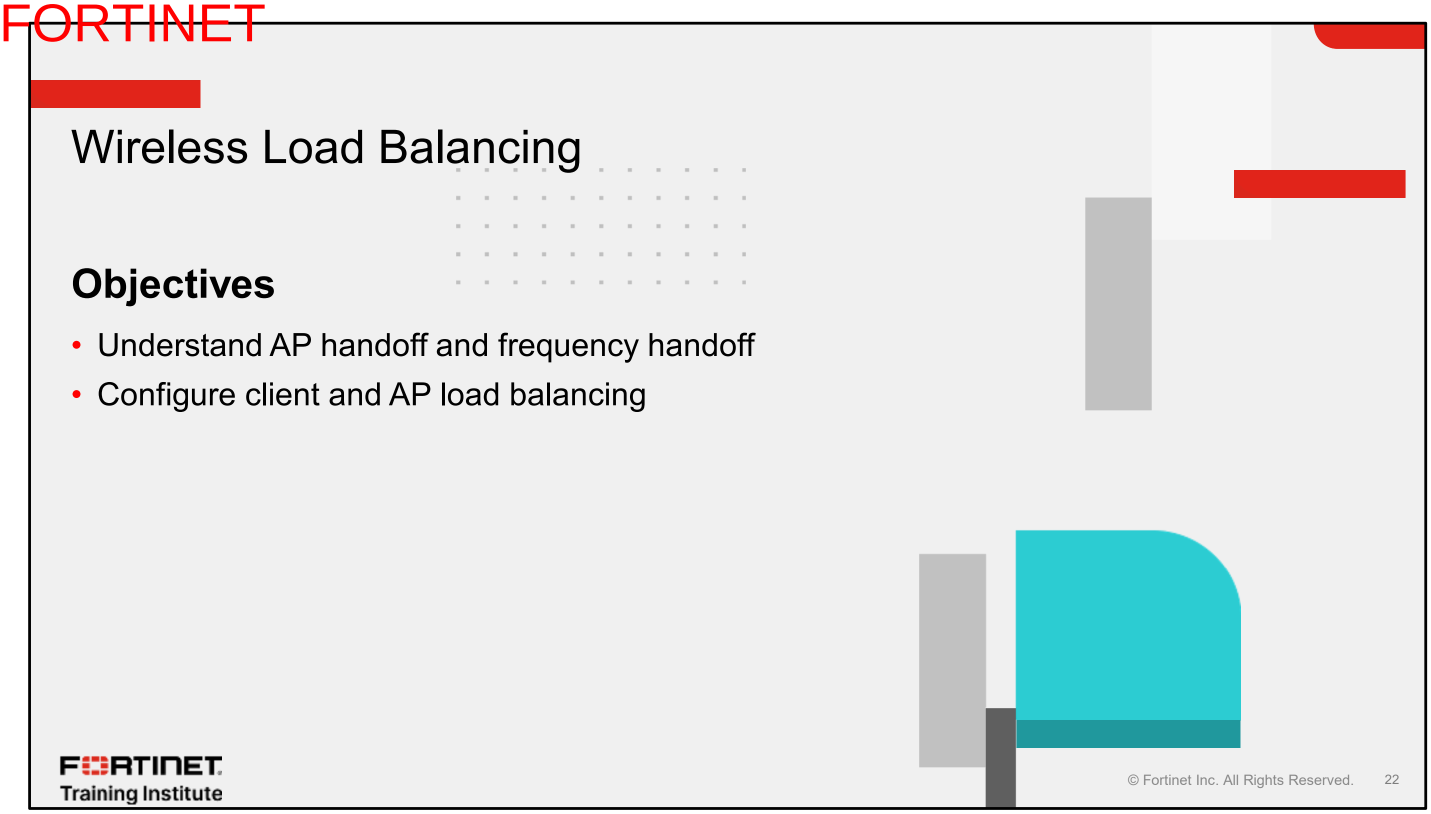
- ✓ Custom FortiAP Profiles and Radio Settings
- Wireless Load Balancing
- Wireless Intrusion Detection System

FORTINET Training Institute

21

Good job! You now understand how to configure FortiAP profiles and assign radio settings on APs.

Now, you will learn about wireless load balancing.



Wireless Load Balancing

Objectives

- Understand AP handoff and frequency handoff
- Configure client and AP load balancing

FORTINET Training Institute

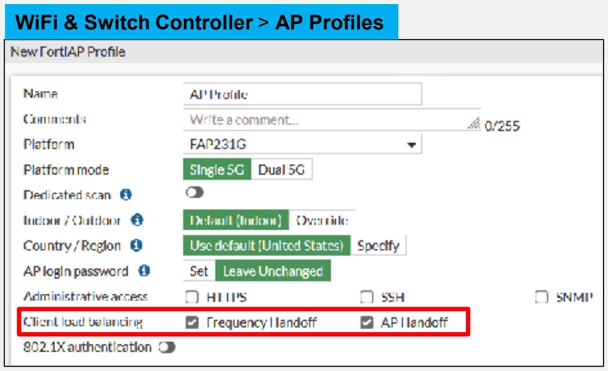
22

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in applying load balancing, you will be able to redistribute the load on the wireless network.

Wireless Client Load Balancing

- Wireless load balancing allows distribution of wireless traffic more efficiently among managed APs and available frequencies
- For high-density deployments
  - Client load balancing across FortiAPs = **AP Handoff**
  - Client load balancing across 2.4 / 5GHz = **Frequency Handoff**
- Configure options per AP profile



WiFi & Switch Controller > AP Profiles

New FortiAP Profile

Name	AP Profile		
Comments	Write a comment... 0/255		
Platform	FAP231G		
Platform mode	[✓ Single 5G] Dual 5G		
Dedicated scan	○		
Indoor / Outdoor	[✓ Default (Indoor)] Override		
Country / Region	[✓ Use default (United States)] Specify		
AP login password	Set [✓ Leave Unchanged]		
Administrative access	□ HTTPS	□ SSH	□ SNMP
Client load balancing	☑ Frequency Handoff	☑ AP Handoff	
802.1X authentication	○		

Fortinet Training Institute

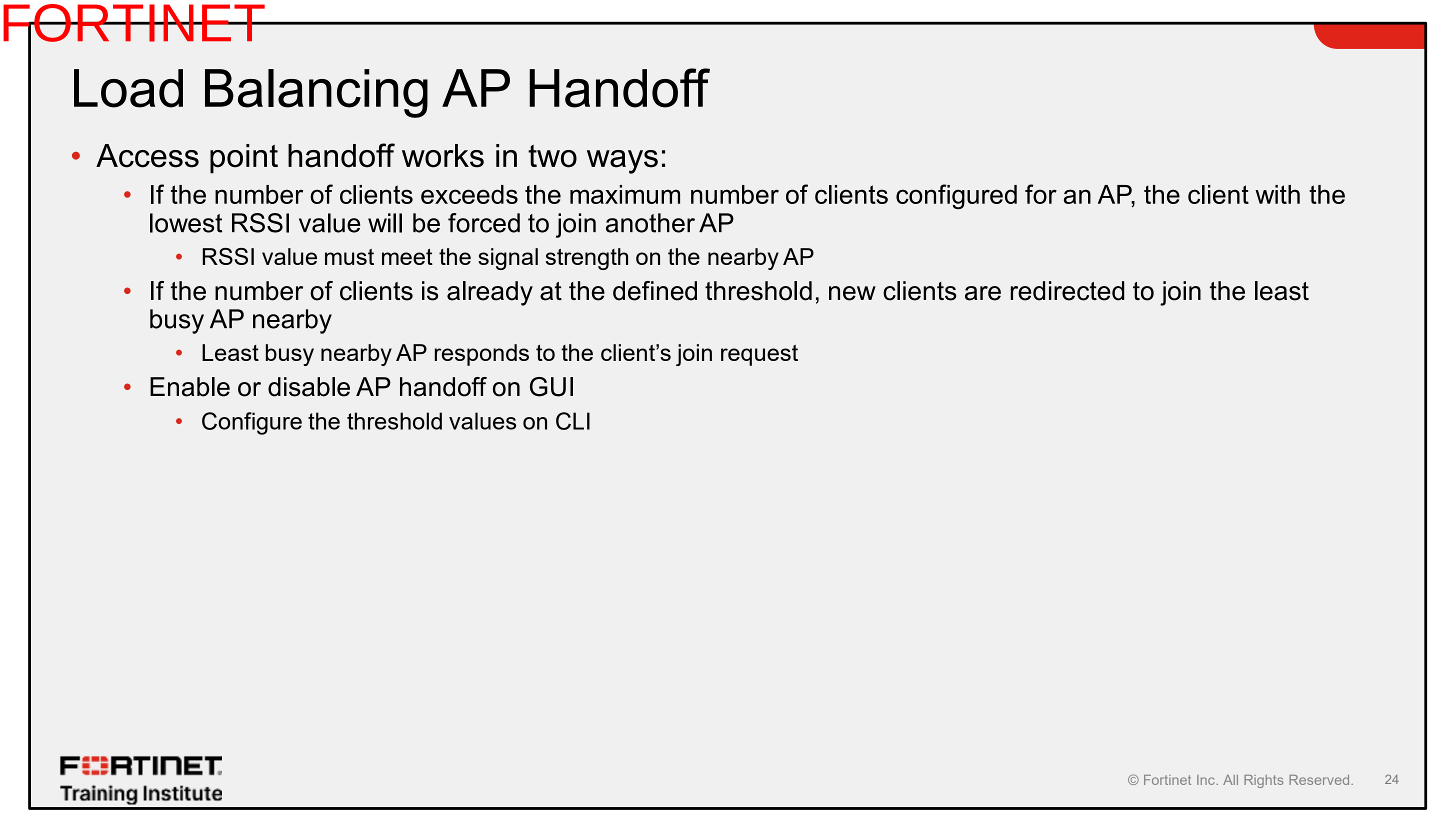
You can use wireless client load balancing techniques in dense deployments such as a conference center. It distributes the load of handling multiple clients among multiple APs or between the two bands. To do this, APs share client load and performance metrics between them.

FortiOS wireless controller supports the following types of client load balancing:

- **AP Handoff**: The wireless controller signals a client to switch to another AP.
- **Frequency Handoff**: The wireless controller monitors the usage of 2.4 GHz, 5 GHz, and 6 GHz bands, and signals clients to switch to the lesser-used frequency.

By default, load balancing is *not applied* to roaming clients.

To enable wireless client load balancing, edit a custom FortiAP profile and select **Frequency Handoff** or **AP Handoff** within the profile.



Load Balancing AP Handoff

- Access point handoff works in two ways:
  - If the number of clients exceeds the maximum number of clients configured for an AP, the client with the lowest RSSI value will be forced to join another AP
    - RSSI value must meet the signal strength on the nearby AP
  - If the number of clients is already at the defined threshold, new clients are redirected to join the least busy AP nearby
    - Least busy nearby AP responds to the client's join request
  - Enable or disable AP handoff on GUI
    - Configure the threshold values on CLI

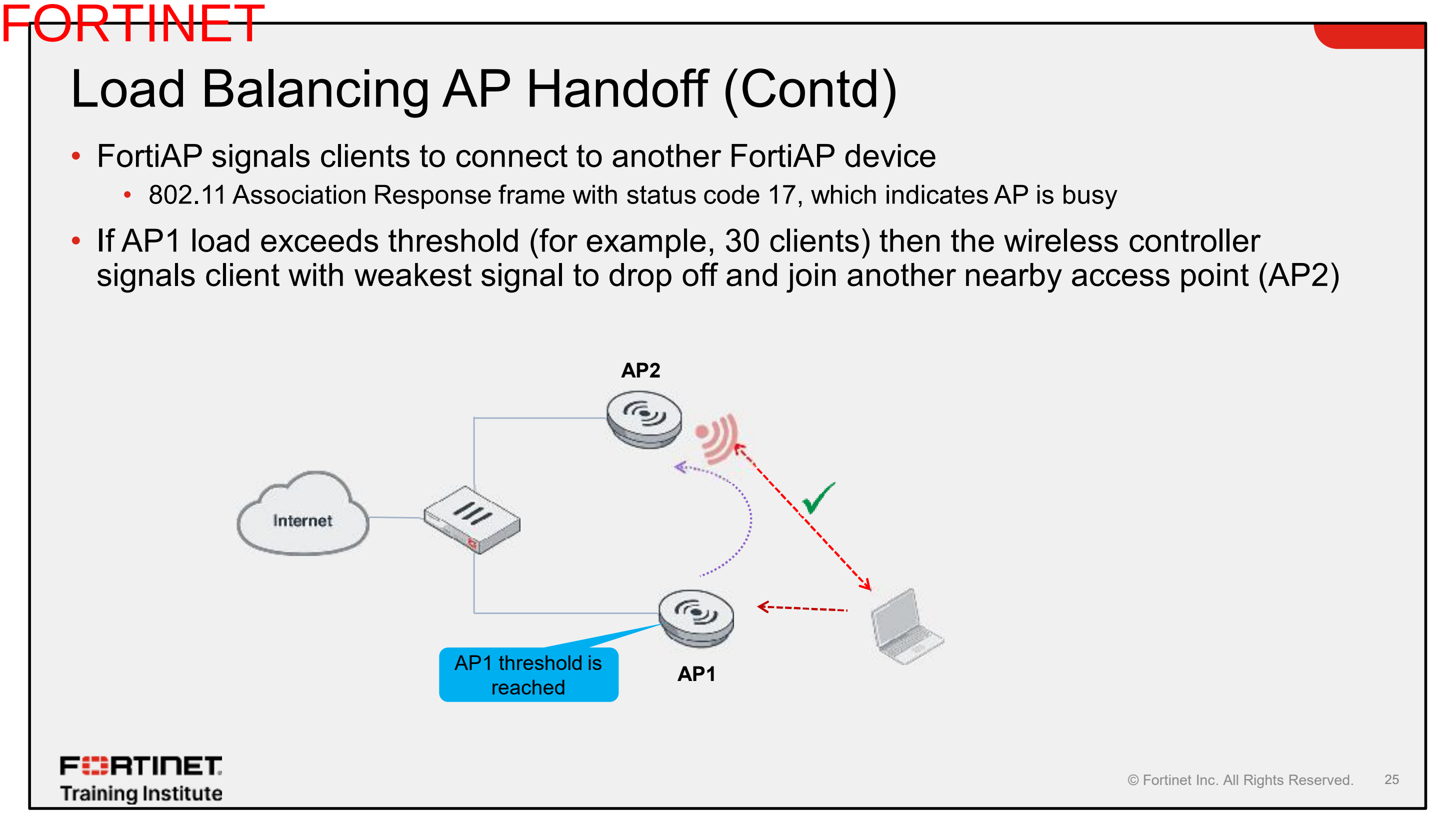
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

AP handoff is a load balancing method that FortiGate uses to increase wireless performance and use the resources on APs more efficiently. AP handoff is a way of load balancing wireless clients among managed APs on FortiGate. If an AP is overloaded and the maximum number of clients is configured for an AP or radio, FortiGate drops the client that has weakest signals and connects the client to a nearby AP.

FortiGate uses the RSSI value threshold defined in the AP profile when a client tries to connect to the second AP. The client`s signal strength must be equal to or more than the defined RSSI value on the AP. Signal strength is determined based on the RSSI value—a higher RSSI value means better signal strength.

`handoff-sta-thresh` in a FortiAP profile defines the value after which the handoff protocol is initiated for a new client. FortiGate instructs the least busy nearby AP to respond to the join request for any new client that tried to connect to an overloaded AP, as long as the configured RSSI value condition is met. You must enable the AP-handoff feature on all radios on an AP.



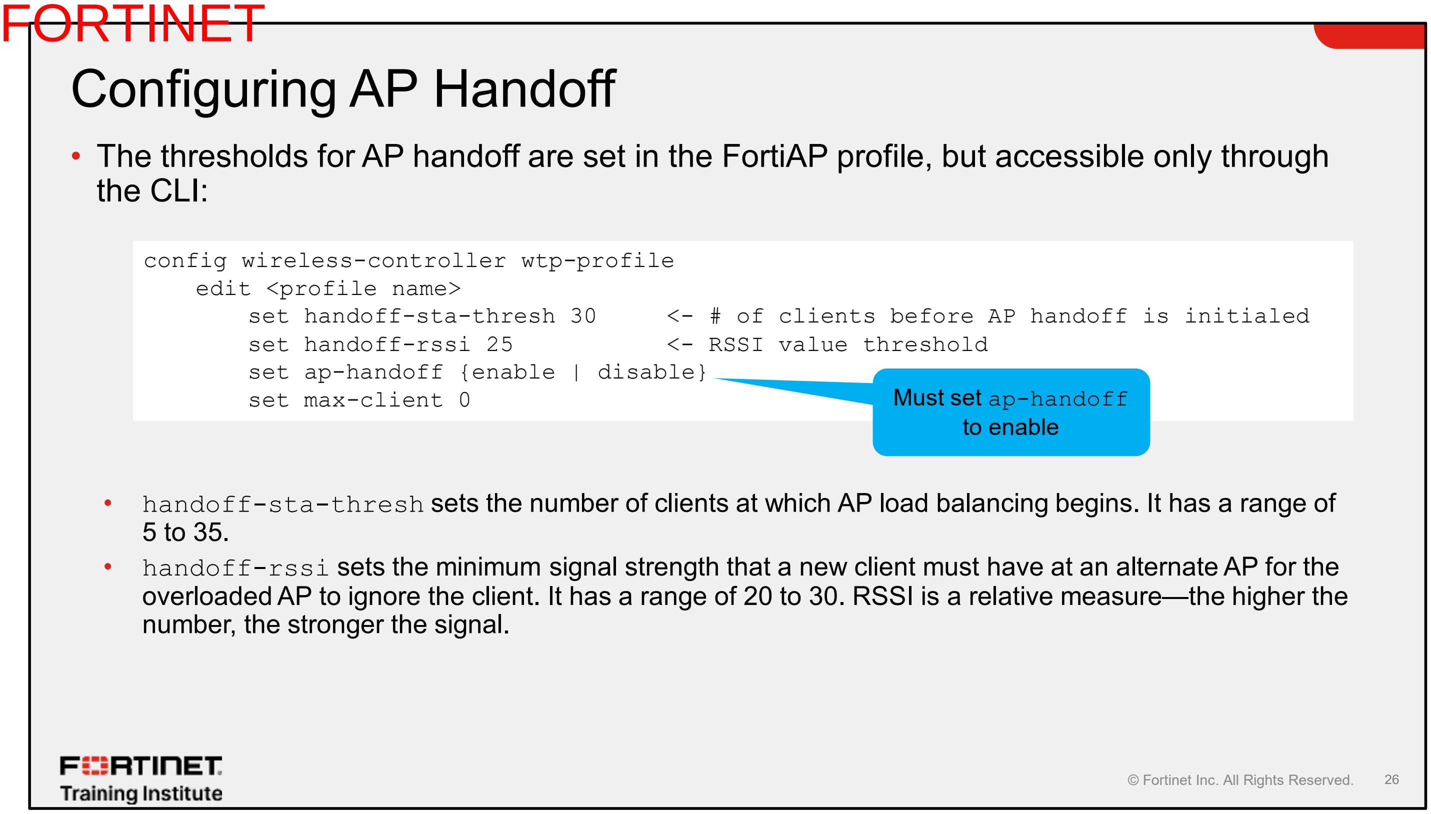
Load Balancing AP Handoff (Contd)

- FortiAP signals clients to connect to another FortiAP device
  - 802.11 Association Response frame with status code 17, which indicates AP is busy
- If AP1 load exceeds threshold (for example, 30 clients) then the wireless controller signals client with weakest signal to drop off and join another nearby access point (AP2)

FORTINET Training Institute

When one or more APs is overloaded (for example, more than 30 clients) and a new client attempts to join the wireless network, the wireless controller selects the least busy AP that is closest to the new client. This AP responds to the client, and the client joins that AP.

Client load-balancing across FortiAP devices: If the load on an AP, for example, AP1, exceeds a threshold, then the wireless controller signals the client with the weakest signal to drop off and join a nearby AP, for example, AP2. When one or more APs is overloaded (for example, more than 30 clients) and a new client attempts to join a wireless network, the wireless controller selects the least busy AP that is closest to the new client and this AP is the one that responds to the client and the one that the client joins.



Configuring AP Handoff

- The thresholds for AP handoff are set in the FortiAP profile, but accessible only through the CLI:

```
config wireless-controller wtp-profile
    edit <profile name>
        set handoff-sta-thresh 30    <- # of clients before AP handoff is initialed
        set handoff-rssi 25          <- RSSI value threshold
        set ap-handoff {enable | disable}
        set max-client 0
```

Must set `ap-handoff` to enable

- `handoff-sta-thresh` sets the number of clients at which AP load balancing begins. It has a range of 5 to 35.
- `handoff-rssi` sets the minimum signal strength that a new client must have at an alternate AP for the overloaded AP to ignore the client. It has a range of 20 to 30. RSSI is a relative measure—the higher the number, the stronger the signal.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

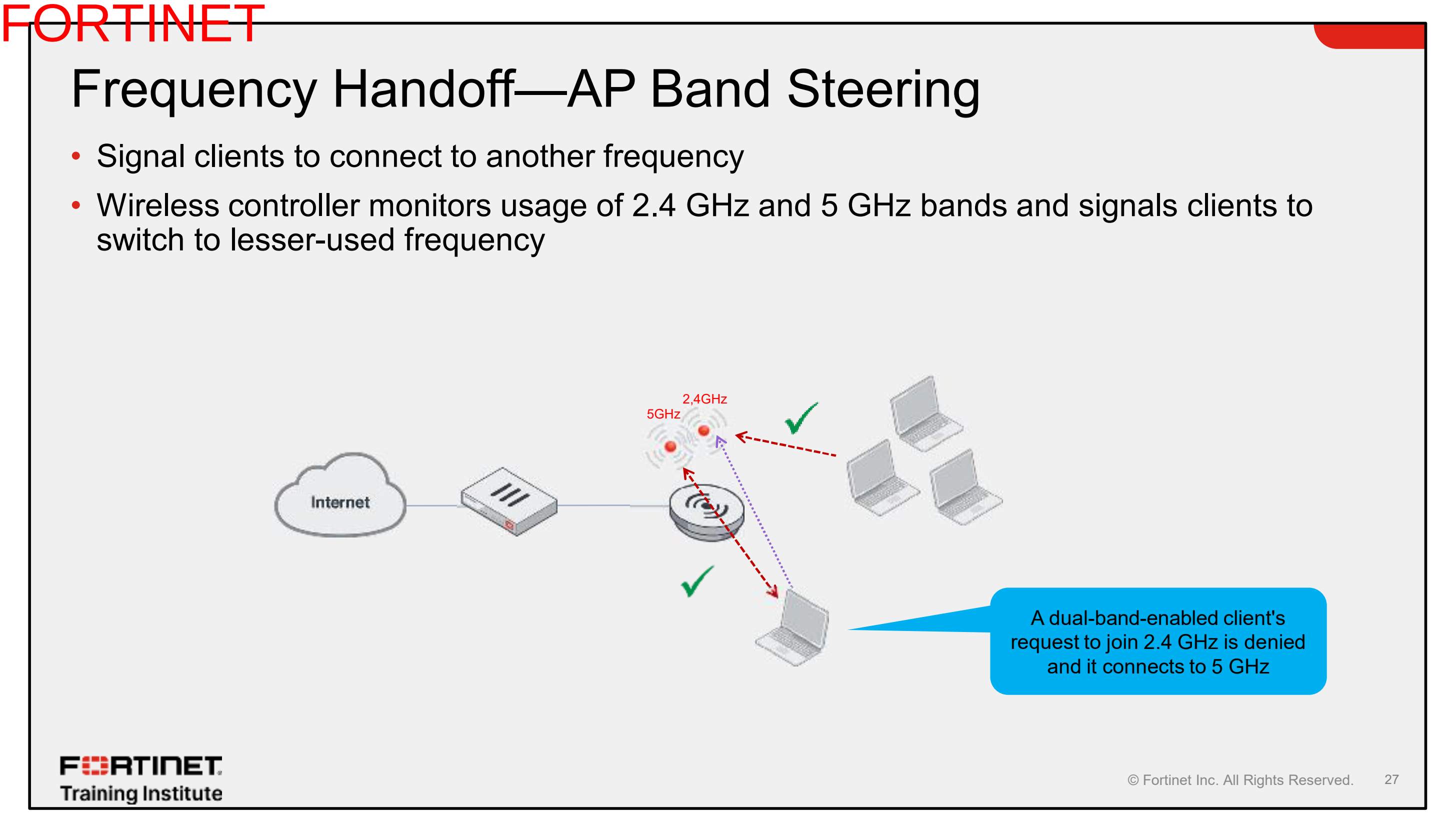
During an AP hand-off configuration, don't confuse `max-client` and `handoff-sta-thresh`.

- `max-client` is the maximum number of clients this AP supports. After the AP reaches this number of clients, it forces a *hard* rejection. 0 means no limit.
- `handoff-sta-thresh` defines the value after which the handoff protocol is initiated for a new client. FortiGate instructs the least busy nearby AP to respond to the join request for any new client that tried to connect to an overloaded AP as long as the configured RSSI value condition is met. If the AP has more clients than this threshold, it is considered busy and clients are moved to another AP. You must enable the AP-handoff feature on all radios on an AP.

As a best practice, you should set up the `handoff-sta-thresh` value between 15 to 20 and up to 10 stations for video streaming.

`set ap-handoff` enables or disables AP load balancing on the AP profile. It is disabled by default.

The `handoff-rssi` is the signal level that another nearby AP must see in order for the controller to include it in the load balancing process. The default value is 25 and is measured in dB relative to the generic noise level -95 dBm. For instance, a value of 25 means that the signal level needs to be -70 dBm or better, and a value of 30 means the signal threshold is -65 dBm.



Frequency Handoff—AP Band Steering

- Signal clients to connect to another frequency
- Wireless controller monitors usage of 2.4 GHz and 5 GHz bands and signals clients to switch to lesser-used frequency

A dual-band-enabled client's request to join 2.4 GHz is denied and it connects to 5 GHz

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

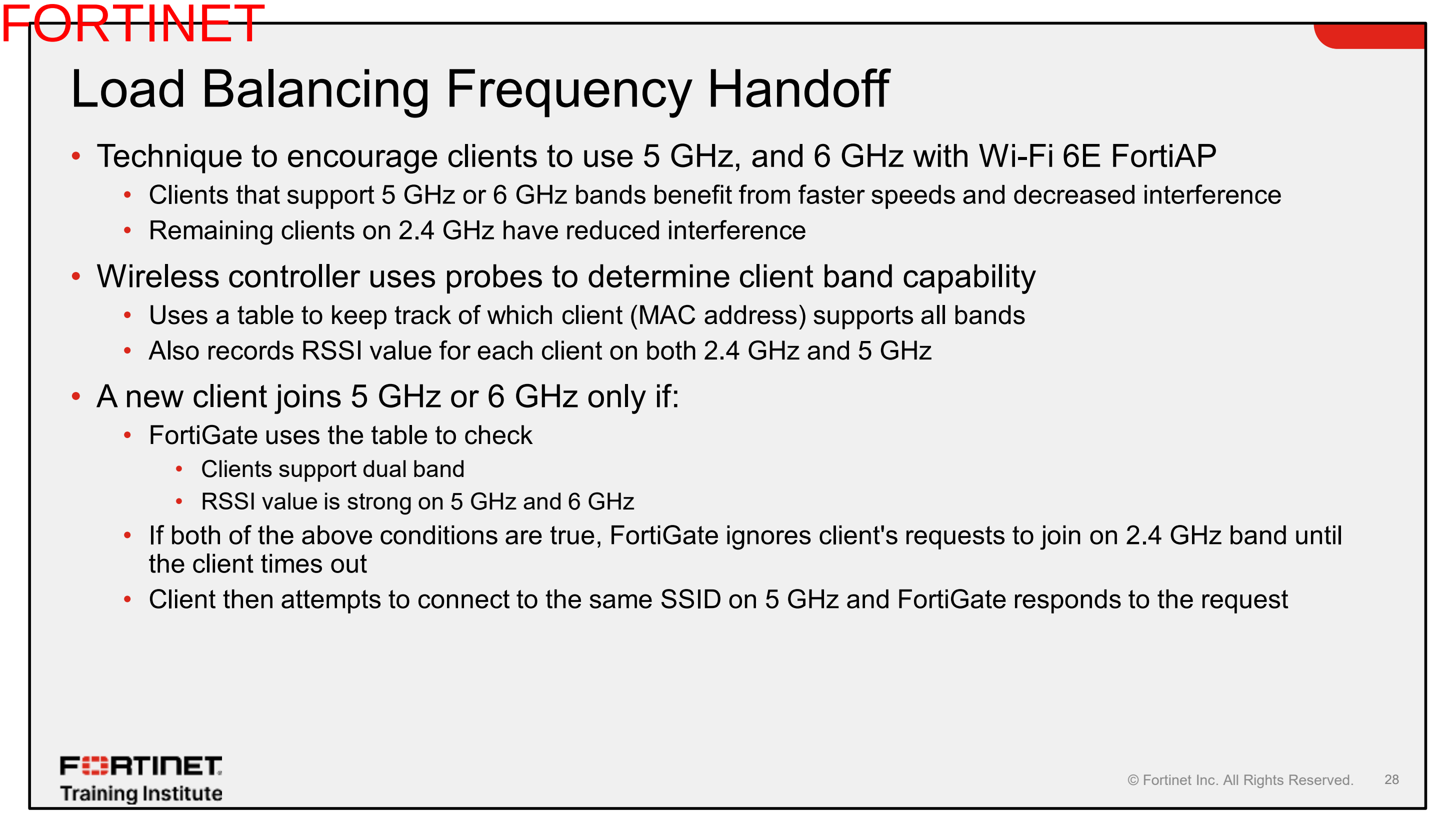
AP bad steering distributes devices across frequency bands to *prevent congestion and interference.*

What if you don’t want to move the client to a different AP? What if you just want to move it to a different radio, with a different frequency?

For example, a client could ask to join the 2.4 GHz channel. The wireless controller would evaluate whether the AP is a dual-band device, and verify if the RSSI value is strong. If so, the wireless controller would not reply to the client’s request, forcing the client to retry until it attempted to join the same SSID on the 5 GHz band.

After the controller sees this new request on the 5 GHz band, the controller measures the RSSI again. If the RSSI is acceptable, the controller allows the client to join. Otherwise, the controller updates the device table and waits for the client to time out again. When the client attempts to connect a second time on the 2.4 GHz band, the controller accepts it.

Configure frequency load balancing in the AP profile to distribute devices across frequency bands to prevent congestion and interference, and encourage clients to use the 5 GHz Wi-Fi band.



Load Balancing Frequency Handoff

- Technique to encourage clients to use 5 GHz, and 6 GHz with Wi-Fi 6E FortiAP
  - Clients that support 5 GHz or 6 GHz bands benefit from faster speeds and decreased interference
  - Remaining clients on 2.4 GHz have reduced interference
- Wireless controller uses probes to determine client band capability
  - Uses a table to keep track of which client (MAC address) supports all bands
  - Also records RSSI value for each client on both 2.4 GHz and 5 GHz
- A new client joins 5 GHz or 6 GHz only if:
  - FortiGate uses the table to check
    - Clients support dual band
    - RSSI value is strong on 5 GHz and 6 GHz
  - If both of the above conditions are true, FortiGate ignores client's requests to join on 2.4 GHz band until the client times out
  - Client then attempts to connect to the same SSID on 5 GHz and FortiGate responds to the request

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

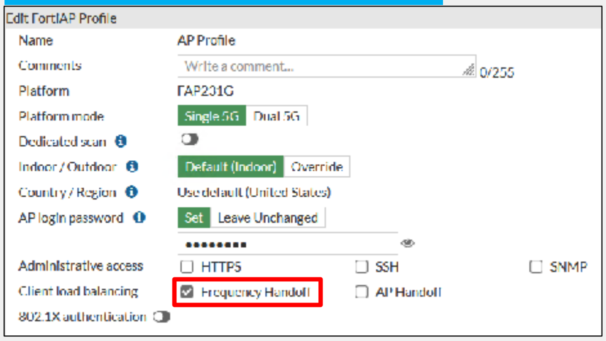
Frequency handoff is a band-steering technique that FortiGate uses to encourage clients to use the 5 GHz frequency, or 6 GHz frequency in the case of Wi-Fi 6E FortiAP. Clients that support 5 GHz or 6 GHz frequency benefit from faster speeds and decreased interference. This also benefits clients that do not support the either faster frequency bands because there is less interference on 2.4 GHz because of the reduced number of clients. FortiGate continuously probes the clients to identify if they can operate on the 5 GHz or 6 GHz frequency. FortiGate maintains a table to track which clients support any of the frequencies, and records the RSSI value along with the other information for each frequency.

When a client tries to connect, FortiGate checks whether it can support faster frequencies and, if so, how good the signals are. If a client supports the 5 GHz frequency and the signal is strong enough to connect, FortiGate ignores the client’s requests to join the network on 2.4 GHz until the request times out. The client then automatically tries to join the same network using 5 GHz. FortiGate instructs the AP to respond to the join request and allow the client to connect.

Frequency Handoff Configuration

- Frequency load balancing is configured on the FortiAP profile
- RSSI value threshold is configurable
- Must enable frequency handoff on 5 GHz or 6 GHz band to learn client’s capability
- Best practice `handoff-rssi:`
  - Voice: 25–30 , Regular data and video: 23–27

WiFi & Switch Controller > FortiAP Profile



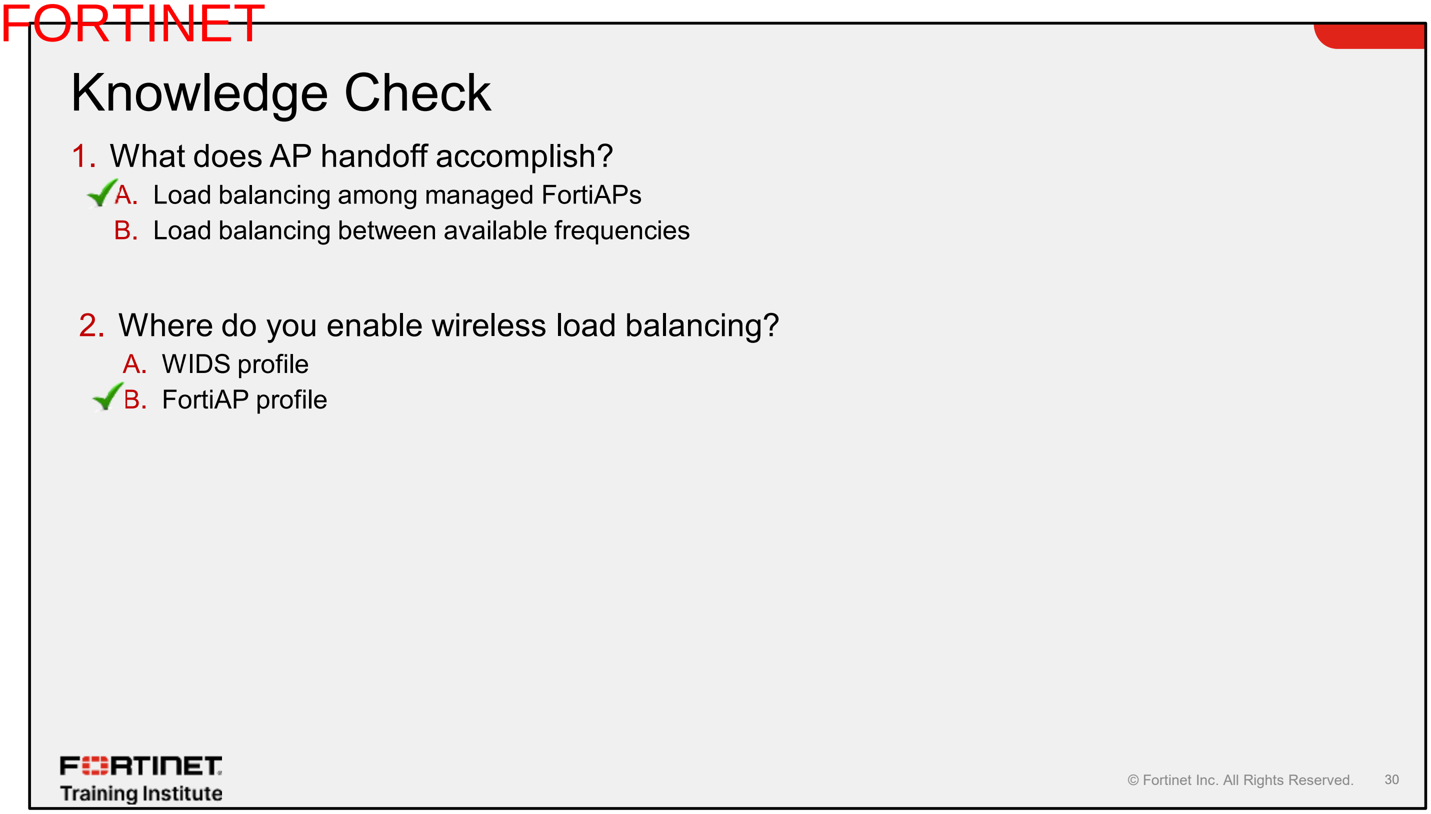
Edit FortiAP Profile

Name	AP Profile
Comments	Write a comment... 0/255
Platform	FAP231G
Platform mode	[✓ Single 5G] Dual 5G
Dedicated scan	○
Indoor / Outdoor	[✓ Default (Indoor)] Override
Country / Region	Use default (United States)
AP login password	[✓ Set] Leave Unchanged ●●●●●●●●●
Administrative access	□ HTTPS □ SSH □ SNMP
Client load balancing	☑ Frequency Handoff □ AP Handoff
802.1X authentication	○

FURTINET Training Institute

Configure frequency handoff in the AP profile. You must enable frequency handoff to learn the client’s capability.

As you learned, you can configure the handoff RSSI value threshold. As a best practice, you should set this value between 25 to 30 for voice traffic to minimize handoff interruptions, but 23 to 27 for regular data.

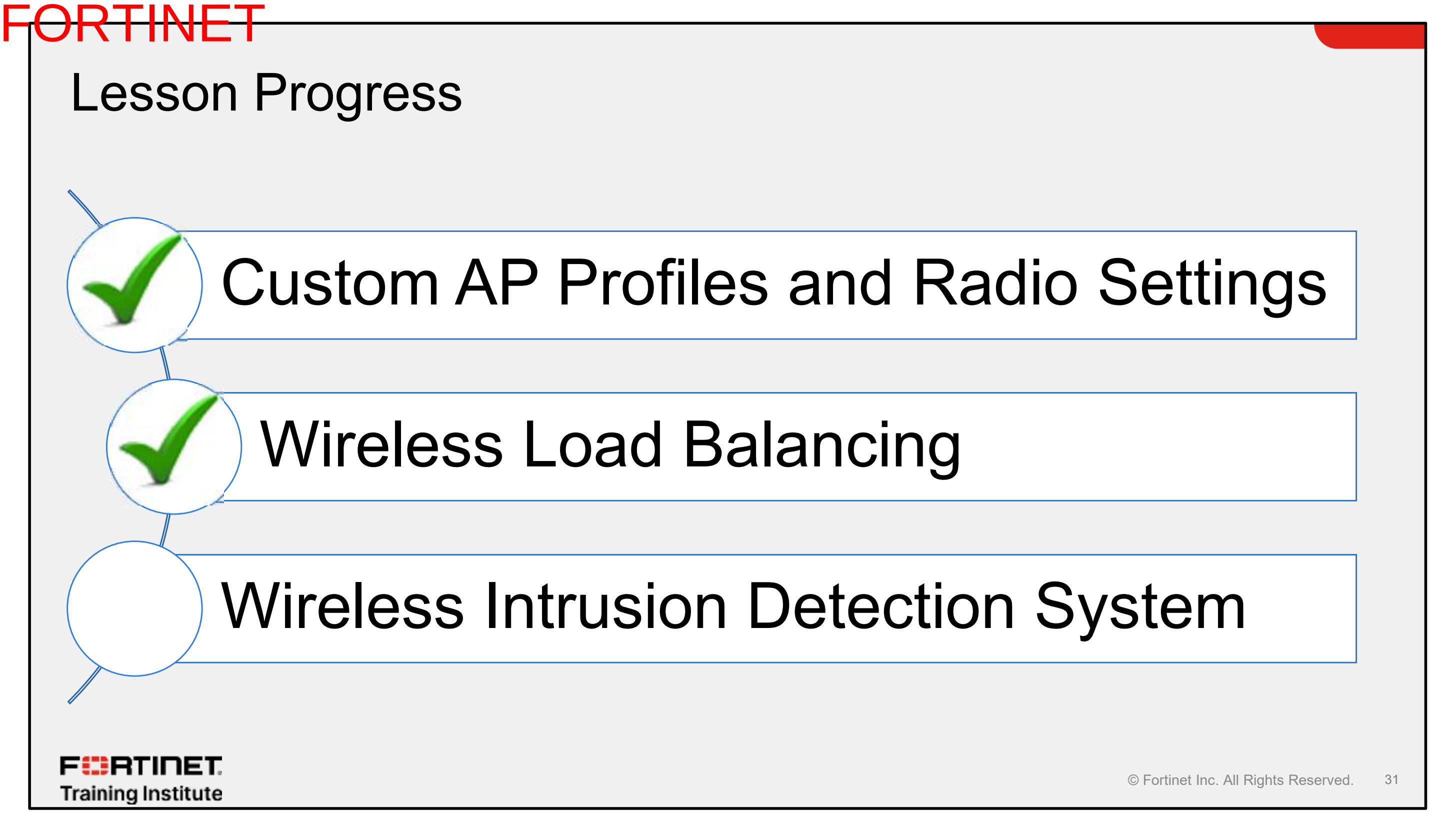


Knowledge Check

1. What does AP handoff accomplish?
   - ✓ A. Load balancing among managed FortiAPs
   - B. Load balancing between available frequencies

2. Where do you enable wireless load balancing?
   - A. WIDS profile
   - ✓ B. FortiAP profile

FORTINET
Training Institute



Lesson Progress

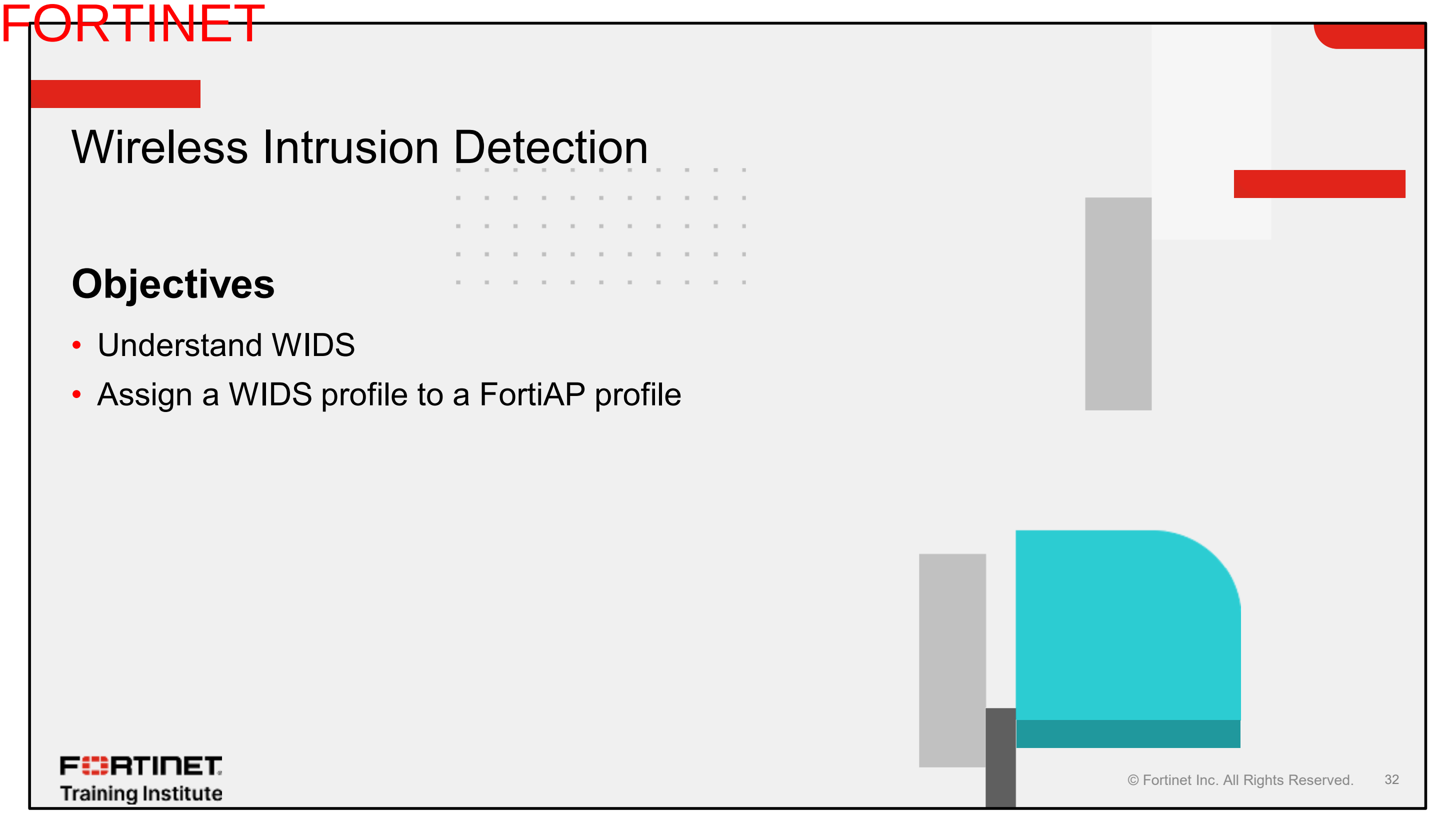
- ✓ Custom AP Profiles and Radio Settings
- ✓ Wireless Load Balancing
- ○ Wireless Intrusion Detection System

Training Institute

31

Good job! You now understand wireless load balancing.

Now, you will learn about Wireless Intrusion Detection System (WIDS) profiles and how to deploy them.



Wireless Intrusion Detection

Objectives

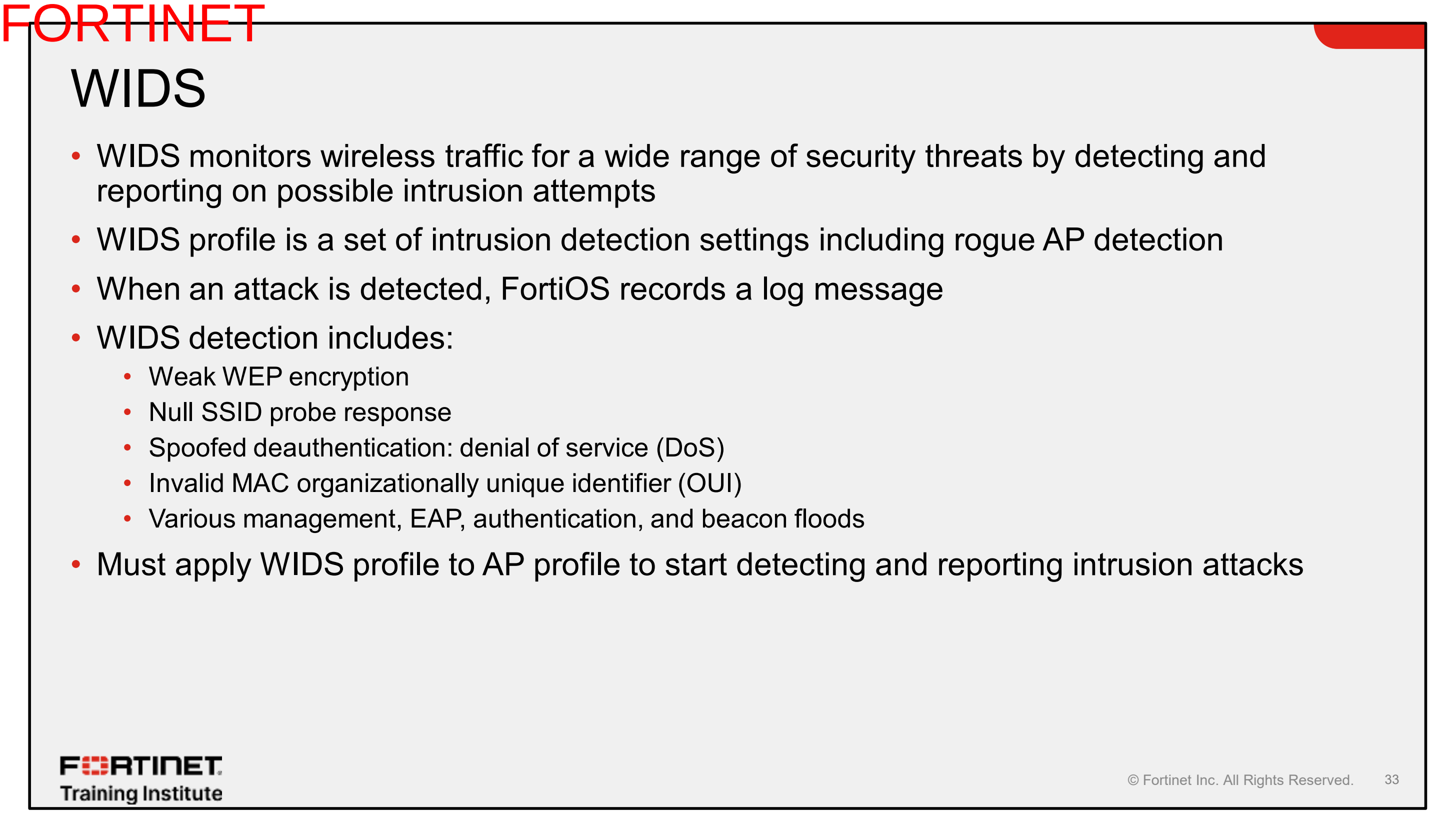
- Understand WIDS
- Assign a WIDS profile to a FortiAP profile

FORTINET
Training Institute

32

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using WIDS, you will be able to configure and deploy a WIDS profile to scan and protect your wireless network.



WIDS

- WIDS monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts
- WIDS profile is a set of intrusion detection settings including rogue AP detection
- When an attack is detected, FortiOS records a log message
- WIDS detection includes:
  - Weak WEP encryption
  - Null SSID probe response
  - Spoofed deauthentication: denial of service (DoS)
  - Invalid MAC organizationally unique identifier (OUI)
  - Various management, EAP, authentication, and beacon floods
- Must apply WIDS profile to AP profile to start detecting and reporting intrusion attacks

33

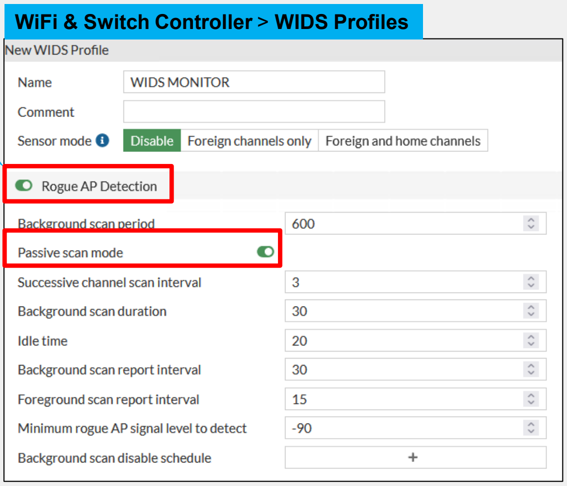
WIDS monitors wireless traffic for a wide range of Wi-Fi-specific security threats by detecting and reporting on possible intrusion attempts, such as:

- Weak WEP IV encryption used to crack WEP keys
- Null SSID probe response that causes many wireless cards and devices to stop responding
- Deauthentication broadcasts that are a DoS attack causing all clients to disconnect from the AP
- Invalid MAC OUI—the first three bytes of the MAC address are the OUI, administered by IEEE
- Various management, EAP, authentication, and beacon floods

When an attack is detected, FortiOS records a log message. You use WIDS profiles to enable and configure the threshold of the individual intrusion type that will be used to generate log messages. Once configured, you must apply the WIDS profile to an AP profile to enable the detection of intrusion attacks.

Provisioning Rogue AP Detection

- Use WIDS profiles to configure intrusion detection settings
  - Provides flexibility to create more than one WIDS profile to address specific security concerns
- Activating rogue AP detection settings in WIDS profile
  - Following settings will enable background rogue AP scanning



WiFi & Switch Controller > WIDS Profiles

New WIDS Profile

Name: WIDS MONITOR
Comment:
Sensor mode: [✓ Disable] Foreign channels only | Foreign and home channels

Rogue AP Detection: enabled

Background scan period	600
Passive scan mode	enabled
Successive channel scan interval	3
Background scan duration	30
Idle time	20
Background scan report interval	30
Foreground scan report interval	15
Minimum rogue AP signal level to detect	-90
Background scan disable schedule	+

RADIO will switch to monitor mode every 600 seconds to perform background scan

AP will not send probe requests on scanned channels

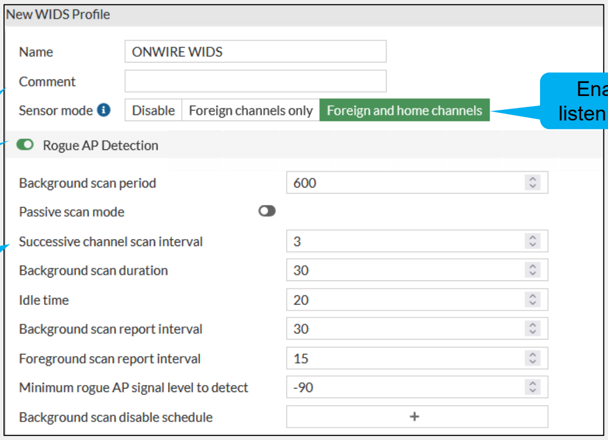
The WIDS profile includes settings for detection of unauthorized (rogue) access points in your wireless network. You can set up the background scan threshold, for example, scan interval, here.

WIDS monitors wireless traffic for a wide range of Wi-Fi-specific security threats by detecting and reporting on possible intrusion attempts, and records a log message. You can create a WIDS profile to enable these types of intrusion detection. By default, all of these options are enabled when you create a new WIDS profile.

Provisioning On-Wire Rogue AP Detection

- Activating on-wire rogue AP detection settings in WIDS profile
  - Following settings will enable foreground rogue AP scanning
- AP or a radio needs to be in dedicated monitor mode to enable on-wire automatic suppression
  - Configure this in the AP profile

WiFi & Switch Controller > WIDS Profiles



New WIDS Profile

Name	ONWIRE WIDS
Comment	
Sensor mode	Disable / Foreign channels only / [✓ Foreign and home channels]

● Rogue AP Detection

Background scan period	600
Passive scan mode	○
Successive channel scan interval	3
Background scan duration	30
Idle time	20
Background scan report interval	30
Foreground scan report interval	15
Minimum rogue AP signal level to detect	-90
Background scan disable schedule	+

Enables FortiAP to listen to station's traffic

All of these settings must be enabled to activate on-wire rogue AP automatic suppression

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

There are two ways to suppress a rogue AP: manually on the **Rogue AP** monitor page, or by enabling **Auto suppress rogue APs in foreground scan**. The manual process requires you to log in to FortiGate and mark an AP as rogue, and then enable suppression. This process can be slow and create a potential security issue. The WIDS profile allows you to automate this process and, whenever a rogue AP is detected on-wire, FortiGate automatically suppresses the AP.

You must enable the following settings to activate automatic on-wire rogue AP suppression:

1. Have an AP or radio in dedicated monitor mode (foreground scanning).
2. Enable **Sensor mode** in WIDS profile.
3. Enable **Enable rogue AP detection** in the WIDS profile.
4. Enable **Auto-suppress rogue APs in foreground scan**.

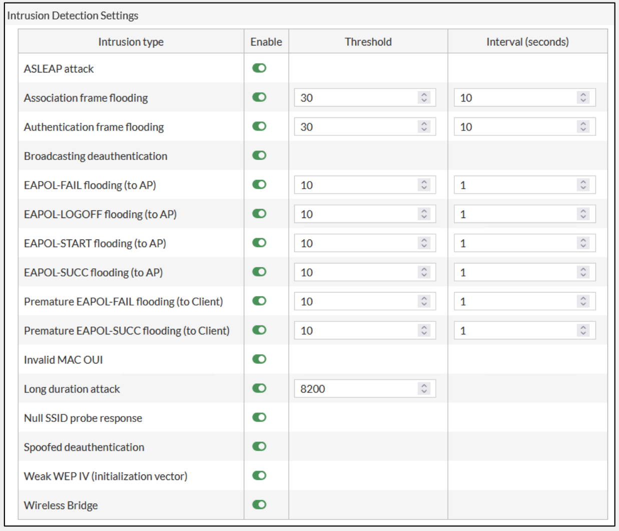
Even for manual rogue AP suppression to work, you must have the first three settings enabled as mentioned above. Otherwise, FortiGate will not be able to listen to the (stations) STAs traffic and send deauthentication frames to suppress the rogue AP.

Provisioning the WIDS Profile

- Use WIDS profiles to enable and configure thresholds of individual intrusion attack types
- All of these intrusion attacks are detected using various techniques
  - For example, If the SSID information element has a value of ASLEAP found in beacon frames and also found in probe request frames, an asleap attack threat is detected
- There are more configurable options available in the CLI

```
# config wireless-controller wids-profile
(wids-profile)# edit <profile name>
```

WiFi & Switch Controller > WIDS Profiles



Intrusion Detection Settings

Intrusion type	Enable	Threshold	Interval (seconds)
ASLEAP attack	●		
Association frame flooding	●	30	10
Authentication frame flooding	●	30	10
Broadcasting deauthentication	●		
EAPOL-FAIL flooding (to AP)	●	10	1
EAPOL-LOGOFF flooding (to AP)	●	10	1
EAPOL-START flooding (to AP)	●	10	1
EAPOL-SUCC flooding (to AP)	●	10	1
Premature EAPOL-FAIL flooding (to Client)	●	10	1
Premature EAPOL-SUCC flooding (to Client)	●	10	1
Invalid MAC OUI	●		
Long duration attack	●	8200	
Null SSID probe response	●		
Spoofed deauthentication	●		
Weak WEP IV (initialization vector)	●		
Wireless Bridge	●		

Training Institute

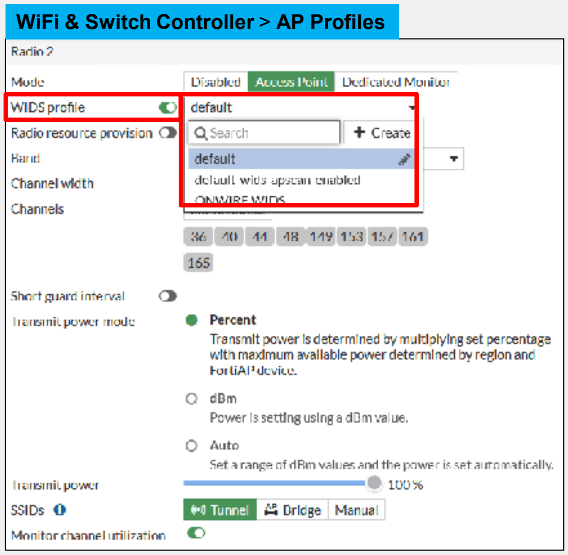
36

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

- ASLEAP attack: ASLEAP is a tool used to perform attacks against LEAP authentication.
- Association frame flooding: A DoS attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
- Authentication frame flooding: A DoS attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
- Broadcasting deauthentication: This is a type of DoS attack. A flood of spoofed deauthentication frames forces wireless clients to deathenticate, then reauthenticate 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 DoS 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 OUI, administered by IEEE. Invalid OUIs are logged.
- Long duration attack: To share radio bandwidth, Wi-Fi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a DoS 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 deauthentication: Spoofed deauthentication frames are a DoS attack. They cause all clients to disconnect from the AP.
- 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: Wi-Fi 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.

Applying WIDS

- Once WIDS profile is configured, you must apply it to a radio or more in FortiAP profile
  - Can apply only one WIDS profile to a radio
  - Can apply same WIDS profile to more than radios and/or other radios in other FortiAP profiles
- Level of FortiAP radio participation in WIDS depends on FortiAP operating mode
  - For example, FortiAP that are not in dedicated monitor mode cannot perform foreground scanning



WiFi & Switch Controller > AP Profiles

Radio 2

Mode: Disabled | Access Point | Dedicated Monitor

WIDS profile: default

Search | + Create

default

default wids apscan enabled

ONWIRE WIDS

Radio resource provision

Band

Channel width

Channels: 36 40 44 48 149 153 157 161 165

Short guard interval

Transmit power mode:

● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

○ dBm
Power is setting using a dBm value.

○ Auto
Set a range of dBm values and the power is set automatically.

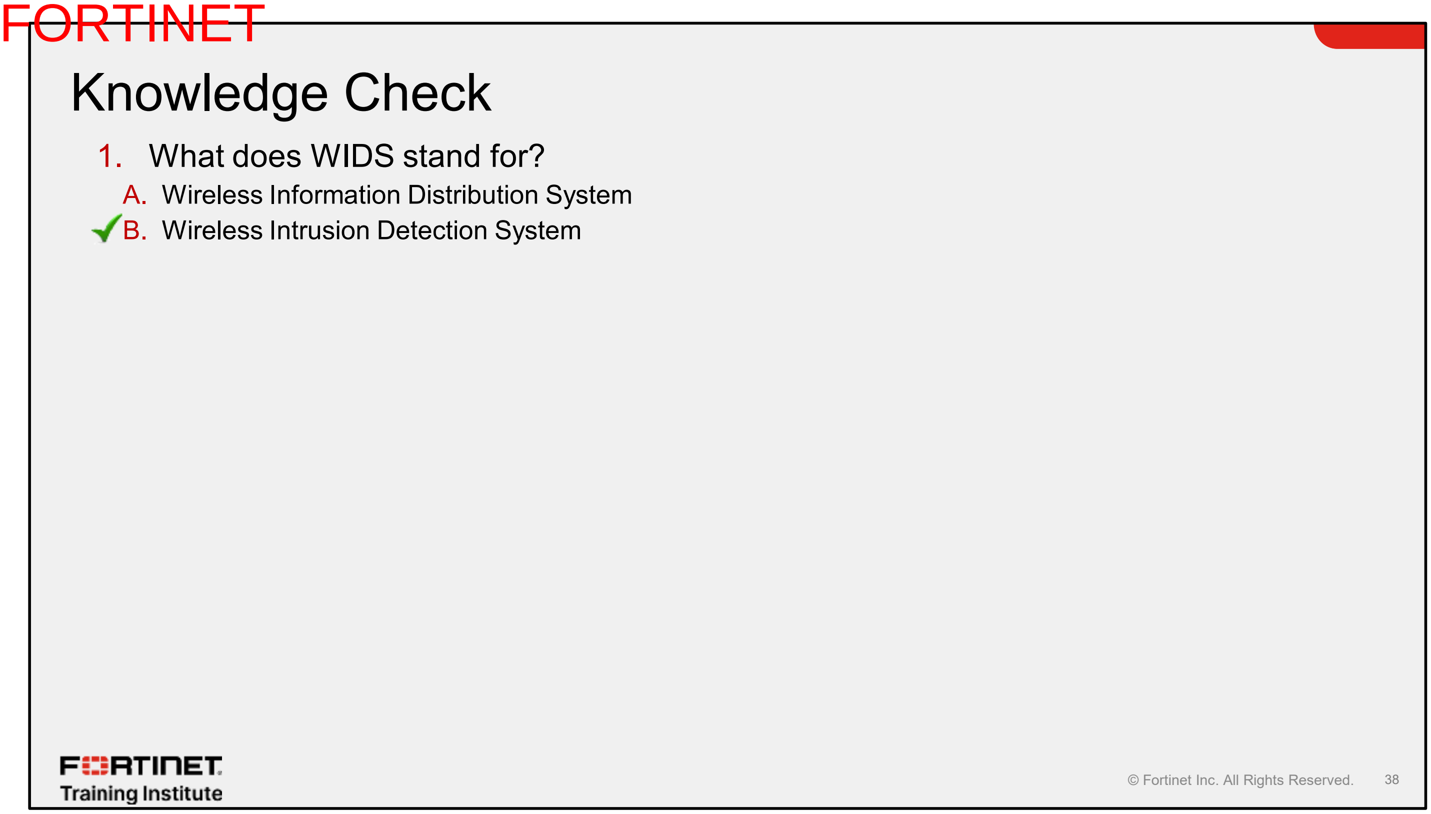
Transmit power: 100 %

SSIDs: Tunnel | Bridge | Manual

Monitor channel utilization

You must apply a WIDS profile to an AP profile to allow assigned APs to participate in WIDS. You can apply only one WIDS profile to an AP profile, and can apply the same WIDS profile to more than one AP profile.

You can choose the appropriate profile from the **WIDS profile** field in an AP profile.

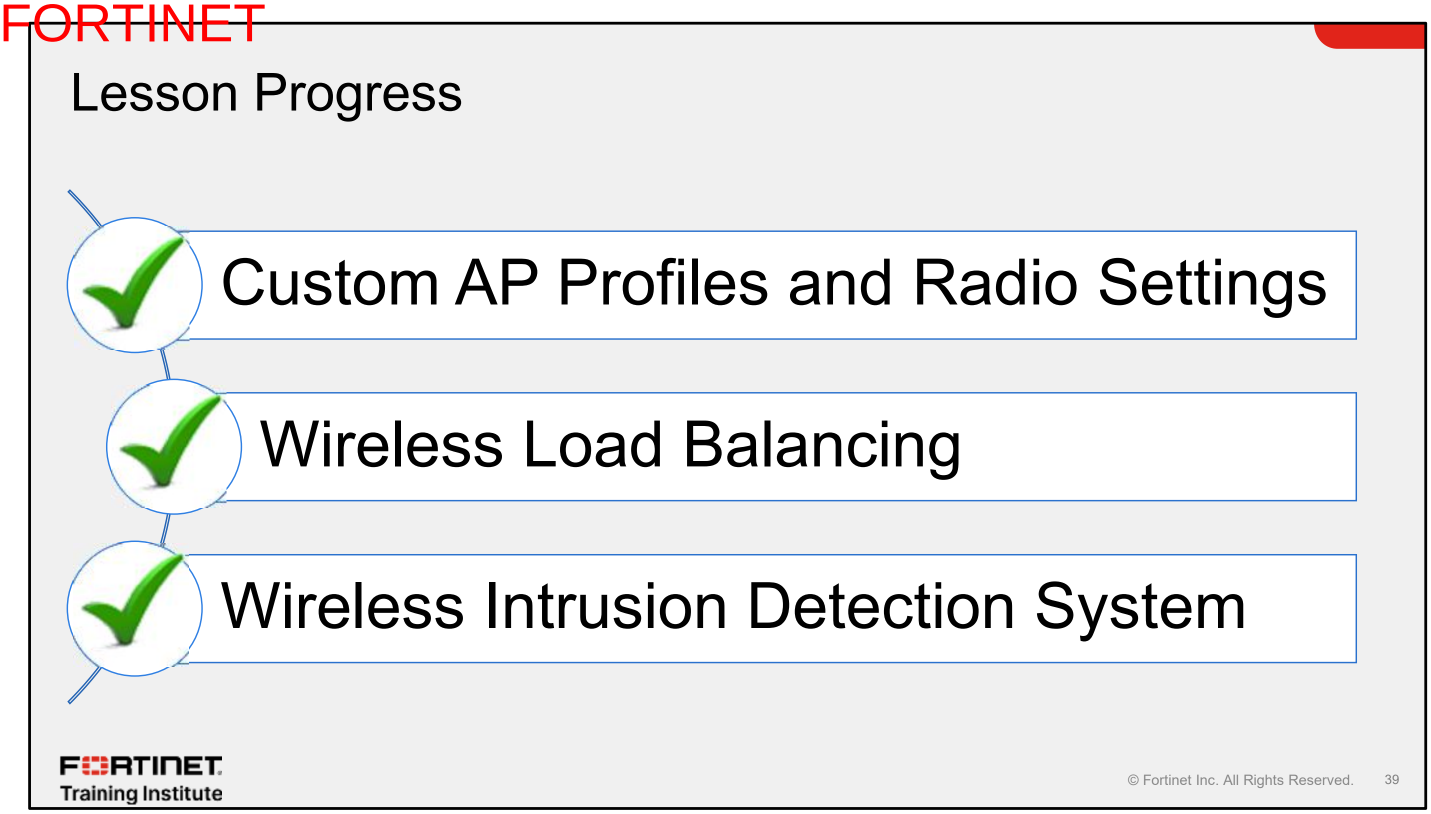


Knowledge Check

1. What does WIDS stand for?
   - A. Wireless Information Distribution System
   - ✓ B. Wireless Intrusion Detection System

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

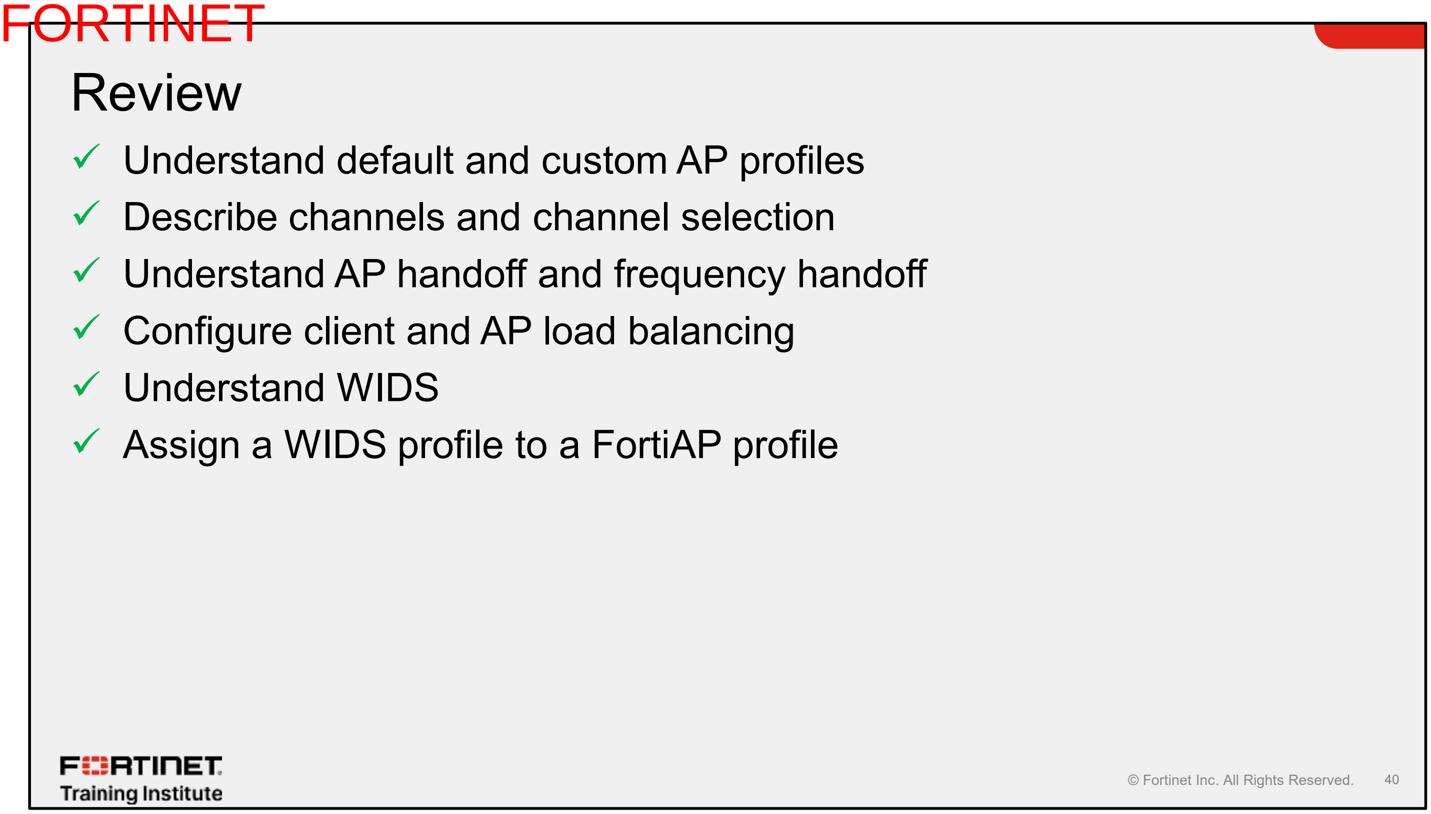


Lesson Progress

- ✓ Custom AP Profiles and Radio Settings
- ✓ Wireless Load Balancing
- ✓ Wireless Intrusion Detection System

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



Review

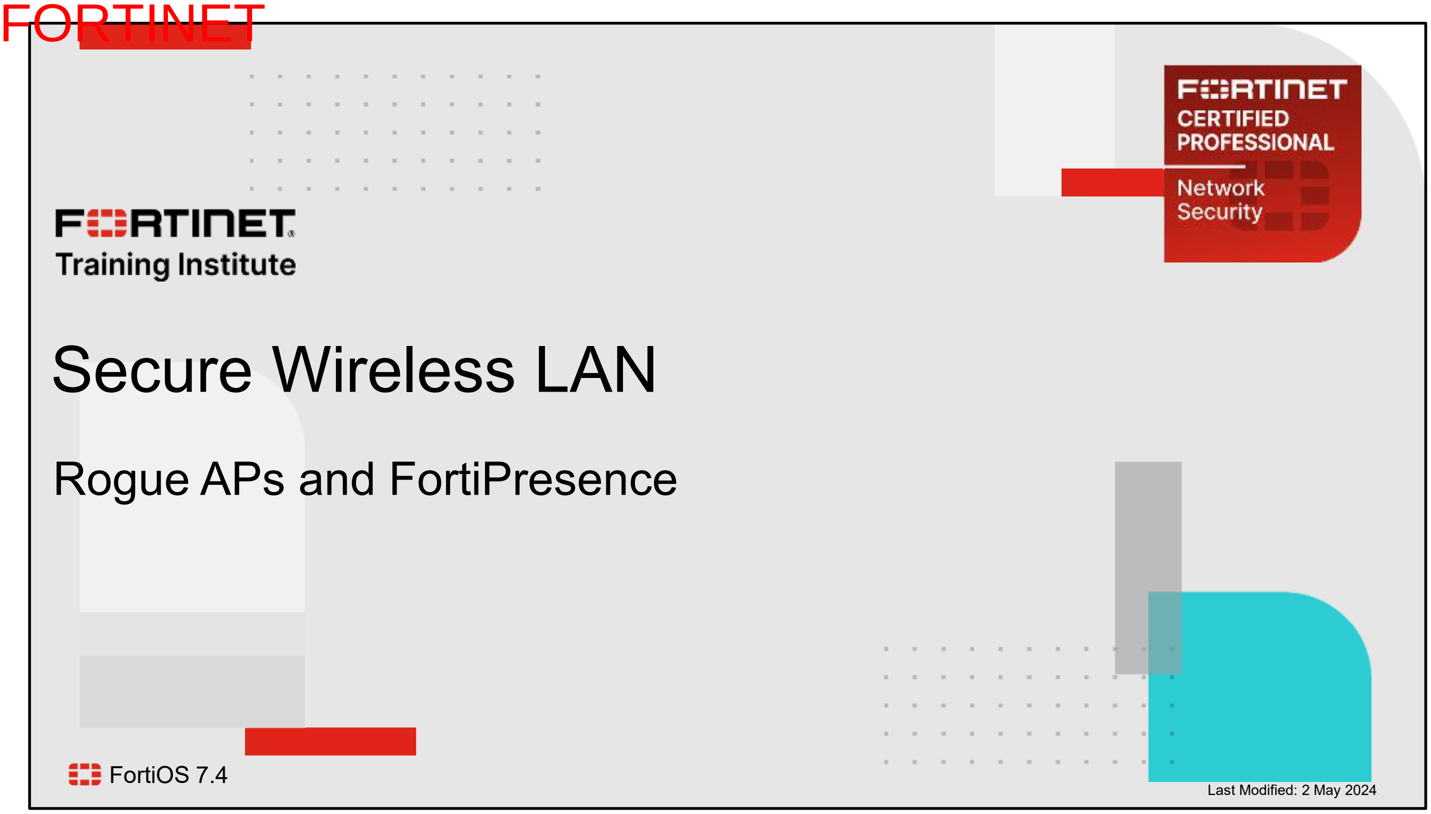
- ✓ Understand default and custom AP profiles
- ✓ Describe channels and channel selection
- ✓ Understand AP handoff and frequency handoff
- ✓ Configure client and AP load balancing
- ✓ Understand WIDS
- ✓ Assign a WIDS profile to a FortiAP profile

Training Institute

40

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about FortiAP profiles, applying radio settings, and using protection systems to monitor the wireless network.



FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL Network Security

Secure Wireless LAN

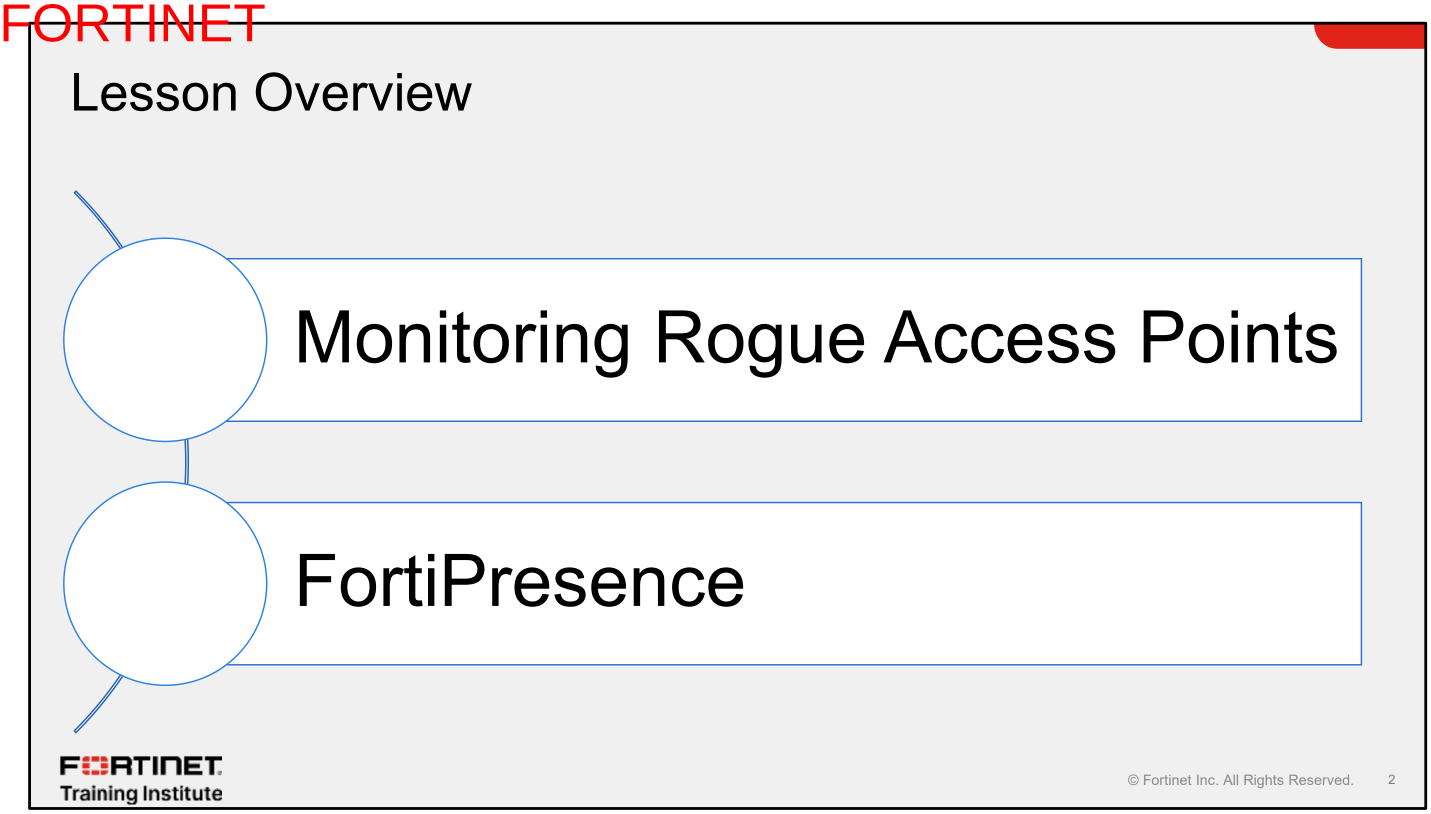
Rogue APs and FortiPresence

FortiOS 7.4

Last Modified: 2 May 2024

In this lesson, you will learn about the wireless technology concepts that you must know to understand Wi-Fi, and wireless technologies in general.

You will also learn how to plan your network for best wireless signal coverage.



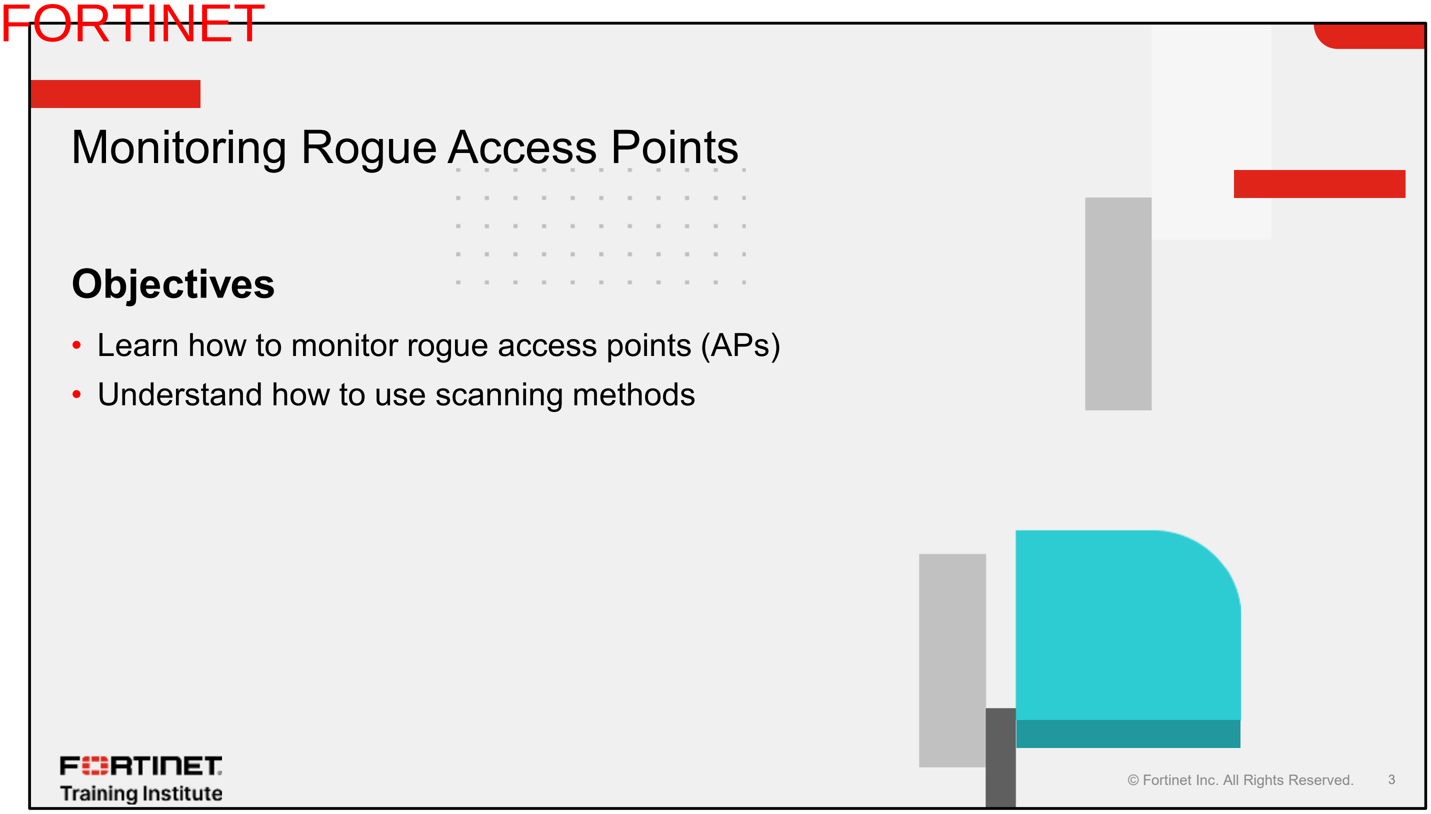
Lesson Overview

Monitoring Rogue Access Points

FortiPresence

2

In this lesson, you will learn about the topics shown on this slide.



Monitoring Rogue Access Points

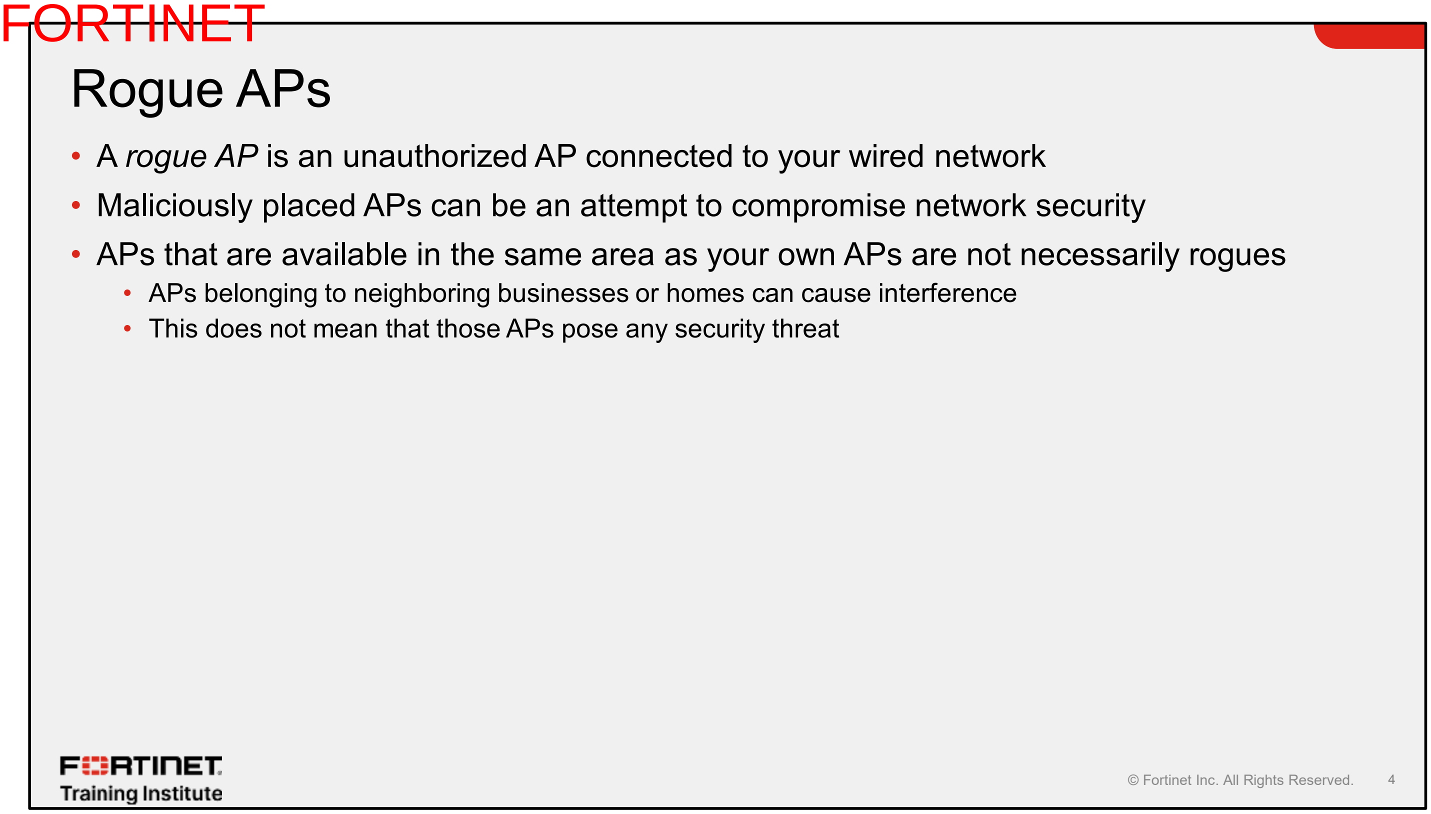
Objectives

- Learn how to monitor rogue access points (APs)
- Understand how to use scanning methods

FORTINET Training Institute

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in monitoring rogue APs and using the scanning options available on FortiOS, you will be able to protect your wireless network from rogue APs.



Rogue APs

- A *rogue AP* is an unauthorized AP connected to your wired network
- Maliciously placed APs can be an attempt to compromise network security
- APs that are available in the same area as your own APs are not necessarily rogues
  - APs belonging to neighboring businesses or homes can cause interference
  - This does not mean that those APs pose any security threat

FERTINET Training Institute

4

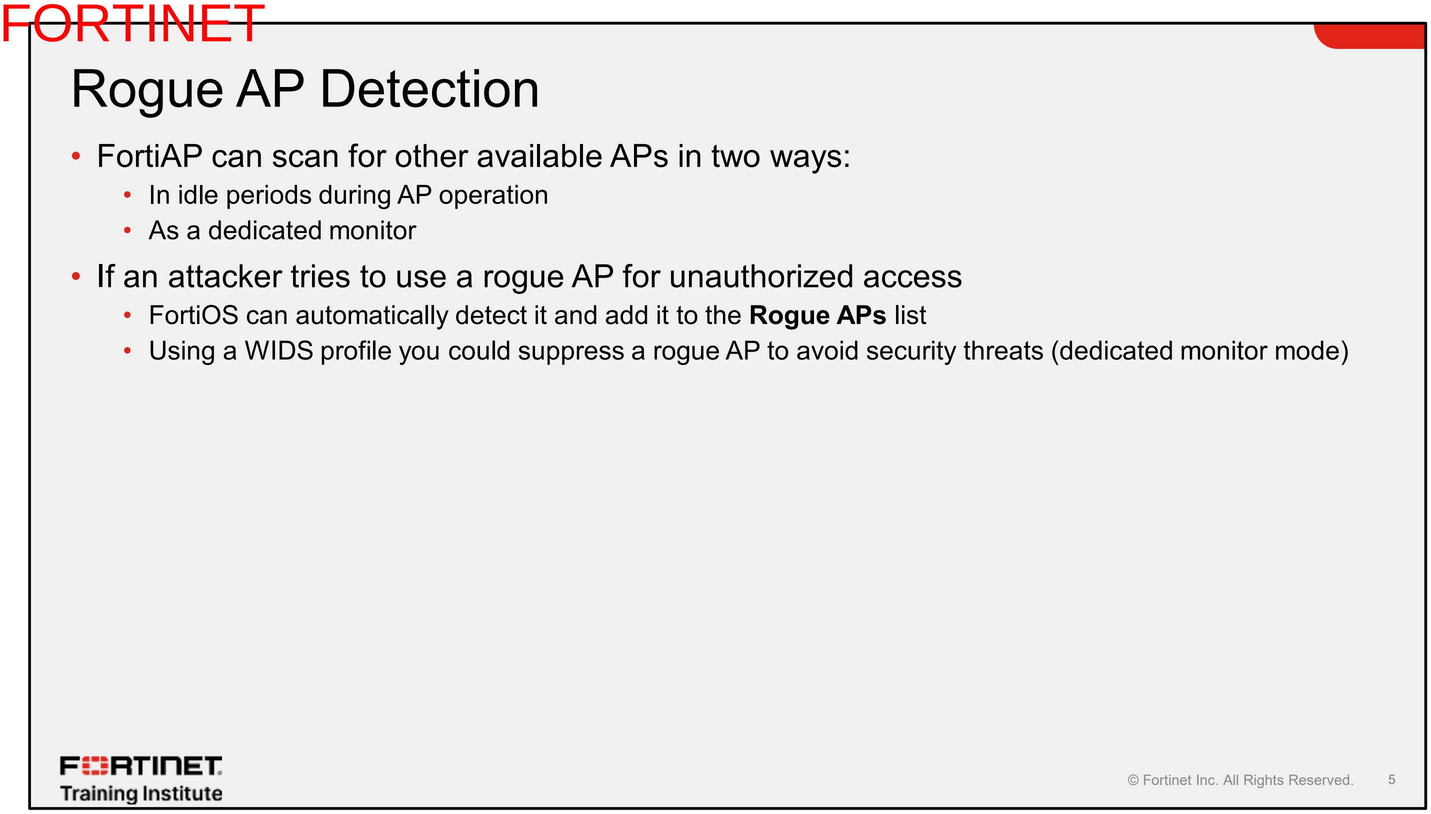
So far, you've seen settings for APs that you control. What about APs that you don't control?

Often, these APs belong to neighboring businesses or homes. They may cause interference, which you will notice if you perform spectrum analysis, but they are not a security threat.

However, this is not always true. Maliciously placed APs (called rogue APs) can be an attempt to compromise network security. If you detect unauthorized APs in the middle of a large warehouse, for example, these are unlikely to belong to a neighbor, who would be out of range. They may be a security threat.

A rogue AP can cause two problems:

- It can cause signal interference, preventing clients from being able to use your wireless network.
- If it's connected to your network, it could provide unauthorized access.



Rogue AP Detection

- FortiAP can scan for other available APs in two ways:
  - In idle periods during AP operation
  - As a dedicated monitor
- If an attacker tries to use a rogue AP for unauthorized access
  - FortiOS can automatically detect it and add it to the **Rogue APs** list
  - Using a WIDS profile you could suppress a rogue AP to avoid security threats (dedicated monitor mode)

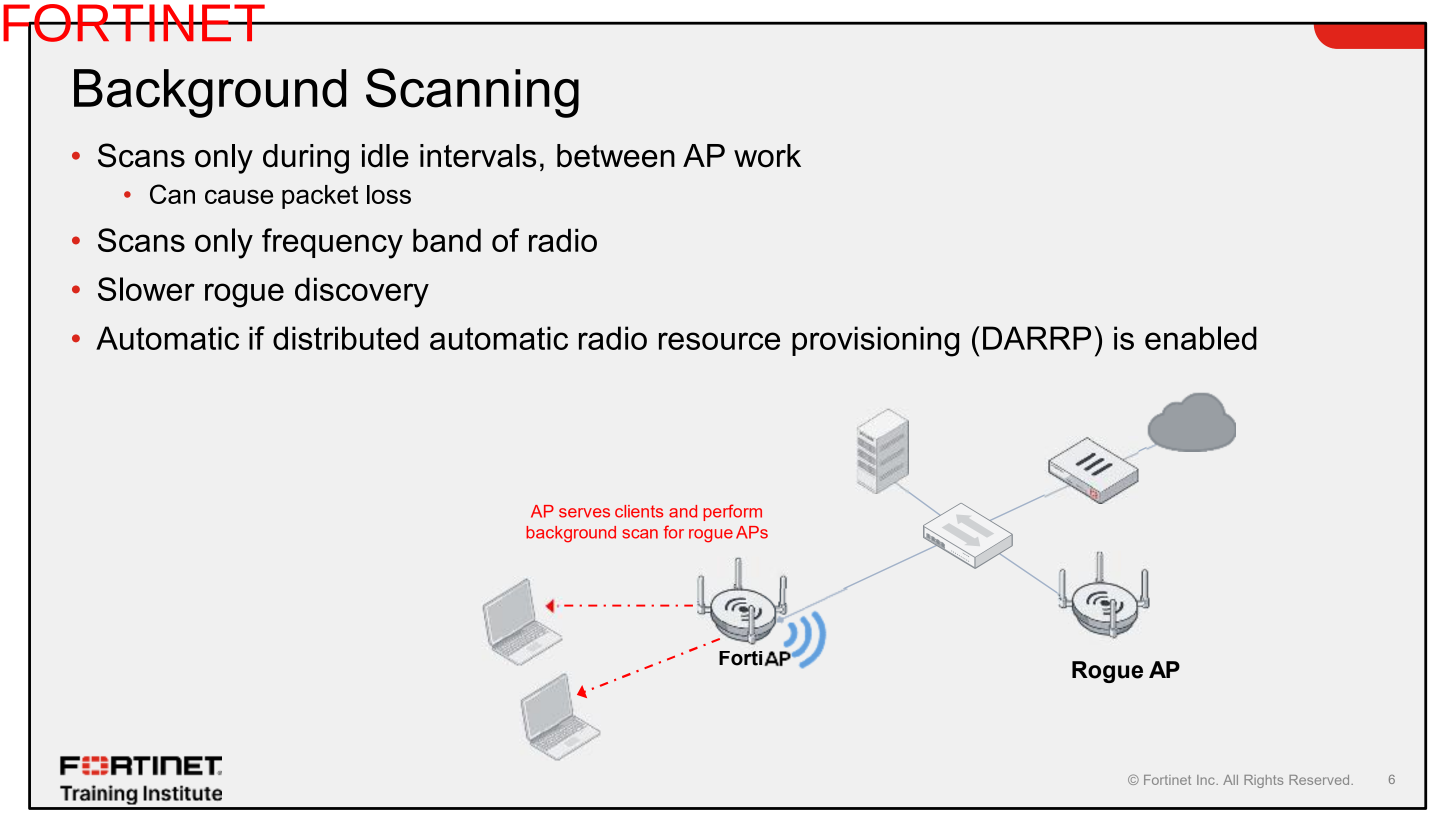
FORTINET Training Institute

5

There are two ways to configure FortiAP to detect rogue APs:

- As a dedicated monitor (can assign one or both radios)
- In idle periods during AP operation

You can also use one radio of an AP for scanning and reserve the other radio for normal AP use, but this will limit you to using only one frequency—2.4 GHz or 5 GHz—because you can use only one band per radio. When a rogue AP is connected, an attacker tries to use it for unauthorized access. FortiOS automatically detects and lists it in the **Rogue AP Monitor**, and you can suppress it to avoid security threats.



Background Scanning

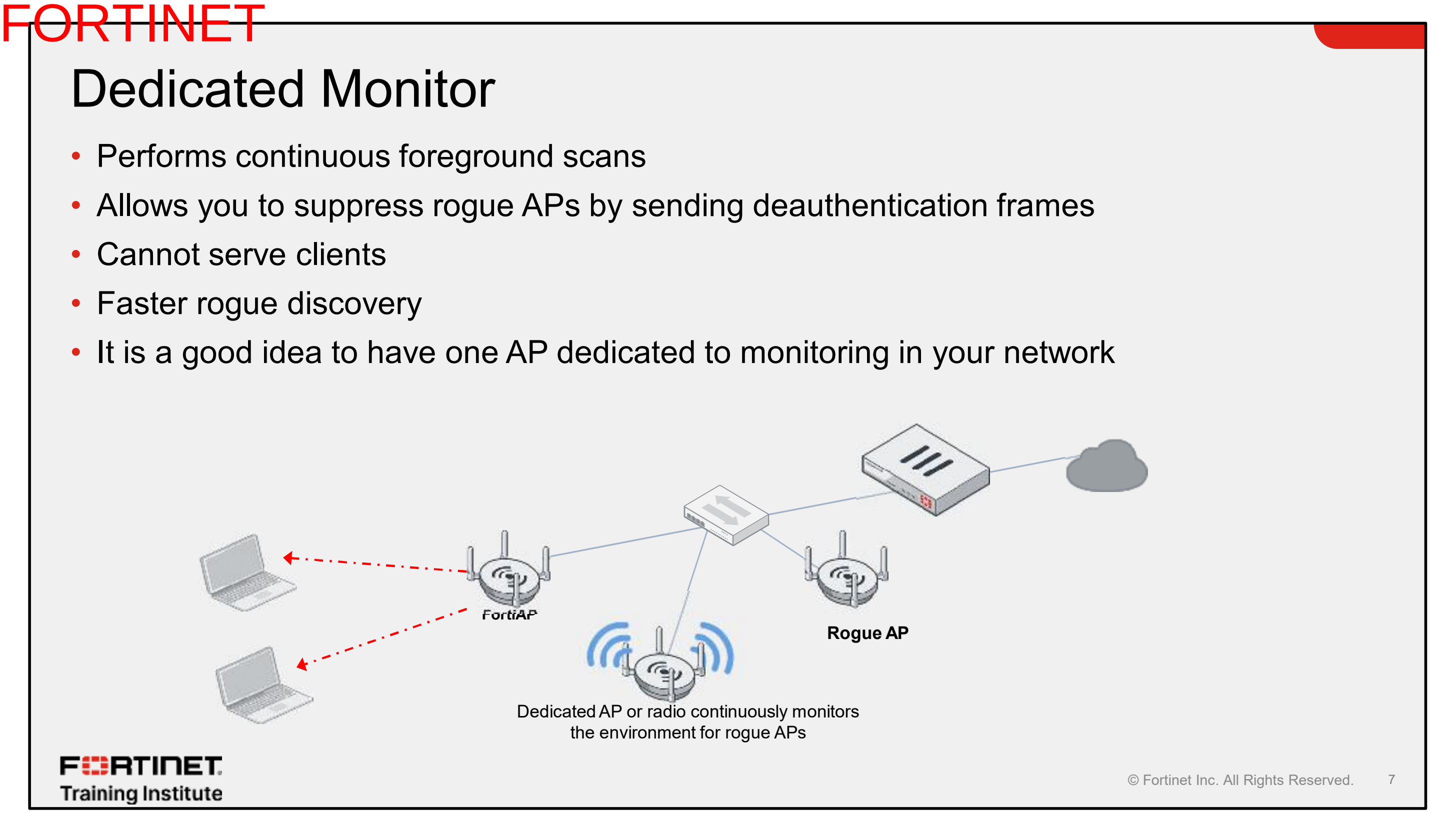
- Scans only during idle intervals, between AP work
  - Can cause packet loss
- Scans only frequency band of radio
- Slower rogue discovery
- Automatic if distributed automatic radio resource provisioning (DARRP) is enabled

AP serves clients and perform background scan for rogue APs

6

If you do not use a dedicated AP or a radio for scanning, you can configure the AP to run a background scan when a radio is idle or at a defined threshold.

A background scan is opportunistic. During idle periods, FortiAP briefly switches the radio from acting as an AP to monitoring. By default, a scan period starts every 600 seconds, and each second a different channel is monitored for 20 ms until all channels have been checked. During heavy AP traffic, it is possible for background spectrum analysis scanning to cause lost packets when the radio switches to monitoring. This technique is enabled with DARRP and offers poor rogue AP detection.



Dedicated Monitor

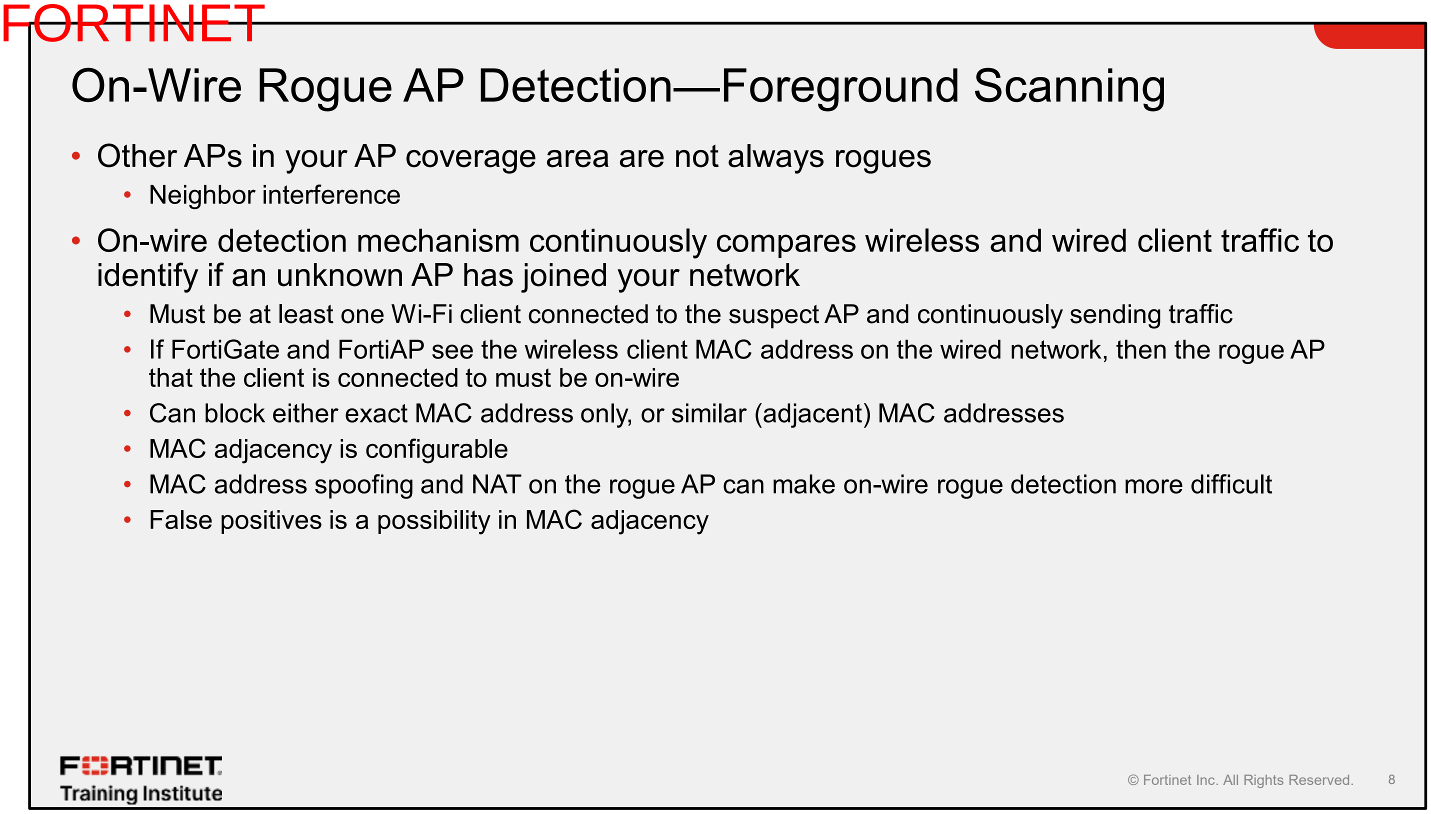
- Performs continuous foreground scans
- Allows you to suppress rogue APs by sending deauthentication frames
- Cannot serve clients
- Faster rogue discovery
- It is a good idea to have one AP dedicated to monitoring in your network

Dedicated AP or radio continuously monitors the environment for rogue APs

How does rogue AP detection in FortiOS work? It uses a radio to *listen* and detect other APs. If your FortiAP device is not using all of its radios, you can dedicate one of them to monitoring for rogue APs. Otherwise, you can configure the AP to run a background scan when a radio is idle.

You should use one AP in your network as a dedicated monitor AP because it can reduce the load on other APs and saves them from switching to AP and monitoring mode.

Dedicated monitor radios are reserved for scanning and suppression, if enabled. They will not broadcast the SSID, and will not allow any wireless clients to join with them. This is the technique required to actively suppress rogue APs.



On-Wire Rogue AP Detection—Foreground Scanning

- Other APs in your AP coverage area are not always rogues
  - Neighbor interference
- On-wire detection mechanism continuously compares wireless and wired client traffic to identify if an unknown AP has joined your network
  - Must be at least one Wi-Fi client connected to the suspect AP and continuously sending traffic
  - If FortiGate and FortiAP see the wireless client MAC address on the wired network, then the rogue AP that the client is connected to must be on-wire
  - Can block either exact MAC address only, or similar (adjacent) MAC addresses
  - MAC adjacency is configurable
  - MAC address spoofing and NAT on the rogue AP can make on-wire rogue detection more difficult
  - False positives is a possibility in MAC adjacency

Training Institute

© Fortinet Inc. All Rights Reserved. 8

Another useful technique for rogue AP detection is on-wire detection. When you enable on-wire detection, FortiOS compares MAC addresses in wireless and wired traffic. If FortiOS and FortiAP see the wireless client MAC address on the wired network, then the rogue AP that the client is connected to must be on-wire. This usually requires the rogue AP to be a Layer 2 bridged AP. Otherwise FortiOS will see only the wireless router Ethernet MAC.

The on-wire can uses two rogue detection methods:

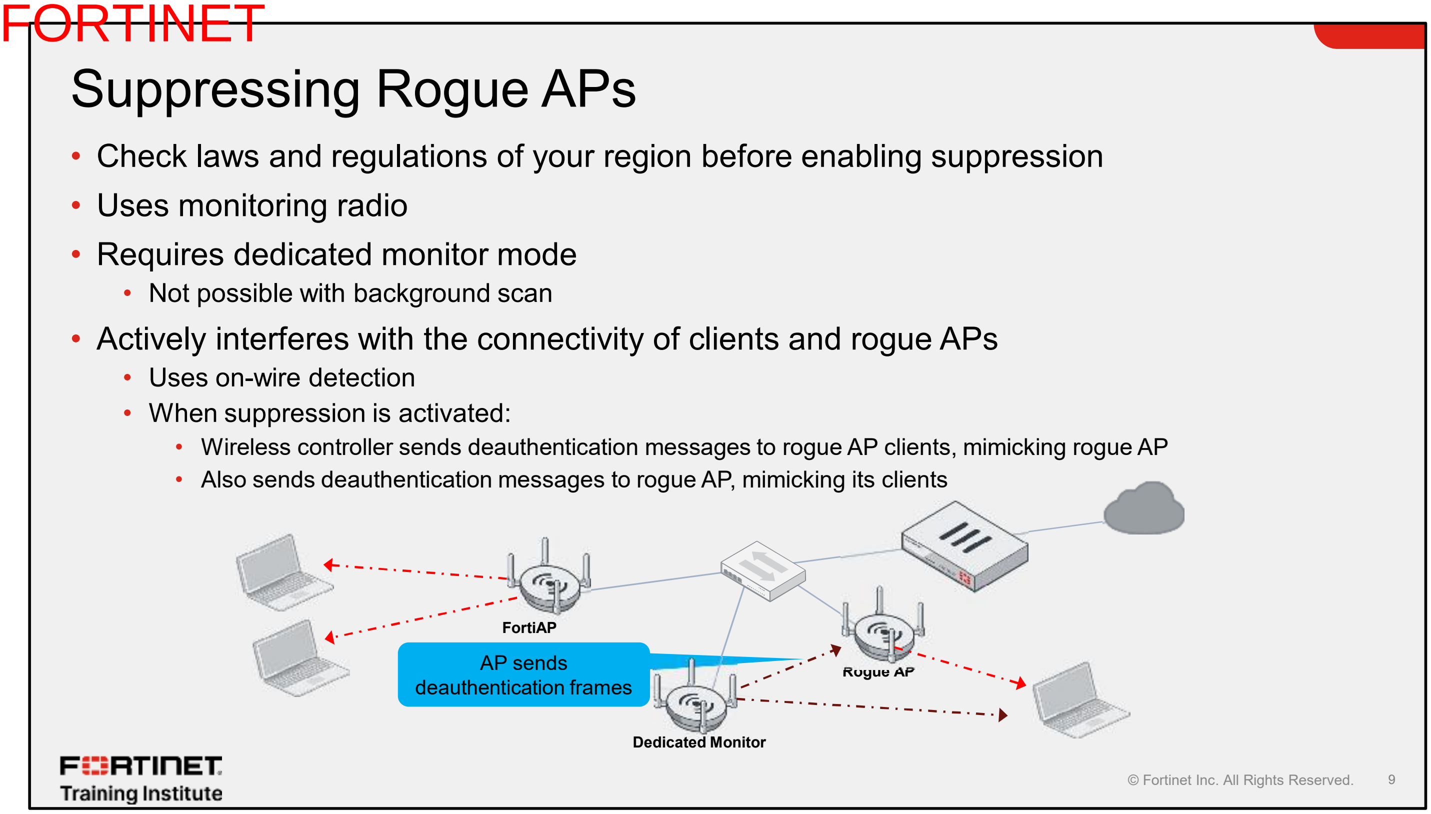
- **Exact MAC address match**: If the same MAC address is seen in frames on the wired LAN and on the Wi-Fi network, this means that the wireless client is connected to the LAN. In your FortiOS configuration, if you did not authorize the AP that the client is using, then FortiOS will treat that AP as an on-wire rogue.
- **MAC adjacency**: If an AP is a wireless router, it applies NAT to Wi-Fi packets. This can make rogue detection more difficult, because the frames in wired and wireless traffic won't have the same MAC address either. Usually, however, an the Wi-Fi interface MAC address of an AP is similar to its wired MAC address. So, the MAC adjacency rogue detection method matches the MAC addresses that have close hexadecimal numbers.
- You can change this setting using the CLI command: `set rogue-scan-mac-adjacency {integer}`.

The integer value 0 to 31 represents the maximum numerical difference between an the Ethernet and wireless MAC values of an AP to match for rogue detection. The default value is 7.

In both cases, whether exact match or MAC adjacency, the process is as follows:

1. A dedicated radio listens for each AP BSSID, and for wireless client MAC addresses connected to that AP.
2. FortiAP collects wired MAC addresses seen through ARP requests, and sends them to the wireless controller.
3. FortiGate compares wireless and wired MAC addresses.
4. If traffic of an unauthorized AP traffic is also seen on the wire, the wireless controller logs an alert. If suppression is enabled, the wireless controller also tries to interfere with the unauthorized connections.

If an AP is found by on-wire detection, it shows up in the AP monitor with in its **On-wire** column. Note that because of the nature of the MAC adjacency method, there is a possibility of false positives.



Suppressing Rogue APs

- Check laws and regulations of your region before enabling suppression
- Uses monitoring radio
- Requires dedicated monitor mode
  - Not possible with background scan
- Actively interferes with the connectivity of clients and rogue APs
  - Uses on-wire detection
  - When suppression is activated:
    - Wireless controller sends deauthentication messages to rogue AP clients, mimicking rogue AP
    - Also sends deauthentication messages to rogue AP, mimicking its clients

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

After you’ve detected a rogue AP, usually you will want to actively prevent your users from connecting to it. You can use the radios of your FortiAPs to suppress them.

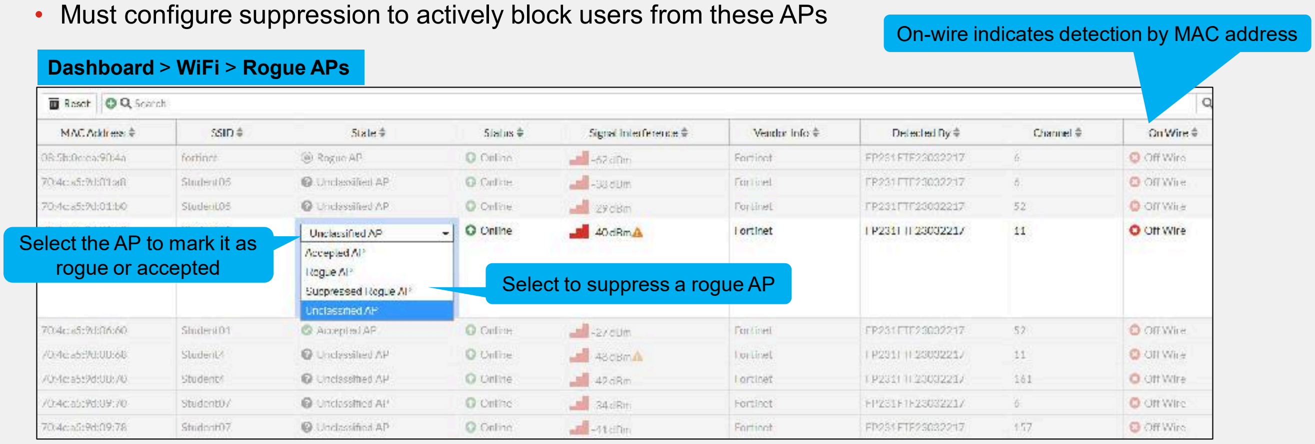
Before enabling this feature, verify that the operation of rogue suppression is compliant with the applicable laws and regulations of your region.

Because it’s an active process, it requires that you dedicate one of the FortiAPs radios. You can’t use it with a background scan.

How does suppression work? While pretending to be the rogue AP, the FortiGate Wi-Fi controller uses the dedicated monitoring radio on a nearby AP. It sends *deauthentication messages* to the rogue AP clients. This makes it difficult for them to maintain a connection with it. FortiOS also mimics the rogue AP clients, sending deauthentication messages to the rogue AP.

Rogue AP Monitor

- Discovered APs are listed in the **Rogue AP Monitor** list
  - You can mark them as **Accepted** or **Rogue**
- This is only a designation to help tracking AP in your environment
  - It does not affect the ability to use these APs
  - Must configure suppression to actively block users from these APs



Dashboard > WiFi > Rogue APs

On-wire indicates detection by MAC address

Select the AP to mark it as rogue or accepted

Select to suppress a rogue AP

MAC Address	SSID	State	Status	Signal Interference	Vendor Info	Detected By	Channel	On Wire
08:5b:0e:ca:90:4a	fortinet	Rogue AP	Online	-62 dBm	Fortinet	FP231FTF23032217	6	Off Wire
70:4c:a5:9d:01:a8	Student05	Unclassified AP	Online	-38 dBm	Fortinet	FP231FTF23032217	6	Off Wire
70:4c:a5:9d:01:b0	Student05	Unclassified AP	Online	29 dBm	Fortinet	FP231FTF23032217	52	Off Wire
		Unclassified AP	Online	40 dBm	Fortinet	FP231FTF23032217	11	Off Wire
70:4c:a5:9d:06:60	Student01	Accepted AP	Online	-27 dBm	Fortinet	FP231FTF23032217	52	Off Wire
70:4c:a5:9d:00:68	Student4	Unclassified AP	Online	48 dBm	Fortinet	FP231FTF23032217	11	Off Wire
70:4c:a5:9d:00:70	Student4	Unclassified AP	Online	42 dBm	Fortinet	FP231FTF23032217	161	Off Wire
70:4c:a5:9d:09:70	Student07	Unclassified AP	Online	34 dBm	Fortinet	FP231FTF23032217	6	Off Wire
70:4c:a5:9d:09:78	Student07	Unclassified AP	Online	-11 dBm	Fortinet	FP231FTF23032217	157	Off Wire

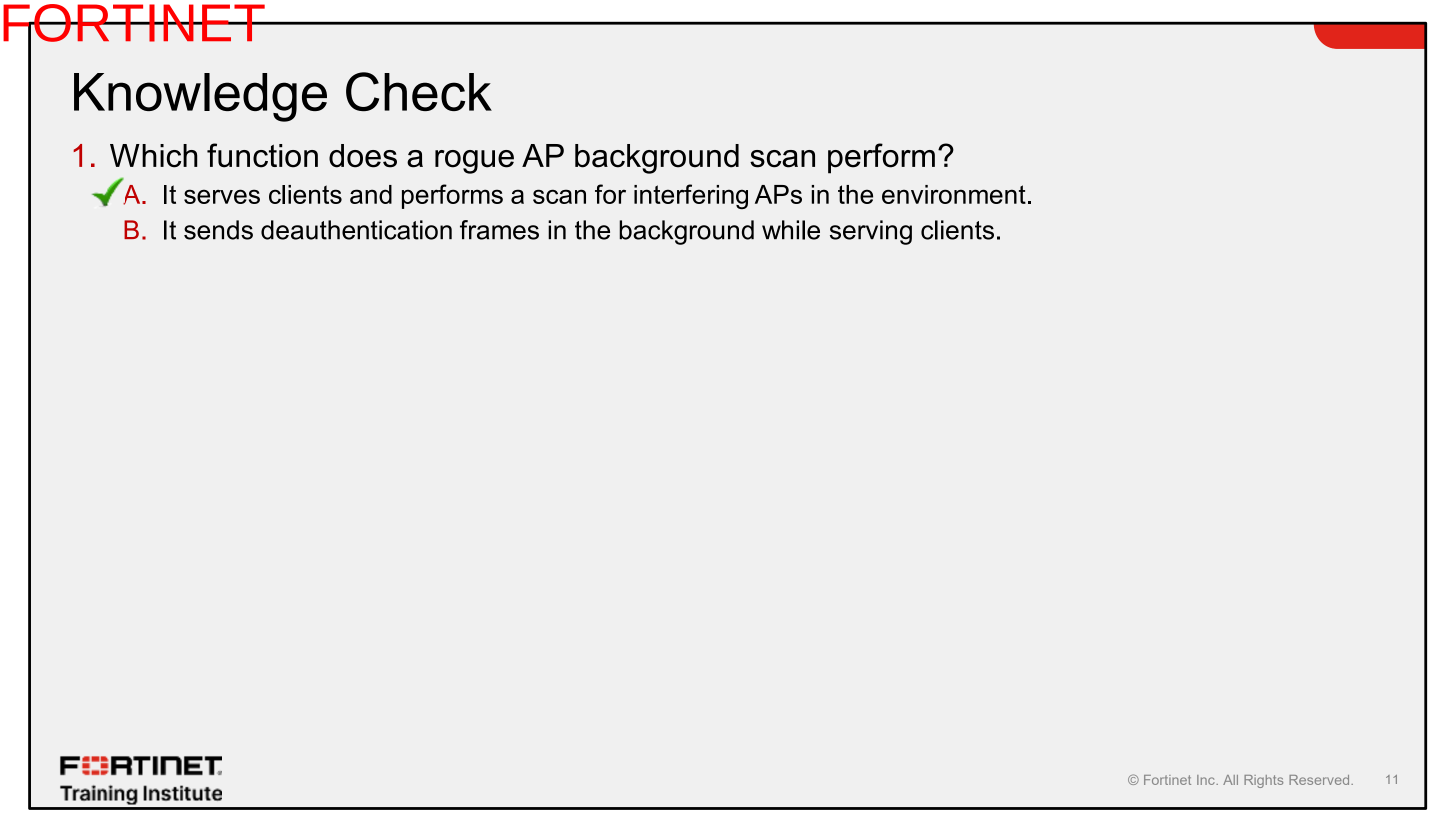
Training Institute

10

When a new AP is detected that is not authorized, this AP appears in the **Rogue APs** list, and you can change the state of each AP to either **Accepted AP** or **Rogue AP**. This helps you to track which APs are authorized by you or not. By default, it does not affect anyone's ability to use these access points. For that, you need to select **Suppressed Rogue AP**.

Note that this mechanism is the only feature that is specifically called a *rogue AP detection* feature in the FortiOS. There are more ways to discover rogue APs, including:

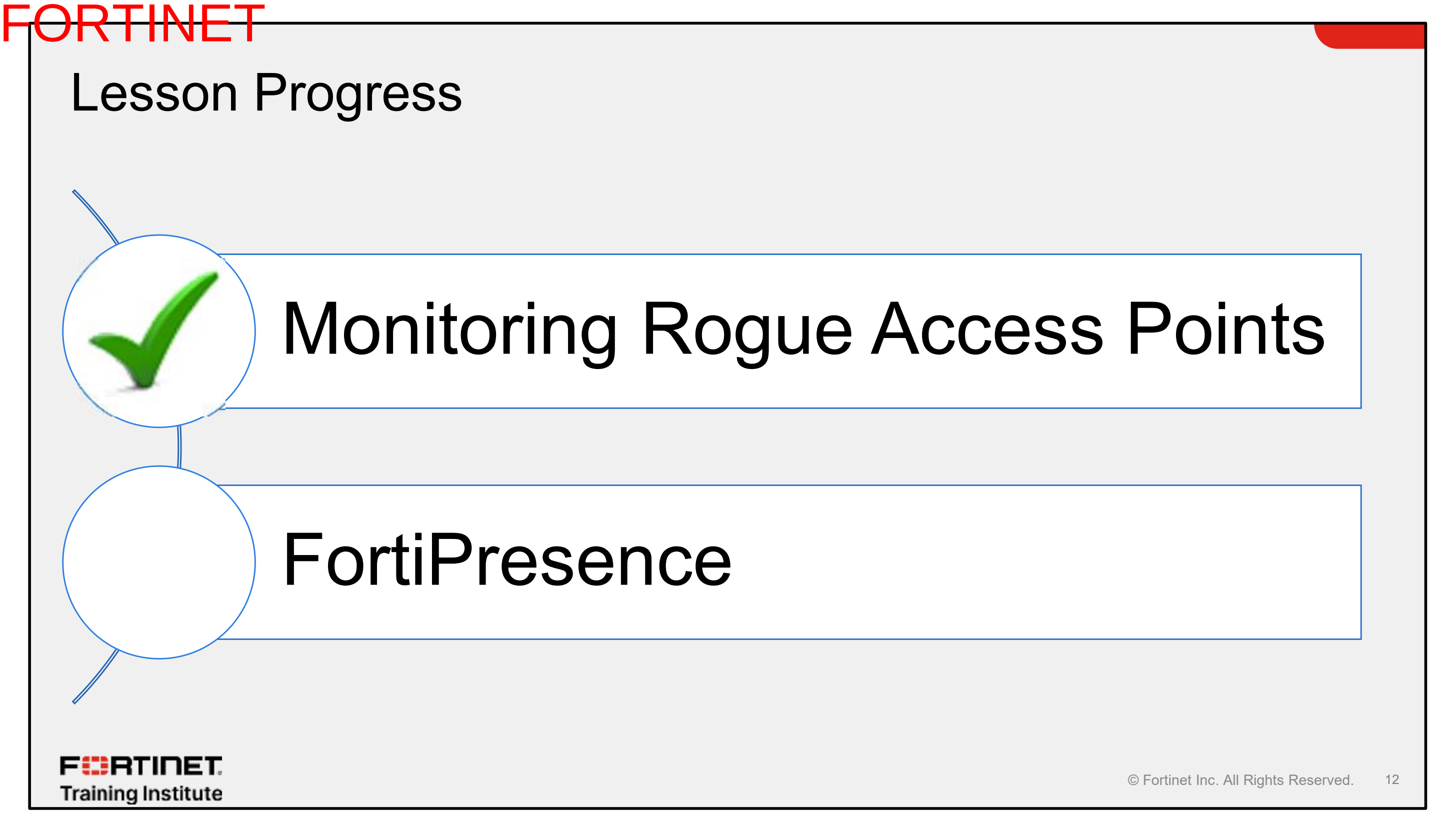
- Audit grade reports
- On-wire correlation
- Automatic suppression
- Wireless IDS (WIDS)



Knowledge Check

1. Which function does a rogue AP background scan perform?
   - ✓ A. It serves clients and performs a scan for interfering APs in the environment.
   - B. It sends deauthentication frames in the background while serving clients.

FORTINET
Training Institute



Lesson Progress

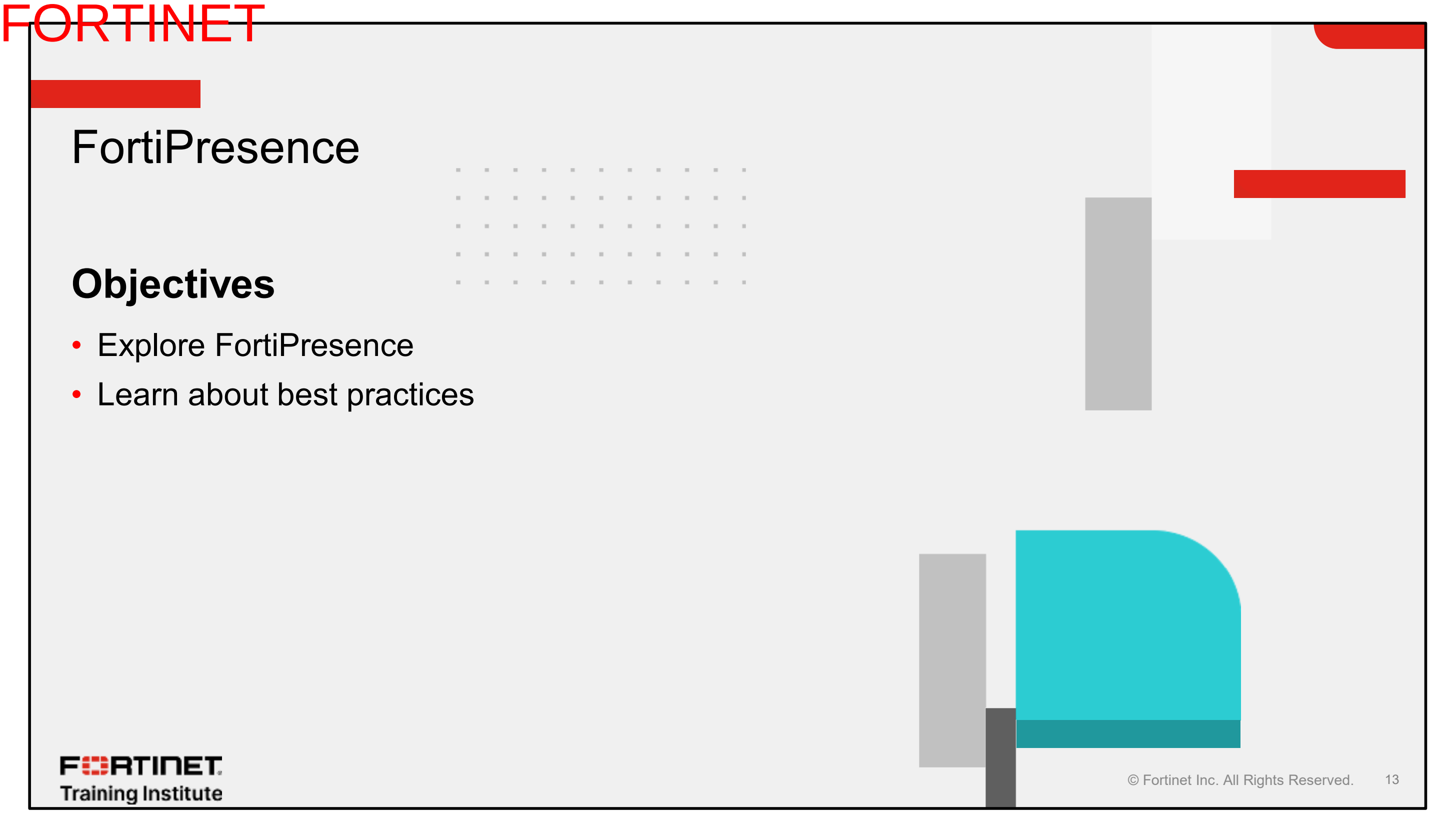
- ✓ Monitoring Rogue Access Points
- FortiPresence

FORTINET Training Institute

12

Good job! You now understand rogue APs and how to monitor them and take action.

Now, you will learn about using FortiPresence.



FortiPresence

Objectives

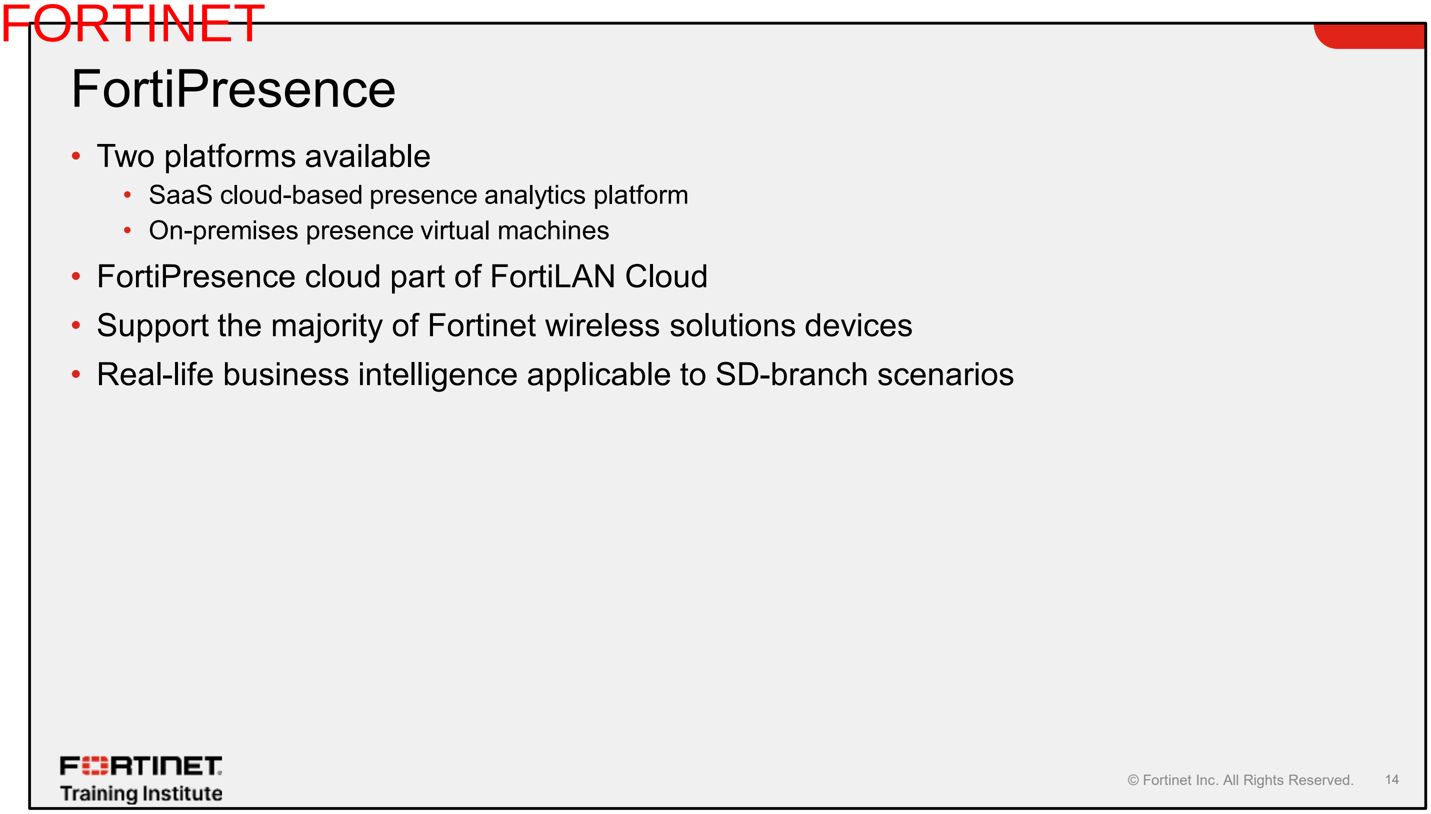
- Explore FortiPresence
- Learn about best practices

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiPresence, you will understand how to implement and use FortiPresence and its dashboard and visitor reports.



FortiPresence

- Two platforms available
  - SaaS cloud-based presence analytics platform
  - On-premises presence virtual machines
- FortiPresence cloud part of FortiLAN Cloud
- Support the majority of Fortinet wireless solutions devices
- Real-life business intelligence applicable to SD-branch scenarios

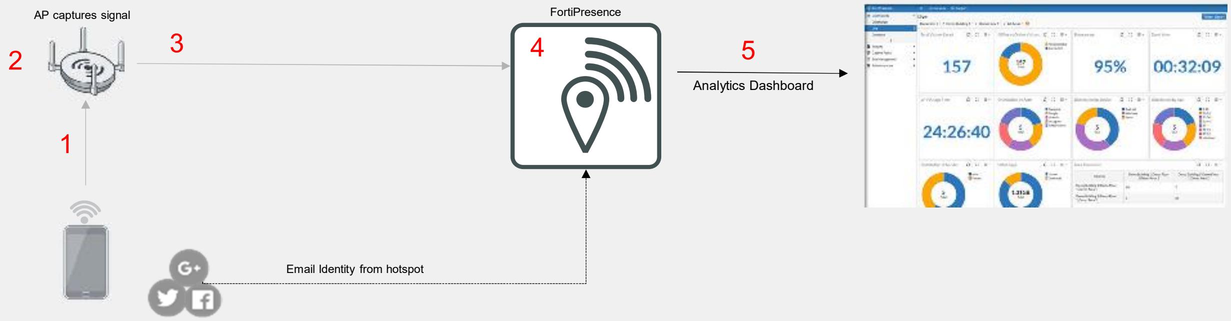
There are two different platforms to use FortiPresence analytics:

- FortiPresence cloud: A SaaS cloud-based presence analytics platform which is supported by all of Fortinet wireless solutions and very applicable to SD-branch scenarios.
- FortiPresence VM: An on-premises solution that runs as virtual machines and run locally on your site.

Designed and built for real-life business intelligence, FortiPresence delivers the insights customers need using the data most never even knew they had.

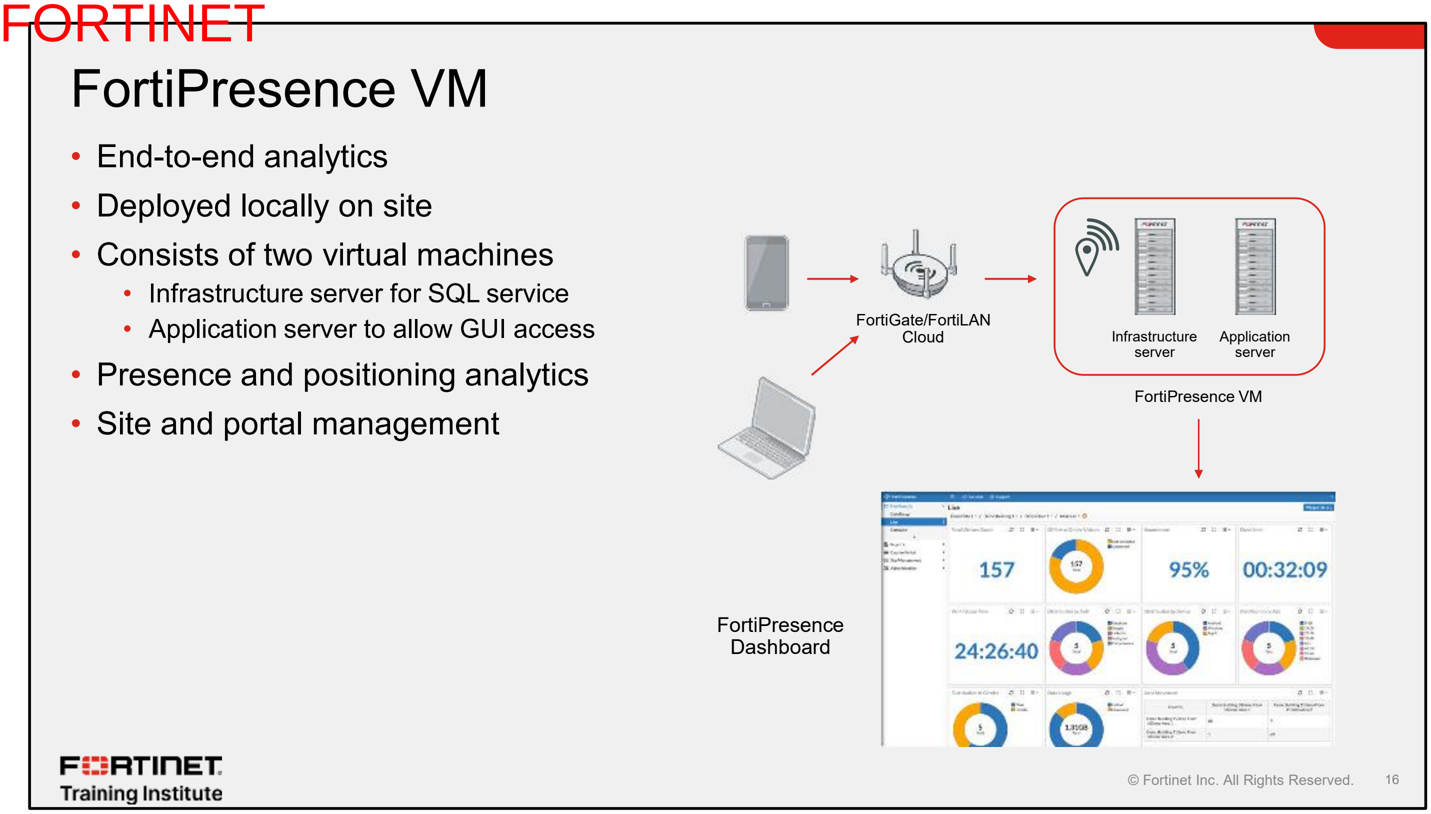
FortiPresence—How It Works

- Smartphone emits Wi-Fi probe
- FortiAP or FortiWiFi captures MAC address and signal strength
- FortiAP collects and summarizes the data records
- FortiAP pushes data to FortiPresence in a secured SSL connection
  - Every 10 seconds (configurable)
- Data is displayed in the analytics dashboard in an actionable format



Here is an overview of how FortiPresence works:

1. A smartphone emits a Wi-Fi probe signal, even if it is in a visitor's pocket and not connected to the Wi-Fi network.
2. FortiAP or FortiWiFi captures the MAC address and signal strength information from the smartphone.
3. Onsite APs or FortiLAN Cloud summarizes and forwards the data records.
4. FortiPresence service receives data.
5. FortiPresence analytics engine processes and correlates the data.
6. Data is displayed in the analytics dashboard in an actionable format.
7. Data collected can show dwell time, visit frequency, visit duration, foot traffic, visitor density, locations comparison, and more.
8. Information can be used to improve business and customer experience.



FortiPresence VM

- End-to-end analytics
- Deployed locally on site
- Consists of two virtual machines
  - Infrastructure server for SQL service
  - Application server to allow GUI access
- Presence and positioning analytics
- Site and portal management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

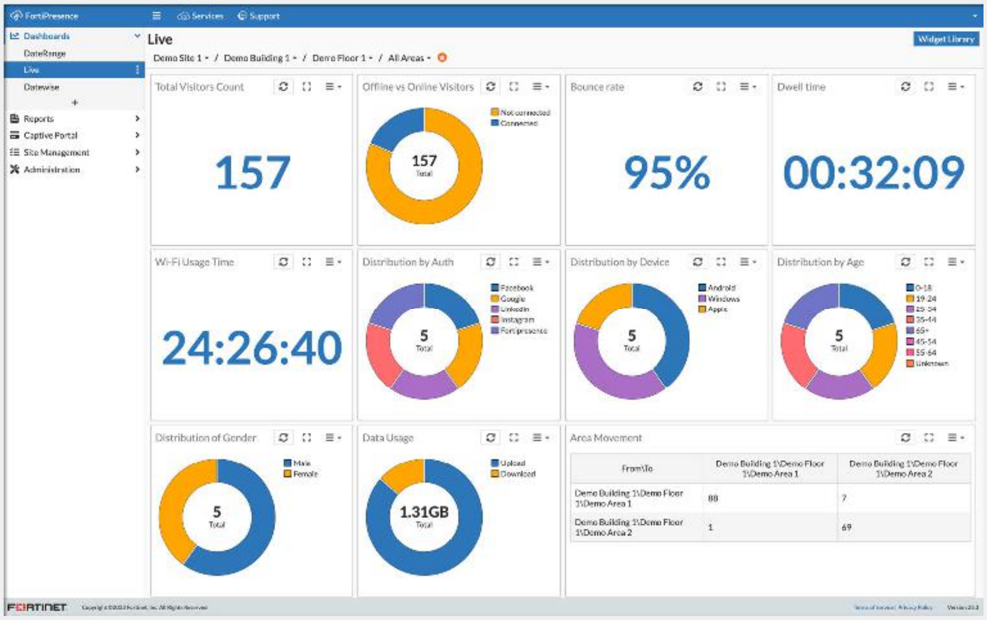
Fortinet APs deployed at business establishments are leveraged to detect wireless signals for the customer. In a typical business setup, visitor smartphones and devices probe for wireless APs.

FortiPresence VM provides an end-to-end presence analytics solution deployed locally, on-premises. It supports all Fortinet wireless APs, whether they are managed by FortiGate or FortiAP Cloud wireless controllers. The APs send visitor data in the form of station reports directly to FortiPresence VM.

The customizable dashboards and reports provide real-time location trends and presence analytics with animated maps and video play options to view and compare visitor data across sites.

The sites can be located using Google maps for effective visitor data analysis. The visitor can log in to the Wi-Fi infrastructure using social media authentication, SMS-OTP authentication, or a customized visitor portal.

FortiPresence—Dashboard



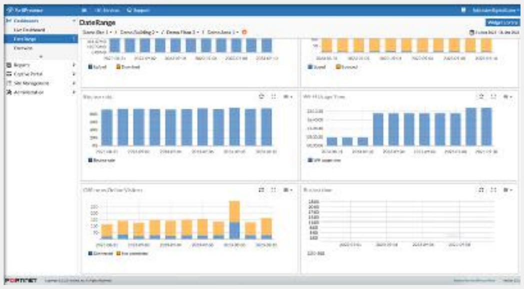
From\To	Demo Building 1\Demo Floor 1\Demo Area 1	Demo Building 1\Demo Floor 1\Demo Area 2
Demo Building 1\Demo Floor 1\Demo Area 1	88	7
Demo Building 1\Demo Floor 1\Demo Area 2	1	69

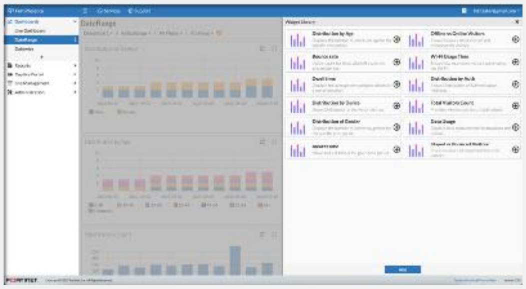
The FortiPresence dashboard provides a summary view of presence analytics. It provides a customizable graphical representation of visitor, device, and site analytics for specific locations and date ranges. This provides a comprehensive data analytics of the consumer traffic patterns in the establishment. The aggregate trends depicted in the dashboard panels are recorded over a period as configured.

The APs through FortiGate and FortiLAN Cloud controllers send the aggregated client data (station reports) to the cloud analytics engine as per configured time intervals. The analytics engine processes this raw data which is then compiled into summary charts and statistics. This data is fetched and displayed on the dashboard when you access it. The panels displayed on the dashboard can be rearranged.

FortiPresence—Analytics

- Gathers details on site visitors
- Compare current data with historical records
- Type of information such as:
  - Dwell time
  - Bounce rate
  - Engagement
  - Floor widget
  - Device type breakdowns
  - Demographics breakdowns





FORTINET Training Institute

18

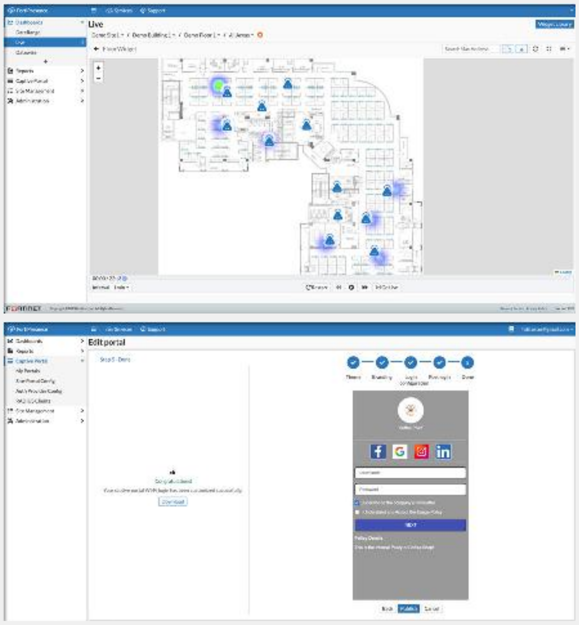
FortiPresence collects information about the organization’s visitors, such as details about devices and locations, and then presents that information as analytical reports. You can compare the data in the reports with previously recorded data to recognize trends as they occur, and then to correlate to events and initiatives being taken at the location.

The dashboard calculates the average statistics during the selected time range and displays it on the dashboard. The dashboard provides real-time data and analytics based on the following parameters:

- Dwell time
- Bounce rate
- Engagement
- Floor widget
- Device type breakdowns
- Demographics breakdowns

FortiPresence—Location Analytics

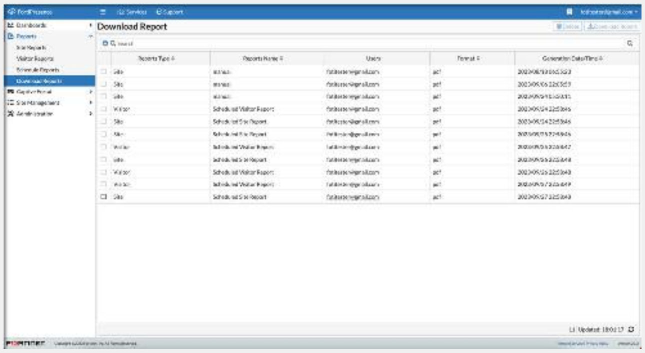
- Collects location data from FortiGate, FortiLAN Cloud
- Includes analytics, heat maps, and reporting
- Offers captive portal-based Wi-Fi access using Facebook, email, or phone number login
- Can be used in stores, shopping malls, airports, and so on, to get visitors' location and behavior data



FortiPresence provides presence and positioning analytics, leveraging existing onsite Fortinet APs to detect each visitor's smartphone Wi-Fi signal. FortiPresence users can gain insight into the behaviors of visitors within their site both in real-time and across time periods. Analytical data from FortiPresence can be used to increase business efficiencies, improve visitor experiences, and positively impact the bottom line of a business.

FortiPresence—Reports

- Different site and visitor report
- Can be exported
  - CSV
  - PDF
- Reports can build
  - At a scheduled time
  - To be sent by email
- Historical list of generated reports



Download Report

	Reports Type	Reports Name	Users	Format	Generation Date/Time
□	Site	[illegible]	[illegible]	pdf	[illegible]
□	Site	[illegible]	[illegible]	pdf	[illegible]
□	Site	[illegible]	[illegible]	pdf	[illegible]
□	Visitor	Scheduled Visitor Report	[illegible]	pdf	[illegible]
□	Site	Scheduled Site Report	[illegible]	pdf	[illegible]
□	Site	Scheduled Site Report	[illegible]	pdf	[illegible]
□	Visitor	Scheduled Visitor Report	[illegible]	pdf	[illegible]
□	Site	Scheduled Site Report	[illegible]	pdf	[illegible]
□	Visitor	Scheduled Visitor Report	[illegible]	pdf	[illegible]
□	Visitor	Scheduled Visitor Report	[illegible]	pdf	[illegible]
□	Site	Scheduled Site Report	[illegible]	pdf	[illegible]

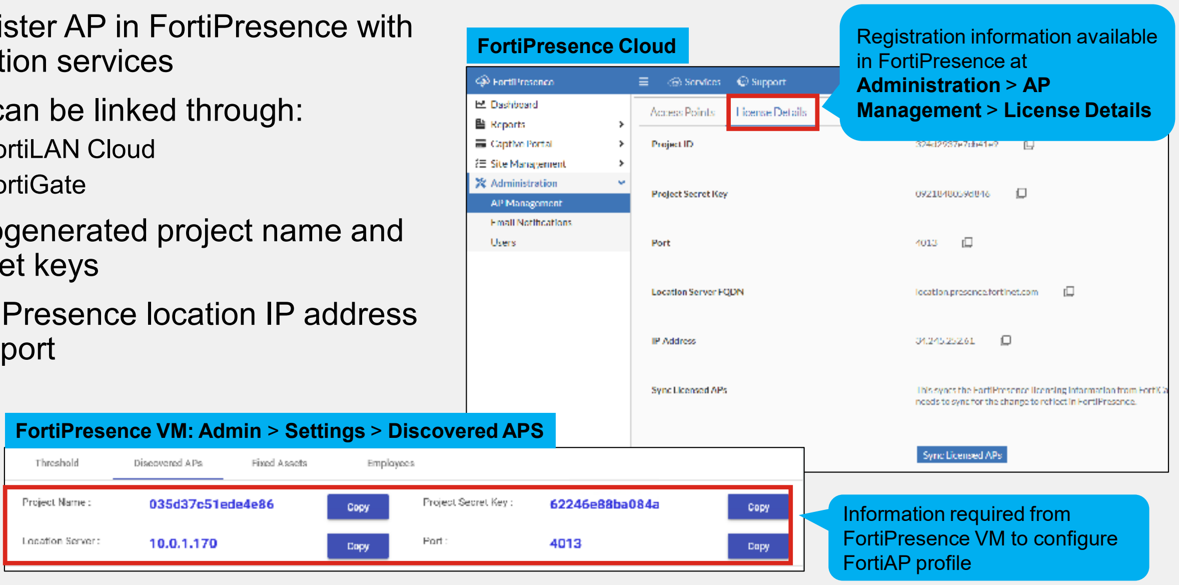
Last Updated: [illegible]

Training Institute

FortiPresence provides customizable standard report types that allow to generate and analyze visitor data for different time periods. You can create reports to view and download them for further analysis in the csv or pdf formats. These reports allow you to perform visitor, network, device, and site analysis at different time periods and for different geographic regions.

FortiPresence—Location Services

- Register AP in FortiPresence with location services
- AP can be linked through:
  - FortiLAN Cloud
  - FortiGate
- Autogenerated project name and secret keys
- FortiPresence location IP address and port



FortiPresence Cloud

Project ID 324d2937e7db41e9

Project Secret Key 09210480059d846

Port 4013

Location Server FQDN location.presence.fortinet.com

IP Address 34.245.25.261

Sync Licensed APs This syncs the FortiPresence licensing information from FortiCl... needs to sync for the change to reflect in FortiPresence.

Sync Licensed APs

Registration information available in FortiPresence at **Administration** > **AP Management** > **License Details**

FortiPresence VM: Admin > Settings > Discovered APS

Project Name : 035d37c51ede4e86 Copy

Project Secret Key : 62246e88ba084a Copy

Location Server : 10.0.1.170 Copy

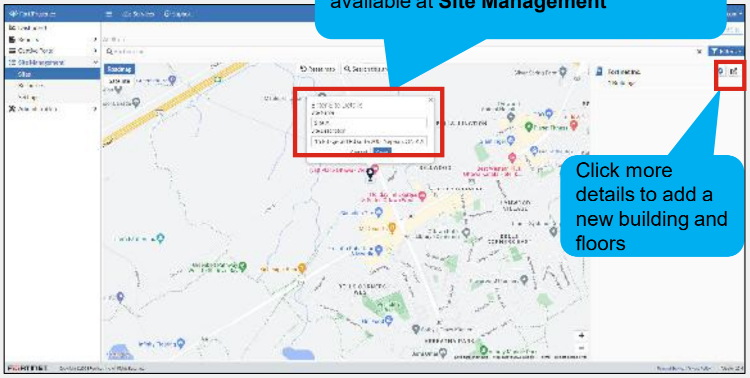
Port : 4013 Copy

Information required from FortiPresence VM to configure FortiAP profile

The FortiPresence registration process requires obtaining autogenerated information for projects to link discovered APs in FortiPresence. The project name and secret key as well as FortiPresence IP and port numbers are values that you enter when configuring FortiAP profiles if managed by FortiGate, or the location service, if managed by FortiLAN Cloud.

FortiPresence—Site Management

- Presence analytics site management
- Uses Google maps integrated UI
- Type of items to add:
  - Sites
  - Buildings
  - Floors
  - Areas
- Areas require floor definition



Creating a new site and building is available at **Site Management**

Click more details to add a new building and floors

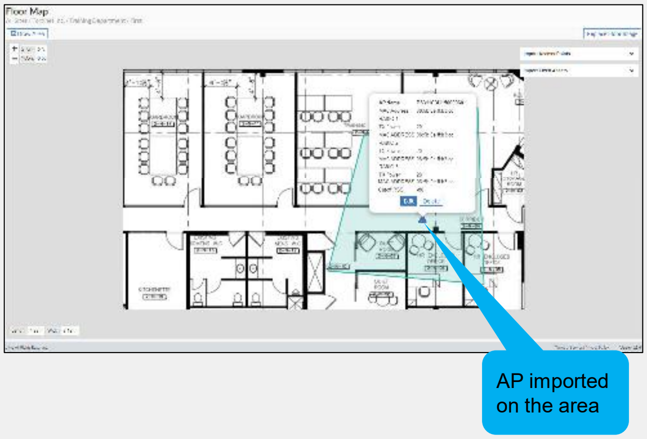
FortiPresence provides data and analytics based on demographic segmentation and visitor movement between areas. These analytics require you to define and manage the site plan where the APs are broadcasting.

This geographical data analysis provides real-time insights into user behavior. The location view of the FortiPresence GUI incorporate Google maps UI to mark locations of the sites and buildings.

Visual floor plans can be uploaded for each building to provide analytics for each floor and for each area that the floor is divided into.

FortiPresence—Site Management (Contd)

- Floor creation requires a floor plan
- Area can be specified based on known distance specified
- Add fixed assets, such as printers
- Import linked discovered AP
- Specify received signal strength indication (RSSI)
- Set effective radiated power (EIRP)



Training Institute

23

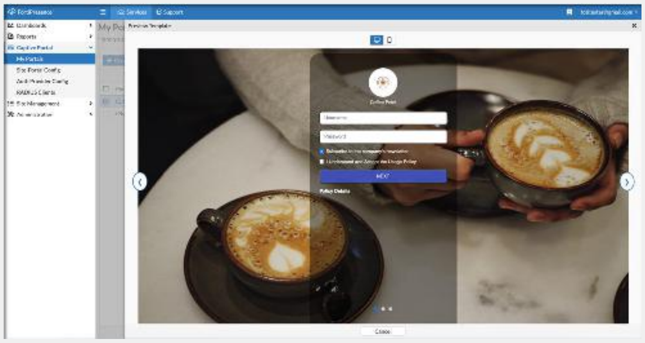
After the floor plan is created, the area design will be based on the selected distance specification that is set using red pointers on the floor map.

As the area gets defined, assets become available to drag and drop. On the floor plan, you can add fixed assets, such as printers and cameras, by dragging and dropping them on the actual location of the asset.

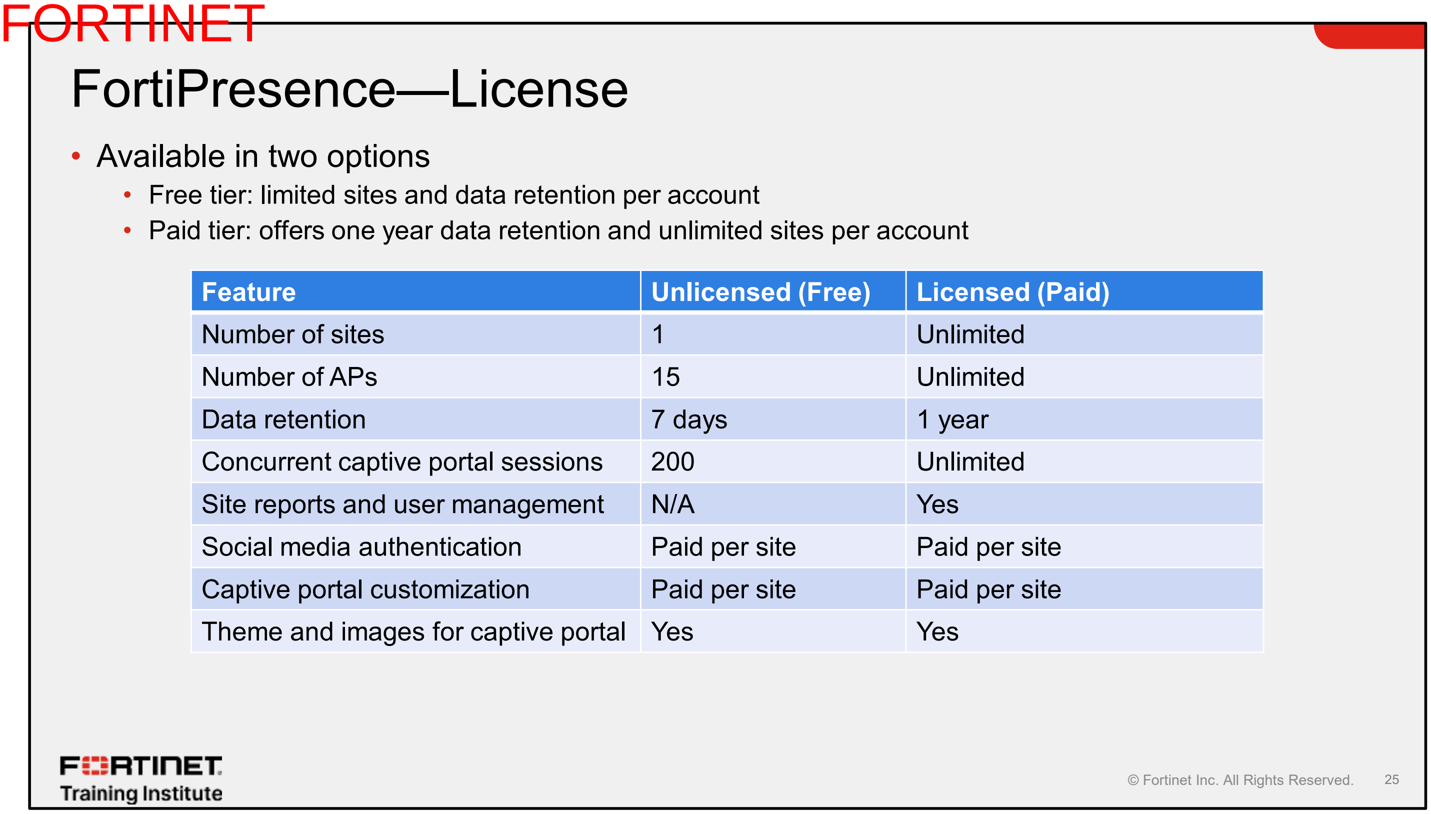
When dragging and dropping the AP, you are prompted to enter the minimum RSSI cutoff value and the EIRP values.

FortiPresence—Social Wi-Fi

- Captive portal
- Guest Wi-Fi
- Social networking credentials
- Demographic information



In our connected world, people have been conditioned to expect Wi-Fi access almost anywhere they go. ForiPresence makes providing guest Wi-Fi easy. In addition, the FortiPresence captive portal can be configured to use social networking logins. Depending on user settings, this can give FortiPresence access to additional demographic information about your visitors (such as gender identity or age).



FortiPresence—License

- Available in two options
  - Free tier: limited sites and data retention per account
  - Paid tier: offers one year data retention and unlimited sites per account

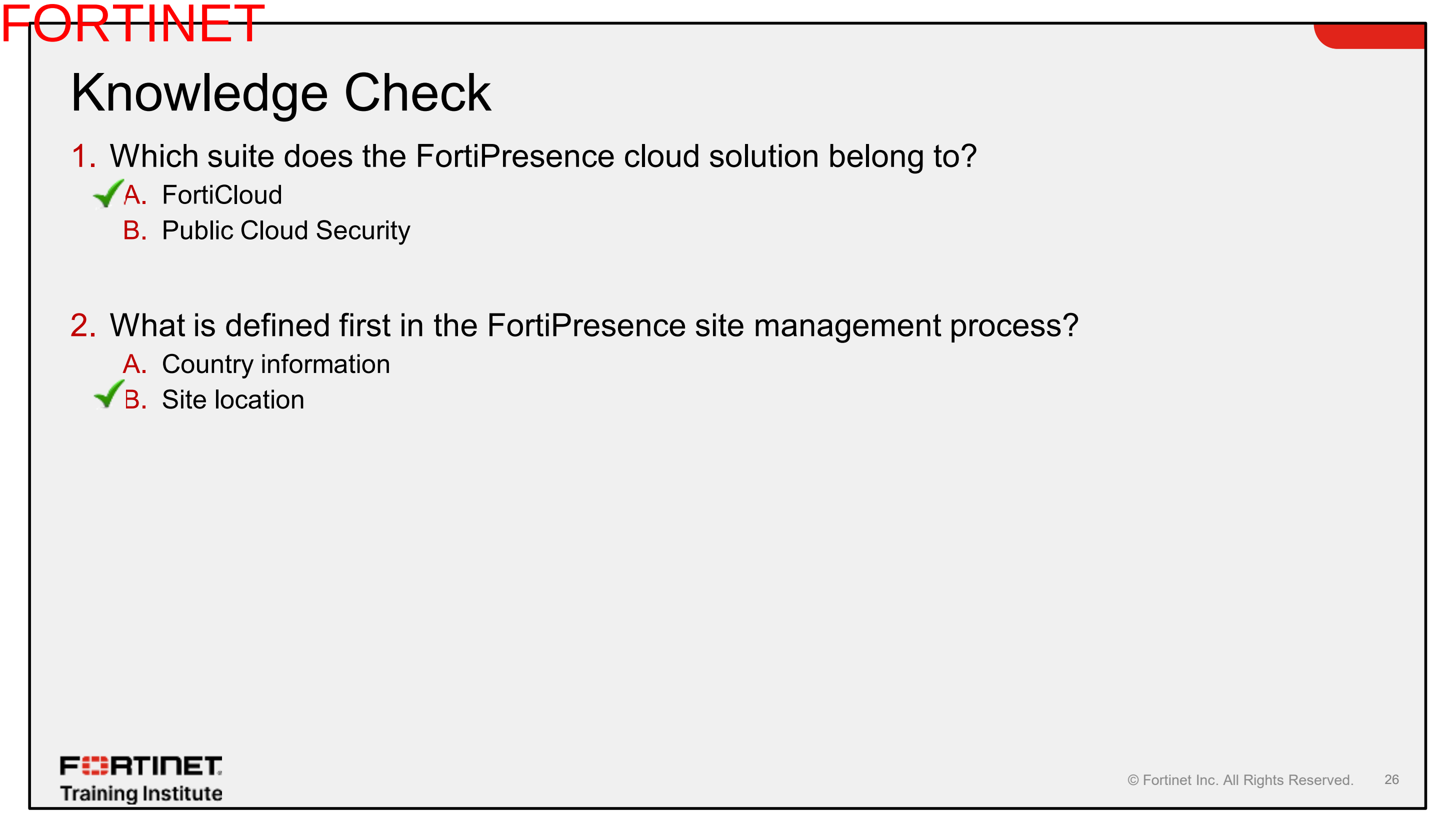
Feature	Unlicensed (Free)	Licensed (Paid)
Number of sites	1	Unlimited
Number of APs	15	Unlimited
Data retention	7 days	1 year
Concurrent captive portal sessions	200	Unlimited
Site reports and user management	N/A	Yes
Social media authentication	Paid per site	Paid per site
Captive portal customization	Paid per site	Paid per site
Theme and images for captive portal	Yes	Yes

FORTINET Training Institute

25

FortiPresence is available in two options: free tier (unlicensed) and paid tier (licensed). Both solutions are hosted on cloud or on-premises. The cloud-based solution comes with no additional onsite hardware to purchase or install, and can be used with any Fortinet wireless management solution.

The table provides a comparison between free tier and paid tier and highlights the features available on each option.



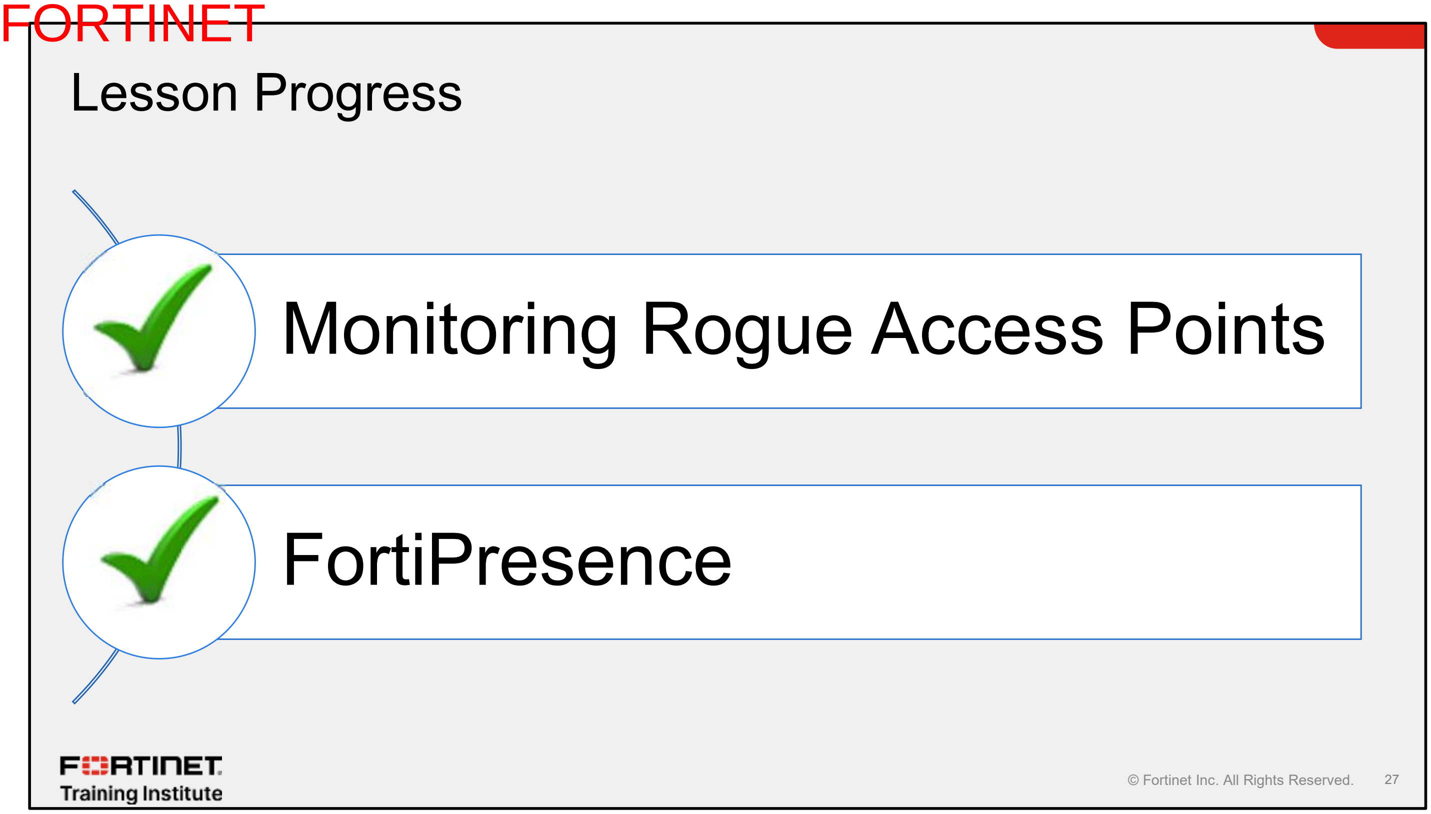
Knowledge Check

1. Which suite does the FortiPresence cloud solution belong to?
   - ✓ A. FortiCloud
   - B. Public Cloud Security

2. What is defined first in the FortiPresence site management process?
   - A. Country information
   - ✓ B. Site location

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26



Lesson Progress

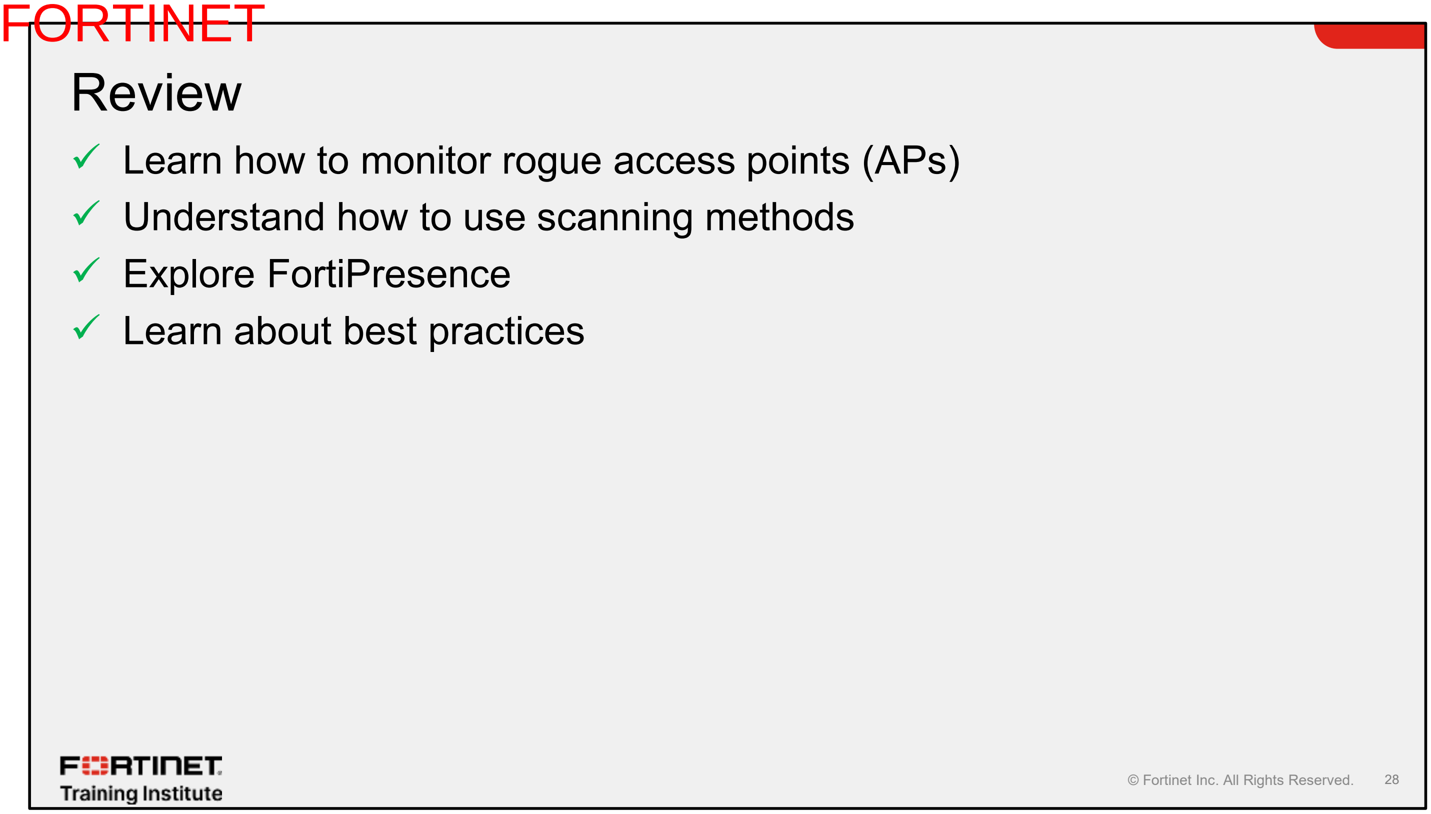
- ✓ Monitoring Rogue Access Points
- ✓ FortiPresence

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



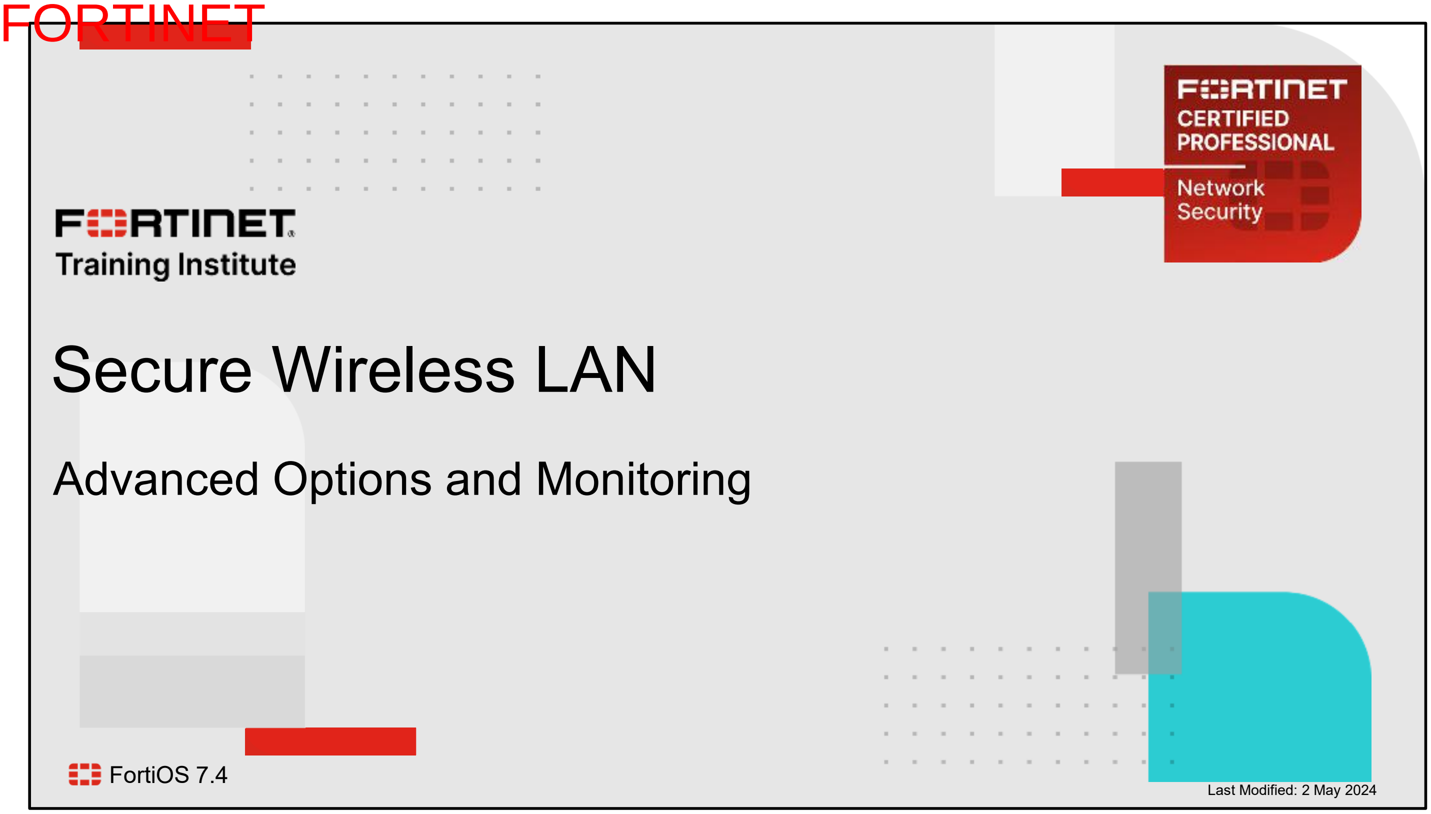
Review

- ✓ Learn how to monitor rogue access points (APs)
- ✓ Understand how to use scanning methods
- ✓ Explore FortiPresence
- ✓ Learn about best practices

28

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the monitoring the wireless network and detect rogue APs and other threats as well as exploring location service on FortiPresence to monitor wireless users in the wireless network.



FORTINET CERTIFIED PROFESSIONAL
Network Security

FORTINET Training Institute

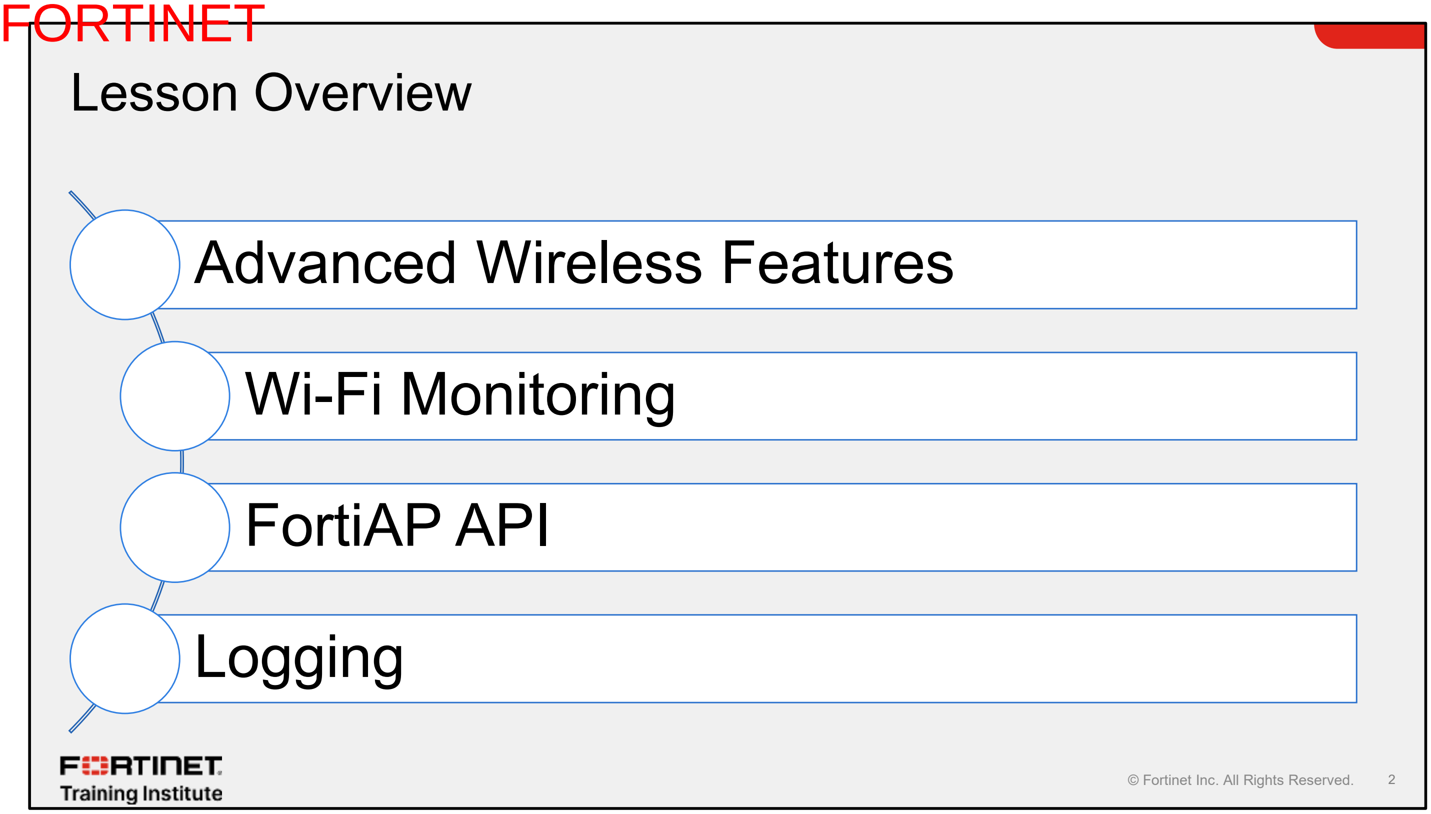
Secure Wireless LAN

Advanced Options and Monitoring

FortiOS 7.4

Last Modified: 2 May 2024

In this lesson, you will learn about the advance wireless features and Wi-Fi monitoring tools.

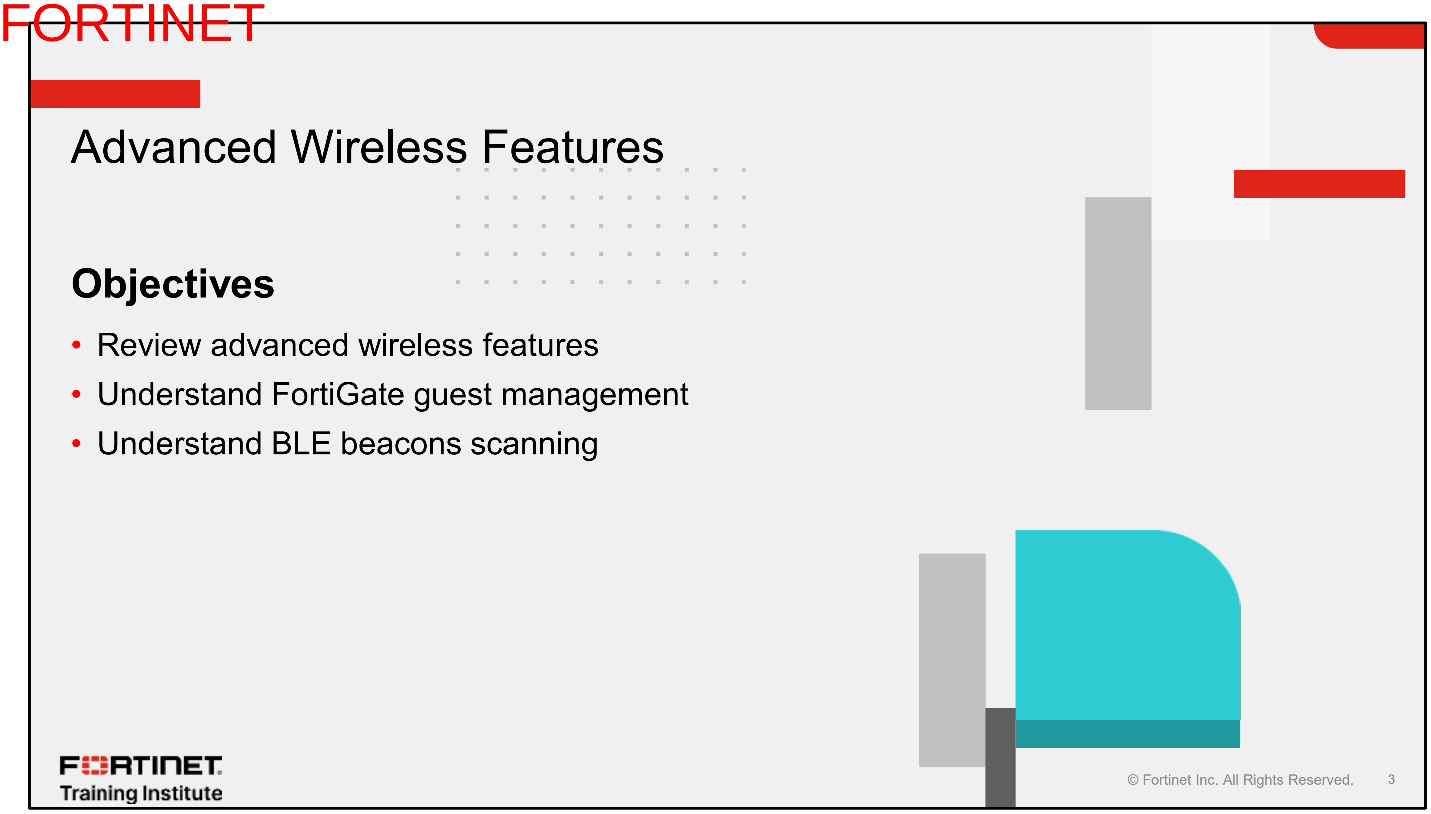


Lesson Overview

- Advanced Wireless Features
- Wi-Fi Monitoring
- FortiAP API
- Logging

2

In this lesson, you will learn about the topics shown on this slide.



Advanced Wireless Features

Objectives

- Review advanced wireless features
- Understand FortiGate guest management
- Understand BLE beacons scanning

FORTINET
Training Institute

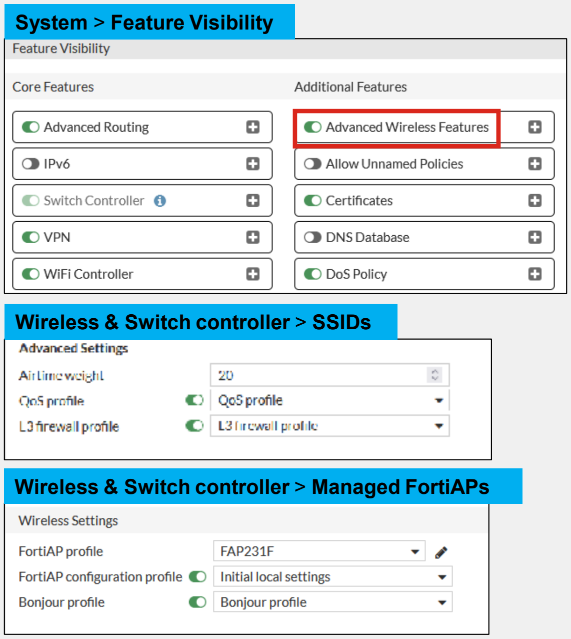
3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in advanced wireless features, you will be able to use the FortiAP advanced settings for better functionality and more effective wireless network monitoring.

Advanced Wireless Features

- Enable advanced features to make them visible on the GUI
- Some core features, such as WIDS, move under different section on GUI
- Some of the advanced features added onto the GUI such as:
  - QoS profiles
  - L3 firewall profiles
  - FortiAP configuration profiles
- Created advanced wireless profiles are then assigned as follows:
  - QoS and L3 firewall profiles in SSID interface settings
  - FortiAP configuration profiles in managed FortiAP settings



System > Feature Visibility

Feature Visibility

Core Features	Additional Features
Advanced Routing	Advanced Wireless Features
IPv6	Allow Unnamed Policies
Switch Controller	Certificates
VPN	DNS Database
WiFi Controller	DoS Policy

Wireless & Switch controller > SSIDs

Advanced Settings

Airtime weight	20
QoS profile	QoS profile
L3 firewall profile	L3 firewall profile

Wireless & Switch controller > Managed FortiAPs

Wireless Settings

FortiAP profile	FAP231F
FortiAP configuration profile	Initial local settings
Bonjour profile	Bonjour profile

FORTINET Training Institute

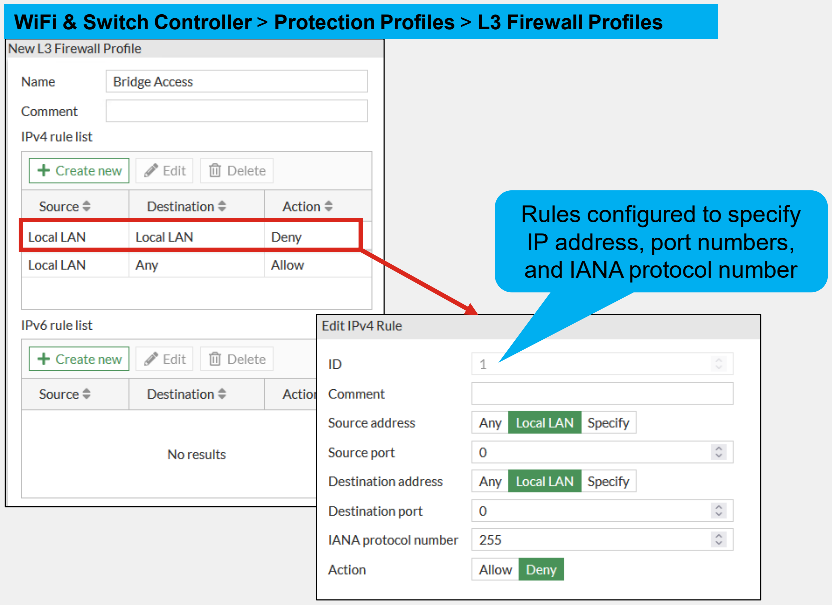
4

To simplify the site layout, advanced wireless features are hidden. You can enable advanced wireless features in the **Feature Visibility** section.

After the advanced wireless profiles are created, you can then assign QoS and L3 firewall profiles in the SSID interface settings. FortiAP configuration profiles are assigned within the managed FortiAP settings.

L3 Firewall Profile

- Configure Wi-Fi bridge access control list
- Available as part of wireless protection profiles
- Available for IPv4 and IPv6
- Assign profile in SSID settings



WiFi & Switch Controller > Protection Profiles > L3 Firewall Profiles

New L3 Firewall Profile

Name: Bridge Access

Comment:

IPv4 rule list

Source	Destination	Action
Local LAN	Local LAN	Deny
Local LAN	Any	Allow

IPv6 rule list

Source	Destination	Action
No results		

Rules configured to specify IP address, port numbers, and IANA protocol number

Edit IPv4 Rule

ID	1
Comment	
Source address	Any [✓ Local LAN] Specify
Source port	0
Destination address	Any [✓ Local LAN] Specify
Destination port	0
IANA protocol number	255
Action	Allow [✓ Deny]

5

You can configure a bridge access control list in the layer 3 firewall profile as part of the advanced wireless features.

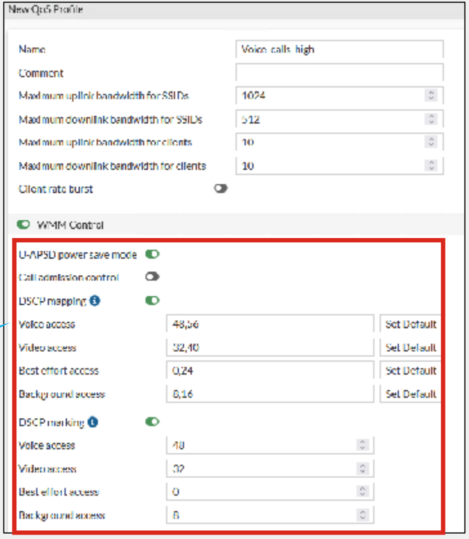
The access lists are rules that allow or deny IPv4 and IPv6 traffic that matches the configured policy. You can specify the IP address, port numbers, and Internet Assigned Numbers Authority (IANA) protocol numbers in the layer 3 firewall rule list.

L3 firewall profiles are assigned in SSID settings as part of the advanced wireless settings.

QoS Profile

- Wireless traffic classification based on parameters such as:
  - Voice
  - Video
  - Data
  - Users
- Set minimum and maximum bandwidth
- Configure WMM markings to DSCP values
- Apply QoS profile in SSID settings

WiFi & Switch Controller > Operation Profiles > QoS Profiles



New QoS Profile

Name	Voice calls high	
Comment		
Maximum uplink bandwidth for SSIDs	1024	
Maximum downlink bandwidth for SSIDs	512	
Maximum uplink bandwidth for clients	10	
Maximum downlink bandwidth for clients	10	
Client rate burst	○	
WMM Control	●	
U-APSD power save mode	●	
Call admission control	○	
DSCP mapping	●	
Voice access	48,56	Set Default
Video access	32,40	Set Default
Best effort access	0,24	Set Default
Background access	8,16	Set Default
DSCP marking	●	
Voice access	48	
Video access	32	
Best effort access	0	
Background access	8	

Translate DSCP values when wireless clients send QoS packets with WMM priority

FORTINET Training Institute

6

Creating a QoS profile helps to set up different QoS parameters for voice, video, data wireless networks, or guest and employee wireless networks.

FortiGate can preserve the Wi-Fi multimedia (WMM) QoS marking of packets by translating them to differentiated services code point (DSCP) values when forwarding upstream.

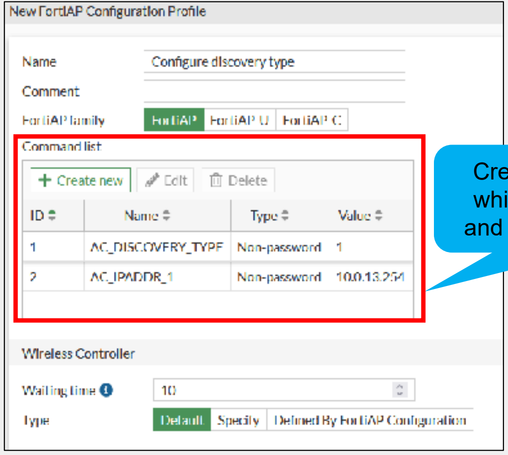
When a wireless client sends QoS packets with WMM priority categories such as `AC_VO`, `AC_VI`, `AC_BE`, and `AC_BK`, FortiAP can forward these packets by translating WMM to DSCP values and transmitting the packets from the Ethernet to their destination.

QoS profiles are assigned in SSID settings as part of the advanced wireless settings.

FortiAP Configuration Profiles

- Define local configuration on a FortiAP family platform using commands
  - FortiAP
  - FortiAP-U
  - FortiAP-C
- Can set these commands to the discovery type on FortiAP
- Create a command list to apply to local FortiAP configuration
  - If password is set on FortiAP, you must define the password
  - Review available commands using CLI command `config wireless-controller apcfg-profile`
- Assign profile in FortiAP managed settings

WiFi & Switch Controller > Operation Profiles > FortiAP Configuration Profiles



New FortiAP Configuration Profile

Name: Configure discovery type

Comment:

FortiAP family: FortiAP | FortiAP U | FortiAP C

Command list

ID	Name	Type	Value
1	AC_DISCOVERY_TYPE	Non-password	1
2	AC_IPADDR_1	Non-password	10.0.13.254

Wireless Controller

Waiting time: 10

Type: Default | Specify | Defined By FortiAP Configuration

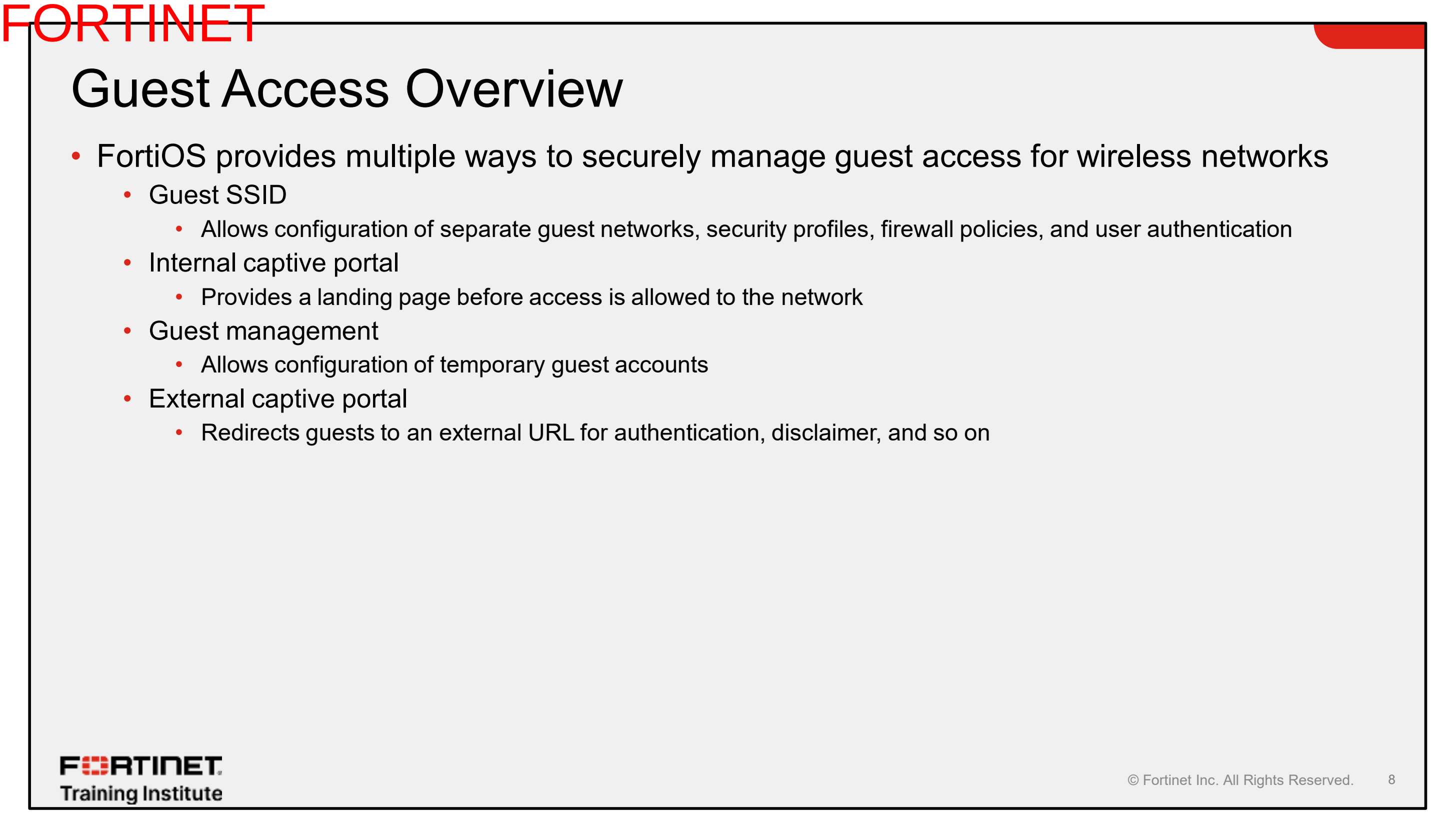
Create a list of commands which define local settings and configuration of FortiAP

Another advanced wireless setting is the FortiAP configuration profile. You can create a profile based on a FortiAP platform and define local settings and configurations using a set of commands.

Each profile is associated with a specific FortiAP family platform. This means you can use a profile for FortiAP 231F and FortiAP 233F since both are on the same FortiAP platform.

To create a command list, you can set the commands available for local configuration using the CLI, such as the command to set `AC_DISCOVERY_TYPE` and `AC_IPADDR_1`. For all available commands, refer to the list of commands available on the CLI.

You can assign a FortiAP profile on the managed FortiAP settings page.

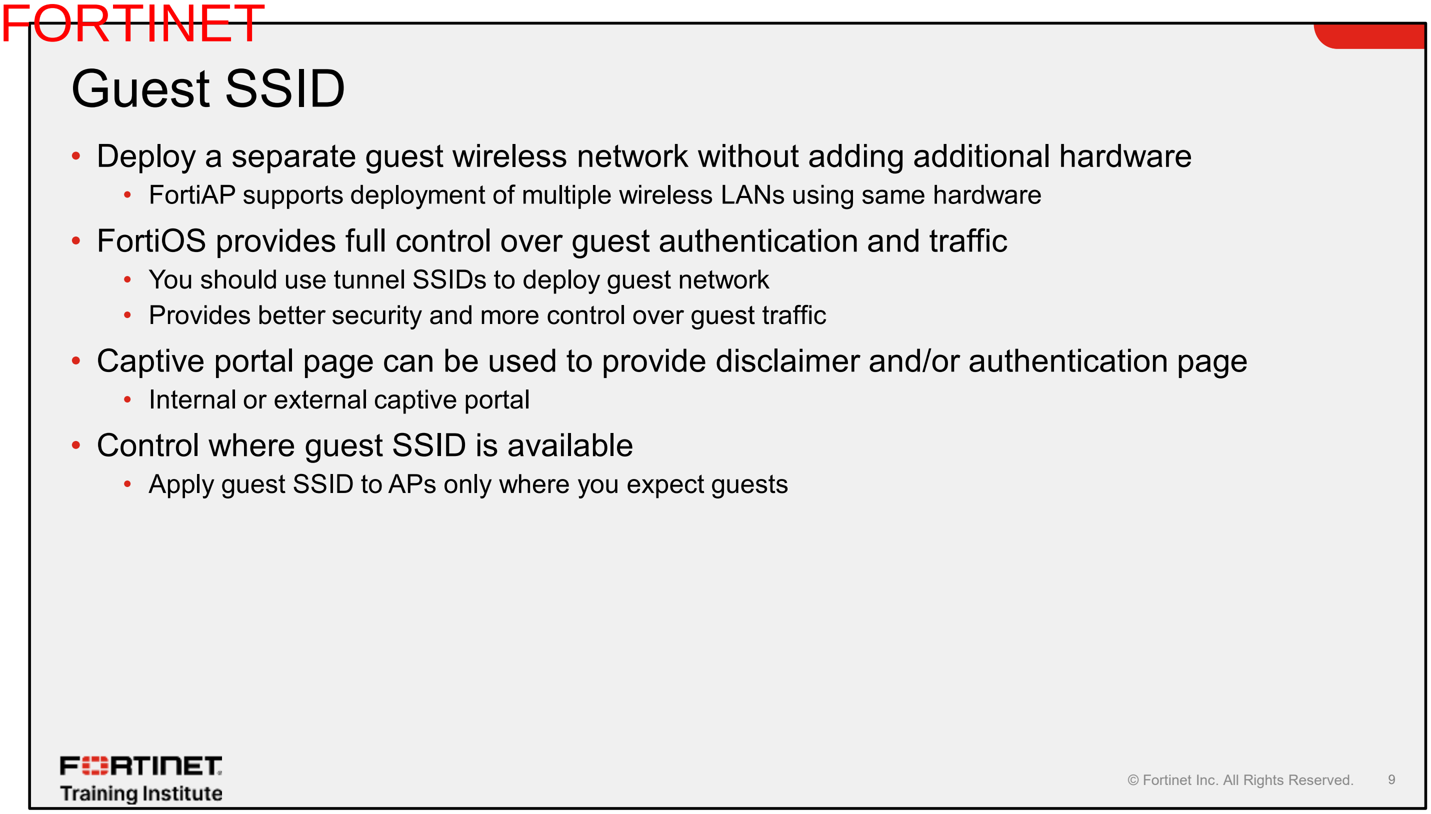


Guest Access Overview

- FortiOS provides multiple ways to securely manage guest access for wireless networks
  - Guest SSID
    - Allows configuration of separate guest networks, security profiles, firewall policies, and user authentication
  - Internal captive portal
    - Provides a landing page before access is allowed to the network
  - Guest management
    - Allows configuration of temporary guest accounts
  - External captive portal
    - Redirects guests to an external URL for authentication, disclaimer, and so on

FortiGate provides multiple ways to securely manage guest access for wireless networks. You can deploy a completely separate wireless network using the existing hardware. FortiGate uses virtual AP (VAP) to deploy multiple SSIDs that are completely isolated from each other. This allows you to have complete control over the traffic, including the ability to assign firewall policies, security profiles, and so on.

FortiGate also has a local captive portal that you can use as a landing page for guests before they are allowed to access the network or local resources. To manage secure guest access, FortiGate offers local guest management tools that you can use to temporarily create and distribute guest accounts. Alternatively, you can redirect guests to an external captive portal server for authentication, disclaimer, and so on. FortiGate will allow access to resources only after it receives a valid response from the external server.



Guest SSID

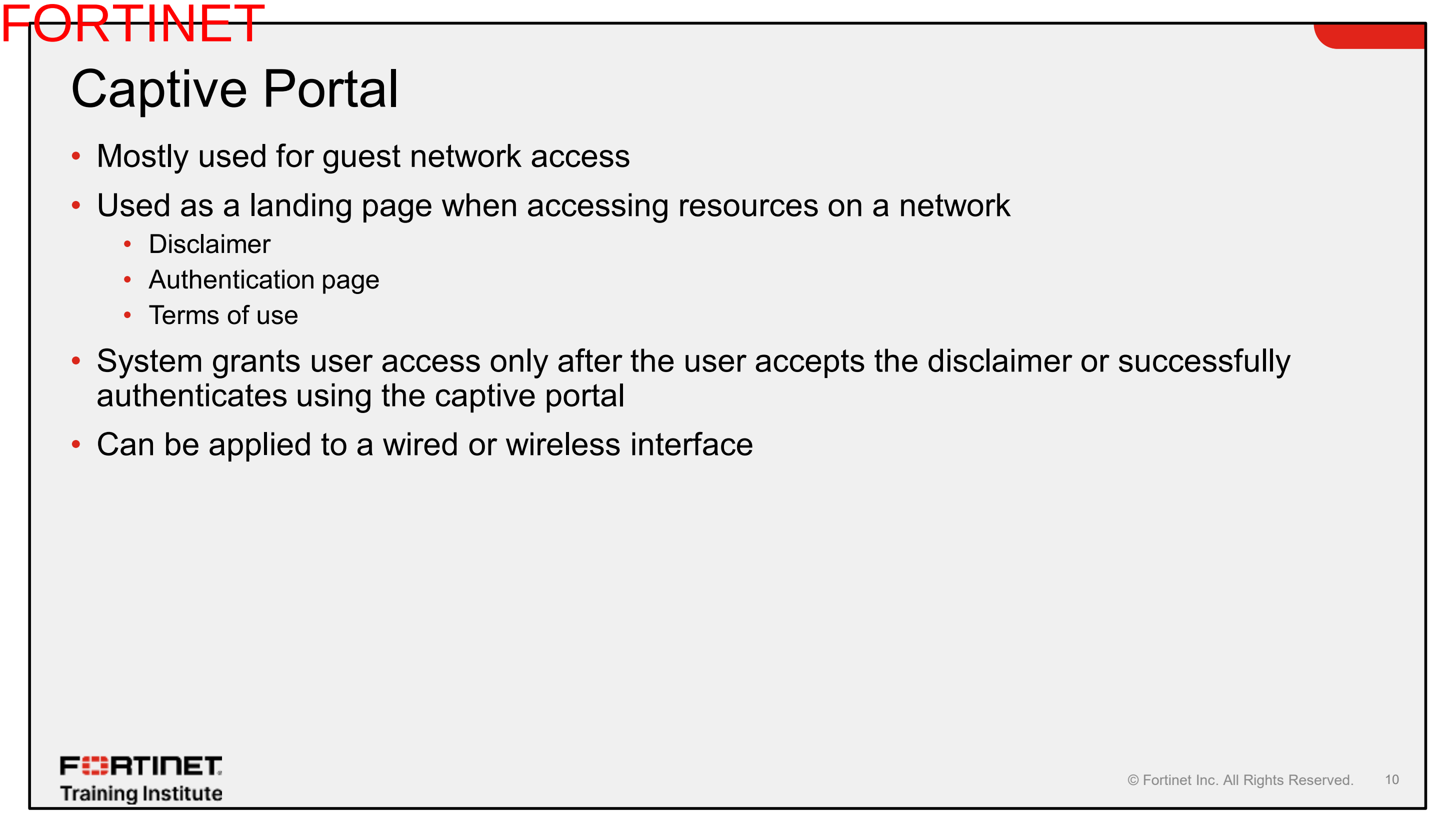
- Deploy a separate guest wireless network without adding additional hardware
  - FortiAP supports deployment of multiple wireless LANs using same hardware
- FortiOS provides full control over guest authentication and traffic
  - You should use tunnel SSIDs to deploy guest network
  - Provides better security and more control over guest traffic
- Captive portal page can be used to provide disclaimer and/or authentication page
  - Internal or external captive portal
- Control where guest SSID is available
  - Apply guest SSID to APs only where you expect guests

© Fortinet Inc. All Rights Reserved. 9

You should deploy a separate service set identifier (SSID) server to guests that do not require access to a corporate or private network. You can deploy multiple SSIDs using the same hardware. Separate SSIDs mean that you will have full control over network traffic flow. You should deploy a guest access SSID in tunnel mode to ensure that all traffic is sent to FortiGate using a Control and Provisioning of Wireless Access Points (CAPWAP) data control channel. This ensures that FortiGate maintains full control over the traffic flow, and can apply security profiles to eliminate security threats before placing traffic on the egress interface.

You can use a local or external captive portal to provide guests with a landing page. You can also use a captive portal to display a disclaimer, or authenticate guest users using guest accounts, or both. Because you will be using a separate wireless network for guest access, you can choose to broadcast the network on access points (APs) that are installed in locations where you expect guest users to be.

Be careful not to transmit too many SSIDs. Excessive numbers of SSIDs can impact wireless performance, and you should carefully plan the number and use of wireless networks. This subject is covered in another lesson.



Captive Portal

- Mostly used for guest network access
- Used as a landing page when accessing resources on a network
  - Disclaimer
  - Authentication page
  - Terms of use
- System grants user access only after the user accepts the disclaimer or successfully authenticates using the captive portal
- Can be applied to a wired or wireless interface

FORTINET Training Institute

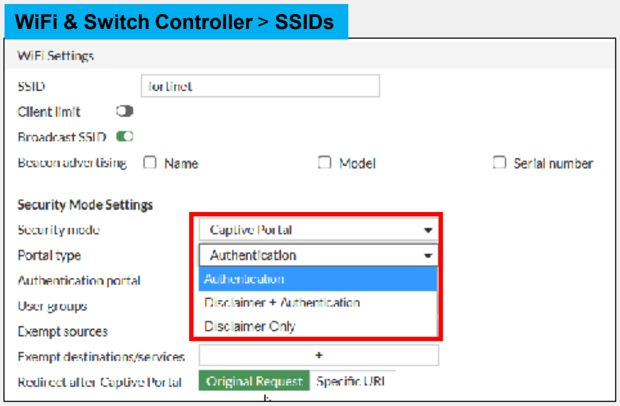
10

The captive portal is used as a landing page after a user connects to a network. This is mostly used for guest access and networks that require a disclaimer. You can also authenticate your users on a captive portal page that requests the user's name and password. Until the user authenticates successfully, the authentication page is returned in response to any HTTP request. After successful authentication, the user can access the requested URL and can access other web resources, as permitted by security policies. Optionally, the captive portal itself can allow web access only to the members of a specified user group.

Captive Portal Types

- Three types of captive portal:
  - **Authentication**: Users are prompted to supply login credentials
  - **Disclaimer + Authentication**: Users must accept a disclaimer and authenticate using valid credentials
  - **Disclaimer Only**: Users need to accept the disclaimer page–local only

WiFi & Switch Controller > SSIDs



WiFi Settings

SSID: fortinet

Client limit

Broadcast SSID

Beacon advertising □ Name □ Model □ Serial number

Security Mode Settings

Security mode: Captive Portal

Portal type: Authentication

Fortinet Training Institute

11

There are four types of captive portals that you can enable on an interface: **Authentication**, **Disclaimer + Authentication**, and **Disclaimer Only**.

Authentication type captive portals request users to authenticate before they are allowed access to the network.

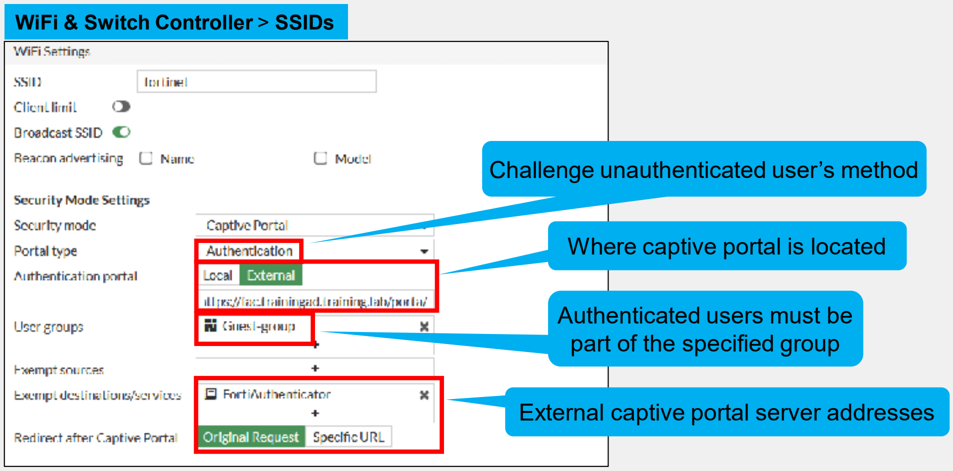
Disclaimer + authentication type captive portals present users with a disclaimer page and an authentication page. The user must accept a disclaimer and authenticate successfully in order to get network access.

Disclaimer only captive portals present users with a disclaimer page. Users do *not* have to authenticate using a username and password; they are allowed to access the network after they accept the disclaimer.

Email collection captive portals present users with a disclaimer page together with a mandatory email request field. Users cannot gain access without entering an email address. The emails are collected and are displayable in **FortiGate Dashboard** > **Users & Devices** > **Collected Email**. You have to enable **Email Collection** in the **Feature Visibility** section.

Captive Portal Authentication Types

- Authentication types:
  - **Local**: FortiGate presents the user with a login page and processes authentication requests
  - **External**: FortiGate redirects users to an external URL where the external captive portal server presents the user with a login page and validates authentication



WiFi & Switch Controller > SSIDs

WiFi Settings

SSID: fortinet
Client limit ○
Broadcast SSID ●
Beacon advertising □ Name □ Model

Security Mode Settings

Security mode: Captive Portal
Portal type: Authentication
Authentication portal: Local [✓ External]
https://fac.trainingad.training.lab/portal/
User groups: Guest-group
Exempt sources
Exempt destinations/services: FortiAuthenticator
Redirect after Captive Portal: [✓ Original Request] Specific URL

Challenge unauthenticated user’s method

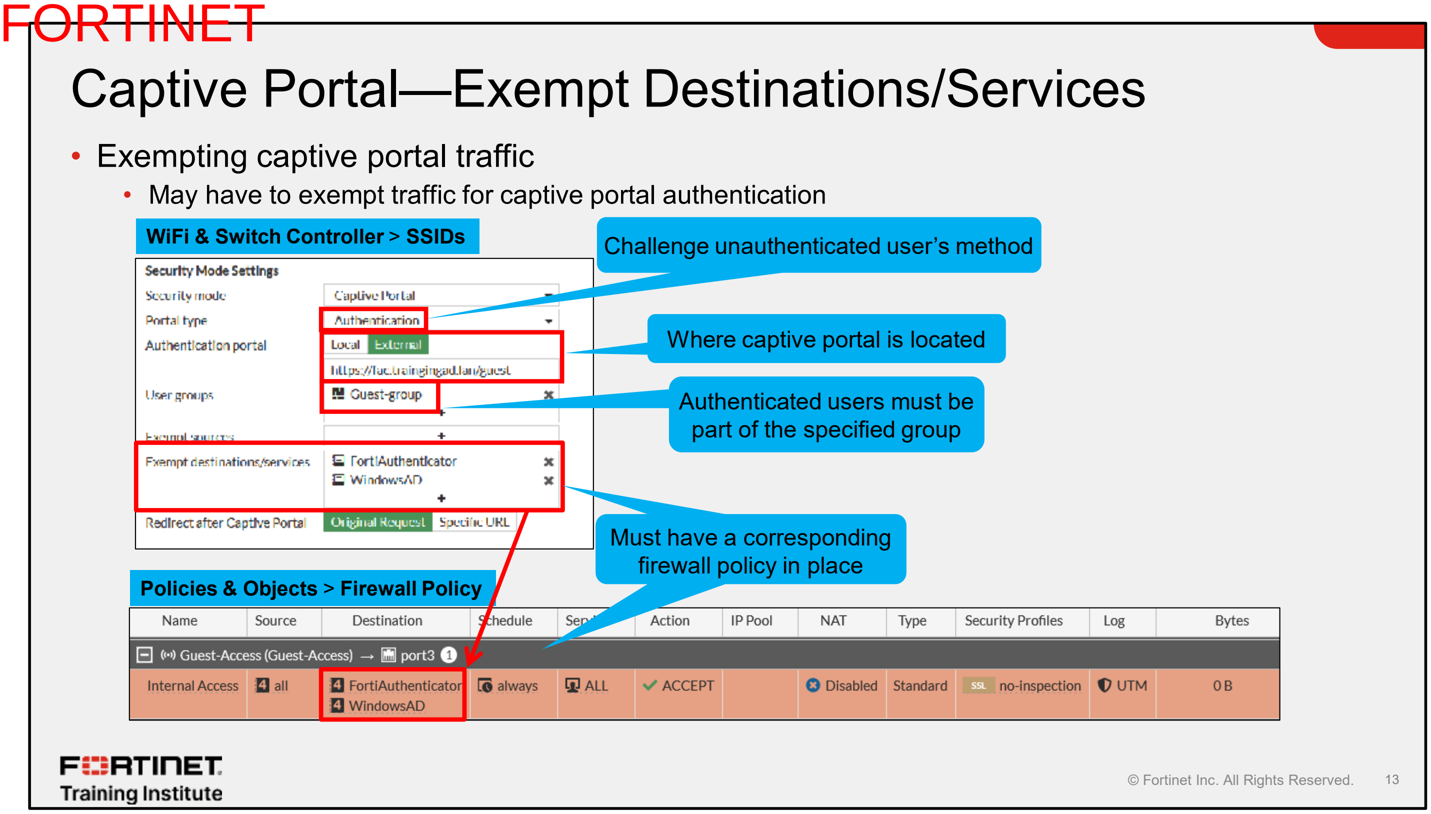
Where captive portal is located

Authenticated users must be part of the specified group

External captive portal server addresses

If you select **Authentication** in the **Portal Type** field, you will have the option of selecting **Local** or **External** in the **Authentication portal** field. If you select **Local** in the **Authentication portal** field FortiGate will use the built-in portal page. All portal configuration options, including the web page that is presented to the users as a landing page, are hosted on FortiGate.

For external captive portals, you can select **External** in the **Authentication portal** field, and type the FQDN or IP address of the external captive portal server. When you do this, FortiGate redirects users to the specified server address. After the user meets the requirements of the external captive portal server, FortiGate allows user access based on the firewall policy configurations.



Captive Portal—Exempt Destinations/Services

- Exempting captive portal traffic
  - May have to exempt traffic for captive portal authentication

WiFi & Switch Controller > SSIDs

Security Mode Settings

Security mode	Captive Portal
Portal type	Authentication
Authentication portal	Local External https://fac.trainingad.lan/guest
User groups	Guest-group
Exempt sources	+
Exempt destinations/services	FortiAuthenticator WindowsAD
Redirect after Captive Portal	Original Request Specific URL

Challenge unauthenticated user's method

Where captive portal is located

Authenticated users must be part of the specified group

Must have a corresponding firewall policy in place

Policies & Objects > Firewall Policy

Name	Source	Destination	Schedule	Ser	Action	IP Pool	NAT	Type	Security Profiles	Log	Bytes
Guest-Access (Guest-Access) → port3 1											
Internal Access	all	FortiAuthenticator WindowsAD	always	ALL	✓ ACCEPT		Disabled	Standard	SSL no-inspection	UTM	0 B

FORTINET Training Institute

13

By default, FortiGate blocks all traffic from users behind an interface that has the security mode set to captive portal. All HTTP traffic is redirected to the captive portal page and other traffic is blocked. However, there is an option to exempt certain traffic to flow through FortiGate without fulfilling captive portal conditions, such as disclaimers and/or authentication.

If you are using an external captive portal server, you must configure a firewall policy and exempt web traffic to the external captive portal IP address. You can exempt destination IP addresses and services on the SSID or interface configuration page. Add the address objects of the destinations that you want to exempt in the **Exempt Destinations/Services** section. Just selecting and applying the address object and selecting the services is not enough to allow the traffic to pass through FortiGate. You must also have a corresponding firewall policy in place to allow the pinhole traffic to pass the through FortiGate.

Therefore, this is a two-step process:

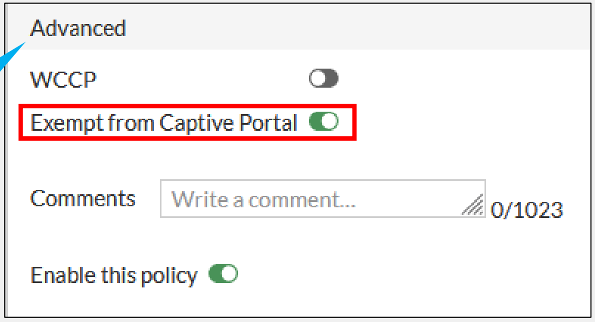
1. Select the destination and services on the SSID or interface configuration page in the **Exempt Destinations/Services** field.
2. Create a firewall policy on the captive portal interface where the external captive portal server is located. You do not have to specify destination objects in the firewall policy.

You can also specify the source IP addresses that you would like to exempt from the captive portal. This can be useful for devices that are unable to accept captive portal conditions using HTTP/HTTPs but require an internet connection. For example, a printer might need to access the internet for firmware upgrades, and so on.

Captive Portal—Firewall Policy Method

- An alternative method to exempt captive portal traffic
- Create a firewall policy
  - Enable the **Exempt from Captive Portal** option

Policy & Objects > **Firewall Policy**



Advanced

WCCP ○

Exempt from Captive Portal ●

Comments: Write a comment... 0/1023

Enable this policy ●

Advanced section visible by enabling policy advanced options in **System** > **Feature Visibility**

Training Institute

14

Alternatively, you can configure a separate firewall policy to allow traffic to reach the external captive portal server without authenticating on the captive portal interface.

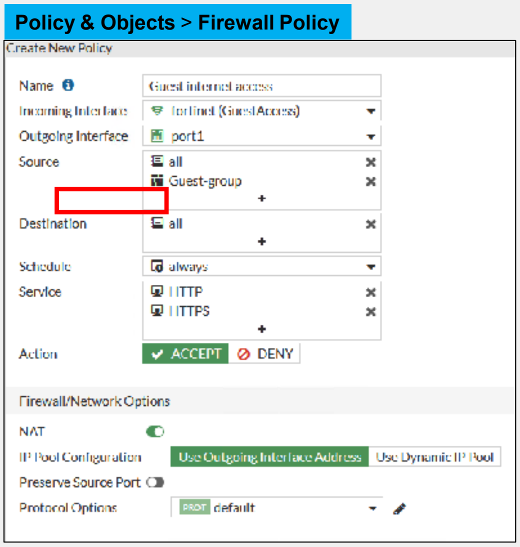
Create a firewall policy and set the destination to your captive portal server, and any other required servers such as DNS or Windows AD. On the CLI, edit the firewall policy rule and enable the exempt from captive portal option on the policy. This option instructs FortiGate to allow traffic to pass through to the specified destinations, without forcing users to authenticate first.

You can use an IP address or an FQDN to point to the captive portal server. If HTTPs is being enforced, the portal address needs to be an FQDN, and match the common name (CN) on the certificate that is being used on FortiGate.

Firewall Policy

- Deploy a firewall policy for authenticated users only
  - Apply the user group that guests will be part of
  - FortiGate authorizes only users who are part of the specified groups to access the internet
  - Do not enable **Exempt from Captive Portal** option for this policy

Policy & Objects > Firewall Policy



Create New Policy

Name	Guest internet access
Incoming Interface	fortinet (GuestAccess)
Outgoing Interface	port1
Source	all Guest-group
Destination	all
Schedule	always
Service	HTTP HTTPS
Action	✓ ACCEPT / DENY

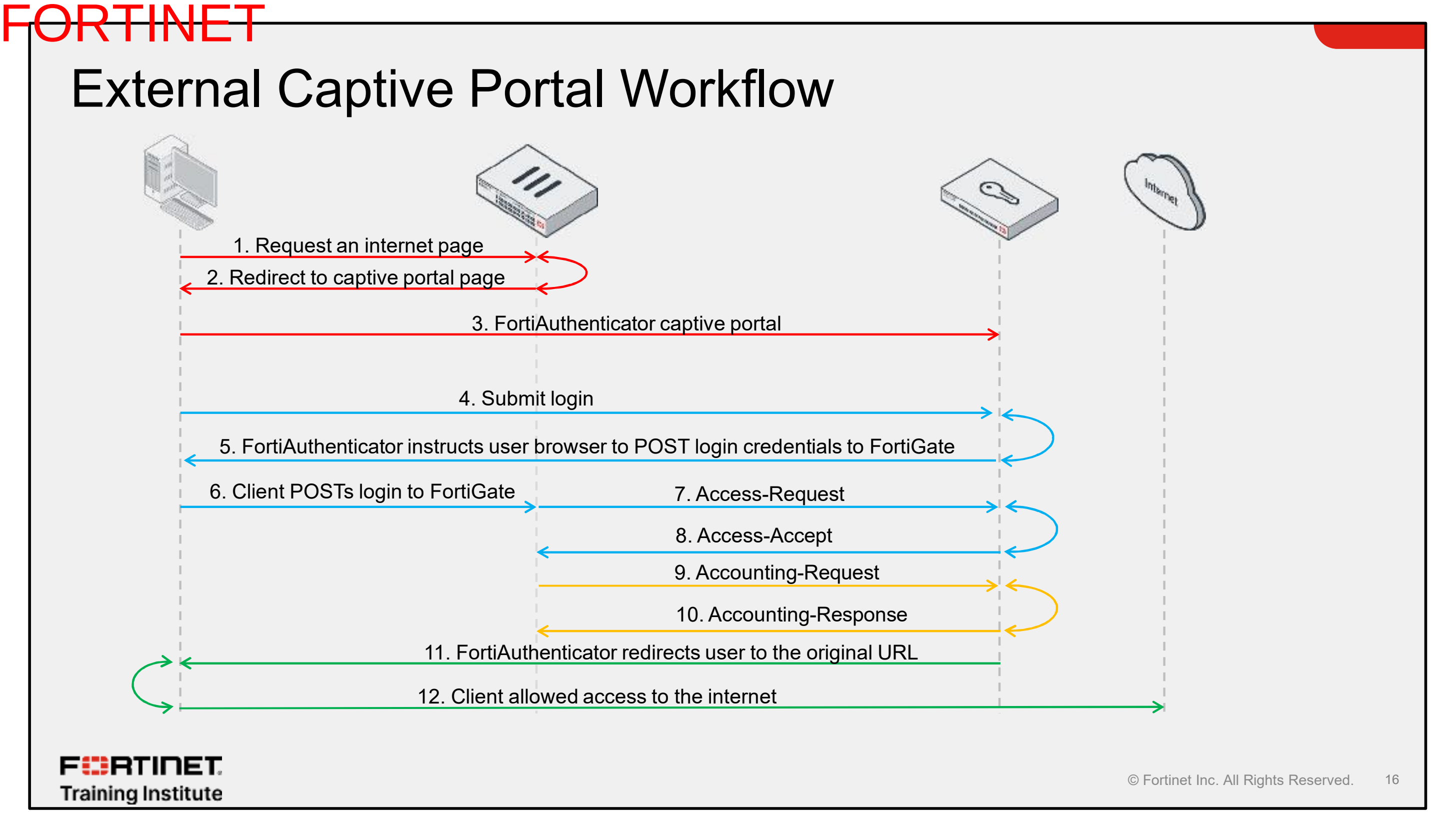
Firewall/Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PROT default

FURTINET
Training Institute

Create a firewall policy from the guest interface to the internet. If you are using a guest user group, make sure you assign it to the firewall policy as the **Source User Group**. When you do this, FortiGate allows access to the internet only for authenticated users who are part of that group.

Do not enable the **Exempt from Captive Portal** option on this firewall policy; otherwise, all the traffic to the internet will be allowed without the users being presented with a captive portal page.



External Captive Portal Workflow

1. Request an internet page
2. Redirect to captive portal page
3. FortiAuthenticator captive portal
4. Submit login
5. FortiAuthenticator instructs user browser to POST login credentials to FortiGate
6. Client POSTs login to FortiGate
7. Access-Request
8. Access-Accept
9. Accounting-Request
10. Accounting-Response
11. FortiAuthenticator redirects user to the original URL
12. Client allowed access to the internet

FORTINET Training Institute

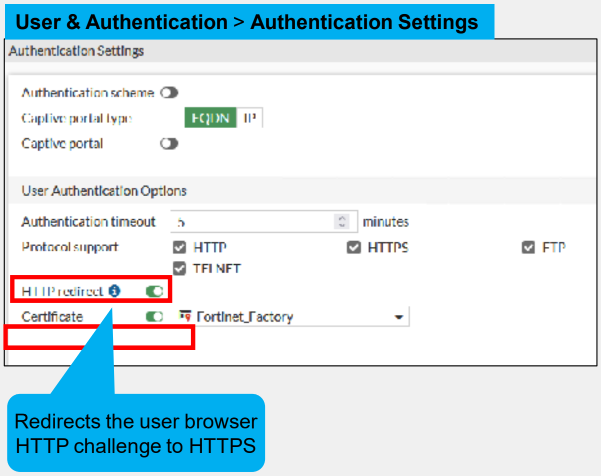
© Fortinet Inc. All Rights Reserved. 16

1. The client tries to access a website.
2. The initial HTTP traffic is intercepted by the FortiGate wireless controller and redirected to the FortiAuthenticator web login page defined in the FortiGate captive portal profile.
3. FortiAuthenticator presents the user with a login page.
4. The client enters their user credentials on the FortiAuthenticator web login page.
5. The login message instructs the guest user's browser to submit the user credentials directly to the FortiGate as an HTTPS POST for authentication processing.
6. When FortiGate receives the client credentials in the HTTPS POST, it sends a RADIUS Access-Request to the FortiAuthenticator RADIUS server to authenticate the user.
7. FortiAuthenticator validates the Access-Request message using its user database, which can be local or remote (LDAP/RADIUS).
8. Based on the results of the authentication and authorization processing, FortiAuthenticator responds with either an Access-Accept or Access-Reject message. If the authentication is successful, the Access-Accept message contains one or more RADIUS attributes to define the context of the client session. These attributes can include, but are not limited to: session duration, bandwidth, and access permissions. When FortiGate receives the Access-Accept message, it changes the role of the client session allowing the device access to the network.
9. A RADIUS accounting request is sent by FortiGate to FortiAuthenticator to verify whether the user has already established a session, or if an existing session in progress.
10. A RADIUS accounting response is sent back after the accounting record is written on FortiAuthenticator after the request has been verified.
11. Following a successful authentication and initiation of the user session, the client is redirected to the originally requested URL, which should now be accessible.
12. The user can access the website and a countdown for the captive portal session timeout begins.

HTTPS POST

- Uses HTTPS instead of HTTP for user authentication
  - Users credentials are protected by an SSL tunnel
- Configurable using the CLI
- The default port used for HTTPS authentication is 1003
  - If required, you can change this port on the CLI:

```
config system settings
    set auth-https-port {integer}
end
```



User & Authentication > Authentication Settings

Authentication Settings

Authentication scheme ○

Captive portal type [✓ FQDN] IP

Captive portal ○

User Authentication Options

Authentication timeout 5 minutes

Protocol support ☑ HTTP ☑ HTTPS ☑ FTP ☑ TELNET

HTTP redirect ●

Certificate ● Fortinet_Factory

Redirects the user browser HTTP challenge to HTTPS

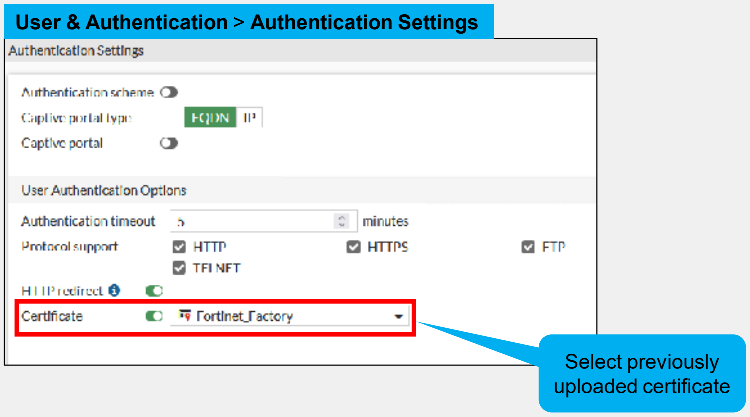
17

During the redirection process, user credentials can be communicated, secured, and encrypted, to the captive portal server. You can configure authentication to use HTTP over SSL.

The default port used for HTTPS authentication is 1003. If you need to change the port, you can use the CLI command **`auth-https-port`** value located in **`config system global`**.

Authentication Certificate

- By default, FortiGate presents users with a factory default certificate on the authentication page
- An alternative certificate can be specified from FortiManager



User & Authentication > Authentication Settings

Authentication Settings

Authentication scheme ○
Captive portal type FQDN IP
Captive portal ○

User Authentication Options

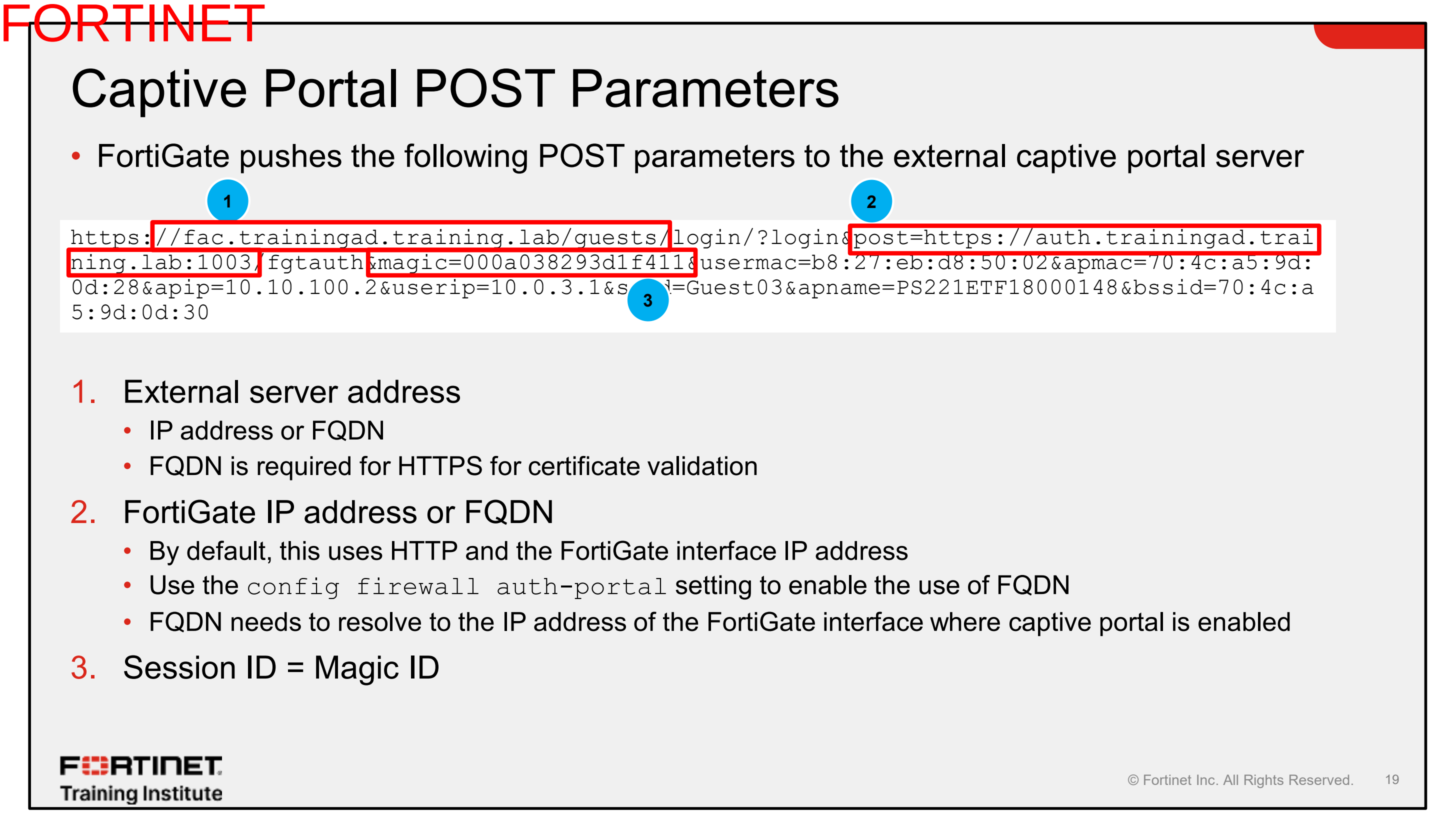
Authentication timeout 5 minutes
Protocol support ☑ HTTP ☑ HTTPS ☑ FTP
☑ TELNET
HTTP redirect ●
Certificate ● Fortinet_Factory

Select previously uploaded certificate

If you redirect the authentication page to an HTTPS page, FortiGate presents the currently configured server certificate.

Note that this certificate is different from the Wi-Fi certificate. This certificate secures the captive portal webpage; the Wi-Fi certificate identifies and authenticates the controller when it is operating as the authentication server.

The FortiGate factory certificate is self signed and will generate a certificate warning in the guest's browser. Most administrators would want to avoid this. In the previous module, you saw how you could install certificates on FortiGate using FortiManager. You can use the same process to install a publicly signed certificate that you can specify here. Assuming the browser trusts this certificate, this will prevent the worrying certificate warnings.



Captive Portal POST Parameters

- FortiGate pushes the following POST parameters to the external captive portal server

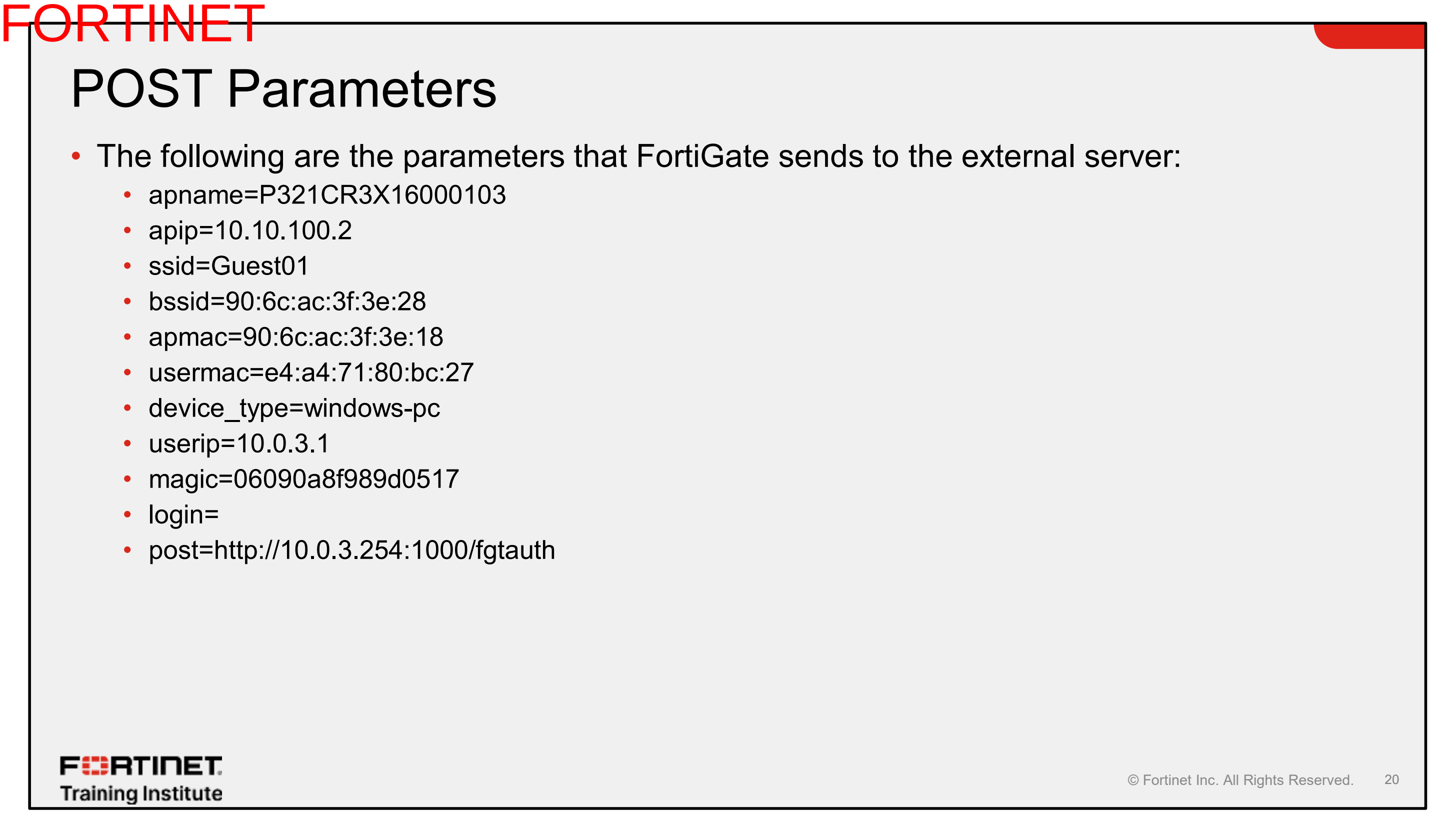
```
https://fac.trainingad.training.lab/guests/login/?login&post=https://auth.trainingad.trai
ning.lab:1003/fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:
0d:28&apip=10.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=PS221ETF18000148&bssid=70:4c:a
5:9d:0d:30
```

1. External server address
   - IP address or FQDN
   - FQDN is required for HTTPS for certificate validation
2. FortiGate IP address or FQDN
   - By default, this uses HTTP and the FortiGate interface IP address
   - Use the `config firewall auth-portal` setting to enable the use of FQDN
   - FQDN needs to resolve to the IP address of the FortiGate interface where captive portal is enabled
3. Session ID = Magic ID

FORTINET Training Institute

19

When FortiGate redirects a user to the external captive server, it adds the parameters shown on this slide to the HTTPS request. You can easily decode the information that FortiGate provides to the external captive portal server. The first part of the redirected URL includes the external server's address, followed by the address of the FortiGate interface address that has the captive portal enabled on it. The magic parameter is the session ID that is used to track the request information.



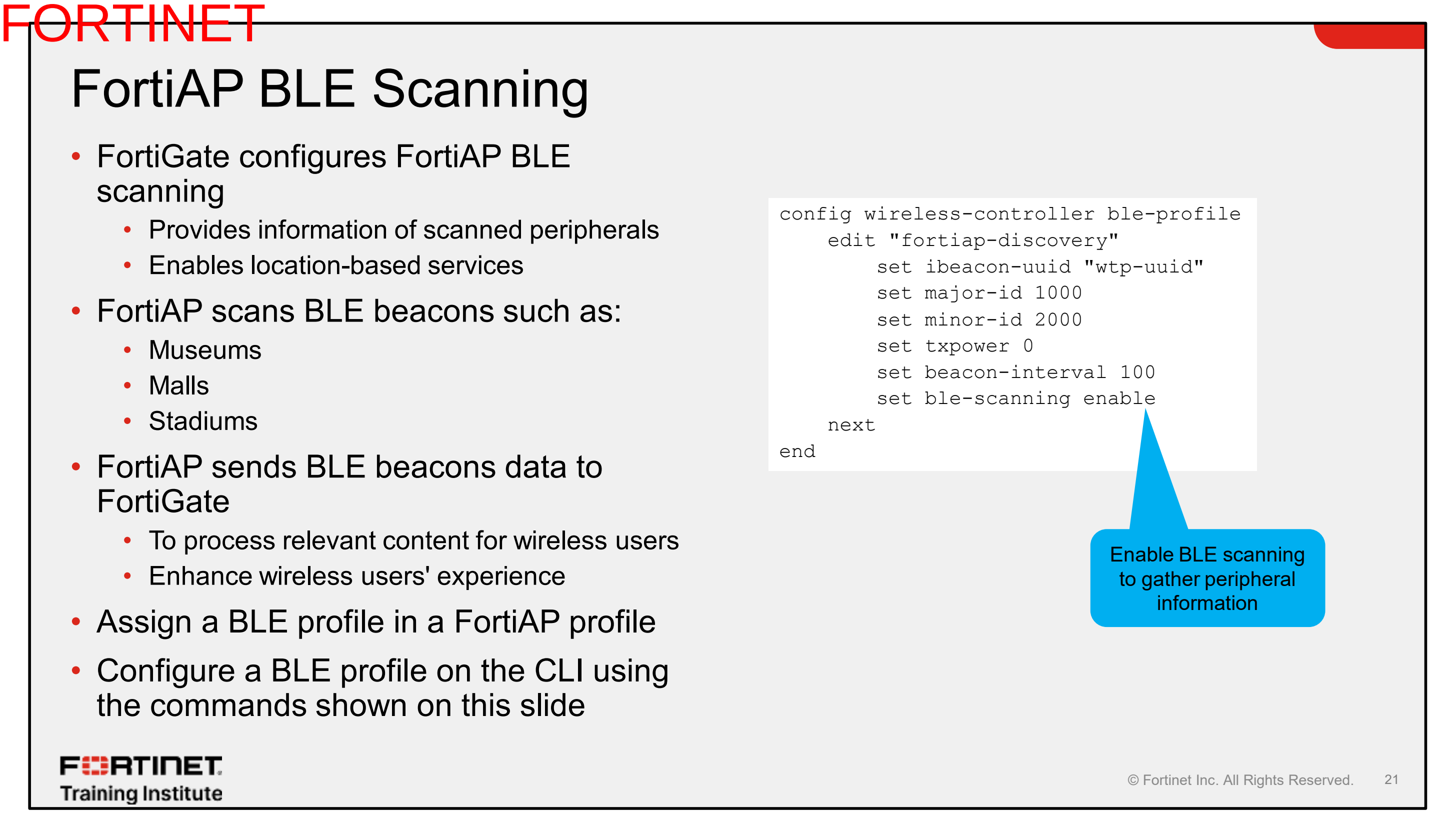
POST Parameters

- The following are the parameters that FortiGate sends to the external server:
  - apname=P321CR3X16000103
  - apip=10.10.100.2
  - ssid=Guest01
  - bssid=90:6c:ac:3f:3e:28
  - apmac=90:6c:ac:3f:3e:18
  - usermac=e4:a4:71:80:bc:27
  - device_type=windows-pc
  - userip=10.0.3.1
  - magic=06090a8f989d0517
  - login=
  - post=http://10.0.3.254:1000/fgtauth

FORTINET
Training Institute

20

This slide contains a list of all the parameters that are sent to the external captive portal from a wireless network on FortiGate.



FortiAP BLE Scanning

- FortiGate configures FortiAP BLE scanning
  - Provides information of scanned peripherals
  - Enables location-based services
- FortiAP scans BLE beacons such as:
  - Museums
  - Malls
  - Stadiums
- FortiAP sends BLE beacons data to FortiGate
  - To process relevant content for wireless users
  - Enhance wireless users' experience
- Assign a BLE profile in a FortiAP profile
- Configure a BLE profile on the CLI using the commands shown on this slide

```
config wireless-controller ble-profile
    edit "fortiap-discovery"
        set ibeacon-uuid "wtp-uuid"
        set major-id 1000
        set minor-id 2000
        set txpower 0
        set beacon-interval 100
        set ble-scanning enable
    next
end
```

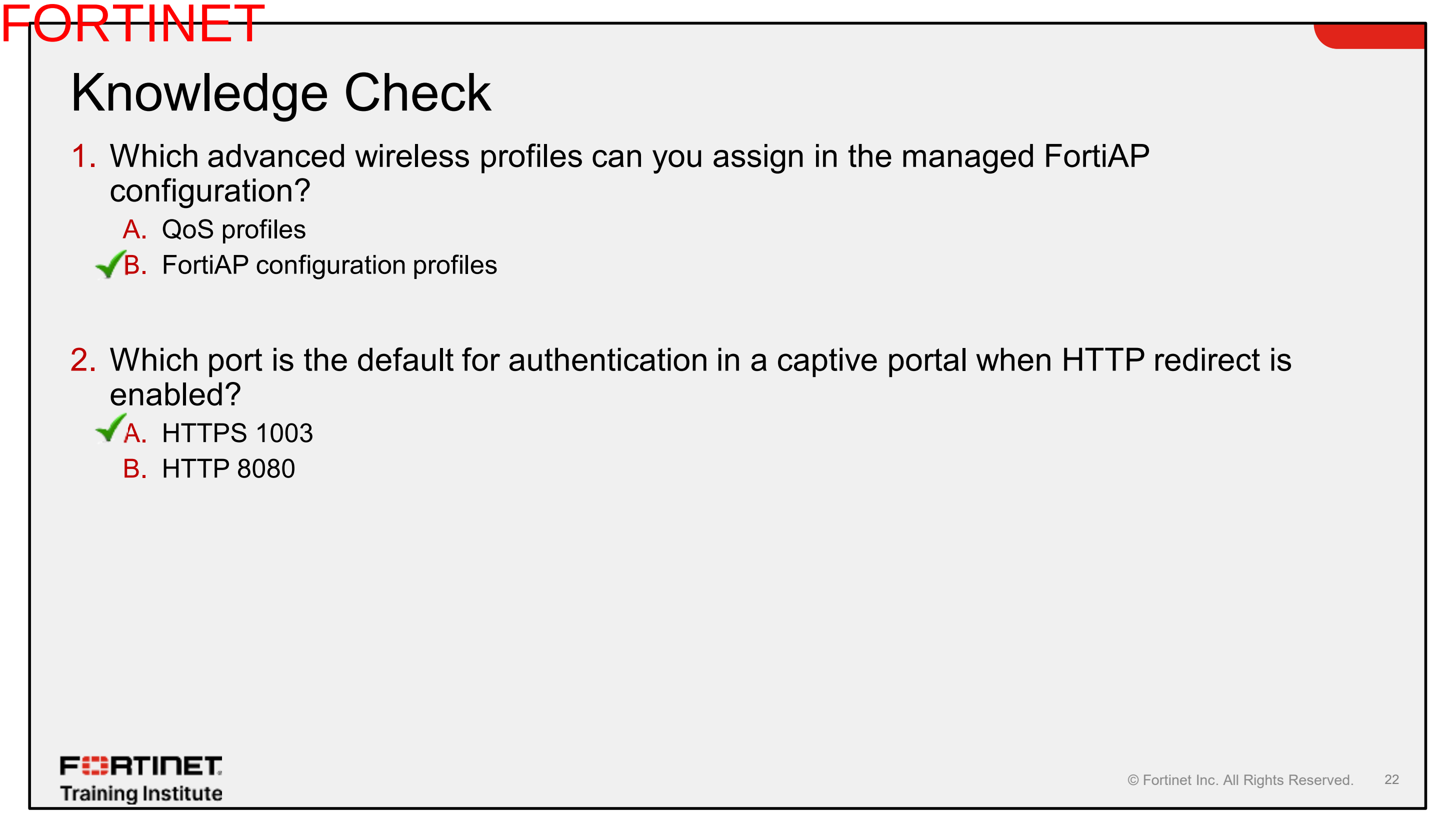
Enable BLE scanning to gather peripheral information

21

Some FortiAP models with built-in Bluetooth radios are configured by the wireless controller to perform BLE scanning and integrate with several BLE beacon profiles.

FortiAP scans wireless beacons that are found in museums, malls, and stadiums while wireless users are visiting these locations. FortiAP collects the BLE beacons data and sends it to FortiGate to process information related to the location service, and uses additional resources such as Pole Star and Eddystone to provide reports about the wireless users’ experience on site.

You can assign a BLE profile to a FortiAP profile or override managed FortiAP settings to specify BLE major and minor parameters, which are used for iBeacon provisioning for real-time location system (RTLS) deployments.



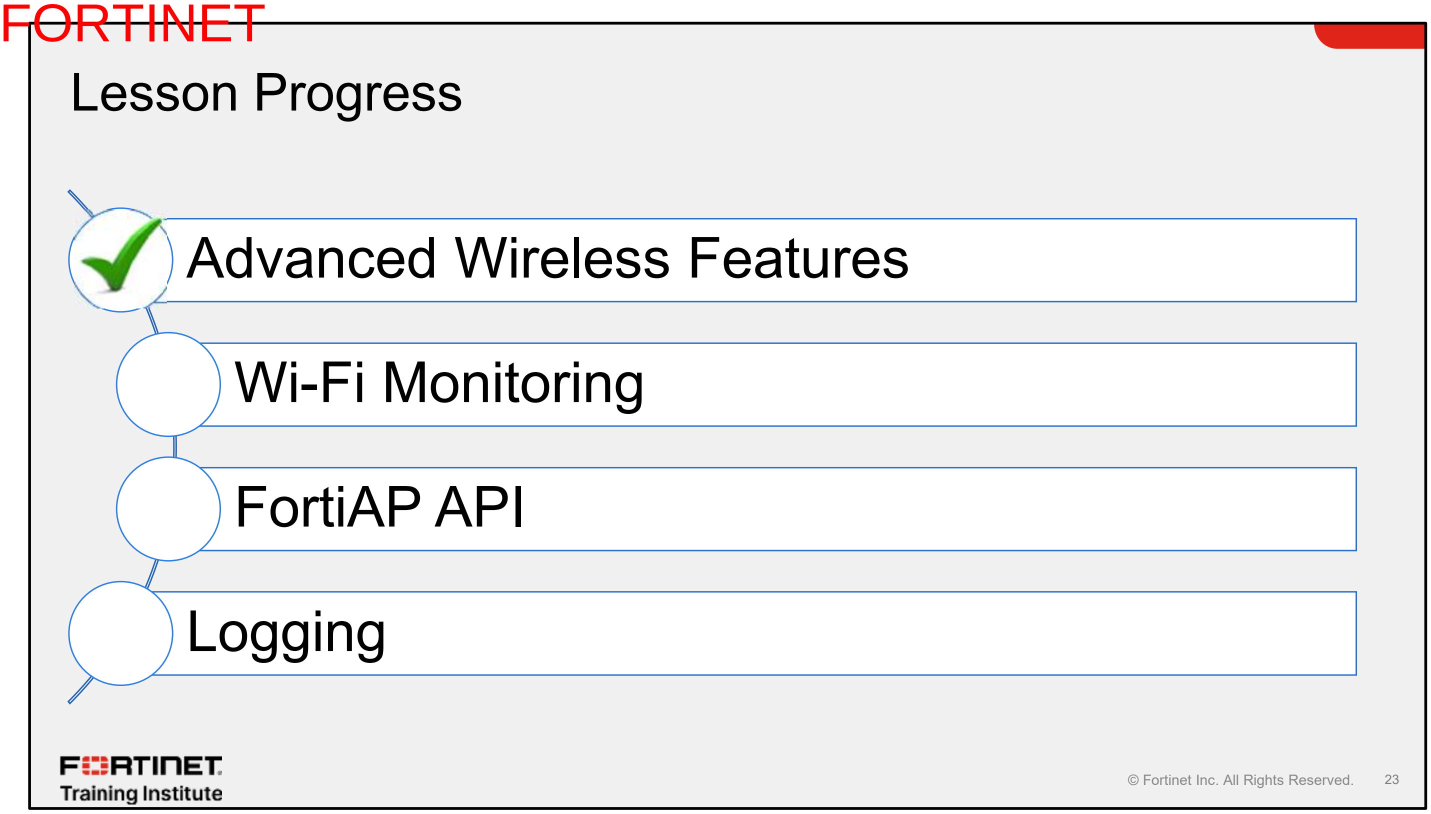
Knowledge Check

1. Which advanced wireless profiles can you assign in the managed FortiAP configuration?
   - A. QoS profiles
   - ✓B. FortiAP configuration profiles

2. Which port is the default for authentication in a captive portal when HTTP redirect is enabled?
   - ✓A. HTTPS 1003
   - B. HTTP 8080

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22



Lesson Progress

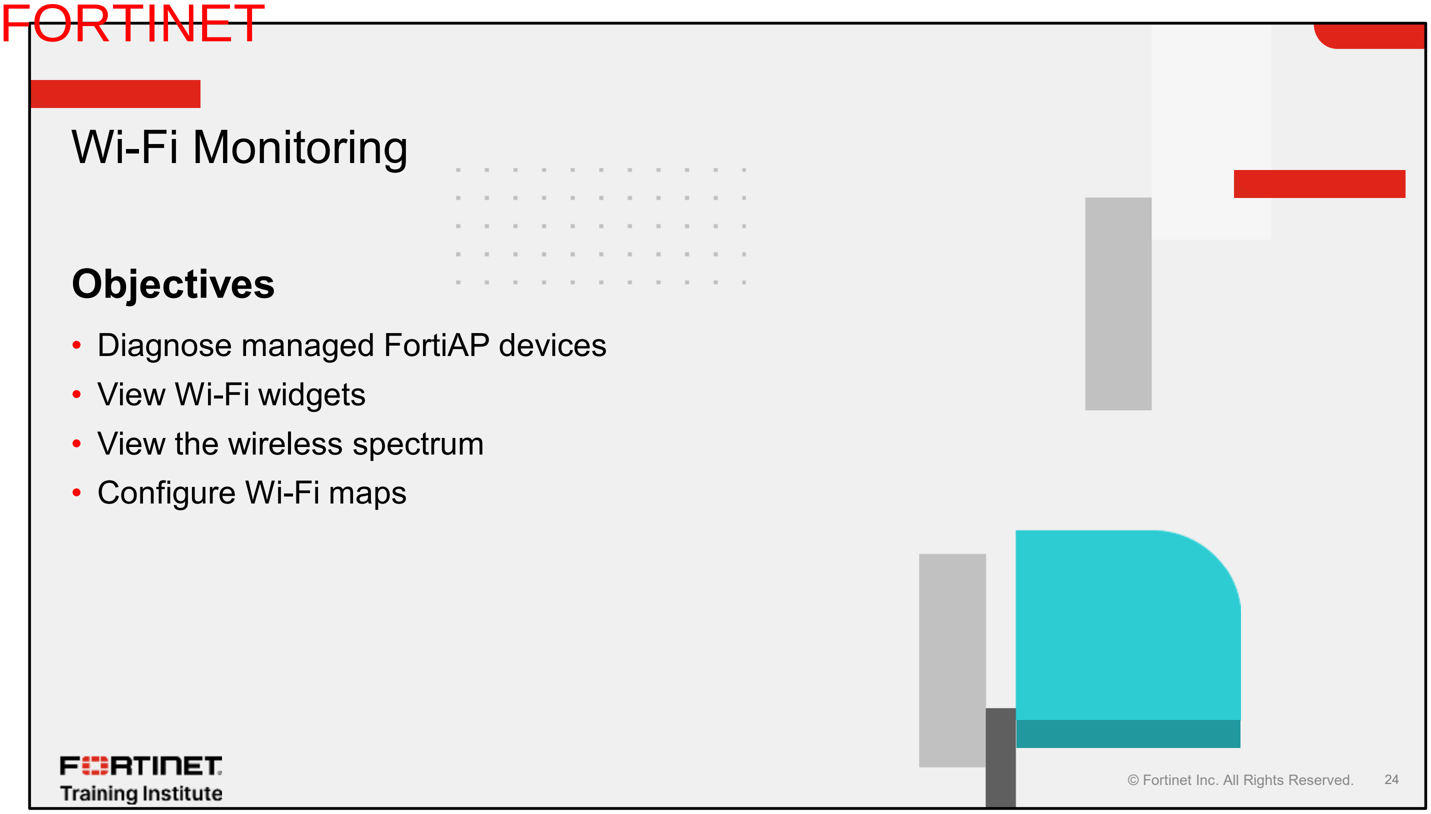
- ✓ Advanced Wireless Features
- ○ Wi-Fi Monitoring
- ○ FortiAP API
- ○ Logging

Training Institute

23

Good job! You now understand some advanced wireless features.

Now, you will learn about Wi-Fi monitoring.



Wi-Fi Monitoring

Objectives

- Diagnose managed FortiAP devices
- View Wi-Fi widgets
- View the wireless spectrum
- Configure Wi-Fi maps

FORTINET
Training Institute

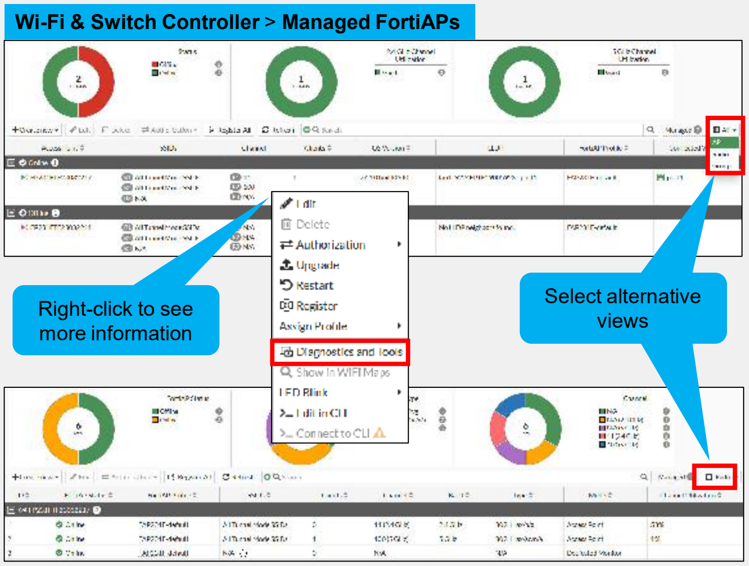
24

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in monitoring Wi-Fi, you will be able to monitor your wireless network and FortiAP device performance.

Managed FortiAPs Table

- Located under **Wi-Fi & Switch Controller**
- Displays detailed information about the installed FortiAPs
- View by **AP**
  - Right-click on column headers and add **Channel Utilization**
- View by **Radio**
  - Sort all radios by utilization and station load
- View by **Group**
  - Place APs in separate groups
- Both **AP** and **Radio** view show:
  - Radio utilization (when column added)
  - Client count



Wi-Fi & Switch Controller > Managed FortiAPs

Right-click to see more information

Select alternative views

FORTINET Training Institute

25

On FortiGate, the **Managed FortiAPs** table contains useful information about the status of connected APs.

Found under **Wi-Fi & Switch Controller** > **Managed FortiAPs**, the table provides three different views.

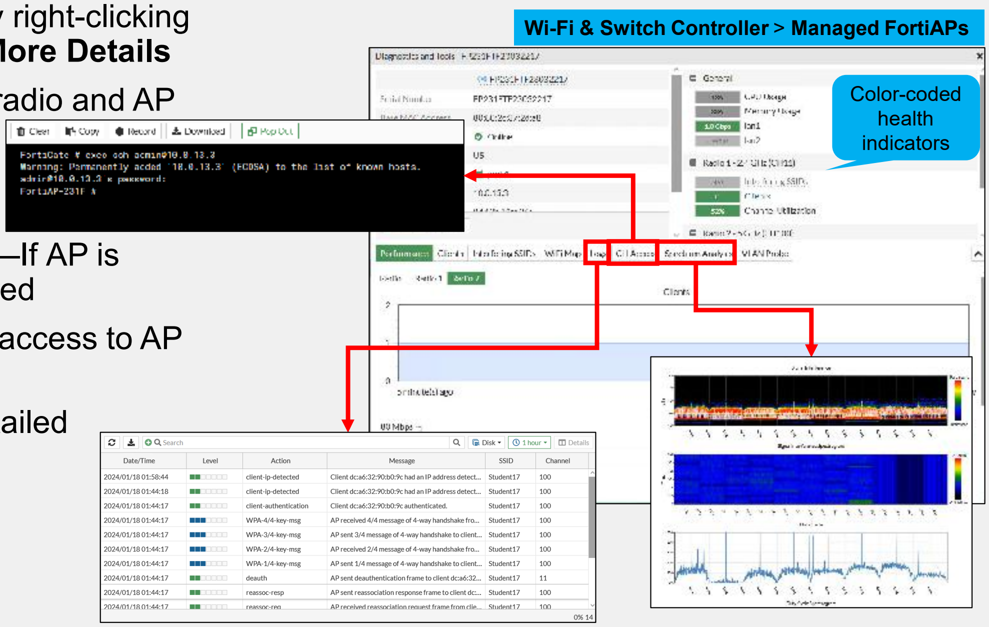
The **AP** view is the default view and groups radio interfaces together under an AP.

The **Radio** view is more useful for assessing load because it allows you to sort the radios to highlight interfaces that are in trouble. Note that you can add useful columns, such as **Channel Utilization**, to a view.

Managed FortiAP table (Contd)

- Focus in on an AP by right-clicking and selecting **View More Details**
- Access to important radio and AP metrics
  - Wireless health
  - Wireless capacity
- **Spectrum Analysis**—If AP is capable and configured
- **CLI Access**—Direct access to AP CLI
- **Wireless Logs**—Detailed operation log

Wi-Fi & Switch Controller > Managed FortiAPs



```
FortiGate # exec ssh admin@10.0.13.3
Warning: Permanently added '10.0.13.3' (ECDSA) to the list of known hosts.
admin@10.0.13.3's password:
FortiAP-231F #
```

Date/Time	Level	Action	Message	SSID	Channel
2024/01/18 01:58:44	🟩🟩□□□□□	client-ip-detected	Client dc:a6:32:90:b0:9c had an IP address detect...	Student17	100
2024/01/18 01:44:18	🟩🟩□□□□□	client-ip-detected	Client dc:a6:32:90:b0:9c had an IP address detect...	Student17	100
2024/01/18 01:44:17	🟩🟩□□□□□	client-authentication	Client dc:a6:32:90:b0:9c authenticated.	Student17	100
2024/01/18 01:44:17	🟦🟦🟦□□□□	WPA-4/4-key-msg	AP received 4/4 message of 4-way handshake fro...	Student17	100
2024/01/18 01:44:17	🟦🟦🟦□□□□	WPA-3/4-key-msg	AP sent 3/4 message of 4-way handshake to client...	Student17	100
2024/01/18 01:44:17	🟦🟦🟦□□□□	WPA-2/4-key-msg	AP received 2/4 message of 4-way handshake fro...	Student17	100
2024/01/18 01:44:17	🟦🟦🟦□□□□	WPA-1/4-key-msg	AP sent 1/4 message of 4-way handshake to client...	Student17	100
2024/01/18 01:44:17	🟩🟩□□□□□	deauth	AP sent deauthentication frame to client dc:a6:32...	Student17	11
2024/01/18 01:44:17	🟩🟩□□□□□	reassoc-resp	AP sent reassociation response frame to client dc:...	Student17	100
2024/01/18 01:44:17	🟩🟩□□□□□	reassoc-req	AP received reassociation request frame from clie...	Student17	100

0% 14

FERTINET Training Institute

When you right-click an AP, you get the option to select **View More Details**. You can see a more detailed summary of the individual AP details and can perform basic actions on the AP, such as upgrade, restart, or deauthorize. It is also possible to edit the configuration directly, which will override the profile settings.

You will see color-coded health indicators in the upper-right corner, which will give you an immediate indication as to the status of the AP and its radios. The colors indicate the severity of the issue, using the colors red, green, and yellow to indicate the severity.

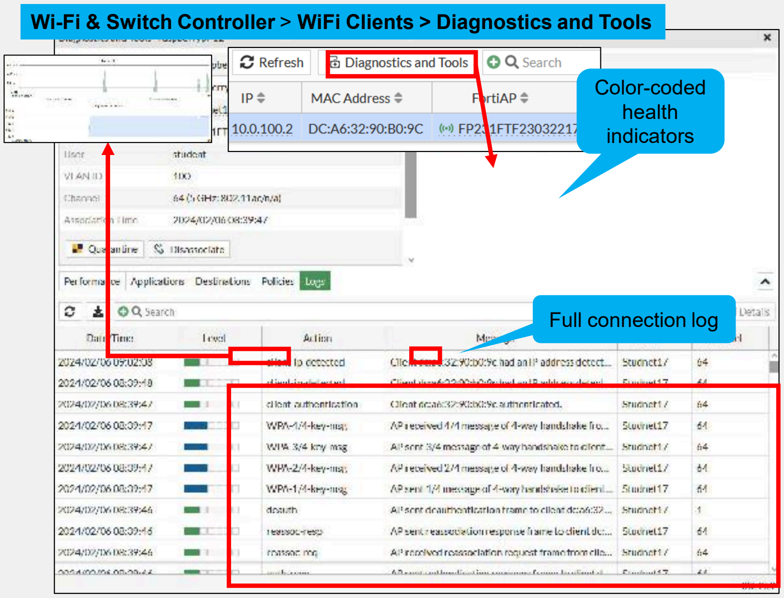
The table shows the configuration and the status of the radios by default. The **Clients** tab shows all the clients that are associated with the AP. You can also drill down into the individual clients, if required. The logs view filters the wireless events just for this AP. Double-click on an event to view the event details.

The **CLI Access** option gives you direct access to the AP CLI. If the AP is capable of and configured for dedicated operation, then you will be able to enable spectrum analysis. Not all APs are capable of spectrum analysis—refer to the release notes for more information. The **Spectrum Analysis** view shows the real-time view of the wireless spectrum, together with any detected interferers.

Wi-Fi Clients

- Detailed client information for all clients currently connected
- Use to assess the client health from the AP point of view
- Provides a small amount of historical information for:
  - Bandwidth
  - Signal-to-noise ratio (SNR)
- Detailed connection log
  - Station connection errors
  - Wireless connection events
  - DHCP events
  - Filterable
  - Exportable

Wi-Fi & Switch Controller > WiFi Clients > Diagnostics and Tools



IP	MAC Address	FortiAP
10.0.100.2	DC:A6:32:90:B0:9C	FP231FTF23032217

User	student
VLAN ID	100
Channel	64 (5 GHz: 802.11ac/n/a)
Association Time	2024/02/06 08:39:47

Date/Time	Level	Action	Message		
2024/02/06 09:02:08		client-ip-detected	Client dc:a6:32:90:b0:9c had an IP address detect...	Student17	64
2024/02/06 08:39:48		client-ip-detected	Client dc:a6:32:90:b0:9c had an IP address detect...	Student17	64
2024/02/06 08:39:47		client authentication	Client dc:a6:32:90:b0:9c authenticated.	Student17	64
2024/02/06 08:39:47		WPA-4/4-key-msg	AP received 4/4 message of 4-way handshake fro...	Student17	64
2024/02/06 08:39:47		WPA-3/4-key-msg	AP sent 3/4 message of 4-way handshake to client...	Student17	64
2024/02/06 08:39:47		WPA-2/4-key-msg	AP received 2/4 message of 4-way handshake fro...	Student17	64
2024/02/06 08:39:47		WPA-1/4-key-msg	AP sent 1/4 message of 4-way handshake to client...	Student17	64
2024/02/06 08:39:46		deauth	AP sent deauthentication frame to client dc:a6:32...	Student17	1
2024/02/06 08:39:46		reassoc-resp	AP sent reassociation response frame to client dc:...	Student17	64
2024/02/06 08:39:46		reassoc-req	AP received reassociation request frame from clie...	Student17	64
2024/02/06 08:39:46		auth-resp	AP sent authentication response frame to client d...	Student17	64

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

Select a station in the client list. Then, right-click and select **Diagnostics and Tools** to open diagnostics about a station.

From here, you can perform basic actions, such as quarantining or disassociating a workstation. The health icons are color-coded and will give an immediate indication of any issues, such as poor signal strength or SnR.

There is an option to display a graph which, by default, will show bandwidth but can also show SnR. The graphing is limited to approximately 10 minutes of data.

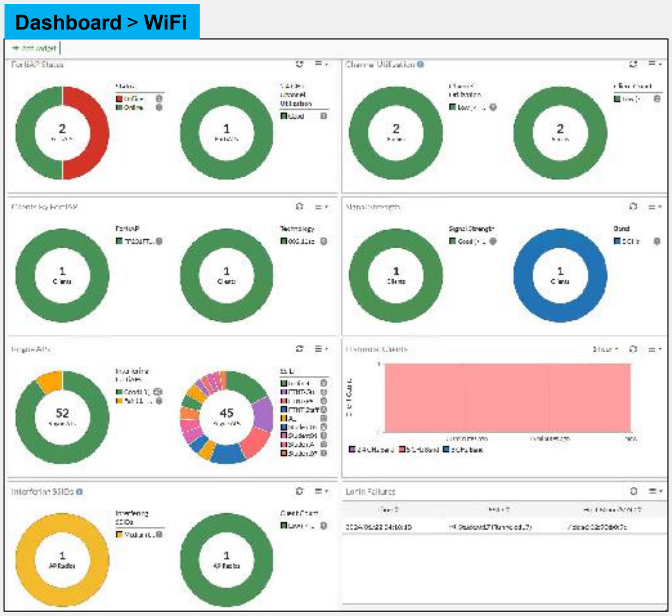
If you select the **Logs** tab is possible to see a logical log of a station connection events. This log is useful for quickly diagnosing common connectivity issues, such as incorrect passwords or pre-shared keys, because the association and authentication steps the wireless client performs are listed in the log. You can see details of each log event by clicking **Details** to see more information about any failures.

Filter the log and export its contents into a text file for a more detailed analysis.

Wi-Fi Dashboard

- Display widgets to monitor wireless connections
- See an overview of FortiAPs, SSIDs, and clients
- See the bands, radios, and Wi-Fi standards used
- Widgets available:
  - **FortiAP Status**
  - **Channel Utilization**
  - **Clients By FortiAP**
  - **Signal Strength**
  - **Rogue APs**
  - **Historical Clients**
  - **Interfering SSIDs**
  - **Login Failures**

Dashboard > WiFi



Training Institute

28

You can see an overview of the wireless devices on the Wi-Fi dashboard. The Wi-Fi dashboard uses widgets to provide a comprehensive view of the health of your network's wireless infrastructure.

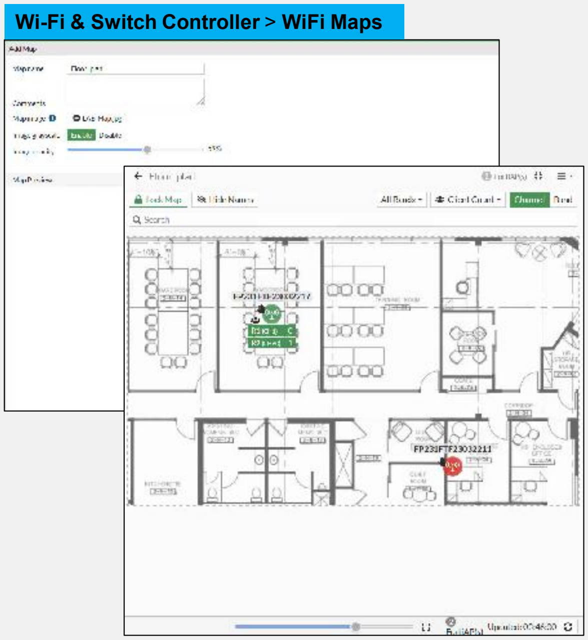
The following widgets are available on the dashboard:

- **FortiAP Status**: Monitor the status of FortiAP devices, both online and offline, and channel utilization.
- **Channel Utilization**: Monitor the radio channel utilization for each FortiAP, and display the number of clients on each channel.
- **Clients By FortiAP**: Monitor the number of clients per FortiAP, and display the Wi-Fi standard used to connect with clients.
- **Signal Strength**: Monitor the signal strength of Wi-Fi clients and of each band broadcasted.
- **Rogue APs**: Monitor rogue APs and interfering SSIDs.
- **Historical Clients**: Monitor the number of Wi-Fi clients in real time over the selected time frame.
- **Interfering SSIDs**: Monitor FortiAPs that are reporting interfering APs and SSIDs.
- **Login Failures**: Monitor failed Wi-Fi login attempts on all SSIDs.

Wi-Fi Map

- Create multiple Wi-Fi maps
- Upload a map image using common image file types
- Place FortiAP devices on a map
- Access FortiAP diagnostics and tools

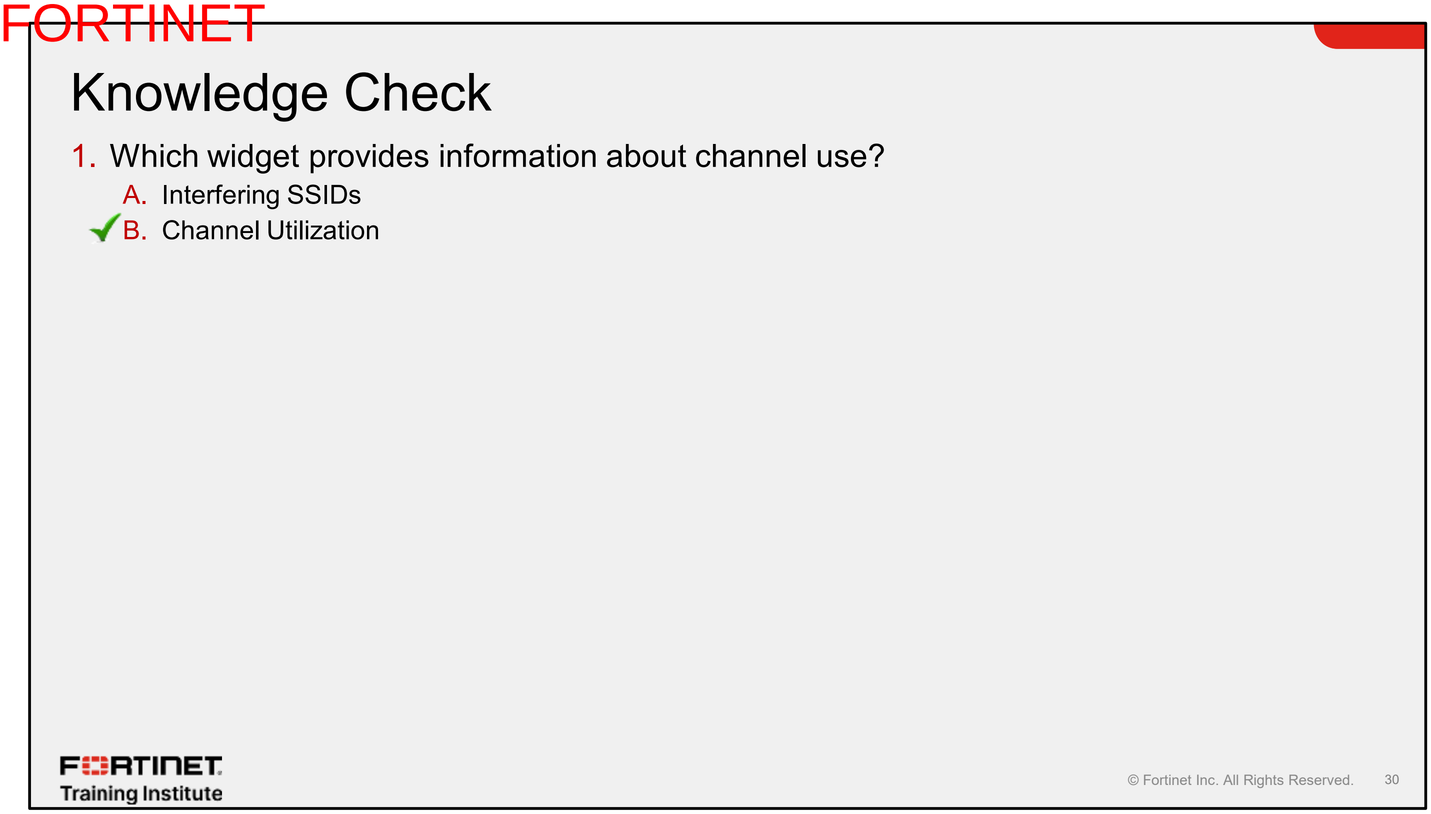
Wi-Fi & Switch Controller > WiFi Maps



29

You can place FortiAP devices on a custom map that you upload, such as an office floor plan. Wi-Fi maps show the real-time statuses of and alerts for FortiAP devices so that you can quickly see the location and status of each FortiAP device on the map.

FortiAP devices on the map provide radio channels and frequencies. You can access FortiAP device diagnostics and tools when you click a FortiAP device.

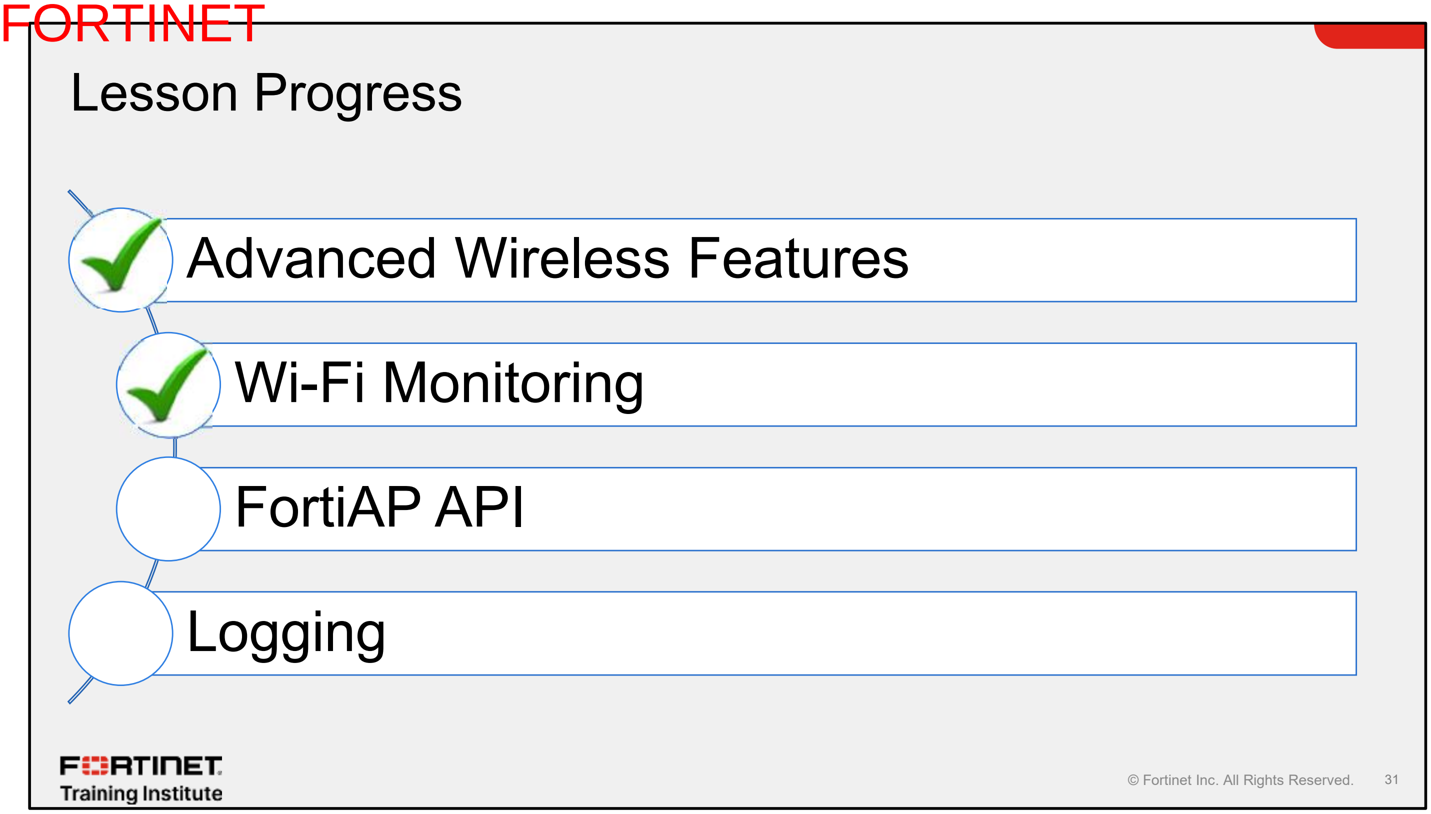


Knowledge Check

1. Which widget provides information about channel use?
   - A. Interfering SSIDs
   - ✓ B. Channel Utilization

FORTINET Training Institute

30



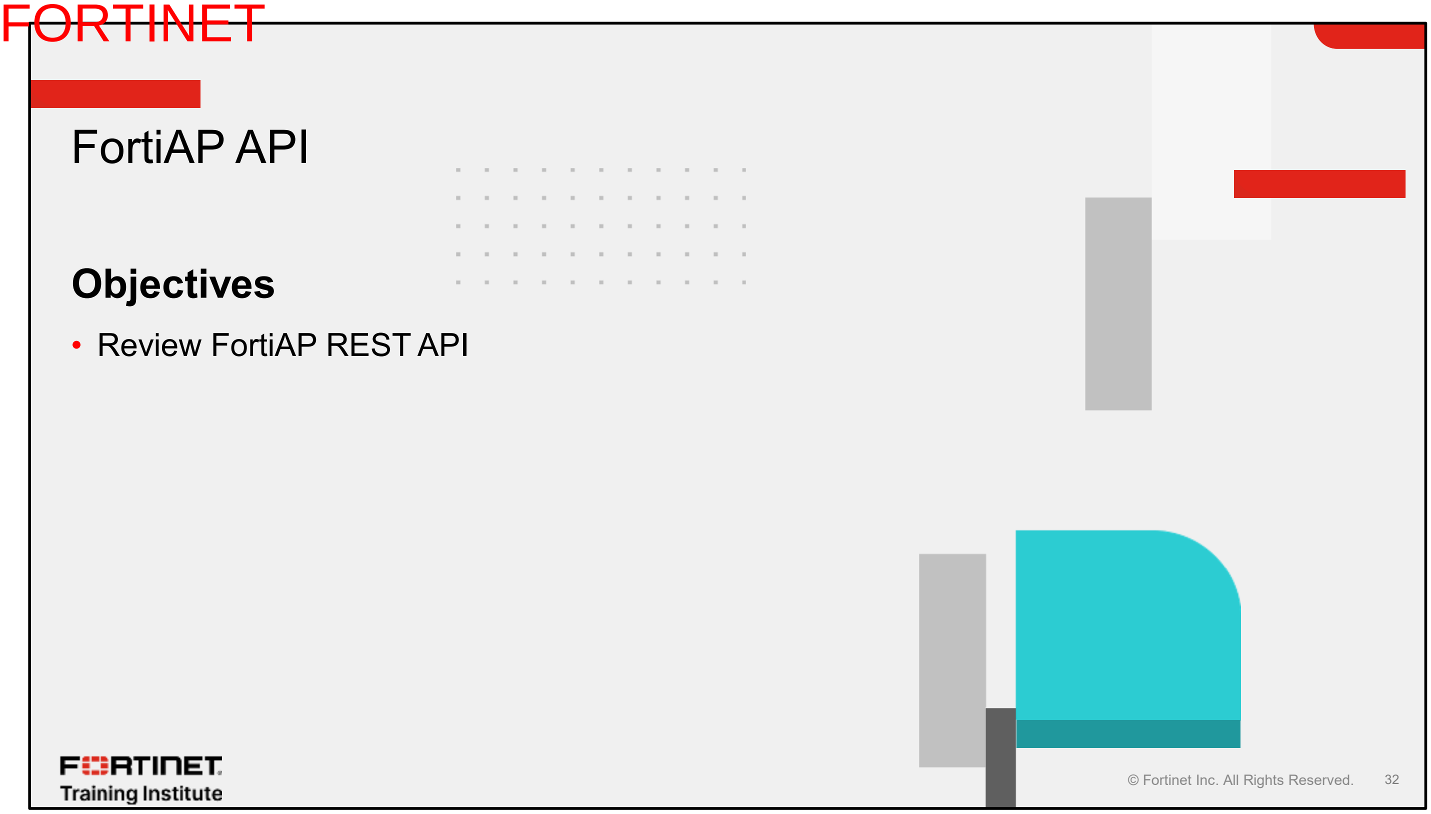
Lesson Progress

- ✓ Advanced Wireless Features
- ✓ Wi-Fi Monitoring
- ○ FortiAP API
- ○ Logging

FORTINET
Training Institute

Good job! You now understand how to monitor wireless network and FortiAP performance.

Now, you will learn about FortiAP API.



FortiAP API

Objectives

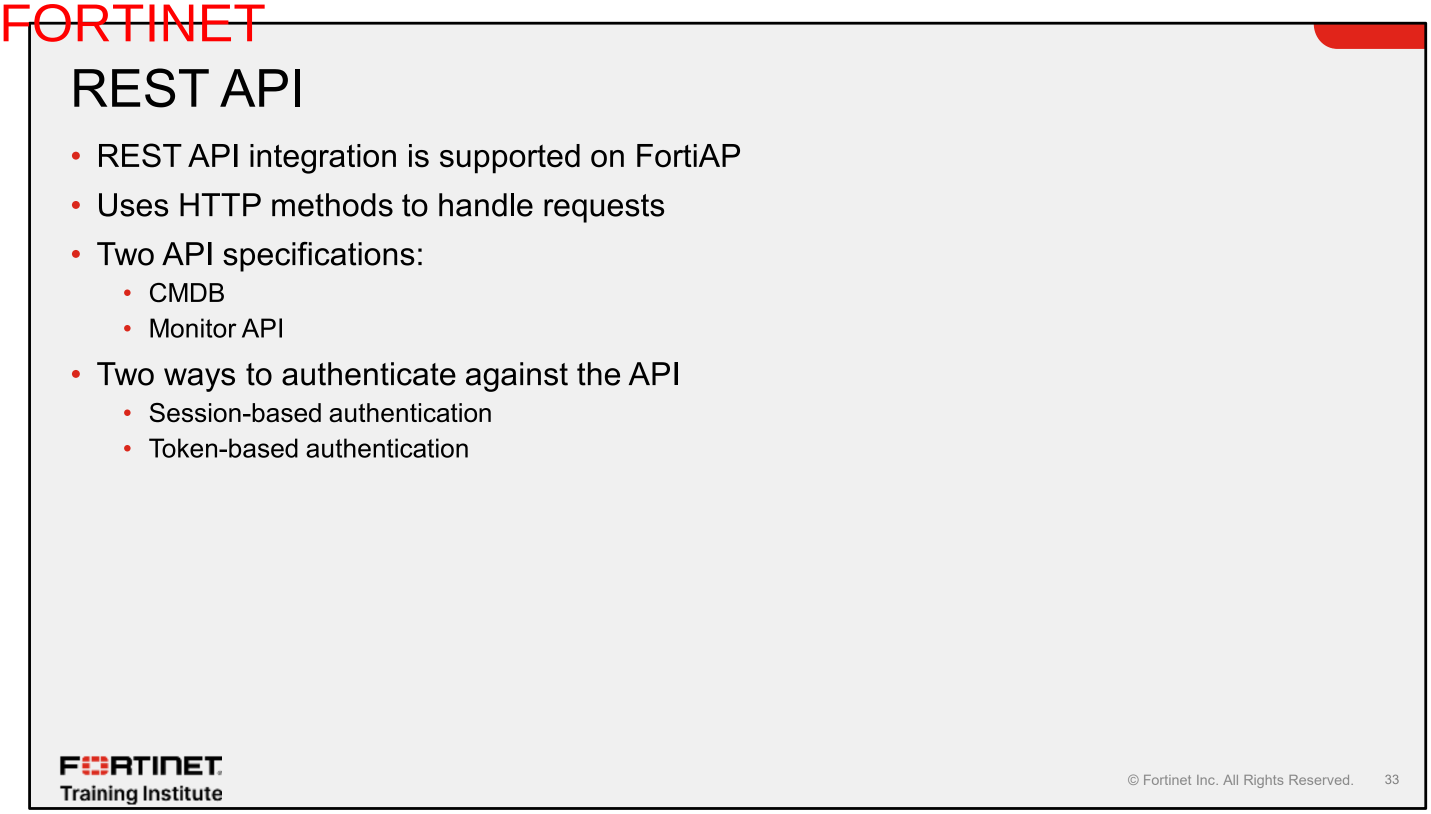
- Review FortiAP REST API

FORTINET
Training Institute

32

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in using FortiAP API, you will be to use REST API calls on FortiAP to monitor and apply changes, as required.



REST API

- REST API integration is supported on FortiAP
- Uses HTTP methods to handle requests
- Two API specifications:
  - CMDB
  - Monitor API
- Two ways to authenticate against the API
  - Session-based authentication
  - Token-based authentication

FORTINET
Training Institute

An API is a set of clearly defined methods of communication between various software components. Web APIs are typically used for communication with web servers or web browsers.

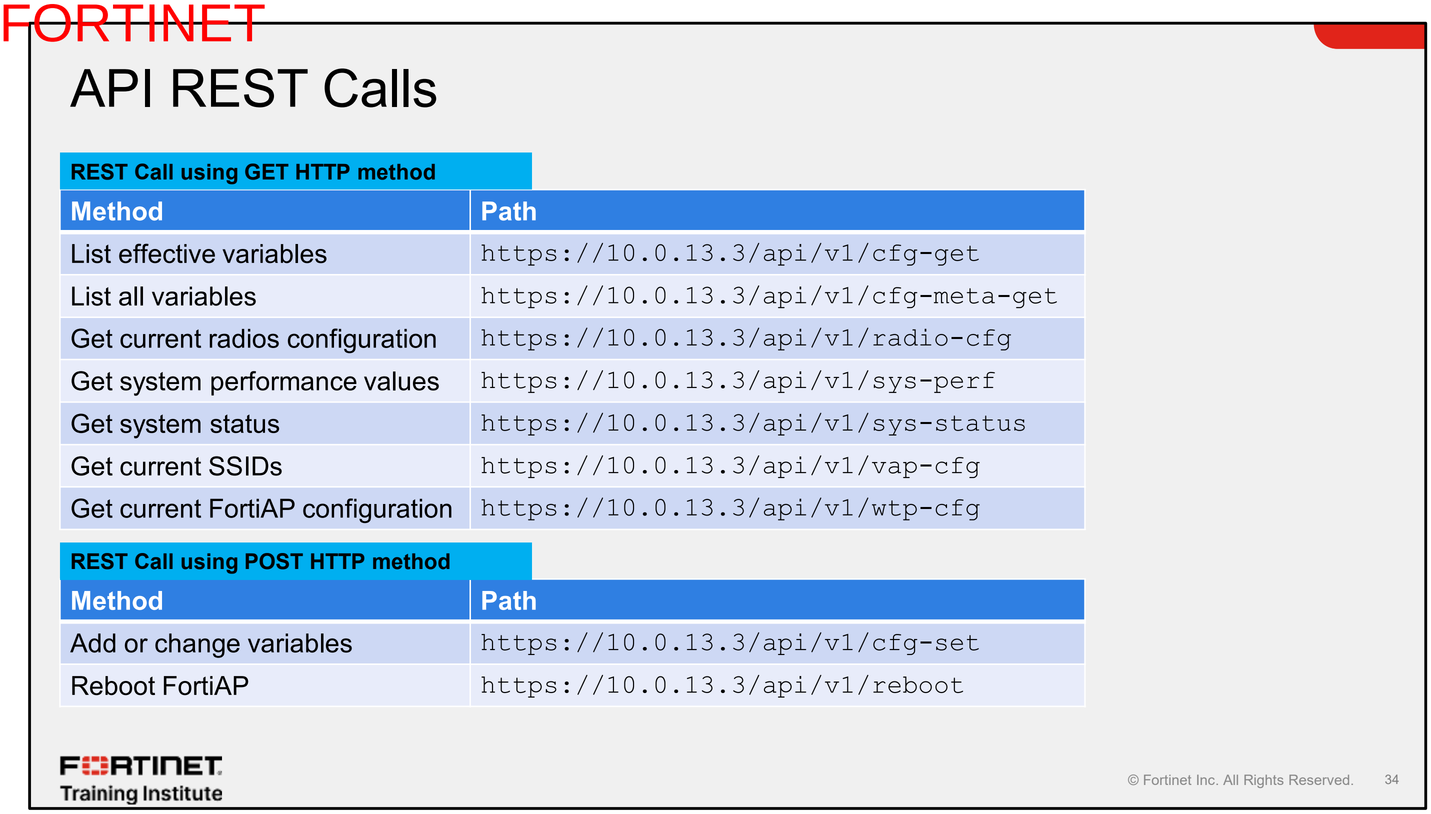
Representational state transfer (REST) is an architectural style often used in the development of web services. It uses lightweight communications between a producer and consumer, making it a popular building style for cloud-based APIs. When web services use REST architecture, they are called RESTful APIs or REST APIs.

FortiAP REST API uses HTTP requests to target specific objects. This results in a much simpler and cleaner interface. There are two API specifications—CMDB API and monitor API.

- CMDB API is used to retrieve and modify CLI configurations, such as creating, editing, and deleting objects.
- Monitor API is used to perform specific actions on endpoint resources, such as restarting, shutting down, and backing up and restoring the configuration file.

There are two ways users can authenticate API REST calls on FortiAP:

1. Session-based authentication: The authentication is valid per login session.
2. Token-based authentication: The authentication is done through a single API token.



API REST Calls

REST Call using GET HTTP method

Method	Path
List effective variables	`https://10.0.13.3/api/v1/cfg-get`
List all variables	`https://10.0.13.3/api/v1/cfg-meta-get`
Get current radios configuration	`https://10.0.13.3/api/v1/radio-cfg`
Get system performance values	`https://10.0.13.3/api/v1/sys-perf`
Get system status	`https://10.0.13.3/api/v1/sys-status`
Get current SSIDs	`https://10.0.13.3/api/v1/vap-cfg`
Get current FortiAP configuration	`https://10.0.13.3/api/v1/wtp-cfg`

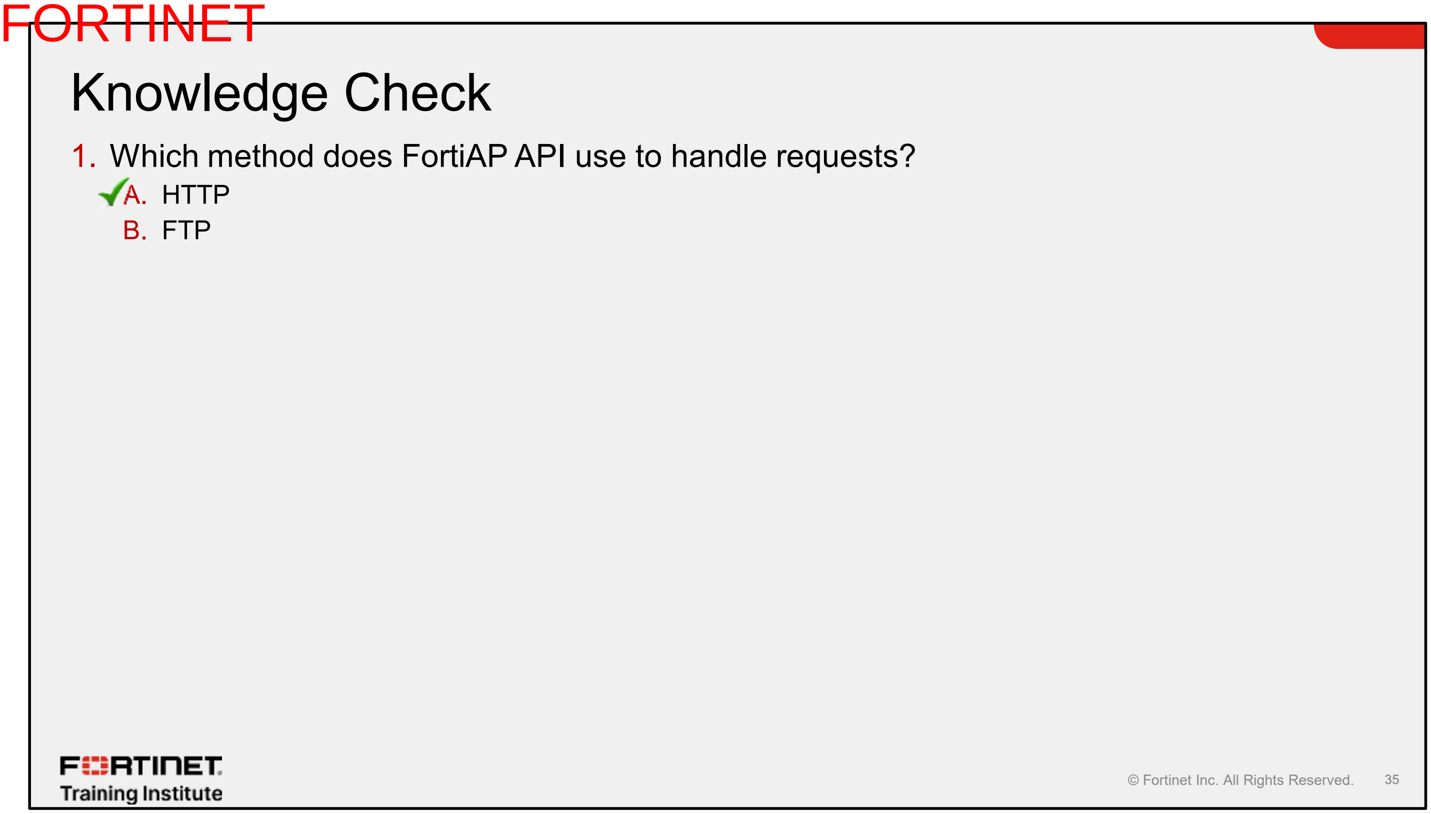
REST Call using POST HTTP method

Method	Path
Add or change variables	`https://10.0.13.3/api/v1/cfg-set`
Reboot FortiAP	`https://10.0.13.3/api/v1/reboot`

FORTINET Training Institute

34

The slide shows a list of API REST calls using GET and POST HTTP methods.

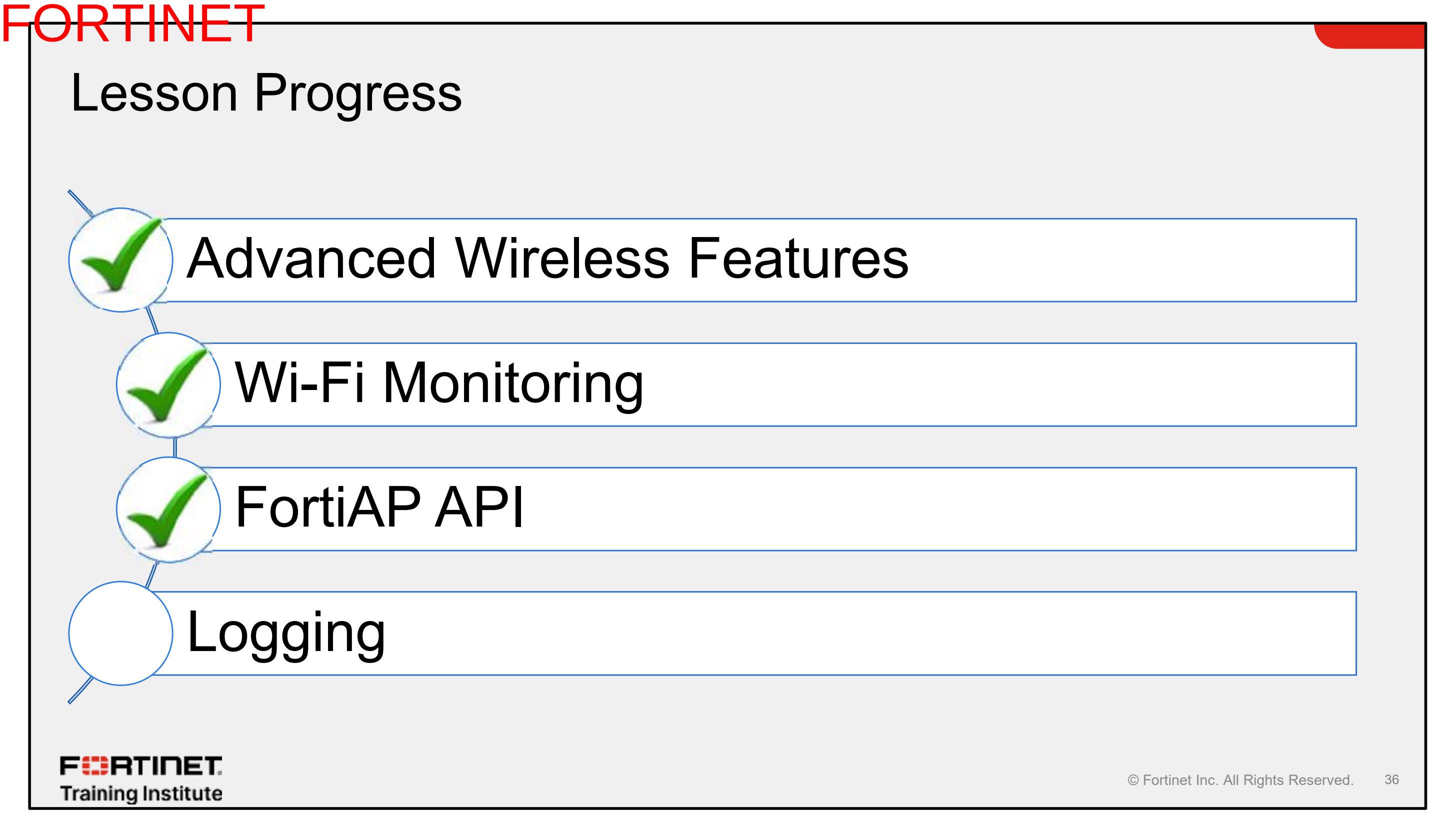


Knowledge Check

1. Which method does FortiAP API use to handle requests?

   ✓A. HTTP

   B. FTP



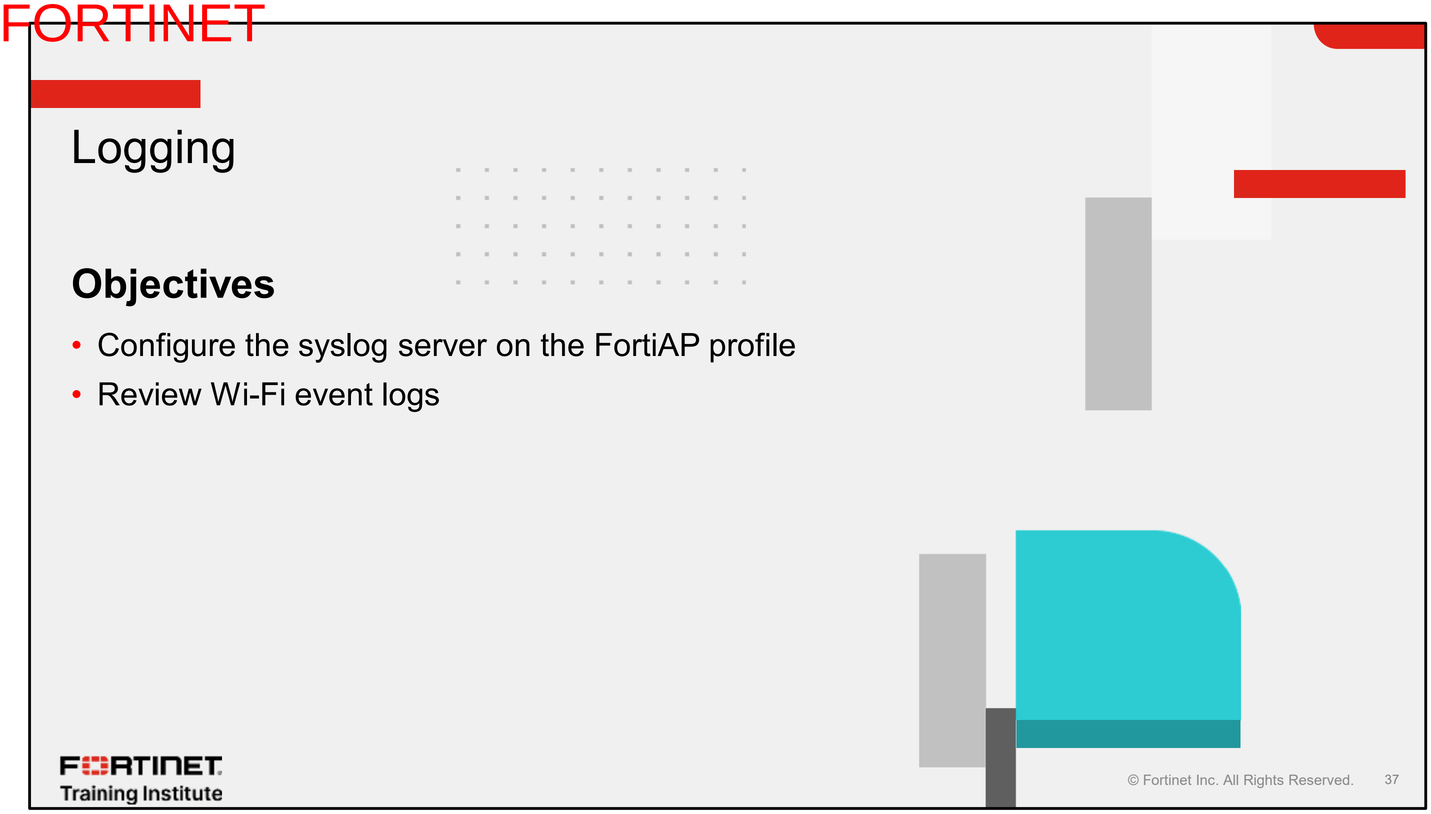
Lesson Progress

- ✓ Advanced Wireless Features
- ✓ Wi-Fi Monitoring
- ✓ FortiAP API
- ○ Logging

FORTINET
Training Institute

Good job! You now understand how to use FortiAP API.

Now, you will learn about wireless logging.



Logging

Objectives

- Configure the syslog server on the FortiAP profile
- Review Wi-Fi event logs

37

After completing this section, you should be able to achieve the objectives shown on this slide.

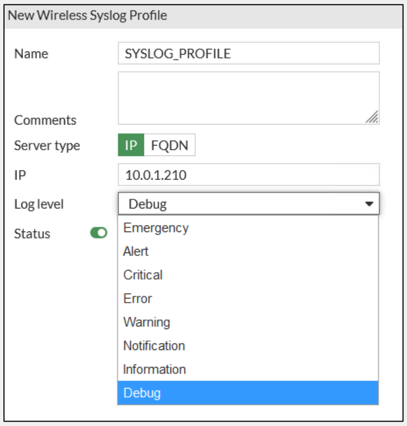
By demonstrating competence in configuring syslog on the FortiAP profile and understanding Wi-Fi event logs, you will be able to effectively analyze the logs and take the actions required to troubleshoot Wi-Fi issues.

Syslog Profile

- FortiAP can send logs to the syslog server
- Available within FortiAP profile settings
  - Possibly assigned in multiple FortiAP profiles
- Specify the log level in the syslog profile
- Use the CLI to specify the port number

```
config wireless-controller syslog-profile
    edit “SYSLOG_PROFILE"
        set server-port 514
    next
end
```

WiFi & Switch Controller > FortiAP Profiles



New Wireless Syslog Profile

Name: SYSLOG_PROFILE

Comments:

Server type: [✓ IP] FQDN

IP: 10.0.1.210

Log level: Debug

Status: ●

FORTINET Training Institute

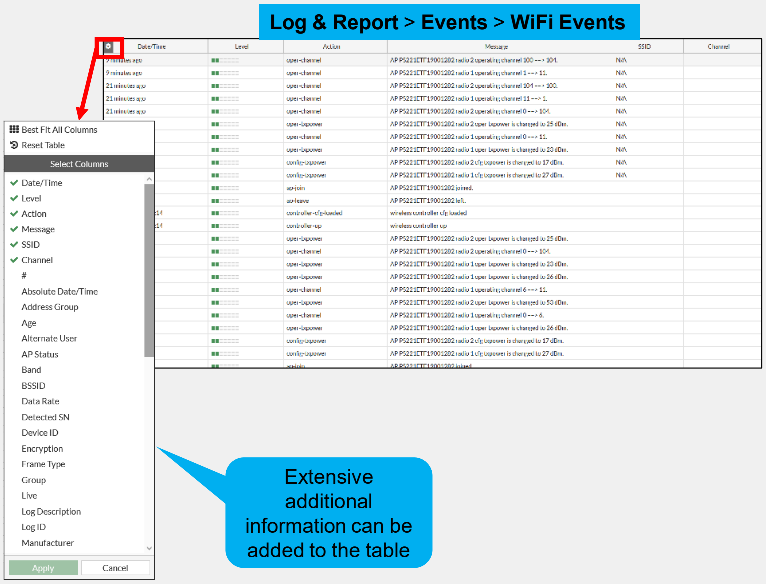
© Fortinet Inc. All Rights Reserved. 38

A FortiAP device that is managed by FortiGate or FortiLAN Cloud can send logs, such as event logs and unified threat management (UTM) logs, to the syslog server. Syslog server information is configured in a syslog profile that is assigned to a FortiAP profile.

You can specify the log level in the syslog profile and a server port number using the CLI.

Wi-Fi Event Logs

- Provide a historical log of wireless-related events
- To view specific station information:
  - Add the following columns:
    - **Band**
    - **Data Rate**
    - **Physical AP**
  - Add a filter for Station Mac
- To monitor a specific AP:
  - Add the following columns
    - **Physical AP**
  - Add a filter for **Physical AP**



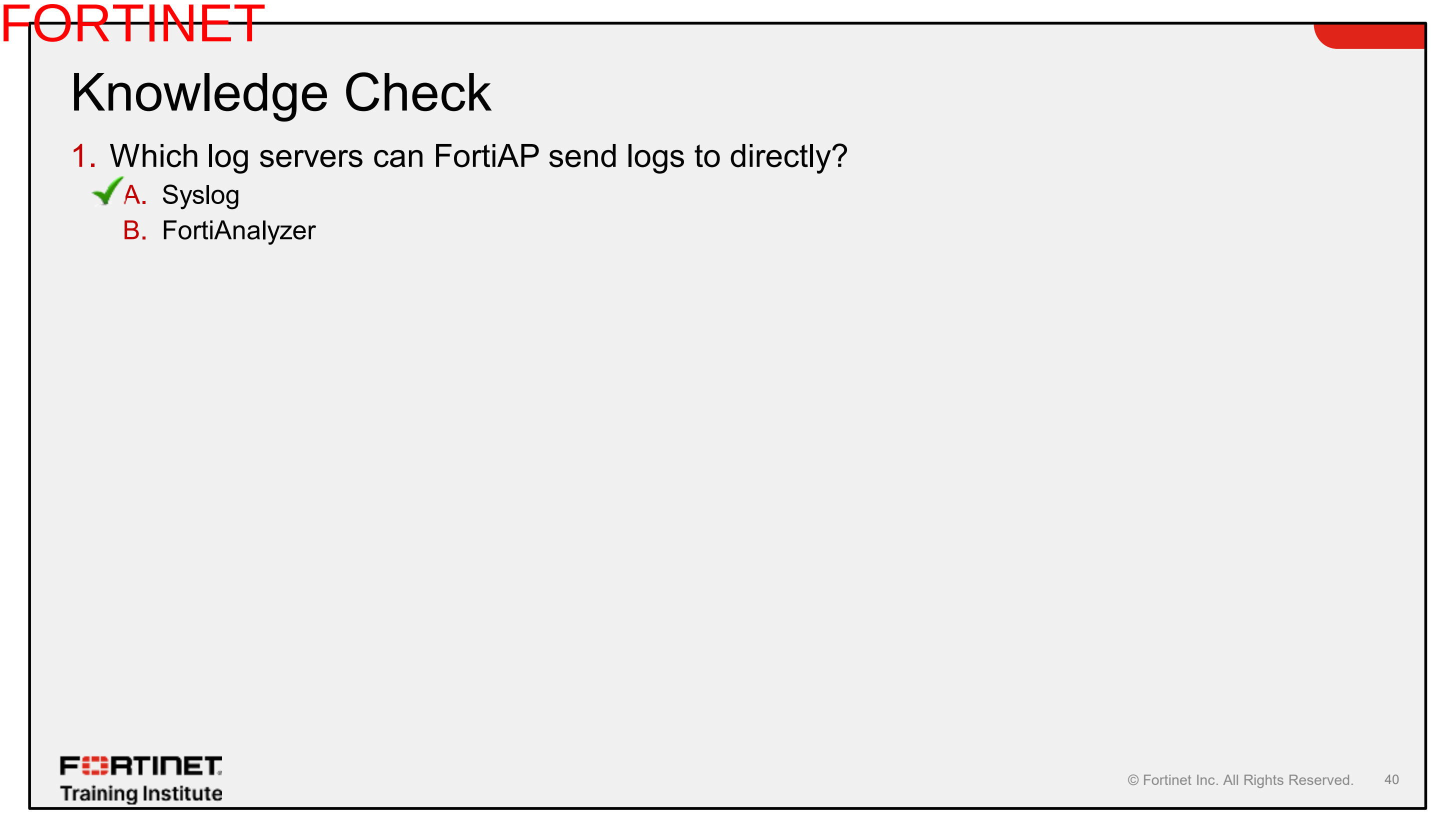
Log & Report > **Events** > **WiFi Events**

Date/Time	Level	Action	Message	SSID	Channel
9 minutes ago	■■	oper-channel	AP PS221ETF19001202 radio 2 operating channel 100 ---> 104.	N/A	
9 minutes ago	■■	oper-channel	AP PS221ETF19001202 radio 1 operating channel 1 ---> 11.	N/A	
21 minutes ago	■■	oper-channel	AP PS221ETF19001202 radio 2 operating channel 104 ---> 100.	N/A	
21 minutes ago	■■	oper-channel	AP PS221ETF19001202 radio 1 operating channel 11 ---> 1.	N/A	
21 minutes ago	■■	oper-channel	AP PS221ETF19001202 radio 2 operating channel 0 ---> 104.	N/A	
	■■	oper-txpower	AP PS221ETF19001202 radio 2 oper txpower is changed to 25 dBm.	N/A	
	■■	oper-channel	AP PS221ETF19001202 radio 1 operating channel 0 ---> 11.	N/A	
	■■	oper-txpower	AP PS221ETF19001202 radio 1 oper txpower is changed to 23 dBm.	N/A	
	■■	config-txpower	AP PS221ETF19001202 radio 2 cfg txpower is changed to 17 dBm.	N/A	
	■■	config-txpower	AP PS221ETF19001202 radio 1 cfg txpower is changed to 27 dBm.	N/A	
	■■	ap-join	AP PS221ETF19001202 joined.		
	■■	ap-leave	AP PS221ETF19001202 left.		
:14	■■	controller-cfg-loaded	wireless controller cfg loaded		
:14	■■	controller-up	wireless controller up		
	■■	oper-txpower	AP PS221ETF19001202 radio 2 oper txpower is changed to 25 dBm.		
	■■	oper-channel	AP PS221ETF19001202 radio 2 operating channel 0 ---> 104.		
	■■	oper-txpower	AP PS221ETF19001202 radio 1 oper txpower is changed to 23 dBm.		
	■■	oper-txpower	AP PS221ETF19001202 radio 1 oper txpower is changed to 26 dBm.		
	■■	oper-channel	AP PS221ETF19001202 radio 1 operating channel 6 ---> 11.		
	■■	oper-txpower	AP PS221ETF19001202 radio 2 oper txpower is changed to 53 dBm.		
	■■	oper-channel	AP PS221ETF19001202 radio 1 operating channel 0 ---> 6.		
	■■	oper-txpower	AP PS221ETF19001202 radio 1 oper txpower is changed to 26 dBm.		
	■■	config-txpower	AP PS221ETF19001202 radio 2 cfg txpower is changed to 17 dBm.		
	■■	config-txpower	AP PS221ETF19001202 radio 1 cfg txpower is changed to 27 dBm.		
	■■	ap-join	AP PS221ETF19001202 joined.		

Extensive additional information can be added to the table

The **Events** table provides a whole-controller historical view of the wireless network. You can use this to identify events that affect both clients and APs over time.

Adding additional columns and filtering allows you to focus in on wireless clients or APs that are misbehaving.

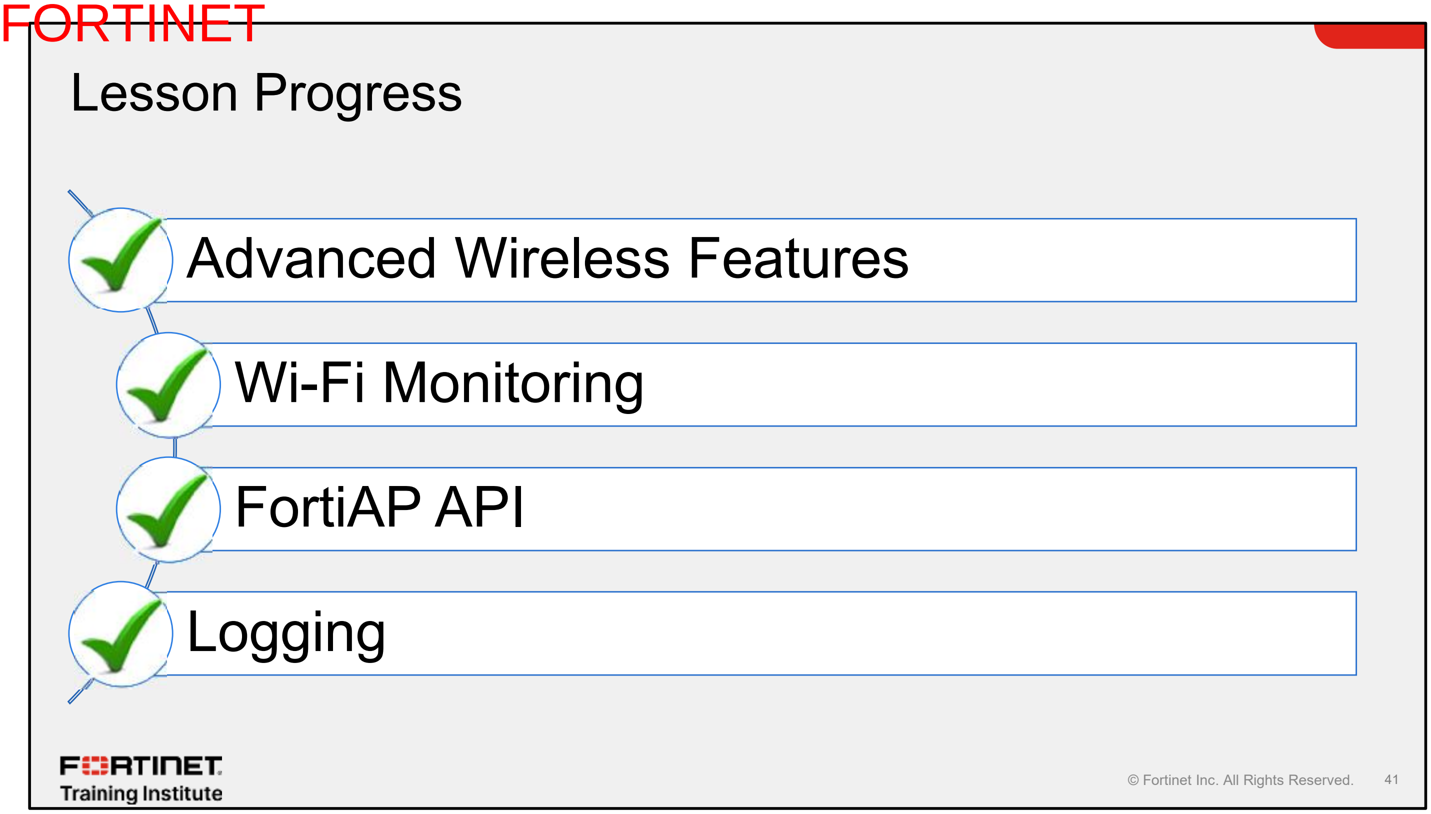


Knowledge Check

1. Which log servers can FortiAP send logs to directly?
   - ✓ A. Syslog
   - B. FortiAnalyzer

FORTINET Training Institute

40



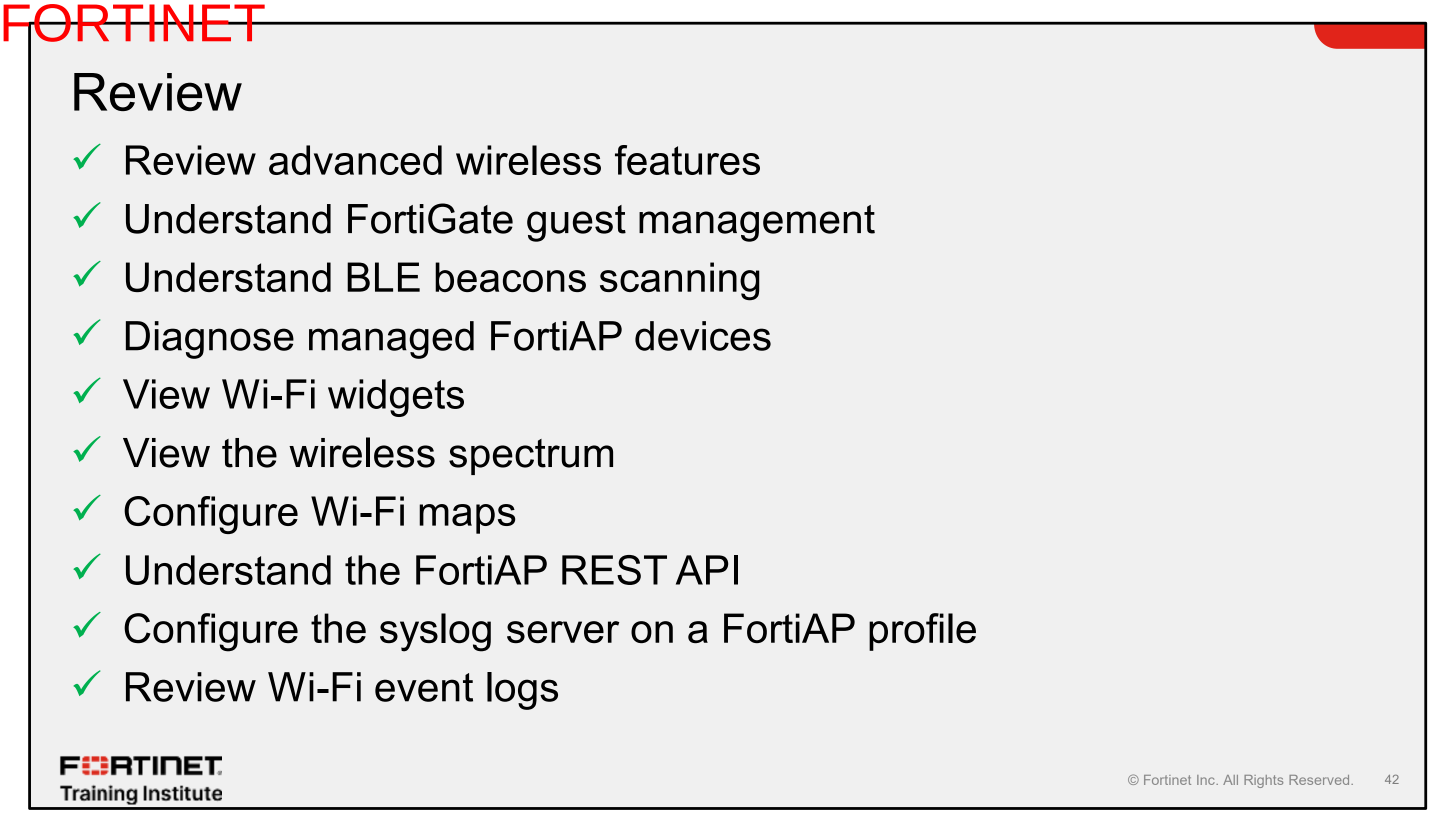
Lesson Progress

- ✓ Advanced Wireless Features
- ✓ Wi-Fi Monitoring
- ✓ FortiAP API
- ✓ Logging

41

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



Review

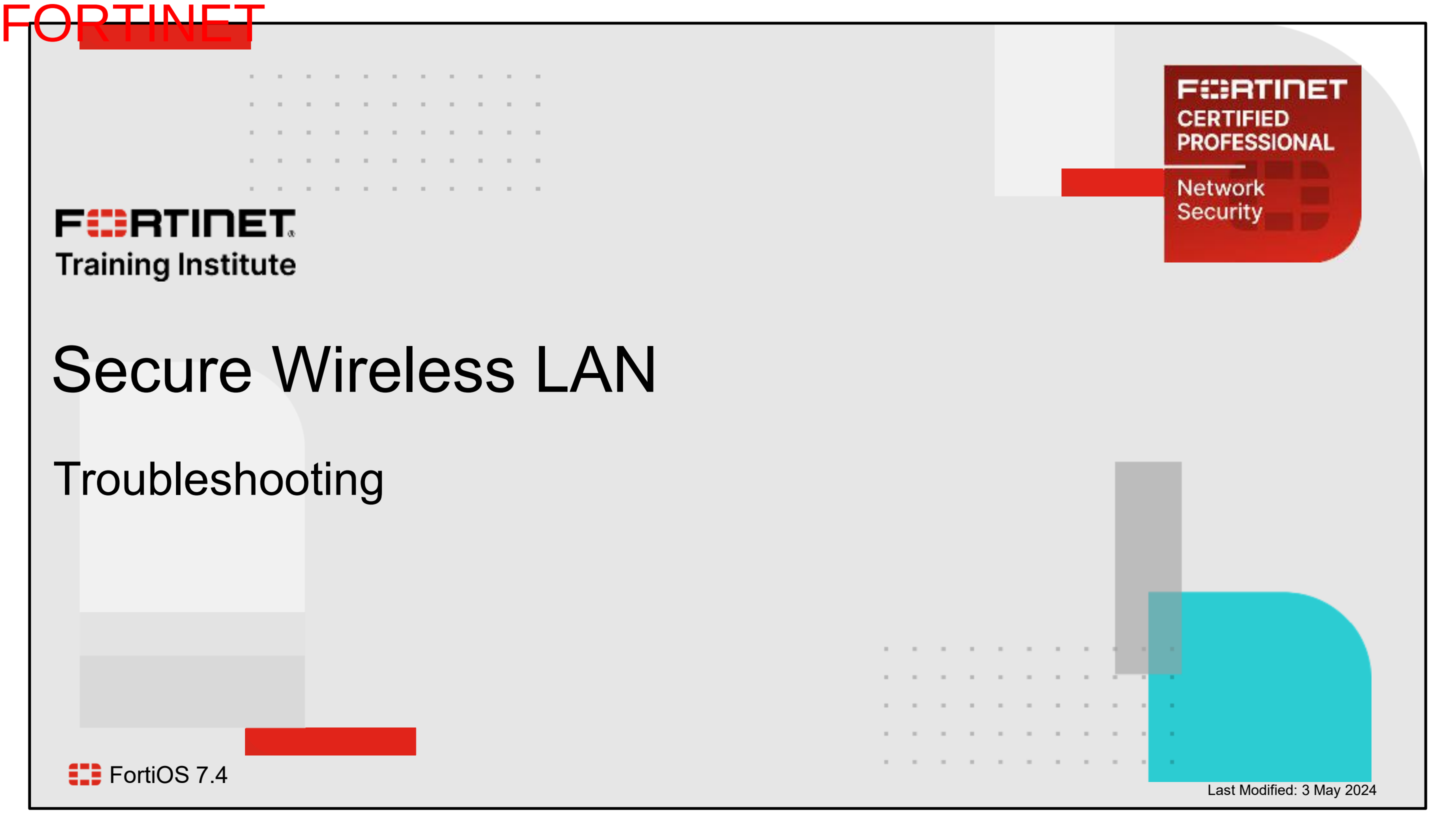
- ✓ Review advanced wireless features
- ✓ Understand FortiGate guest management
- ✓ Understand BLE beacons scanning
- ✓ Diagnose managed FortiAP devices
- ✓ View Wi-Fi widgets
- ✓ View the wireless spectrum
- ✓ Configure Wi-Fi maps
- ✓ Understand the FortiAP REST API
- ✓ Configure the syslog server on a FortiAP profile
- ✓ Review Wi-Fi event logs

FORTINET Training Institute

42

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the wireless technology concepts that you must know to understand Wi-Fi and wireless technologies in general. You also learned how to plan your network for the best wireless signal coverage.



FORTINET CERTIFIED PROFESSIONAL
Network Security

FORTINET
Training Institute

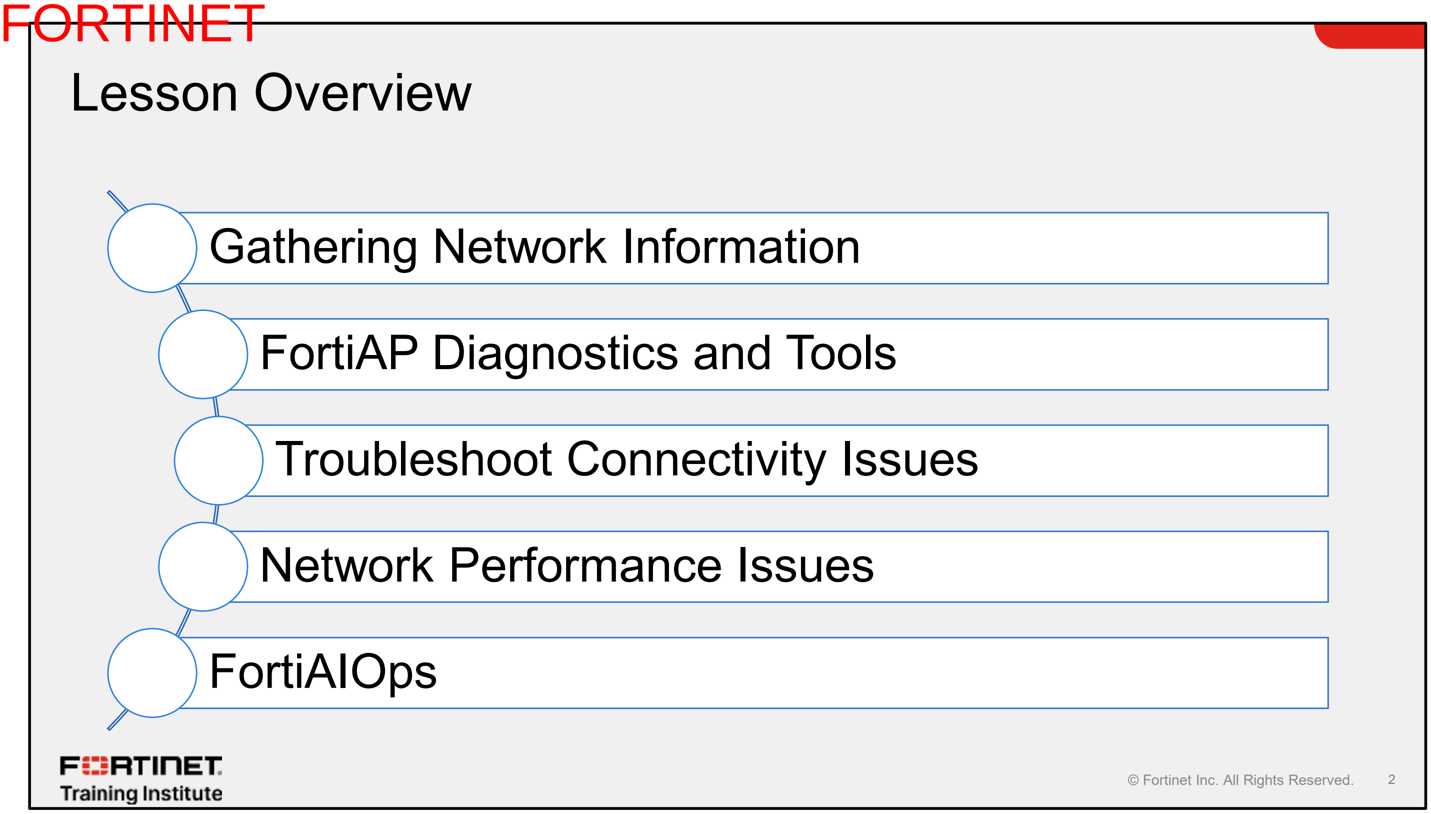
Secure Wireless LAN

Troubleshooting

FortiOS 7.4

Last Modified: 3 May 2024

In this lesson, you will learn about troubleshooting secure wireless LAN.



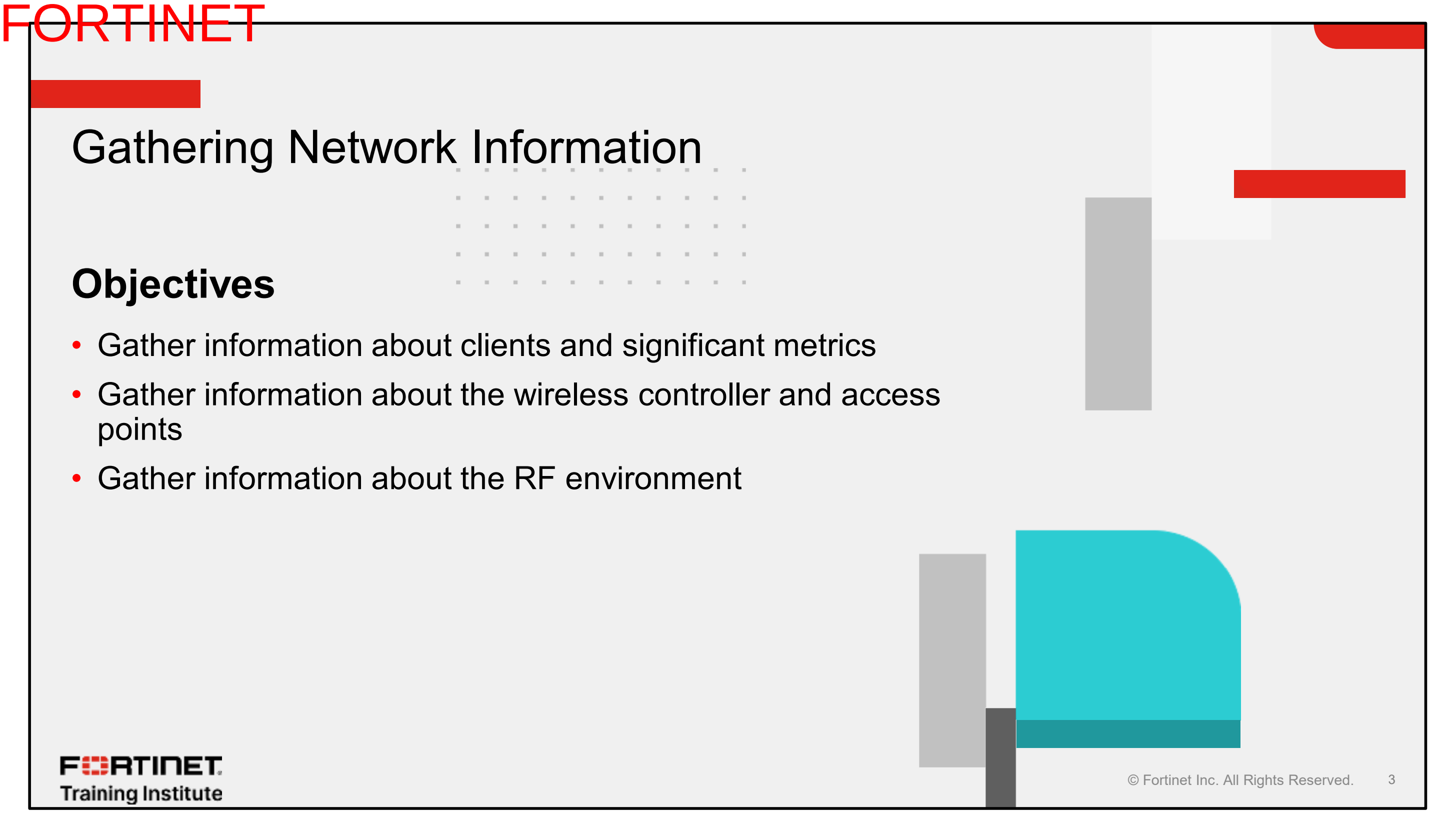
Lesson Overview

- Gathering Network Information
- FortiAP Diagnostics and Tools
- Troubleshoot Connectivity Issues
- Network Performance Issues
- FortiAIOps

FORTINET Training Institute

2

In this lesson, you will learn about the topics shown on this slide.



Gathering Network Information

Objectives

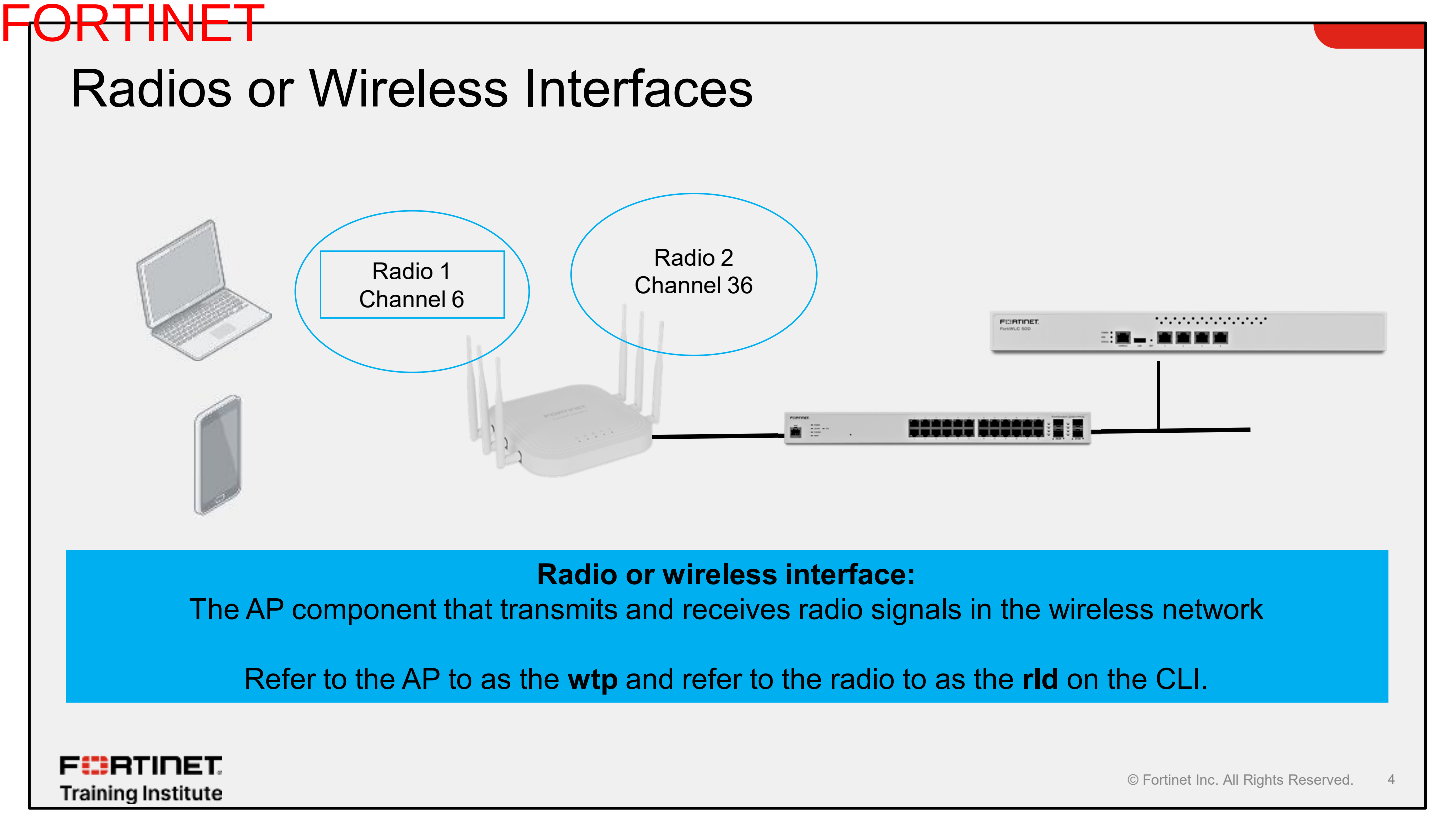
- Gather information about clients and significant metrics
- Gather information about the wireless controller and access points
- Gather information about the RF environment

Training Institute

3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the wireless controller, you will be able to identify, collect, and monitor important information about the wireless network.

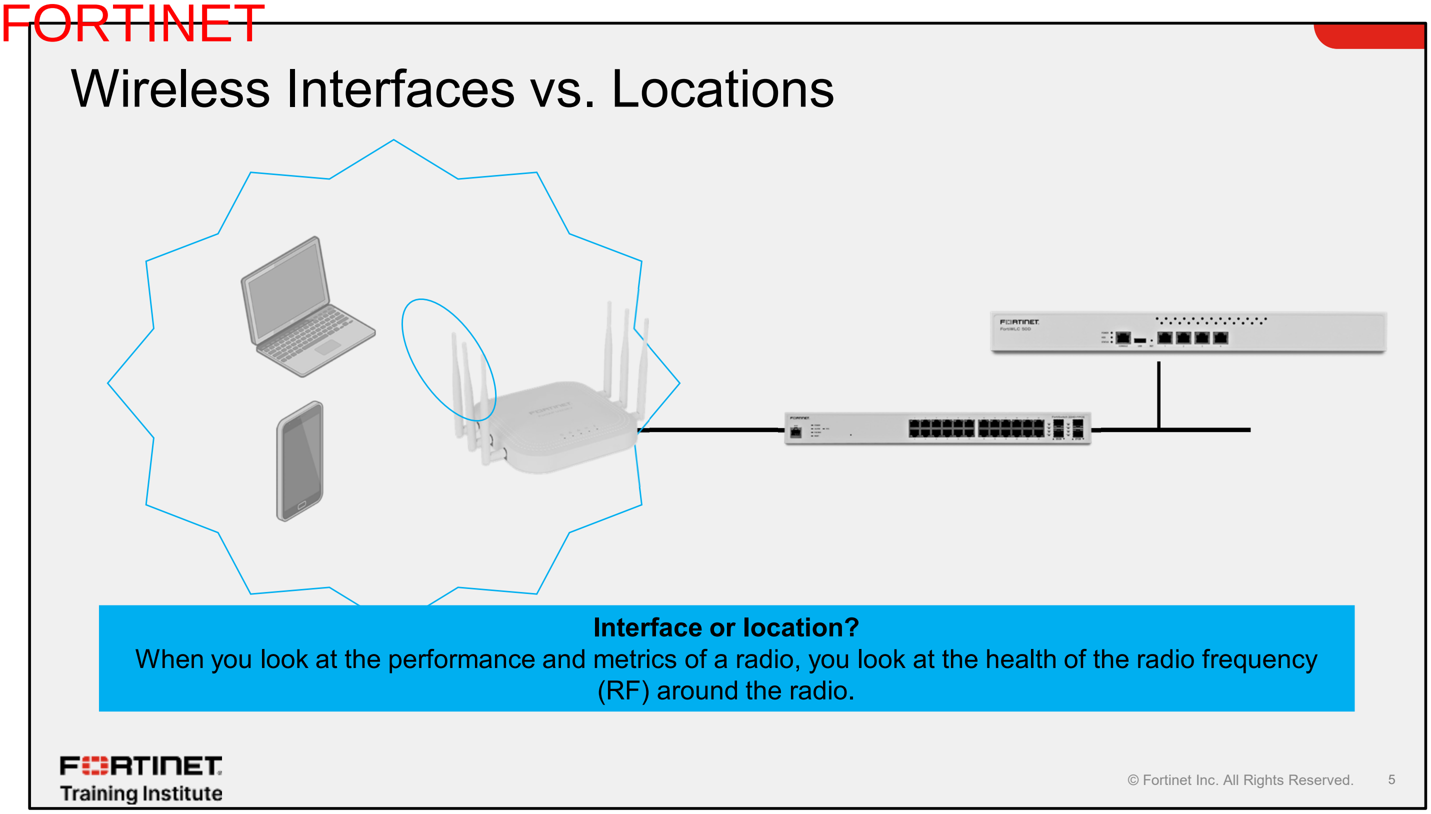


Radios or Wireless Interfaces

Radio or wireless interface:
The AP component that transmits and receives radio signals in the wireless network

Refer to the AP to as the **wtp** and refer to the radio to as the **rld** on the CLI.

On FortiAP, the component on the access point (AP) that transmits and receives radio signals is called a radio, or wireless, interface. Both terms are used in the controller management interfaces.

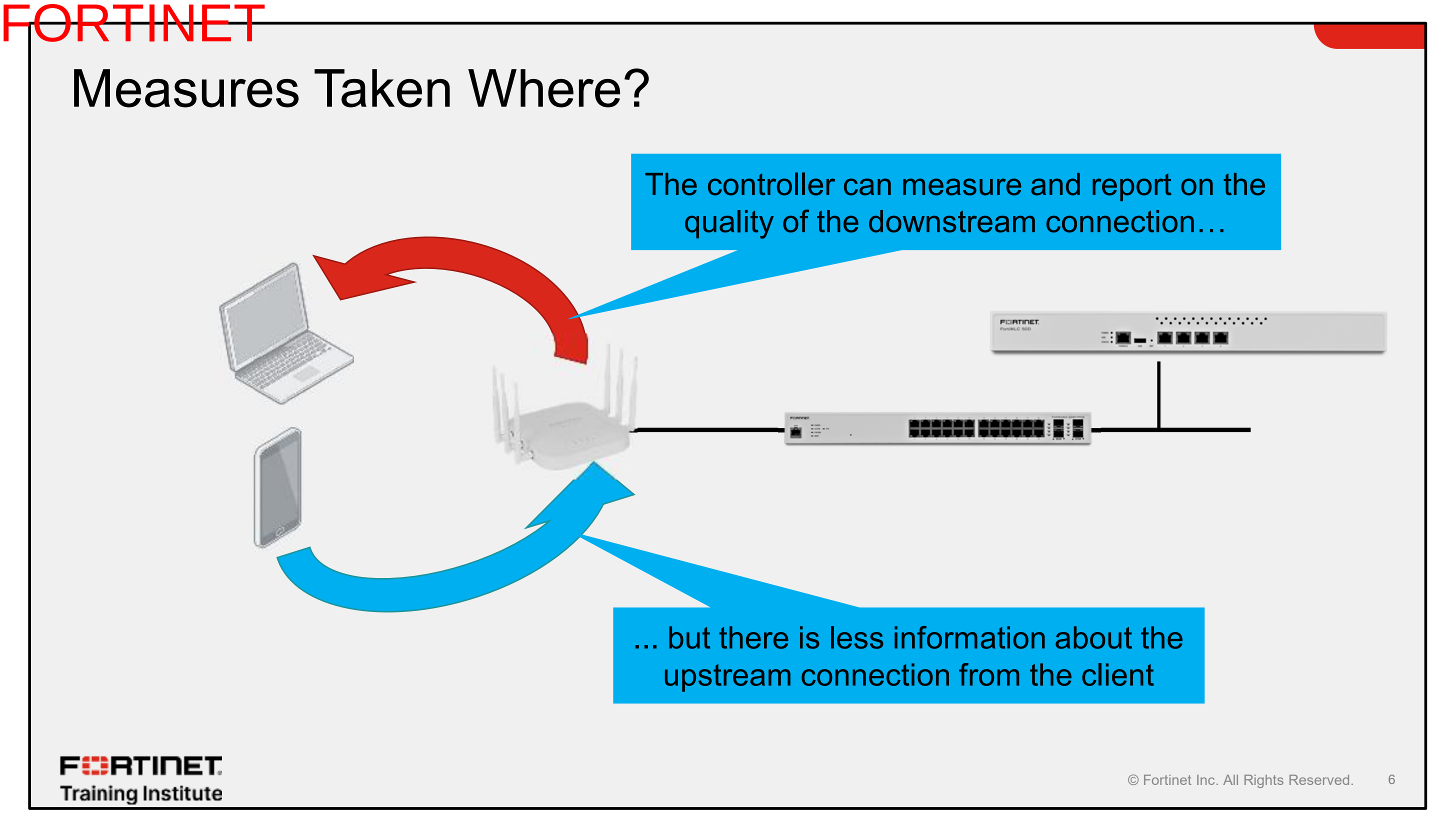


Wireless Interfaces vs. Locations

Interface or location?
When you look at the performance and metrics of a radio, you look at the health of the radio frequency (RF) around the radio.

When you look at the metrics and diagnostics of wireless interfaces, it is easy to think only about the radio itself and that it has a retry rate or a percentage of channel utilization.

While this is true, retry rate and percentage of channel utilization indicate the quality and capacity of the air, or RF, *around* the AP. This assessment also includes the clients that use the RF. Many of the measures you take at the AP also impact the clients.



Measures Taken Where?

The controller can measure and report on the quality of the downstream connection…

... but there is less information about the upstream connection from the client

6

Most of the metrics shown on the controller are measured from the *AP or controller point of view.*

When an AP transmits network traffic to a client, the controller shows the connection quality of the AP when it transmits *to* the client.

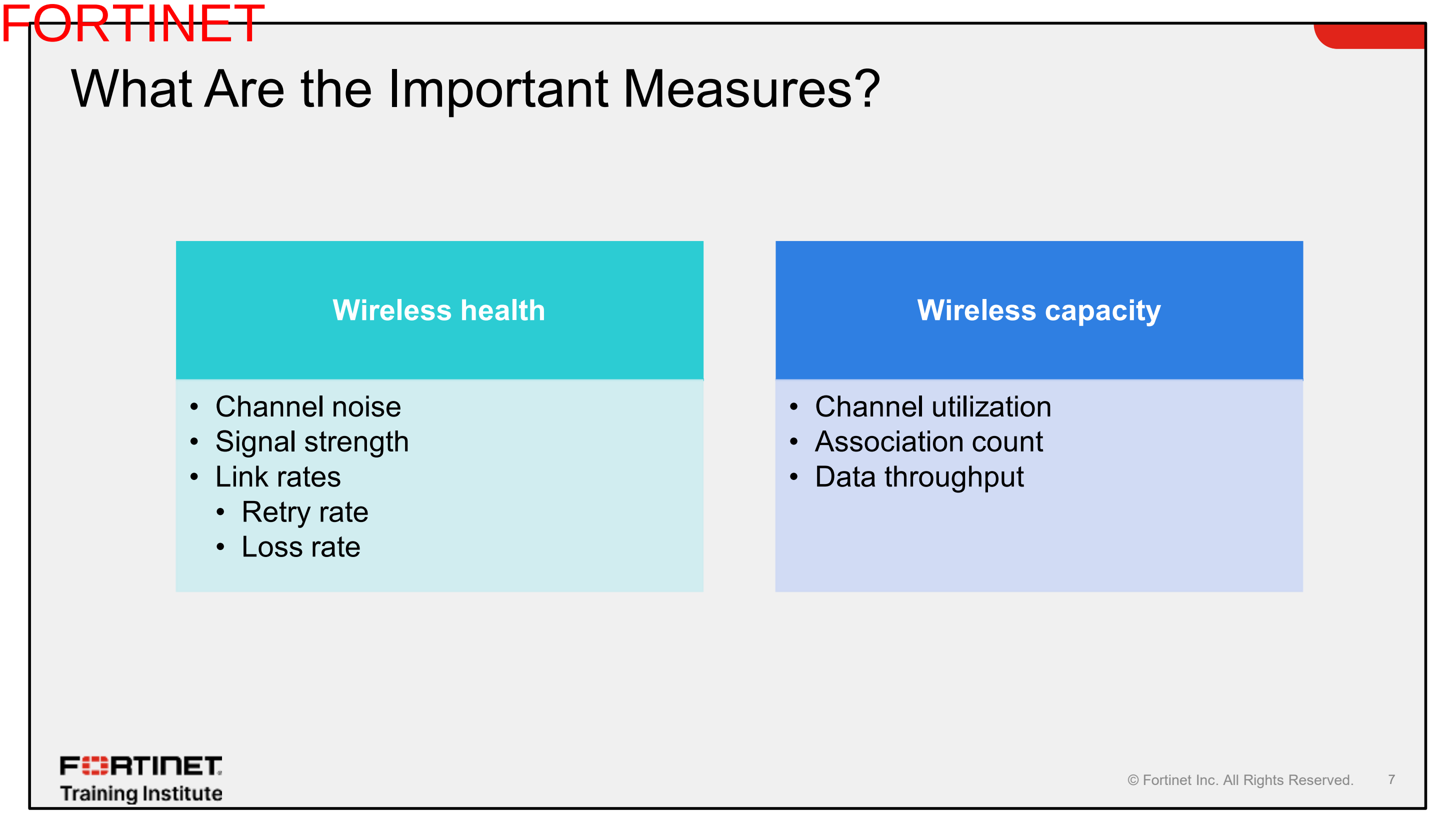
The client is subject to the same RF environment and is likely to have as much difficulty, if not more, to transmit traffic back to the AP.

The client connection quality is *usually* poorer than the AP connection because its transmit power rate is less than the AP, and the antennas on clients tend not to be as good.

This can result in clients being *more* susceptible to interference, for example.

The AP can't measure the client signal quality directly. Only the client network card can measure this and there is no way for these metrics to be sent back to the wireless network. Often the client operating system doesn't report these metrics to the end user. Usually, the client must install a tool designed specifically to capture these metrics.

Regardless, you can learn a lot about the client wireless experience from the metrics gathered on the controller.



What Are the Important Measures?

Wireless health

- Channel noise
- Signal strength
- Link rates
  - Retry rate
  - Loss rate

Wireless capacity

- Channel utilization
- Association count
- Data throughput

FORTINET Training Institute

7

For a large proportion of wireless clients, troubleshooting revolves around ensuring that a number of wireless metrics are within acceptable ranges.

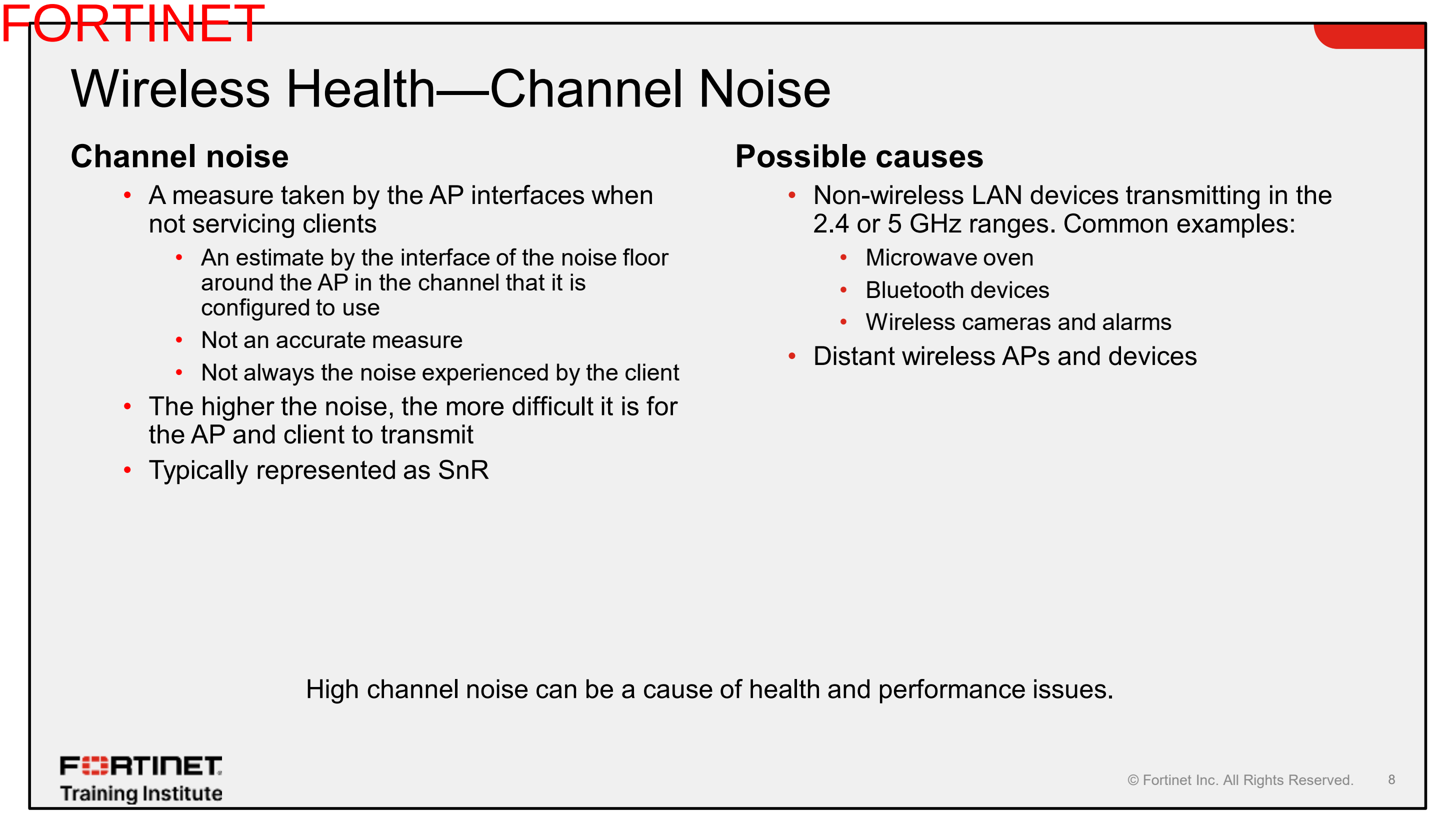
The important measures belong to two broad categories—wireless health and wireless capacity.

Wireless health includes measures of factors that affect connection reliability, such as getting or staying connected to a wireless network. It is a measure of how healthy the RF is around a specific interface. Wireless health assesses how well wireless frames are being transmitted from the APs to the clients. You can check wireless health by looking at the channel noise measured by the interface in a specific area, the signal strength of the client, and the link rates that the client is using.

Wireless capacity measures factors that affect the capacity of the interface and the channel capacity around the interface. It is a measure of channel utilization—how busy the interface and the spectrum is, and the number of clients on an interface. The retry rate can be an indication that the collision rate is high, which can occur when there are large numbers of clients in the network, which is, again, a capacity measure.

A number of metrics are relevant to both categories, however, some are more important than others.

Some of these measures, such as retry and loss rates, are not easily measurable in a FortiWiFi system, however, because these measures are important in the AP and client calculation of link rates, you can use the link rate as a prime indicator of connection quality.



Wireless Health—Channel Noise

Channel noise

- A measure taken by the AP interfaces when not servicing clients
  - An estimate by the interface of the noise floor around the AP in the channel that it is configured to use
  - Not an accurate measure
  - Not always the noise experienced by the client
- The higher the noise, the more difficult it is for the AP and client to transmit
- Typically represented as SnR

Possible causes

- Non-wireless LAN devices transmitting in the 2.4 or 5 GHz ranges. Common examples:
  - Microwave oven
  - Bluetooth devices
  - Wireless cameras and alarms
- Distant wireless APs and devices

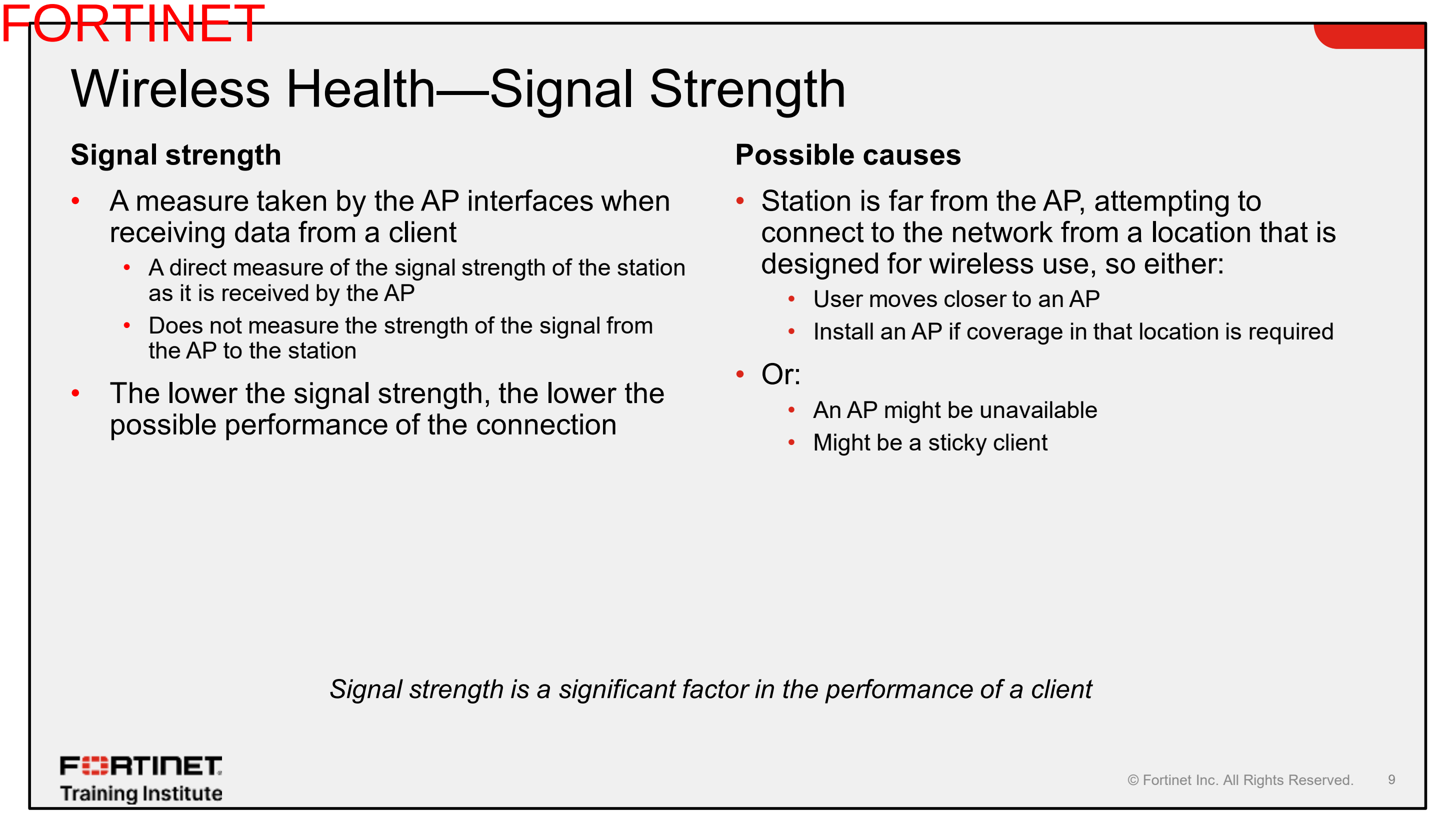
High channel noise can be a cause of health and performance issues.

FORTINET Training Institute

8

The AP interfaces are constantly monitoring the wireless channel they are tuned in to. One of the things an interface can do when it is not servicing clients is take a measurement of the noise floor. Channel noise is a measure of the background wireless signal that the radio cannot interpret as a wireless LAN signal. To a radio, any signal that comes from another device sounds like radio static sounds to a human. Ambient channel noise is generated by many different sources that can interfere with a network. The higher the level of noise the lower the signal-to-noise ratio (SnR), which can affect both the AP and client ability to send a frame. Often both the client and AP radios will respond to the decrease in SnR by reducing the connection link rates. This can result in an acceptable signal strength but an unusually low link rate, indicating that there is potentially a noise issue.

Because the interface is not a dedicated spectrum analyzer, this measure is only an *estimate*. However, it is a very important indicator of potential interference in a specific area of the network. Such interference would cause significant issues with the network if it was both powerful and frequent (a high duty cycle).



Wireless Health—Signal Strength

Signal strength

- A measure taken by the AP interfaces when receiving data from a client
  - A direct measure of the signal strength of the station as it is received by the AP
  - Does not measure the strength of the signal from the AP to the station
- The lower the signal strength, the lower the possible performance of the connection

Possible causes

- Station is far from the AP, attempting to connect to the network from a location that is designed for wireless use, so either:
  - User moves closer to an AP
  - Install an AP if coverage in that location is required
- Or:
  - An AP might be unavailable
  - Might be a sticky client

Signal strength is a significant factor in the performance of a client

Training Institute

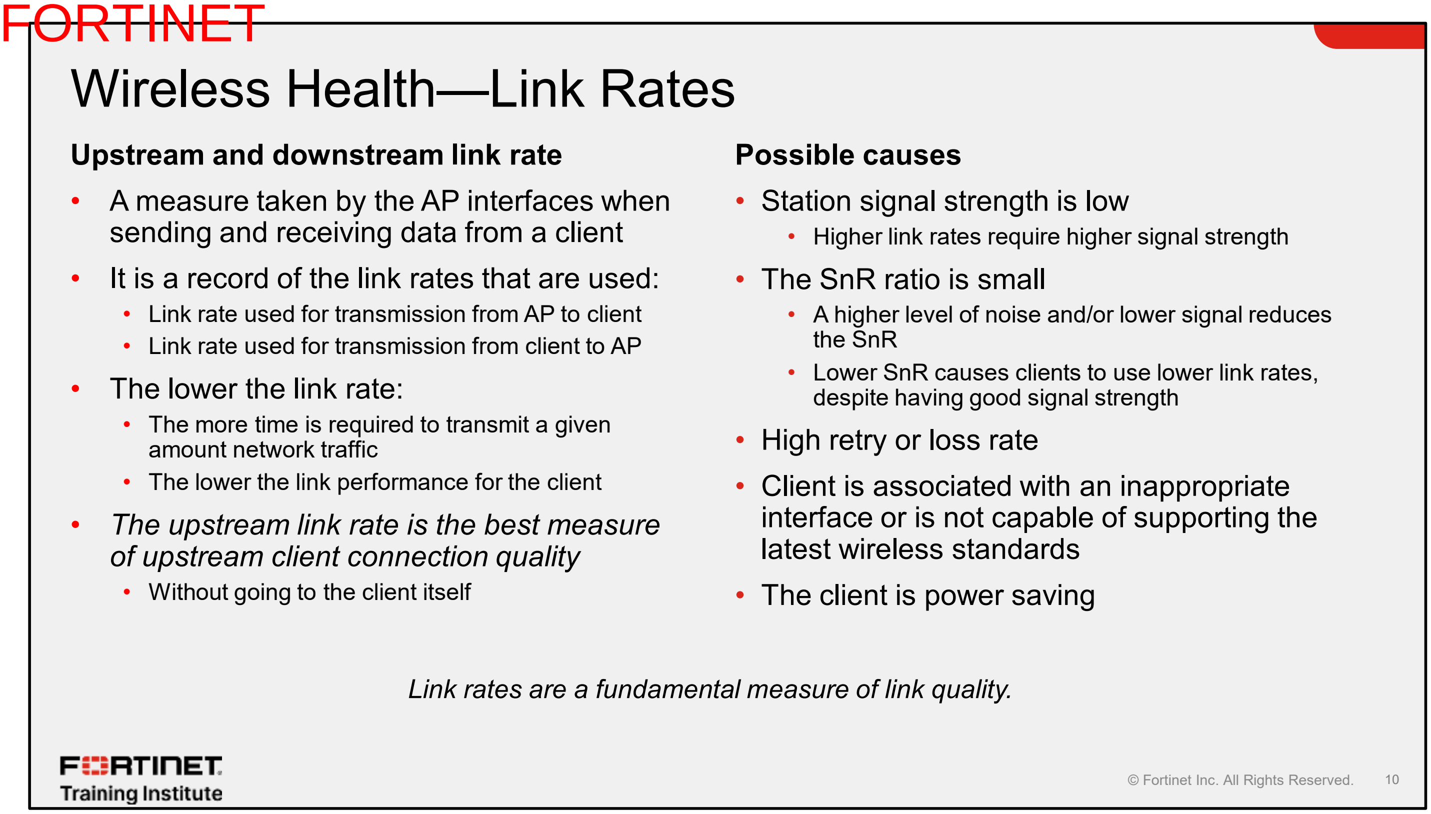
The controller maintains a list of the receive signal strength (RSSI) for all clients. RSSI is measured by the AP of each client as transmissions occur. It is not a measure taken by the client of the AP signal strength, which arguably is more important, because the majority of data is downstream.

However, it is still possible to infer that the downstream signal strength is somewhat stronger than the upstream signal strength. In general, the transmission power of the AP can be higher than the transmission power of the client, so it is reasonable to expect that the client’s signal strength is somewhat less than the signal of the AP.

The lower the signal strength, the lower the ability of the radio to use higher modulation rates. The lower those rates, the lower the connection performance of the client. Low signal scenarios can occur for a number of reasons. Most commonly, someone is trying use the wireless network from a location that was never designed to support wireless devices. As a result, they are simply standing too far away from the AP. At that point, the user must choose to either move to a location that is designed to be supported by the wireless network or, if the location warrants it, install a new AP to improve the signal strength.

Low signal strength may also indicate that an AP has stopped running. The network is designed with overlap to allow for RF redundancy. In the event of an AP failure, there is usually another AP within range even if it has a much lower signal strength. The result is that the client will associate with that other AP, but will appear as a low-signal-strength client.

In more complex RF environments, a client might maintain a connection to the original AP. After the client moves to another location, they remain “stuck” to the original AP, and are known as a sticky client. In these types of design scenarios, low-signal-strength stations can be a fact of life. It may not be possible to eliminate low-signal-strength stations completely, but it is possible to monitor the number of devices that are poorly connected.



Wireless Health—Link Rates

Upstream and downstream link rate

- A measure taken by the AP interfaces when sending and receiving data from a client
- It is a record of the link rates that are used:
  - Link rate used for transmission from AP to client
  - Link rate used for transmission from client to AP
- The lower the link rate:
  - The more time is required to transmit a given amount network traffic
  - The lower the link performance for the client
- *The upstream link rate is the best measure of upstream client connection quality*
  - Without going to the client itself

Possible causes

- Station signal strength is low
  - Higher link rates require higher signal strength
- The SnR ratio is small
  - A higher level of noise and/or lower signal reduces the SnR
  - Lower SnR causes clients to use lower link rates, despite having good signal strength
- High retry or loss rate
- Client is associated with an inappropriate interface or is not capable of supporting the latest wireless standards
- The client is power saving

Link rates are a fundamental measure of link quality.

FORTINET Training Institute

10

The transmit and receive link rates show the data rates that are being used by the AP, which is the TX, or transmit rate, and client, which is the RX, or receive rate. Both are closely linked to signal strength—they often go hand in hand, but are also impacted by other factors. The AP keeps a record of the link rates used when transmitting to and from each associated client. The ultimate aim for all wireless implementations is to ensure that the link rates are as high as possible for clients. A high link rate means that both the signal strength and the signal quality are good. Because it is possible to measure the upstream link rate directly, this is a great way to check if the client is suffering from RF issues.

The higher the link rates, the faster data is transferred, and the less air time is used for transmissions. This not only ensures high performance for the client, but also allows maximum opportunity for other clients to transmit as well, improving their overall performance. The link rates are calculated by the wireless chipset, based on signal strength, the SnR, and the retry and loss rate of frames. A client might have very good signal strength but a low link rate, which could indicate that the noise floor is higher than is optimal because the SnR is potentially quite small. This prevents the client from using the upper link rates regardless of how strong the signal is. The frame retry and loss rates will also cause a lower connection rate. If either the client or the AP radio is struggling to send frames, for example, there are a large number of collisions because of stations on neighboring APs, the radio can reduce its link rate to attempt to make transmissions more reliable.

Lower link rates may also indicate that the wireless client might be an older client and, as such, might support only older wireless standards where the link rates are a lot less. For maximum efficiency, it is often worthwhile to ensure you replace these older clients as soon as possible with newer-standard clients that support more efficient link rates. Finally, upstream link rates can be reduced when a client enters power save mode. Many handheld devices aggressively reduce links when they are not transmitting data because this can save significant amounts of battery power. However, this does make the client appear as if he is having a poor experience because the signal strength is often strong. Lower link rates are relevant in this scenario when you can see that the client is transmitting data. The radio should be trying to attain the highest link rates possible, and the fact that it isn't indicates that the client might have an RF issue.

Wireless Capacity—Channel Utilization

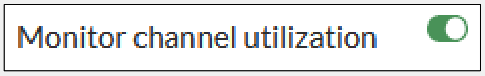
Channel utilization

- A percentage count of used airtime on the interface channel
  - Around each AP for all interfaces
- It measures all wireless traffic in the channel
  - Controllers own AP and station traffic
  - Any other traffic from any other APs or station in the locality
- The higher the channel utilization the less capacity there is

Possible causes

- Large number of station connections
- Poorly connected stations with low link rates
- High throughput applications
- High numbers of neighboring wireless networks on the same channel

Wi-Fi & Switch Controller > FortiAP Profiles



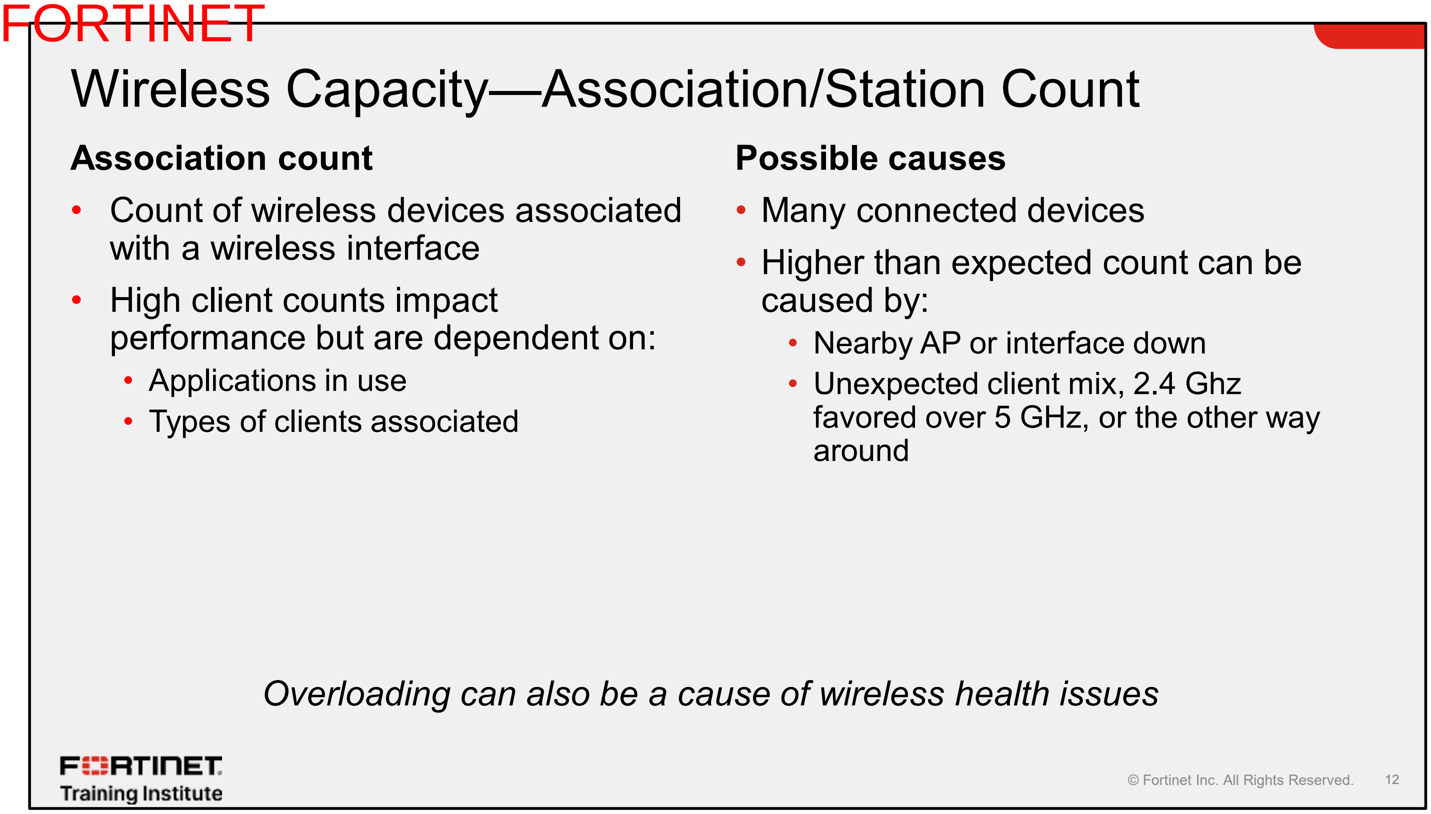
Monitor channel utilization ●

Channel utilization is a primary indicator of capacity.

Channel utilization is the primary indicator of capacity around an interface. When enabled, the AP is constantly monitoring the amount of wireless traffic it can decode in the channel, and providing a measure. It is not only accounting for traffic transmitted by its own clients, but it is also is accounting for other wireless traffic on the channel, which could be coming from neighboring APs and wireless clients not associated with your wireless network. The neighboring APs and wireless clients still use capacity, and your network cannot transmit data while those other transmissions are occurring.

The higher the channel utilization, which is measured in percent, the less the spare airtime that is available. Channel utilization is the most important indicator of wireless capacity.

High channel utilization is usually caused by a high number of station connections, but can also be caused by a smaller number of stations transmitting a large amount of traffic. It does not matter if the stations and APs are your own or if they are neighboring devices.



Wireless Capacity—Association/Station Count

Association count

- Count of wireless devices associated with a wireless interface
- High client counts impact performance but are dependent on:
    - Applications in use
    - Types of clients associated

Possible causes

- Many connected devices
- Higher than expected count can be caused by:
    - Nearby AP or interface down
    - Unexpected client mix, 2.4 Ghz favored over 5 GHz, or the other way around

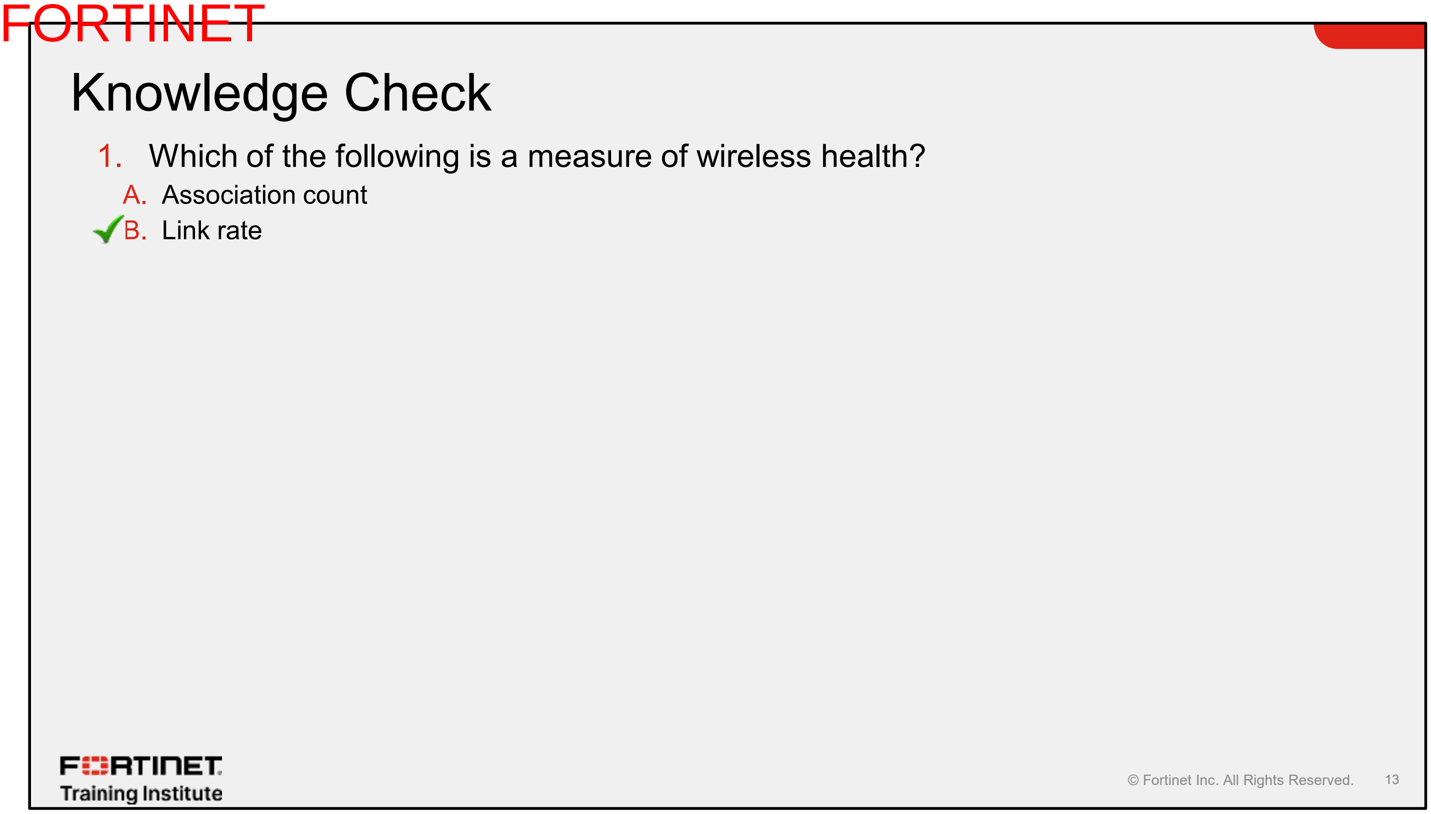
Overloading can also be a cause of wireless health issues

FORTINET Training Institute

12

Another critical metric for your wireless interface is the associated client count. Association count is a measure of the number of clients associated with each interface. A high client count will always affect performance, but the applications in use and the types of clients also matter.

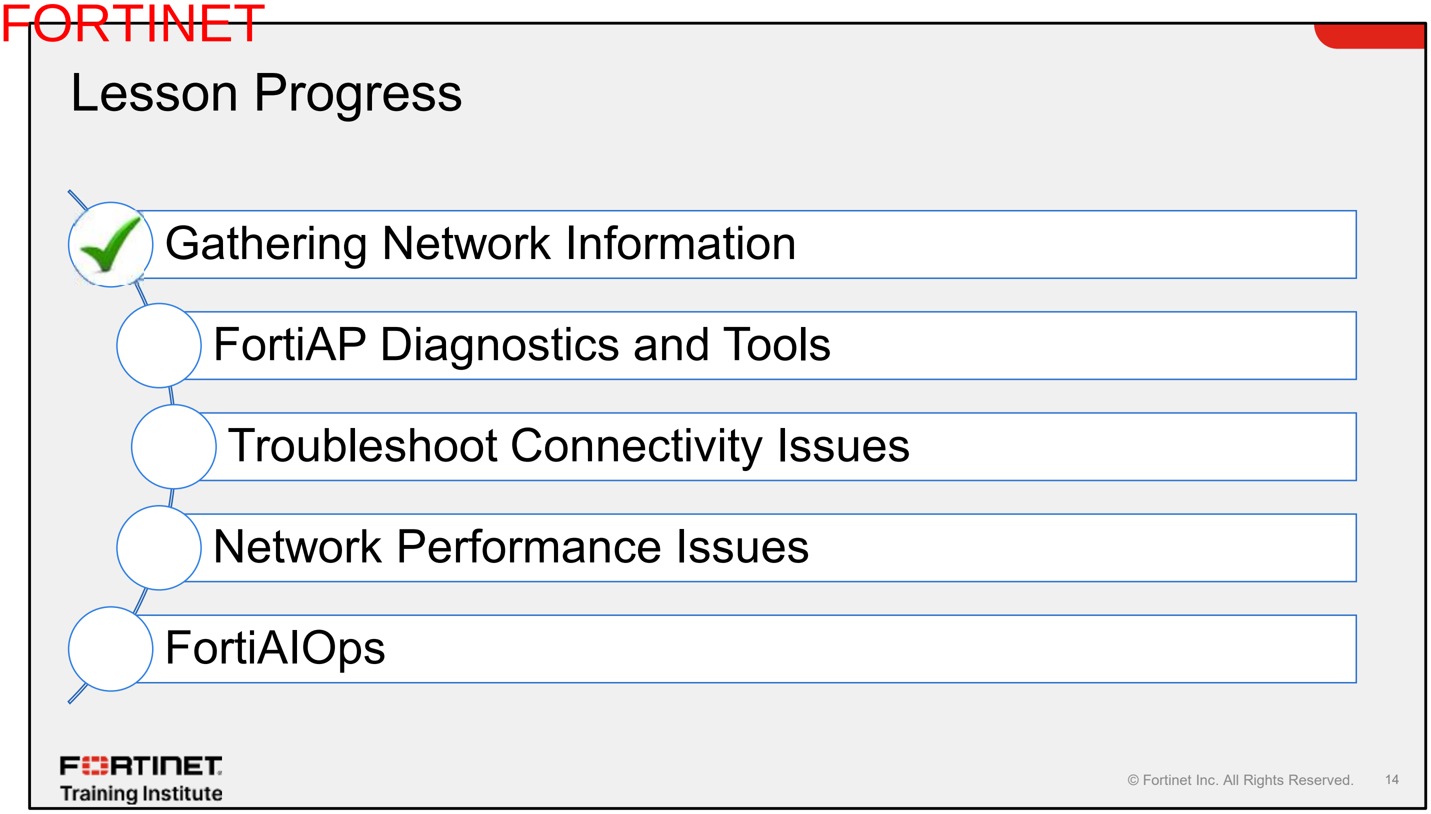
Many devices means many associations. A higher than expected count can be caused by a nearby AP that stops running, or an unexpected mix of clients that prefer one frequency range over another.



Knowledge Check

1. Which of the following is a measure of wireless health?
   - A. Association count
   - ✓B. Link rate

FORTINET
Training Institute



Lesson Progress

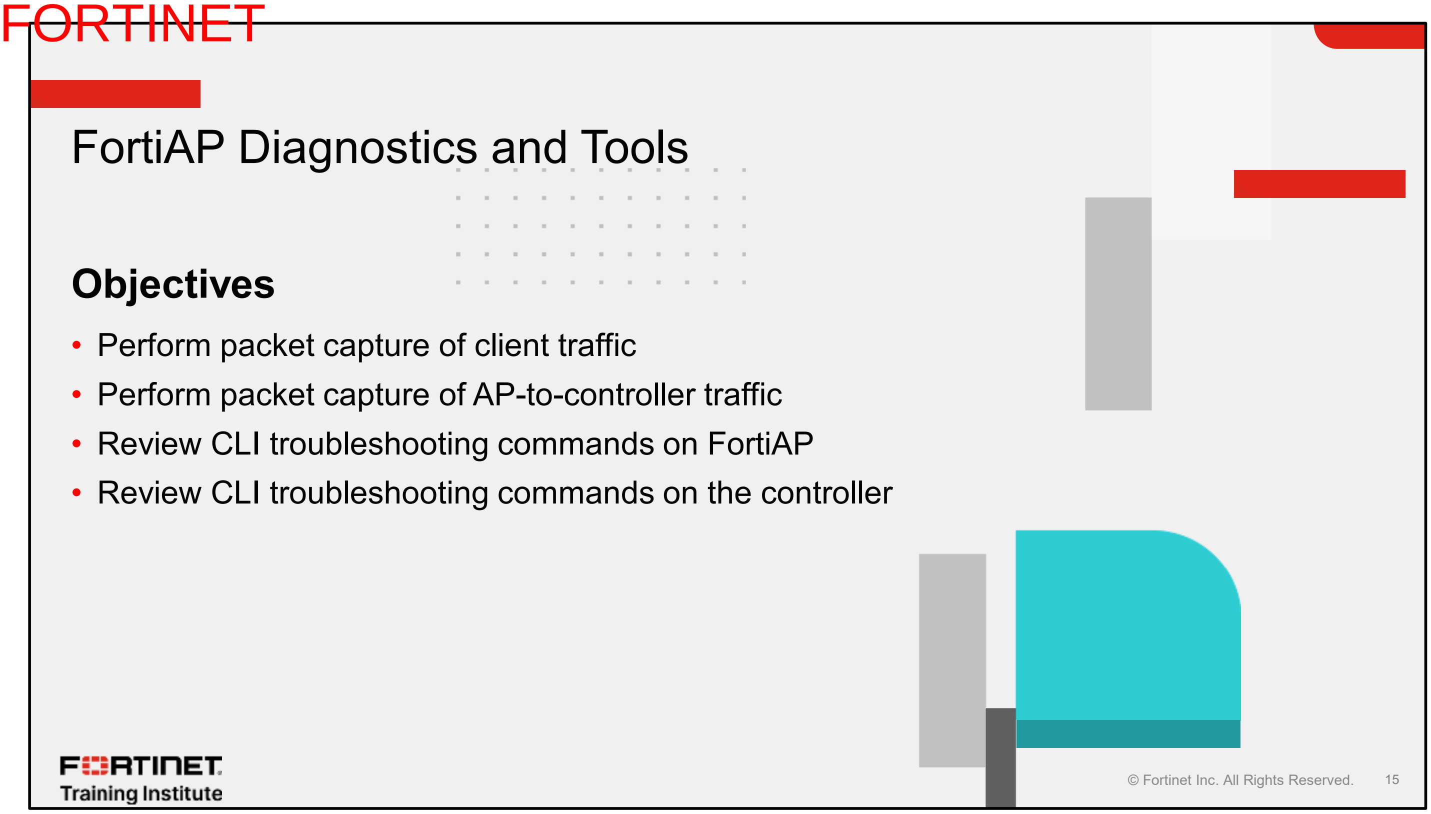
- ✓ Gathering Network Information
- ○ FortiAP Diagnostics and Tools
- ○ Troubleshoot Connectivity Issues
- ○ Network Performance Issues
- ○ FortiAIOps

FORTINET
Training Institute

14

Good job! You now understand how to gather useful information about your wireless network.

Now, you will learn about some of the more common wireless network issues you might come across.



FortiAP Diagnostics and Tools

Objectives

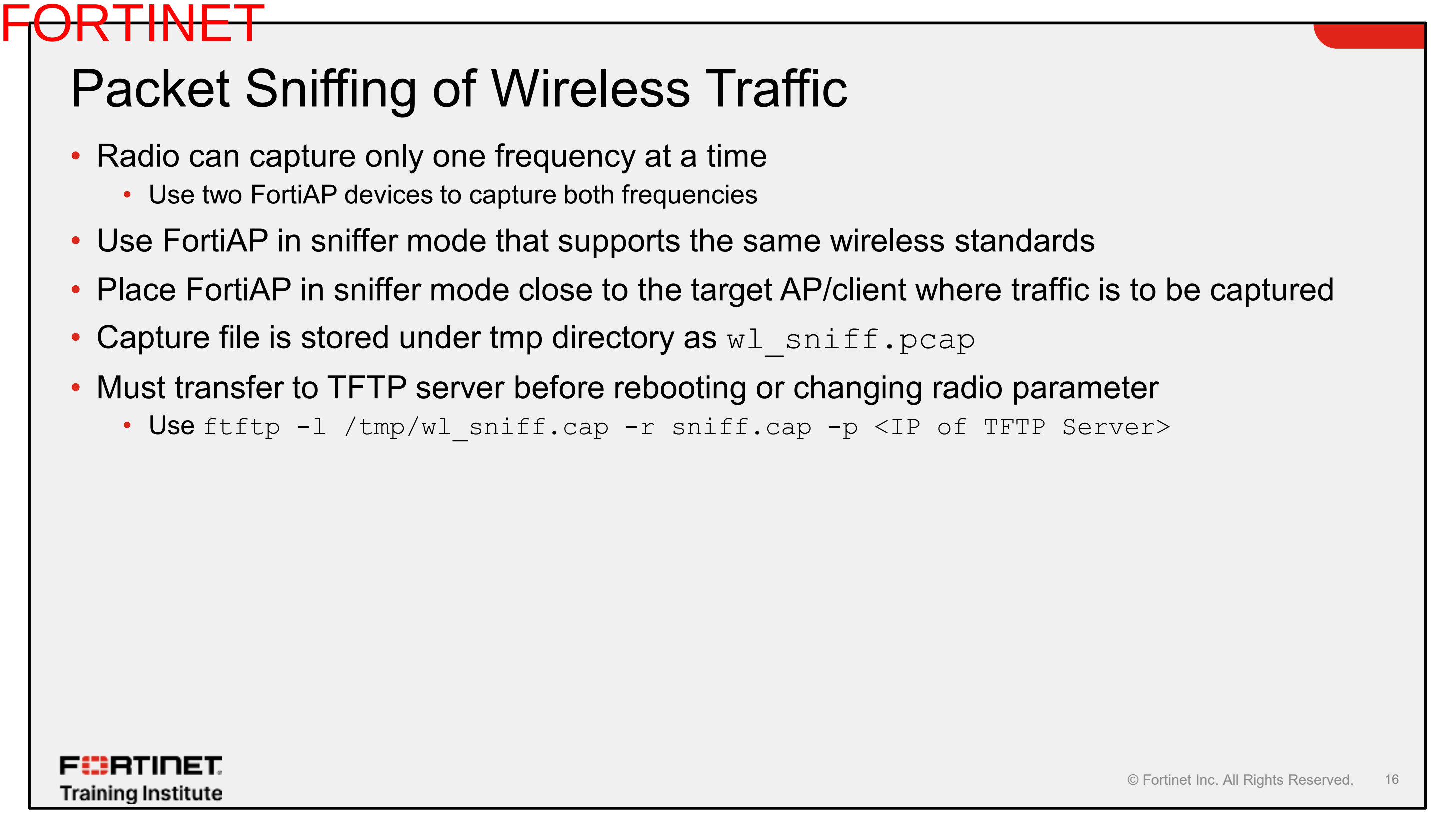
- Perform packet capture of client traffic
- Perform packet capture of AP-to-controller traffic
- Review CLI troubleshooting commands on FortiAP
- Review CLI troubleshooting commands on the controller

FORTINET Training Institute

15

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in advanced diagnostics, you will be able to use the packet capture of client and AP-to-controller traffic when escalating connectivity issues to support. You will also be able to use the available debugging tools to resolve issues.



Packet Sniffing of Wireless Traffic

- Radio can capture only one frequency at a time
  - Use two FortiAP devices to capture both frequencies
- Use FortiAP in sniffer mode that supports the same wireless standards
- Place FortiAP in sniffer mode close to the target AP/client where traffic is to be captured
- Capture file is stored under tmp directory as `wl_sniff.pcap`
- Must transfer to TFTP server before rebooting or changing radio parameter
  - Use `ftftp -l /tmp/wl_sniff.cap -r sniff.cap -p <IP of TFTP Server>`

FURTINET Training Institute

Packet captures are useful for troubleshooting all wireless client-related issues, because you can verify the data rate and 802.11 parameters, such as radio capabilities, and identify issues with wireless signal strength, interference, or congestion on the network.

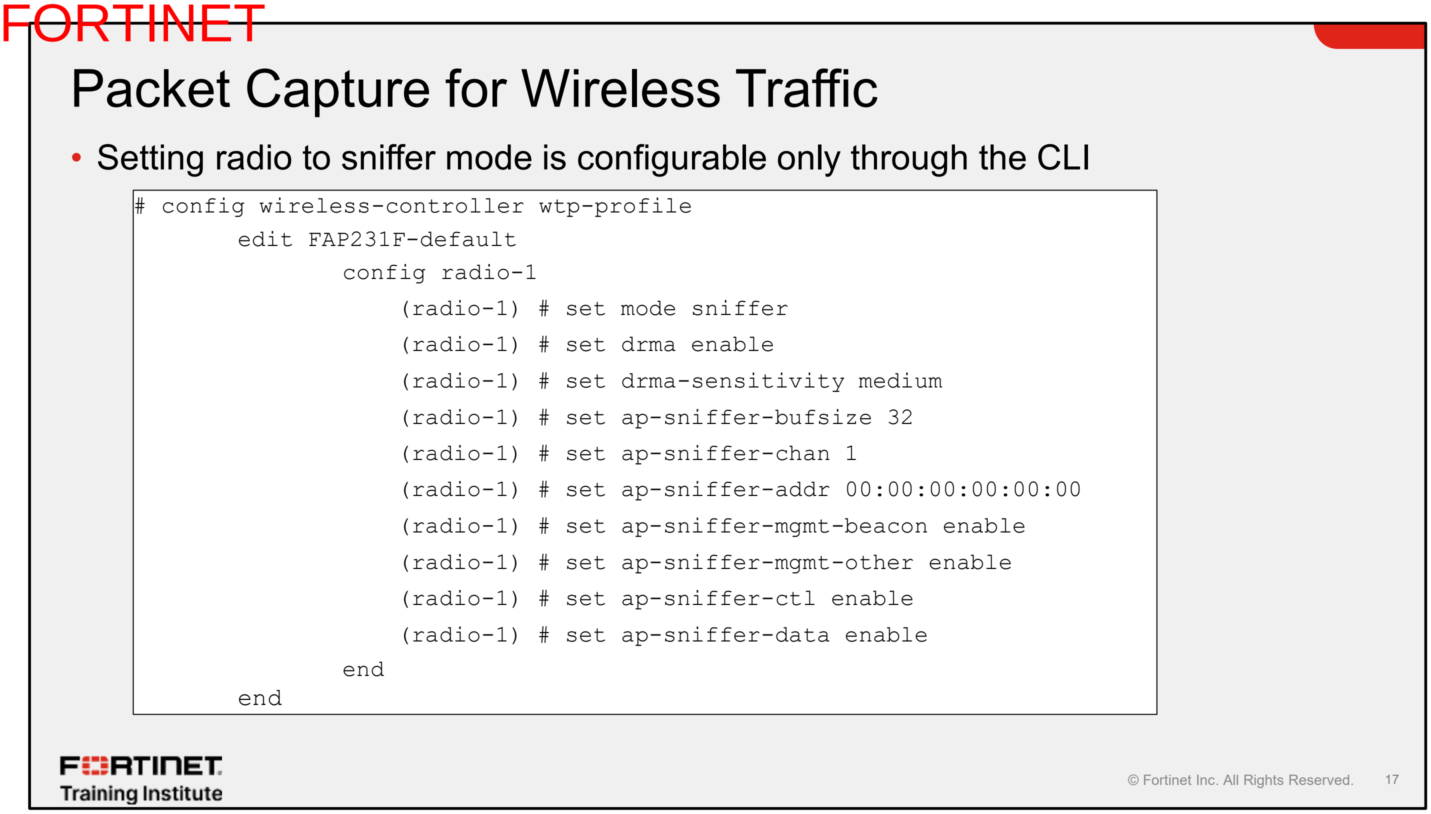
This technique consists of sniffing the wireless traffic directly on the air using FortiAP. Rather than using an existing AP in the network, which risks changing the network behavior or configuration, try using an additional AP as a dedicated sniffer AP.

To make a packet capture, you must set one of the radios to monitor mode. Remember that a radio can listen on only one frequency of traffic at a time. For example, on a FortiAP 222 device set the sniffer mode of radio 2 to capture 5 GHz band traffic, and radio 1 to capture 2.4 GHz band traffic.

If you need to capture both frequencies at the same time, use two FortiAP devices.

Try to use the same capture AP model as the AP for which packets are being captured (or at least one that supports the same wireless standards) and make sure you place it close to either the target AP or client. This ensures that all the traffic is captured.

The capture file is stored only temporarily. You must upload it to a TFTP server before rebooting or changing the radio settings. Do so by using the `ftftp` command on the AP CLI.



Packet Capture for Wireless Traffic

- Setting radio to sniffer mode is configurable only through the CLI

```
# config wireless-controller wtp-profile
      edit FAP231F-default
             config radio-1
                 (radio-1) # set mode sniffer
                 (radio-1) # set drma enable
                 (radio-1) # set drma-sensitivity medium
                 (radio-1) # set ap-sniffer-bufsize 32
                 (radio-1) # set ap-sniffer-chan 1
                 (radio-1) # set ap-sniffer-addr 00:00:00:00:00:00
                 (radio-1) # set ap-sniffer-mgmt-beacon enable
                 (radio-1) # set ap-sniffer-mgmt-other enable
                 (radio-1) # set ap-sniffer-ctl enable
                 (radio-1) # set ap-sniffer-data enable
             end
      end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

This slide shows how to set up the radio in sniffer mode. You can configure sniffer mode using the CLI only.

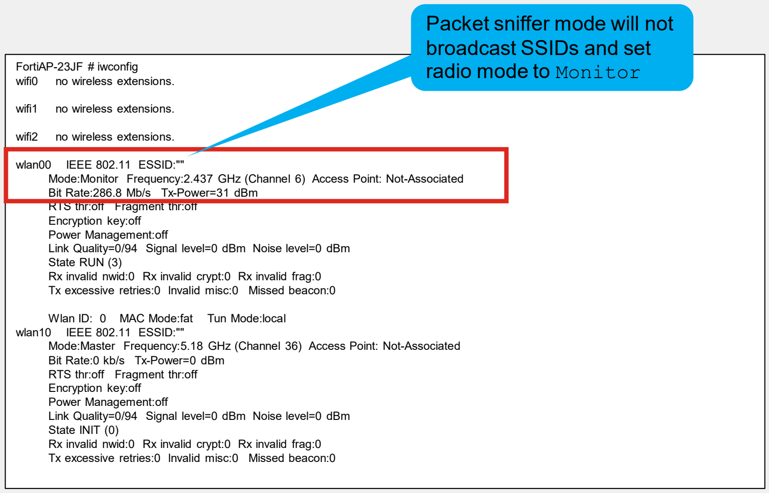
This slide shows an example of editing the FAP220B-default FortiAP profile. You might create a separate profile for a packet capture and assign an appropriate AP to that profile when a packet capture is required.

Note that you can determine the buffer size, which channel to sniff, and the AP MAC address. You can also sniff the beacons, probes, and control and data channels.

With a wildcard of `00:00:00:00:00:00` the AP decodes ALL traffic on that channel resulting in capturing a lot of traffic that might not be required.

Packet Sniffer for Wireless Traffic

- To verify the radio mode, on FortiAP CLI use `iwconfig` :



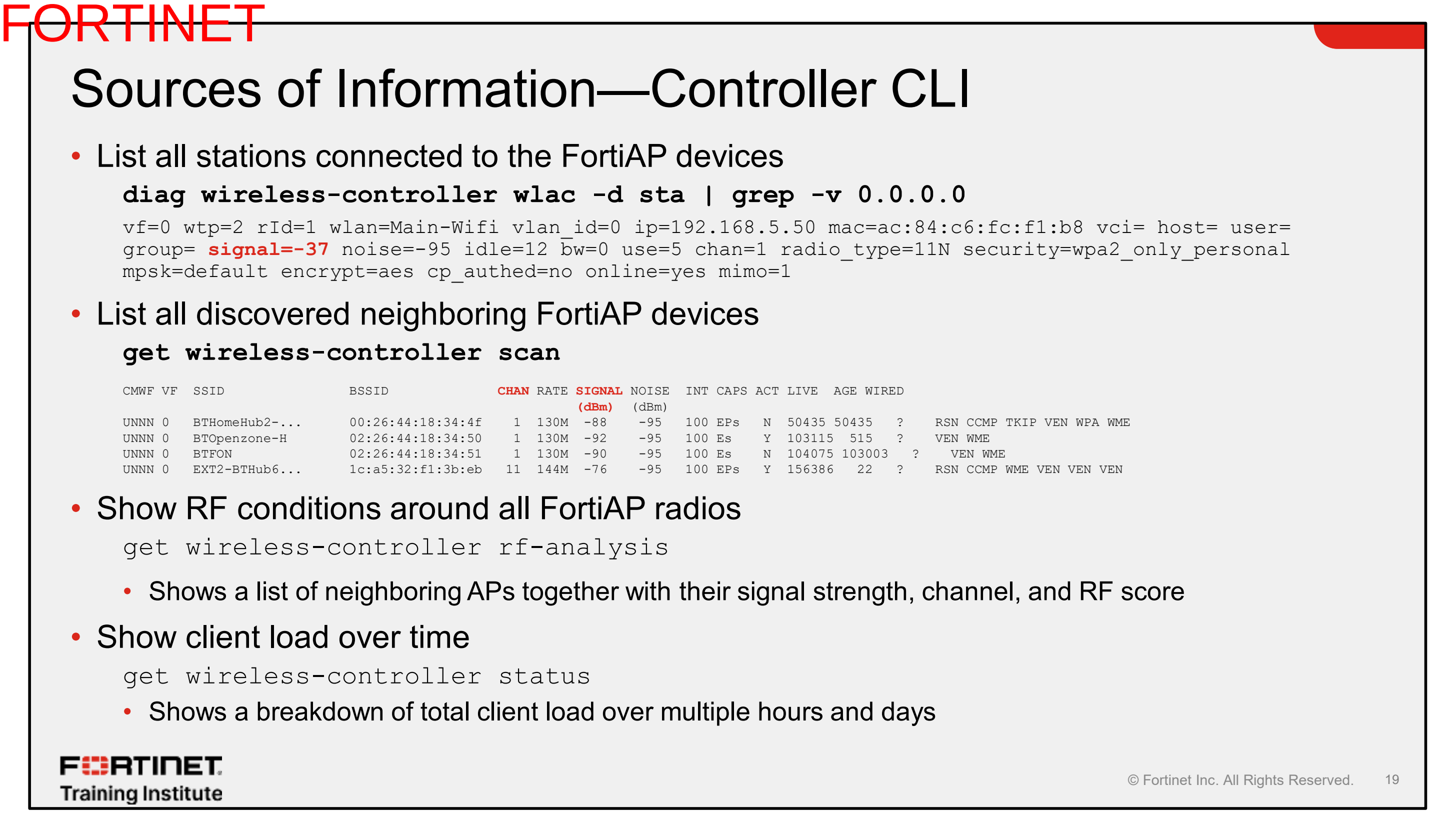
Packet sniffer mode will not broadcast SSIDs and set radio mode to `Monitor`

```
FortiAP-23JF # iwconfig
wifi0     no wireless extensions.

wifi1     no wireless extensions.

wifi2     no wireless extensions.

wlan00    IEEE 802.11  ESSID:""
          Mode:Monitor  Frequency:2.437 GHz (Channel 6)  Access Point: Not-Associated
          Bit Rate:286.8 Mb/s   Tx-Power=31 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=0 dBm  Noise level=0 dBm
          State RUN (3)
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

          Wlan ID:  0    MAC Mode:fat    Tun Mode:local
wlan10    IEEE 802.11  ESSID:""
          Mode:Master  Frequency:5.18 GHz (Channel 36)  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power=0 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=0 dBm  Noise level=0 dBm
          State INIT (0)
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Training Institute

18

This slide shows that the `wlan00` interface is in monitor mode, together with the freqency that is being captured.



Sources of Information—Controller CLI

- List all stations connected to the FortiAP devices

```
diag wireless-controller wlac -d sta | grep -v 0.0.0.0
vf=0 wtp=2 rId=1 wlan=Main-Wifi vlan_id=0 ip=192.168.5.50 mac=ac:84:c6:fc:f1:b8 vci= host= user=
group= signal=-37 noise=-95 idle=12 bw=0 use=5 chan=1 radio_type=11N security=wpa2_only_personal
mpsk=default encrypt=aes cp_authed=no online=yes mimo=1
```

- List all discovered neighboring FortiAP devices

```
get wireless-controller scan

CMWF VF  SSID               BSSID             CHAN RATE SIGNAL NOISE  INT CAPS ACT LIVE   AGE WIRED
                                                        (dBm)  (dBm)
UNNN 0   BTHomeHub2-...     00:26:44:18:34:4f   1  130M  -88    -95   100 EPs   N  50435 50435   ?    RSN CCMP TKIP VEN WPA WME
UNNN 0   BTOpenzone-H       02:26:44:18:34:50   1  130M  -92    -95   100 Es    Y  103115  515   ?    VEN WME
UNNN 0   BTFON              02:26:44:18:34:51   1  130M  -90    -95   100 Es    N  104075 103003   ?    VEN WME
UNNN 0   EXT2-BTHub6...     1c:a5:32:f1:3b:eb  11  144M  -76    -95   100 EPs   Y  156386   22   ?    RSN CCMP WME VEN VEN VEN
```

- Show RF conditions around all FortiAP radios

  `get wireless-controller rf-analysis`

  - Shows a list of neighboring APs together with their signal strength, channel, and RF score

- Show client load over time

  `get wireless-controller status`

  - Shows a breakdown of total client load over multiple hours and days

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

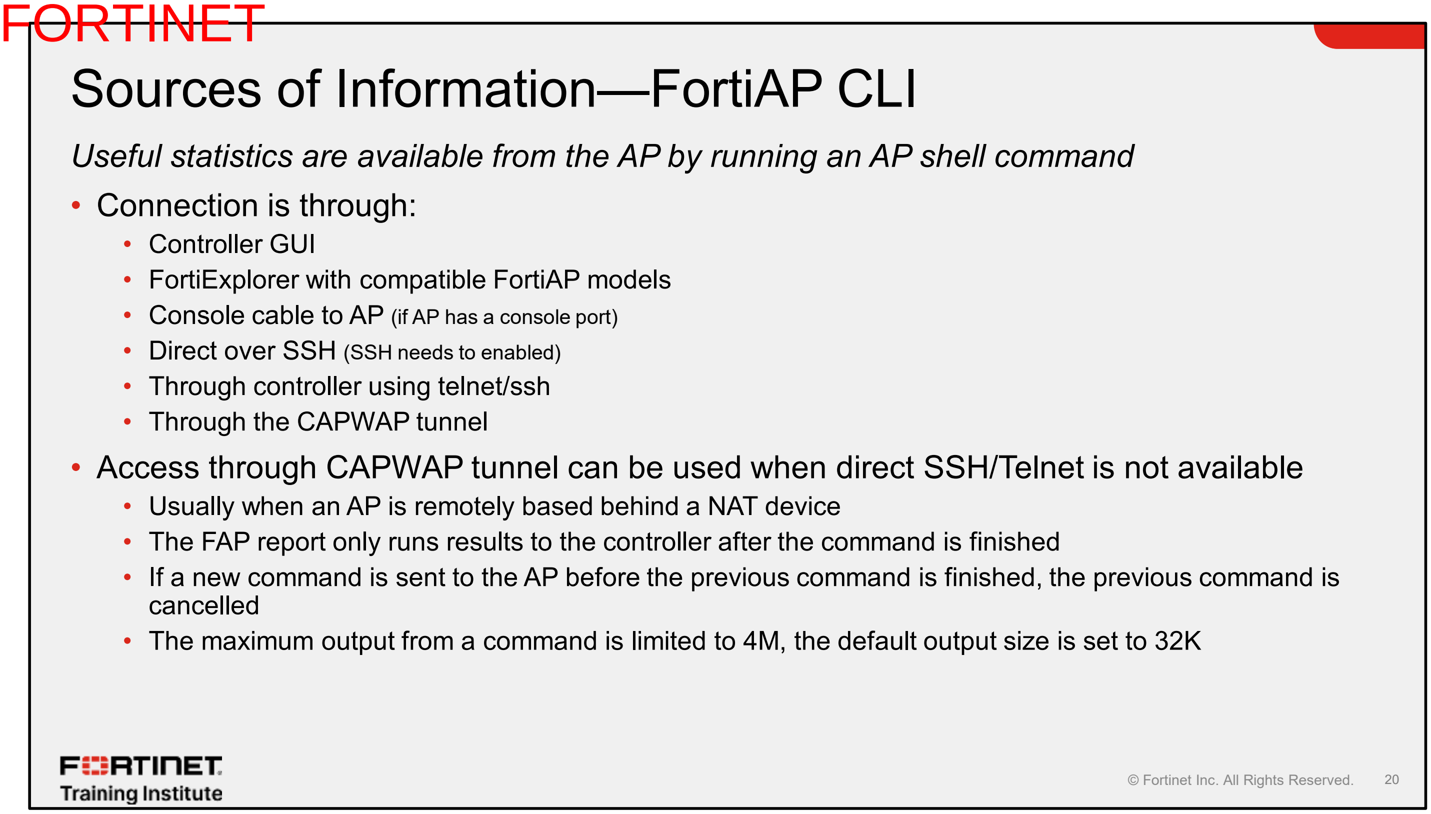
In addition to gathering information from the controller GUI, it is also possible to gather information from the controller CLI.

You can generate a list of connected stations and APs as you would see on the GUI.

You can get a better view of the RF status of all the APs by using the `get wireless-controller rf-analysis` command. Unlike the GUI, which lists only the top most interfered with, you can list all the interfaces.

Specify the wireless termination point (WTP) ID (AP serial number) to focus on one AP.

There is little historical information available from the GUI, so `get wireless-controller status` is a useful command for monitoring client load over time.



Sources of Information—FortiAP CLI

Useful statistics are available from the AP by running an AP shell command

- Connection is through:
  - Controller GUI
  - FortiExplorer with compatible FortiAP models
  - Console cable to AP (if AP has a console port)
  - Direct over SSH (SSH needs to enabled)
  - Through controller using telnet/ssh
  - Through the CAPWAP tunnel
- Access through CAPWAP tunnel can be used when direct SSH/Telnet is not available
  - Usually when an AP is remotely based behind a NAT device
  - The FAP report only runs results to the controller after the command is finished
  - If a new command is sent to the AP before the previous command is finished, the previous command is cancelled
  - The maximum output from a command is limited to 4M, the default output size is set to 32K

FORTINET Training Institute

20

The AP CLI can provide specific information about AP and client connectivity.

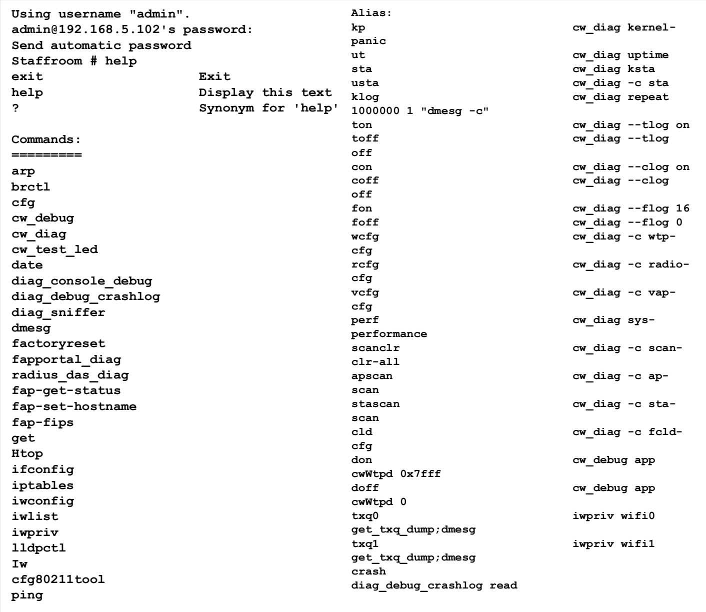
You can access the AP through the following:

- Controller GUI
- FortiExplorer with FortiAP G models and later
- Console cable to AP (if AP has a console port)
- Direct over SSH (SSH needs to enabled and password known)
- Through controller using telnet/SSH
- Through the CAPWAP tunnel

Connecting through the CAPWAP tunnel is really useful when an AP is remotely based and cannot be reached by any other method.

Sources of Information—FortiAP CLI (Contd)

- To connect using the controller GUI
  - **WiFi & Switch Controller** > **Managed FortiAPs**
  - Right-click the row of the FortiAP that you want to connect to and then select **Connect to CLI**
- Help or ? to display list of commands
- Some commands are aliased
- Each AP has a set of configuration and diagnostic commands available
  - `cw_diag` commands are used or monitoring/diagnostics
  - To increase timeout:
  - `cfg -a ADMIN_TIMEOUT=`*`mins`*
  - `cfg -c`



```
Using username "admin".
admin@192.168.5.102's password:
Send automatic password
Staffroom # help
exit                    Exit
help                    Display this text
?                       Synonym for 'help'

Commands:
=========
arp
brctl
cfg
cw_debug
cw_diag
cw_test_led
date
diag_console_debug
diag_debug_crashlog
diag_sniffer
dmesg
factoryreset
fapportal_diag
radius_das_diag
fap-get-status
fap-set-hostname
fap-fips
get
Htop
ifconfig
iptables
iwconfig
iwlist
iwpriv
lldpctl
Iw
cfg80211tool
ping
```

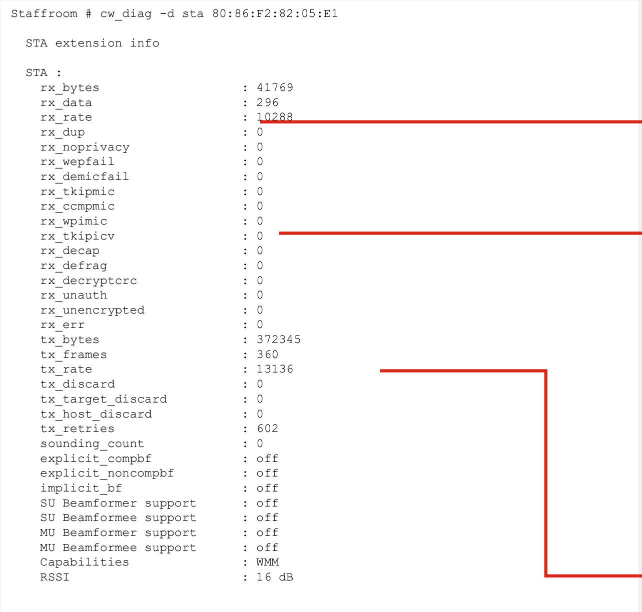
```
Alias:
kp                              cw_diag kernel-
panic
ut                              cw_diag uptime
sta                             cw_diag ksta
usta                            cw_diag -c sta
klog                            cw_diag repeat
1000000 1 "dmesg -c"
ton                             cw_diag --tlog on
toff                            cw_diag --tlog
off
con                             cw_diag --clog on
coff                            cw_diag --clog
off
fon                             cw_diag --flog 16
foff                            cw_diag --flog 0
wcfg                            cw_diag -c wtp-
cfg
rcfg                            cw_diag -c radio-
cfg
vcfg                            cw_diag -c vap-
cfg
perf                            cw_diag sys-
performance
scanclr                         cw_diag -c scan-
clr-all
apscan                          cw_diag -c ap-
scan
stascan                         cw_diag -c sta-
scan
cld                             cw_diag -c fcld-
cfg
don                             cw_debug app
cwWtpd 0x7fff
doff                            cw_debug app
cwWtpd 0
txq0                            iwpriv wifi0
get_txq_dump;dmesg
txq1                            iwpriv wifi1
get_txq_dump;dmesg
crash
diag_debug_crashlog read
```

The easiest way to obtain information about an AP is to highlight it in the **Managed FortiAP** table and then use the **Connect to CLI** option. However, it is possible to connect directly to the AP if it has a console port, or by one of the other methods listed on this slide.

As with other FortiGate CLI commands, context-sensitive help is available.

By default, the CLI times out in 5 minutes, which can be an issue if you are trying to troubleshoot. You can extend the timeout period by using the `cfg` command.

Sources of Information—Useful AP CLI Commands



```
Staffroom # cw_diag -d sta 80:86:F2:82:05:E1

  STA extension info

  STA :
    rx_bytes                    : 41769
    rx_data                     : 296
    rx_rate                     : 10288
    rx_dup                      : 0
    rx_noprivacy                : 0
    rx_wepfail                  : 0
    rx_demicfail                : 0
    rx_tkipmic                  : 0
    rx_ccmpmic                  : 0
    rx_wpimic                   : 0
    rx_tkipicv                  : 0
    rx_decap                    : 0
    rx_defrag                   : 0
    rx_decryptcrc               : 0
    rx_unauth                   : 0
    rx_unencrypted              : 0
    rx_err                      : 0
    tx_bytes                    : 372345
    tx_frames                   : 360
    tx_rate                     : 13136
    tx_discard                  : 0
    tx_target_discard           : 0
    tx_host_discard             : 0
    tx_retries                  : 602
    sounding_count              : 0
    explicit_compbf             : off
    explicit_noncompbf          : off
    implicit_bf                 : off
    SU Beamformer support       : off
    SU Beamformee support       : off
    MU Beamformer support       : off
    MU Beamformee support       : off
    Capabilities                : WMM
    RSSI                        : 16 dB
```

For station-specific layer 1 metrics

`cw_diag -d sta` *`mac-address`*

- Lost frames
  - Show the AP was unable to successfully send a data frame after numerous retries
- Retry frames
  - Frames can be retransmitted multiple times, sometimes the number of retry frames can exceed the tx_frames count
- Lists signal to noise

FORTINET Training Institute

22

For specific stations, it is possible to list more detailed RF information by using the `cw_diag -d sta` command for the MAC address of a specific station.

This can reveal the frames that were lost when the AP failed to send them to a client, together with frames that were retried.

It is not unusual to see a very low number of loss frames (in relation to the TX frame count), but an increasingly large number show that the AP was unable to successfully send a data frame after numerous retries. This can indicate that the station is unable to clearly receive or decode frames from the AP with the result that it is not sending an acknowledgement frame. This can indicate poor signal strength at the client, or a high noise floor.

Retry frames are not unusual. Retries are part of normal wireless LAN network operation, but again, a high number indicates an issue.

Sources of Information—Useful AP CLI Commands

- Show the last minute of channel utilization for the AP configured channel

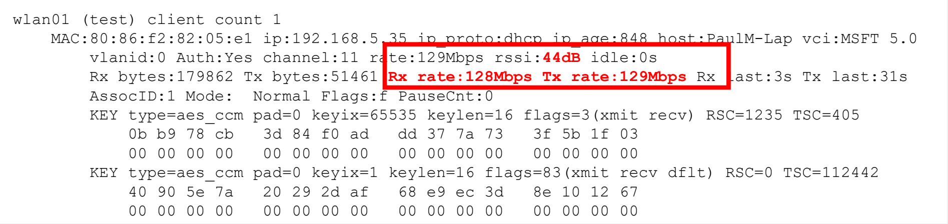
  `cw_diag -c his-chutil`

- Show channel utilization for all allowed channels at the AP

  `cw_diag -c all-chutil`

- Show associated stations

  `cw_diag ksta` (or aliased to `sta`)



```
wlan01 (test) client count 1
    MAC:80:86:f2:82:05:e1 ip:192.168.5.35 ip_proto:dhcp ip_age:848 host:PaulM-Lap vci:MSFT 5.0
        vlanid:0 Auth:Yes channel:11 rate:129Mbps rssi:44dB idle:0s
        Rx bytes:179862 Tx bytes:51461 Rx rate:128Mbps Tx rate:129Mbps Rx last:3s Tx last:31s
        AssocID:1 Mode:  Normal Flags:f PauseCnt:0
        KEY type=aes_ccm pad=0 keyix=65535 keylen=16 flags=3(xmit recv) RSC=1235 TSC=405
            0b b9 78 cb   3d 84 f0 ad   dd 37 7a 73   3f 5b 1f 03
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
        KEY type=aes_ccm pad=0 keyix=1 keylen=16 flags=83(xmit recv dflt) RSC=0 TSC=112442
            40 90 5e 7a   20 29 2d af   68 e9 ec 3d   8e 10 12 67
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
```

  - Both upstream and downstream link rates listed together with single-to-noise ratio (SNR)

FORTINET Training Institute

23

The `cw_diag -c his-chutel` command provides a short history of AP channel utilization for the AP radios. So, rather than taking a one-time measurement, which could be a peak, you can see a plot of the channel utilization for 1 minute.

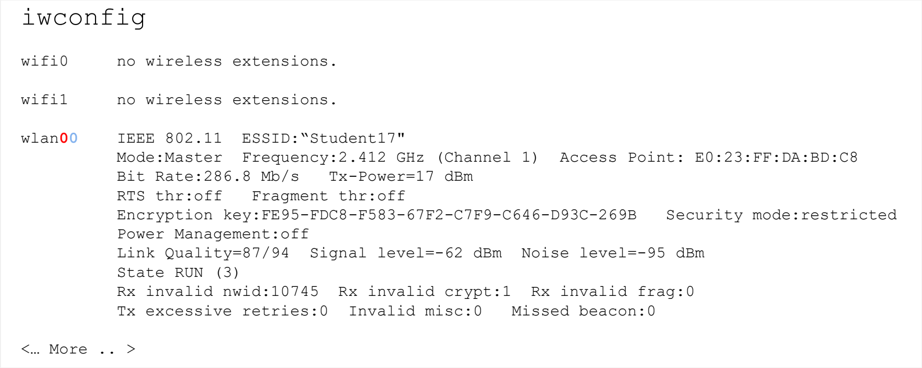
`cw_diag ksta` is an aliased command. The key information that is not available anywhere else is the downstream (AP-to-client) **AND** upstream link rate. Both are great measures of connection quality, but you must understand the range of connection rates the AP and clients are capable of.

For instance, handheld clients will likely have only a single- or dual-stream radio and, as such, would never achieve the same link rates as an Apple MacBook Pro. Review the specifications of the client indicates the maximum rate it is capable of. Reviewing its connection using the `cw_diag ksta` command shows how close it is to the maximum connection speed.

Note that many devices save battery power by reducing the link rate when the connection is idle. Often, to get a good representation of the link rates, some data must be transmitted and received.

Sources of Information—Useful AP CLI Commands

- Display radio interfaces on an AP:



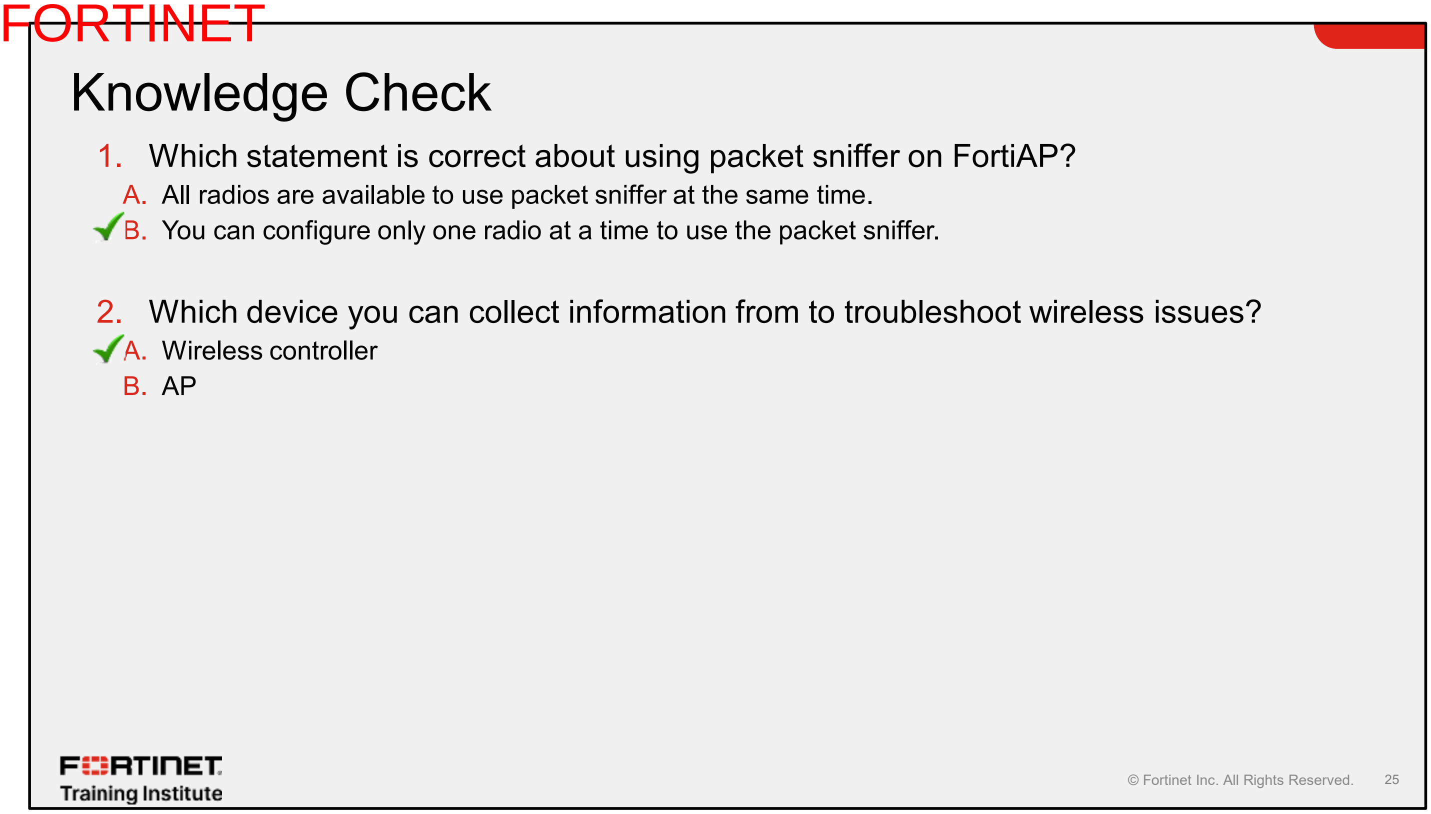
```
iwconfig

wifi0     no wireless extensions.

wifi1     no wireless extensions.

wlan00    IEEE 802.11  ESSID:“Student17"
          Mode:Master  Frequency:2.412 GHz (Channel 1)  Access Point: E0:23:FF:DA:BD:C8
          Bit Rate:286.8 Mb/s   Tx-Power=17 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:FE95-FDC8-F583-67F2-C7F9-C646-D93C-269B   Security mode:restricted
          Power Management:off
          Link Quality=87/94  Signal level=-62 dBm  Noise level=-95 dBm
          State RUN (3)
          Rx invalid nwid:10745  Rx invalid crypt:1  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

<… More .. >
```

- All SSIDs are in the form of `wlan XY`
  - Where **X** is 0 for 2.4 GHz, 1 for 5 GHz, and 2 for 6 GHz
  - Where **Y** is increased by function of the SSIDs
- To see statistics on a single interface : `cw_diag stats` *`wlanXY`*

FORTINET
Training Institute

24

You can display more detailed interface information using the `Iwconfig` command.



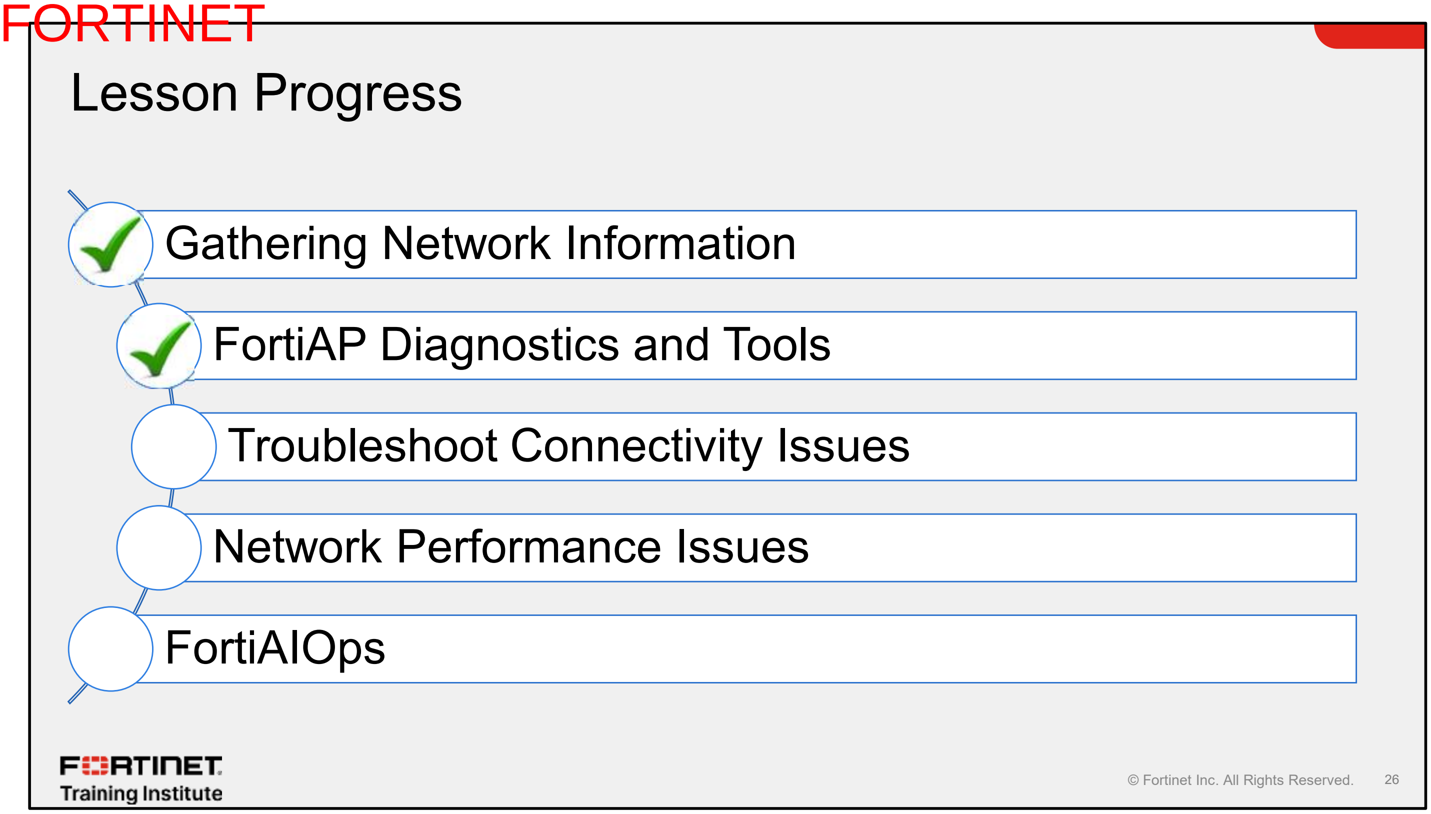
Knowledge Check

1. Which statement is correct about using packet sniffer on FortiAP?
   - A. All radios are available to use packet sniffer at the same time.
   - ✓ B. You can configure only one radio at a time to use the packet sniffer.

2. Which device you can collect information from to troubleshoot wireless issues?
   - ✓ A. Wireless controller
   - B. AP

FORTINET Training Institute

25



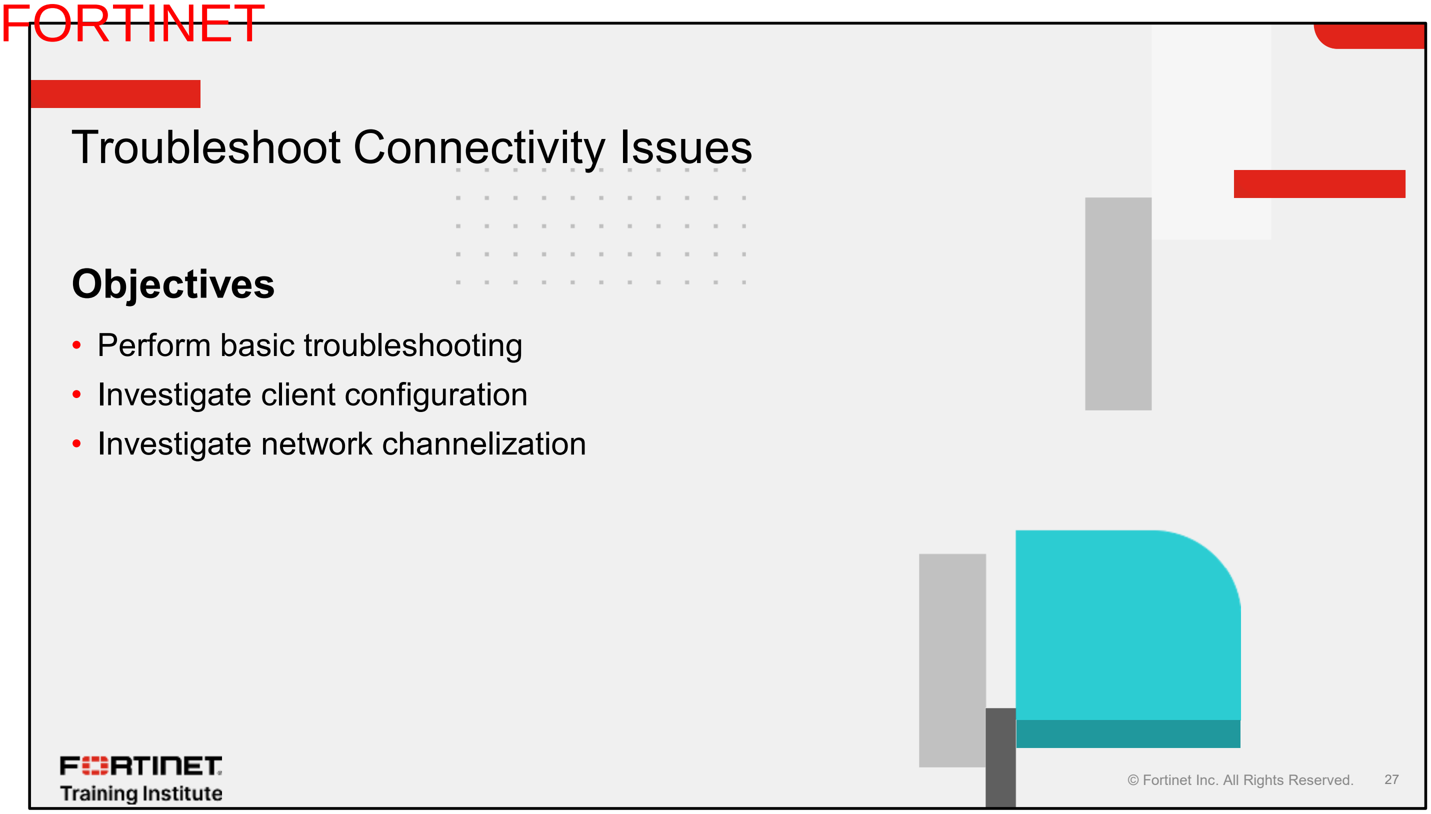
Lesson Progress

- ✓ Gathering Network Information
- ✓ FortiAP Diagnostics and Tools
- ○ Troubleshoot Connectivity Issues
- ○ Network Performance Issues
- ○ FortiAIOps

FORTINET
Training Institute

Good job! You now understand advanced diagnostics.

Now, you will learn about network connectivity issues.



Troubleshoot Connectivity Issues

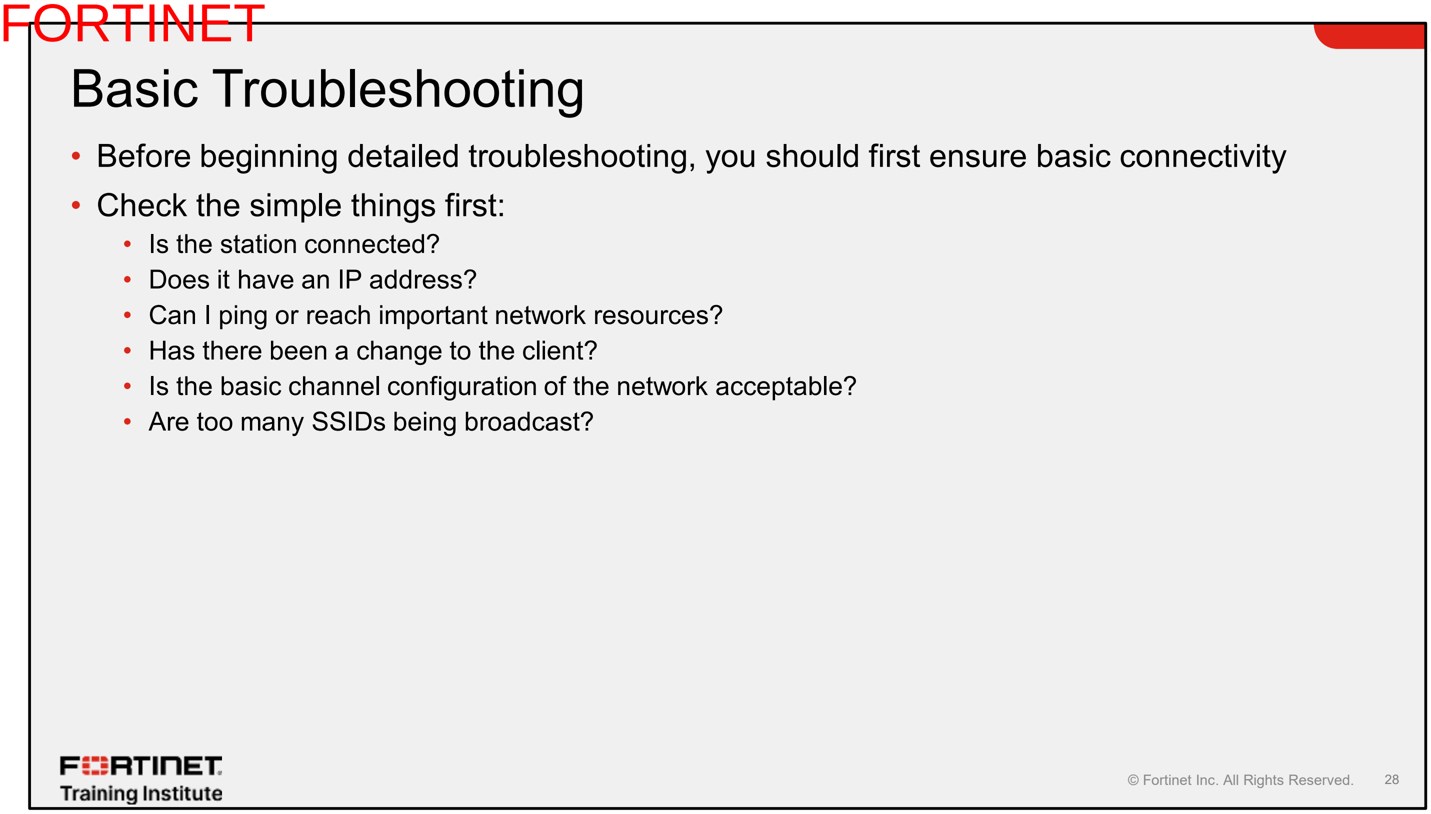
Objectives

- Perform basic troubleshooting
- Investigate client configuration
- Investigate network channelization

27

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in investigating common network issues, you will be able to perform basic troubleshooting and configuration checks on the network.



Basic Troubleshooting

- Before beginning detailed troubleshooting, you should first ensure basic connectivity
- Check the simple things first:
  - Is the station connected?
  - Does it have an IP address?
  - Can I ping or reach important network resources?
  - Has there been a change to the client?
  - Is the basic channel configuration of the network acceptable?
  - Are too many SSIDs being broadcast?

28

Before beginning detailed troubleshooting, you should first ensure that there is basic connectivity.

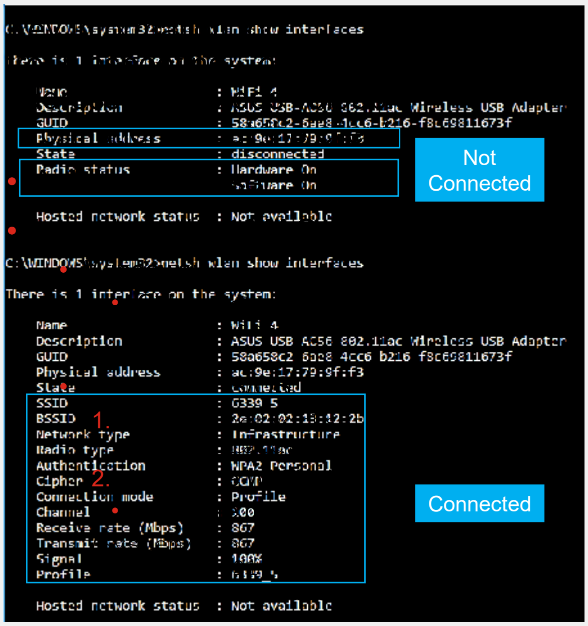
It can be easy to assume that there is a complex issue with the network. Check the basics first as they can save a lot of time.

Locating the Client MAC and IP Addresses

Key information for troubleshooting—obtaining (or not) provides valuable information about the client

- Ask the end user
- Locating client MAC address:
  - Windows:
    - CLI: `netsh wlan show interfaces`
  - Apple Mac OS/OS X:
    1. Terminal: `networksetup -listallhardwareports`
    2. Locate the Wi-Fi adaptor
       - For more detailed information:

       `/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport-I`



```
C:\WINDOWS\system32>netsh wlan show interfaces

There is 1 interface on the system:

    Name                   : WiFi 4
    Description            : ASUS USB-AC56 802.11ac Wireless USB Adapter
    GUID                   : 58a658c2-6ae8-4cc6-b216-f8c69811673f
    Physical address       : ac:9e:17:79:9f:f3
    State                  : disconnected
    Radio status           : Hardware On
                             Software On

    Hosted network status  : Not available


C:\WINDOWS\system32>netsh wlan show interfaces

There is 1 interface on the system:

    Name                   : WiFi 4
    Description            : ASUS USB AC56 802.11ac Wireless USB Adapter
    GUID                   : 58a658c2 6ae8 4cc6 b216 f8c69811673f
    Physical address       : ac:9e:17:79:9f:f3
    State                  : connected
    SSID                   : G339 5
    BSSID                  : 2e:02:02:13:12:2b
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2 Personal
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 100
    Receive rate (Mbps)    : 867
    Transmit rate (Mbps)   : 867
    Signal                 : 100%
    Profile                : G339_5

    Hosted network status  : Not available
```

To troubleshoot an issue with a wireless client, you must have its MAC address and optionally, its IP address.

Normally you can find these details using the controller or AP interface, but if you are troubleshooting a no-connection issue, the controller or AP will not have them. If this is the case, you must locate it manually. In some networks, it's possible to analyze DHCP or DNS to find the client MAC address. Other networks might have security appliances that make a record of the MAC address. Often, the easiest way to find out the MAC address is by looking on the client device.

Different client operating systems have different ways of revealing the wireless card MAC address. On Windows, you can use the GUI, but in later versions it can be easier to use the CLI and enter the NetShell (`netsh`) command. This command produces a simplified output—MAC addresses are easy to find, as well as the status of the radio. Later versions of Windows can identify whether the radio is turned on or turned off by software or hardware. This can be useful for making sure the end user has turned on the wireless switch on a laptop that can't connect to the network. Many laptops have hardware switches to enable or disable wireless connectivity. One of the most common reasons that a laptop can't connect to the wireless network is because that switch is turned off.

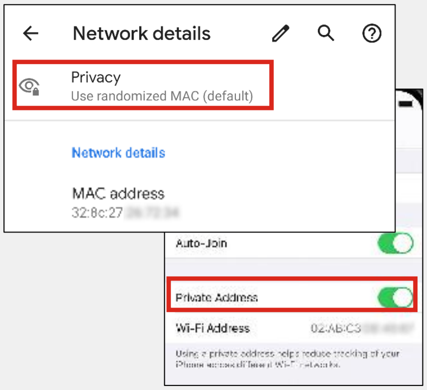
`netsh` reveals different information depending on whether the client is connected or not, including the channel connected. You can see the channel that is in use, an estimate of the receive and transmit rates, and the percent signal strength.

These measures can vary in accuracy, depending on the quality of the driver, and you should use them cautiously.

Other operating systems use other methods. macOS has a similar CLI option.

Locating a Client MAC and IP Address (Contd)

- Locating client MAC address on mobile:
  - Android:
    1. In the **App Drawer: Settings** > **About Phone** > **Status**
    2. Locate the Wi-Fi MAC address
  - Apple iOS:
    1. On the Home screen **Settings** > **General** > **About**
    2. Scroll down to **Wi-Fi Address**
- MAC address privacy enabled by default:
  - Android: Randomized MAC address
    - Privacy setting can be changed in the SSID network details
  - Apple iOS: Private Address
    - Each Wi-Fi network profile has the option to disable **Private Address**



Network details

Privacy
Use randomized MAC (default)

Network details

MAC address
32:8c:27 [redacted]

Auto-Join

Private Address

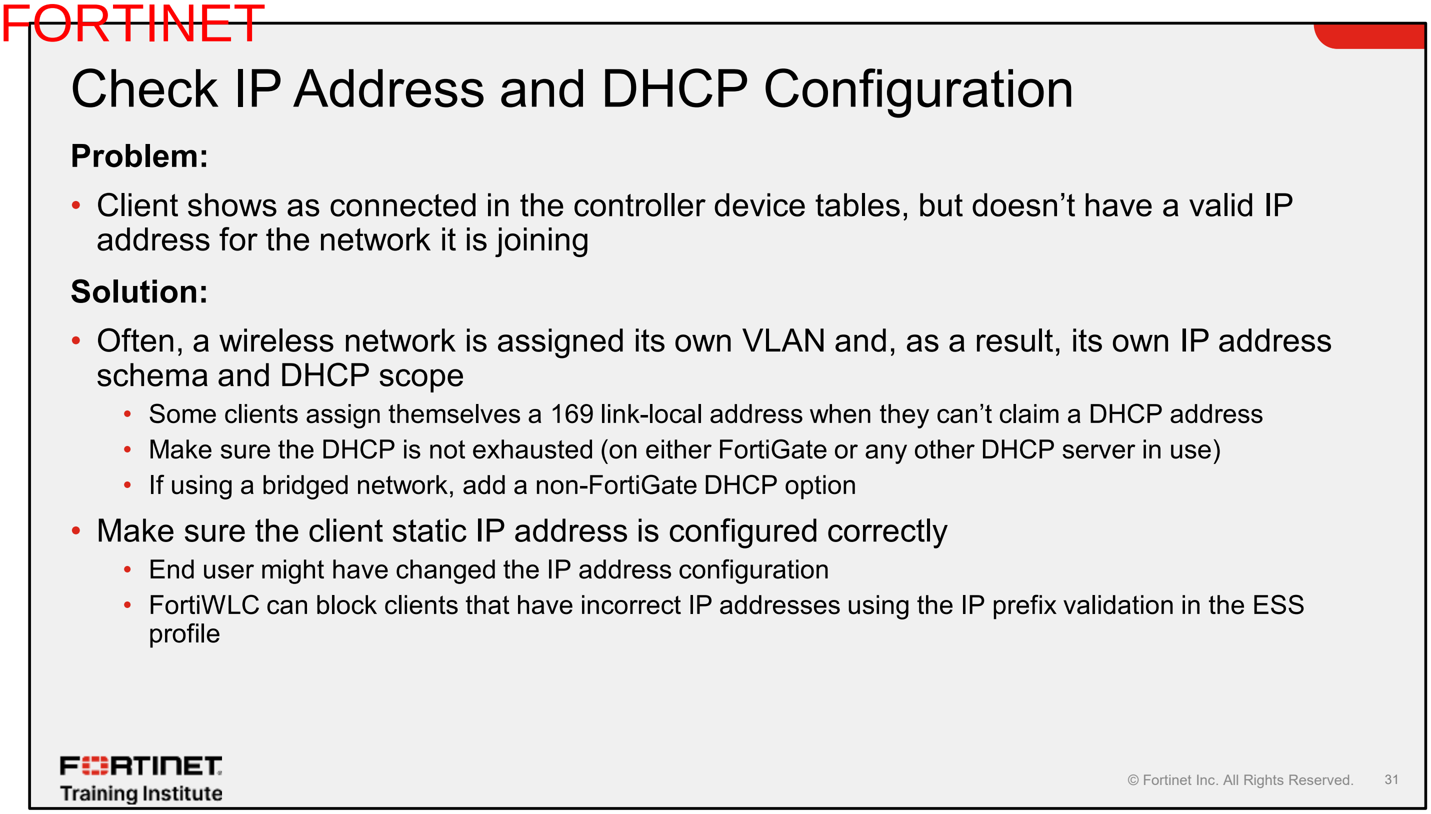
Wi-Fi Address 02:AB:C3 [redacted]

Using a private address helps reduce tracking of your iPhone across different Wi-Fi networks.

FORTINET Training Institute

30

For Android and other mobile OSs, you can locate the MAC address in the phone settings. However, in recent mobile OS updates, you can set a virtual MAC address when connected to a new wireless network SSID. This address could be different than the MAC hardware address found in the mobile settings. The virtual MAC address is enabled by default, but can be disabled in the network details of each SSID.



Check IP Address and DHCP Configuration

Problem:

- Client shows as connected in the controller device tables, but doesn't have a valid IP address for the network it is joining

Solution:

- Often, a wireless network is assigned its own VLAN and, as a result, its own IP address schema and DHCP scope
  - Some clients assign themselves a 169 link-local address when they can't claim a DHCP address
  - Make sure the DHCP is not exhausted (on either FortiGate or any other DHCP server in use)
  - If using a bridged network, add a non-FortiGate DHCP option
- Make sure the client static IP address is configured correctly
  - End user might have changed the IP address configuration
  - FortiWLC can block clients that have incorrect IP addresses using the IP prefix validation in the ESS profile

FORTINET Training Institute

31

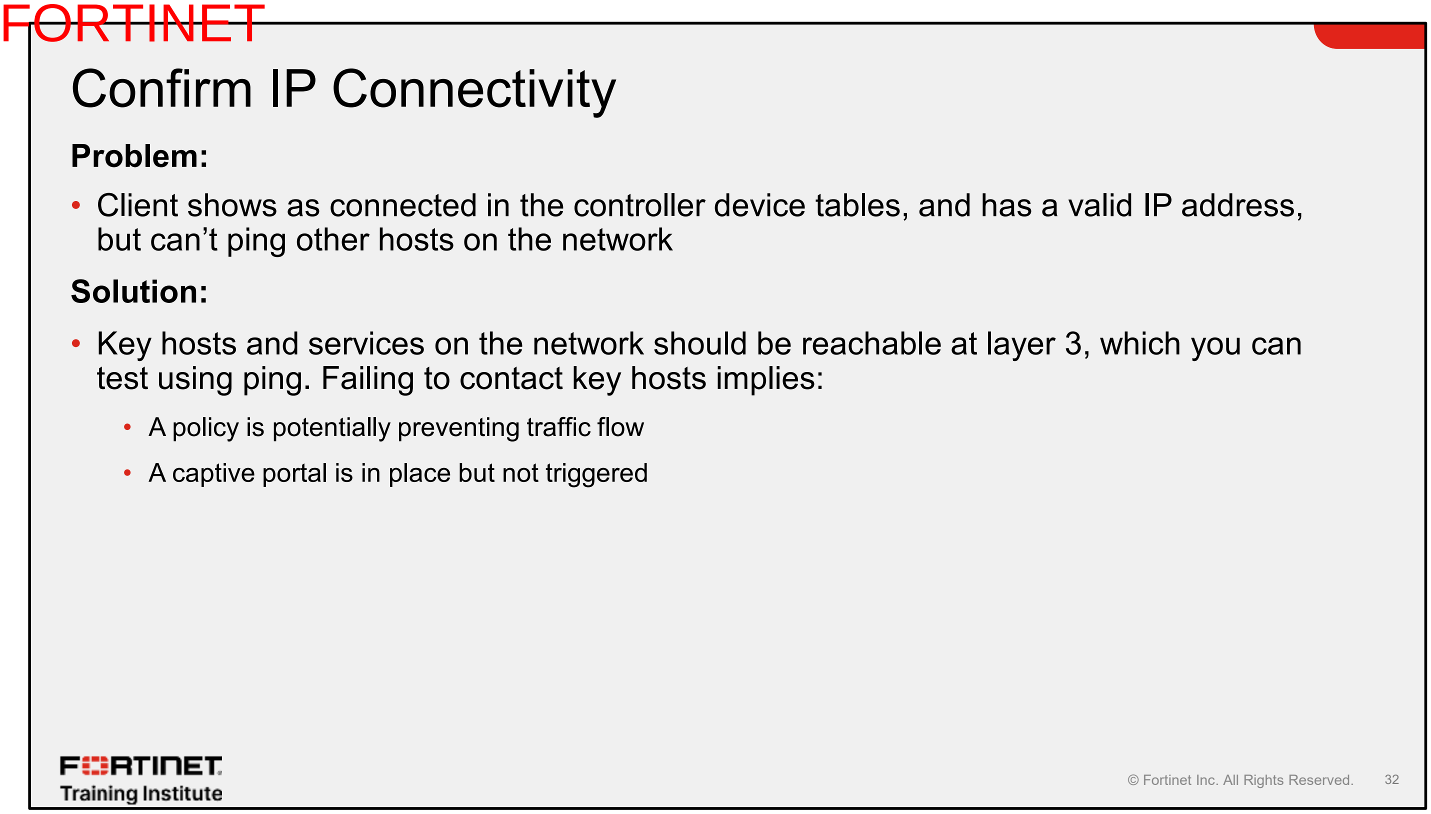
If the controller's device tables show the client is connected but doesn't show a valid IP address for the network the client is joining, this can indicate a problem with the underlying DHCP infrastructure.

Depending on the type of client, you might not see an IP address or a 169 link-local address in the device tables, which indicates that the client couldn't obtain a DHCP IP address. One of the most common causes of this problem is DHCP scope exhaustion. Often, when a wireless network is first implemented, the expectation is that only a few clients will use it. However, over time, more and more clients join the network, especially if it is reliable. The result is that the DHCP scope runs out of IP addresses because it was not designed to handle so many devices.

Many network managers assume a wireless issue on the controller is causing the connectivity problem. Make sure that the supporting infrastructure is working for DHCP, as well as other services that the wireless network relies on, such as the RADIUS server.

More complex networks that use enterprise authentication might contain dynamic VLANs. Dynamic VLANs depend upon the RADIUS server to return the correct tags, otherwise, the client is placed in the incorrect area of the LAN and won't meet the correct connectivity requirements.

Other IP address issues can occur when a device moves between a wireless home network and a wireless work network. For example, if the end user applies a static IP address to the device manually to access the home network, the device won't connect correctly to the work network. Users might also change the IP configuration of the device to avoid security devices. By default, FortiWLC stops a client from joining a tunnelled wireless network if the client's manually configured IP address doesn't match the IP address range in use on the wireless network.



Confirm IP Connectivity

Problem:

- Client shows as connected in the controller device tables, and has a valid IP address, but can’t ping other hosts on the network

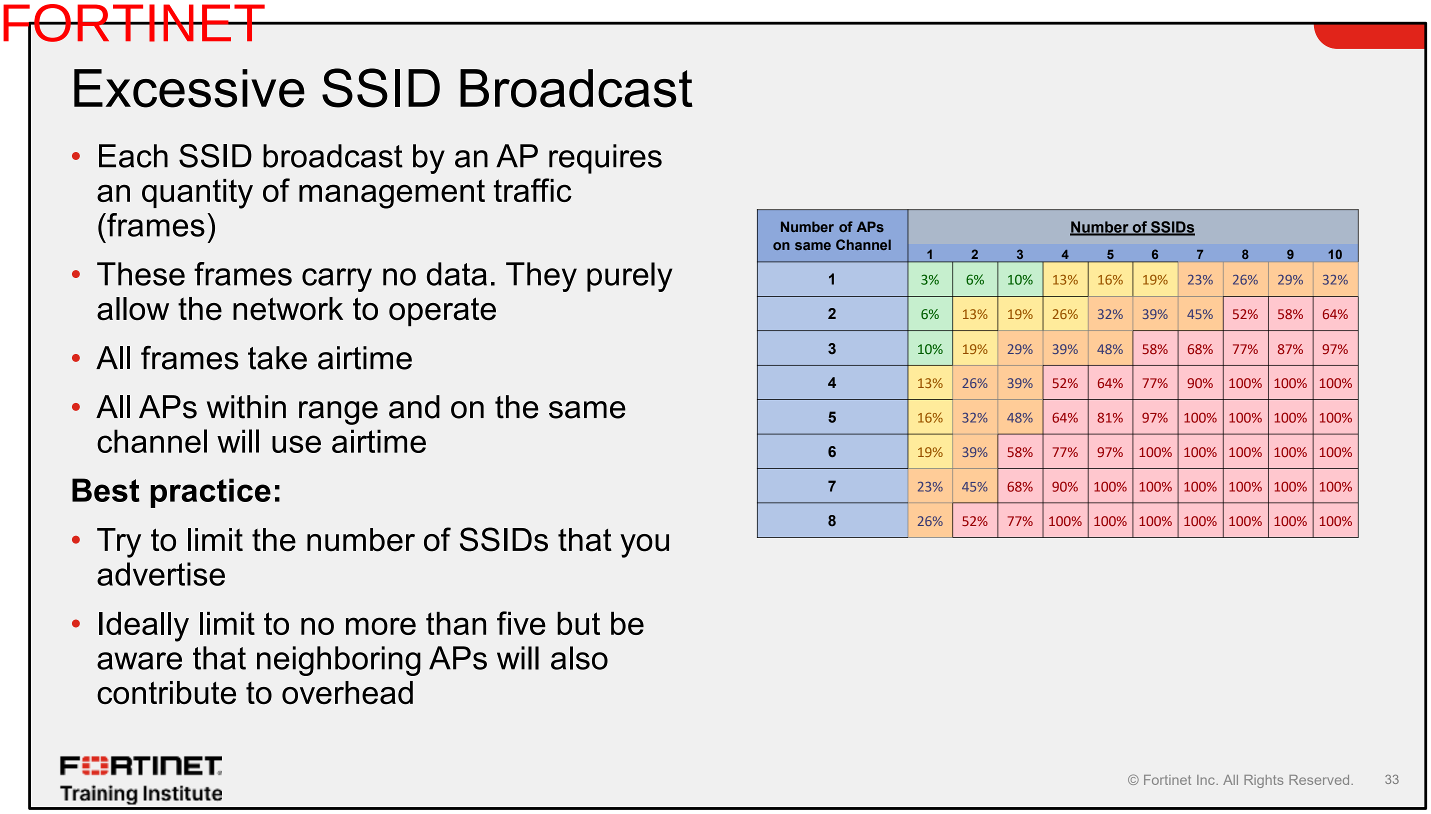
Solution:

- Key hosts and services on the network should be reachable at layer 3, which you can test using ping. Failing to contact key hosts implies:
  - A policy is potentially preventing traffic flow
  - A captive portal is in place but not triggered

32

Often a basic ping check of network resources can reveal a layer 3 issue. If IP addresses, such as gateways, DNS servers, and other key resources, are failing to respond, then investigate an intermediate network problem. Often wireless networks are deployed on a new VLAN, so it may be possible that a routing issue or policy is preventing traffic flow, rather than a wireless issue.

One situation in which a wireless AP or controller can interrupt IP address connectivity is when the captive portal is configured and the client’s browser fails to be triggered. This can cause the client to be isolated, awaiting the captive portal authentication, and the user does not see a login page when they launch the browser.



Excessive SSID Broadcast

- Each SSID broadcast by an AP requires an quantity of management traffic (frames)
- These frames carry no data. They purely allow the network to operate
- All frames take airtime
- All APs within range and on the same channel will use airtime

Best practice:

- Try to limit the number of SSIDs that you advertise
- Ideally limit to no more than five but be aware that neighboring APs will also contribute to overhead

Number of APs on same Channel	Number of SSIDs									
	1	2	3	4	5	6	7	8	9	10
1	3%	6%	10%	13%	16%	19%	23%	26%	29%	32%
2	6%	13%	19%	26%	32%	39%	45%	52%	58%	64%
3	10%	19%	29%	39%	48%	58%	68%	77%	87%	97%
4	13%	26%	39%	52%	64%	77%	90%	100%	100%	100%
5	16%	32%	48%	64%	81%	97%	100%	100%	100%	100%
6	19%	39%	58%	77%	97%	100%	100%	100%	100%	100%
7	23%	45%	68%	90%	100%	100%	100%	100%	100%	100%
8	26%	52%	77%	100%	100%	100%	100%	100%	100%	100%

FORTINET Training Institute

33

Another best practice that you should consider is the reduction or minimization of the number of wireless networks that your APs broadcast.

The temptation is to broadcast many wireless networks to fulfil many purposes.

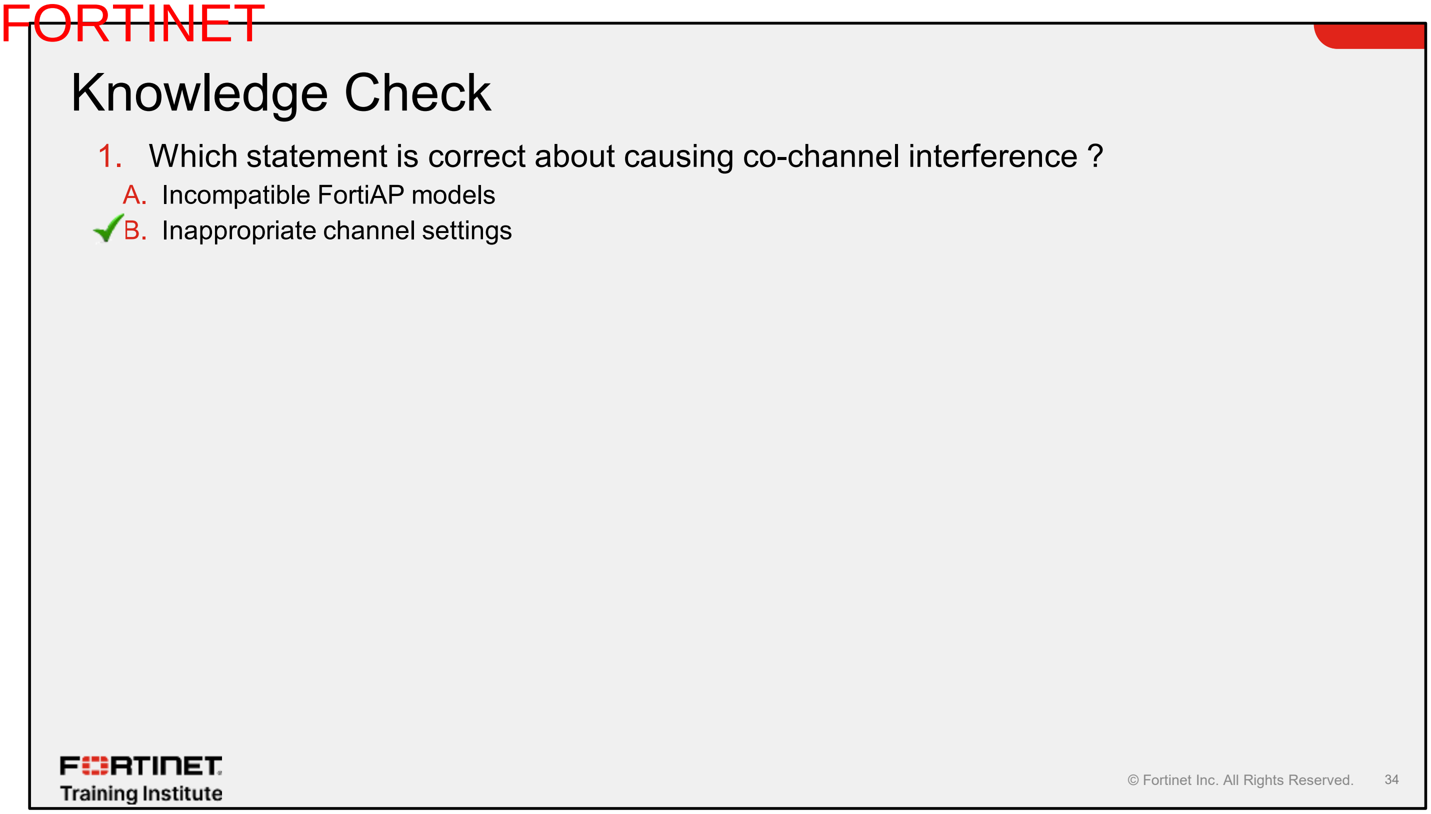
However, each wireless network broadcast from an AP requires an amount of wireless management traffic. This traffic, or these management frames, carry no data and take up airtime or wireless capacity.

The table on this slide shows an approximate calculation of the amount of airtime used when the number of APs in a channel broadcast a number of wireless networks (or SSIDs).

For example, if only one AP broadcast 10 networks or SSIDs, approximately 32% of available airtime would be used sending and receiving management frames without actually exchanging any useful data. This calculation also assumes an ideal environment with little or no interference. In the real world, it is likely that additional capacity could be lost to this as well.

Note that it makes no difference if the AP is your AP or a neighboring AP, the same overhead applies.

To minimize the effects, it is a best practice to limit the number of broadcasting networks to five, but preferably fewer. Note that there are various mechanisms, such as dynamic VLANs, that can help limit the need to have multiple wireless networks being broadcast.

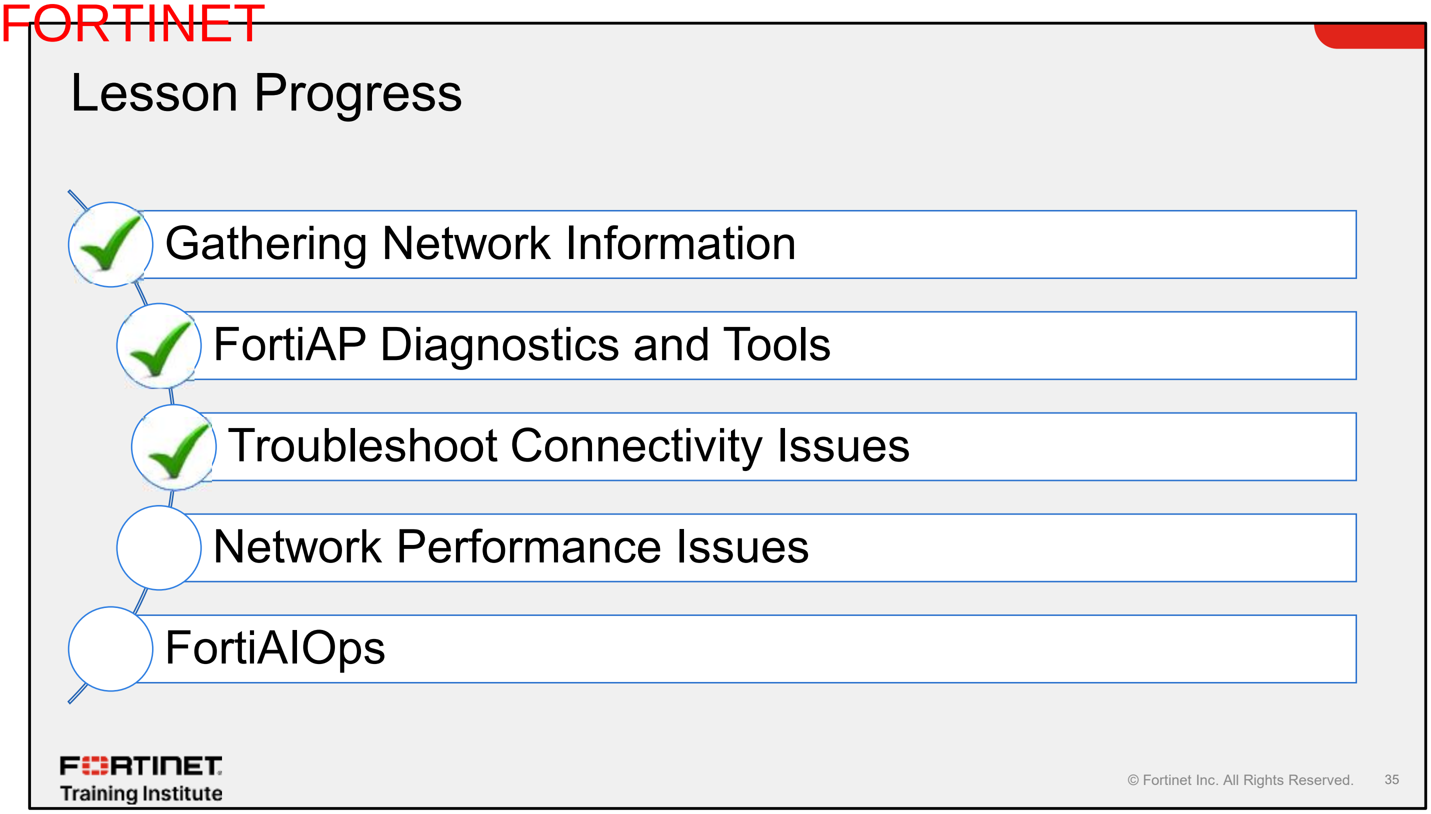


Knowledge Check

1. Which statement is correct about causing co-channel interference ?
   - A. Incompatible FortiAP models
   - ✓ B. Inappropriate channel settings

FORTINET
Training Institute

34



Lesson Progress

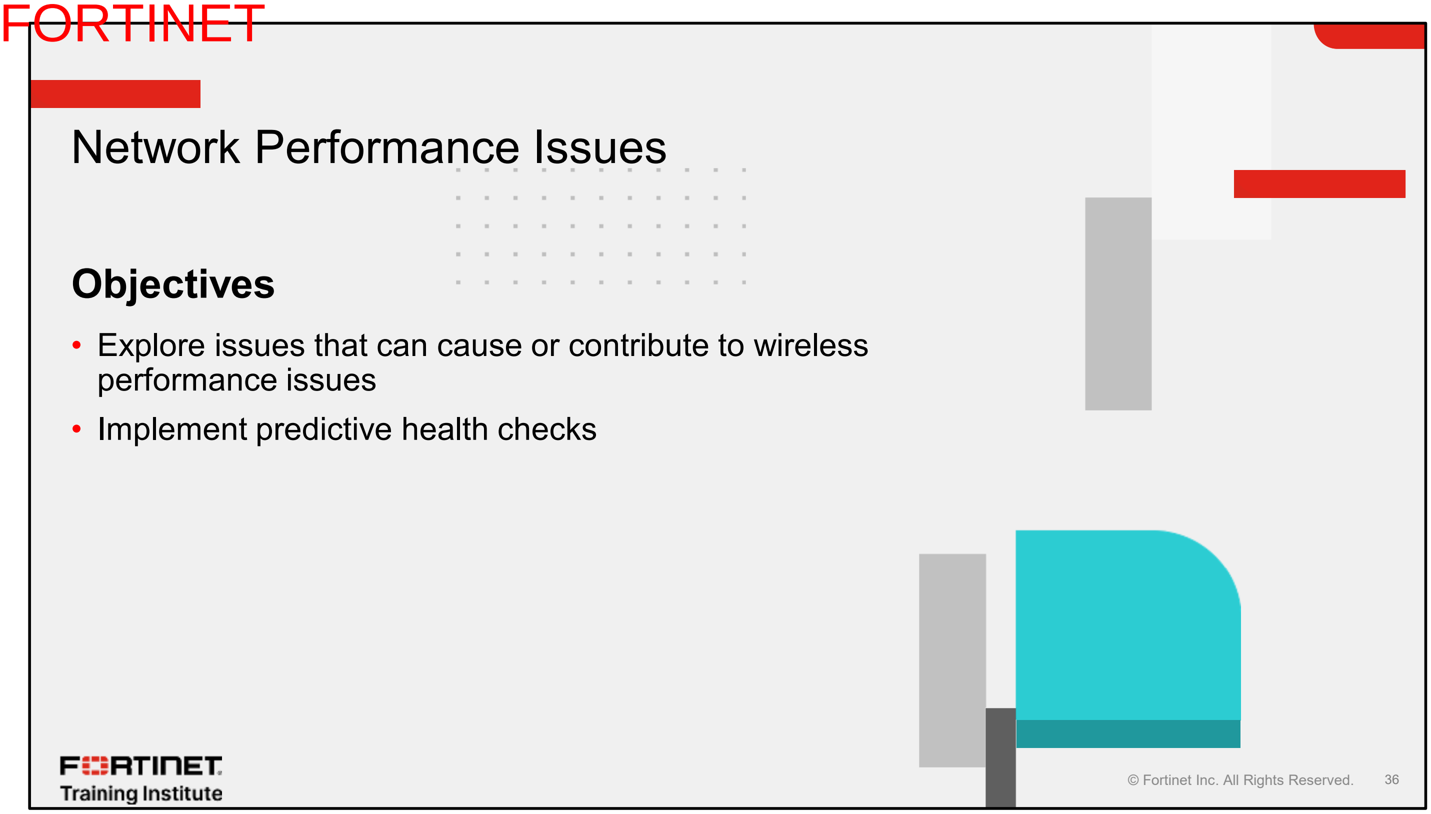
- ✓ Gathering Network Information
- ✓ FortiAP Diagnostics and Tools
- ✓ Troubleshoot Connectivity Issues
- ○ Network Performance Issues
- ○ FortiAIOps

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

Good job! You now understand network connectivity issues.

Now, you will learn about network performance issues.



Network Performance Issues

Objectives

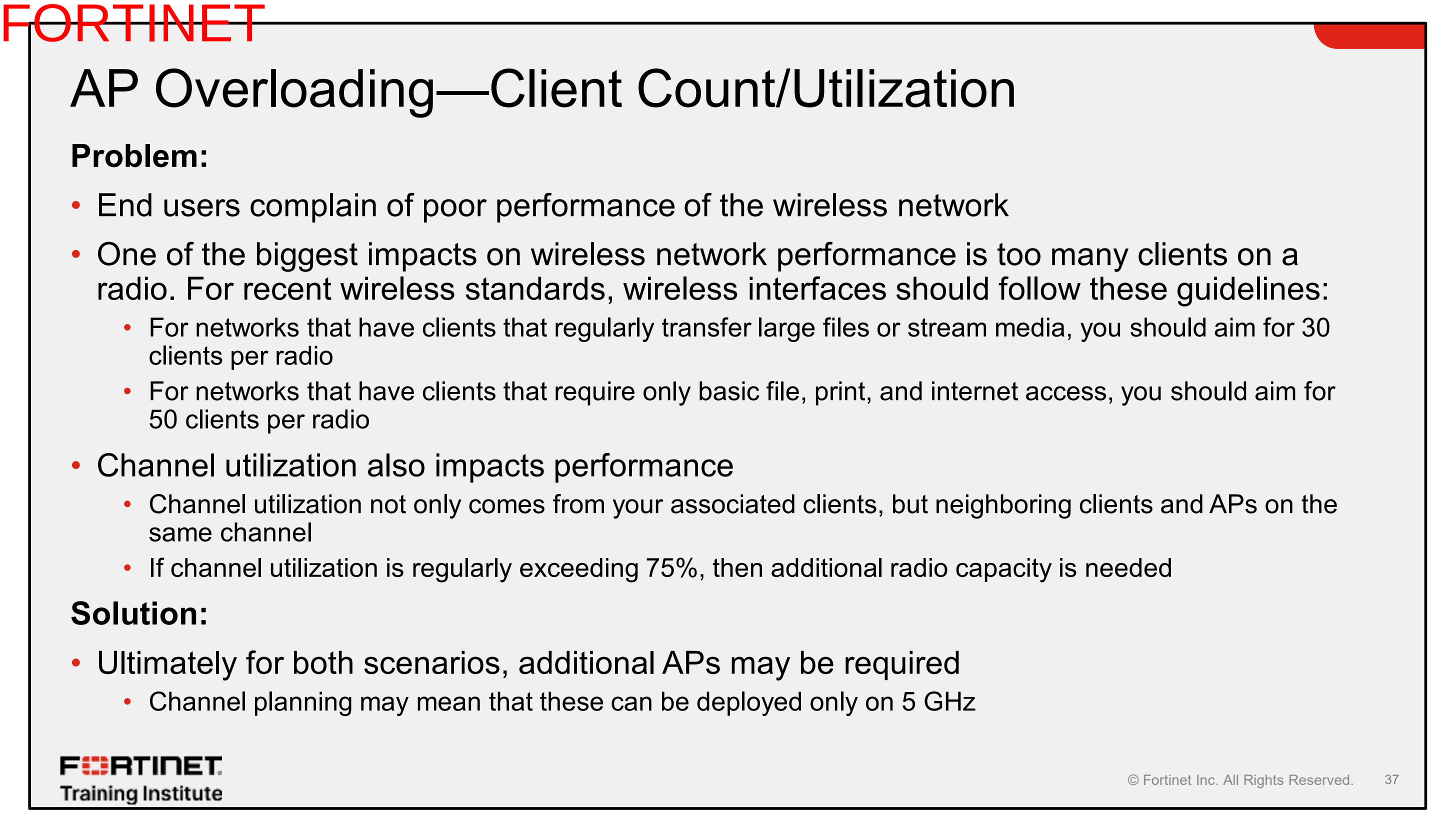
- Explore issues that can cause or contribute to wireless performance issues
- Implement predictive health checks

FORTINET
Training Institute

36

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding network performance issues, you will be able to resolve these types of problems. You will also be able to resolve issues with Service Assurance Manager (SAM) before wireless clients are affected.



AP Overloading—Client Count/Utilization

Problem:

- End users complain of poor performance of the wireless network
- One of the biggest impacts on wireless network performance is too many clients on a radio. For recent wireless standards, wireless interfaces should follow these guidelines:
  - For networks that have clients that regularly transfer large files or stream media, you should aim for 30 clients per radio
  - For networks that have clients that require only basic file, print, and internet access, you should aim for 50 clients per radio
- Channel utilization also impacts performance
  - Channel utilization not only comes from your associated clients, but neighboring clients and APs on the same channel
  - If channel utilization is regularly exceeding 75%, then additional radio capacity is needed

Solution:

- Ultimately for both scenarios, additional APs may be required
  - Channel planning may mean that these can be deployed only on 5 GHz

Training Institute

© Fortinet Inc. All Rights Reserved. 37

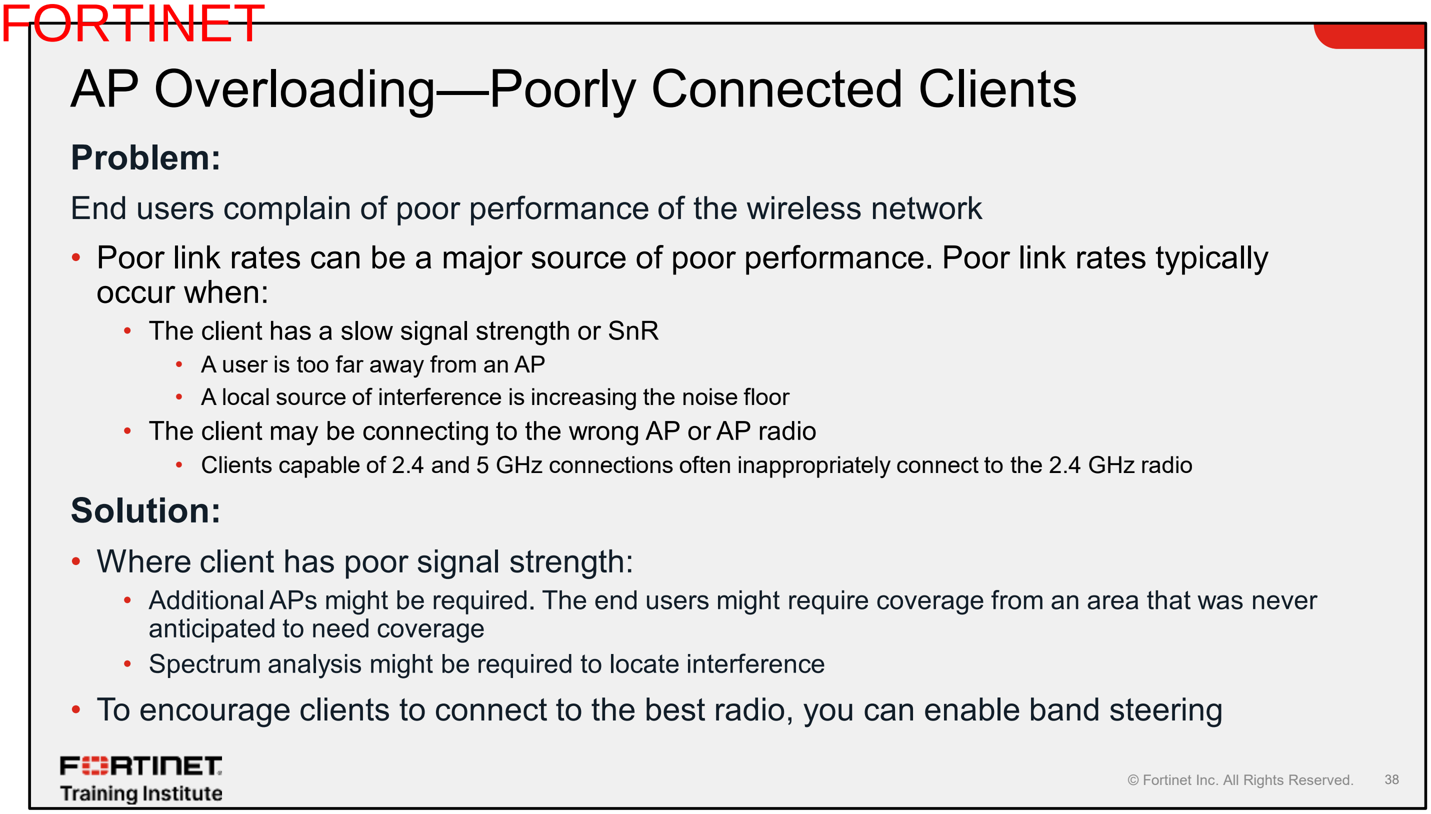
If you are able to correctly design and configure a wireless network then the experience for end users will be great. However, this generally results in end users wanting to connect *more* wireless devices. As a result, one of the most common problems with wireless networks can occur—overloading.

It is important to be continually aware of the number of clients that are connecting to a radio. Modern wireless standards allow clients to transmit and receive data faster than ever, however, it is important to remember that the wireless channel is still a *shared* resource and there are still practical limits on the number of clients that can share the airtime pie, regardless of how fast they can talk.

Future technologies based around multiuser-MIMO will possibly allow clients to simultaneously access the channel at the same time. (MIMO stands for multiple input multiple output.) However, it is currently recommended that interfaces should connect to a maximum of 50 clients when those clients require only basic file and print services. For higher bandwidth clients, such as those used in education environments, then that limit should be closer to 30.

Channel utilization is also a primary indication of capacity. Utilization is not generated only by your APs and clients. Any other neighboring APs and clients also contribute. It might be that your AP has only two stations using it, but when you inspect the channel utilization you might see high numbers. This could be because your workstations are transferring large files, Equally, it could be neighboring networks generating that utilization. If channel utilization is regularly exceeding *75%,* you must consider either adding AP capacity, or, in the case of neighboring networks generating utilization, changing your channel.

When adding APs in a high-density environment, 2.4 GHz channel planning becomes an issue. If you have large numbers of 2.4-only clients, you may not be able to accommodate them easily without resorting to ultra high-density-design practices. Covering these design practices is outside of the scope of this course.



AP Overloading—Poorly Connected Clients

Problem:

End users complain of poor performance of the wireless network

- Poor link rates can be a major source of poor performance. Poor link rates typically occur when:
  - The client has a slow signal strength or SnR
    - A user is too far away from an AP
    - A local source of interference is increasing the noise floor
  - The client may be connecting to the wrong AP or AP radio
    - Clients capable of 2.4 and 5 GHz connections often inappropriately connect to the 2.4 GHz radio

Solution:

- Where client has poor signal strength:
  - Additional APs might be required. The end users might require coverage from an area that was never anticipated to need coverage
  - Spectrum analysis might be required to locate interference
- To encourage clients to connect to the best radio, you can enable band steering

FORTINET Training Institute

38

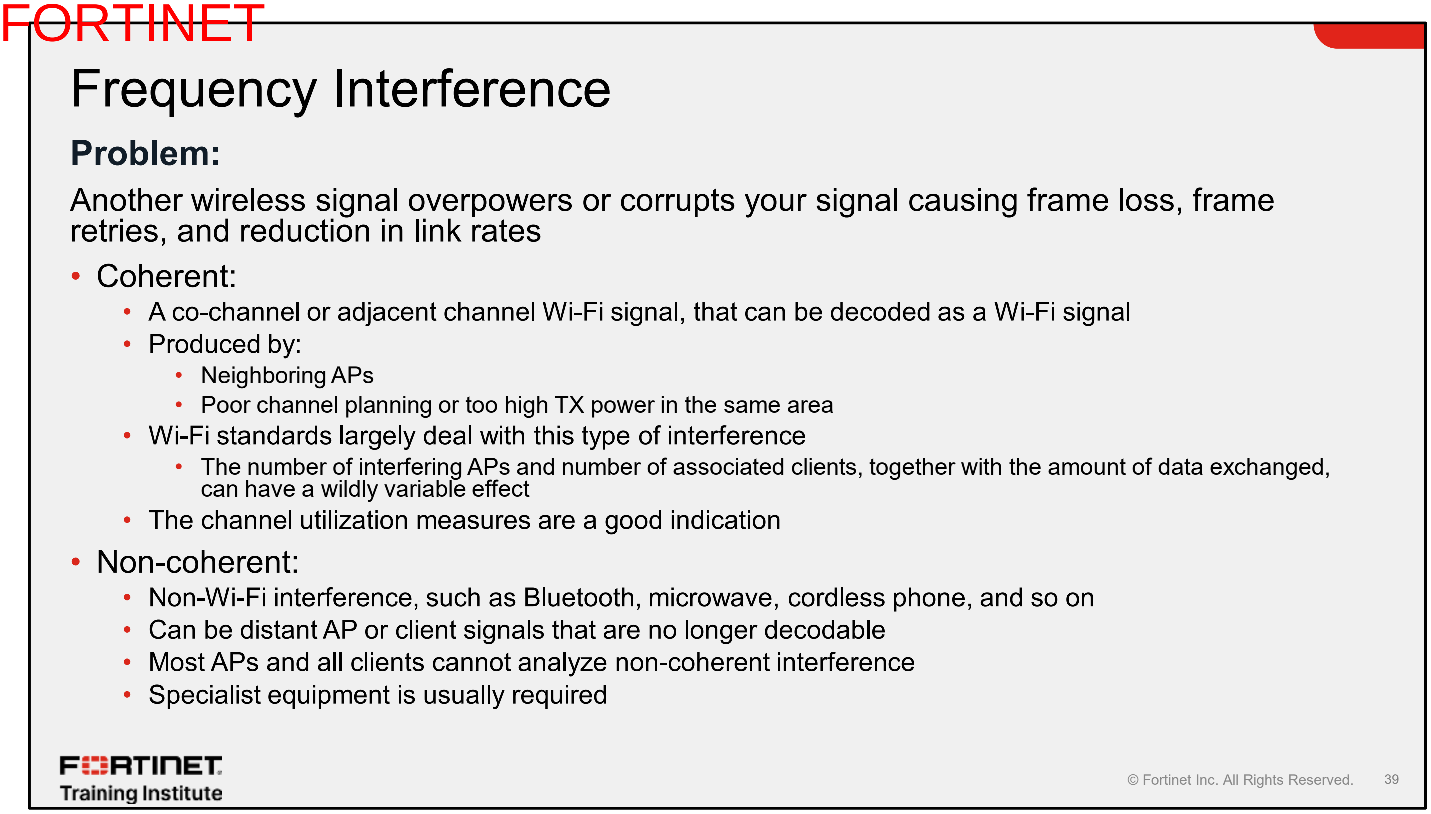
While AP overloading is a big issue, poor link rates can have an equal impact on throughput performance. A client that has a poor link rate is taking much longer to transfer data and is taking excessive amounts of airtime. Multiple reasons cause reduced link rates, but the primary reasons are generally to do with signal quality or that the client is connecting to an inappropriate radio.

The most common cause of poor signal quality is the user not having enough signal. This is often caused when users try to access the wireless network from a location where it was never designed to be. This will also affect any other clients usually connected to the same AP, because that poorly connected client is taking up more than its fair share of their time.

In the scenario shown on this slide, a decision must be made about coverage. It might be that you should install an AP to allow a good quality connection, or perhaps you should discourage end users from trying to connect.

Interference also impacts the connection rates. Note that interference can be highly localized. Interference may not affect the AP, but a client connecting to the AP, which is 20 metres away, could be significantly affected by a local interferer.

Most modern clients are capable of connecting on both the 2.4 and 5 GHz bands. Often when an AP broadcasts a wireless network on both 2.4 and 5 GHz, a client can make the wrong decision when connecting. This can result in an otherwise high-performance client talking very slowly on an inappropriate radio at low link rates. Frequency band steering is an option that is available on FortiAP devices. This allows the AP to encourage the client to associate with the most suitable radio. If you find that large numbers of 5 GHz clients are not connecting on the 5 GHz radio, then you should enable frequency handoff as a load balancing mechanism.



Frequency Interference

Problem:

Another wireless signal overpowers or corrupts your signal causing frame loss, frame retries, and reduction in link rates

- Coherent:
  - A co-channel or adjacent channel Wi-Fi signal, that can be decoded as a Wi-Fi signal
  - Produced by:
    - Neighboring APs
    - Poor channel planning or too high TX power in the same area
  - Wi-Fi standards largely deal with this type of interference
    - The number of interfering APs and number of associated clients, together with the amount of data exchanged, can have a wildly variable effect
  - The channel utilization measures are a good indication
- Non-coherent:
  - Non-Wi-Fi interference, such as Bluetooth, microwave, cordless phone, and so on
  - Can be distant AP or client signals that are no longer decodable
  - Most APs and all clients cannot analyze non-coherent interference
  - Specialist equipment is usually required

Wireless energy can take many forms. This energy can present challenges to the successful reception of a wireless signal.

There are typically two types of interference. Coherent interference is generally a reference to wireless devices that are broadcasting nearby. This is not interference in the traditional sense, because our wireless APs and clients recognize it as a wireless signal and, as such, can cope with it. It is still an issue because it reduces utilization, and thus performance.

Non-coherent interference is the traditional interference that can cause issues. This is wireless energy that cannot be recognized as a wireless signal. It could be random energy, for instance, generated by a microwave. Or, it could be another signal generated by a cordless phone, but it's a logical signal that is not recognized as such by the wireless devices.

All of this energy is additive, meaning the more interference there is, the more wireless energy there is. This causes the noise floor to rise, which can cause the signal-to-noise ratio link rates to reduce as well. In some scenarios, the amount of wireless energy can be excessive and can result in the wireless signal being completely overpowered resulting in a loss of connection.

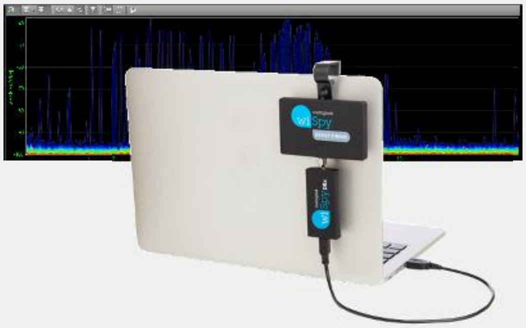
The 2.4 GHz frequency is particularly prone to interference because so many different devices are allowed to operate in that frequency. While APs and clients can assess the level of noise, they cannot identify it or locate it. Specialist hardware is usually required to track down an interferer.

Dedicated Spectrum Analysis

Solution:

Non-Wi-Fi or non-coherent interference requires dedicated equipment to detect

- Some AP chipsets can operate in spectrum analyzer mode
  - APs can be left in place to continually monitor interference
  - Can be difficult to pinpoint interferers
- Also dedicated equipment available
  - Dedicated equipment is typically mobile and can have a directional antenna. This makes it easy to pinpoint the interferer
  - Has to be onsite at the time of interference
- Interference is typically a problem in 2.4 GHz
- A very useful tool in a toolkit



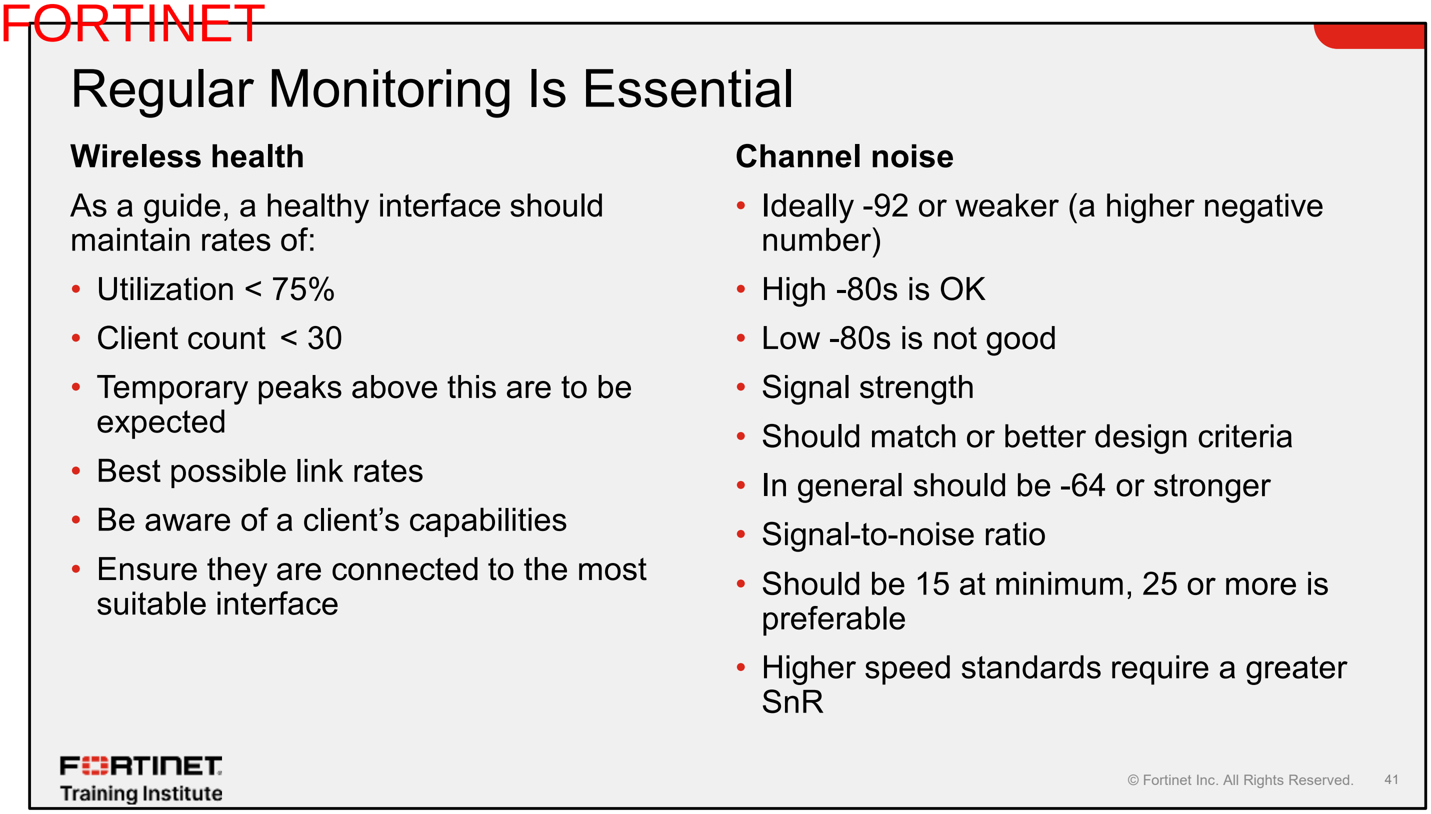
FORTINET Training Institute

40

Some modern APs now have the ability to operate in spectrum analyzer mode. This can be very useful for ongoing monitoring in a noisy environment because they can generally be left to log interference events. However, they are less useful when trying to identify the exact location because APs generally lack highly directional antennas that can pinpoint the source. Some chipsets can operate only in AP mode or in spectrum analyzer mode, which can mean that you need to dedicate APs to the task.

Most wireless engineers dealing with networks of any size often purchase a dedicated spectrum analyzer tool. The chipsets and software used in these tools are specifically designed for the analysis of wireless interference. They often come with a highly directional antenna and are mobile, allowing the engineer to walk the site and locate any sort of interference with relative ease. Typically, the software also has a library of interferer signatures that allows the classification of anything detected, for example, microwaves and Bluetooth devices are commonly identified. The downside of dedicated equipment such as this is that it has to be onsite when the interference is occurring.

If the majority of your wireless networks broadcast in the 5 GHz range, then the chance of interference is far less because this range of frequencies was only ever available for wireless LAN use. It may be that you decide that a spectrum analyzer is not required, however, because 2.4 GHz is not going away and is increasingly being used for IoT devices, it is highly advisable for an engineering team looking after a large wireless network to have access to one. There are multiple vendors and multiple devices available on the market. Metageek equipment is commonly used by wireless engineers.



Regular Monitoring Is Essential

Wireless health

As a guide, a healthy interface should maintain rates of:

- Utilization < 75%
- Client count < 30
- Temporary peaks above this are to be expected
- Best possible link rates
- Be aware of a client's capabilities
- Ensure they are connected to the most suitable interface

Channel noise

- Ideally -92 or weaker (a higher negative number)
- High -80s is OK
- Low -80s is not good
- Signal strength
- Should match or better design criteria
- In general should be -64 or stronger
- Signal-to-noise ratio
- Should be 15 at minimum, 25 or more is preferable
- Higher speed standards require a greater SnR

41

The lower the channel noise, the better. Signal strength is measured in negative decibels—the greater the negative number, the weaker the signal.

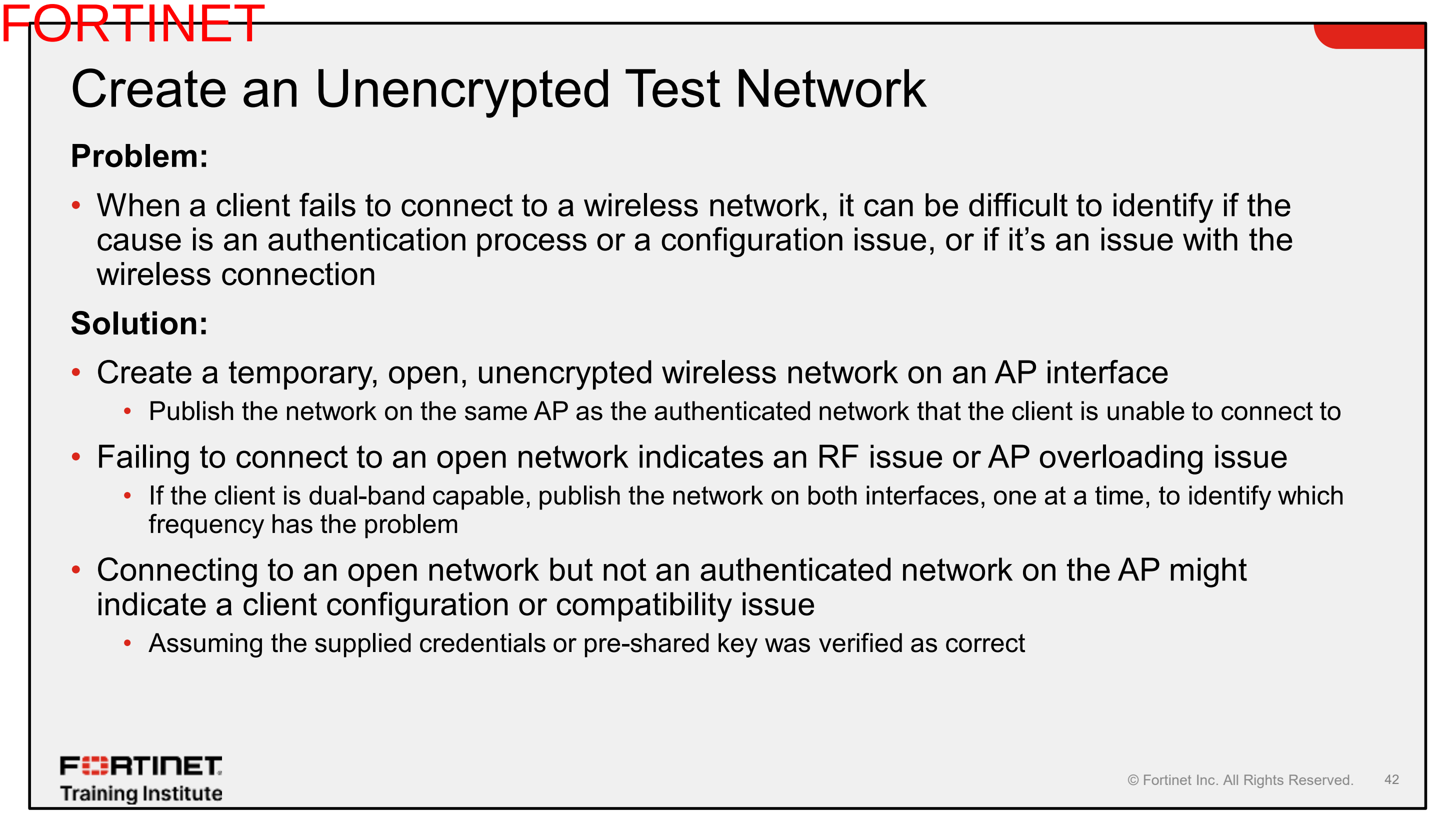
For noise, a signal weaker than -92 is considered optimal. A signal in the high -80s is acceptable. A signal in the low -80s or -70s indicates significant interference that you should investigate using a spectrum analyzer.

The wireless network would have been designed and specified with a target signal strength for clients. You should make sure that the majority of your clients have that minimum signal strength or greater.

It is not unusual to have a small number of stations that are weaker. For example, wireless devices enter and leave buildings, which can cause small numbers of low-signal-strength clients to appear and disappear.

Generally, you should see signal strengths of *-64 or stronger*, with a good SnR of *at least 15*, but preferably 25 or more. Newer, higher speed standards will generally require a higher signal strength AND a greater SnR but these numbers provide a good baseline and allow most wireless connections to work.

Finally, the ultimate indicator of health is the link rates that the client and AP use to communicate with each other. Before you can make a judgment on the link rates, you first must understand the specification of the wireless client to determine the maximum link rate you can use. Often devices will be equipped with 1 or 2 stream 2.4 and 5 GHz capable clients. Analysis of the link rates being used may show that rather than connecting near the theoretical maximums 433 or 866 Mbps that you might expect, they are connecting closer to 65 Mbps. Often this is simply a result of the clients connecting to the 2.4 GHz radio rather than a more "suitable" 5 GHz radio. Equally, link rates will be reduced if the underlying metrics (loss/retry/signal strength/noise) are impacted.



Create an Unencrypted Test Network

Problem:

- When a client fails to connect to a wireless network, it can be difficult to identify if the cause is an authentication process or a configuration issue, or if it's an issue with the wireless connection

Solution:

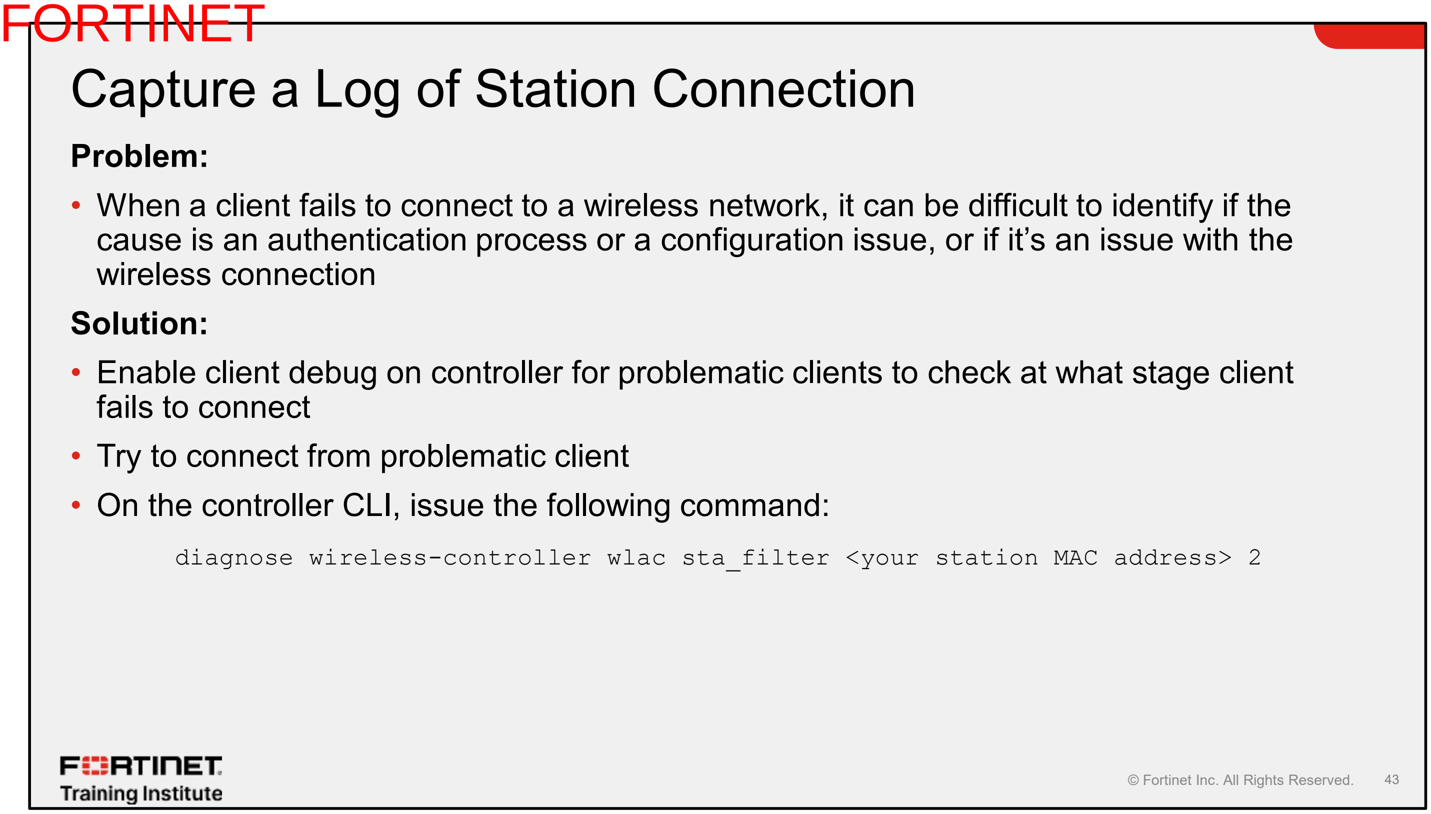
- Create a temporary, open, unencrypted wireless network on an AP interface
  - Publish the network on the same AP as the authenticated network that the client is unable to connect to
- Failing to connect to an open network indicates an RF issue or AP overloading issue
  - If the client is dual-band capable, publish the network on both interfaces, one at a time, to identify which frequency has the problem
- Connecting to an open network but not an authenticated network on the AP might indicate a client configuration or compatibility issue
  - Assuming the supplied credentials or pre-shared key was verified as correct

Training Institute

42

It can be difficult to diagnose where a connection issue is located. An easy way to diagnose this is to remove the authentication process. To do this, create an open network on a single interface of the AP that the client is unable to connect to. If the client *can't* connect to the unencrypted network, then there is an underlying RF issue or AP overloading issue that is causing the connectivity problem. You can also move the network to a different interface enabling you to check connectivity on both the 2.4 and the 5 GHz ranges.

If the client can connect to the open network but not the encrypted network, and the client entered the correct credentials during the authentication process, then RF is not the problem and you should focus your troubleshooting efforts on the client configuration.



Capture a Log of Station Connection

Problem:

- When a client fails to connect to a wireless network, it can be difficult to identify if the cause is an authentication process or a configuration issue, or if it's an issue with the wireless connection

Solution:

- Enable client debug on controller for problematic clients to check at what stage client fails to connect
- Try to connect from problematic client
- On the controller CLI, issue the following command:

```
diagnose wireless-controller wlac sta_filter <your station MAC address> 2
```

Training Institute

43

While connecting to an unencrypted test network is a useful test, often there is a need to drill down into the connection process to see what is failing.

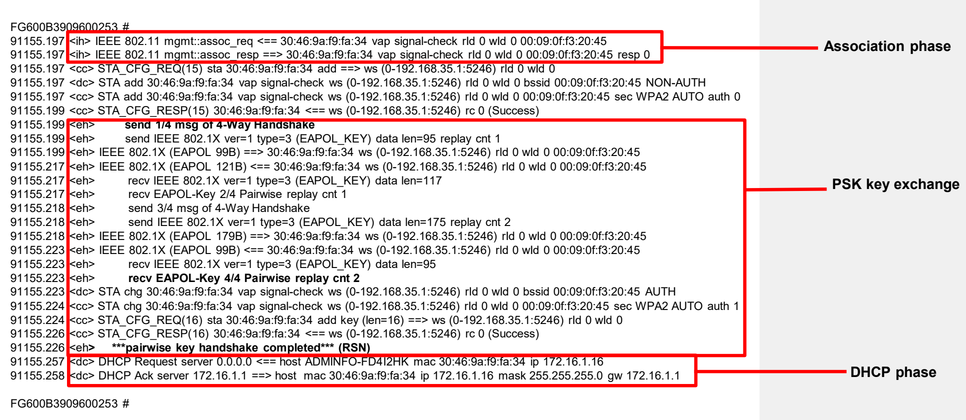
You can do this using the `diagnose wireless-controller wlac sta_filter` command on the CLI.

This will capture a step-by-step log of connection attempts made by your station.

By using this log, you should be able to determine which bond process is failing.

Capture a Log of Station Connection (Contd)

- Sample debug message for *successful* client association with WPA_PSK security



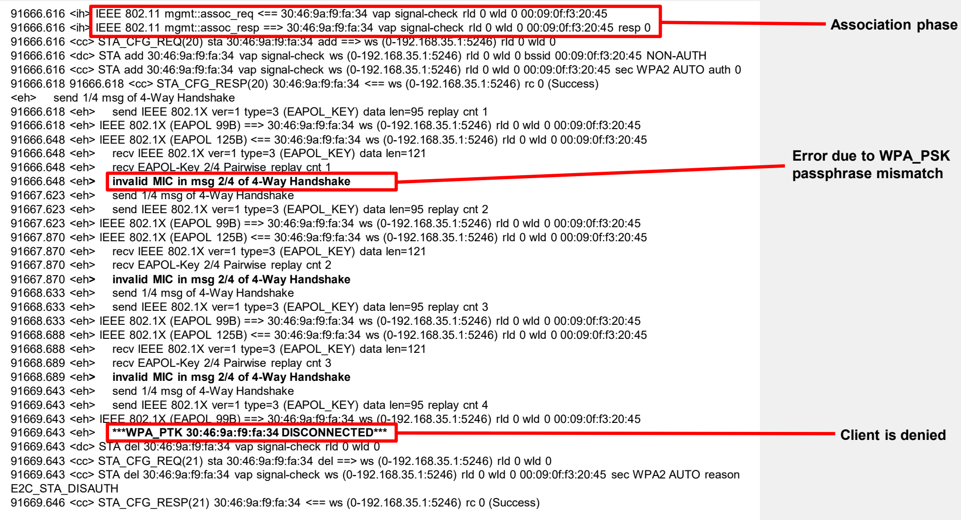
```
FG600B3909600253 #
91155.197 <ih> IEEE 802.11 mgmt::assoc_req <== 30:46:9a:f9:fa:34 vap signal-check rld 0 wld 0 00:09:0f:f3:20:45
91155.197 <ih> IEEE 802.11 mgmt::assoc_resp ==> 30:46:9a:f9:fa:34 vap signal-check rld 0 wld 0 00:09:0f:f3:20:45 resp 0
91155.197 <cc> STA_CFG_REQ(15) sta 30:46:9a:f9:fa:34 add ==> ws (0-192.168.35.1:5246) rld 0 wld 0
91155.197 <dc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rld 0 wld 0 bssid 00:09:0f:f3:20:45 NON-AUTH
91155.197 <cc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45 sec WPA2 AUTO auth 0
91155.199 <cc> STA_CFG_RESP(15) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0 (Success)
91155.199 <eh>       send 1/4 msg of 4-Way Handshake
91155.199 <eh>       send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95 replay cnt 1
91155.199 <eh> IEEE 802.1X (EAPOL 99B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91155.217 <eh> IEEE 802.1X (EAPOL 121B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91155.217 <eh>        recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=117
91155.217 <eh>        recv EAPOL-Key 2/4 Pairwise replay cnt 1
91155.218 <eh>        send 3/4 msg of 4-Way Handshake
91155.218 <eh>        send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=175 replay cnt 2
91155.218 <eh> IEEE 802.1X (EAPOL 179B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91155.223 <eh> IEEE 802.1X (EAPOL 99B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91155.223 <eh>        recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95
91155.223 <eh>        recv EAPOL-Key 4/4 Pairwise replay cnt 2
91155.223 <dc> STA chg 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rld 0 wld 0 bssid 00:09:0f:f3:20:45 AUTH
91155.224 <cc> STA chg 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45 sec WPA2 AUTO auth 1
91155.224 <cc> STA_CFG_REQ(16) sta 30:46:9a:f9:fa:34 add key (len=16) ==> ws (0-192.168.35.1:5246) rld 0 wld 0
91155.226 <cc> STA_CFG_RESP(16) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0 (Success)
91155.226 <eh>    ***pairwise key handshake completed*** (RSN)
91155.257 <dc> DHCP Request server 0.0.0.0 <== host ADMINFO-FD4I2HK mac 30:46:9a:f9:fa:34 ip 172.16.1.16
91155.258 <dc> DHCP Ack server 172.16.1.1 ==> host  mac 30:46:9a:f9:fa:34 ip 172.16.1.16 mask 255.255.255.0 gw 172.16.1.1

FG600B3909600253 #
```

This slide shows a sample debug message for successful client association with WPA_PSK security.

It is important to note the messages for a correct association phase, four-way handshake, and the DHCP phase.

Capture a Log of Station Connection (Contd)

- Sample client association *failed* because of WPA_PSK passphrase mismatch



```
91666.616 <ih> IEEE 802.11 mgmt::assoc_req <== 30:46:9a:f9:fa:34 vap signal-check rld 0 wld 0 00:09:0f:f3:20:45
91666.616 <ih> IEEE 802.11 mgmt::assoc_resp ==> 30:46:9a:f9:fa:34 vap signal-check rld 0 wld 0 00:09:0f:f3:20:45 resp 0
91666.616 <cc> STA_CFG_REQ(20) sta 30:46:9a:f9:fa:34 add ==> ws (0-192.168.35.1:5246) rld 0 wld 0
91666.616 <dc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rld 0 wld 0 bssid 00:09:0f:f3:20:45 NON-AUTH
91666.616 <cc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45 sec WPA2 AUTO auth 0
91666.618 91666.618 <cc> STA_CFG_RESP(20) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0 (Success)
<eh>     send 1/4 msg of 4-Way Handshake
91666.618 <eh>     send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95 replay cnt 1
91666.618 <eh> IEEE 802.1X (EAPOL 99B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91666.648 <eh> IEEE 802.1X (EAPOL 125B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91666.648 <eh>     recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=121
91666.648 <eh>     recv EAPOL-Key 2/4 Pairwise replay cnt 1
91666.648 <eh>     invalid MIC in msg 2/4 of 4-Way Handshake
91667.623 <eh>     send 1/4 msg of 4-Way Handshake
91667.623 <eh>     send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95 replay cnt 2
91667.623 <eh> IEEE 802.1X (EAPOL 99B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91667.870 <eh> IEEE 802.1X (EAPOL 125B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91667.870 <eh>     recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=121
91667.870 <eh>     recv EAPOL-Key 2/4 Pairwise replay cnt 2
91667.870 <eh>     invalid MIC in msg 2/4 of 4-Way Handshake
91668.633 <eh>     send 1/4 msg of 4-Way Handshake
91668.633 <eh>     send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95 replay cnt 3
91668.633 <eh> IEEE 802.1X (EAPOL 99B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91668.688 <eh> IEEE 802.1X (EAPOL 125B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91668.688 <eh>     recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=121
91668.689 <eh>     recv EAPOL-Key 2/4 Pairwise replay cnt 3
91668.689 <eh>     invalid MIC in msg 2/4 of 4-Way Handshake
91669.643 <eh>     send 1/4 msg of 4-Way Handshake
91669.643 <eh>     send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95 replay cnt 4
91669.643 <eh> IEEE 802.1X (EAPOL 99B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45
91669.643 <eh>     ***WPA_PTK 30:46:9a:f9:fa:34 DISCONNECTED***
91669.643 <dc> STA del 30:46:9a:f9:fa:34 vap signal-check rld 0 wld 0
91669.643 <cc> STA_CFG_REQ(21) sta 30:46:9a:f9:fa:34 del ==> ws (0-192.168.35.1:5246) rld 0 wld 0
91669.643 <cc> STA del 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rld 0 wld 0 00:09:0f:f3:20:45 sec WPA2 AUTO reason
E2C_STA_DISAUTH
91669.646 <cc> STA_CFG_RESP(21) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0 (Success)
```

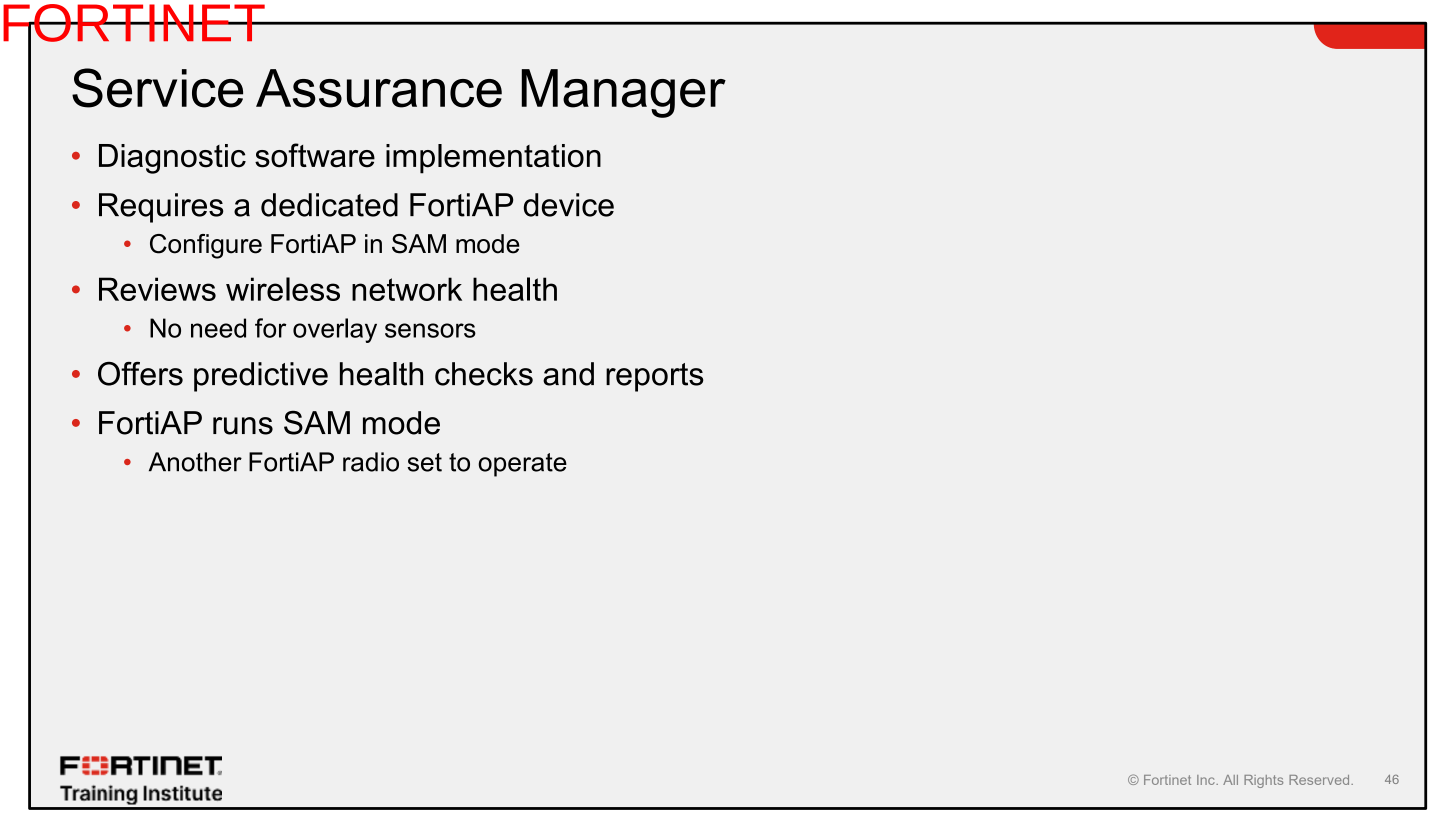
Association phase

Error due to WPA_PSK passphrase mismatch

Client is denied

For comparison, this slide shows a failed client association because of a WPA_PSK passphrase mismatch.

Note the error message on the four-way handshake process, which indicates an invalid MIC, and after many tries, the client is denied.

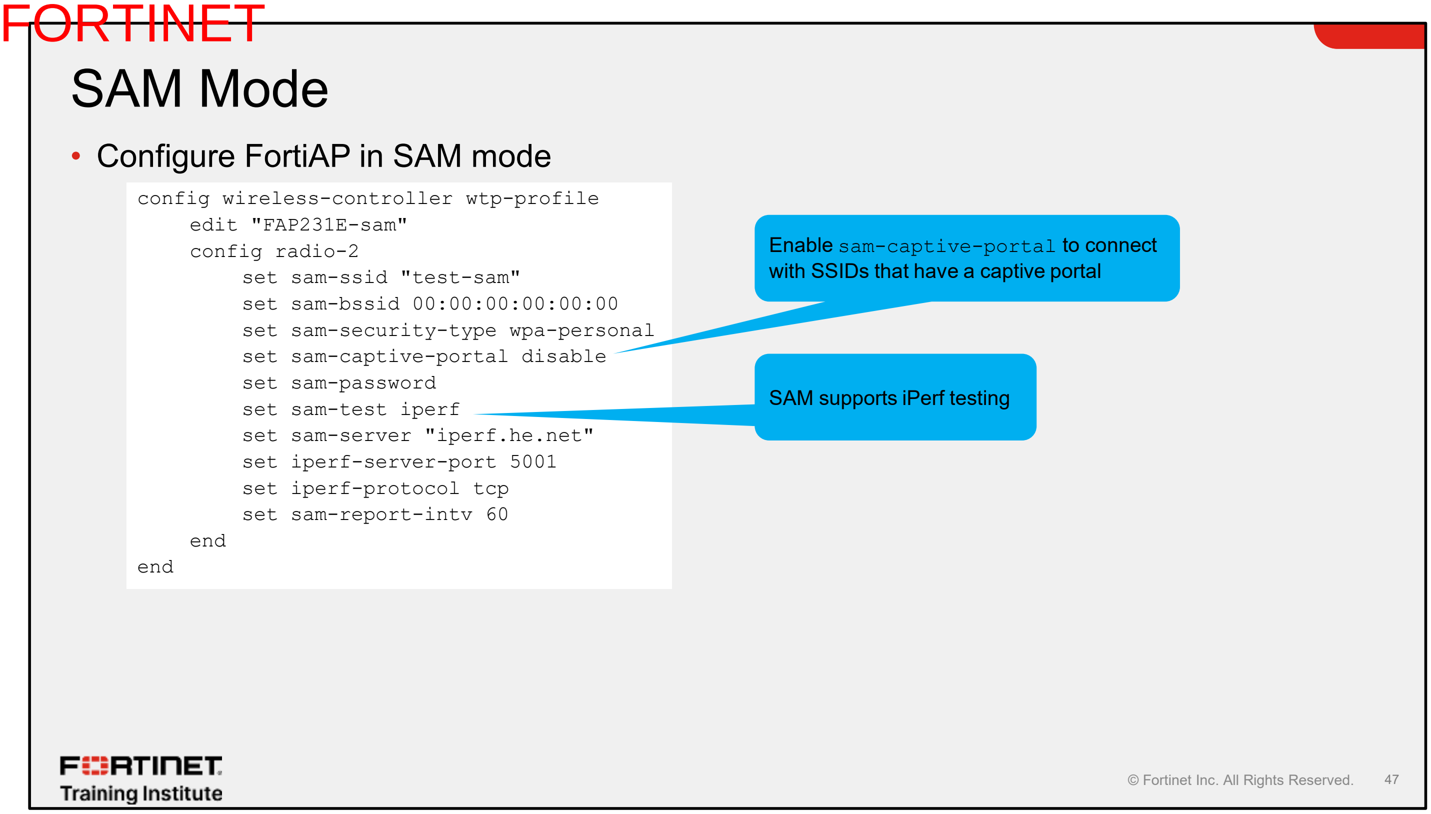


Service Assurance Manager

- Diagnostic software implementation
- Requires a dedicated FortiAP device
  - Configure FortiAP in SAM mode
- Reviews wireless network health
  - No need for overlay sensors
- Offers predictive health checks and reports
- FortiAP runs SAM mode
  - Another FortiAP radio set to operate

SAM is a predictive diagnostic software tool for remotely diagnosing the health of wireless networks without requiring overlay sensors. With SAM, the network automatically performs predictive health checks and reports any issues before end users are impacted.

You can configure FortiAP to run in SAM mode, where a radio is designated to operate as a client and perform tests on another FortiAP device. SAM conducts ping tests and iPerf tests are used in intervals, with results captured in the Wi-Fi event logs. This allows FortiGate to verify and ensure that an existing Wi-Fi network can provide acceptable services.



SAM Mode

- Configure FortiAP in SAM mode

```
config wireless-controller wtp-profile
    edit "FAP231E-sam"
    config radio-2
        set sam-ssid "test-sam"
        set sam-bssid 00:00:00:00:00:00
        set sam-security-type wpa-personal
        set sam-captive-portal disable
        set sam-password
        set sam-test iperf
        set sam-server "iperf.he.net"
        set iperf-server-port 5001
        set iperf-protocol tcp
        set sam-report-intv 60
    end
end
```

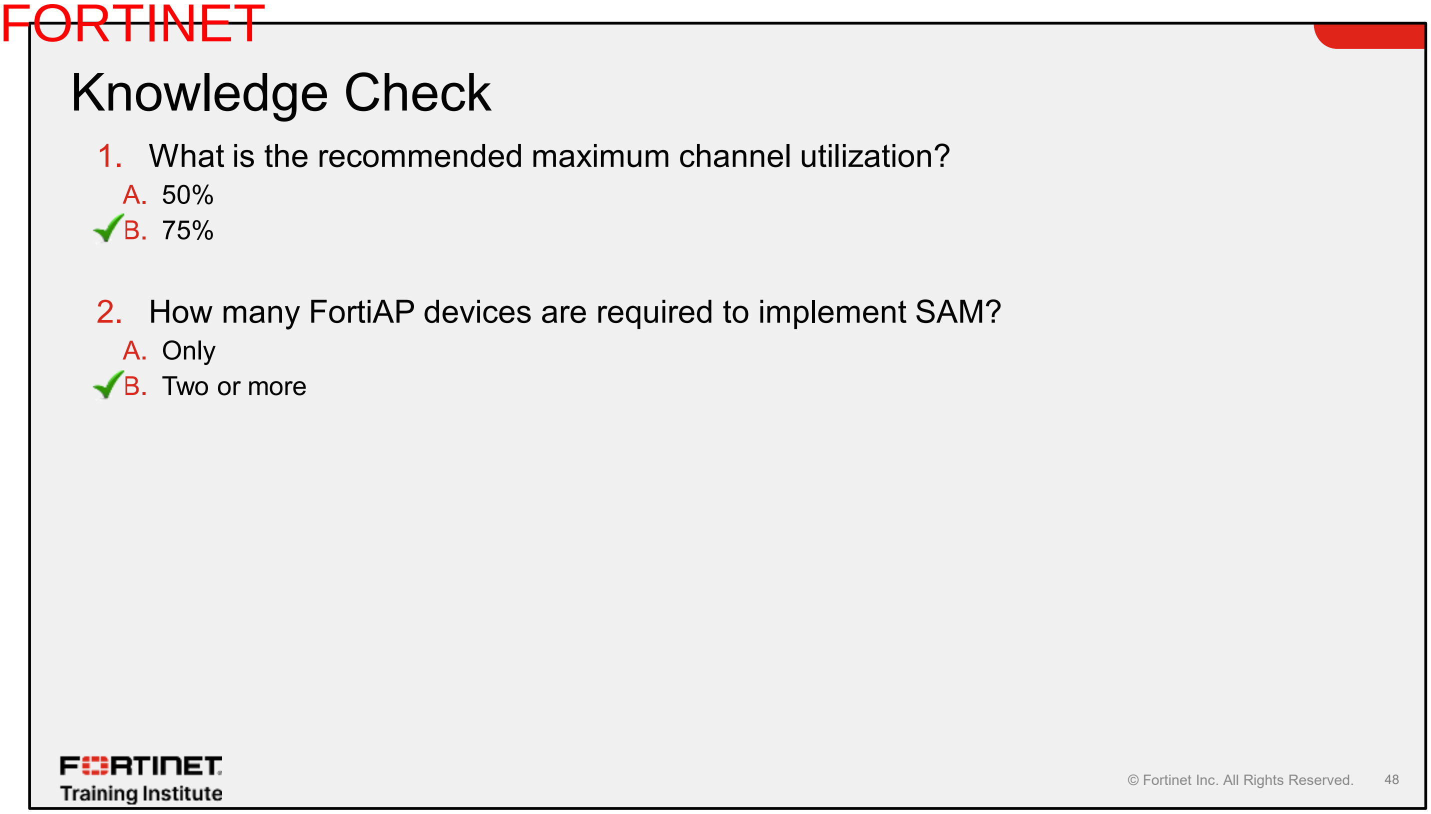
Enable `sam-captive-portal` to connect with SSIDs that have a captive portal

SAM supports iPerf testing

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 47

Configure the managed FortiAP profile to use SAM mode to diagnose the health of wireless networks of the production FortiAP device. If the SSID in the production FortiAP device is using captive portal, enable `sam-captive-portal` on the SAM-mode FortiAP device to configure further settings such as username and password.

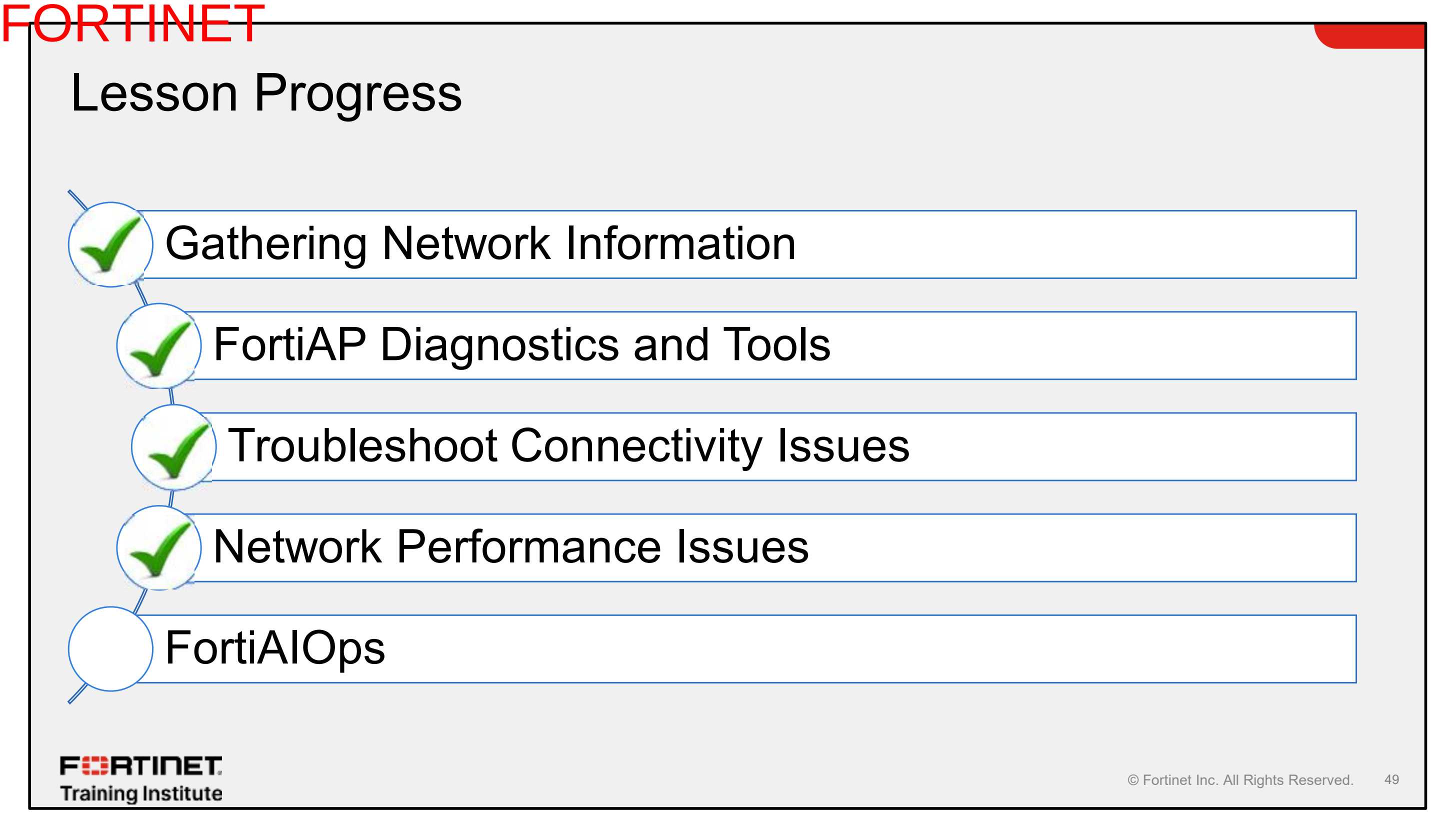


Knowledge Check

1. What is the recommended maximum channel utilization?
   - A. 50%
   - ✓ B. 75%

2. How many FortiAP devices are required to implement SAM?
   - A. Only
   - ✓ B. Two or more

48



Lesson Progress

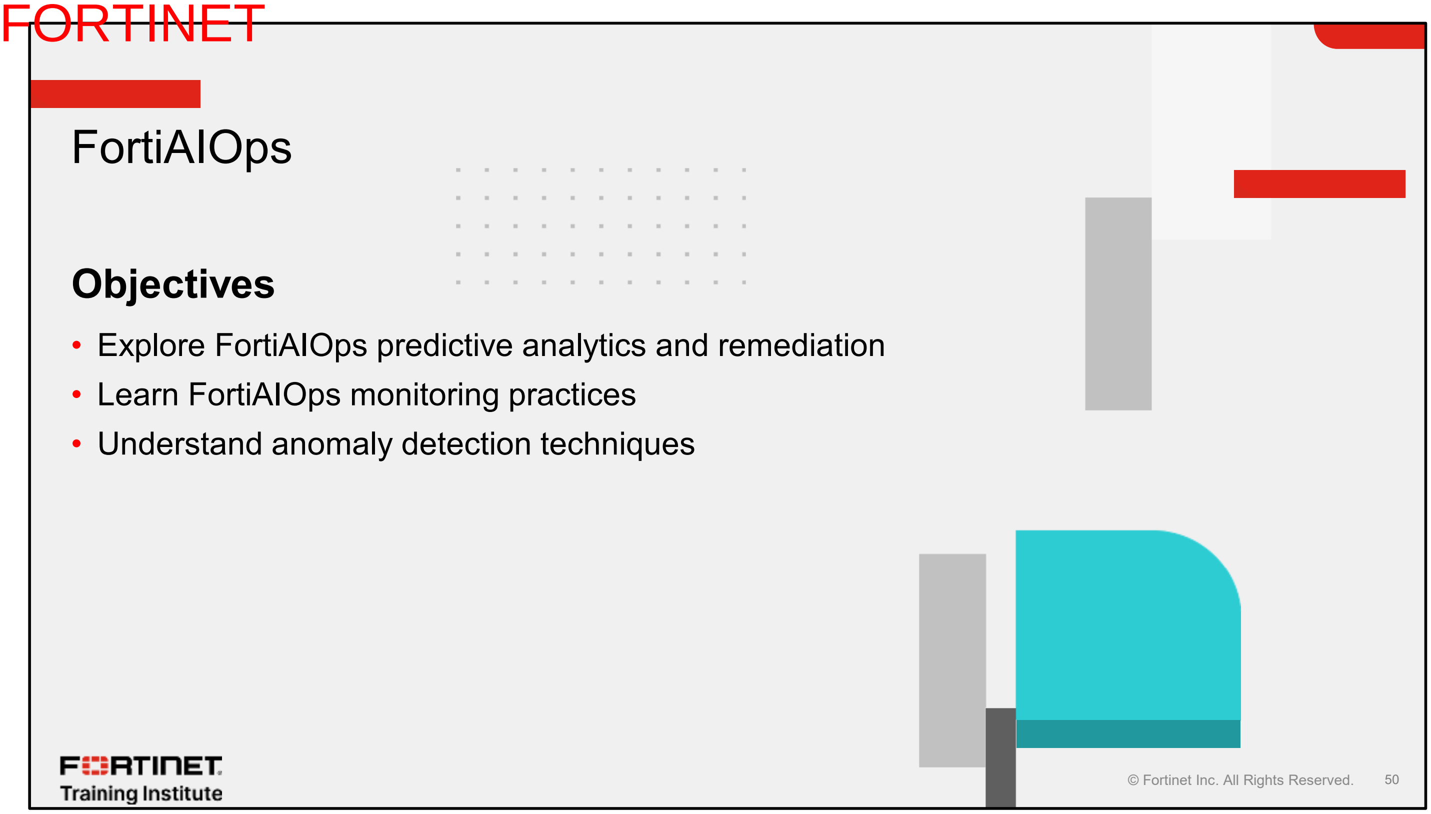
- ✓ Gathering Network Information
- ✓ FortiAP Diagnostics and Tools
- ✓ Troubleshoot Connectivity Issues
- ✓ Network Performance Issues
- ○ FortiAIOps

FORTINET Training Institute

49

Good job! You now understand network performance issues.

Now, you will learn about FortiAIOps.



FortiAIOps

Objectives

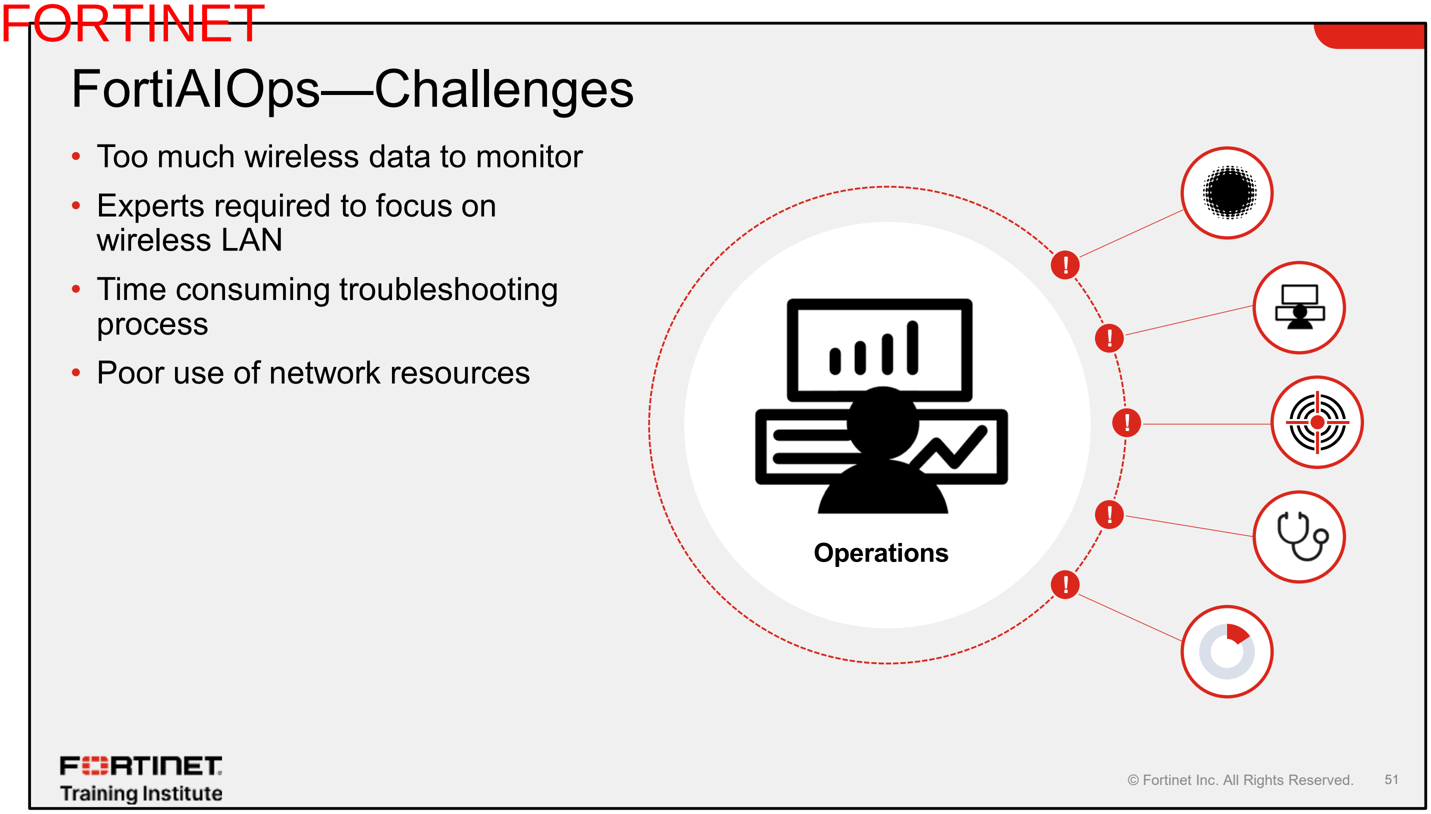
- Explore FortiAIOps predictive analytics and remediation
- Learn FortiAIOps monitoring practices
- Understand anomaly detection techniques

FORTINET Training Institute

50

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiAIOps, you will be able to explore methods to detect unusual patterns to troubleshoot network and security issues in wireless LAN.



FortiAIOps—Challenges

- Too much wireless data to monitor
- Experts required to focus on wireless LAN
- Time consuming troubleshooting process
- Poor use of network resources

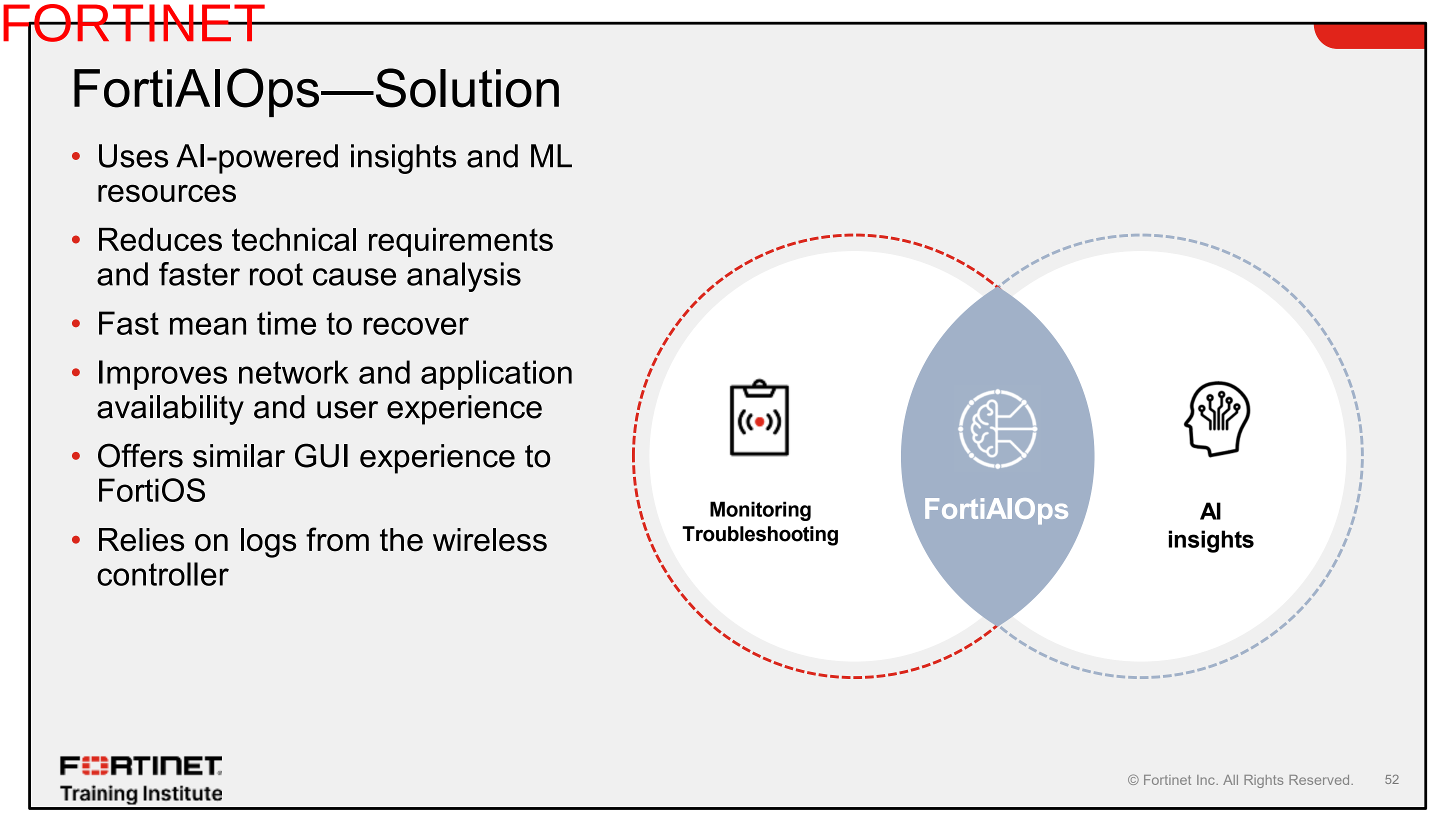
Training Institute

51

The common problems administrators face when troubleshooting networks usually require highly skilled and time-intensive investigation and remediation. Network administrators are required to be experts in various technologies such as wireless LAN, routing, and switching.

Users often report issues using vague statements, such as "slow connection" or "unable to open a web page". Administrators as a result struggle to understand the issues from the initial report.

Inadequate resources can lead to poor use of network resource. Whether it is insufficient bandwidth, outdated hardware, or lack of proper network infrastructure, lack of these resources increase the challenges network administrators face to troubleshoot the issues.



FortiAIOps—Solution

- Uses AI-powered insights and ML resources
- Reduces technical requirements and faster root cause analysis
- Fast mean time to recover
- Improves network and application availability and user experience
- Offers similar GUI experience to FortiOS
- Relies on logs from the wireless controller

Monitoring Troubleshooting

FortiAIOps

AI insights

FORTINET Training Institute

52

FortiAIOps leverages artificial intelligence (AI) and machine learning (ML) to enhance network operations. FortiAIOps easily monitors large amounts of data points and reports of wireless LAN and LAN traffic, including layer 1 details. These details can include full radio frequency (RF) spectrum analysis to help understand interference on the Wi-Fi network.

FortiAIOps includes built-in tools to probe the network to help you understand and diagnose network issues.

You can use FortiAIOps to help reduce technical support tickets by identifying and correcting issues before they start impacting users.

The FortiAIOps GUI is like the FortiOS GUI. It offers tools that are available in FortiOS, but with more GUI elements to help improve user experience.

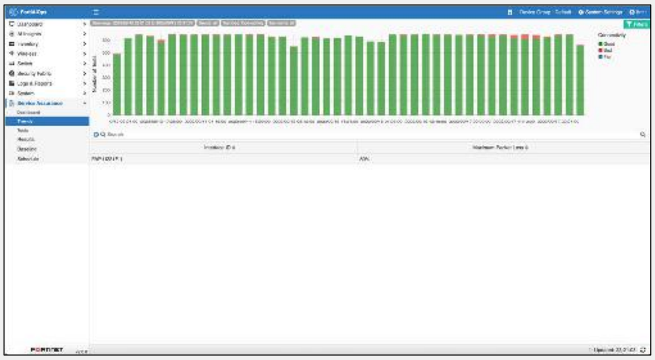
FortiAIOps Single-Pane Management

- Offers unified LAN and WAN edge monitoring and troubleshooting using AI-powered insights
- Single-pane management with GUI aligned to Fortinet GUI experience
- Historical data and trends with drill-down data
- SAM predictive diagnostics

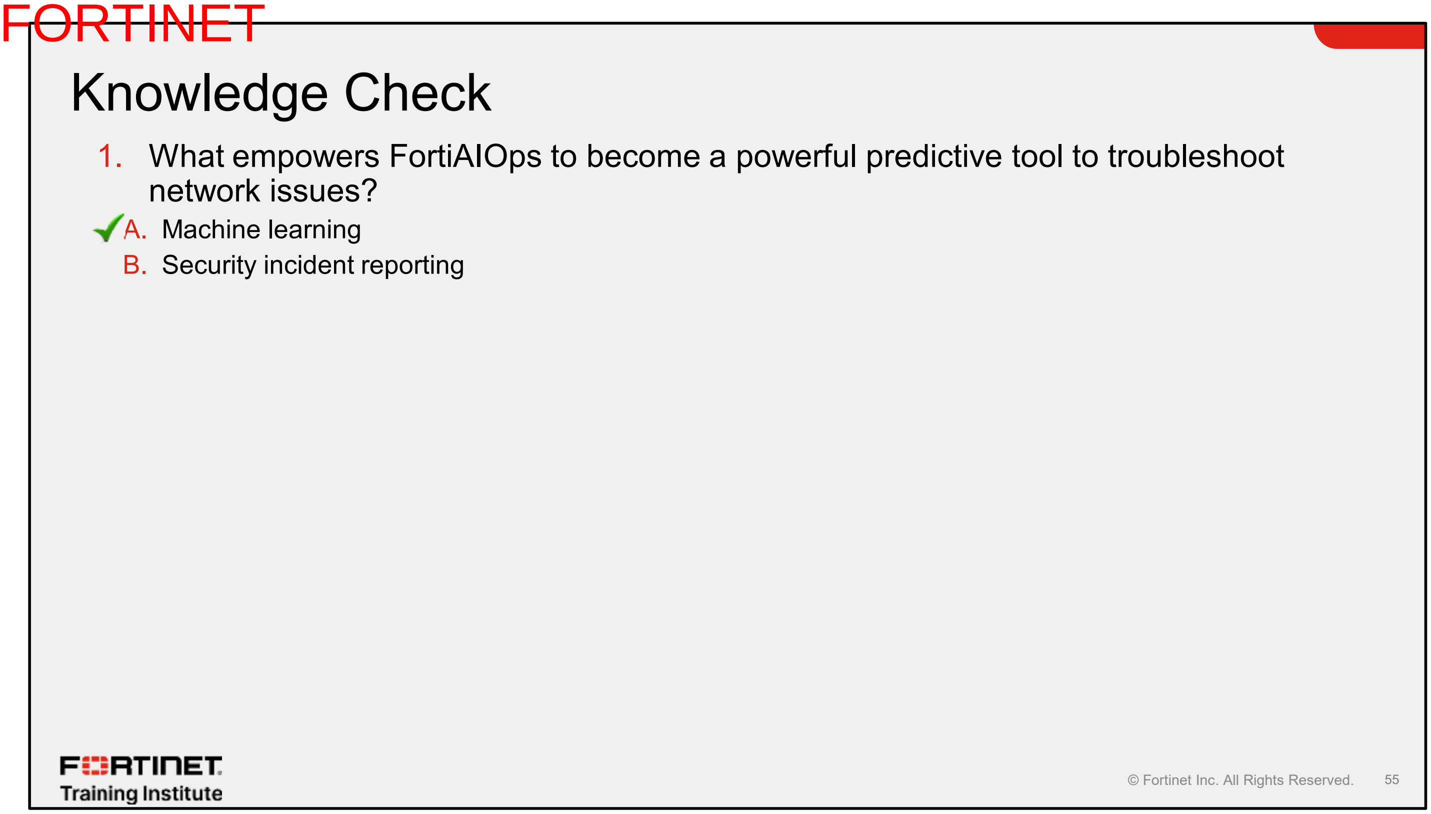
FortiAIOps single-pane management provides unified monitoring and troubleshooting for both LAN and WAN edges, leveraging AI-powered insights. It offers a single-pane management interface with a GUI aligned to the Fortinet experience. Additionally, users can access historical data and trends, along with drill-down capabilities, and benefit from Service Assurance Manager (SAM) predictive diagnostics.

FortiAIOps Wireless SAM

- Proactive baseline monitoring
- Schedule measurement and threshold testing
  - Evaluate connectivity
  - Measure throughput
- Support FortiGate managing FortiAP devices



FortiAIOps wireless SAM offers proactive baseline monitoring. You can schedule performance measurements to evaluate connectivity and throughput of FortiAP devices. FortiAIOps supports the FortiGate wireless controller in managing compatible FortiAP devices.



Knowledge Check

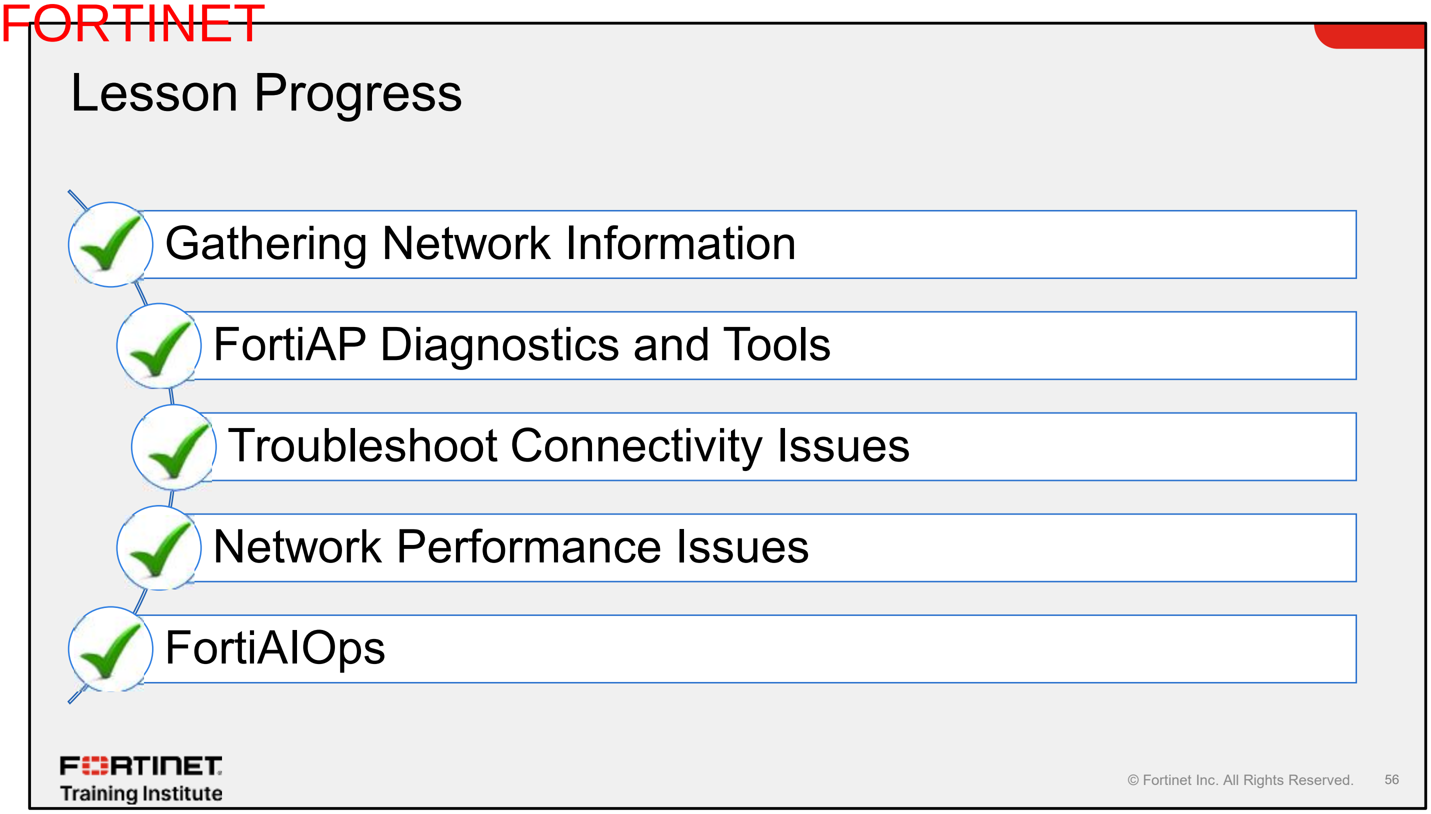
1. What empowers FortiAIOps to become a powerful predictive tool to troubleshoot network issues?

✓ A. Machine learning

B. Security incident reporting

FORTINET Training Institute

55



Lesson Progress

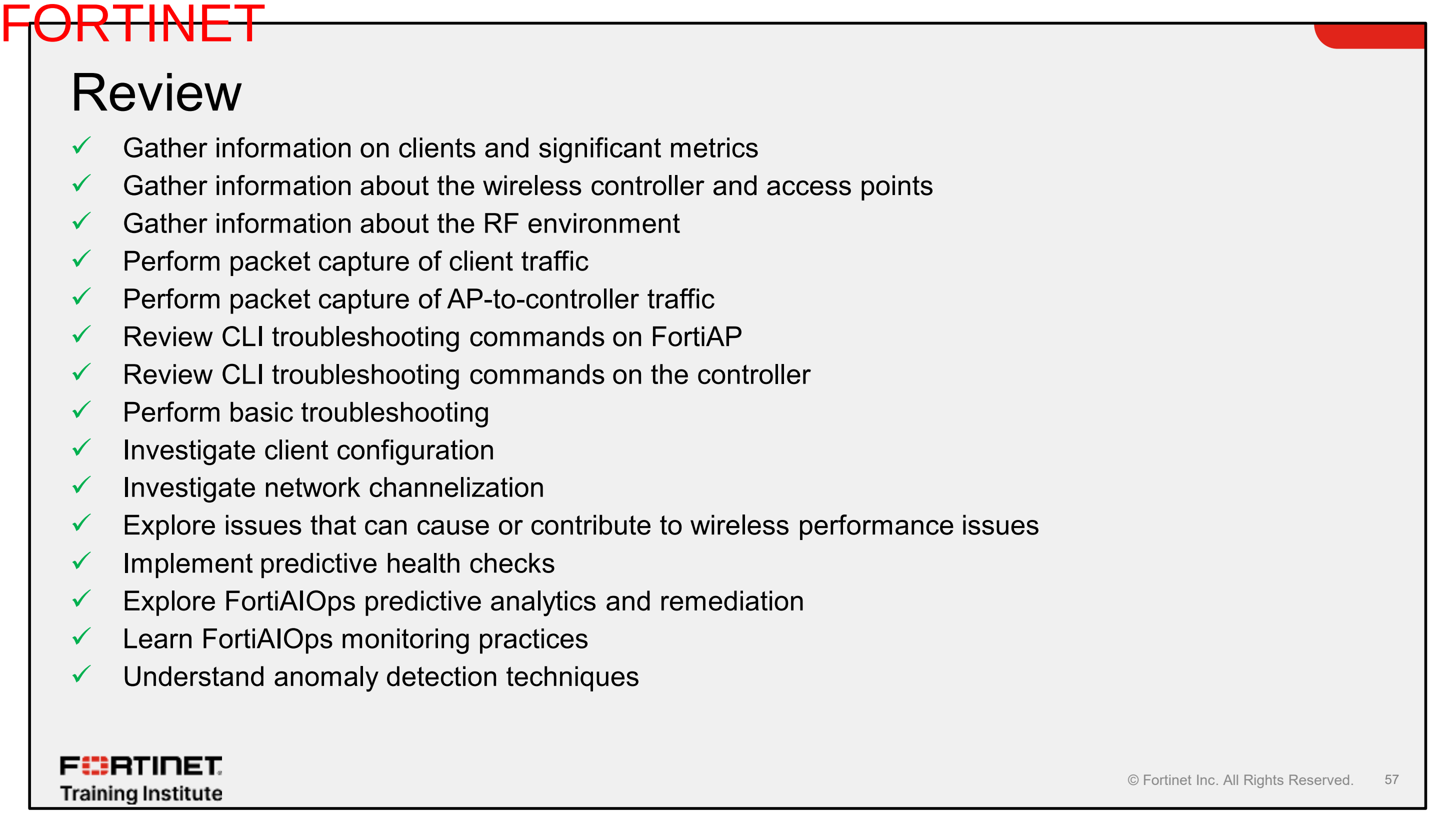
- ✓ Gathering Network Information
- ✓ FortiAP Diagnostics and Tools
- ✓ Troubleshoot Connectivity Issues
- ✓ Network Performance Issues
- ✓ FortiAIOps

FURTINET Training Institute

56

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.



Review

- ✓ Gather information on clients and significant metrics
- ✓ Gather information about the wireless controller and access points
- ✓ Gather information about the RF environment
- ✓ Perform packet capture of client traffic
- ✓ Perform packet capture of AP-to-controller traffic
- ✓ Review CLI troubleshooting commands on FortiAP
- ✓ Review CLI troubleshooting commands on the controller
- ✓ Perform basic troubleshooting
- ✓ Investigate client configuration
- ✓ Investigate network channelization
- ✓ Explore issues that can cause or contribute to wireless performance issues
- ✓ Implement predictive health checks
- ✓ Explore FortiAIOps predictive analytics and remediation
- ✓ Learn FortiAIOps monitoring practices
- ✓ Understand anomaly detection techniques

FORTINET Training Institute

57

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about troubleshooting tools and commands and collect information of the wireless network.

FORTINET®