FortiWiFi and FortiAP - Cookbook

Version 6.2

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-09-17	Initial release
2019-10-09	Updated to include Configuring wildcard address in captive portal walled garden on page 24.
2020-04-06	Updated to include Remote AP setup on page 68.
2021-03-26	Updated 1+1 fast failover between FortiGate WiFi controllers on page 78.
2021-04-21	Updated Deploying WPA2-Personal SSID to FortiAP units on page 27 and Deploying WPA2-Enterprise SSID to FortiAP units on page 30.
2021-10-25	Updated WiFi with WSSO using Windows NPS and user groups on page 45.
2021-11-02	Updated 1+1 fast failover between FortiGate WiFi controllers on page 78.
2024-02-23	Updated Direct SNMP monitor on page 57.

FortiAP / FortiWiFi cookbook

This guide contains topics about configuring FortiAP and FortiWiFi devices:

FortiAP management

This section contains topics about FortiAP management in FortiOS.

Configuring the FortiGate interface to manage FortiAP units

This guide describes how to configure a FortiGate interface to manage FortiAPs.
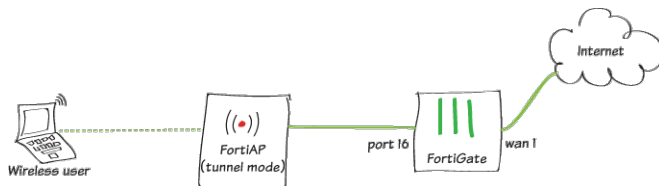
Based on the above topology, this example uses port16 as the interface used to manage connection to FortiAPs.

1. You must enable a DHCP server on port16:
    a. In FortiOS, go to *Network > Interfaces*.
    b. Edit port16.
    c. In the *IP/Network Mask* field, enter an IP address for port16.
    d. Enable *DHCP Server*, keeping the default settings.
2. If required, you can enable the VCI-match feature using the CLI. When VCI-match is enabled, only devices with a VCI name that matches the preconfigured string can acquire an IP address from the DHCP server. To configure VCI-match, run the following commands:
```
config system dhcp server
    edit 1
        set interface port16
        set vci-match enable
        set vci-string "FortiAP"
    next
end
```
3. As it is a minimum management requirement that FortiAP establish a CAPWAP tunnel with the FortiGate, you must enable CAPWAP access on port16 to allow it to manage FortiAPs:
    a. Go to *Network > Interfaces*.
    b. Double-click port16.
    c. Under *Administrative Access*, select *Security Fabric Connection*.
    d. Click *OK*.
4. To create a new FortiAP entry automatically when a new FortiAP unit is discovered, run the following command. By default, this option is enabled.

```
config system interface
   edit port16
      set allow-access fabric
      set ap-discover enable
   next
end
```

5. To allow FortiGate to authorize a newly discovered FortiAP to be controlled by the FortiGate, run the following command. By default, this option is disabled.
```
config system interface
   edit port16
      set allow-access fabric
      set auto-auth-extension-device enable
   next
end
```

Discovering, authorizing, and deauthorizing FortiAP units

Discovering a FortiAP unit

For a FortiGate acting as an AP controller (AC) to discover a FortiAP unit, the FortiAP must be able to reach the AC. A FortiAP with the factory default configuration has various ways of acquiring an AC's IP address to reach it.

AC discovery type	Description
Auto	The FortiAP attempts to be discovered in the below ways sequentially within an endless loop.
Static	The FortiAP sends discover requests to a preconfigured IP address that an AC owns.
DHCP	The FortiAP acquires the IP address of an AC in DHCP option 138 (the factory default) of a DHCP offer, which the FortiAP acquires its own IP address from.
DNS	The FortiAP acquires the AC's IP address by resolving a preconfigured FQDN.

AC discovery type	Description
FortiCloud	FortiGate Cloud discovers the FortiAP.
Broadcast	FortiAP is discovered by sending broadcasts in its local subnet.
Multicast	FortiAP is discovered by sending discovery requests to a multicast address of 224.0.1.140, which is the factory default.

AC actions when a FortiAP attempts to get discovered

Enable `ap-discover` on the AC for the interface designed to manage FortiAPs:

```
config system interface
   edit "lan"
      set ap-discover enable
   next
end
```

The `ap-discover` command allows the AC to create an entry in the managed FortiAPs table when it receives the FortiAP's discovery request. The `ap-discover` command is enabled by default. When the FortiAP entry is created automatically, it is marked as *discovered* status, and is pending for an administrator's authorization, unless the following setting is present:

```
config system interface
    edit "lan"
        set auto-auth-extension-device enable
    next
end
```

The `auto-auth-extension-device` command will allow AC authorize an new discovered FortiAP automatically without an administrator's manual authorization operation. The `auto-auth-extension-device` command is disabled by default.

Authorize a discovered FortiAP

Once the FortiAP discovery request is received by AC, an FortiAP entry will be added to the managed FortiAP table, and shown on *GUI > Managed FortiAP* list page.

"Status" showing "Waiting for Authorization"

To authorize the specific AP, click to select the FortiAP entry, then click *Authorize* button on the top of the table or *Authorize* entry in the pop-out menu.

Through GUI, authorization can also be done in FortiAP detail panel, under *Action* menu.

The authorization can also be done through CLI with follow commands.

```
config wireless-controller wtp
    edit "FP423E3X16000320"
        set admin enable
    next
end
```

De-authorize a managed FortiAP

To de-authorize a managed FortiAP, click to select the FortiAP entry, then click *Deauthorize* button on the top of the table or *Deauthorize* entry in the pop-out menu.

Through GUI, de-authorization can also be done in the FortiAP detail panel, under the *Action* menu.
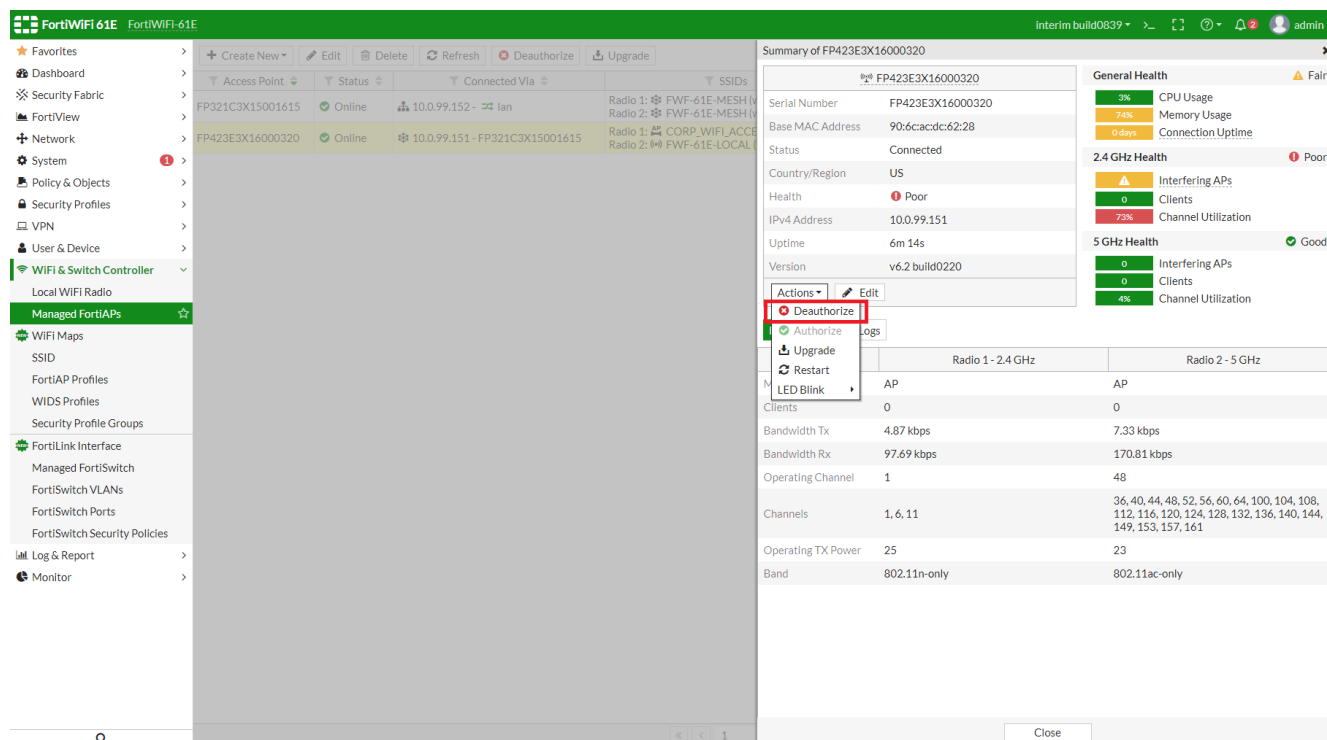
The de-authorization can also be done through CLI with follow commands.

```
config wireless-controller wtp
    edit "FP423E3X16000320"
        set admin discovered
    next
end
```

Extended details on FortiAP drill down

This function provides extended details of a FortiAP. On the *Managed FortiAPs* page, you can drill down to view all available details of a FortiAP, including:

- FortiAP system information.
- Dynamic health and performance information.
- Dynamic radio and client details.
- Relevant links such as location of the FortiAP in the location map.

Sample topology
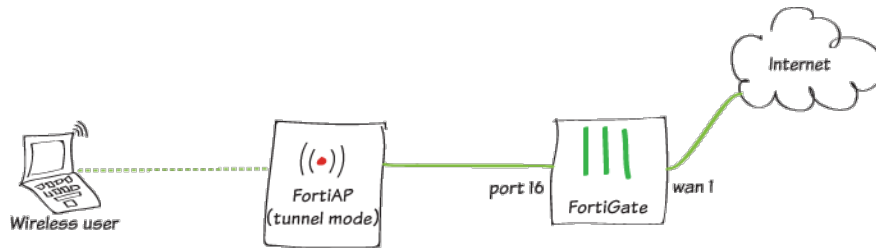
Sample configuration

In *WiFi & Switch Controller > Managed FortiAPs*, right-click a FortiAP and select *Drill Down to Details*.

The details pane includes the following information:

- The top left shows a summary of configuration and connection status for the AP. The *Actions* button provides some actions to the AP such as Authorize/Deauthorize, Upgrade, Restart, and LED Blink. The *Edit* button opens the *Managed FortiAP* page.
- The top right shows the *General Health* assessment of the AP and the health assessment based on radio band.
- The *Locate* button appears if the FortiAP is on a WiFi Map.
- The bottom section includes tabs to show the *Radios* summary, *Clients* list, and a filtered *Logs* view of all logs of the FortiAP.

If a FortiAP is on a WiFi Map, click the *Locate* button and that FortiAP is highlighted with a flashing yellow circle on the WiFi Map.

Click *Edit* to open the *Managed FortiAP* page to show the FortiAP's operation information and a summary of its health status. Click *View More Details* to open the details pane.

On the WiFi Map, click a FortiAP icon to open its details pane.

Setting up a mesh connection between FortiAP units

To set up a WiFi mesh connection, a minimum of three devices are required:

1. A FortiGate as the AP Controller (AC)
2. A FortiAP as the Mesh Root AP (MRAP)
3. A FortiAP as a Mesh Leaf AP (MLAP).
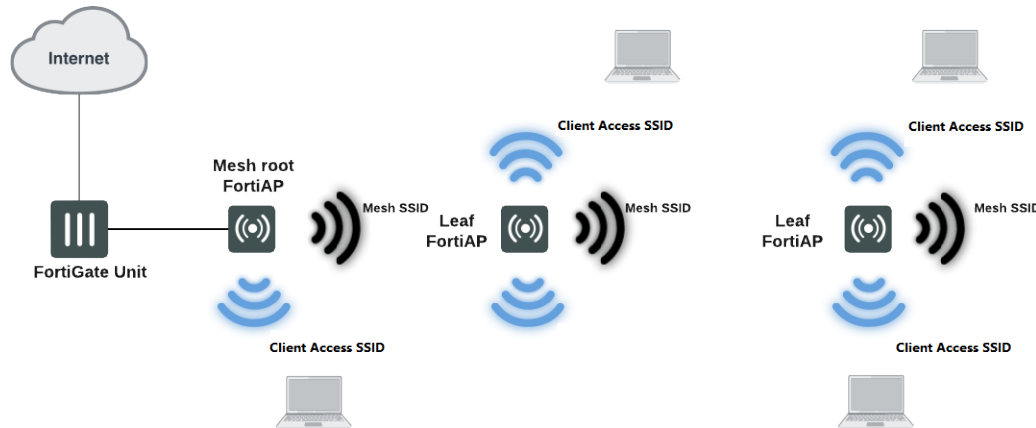
Configuring the AC

These instructions assume that the MRAP is already being managed by the AC (see Configuring the FortiGate interface to manage FortiAP units on page 7 and Discovering, authorizing, and deauthorizing FortiAP units on page 8).

To configure the AC:

1. Go to *WiFi & Switch Controller > SSID* and create a mesh SSID.
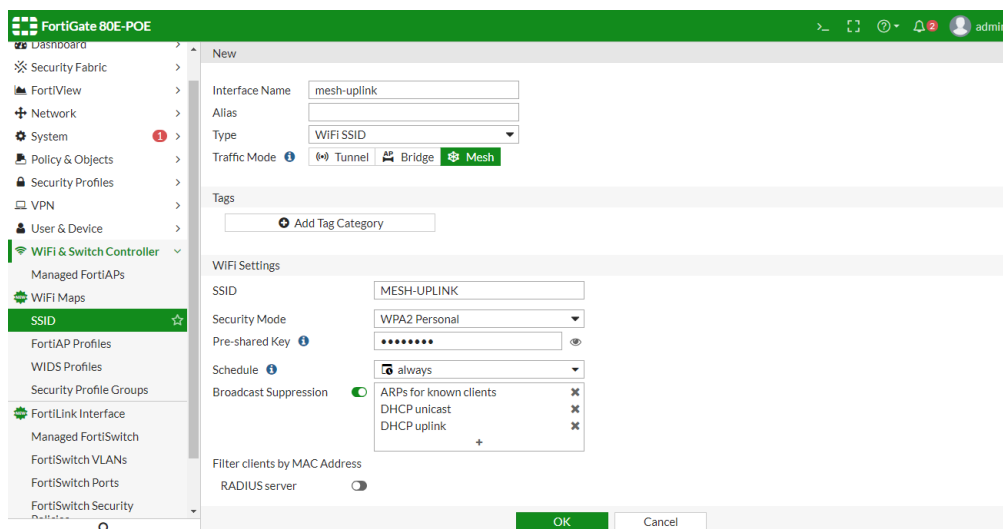
2. Go to *WiFi & Switch Controller > Managed FortiAPs*, edit the MRAP, and assign the mesh SSID to the MRAP, and

wait for a connection.
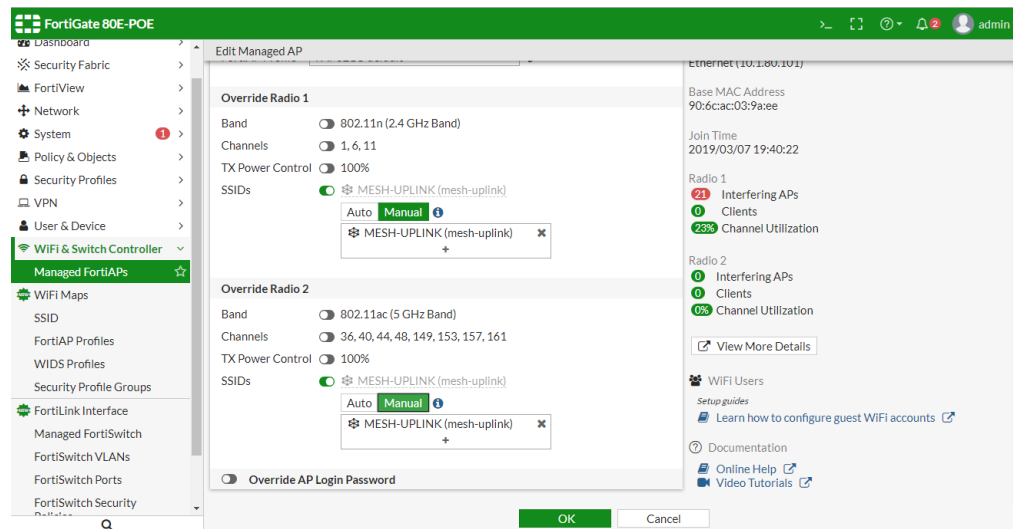
Configuring the MLAP

The MLAP can be configured to use the mesh link as its Main uplink or a Backup link for Ethernet connections.

To configure the MLAP:

1. On the FortiAP, go to *Connectivity*.
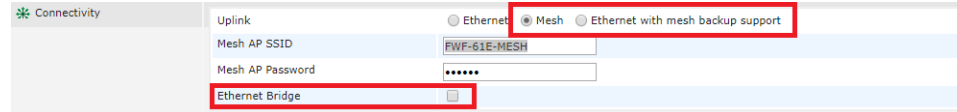
2. Set *Uplink* to *Mesh* or *Ethernet with mesh backup support*.
3. Enter a mesh SSID and password.
4. Optionally, select *Ethernet Bridge* (see Main uplink on page 18). This option is not available if *Uplink* is set to *Ethernet with mesh backup support*.

Once the MLAP has joined the AC, it can be managed in the same way as a wired AP.

A mesh SSID can also be assigned to an MLAP for other downstream MLAPs, creating a multi-hop WiFi mesh network. The maximum hop count has a default value of 4, and can be configured in the FAP console with the following commands:

```
cfg -a MESH_MAX_HOPS=n
cfg -c
```

Main uplink

When a mesh link is set as the main uplink of the MLAP, the Ethernet port on the MLAP can be set up as a bridge to the mesh link. This allows downstream wired devices to use the mesh link to connect to the network.
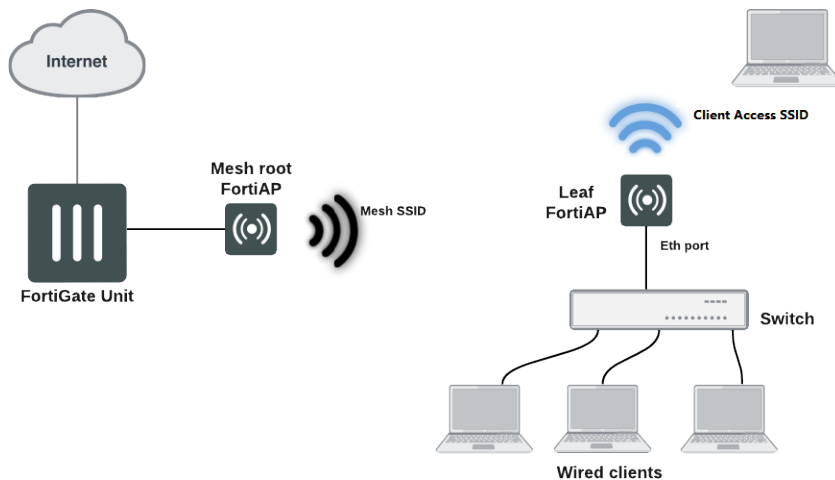
To enable a mesh Ethernet bridge, select *Ethernet Bridge* in the FortiAP *Connectivity* section in the GUI, or use the following console commands:

```
cfg -a MESH_ETH_BRIDGE=1
cfg -c
```

Backup link for Ethernet connections

When a mesh link is set to be the backup link for an Ethernet connection, the mesh link will not be established unless the Ethernet connection goes offline. When a mesh link is in this mode, the Ethernet port cannot be used as a bridge to the mesh link.

Data channel security: clear-text, DTLS, and IPsec VPN

After the AP joins, a CAPWAP tunnel is established between the FortiGate and FortiAP.

There are two channels inside the CAPWAP tunnel:

- The control channel for managing traffic, which is always encrypted by DTLS.
- The data channel for carrying client data packets, which can be configured to be encrypted or not.

The default setting for `dtls-policy` is `clear-text`, meaning it is non-encrypted. There are two settings available to encrypt the data channel: `dtls-enabled` and `ipsec-vpn`:

```
config wireless-controller wtp-profile
    edit "FortiAP-profile-name"
        set dtls-policy clear-text|dtls-enabled|ipsec-vpn
    next
end
```

Of the three settings, `clear-text` has the highest possible data throughput. Furthermore, FortiGates with hardware acceleration chips can offload CAPWAP data traffic in `clear-text` and achieve much higher throughput performance.

> You can only configure the data channel using the CLI.

When data security is not a major concern, we recommend that you set the data channel to non-encrypted. For example, when the FortiGate and FortiAP are operating in an internal network.

To set the data channel to non-encrypted using the CLI:

```
config wireless-controller wtp-profile
    edit "FortiAP-profile-name"
        set dtls-policy clear-text
    next
end
```

Encrypting the data channel

When the FortiGate and FortiAP are in different networks, and the data channel might transit through a public network, we recommend that you encrypt the data channel to protect your data with either DTLS or IPsec VPN.

DTLS

To encrypt the data channel with DTLS using the CLI:

```
config wireless-controller wtp-profile
    edit "FortiAP-profile-name"
        set dtls-policy dtls-enabled
        set dtls-in-kernel disable|enable
    next
end
```

`set dtls-in-kernel` is only available after `dtls-policy` is set to `dtls-enabled`. When you enable `dtls-in-kernel`, the FortiAP OS kernel processes the traffic encryption and decryption, which could provide better throughput performance. DTLS encryption cannot be hardware-accelerated on the FortiGate so when DTLS is enabled, data throughput performance is significantly lower than with `clear-text`.

IPsec VPN

To encrypt the data channel with IPsec VPN using the CLI:

```
config wireless-controller wtp-profile
    edit "FortiAP-profile-name"
        set dtls-policy ipsec-vpn
    next
end
```

This automatically establishes an IPsec VPN tunnel between the FortiGate and FortiAP that carries CAPWAP data packets. FortiGates with NP6 chips can offload CAPWAP data traffic in IPsec, so this encryption option has better throughput performance than DTLS. Because there is no built-in hardware acceleration chip, the FortiAP is considered the performance bottleneck in this scenario.

SSID authentication

This section contains the following topics about SSID authentication:

Replacing WiFi certificate

You can replace the built-in WiFi certificate with one you upload.

> These instruction apply to FortiWiFi devices using internal WiFi radios and FortiGate/FortiWiFi devices configured as WiFi Controllers that are managing FortiAP devices, and have WiFi clients that are connected to WPA2-Enterprise SSID and authenticated with local user groups.

On FortiOS, the built-in *Fortinet_Wifi* certificate is a publicly signed certificate that is only used in WPA2-Enterprise SSIDs with local user-group authentication. The default WiFi certificate configuration is:

```
config system global
    set wifi-ca-certificate "Fortinet_Wifi_CA"
    set wifi-certificate "Fortinet_Wifi"
end
```

Consider the following factors:

- The *Fortinet_Wifi* certificate is issued to *Fortinet Inc.* with common name (CN) *auth-cert.fortinet.com*. If a company or organization requires their own CN in their WiFi deployment, they must replace it with their own certificate.
- The *Fortinet_Wifi* certificate has an expiry date. When it expires, it must be renewed or replaced with a new certificate.

To replace a WiFi certificate:

1. Get new certificate files, including a root CA certificate, a certificate signed by the CA, and the corresponding private key file.
   You can purchase a publicly signed certificate from a commercial certificate service provider or generate a self-signed certificate.

2. Import the new certificate files into FortiOS:

    a. In FortiGate, go to *System > Certificates*.
        If VDOMs are enabled, go to *Global > System > Certificates*.

    b. Click *Import > CA Certificate*.

    c. Set the *Type* to *File* and upload the CA certificate file from the management computer.
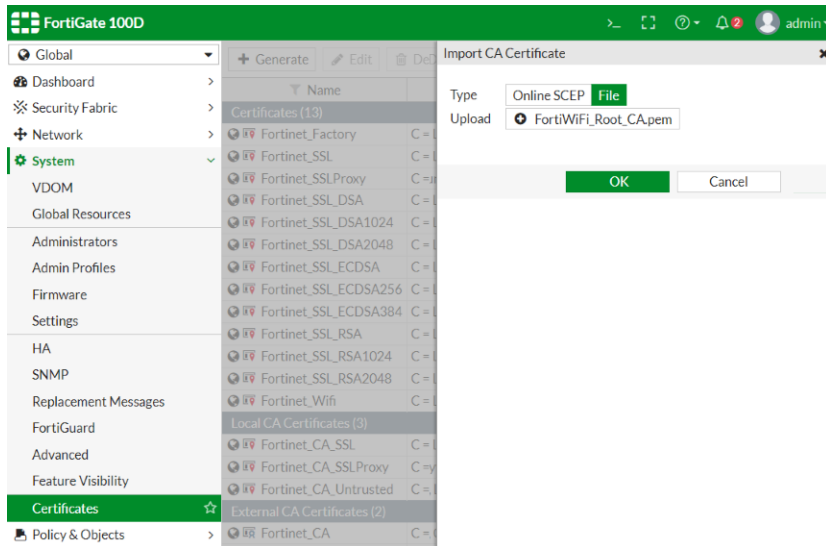
    d. Click *OK*.
        The imported CA certificate is named *CA_Cert_N* or *G_CA_Cert_N* when VDOMs are enabled, where *N* starts from *1* and increments for each imported certificate, and *G* stands for global range.

    e. Click *Import > Local Certificate*.

    f. Set the *Type* to *Certificate*, upload the certificate file and key file, enter the password, and enter the certificate name.
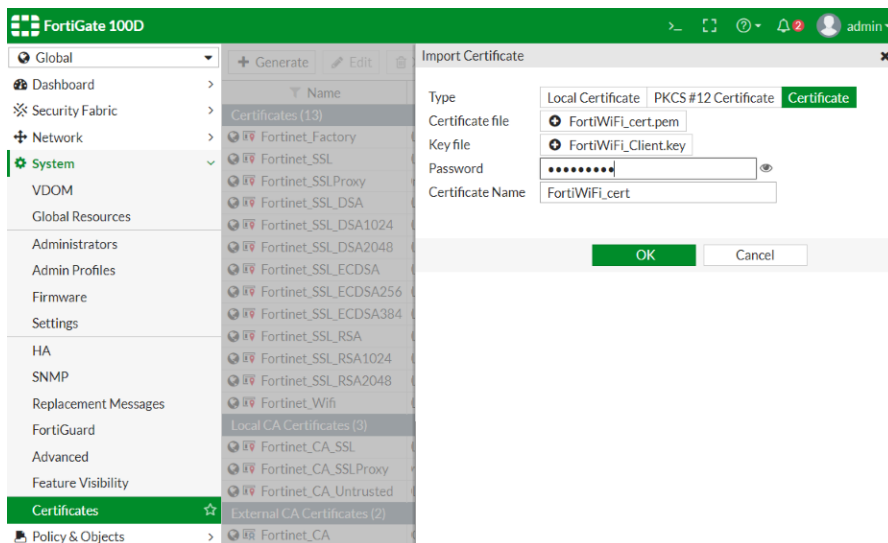
    g. Click *OK*.
        The imported certificates are listed on the *Certificates* page.

3. Change the WiFi certificate settings:

    a. Go to *System > Settings* and scroll down to the *WiFi Settings* section.

    b. In the *WiFi certificate* dropdown menu, select the imported local certificate.

c. In the *WiFi CA certificate* dropdown menu, select the imported CA certificate.

d. Click *Apply*.

To replace a WiFi certificate using the CLI:

```
config system global
    set wifi-ca-certificate <name of the imported CA certificate>
    set wifi-certificate <name of the imported certificate signed by the CA>
end
```

To restore the factory default WiFi certificates using the CLI:

```
config system global
    set wifi-ca-certificate "Fortinet_CA"
    set wifi-certificate "Fortinet_Factory"
end
```

As the factory default certificates are self-signed, WiFi clients need to accept it at the connection prompt or import the *Fortinet_CA* certificate to validate it.

Additional Information

The *Fortinet_Wifi* certificate can be updated automatically through the FortiGuard service certificate bundle update.

If the built-in *Fortinet_Wifi* certificate has expired and not been renewed or replaced, WiFi clients can still connect to the WPA2-Enterprise SSID with local user-group authentication by ignoring any warning messages or bypassing *Validate server certificate* (or similar) options.

Configuring wildcard address in captive portal walled garden

This topic describes how to add and apply wildcard domain names to the walled garden of captive-portal SSID.

Captive portal SSID supports the walled garden function where WiFi clients can access preconfigured hostnames and addresses that are exempted from portal authentication.

You can configure FQDN entries using wildcard domain names, for example, `*.google.*`, `*.facebook.com`, and so on, so that one entry can have multiple matches.

Sample topology
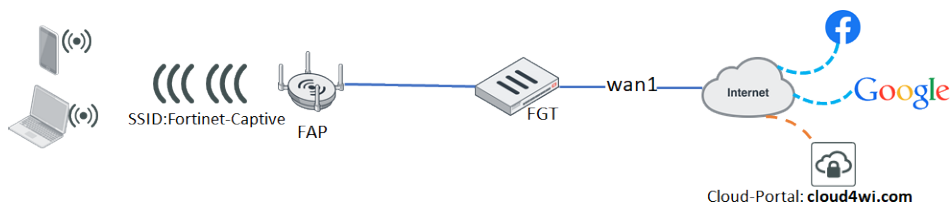
This example uses the wildcard address feature in the following ways:

- A tunnel mode captive portal works with the third-party cloud based portal server **cloud4wi.com**.
- Connected wireless clients can access Facebook and Google websites directly even before firewall authentication via FortiGate.
- Connected wireless clients opens the portal page of cloud4wi.com and can access other Internet resources as soon as they pass authentication by FortiGate.

Sample configuration

To create the wildcard FQDN address using the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. In the *New Address* page, enter the address *Name*, for example, *facebook* and *google*.
3. For *Type*, select *FQDN*.
4. For *FQDN*, enter a wildcard FQDN name, for example **.facebook.com* and **.google.**.
5. Click *OK*.

This wildcard FQDN type firewall address is different from entries in *Policy & Objects > Wildcard FQDN Addresses* that cannot be used directly in firewall policy source or destination addresses.

To create a third-party cloud portal server address using the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. In the *New Address* page, enter the address *Name*, for example, *cloud-portal*.
3. For *Type*, select *FQDN*.
4. For *FQDN*, enter the FQDN name, for example, *cloud4wi.com*.
5. Click *OK*.

To create a captive portal VAP with the third-party cloud portal server using the GUI:

1. Go to *WiFi & Switch Controller > SSID* and select *Create New > SSID*.
2. In the *New* page, enter an *Interface Name*, for example, *wifi-vap*.
3. For *Traffic Mode*, select *Tunnel*.
4. In the *Address* section, enter the *IP/Network Mask*, for example, *10.10.80.1/24*.
5. Optionally, you can change the DHCP *Address Range* in the *DHCP Server* section.
6. In the *WiFi Settings* section:
    a. Enter the *SSID* name, for example, *Fortinet-Captive*.
    b. For *Security Mode*, select *Captive Portal*.
    c. For *Portal Type*, select *Authentication*.
    d. For *Authentication Portal*, select *External* and enter *cloud4wi.com*.
    e. Click *User Groups* and select the created user group, for example, *group-local*; or click *Create* to create a new user group.
7. Click *OK*.

To support a third-party cloud portal, use one of the following methods.

To support a third-party cloud portal using Exempt Destinations/Services using the GUI:

1. Go to *WiFi & Switch Controller > SSID*.
2. Select the SSID you created, for example, *Fortinet-Captive* and click *Edit*.
3. In the *WiFi Settings* section, click *Exempt Destinations/Services*.
4. In the *Select Entries* pane *Address* list, select the wildcard FQDN addresses, for example, *facebook* and *google*, and the cloud portal address, for example, *cloud-portal*.
5. Still in the *Select Entries* pane, click *Service* and select *HTTP*, *HTTPS*, and *DNS*.
6. Click *OK*.

To support a third-party cloud portal using IPv4 policy using the GUI:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Enter the *Name*, for example, *Exempt Service*.
3. Click *Incoming Interface* and select *wifi-vap*.
4. Click *Outgoing Interface* and select *wan1*.
5. Click *Source* and select *all*.
6. Click *Destination* and select the wildcard FQDN addresses, for example, *facebook* and *google*, and the cloud portal address, for example, *cloud-portal*.
7. Click *Service* and select *HTTP*, *HTTPS*, and *DNS*.
8. Click *OK*.
9. Use CLI commands to enable `captive-portal-exempt`. In this example, the `policy_id` is 2.

```
config firewall policy
  edit 2
      set captive-portal-exempt enable
  next
end
```

To create the wildcard FQDN address using the CLI:

```
config firewall address
    edit "facebook"
      set type fqdn
      set fqdn "*.facebook.com"  <-- New support for "*" in fqdn address
    next
    edit "google"
      set type fqdn
      set fqdn "*.google.*"      <-- New support for "*" in fqdn address
    next
end
```

To create a third-party cloud portal server address using the CLI:

```
config firewall address
    edit "cloud-portal"
      set type fqdn
      set fqdn "cloud4wi.com"
    next
end
```

To create a tunnel mode captive portal VAP with the third-party cloud portal server using the CLI:

```
config wireless-controller vap
    edit "wifi-vap"
        set ssid "Fortinet-Captive"
        set security captive-portal
        set external-web "cloud4wi.com"
        set selected-usergroups "group-local"
        set intra-vap-privacy enable
    next
end
```

To create security-exempt-list and select it in vap using the CLI:

```
config user security-exempt-list
    edit "wifi-vap-exempt-list"
        config rule
            edit 1
                set dstaddr "facebook" "google" "cloud-portal"
                set service "HTTP" "HTTPS" "DNS"
            next
        end
end
config wireless-controller vap
    edit "wifi-vap"
        set security-exempt-list "wifi-vap-exempt-list"
    next
end
```

To create a captive-portal-exempt firewall policy and move it before the regular outgoing policy using the CLI:

```
config firewall policy
    edit 2
        set name "Exempt Service"
        set srcintf "wifi-vap"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "cloud-portal" "facebook" "google"
        set action accept
        set schedule "always"
        set service "DNS" "HTTP" "HTTPS"
        set captive-portal-exempt enable
        set nat enable
    next
    edit 1
        set name "outgoing"
        set srcintf "wifi-vap"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    move 2 before 1
end
```

Although `destination-hostname-visibility` is enabled by default, ensure this setting is enabled so that FQDN addresses can be resolved.

To enable destination-hostname-visibility:

```
config system network-visibility
    set destination-hostname-visibility enable
end
```

Deploying WPA2-Personal SSID to FortiAP units

This topic provides simple configuration instructions for deploying WPA2-Personal SSID with FortiAP. The steps include creating an SSID, selecting the SSID for the FortiAP, and creating a policy from the SSID to the Internet.

The following shows a simple network topology for this recipe:
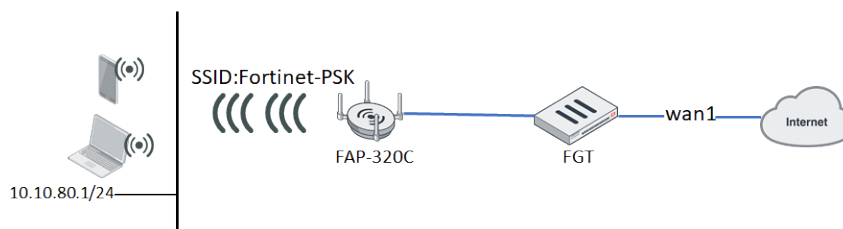
To deploy WPA2-Personal SSID to FortiAP units on the FortiWiFi and FortiAP GUI:

1. Create a WPA2-Personal SSID:
   a. Go to *WiFi & Switch Controller > SSID*, select *SSID*, then click *Create New*.
   b. Enter the desired interface name. For *Traffic mode*, select *Tunnel*.
   c. In the *Address > IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.
   d. In the *SSID* field, enter the desired SSID name. For *Security*, select *WPA2 Personal*.
   e. In the *Pre-Shared Key* field, enter the password. The password must be 8 to 63 characters long, or exactly 64 academical digits.
   f. Click *OK*.
2. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C. Do one of the following:
   a. Select the SSID by editing the FortiAP:
      i. Go to *WiFi & Switch Controller > Managed FortiAPs*. Select the FortiAP-320C and click *Edit*.
      ii. Ensure that *Managed AP Status* is *Connected*.
      iii. Under *WiFi Setting*, ensure that the configured FortiAP profile is the desired profile, in this case FAP320C-default. Click *Edit entry*.
      iv. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1 > SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.
      v. To broadcast the SSID from 5 G radio, scroll to *Radio 2 > SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.
      vi. Click *OK*.
   b. Select the SSID by editing the FortiAP profile:
      i. Go to *WiFi & Switch Controller > FortiAP Profile*. Select the FAP320C-default profile, then click *Edit*.
      ii. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
      iii. To broadcast the SSID from 5 G radio, scroll to *Radio 2 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
      iv. Click *OK*.
3. Create the SSID-to-Internet firewall policy:
   a. Go to *Policy & Objects > IPv4 Policy*, then click *Create New*.
   b. Enter the desired policy name.
   c. From the *Incoming Interface* dropdown list, select the source interface, such as wifi-vap.
   d. From the *Outgoing Interface* dropdown list, select the destination interface, such as wan1.
   e. In the *Source* and *Destination* fields, select all. In the *Service* field, select *ALL*. If desired, you can configure different values for these fields.
   f. Click *OK*.

To deploy WPA2-Personal SSID to FortiAP units using the FortiWiFi and FortiAP CLI:

1. Create a WPA2-Personal SSID:
   a. Create a VAP interface named "wifi-vap":
```
config wireless-controller vap
   edit "wifi-vap"
      set ssid "Fortinet-psk"
      set security wpa2-only-personal
      set passphrase fortinet
```

```
         next
      end
```

b. Configure an IP address and enable DHCP:

```
config system interface
   edit "wifi-vap"
      set ip 10.10.80.1 255.255.255.0
   next
end
config system dhcp server
   edit 1
      set dns-service default
      set default-gateway 10.10.80.1
      set netmask 255.255.255.0
      set interface "wifi-vap"
      config ip-range
         edit 1
            set start-ip 10.10.80.2
            set end-ip 10.10.80.254
         next
      end
      set timezone-option default
   next
end
```

2. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C:

```
config wireless-controller wtp
   edit "FP320C3X14000640"
      set admin enable
      set wtp-profile "FAP320C-default"
   next
end
config wireless-controller wtp-profile
   edit "FAP320C-default"
      config radio-1
         set vap-all disable
         set vaps "wifi-vap"
      end
      config radio-2
         set vap-all disable
         set vaps "wifi-vap"
      end
   next
end
```

3. Create the SSID-to-Internet firewall policy:

```
config firewall policy
   edit 1
      set name "WiFi to Internet"
      set srcintf "wifi-vap"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set fsso disable
      set nat enable
```

```
        next
    end
```

Deploying WPA2-Enterprise SSID to FortiAP units

This topic provides simple configuration instructions for deploying WPA2-Enterprise SSID with FortiAP. The steps include creating an SSID, selecting the SSID for the FortiAP, and creating a policy from the SSID to the Internet.

The following shows a simple network topology for this recipe:
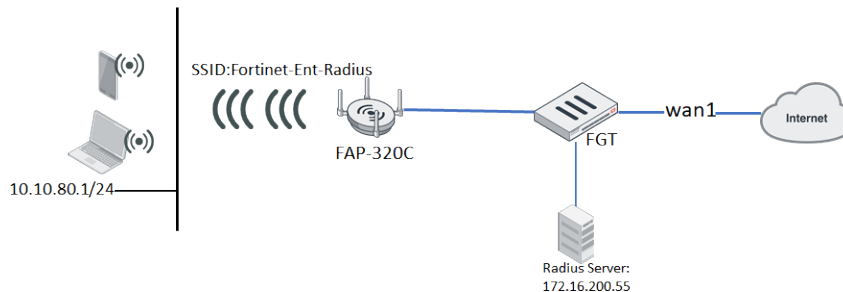
To deploy WPA2-Enterprise SSID to FortiAP units on the FortiWiFi and FortiAP GUI:

Create an SSID as WPA2-Enterprise. Do one of the following:

1. Create an SSID as WPA2-Enterprise with authentication from a RADIUS server:
   a. Create a RADIUS server:
      i. Go to *User & Device > RADIUS Servers*, then click *Create New*.
      ii. Enter a server name.
      iii. In the *Primary Server > IP/Name* field, enter the IP address or server name.
      iv. In the *Primary Server > Secret* field, enter the secret key.
      v. Click *Test Connectivity* to verify the connection with the RADIUS server.
      vi. Click *Test User Credentials* to verify that the user account can be authenticated with the RADIUS server.
      vii. Click *OK*.
   b. Create a WPA2-Enterprise SSID:
      i. Go to *WiFi & Switch Controller > SSID*, select *SSID*, then click *Create New*.
      ii. Enter the desired interface name. For *Traffic mode*, select *Tunnel*.
      iii. In the *Address > IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.
      iv. In the *SSID* field, enter the desired SSID name. For *Security*, select *WPA2 Enterprise*.
      v. In the *Authentication* field, select *RADIUS Server*. From the dropdown list, select the RADIUS server created in step i.
      vi. Click *OK*.
2. Create an SSID as WPA2-Enterprise with authentication from a user group:
   a. Create a user group:
      i. Go to *User & Device > User Groups*, then click *Create New*.
      ii. Enter the desired group name.
      iii. For *Type*, select *Firewall*.

> iv. For *Remote Groups*, click the + button. In the dropdown list, select the desired RADIUS server. Click *OK*.
>
> v. Click *OK*.

 b. Create a WPA2-Enterprise SSID:

> i. Go to *WiFi & Switch Controller > SSID*, select *SSID*, then click *Create New*.
>
> ii. Enter the desired interface name. For *Traffic mode*, select *Tunnel*.
>
> iii. In the *Address > IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.
>
> iv. In the *SSID* field, enter the desired SSID name. For *Security*, select *WPA2 Enterprise*.
>
> v. In the *Authentication* field, select *RADIUS Server*. From the dropdown list, select the RADIUS server created in step i.
>
> vi. Click *OK*.

Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C. Do one of the following:

1. Select the SSID by editing the FortiAP:

 a. Go to *WiFi & Switch Controller > Managed FortiAPs*. Select the FortiAP-320C and click *Edit*.

 b. Ensure that *Managed AP Status* is *Connected*.

 c. Under *WiFi Setting*, ensure that the configured FortiAP profile is the desired profile, in this case FAP320C-default. Click *Edit entry*.

 d. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1 > SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.

 e. To broadcast the SSID from 5 G radio, scroll to *Radio 2 > SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.

 f. Click *OK*.

2. Select the SSID by editing the FortiAP profile:

 a. Go to *WiFi & Switch Controller > FortiAP Profile*. Select the FAP320C-default profile, then click *Edit*.

 b. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.

 c. To broadcast the SSID from 5 G radio, scroll to *Radio 2 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.

 d. Click *OK*.

Create the SSID-to-Internet firewall policy:

1. Go to *Policy & Objects > IPv4 Policy*, then click *Create New*.
2. Enter the desired policy name.
3. From the *Incoming Interface* dropdown list, select the source interface, such as wifi-vap.
4. From the *Outgoing Interface* dropdown list, select the destination interface, such as wan1.
5. In the *Source* and *Destination* fields, select all. In the *Service* field, select *ALL*. If desired, you can configure different values for these fields.
6. Click *OK*.

To deploy WPA2-Enterprise SSID to FortiAP units using the FortiWiFi and FortiAP CLI:

1. Create a RADIUS server:
```
config user radius
```

```
        edit "wifi-radius"
            set server "172.16.200.55"
            set secret fortinet
        next
    end
```

2. Create a user group:
```
config user group
    edit "group-radius"
        set member "wifi-radius"
    next
end
```

3. Create a WPA2-Enterprise SSID:
   a. Create an SSID with authentication from the RADIUS server:
```
config wireless-controller vap
    edit "wifi-vap"
        set ssid "Fortinet-Ent-Radius"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "wifi-radius"
    next
end
```
   b. Create an SSID with authentication from the user group:
```
config wireless-controller vap
    edit "wifi-vap"
        set ssid "Fortinet-Ent-Radius"
        set security wpa2-only-enterprise
        set auth usergroup
        set usergroup "group-radius"
    next
end
```
   c. Configure an IP address and enable DHCP:
```
config system interface
    edit "wifi-vap"
        set ip 10.10.80.1 255.255.255.0
    next
end
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.10.80.1
        set netmask 255.255.255.0
        set interface "wifi-vap"
        config ip-range
            edit 1
                set start-ip 10.10.80.2
                set end-ip 10.10.80.254
            next
        end
        set timezone-option default
    next
end
```

4. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed
   FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C:
```
config wireless-controller wtp
    edit "FP320C3X14000640"
```

```
            set admin enable
            set wtp-profile "FAP320C-default"
        next
    end
    config wireless-controller wtp-profile
        edit "FAP320C-default"
            config radio-1
                set vap-all disable
                set vaps "wifi-vap"
            end
            config radio-2
                set vap-all disable
                set vaps "wifi-vap"
            end
        next
    end
```

5. Create the SSID-to-Internet firewall policy:

```
    config firewall policy
        edit 1
            set name "WiFi to Internet"
            set srcintf "wifi-vap"
            set dstintf "wan1"
            set srcaddr "all"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set service "ALL"
            set fsso disable
            set nat enable
        next
    end
```

Deploying captive portal SSID to FortiAP units

This topic provides simple configuration instructions for developing captive portal SSID with FortiAP. The steps include creating an SSID, selecting the SSID for the FortiAP, and creating a policy from the SSID to the Internet.

The following shows a simple network topology for this recipe:
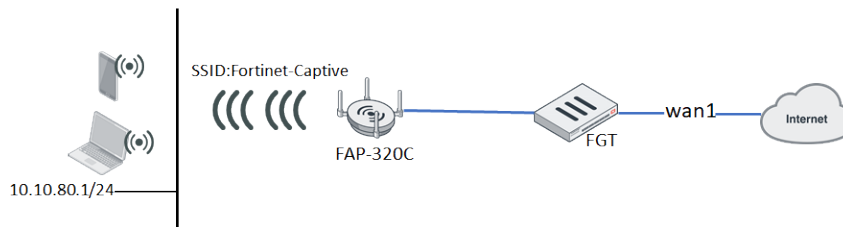
To deploy captive portal SSID to FortiAP units on the FortiWiFi and FortiAP GUI:

1. Create a local user:
    a. Go to *User & Device > User Definition*, then click *Create New*.
    b. In the *Users/Groups Creation Wizard,* select *Local User*, then click *Next*.

    c. Enter the desired values in the *Username* and *Password* fields, then click *Next*.

    d. On the *Contact Info* tab, fill in any information as desired, then click *Next.* You do not need to configure any contact information for the user.

    e. On the *Extra Info* tab, set the *User Account Status* to *Enabled*.

    f. If the desired user group already exists, enable *User Group*, then select the desired user group.

    g. Click *Submit*.

2. Create a user group:

    a. Go to *User & Device > User Groups*, then click *Create New*.

    b. Enter the desired group name.

    c. For *Type*, select *Firewall*.

    d. For *Members*, click the + button. In the dropdown list, select the local user created in step 1. Click *OK*.

    e. Click *OK*.

3. Create a captive portal SSID:

    a. Go to *WiFi & Switch Controller > SSID*, select *SSID*, then click *Create New*.

    b. Enter the desired interface name. For *Traffic mode*, select *Tunnel*.

    c. In the *Address > IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.

    d. In the *SSID* field, enter the desired SSID name. For *Captive Portal*, select *Security*.

    e. Configure the portal type as one of the following:

        i. For *Portal Type*, select *Authentication*. In the *User Group* dropdown list, select the user group created in step 2.

        ii. For *Portal Type*, select *Disclaimer + Authentication*. In the *User Group* dropdown list, select the user group created in step 2.

        iii. For *Portal Type*, select *Disclaimer Only*.

        iv. To configure the portal type as email collection, go to *System > Feature Visibility*, and enable *Email Collection*, then select *Email Collection* for *Portal Type*.

    f. Click *OK*.

4. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C. Do one of the following:

    a. Select the SSID by editing the FortiAP:

        i. Go to *WiFi & Switch Controller > Managed FortiAPs*. Select the FortiAP-320C and click *Edit*.

        ii. Ensure that *Managed AP Status* is *Connected*.

        iii. Under *WiFi Setting*, ensure that the configured FortiAP profile is the desired profile, in this case FAP320C-default. Click *Edit entry*.

        iv. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.

        v. To broadcast the SSID from 5 G radio, scroll to *Radio 2 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.

        vi. Click *OK*.

    b. Select the SSID by editing the FortiAP profile:

        i. Go to *WiFi & Switch Controller > FortiAP Profile*. Select the FAP320C-default profile, then click *Edit*.

        ii. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.

        iii. To broadcast the SSID from 5 G radio, scroll to *Radio 2 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.

        iv. Click *OK*.

5. Create the SSID-to-Internet firewall policy:

    a. Go to *Policy & Objects > IPv4 Policy*, then click *Create New*.

    b. Enter the desired policy name.

    c. From the *Incoming Interface* dropdown list, select the source interface, such as wifi-vap.

    d. From the *Outgoing Interface* dropdown list, select the destination interface, such as wan1.

    e. In the *Source* and *Destination* fields, select all. In the *Service* field, select *ALL*. If desired, you can configure different values for these fields.

    f. Click *OK*.

To deploy captive portal SSID to FortiAP units using the FortiWiFi and FortiAP CLI:

1. Create a local user:
```
config user local
   edit "local"
      set type password
      set passwd 123456
   next
end
```

2. Create a user group:
```
config user group
   edit "group-local"
      set member "local"
   next
end
```

3. Create a captive portal SSID. Do one of the following:

    a. Create a captive portal SSID with portal type *Authentication*:
```
config wireless-controller vap
   edit "wifi-vap"
      set ssid "Fortinet-Captive"
      set security captive-portal
      set portal-type auth
      set selected-usergroups "group-local"
   next
end
```

    b. Create a captive portal SSID with portal type *Disclaimer + Authentication*:
```
config wireless-controller vap
   edit "wifi-vap"
      set ssid "Fortinet-Captive"
      set security captive-portal
      set portal-type auth+disclaimer
      set selected-usergroups "group-local"
   next
end
```

    c. Create a captive portal SSID with portal type *Disclaimer Only*:
```
config wireless-controller vap
   edit "wifi-vap"
      set ssid "Fortinet-Captive"
      set security captive-portal
      set portal-type disclaimer
   next
end
```

    d. Create a captive portal SSID with portal type *Email Collection*:
```
config wireless-controller vap
```

```
        edit "wifi-vap"
            set ssid "Fortinet-Captive"
            set security captive-portal
            set portal-type email-collect
        next
    end
```

e. Configure an IP address and enable DHCP:

```
config system interface
    edit "wifi-vap"
        set ip 10.10.80.1 255.255.255.0
    next
end
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.10.80.1
        set netmask 255.255.255.0
        set interface "wifi-vap"
        config ip-range
            edit 1
                set start-ip 10.10.80.2
                set end-ip 10.10.80.254
            next
        end
        set timezone-option default
    next
end
```

4. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C:

```
config wireless-controller wtp
    edit "FP320C3X14000640"
        set admin enable
        set wtp-profile "FAP320C-default"
    next
end
config wireless-controller wtp-profile
    edit "FAP320C-default"
        config radio-1
            set vap-all disable
            set vaps "wifi-vap"
        end
        config radio-2
            set vap-all disable
            set vaps "wifi-vap"
        end
    next
end
```

5. Create the SSID-to-Internet firewall policy:

```
config firewall policy
    edit 1
        set name "WiFi to Internet"
        set srcintf "wifi-vap"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
```

```
        set schedule "always"
        set service "ALL"
        set fsso disable
        set nat enable
    next
end
```

Configuring quarantine on SSID

This topic provides instructions on simple configuration for on SSID. Consider the following for this feature:

- The quarantine function only works with SSID tunnel mode.
- The quarantine function is independent of SSID security mode.

The following shows a simple network topology for this recipe:
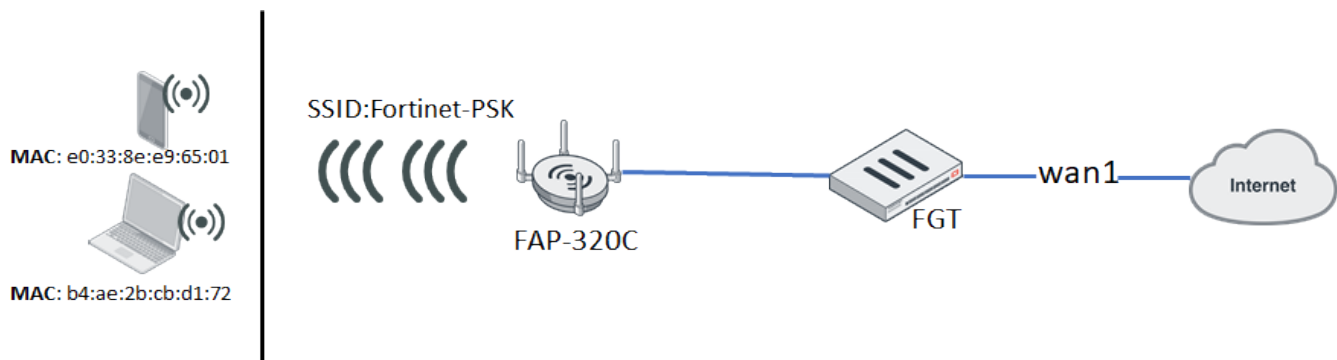
To quarantine a wireless client on the FortiWiFi and FortiAP GUI:

1. In FortiWiFi and FortiAP, go to the policy applied to the SSID and enable *All Sessions* for *Log Allowed Traffic*.
2. Edit the SSID:
   a. Go to WiFi & Switch Controller > SSID, and select the desired SSID.
   b. Enable *Device Detection*.
   c. Enable *Quarantine Host*.
   d. Click *OK*.
3. Quarantine a wireless client:
   a. Do one of the following:
      i. Go to *Security Fabric > Physical Topology*. View the topology by access device.
      ii. Go to *FortiView > Traffic from LAN/DMZ > Source*.
      iii. Go to *FortiView > Traffic from LAN/DMZ > WiFi Clients*.
   b. Right-click the wireless client, then click *Quarantine Host*.

To quarantine a wireless client using the FortiWiFi and FortiAP CLI:

1. Under global quarantine settings, enable quarantine:
   ```
   config user quarantine
       set quarantine enable
   end
   ```

2. Under virtual access point (VAP) settings, enable quarantine:

```
config wireless-controller vap
    edit wifi-vap
        set ssid "Fortinet-psk"
        set security wpa2-only-personal
        set passphrase fortinet
        set quarantine enable
    next
end
```

3. Quarantine a wireless client. The example client has the MAC address b4:ae:2b:cb:d1:72:

```
config user quarantine
    config targets
        edit "DESKTOP-Surface"
            config macs
                edit b4:ae:2b:cb:d1:72
                    set description "Surface"
                next
            end
        next
    end
end
```

Configuring MAC filter on SSID

Follow these instructions to enable MAC filter on SSID. Consider the following when using this function:

- The MAC filter function is independent of the SSID security mode.
- To enable MAC filter on SSID, first configure the wireless controller address and address group. See instructions below.

Sample topology
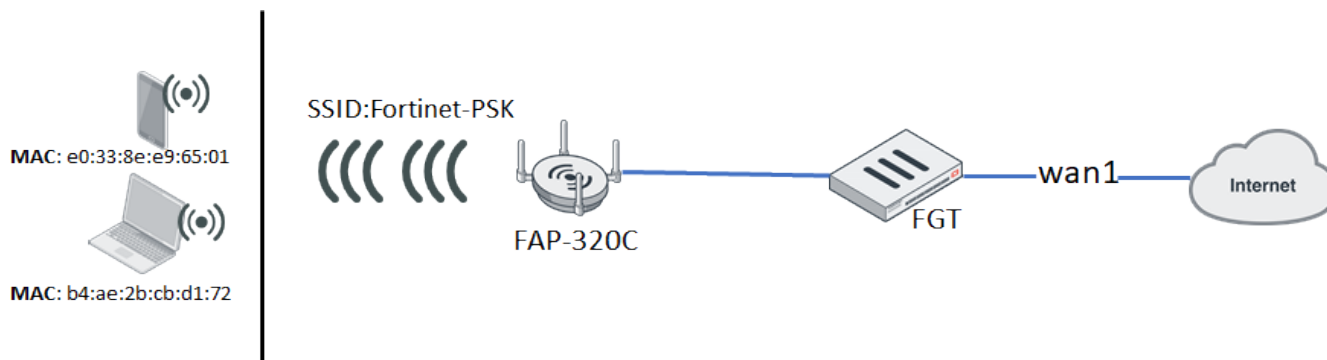
To block a specific client from connecting to the SSID using MAC filter:

1. Create a wireless controller address with the client MAC address and set the policy to deny. In this example, the client MAC address is b4:ae:2b:cb:d1:72.

```
config wireless-controller address
    edit "client_1"
```

```
        set mac b4:ae:2b:cb:d1:72
        set policy deny
    next
end
```

2. Create a wireless controller address group using the above address and set the default policy to allow.
```
config wireless-controller addrgrp
    edit mac_grp
        set addresses "client_1"
        set default-policy allow
    next
end
```

3. On the virtual access point (VAP), select the above address group.
```
config wireless-controller vap
    edit wifi-vap
        set ssid "Fortinet-psk"
        set security wpa2-only-personal
        set passphrase fortinet
        set address-group "mac_grp"
    next
end
```

After this configuration, the client (MAC address b4:ae:2b:cb:d1:72) is denied connecting to SSID `Fortinet-psk`. Other clients can connect, such as a client with MAC address e0:33:8e:e9:65:01.

To allow a specific client to connect to the SSID using MAC filter:

1. Create a wireless controller address with the same MAC address as the client and set the policy to allow. In this example, the client's MAC address is b4:ae:2b:cb:d1:72.
```
config wireless-controller address
    edit "client_1"
        set mac b4:ae:2b:cb:d1:72
        set policy allow
    next
end
```

2. Create a wireless controller address group using the above address and set the default policy to deny.
```
config wireless-controller addrgrp
    edit mac_grp
        set addresses "client_1"
        set default-policy deny
    next
end
```

3. On the virtual access point, select the above address group.
```
config wireless-controller vap
    edit wifi-vap
        set ssid "Fortinet-psk"
        set security wpa2-only-personal
        set passphrase fortinet
        set address-group "mac_grp"
    next
end
```

After this configuration, the client (MAC address b4:ae:2b:cb:d1:72) can connect to SSID `Fortinet-psk`. Other clients are denied from connecting, such as a client with MAC address e0:33:8e:e9:65:01.

WPA3 on FortiAP

WPA3 is supported by FortiGate devices running FortiOS 6.2.0 and later, and FortiAP-S and FortiAP-W2 device running 6.2.0 and later.

WPA3 Opportunistic Wireless Encryption (OWE), Simultaneous Authentication of Equals (SAE), and Enterprise are supported, including OWE and SAE transition mode.

To configure WPA3 OWE:

- WPA3 OWE only:
  Clients that support WPA3 can connect with this SSID.

```
config wireless-controller vap
    edit "80e_owe"
        set ssid "80e_owe"
        set security owe
        set pmf enable
        set schedule "always"
    next
end
```

- WPA3 OWE Transition:
  Clients connect with normal OPEN or OWE depending on its capability. Clients which support WPA3 connect with OWS standard. Clients which cannot support WPA3 connect with Open SSID.

```
config wireless-controller vap
    edit "80e_open"
        set ssid "80e_open"
        set security open
        set owe-transition enable
        set owe-transition-ssid "wpa3_open"
        set schedule "always"
    next
    edit "wpa3_owe_tr"
        set ssid "wpa3_open"
        set broadcast-ssid disable
        set security owe
        set pmf enable
        set owe-transition enable
        set owe-transition-ssid "80e_open"
        set schedule "always"
    next
end
```

To configure WPA3 SAE:

- WPA3 SAE:
  Clients that support WPA3 can connect with this SSID.

```
config wireless-controller vap
    edit "80e_sae"
        set ssid "80e_sae"
        set security wpa3-sae
        set pmf enable
```

```
            set schedule "always"
            set sae-password 12345678
        next
    end
```

- WPA3 SAE Transition:

  There are two passwords in the SSID. If *passphrase* is used, the client connects with WPA2 PSK. If *sae-password* is used, the client connects with WPA3 SAE.

```
config wireless-controller vap
    edit "80e_sae-tr"
        set ssid "80e_sae-transition"
        set security wpa3-sae-transition
        set pmf optional
        set passphrase 11111111
        set schedule "always"
        set sae-password 22222222
    next
end
```

To configure WPA3 Enterprise:

Using this option, you can select the `auth` type to use either RADIUS authentication or local user authentication.

```
config wireless-controller vap
    edit "80e_wpa3"
        set ssid "80e_wpa3"
        set security wpa3-enterprise
        set pmf enable
        set auth radius
        set radius-server "wifi-radius"
        set schedule "always"
    next
    edit "80e_wpa3_user"
        set ssid "80e_wpa3_user"
        set security wpa3-enterprise
        set pmf enable
        set auth usergroup
        set usergroup "usergroup"
        set schedule "always"
    next
end
```

Monitoring and suppressing phishing SSID

In addition to rogue AP detection, another concern is phishing SSIDs, which are defined as:

- An SSID defined on FortiGate that is broadcast from an uncontrolled AP.
- A pre-defined pattern for an offending SSID pattern. For example, you can define any SSID that contains your company name to be a phishing SSID.

This function enables FortiAP to monitor and report these SSIDs in logs with the option to suppress them. You can only configure this function using the CLI.

To configure phishing SSID functions:

```
config wireless-controller setting
     set phishing-ssid-detect enable|disable
     set fake-ssid-action log|suppress
     config offending-ssid
        edit 1
           set ssid-pattern "OFFENDING*"
           set action log|suppress
        next
     end
end
```

`set phishing-ssid-detect enable|disable`	Enable or disable the phishing SSID detection function. The default is `enable`.
`set fake-ssid-action log|suppress`	Specify the FortiGate action after detecting a fake SSID. The default is `log` and can be set to either one or both.
`set ssid-pattern "OFFENDING*"`	Specify the criteria to match an offending SSID. This example shows all SSID names with a leading string `OFFENDING` (not case-sensitive).
`set action log|suppress`	Specify the FortiGate action after detecting the offending SSID pattern entry. The default setting is `log` and can be set to either one or both.

Log examples

WiFi event log sample for fake SSID detection

Following is a sample of the log that is generated when a fake SSID is first detected:

```
1: date=2019-03-01 time=14:53:23 logid="0104043567" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480803 logdesc="Fake AP detected" ssid="CORP_
     WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130 radioband="802.11n-5G"
     channel=149 action="fake-ap-detected" manuf="Fortinet, Inc." security="WPA2 Personal"
     encryption="AES" signal=-41 noise=-95 live=173397 age=0 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="FP321C3X15001615"
     radioiddetected=1 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="Detected Fake AP CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173397 age 0"
```

Following is a sample of the log that is periodically generated when a fake SSID is continuously detected:

```
1: date=2019-03-01 time=14:58:53 logid="0104043568" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551481133 logdesc="Fake AP on air" ssid="CORP_
     WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130 radioband="802.11n-5G"
     channel=149 action="fake-ap-on-air" manuf="Fortinet, Inc." security="WPA2 Personal"
     encryption="AES" signal=-41 noise=-95 live=173728 age=330 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A" radioiddetected=0
     stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0 msg="Fake AP On-
     air CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173728 age 330"
```

WiFi event log sample for fake SSID suppression

Following is a sample of the log that is generated when a fake SSID is suppressed:

```
1: date=2019-03-01 time=14:53:23 logid="0104043569" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480803 logdesc="Rogue AP suppressed"
     ssid="CORP_WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130
```

```
radioband="802.11n-5G" channel=149 action="rogue-ap-suppressed" manuf="Fortinet, Inc."
    security="WPA2 Personal" encryption="AES" signal=-41 noise=-95 live=173397 age=0
    onwire="no" detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A"
    radioiddetected=0 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
    msg="AP CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173397 age 0"
```

WiFi event log sample for offending SSID detection

Following a sample of the log that is generated when an offending SSID is first detected:

```
1: date=2019-03-01 time=14:53:33 logid="0104043619" type="event" subtype="wireless"
    level="warning" vd="root" eventtime=1551480811 logdesc="Offending AP detected"
    ssid="OFFENDING_SSID" bssid="1a:5b:0e:b5:f3:bf" aptype=0 rate=130 radioband="802.11n-
    5G" channel=153 action="offending-ap-detected" manuf="Fortinet, Inc." security="WPA2
    Personal" encryption="AES" signal=-41 noise=-95 live=173406 age=8 onwire="no"
    detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="FP321C3X15001615"
    radioiddetected=1 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
    msg="Detected Offending AP OFFENDING_SSID 1a:5b:0e:b5:f3:bf chan 153 live 173406 age
    8"
```

Following is a sample of a log that is periodically generated when an offending SSID is continuously detected:

```
1: date=2019-03-01 time=14:55:54 logid="0104043620" type="event" subtype="wireless"
    level="warning" vd="root" eventtime=1551480952 logdesc="Offending AP on air"
    ssid="OFFENDING_SSID_TEST" bssid="9a:5b:0e:18:1b:d0" aptype=0 rate=130
    radioband="802.11n-5G" channel=149 action="offending-ap-on-air" manuf="N/A"
    security="WPA2 Personal" encryption="AES" signal=-41 noise=-95 live=173548 age=150
    onwire="no" detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A"
    radioiddetected=0 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
    msg="Offending AP On-air OFFENDING_SSID_TEST 9a:5b:0e:18:1b:d0 chan 149 live 173548
    age 150"
```

WiFi event log sample for offending SSID suppression

Following is a sample of the log that is generated when an offending SSID is suppressed:

```
1: date=2019-03-01 time=14:53:33 logid="0104043569" type="event" subtype="wireless"
    level="warning" vd="root" eventtime=1551480811 logdesc="Rogue AP suppressed"
    ssid="OFFENDING_SSID" bssid="1a:5b:0e:b5:f3:bf" aptype=0 rate=130 radioband="802.11n-
    5G" channel=153 action="rogue-ap-suppressed" manuf="Fortinet, Inc." security="WPA2
    Personal" encryption="AES" signal=-41 noise=-95 live=173406 age=8 onwire="no"
    detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A" radioiddetected=0
    stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0 msg="AP OFFENDING_
    SSID 1a:5b:0e:b5:f3:bf chan 153 live 173406 age 8"
```

Changing SSID to VDOM only

This feature changes the wireless-controller VAP (for SSID configuration) from a global object to a VDOM object, simplifying tracking the object reference count. It also removes the `vdom` setting from VAP configuration. When multi-vdom is enabled on a FortiGate, the wireless-controller VAP can be added, edited, or deleted only inside of a VDOM.

To create a VAP entry:

- When `vdom-mode` is `no-vdom`:

```
# config wireless-controller vap
(vap) # edit new
    new entry 'new' added
(new) # set ssid new
(new) # set passphrase 12345678
(new) # set vdom
    command parse error before 'vdom'
(new) # end
# show wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
            set passphrase ENC
qmVlo9Zn3C4aVZMIw9LrHhXX+wDNn2BMT9hP3vmZGQFZZz+gQ6Lb1jS9UkAkbQabWkGq8uDZDfqwtWV8lZdMDOFy
DC0Kgh/yCuCkM5xM1bm9gvnGC9+84VY2mvkV4pUeiugJ/8o1m++buXmP9CdUmLz7eY/VZwYlKnSyFvk7DphbfZJa
pCOXtgN2zseNoITPQUTKLA==
            next
    end
```

- When `vdom-mode` is `multi-vdom`:
  - A VAP cannot be created in global:

```
# config global
(global) # config wireless-controller vap
command parse error before 'vap'
Command fail. Return code 1
```

  - A VAP can be created in a VDOM:

```
# config vdom
(vdom) # edit vdom2
    current vf=vdom2:1
(vdom2) # config wireless-controller vap
(vap) # edit new
    new entry 'new' added
(new) # set ssid new
(new) # set passphrase 12345678
(new) # set vdom
    command parse error before 'vdom'
(new) # end
(vdom2) # sh wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
            set passphrase ENC
IidSvoD1C6feNonhsYfUTnOtO89UE/S/wWmOxRHLCudeR0LD8xuYzWzsRg9/c299Vd2UA809NSUfyRBRD/pF
Fd/QS6ArQPs4sLVtPiftE63uI53d9azeQv6e5tkQjg4Z7Ztlv2hE47nKkdVXeWZE3mpfRhSxvDUKVzwpR1b8
pdwbzDGFlPs+JcoNso6ZeRCuMg54g==
            next
    end
```

To check multi-vdom VAP entry authentication:

- When `vdom-mode` is `multi-vdom`, references to user-group and radius can be checked correctly when they are used by a VAP interface:
  - A VAP interface with security-mode set to WPA2-Enterprise and RADIUS authentication:

```
(vdom2) # show wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
            set security wpa2-only-enterprise
            set auth radius
            set radius-server "peap"
        next
    end
(vdom2) # diagnose sys cmdb refcnt show user.radius.name peap
    entry used by table wireless-controller.vap:name 'new'
```

  - A VAP interface with security-mode set to WPA2-Enterprise and User-group authentication:

```
(vdom2) # show wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
            set security wpa2-only-enterprise
            set auth usergroup
            set usergroup "group-radius"
        next
    end
(vdom2) # diagnose sys cmdb refcnt show user.group.name group-radius
    entry used by child table usergroup:name 'group-radius' of table wireless-
controller.vap:name 'new'
```

WiFi with WSSO using Windows NPS and user groups

You can configure wireless single sign-on (WSSO) using a Network Policy Server (NPS) and FortiGate user groups.

In the following example, the WiFi users are students at a school. The user group belongs to a Windows Active Directory (AD) group called *WiFiAccess*. When the users enter their WiFi user names and passwords, the FortiGate checks the local group *WiFi*. Since this user group has been set up on a remote authentication dial-in user service (RADIUS) server, the FortiGate performs user authentication against the NPS or RADIUS server. If the user is successfully authenticated, the FortiGate checks for a policy that allows the *WiFi* group access.
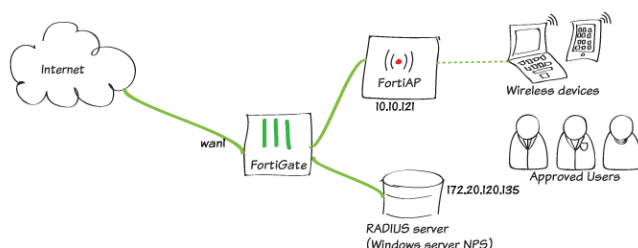
**To configure WSSO using Windows NPS and user groups:**

1. Register the FortiGate as a RADIUS client on the NPS:
    a. In the NPS, go to *RADIUS Clients and Servers > RADIUS Clients*.
    b. Right-click *RADIUS Clients* and select *New*.
    c. Enter the FortiGate information:
        - Name
        - IP address (`172.20.120.142`)
        - Shared secret (password)
    d. Click *OK*.
        The FortiGate properties view:
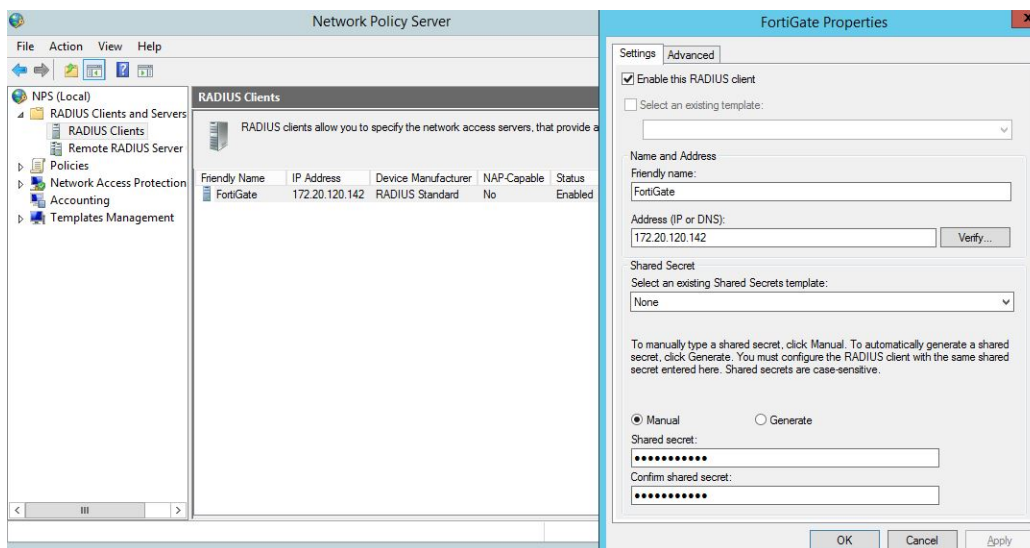
2. Create a connection request policy:
    a. Go to *Policies > Connection Request Policies*.
    b. Right-click *Connection Request Policies* and select *New*.
    c. Enter the policy name (`WiFi`) and select the type of network access server.
    d. Click *Next*. The *Specify Conditions* window opens.
    e. Click *Add* and under *Connection Properties*, select *Client IPv4 Address*.
    f. Configure the *Client IPv4 Address* as the FortiGate IP address.

**g.** Keep clicking *Next* and leave the default settings until you can click *Finish*.
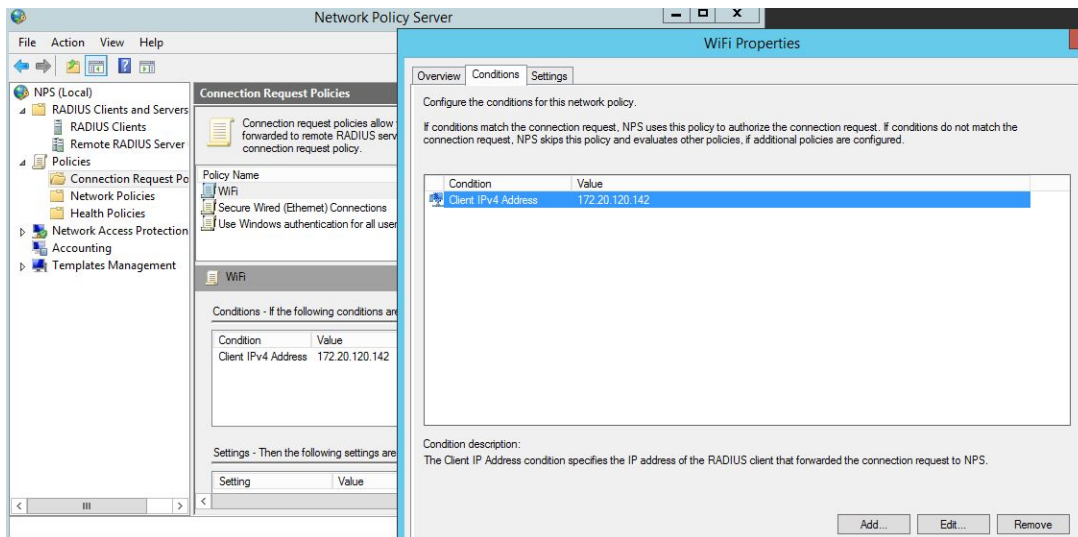
3. Create a network policy:

a. Go to *Policies > Network Policies*.

b. Right-click *Network Policies* and select *New*.

c. Enter the policy name (`WiFi-Access`) and select the type of network access server.

d. Click *Next*. The *Specify Conditions* window opens.

e. Click *Add* and under *Groups*, select *Windows Groups*.

f. Click *Add Groups* and enter the Windows AD group, *WiFiAccess*, as the *object name to select*.

g. Click *OK*, then *Next* twice to advance to the *Configure Authentication Methods* window.

h. For *EAP Types*, click *Add* and select *Microsoft: Protected EAP (PEAP)*.

i. Click *OK*.

j. For *Less secure authentication methods*, make sure only the *Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)* and *User can change password after it has expired* checkboxes are selected.

k. Keep clicking *Next* and leave the default settings until you can click *Finish*.
The WiFi-Access network policy conditions properties view:
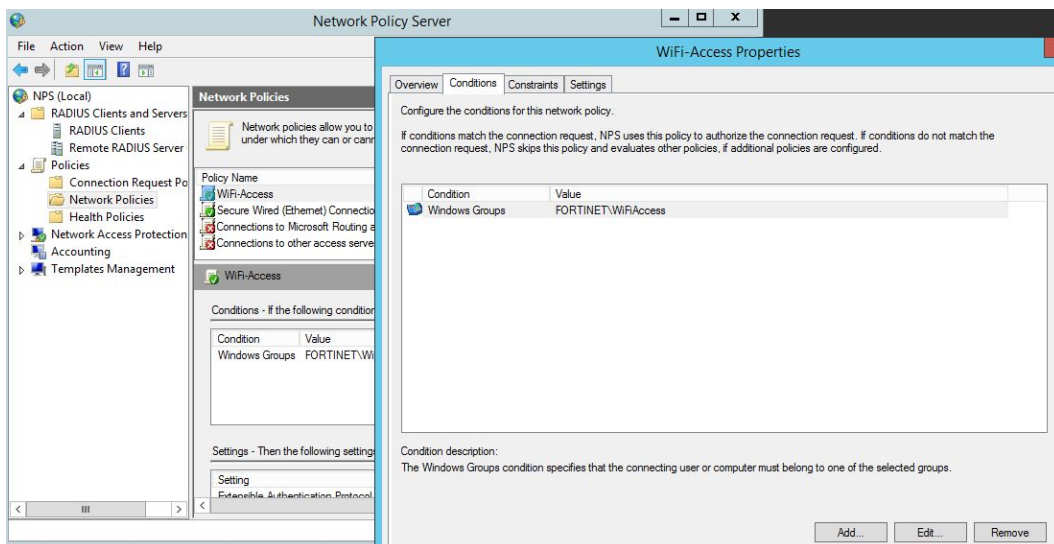
The WiFi-Access network policy constraints properties view:
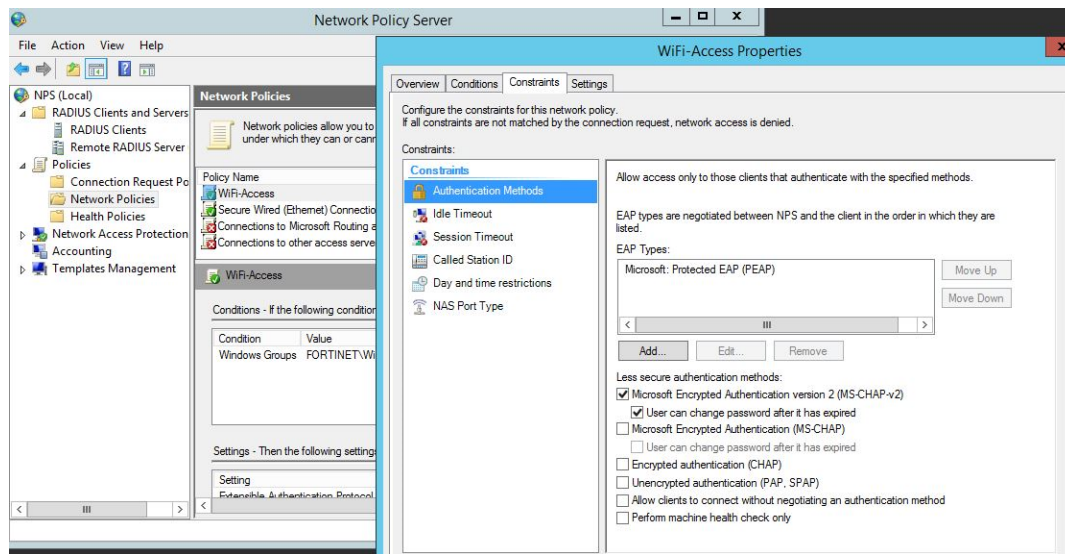
4. Configure the FortiGate to use the RADIUS server:

   a. In FortiOS, go to *User & Device > RADIUS Servers*.

   b. Click *Create New*.

   c. Enter the server information:

      - Name (`DC-RADIUS`)
      - Authentication method (click *Specify* and select *MS-CHAP-v2*)
      - Domain controller IP address
      - Server secret

   d. Optionally, you can click *Test Connectivity*. After you enter the user ID and password, the result should be successful.

   e. Click *OK*.

5. Configure the WiFi user group:

   a. Go to *User & Device > User Groups*.

   b. Click *Create New*.

   c. Enter the user group information:

      - Name
      - Type (select *Firewall*)

   d. Under *Remote Groups*, click *Add*. The *Add Group Match* pane opens.

e. In the *Remote Server* dropdown, select the RADIUS server you just configured (*DC-RADIUS*).

f. For *Groups*, click *Any*.

g. Click *OK* to add the server.

h. Click *OK* to save the user group.

New User Group

Name	WiFi
Type	Firewall / Fortinet Single Sign-On (FSSO) / RADIUS Single Sign-On (RSSO) / Guest
Members	+

Remote Groups

+ Add | Edit | Delete

Remote Server	Group Name
DC-RADIUS	Any

OK | Cancel

6. Create an SSID with RADIUS authentication:

a. Go to *WiFi & Switch Controller > SSIDs*.

b. Click *Create New > SSID*.

c. Configure the interface and *enable DHCP Server*.

d. Click *Create New* to add the address range.

New

Interface Name	FAP223C-5G
Alias	
Type	WiFi SSID
Traffic Mode	Tunnel / Bridge / Mesh

Address

IP/Network Mask	10.10.12.1/255.255.255.0
IPv6 Address/Prefix	::/0
Create address object matching subnet	
Name	FAP223C-5G address
Definition	10.10.12.0/24

Administrative Access

IPv4	HTTPS	PING	FMG-Access	SSH
	SNMP	FTM	RADIUS Accounting	
	FortiTelemetry			
IPv6 Administrative Access	HTTPS	PING	FMG-Access	SSH
	SNMP	FTM		

DHCP Server

Address Range

+ Create New | Edit | Delete

Starting IP	End IP
10.10.12.2	10.10.12.254

Netmask	255.255.255.0
Default Gateway	Same as Interface IP / Specify
DNS Server	Same as System DNS / Same as Interface IP / Specify
Advanced...	

e. Configure the *WiFi Settings* section:

- For *Security Mode*, select *WPA2 Enterprise*.
- For *Authentication*, click *Local* and add the *WiFi* user group.

New	
Networked Devices	
Device Detection ⓘ ⬤	
WiFi Settings	
SSID	FAP223C-5G
Security Mode	WPA2 Enterprise ▼
Client Limit	◯
Authentication	**Local** RADIUS Server
	▦ WiFi ✕
	+
Broadcast SSID	⬤
Schedule ⓘ	⏰ always ✕
	+

Local vs RADIUS Server Authentication:

- Local: PEAP terminates on the FortiGate, and FortiGate uses the built-in Fortinet_ WiFi certificate for the connection by default. To select a different certificate, see Replacing WiFi certificate on page 21 for details.
- RADIUS Server: PEAP is forwarded to the RADIUS Server.

f. Click *OK*.

7. Create a security policy:

a. Go to *Policy & Objects > IPv4 Policy*.

b. Click *Create New*.

c. Configure the policy to have the SSID you created in step 6 as the *Incoming Interface* and the WiFi user group you created in step 5 as the *Source*.

d. Configure other settings as needed.

e. Click *OK*.

To verify the WSSO authentication:

1. From the wireless client, the wireless settings may ask for the CA certificate for the PEAP connection.
   - On Android devices, you can select *Use system certificate* since the default FortiGate_WiFi certificate is signed by a public CA. If asked to specify the domain, enter *fortinet.com*. See the example Android WiFi client settings:

- Alternatively, select *Don't Validate* to bypass validating the certificate used in the PEAP connection.

2. Use the credentials of a user that belongs to the Windows AD WiFiAccess group to verify that you have been successful authenticated.
   a. Try connecting to the WiFi network.
   b. Get authenticated.
   c. Browse the internet.

3. In FortiOS 6.2 and earlier, go to *Monitor > Firewall User Monitor*.

   For the credentials you tested, you will be able to view the user name, user group, IP address, and if the WSSO authentication method was used:

User Name	User Group	IP Address	Method
test_user	WiFi	10.10.12.2	🛜 WSSO

Statistics

This section contains topics about WiFi statistics:

- WiFi maps on page 53
- Fortinet Security Fabric on page 57
- Direct SNMP monitor on page 57

WiFi maps

WiFi Maps allow you to place FortiAP units on a custom map that you upload, such as an office floor plan. *WiFi Maps* show real-time status and alerts of FortiAP units so that you can quickly see the location and status of each FortiAP unit on the map.

**To configure WiFi maps on the FortiWiFi and FortiAP GUI:**

1. Obtain a floor plan or map (in PNG, JPEG, or GIF format) of where FortiAP units are located.
2. Go to *WiFi & Switch Controller > WiFi Maps*.
3. Click the *+* or *Add Map* button.
   You must use the GUI to upload WiFi maps.
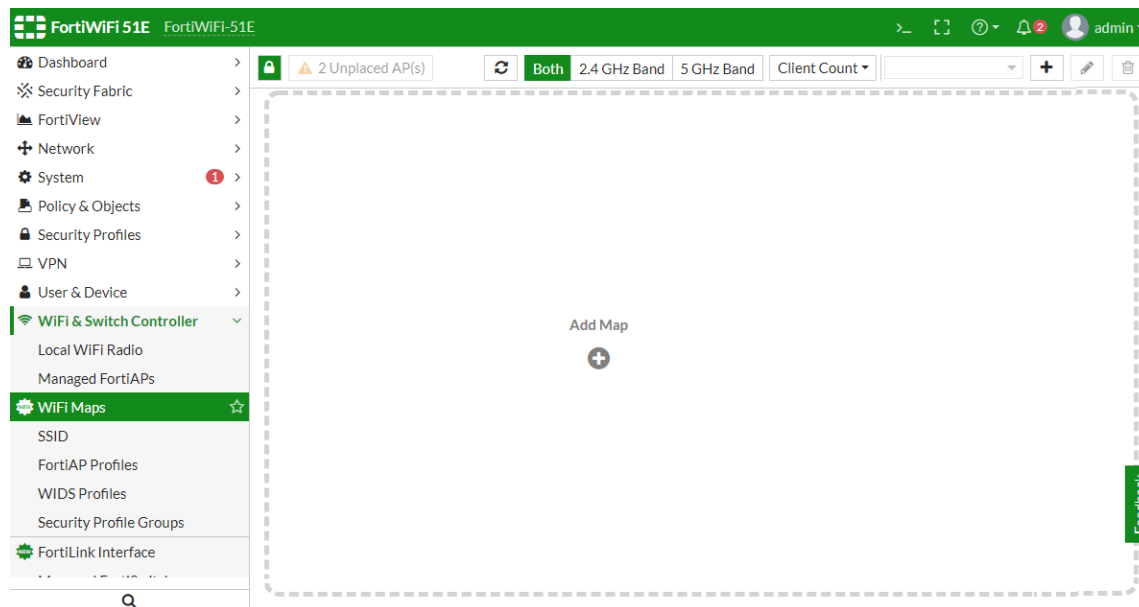
4. Click *Upload* and specify the map to be uploaded.
   a. Enter the *Map name*, for example, *Level-2*.
   b. If you want, enable *Image grayscale* to change a color map to grayscale.
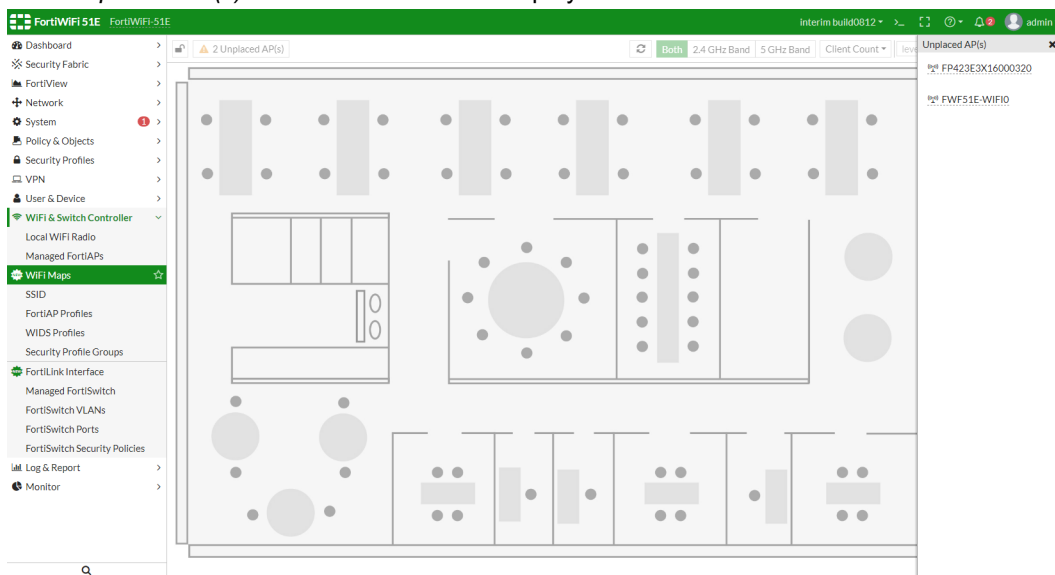
    c. Set *Image opacity* to specify map transparency.
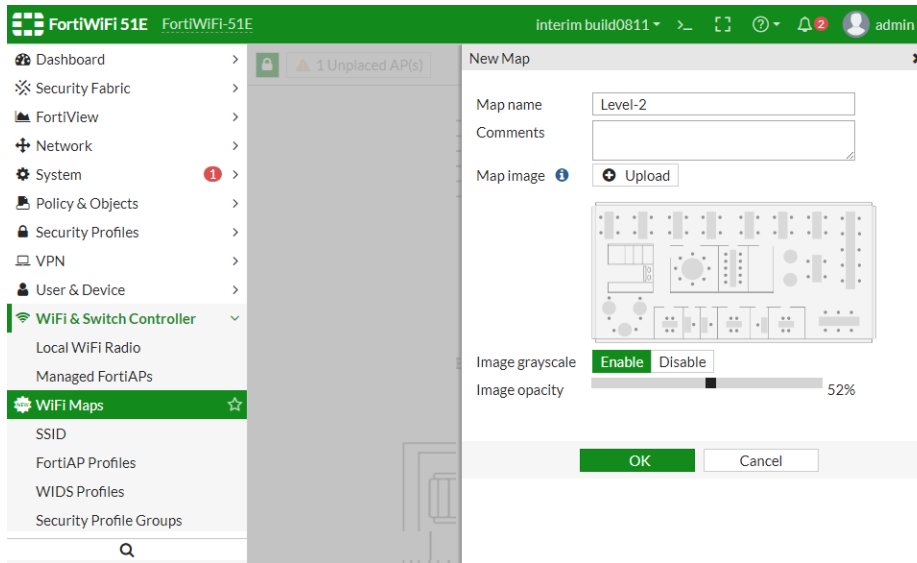
    d. Click OK.

5. Place FortiAP units on the map you uploaded.

    a. Unlock the map by clicking the lock icon in the top left.

    b. Click *Unplaced AP(s)* beside the lock icon to display the list of candidate APs.

c. Drag and drop each FortiAP unit onto its location on the map.
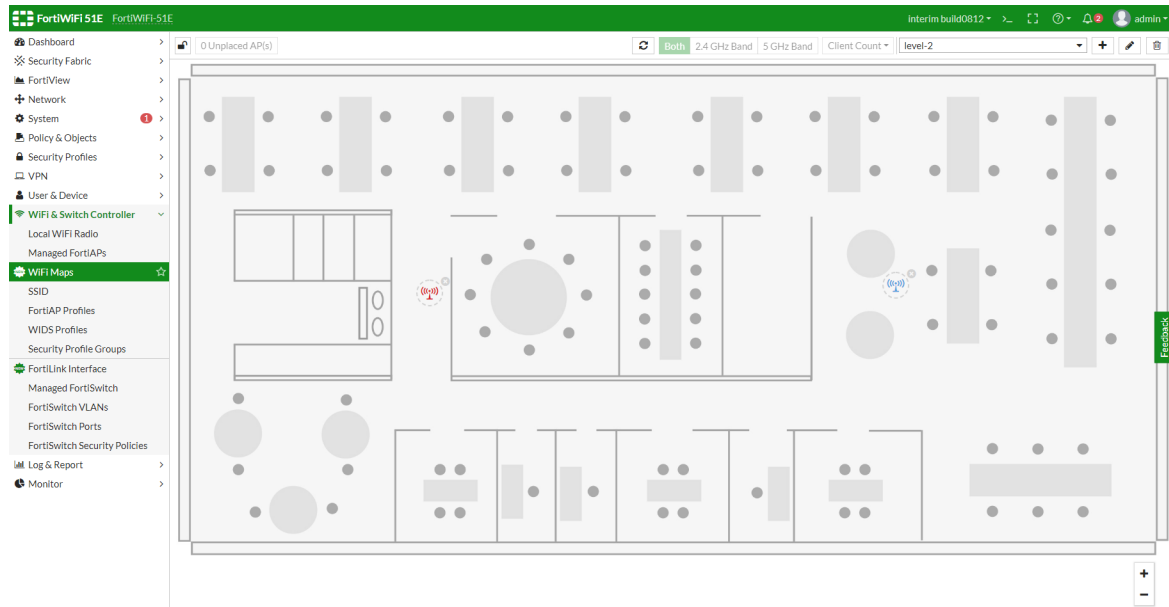
d. When all FortiAP units have been placed on the map, click the lock icon.

The WiFi map shows where each FortiAP unit is located.

6. Hover the cursor over a FortiAP icon to view the FortiAP unit's operating data.

7. To view a FortiAP unit's detailed operating data or to configure AP settings, click that FortiAP icon.
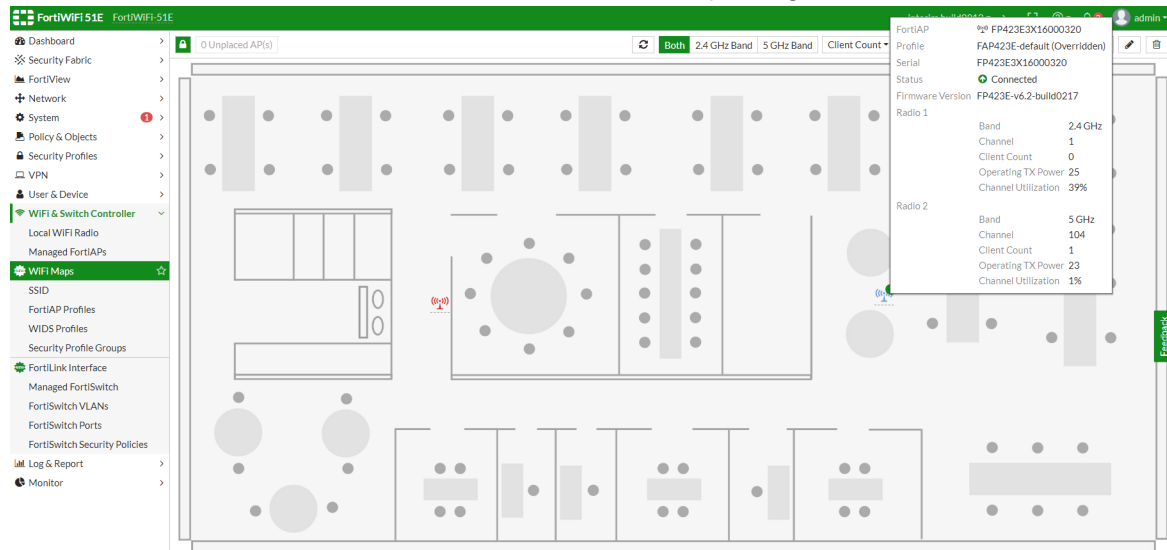

8. Use the dropdown lists above the map to show one or both the 2.4 GHz or 5 GHz band. You can also show numerical operating data such as client count, channel, radio TX power, and channel utilization using the options in the dropdown list above the map.

To configure WiFi maps using the FortiWiFi and FortiAP CLI:

```
config wireless-controller region
   edit <MAP_NAME>
      set grayscale enable <enable|disable>
      set opacity 40 <0-100>
   next
end
config wireless-controller wtp
   edit <FAP_SN>
      set region <MAP_NAME>
      set region-x "0.419911" <0-1>
      set region-y "0.349466" <0-1>
   next
```

```
end
```

Fortinet Security Fabric

The following shows a simple network topology when using FortiAP as part of the Security Fabric:
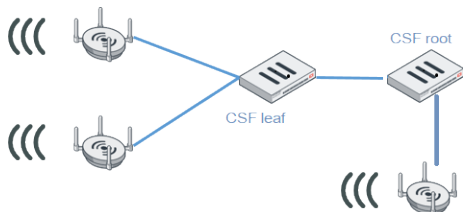
The *Security Fabric > Settings* page on the root FortiGate lists all FortiAP devices on the CSF root and leaf.
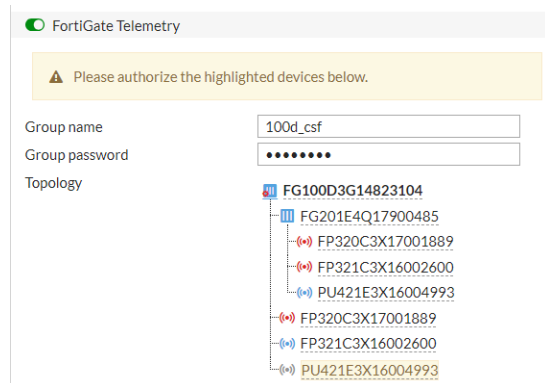
The *Security Fabric > Physical Topology* view on the root FortiGate shows the devices in the Security Fabric and the devices they are connected to.
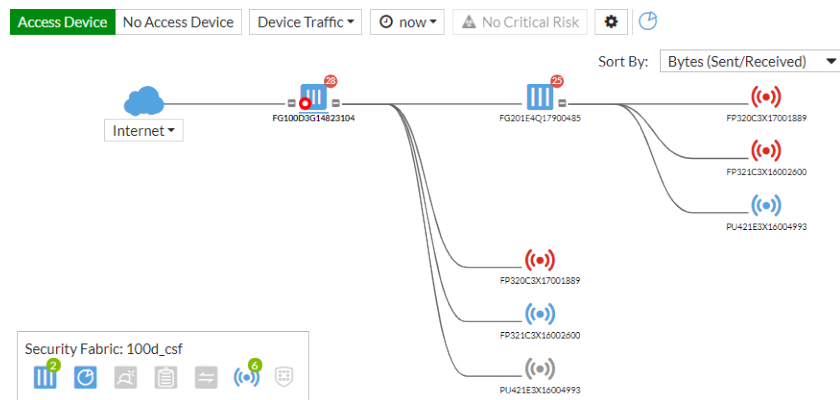
Direct SNMP monitor

You can enable SNMP directly on FortiAP by implementing a SNMPD daemon/subagent on the FortiAP side.

To configure SNMP operation settings per VDOM:

```
config wireless-controller snmp
    set engine-id "fap-fortinet"
    set contact-info "user@example.com"
    set trap-high-cpu-threshold 80
    set trap-high-mem-threshold 80
    config community
        edit 1
            set name "fap-comm-1"
            set status enable
            set query-v1-status enable
            set query-v2c-status enable
            set trap-v1-status enable
            set trap-v2c-status enable
            config hosts
                edit 1
                    set ip 192.168.1.168 255.255.255.0
                next
            end
        next
    end
    config user
        edit "fap"
            set status enable
            set queries enable
            set trap-status enable
            set security-level no-auth-no-priv
            set notify-hosts 192.168.1.168
        next
    end
end
```

To allow SNMP access in FortiAP profiles or per FortiAP device:

```
config wireless-controller wtp-profile
    edit FAP423E-default
        append allowaccess snmp
    next
end
```

To disallow SNMP access in FortiAP profiles or per FortiAP device:

```
config wireless-controller wtp-profile
    edit FAP423E-default
        unselect allowaccess snmp
    next
end
```

FortiAP SNMP implementation

FortiAP-S and FortiAP-W2 6.2 and later support SNMP query and trap messages according to the wireless controller SNMP settings pushed from the FortiGate device.

The example below shows an Ubuntu-OS querying a FortiAP 222E unit with the `snmpwalk` command. The SNMP agent software has the FORTINET-FORTIAP-MIB already imported.

```
tester@ControlPC:~$ snmpwalk -v 2c -c QAMikeAn 172.18.56.32 .1.3.6.1.4.1.12356.120.1
FORTINET-FORTIAP-MIB::fapVersion.0 = STRING: FP222E-v6.2-build0231
FORTINET-FORTIAP-MIB::fapSerialNum.0 = STRING: FP222E3X17000073
FORTINET-FORTIAP-MIB::fapHostName.0 = STRING: FortiAP-222E
FORTINET-FORTIAP-MIB::fapRegionCode.0 = STRING: A
FORTINET-FORTIAP-MIB::fapBaseMacAddr.0 = STRING: 70:4c:a5:5d:ea:d0
FORTINET-FORTIAP-MIB::fapBiosVer.0 = STRING: 04000002
FORTINET-FORTIAP-MIB::fapBiosDataVer.0 = INTEGER: 3
FORTINET-FORTIAP-MIB::fapSysPartNum.0 = STRING: 20844-04
```

Five kinds of trap messages can be sent by the FortiAP-S and FortiAP-W2 devices:

- fapDevUp: Indicates that the specified AP device is up.
- CpuOverloadfap: Indicates that the CPU usage of the specified AP has exceeded the configured threshold.
- MemOverload: Indicates that the memory usage of the specified AP has exceeded the configured threshold.
- fapDevDown: Indicates that the specified AP device is down.
- fapfapAcConnected: Indicates that the specified AP device has connected to the specified AC.

The following screenshot shows an SNMP trap receiver (SnmpB) that has received one `fapDevUp` trap message from a FortiAP unit (serial number: FP222E3X17000000).
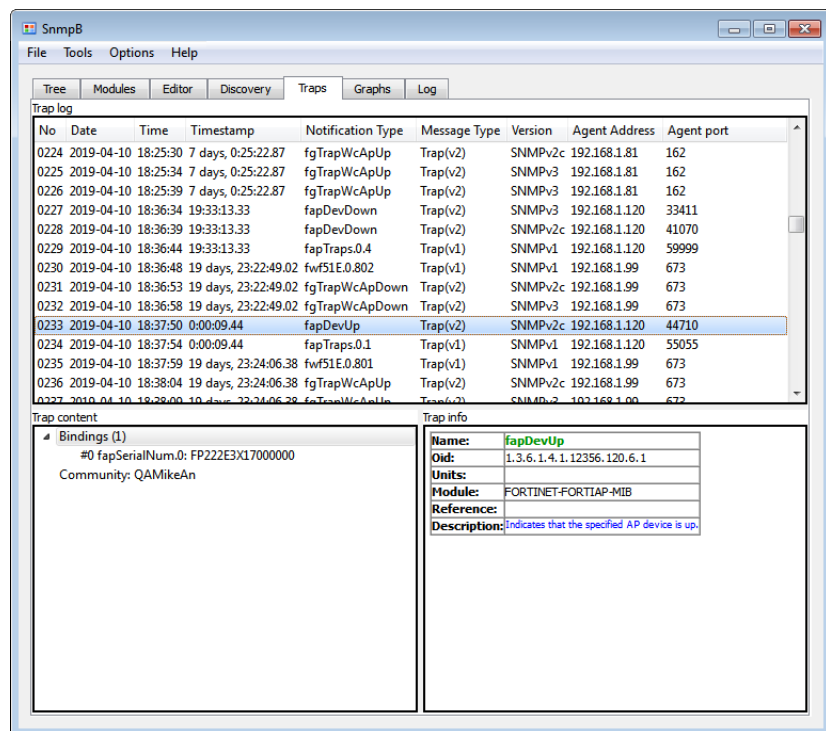
Wireless security

This section contains topics about configuring wireless security with WiFi connections:

- Enabling rogue AP scan on page 60
- Enabling rogue AP suppression on page 61
- Wireless Intrusion Detection System on page 62
- WiFi QoS WMM marking on page 63
- WPA3 support on page 65

Enabling rogue AP scan

The guide provides simple configuration instructions for enabling ap-scan on FortiAP. The steps include creating a WIDS profile and selecting the WIDS profile on the managed FortiAP.

To enable rogue AP scan on the FortiWiFi and FortiAP GUI:

1. Create a WIDS profile:
   a. In FortiWiFi and FortiAP, go to *WiFi & Switch Controller > WIDS Profiles*. Click *Create New*.
   b. Enable *Enable Rogue AP Detection*.
   c. Complete the configuration, then click *OK*.
2. Select the WIDS profile for the managed FortiAP:
   a. Go to *WiFi & Switch Controller > FortiAP Profiles*.
   b. Select the FortiAP profile applied to the managed FortiAP, then click *Edit*.
   c. Enable *WIDS Profile*. Select the profile created in step 1. Click *OK*.

To enable rogue AP scan using the FortiWiFi and FortiAP CLI:

1. Create a WIDS profile:
```
config wireless-controller wids-profile
   edit "example-wids-profile"
      set ap-scan enable
   next
end
```
2. Select the WIDS profile for the managed FortiAP:
```
config wireless-controller wtp-profile
   edit "example-FAP-profile"
      config platform
         set type <FAP-model-number>
      end
      set handoff-sta-thresh 55
      set ap-country US
      config radio-1
         set band 802.11n
         set wids-profile "example-wids-profile"
```

```
            set vap-all disable
        end
        config radio-2
            set band 802.11ac
            set vap-all disable
        end
    next
end
```

Enabling rogue AP suppression

The guide provides simple configuration instructions for suppressing rogue APs on FortiAP. The steps include creating a WIDS profile and suppressing rogue APs.

To enable rogue AP suppression on the FortiWiFi and FortiAP GUI:

1. Create a WIDS profile:
   a. In FortiWiFi and FortiAP, go to *WiFi & Switch Controller > WIDS Profiles*. Click *Create New*.
   b. For *Sensor Mode*, select *Foreign and Home Channels*.
   c. Enable *Enable Rogue AP Detection*.
   d. Complete the configuration, then click *OK*.
2. Select the WIDS profile for the managed FortiAP. The monitoring radio must be in Dedicated Monitor mode:
   a. Go to *WiFi & Switch Controller > FortiAP Profiles*.
   b. Select the FortiAP profile applied to the managed FortiAP, then click *Edit*.
   c. Select *Dedicated Monitor* on *Radio 1* or *Radio 2*.
   d. Enable *WIDS Profile*. Select the profile created in step 1. Click *OK*.
3. Suppress FortiAP:
   a. Go to *Monitor > Rogue AP Monitor*.
   b. Right-click the desired SSID, then select *Mark as Rogue*.
   c. Right-click the SSID again, then select *Suppress AP*.

To enable rogue AP scan using the FortiWiFi and FortiAP CLI:

1. Create a WIDS profile:
```
config wireless-controller wids-profile
   edit "example-wids-profile"
      set sensor-mode both
      set ap-scan enable
   next
end
```
2. Select the WIDS profile for the managed FortiAP:
```
config wireless-controller wtp-profile
   edit "example-FAP-profile"
      config platform
         set type <FAP-model-number>
      end
      config radio-1
         set mode monitor
         set wids-profile "example-wids-profile"
```

```
            end
        next
    end
```

3. Suppress FortiAP:

```
config wireless-controller ap-status
    edit 1
        set bssid 90:6c:ac:da:a7:f1
        set ssid "example-SSID"
        set status suppressed
    next
end
```

Wireless Intrusion Detection System

The guide provides simple configuration instructions for enabling a Wireless Intrusion Detection System (WIDS) profile on FortiAP.

To enable a WIDS profile on the FortiWiFi and FortiAP GUI:

1. Create a WIDS profile:
   a. In FortiWiFi and FortiAP, go to *WiFi & Switch Controller > WIDS Profiles*. Click *Create New*.
   b. In the *Name* field, enter the desired name.
   c. Under *Intrusion Detection Settings*, enable all intrusion types as desired.
   d. Complete the configuration, then click *OK*.
2. Select the WIDS profile for the managed FortiAP:
   a. Go to *WiFi & Switch Controller > FortiAP Profiles*.
   b. Select the FortiAP profile applied to the managed FortiAP, then click *Edit*.
   c. Enable *WIDS Profile*. Select the profile created in step 1. Click *OK*.

To enable a WIDS profile using the FortiWiFi and FortiAP CLI:

```
config wireless-controller wtp-profile
    edit "example-FAP-profile"
        config platform
            set type <FAP-model-number>
        end
        set handoff-sta-thresh 55
        set ap-country US
        config radio-1
            set band 802.11n
            set wids-profile "example-wids-profile"
            set vap-all disable
        end
        config radio-2
            set band 802.11ac
            set wids-profile "example-wids-profile"
            set vap-all disable
        end
    next
end
```

WiFi QoS WMM marking

This function enables FortiGate to preserve the WiFi Multi-Media (WMM) QoS marking of packets by translating them to Differentiated Services Code Point (DSCP) values when forwarding upstream.

> This function requires a FortiAP-S or FortiAP-W2 device.

Use the following QoS profile CLI commands to implement this function:

`wmm-dscp-marking`	Enable/disable WMM Differentiated Services Code Point (DSCP) marking (default = disable).
`wmm-vo-dscp`	DSCP marking for voice access (default = 48).
`wmm-vi-dscp`	DSCP marking for video access (default = 32).
`wmm-be-dscp`	DSCP marking for best effort access (default = 0).
`wmm-bk-dscp`	DSCP marking for background access (default = 8).
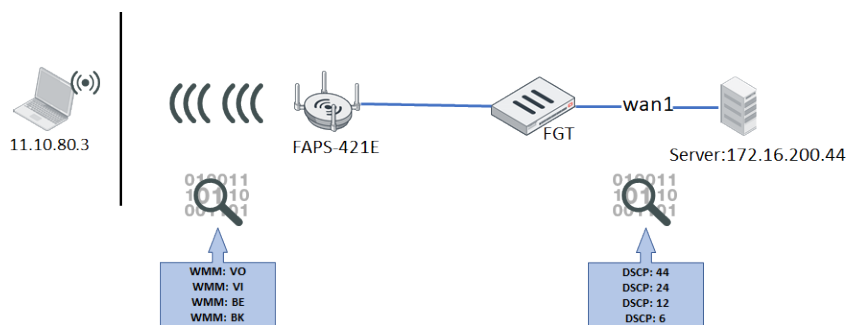
To configure WMM QoS marking of packets:

1. Create a QoS profile with `wmm-dscp-marking` enabled, and modify the `wmm-dscp` settings.

   ```
   config wireless-controller qos-profile
       edit qos-wifi
           set wmm-dscp-marking enable
           set wmm-vo-dscp 44
           set wmm-vi-dscp 24
           set wmm-be-dscp 12
           set wmm-bk-dscp 6
   end
   ```

2. Select the QoS profile on a VAP interface.

   ```
   config wireless-controller vap
       edit "stability3"
           set qos-profile "qos-wifi"
       next
   end
   ```

3. Verify that the `wmm-dscp-marking` values are pushed on FortiAP.

```
cw_diag -c k-qos wlan00
WLAN Kernel QoS Settings
..
....
WLAN wlan00 :
    wmm                           : 1
    wmm uapsd                     : 1
    call admission control        : 0
    call capacity                 : 0
    bandwidth admission control   : 0
    bandwidth capacity            : 0
    dscp mapping                  : 0
    dscp marking                  : 1
        vo dscp                   : 44
        vi dscp                   : 24
        be dscp                   : 12
        bk dscp                   : 6
```

4. Verify that, when sending traffic from a client with a WMM setting of VO, the FortiGate receives the packets with a DSCP TID value or 44.

5. Verify that, when sending traffic from a client with a WMM setting of VI, the FortiGate receives the packets with a DSCP TID value or 24.

6. Verify that, when sending traffic from a client with a WMM setting of BE, the FortiGate receives the packets with a DSCP TID value or 12.

7. Verify that, when sending traffic from a client with a WMM setting of BK, the FortiGate receives the packets with a DSCP TID value or 6.

```
Transmitter address: IntelCor_1c:ce:b0 (7c:7a:91:1c:ce:b0)
Source address: IntelCor_1c:ce:b0 (7c:7a:91:1c:ce:b0)
BSS Id: Fortinet_c7:65:39 (90:6c:ac:c7:65:39)
STA address: IntelCor_1c:ce:b0 (7c:7a:91:1c:ce:b0)
.... .... .... 0000 = Fragment number: 0
0000 0000 0000 .... = Sequence number: 0
Frame check sequence: 0xf008a251 [correct]
[FCS Status: Good]
Qos Control: 0x0001
    .... .... .... 0001 = TID: 1
    [.... .... .... .001 = Priority: Background (Background) (1)]
    .... .... ...0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
    .... .... .00. .... = Ack Policy: Normal Ack (0x0)
    .... .... 0... .... = Payload Type: MSDU
    0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
```

```
> Ethernet II, Src: IntelCor_1c:ce:b0 (7c:7a:91:1c:ce:b0), Dst: 00:ff:96:54:a7:74 (00:ff:96:54:a7:74)
∨ Internet Protocol Version 4, Src: 11.10.80.3, Dst: 172.16.200.44
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ∨ Differentiated Services Field: 0x18 (DSCP: Unknown, ECN: Not-ECT)
      0001 10.. = Differentiated Services Codepoint: Unknown (6)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```

WPA3 support

WPA3 security modes can be selected when configuring SSIDs.

To configure WPA3 in the GUI:

1. Go to *WiFi & Switch Controller > SSID*.
2. Create a new SSID, or edit a current one.
3. In the *WiFi Settings* section, set the *Security Mode* to a WPA3 option.
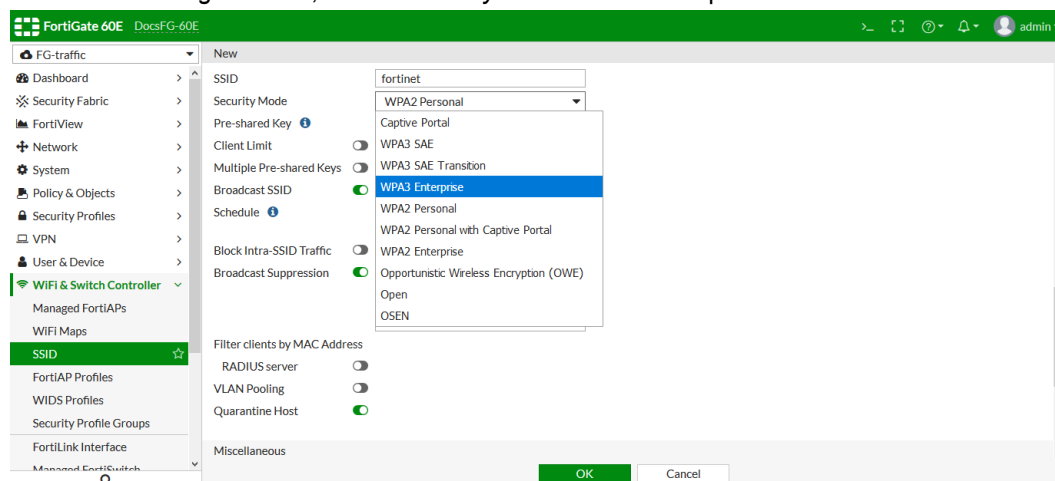
4. Configure the remaining settings as needed.
5. Click *OK*.
6. Use a client with WPA3 to verify the connection.

To configure WPA3 in the CLI:

1. WPA3 OWE:
    a. WPA3 OWE only.
       Clients that support WPA3 can connect with this SSID.

```
config wireless-controller vap
    edit "80e_owe"
        set ssid "80e_owe"
        set security owe
        set pmf enable
        set schedule "always"
```

```
        next
    end
```

    b. WPA3 OWE TRANSITION.

Clients connect with normal OPEN or OWE depending on its capability: Clients that support WPA3 connect with OWS standard, and clients that cannot support WPA3 connect with Open SSID.

```
config wireless-controller vap
    edit "80e_open"
        set ssid "80e_open"
        set security open
        set owe-transition enable
        set owe-transition-ssid "wpa3_open"
        set schedule "always"
    next
    edit "wpa3_owe_tr"
        set ssid "wpa3_open"
        set broadcast-ssid disable
        set security owe
        set pmf enable
        set owe-transition enable
        set owe-transition-ssid "80e_open"
        set schedule "always"
    next
end
```

2. WPA3 SAE:

    a. WPA3 SAE.

Clients that support WPA3 can connect with this SSID.

```
config wireless-controller vap
    edit "80e_sae"
        set ssid "80e_sae"
        set security wpa3-sae
        set pmf enable
        set schedule "always"
        set sae-password 12345678
    next
end
```

    b. WPA3 SAE TRANSITION.

There are two passwords in the SSID. If *passphrase* is used, the client connects with WPA2 PSK. If *sae-password* is used, the client connects with WPA3 SAE.

```
config wireless-controller vap
    edit "80e_sae-tr"
        set ssid "80e_sae-transition"
        set security wpa3-sae-transition
        set pmf optional
        set passphrase 11111111
        set schedule "always"
        set sae-password 22222222
    next
end
```

3. WPA3 Enterprise.

Select the `auth` type to use either RADIUS authentication or local user authentication.

```
config wireless-controller vap
    edit "80e_wpa3"
        set ssid "80e_wpa3"
        set security wpa3-enterprise
        set pmf enable
        set auth radius
        set radius-server "wifi-radius"
        set schedule "always"
    next
    edit "80e_wpa3_user"
        set ssid "80e_wpa3_user"
        set security wpa3-enterprise
        set pmf enable
        set auth usergroup
        set usergroup "usergroup"
        set schedule "always"
    next
end
```

4. Use a client with WPA3 to verify the connection.

Remote AP setup

This section guides you through the process of setting up remote FortiAPs to work with FortiGates:

1. Configuring FortiGate before deploying remote APs on page 69
2. Configuring FortiAPs to connect to FortiGate on page 73
3. Final FortiGate configuration tasks on page 75

Elements of a Teleworker Solution Power User
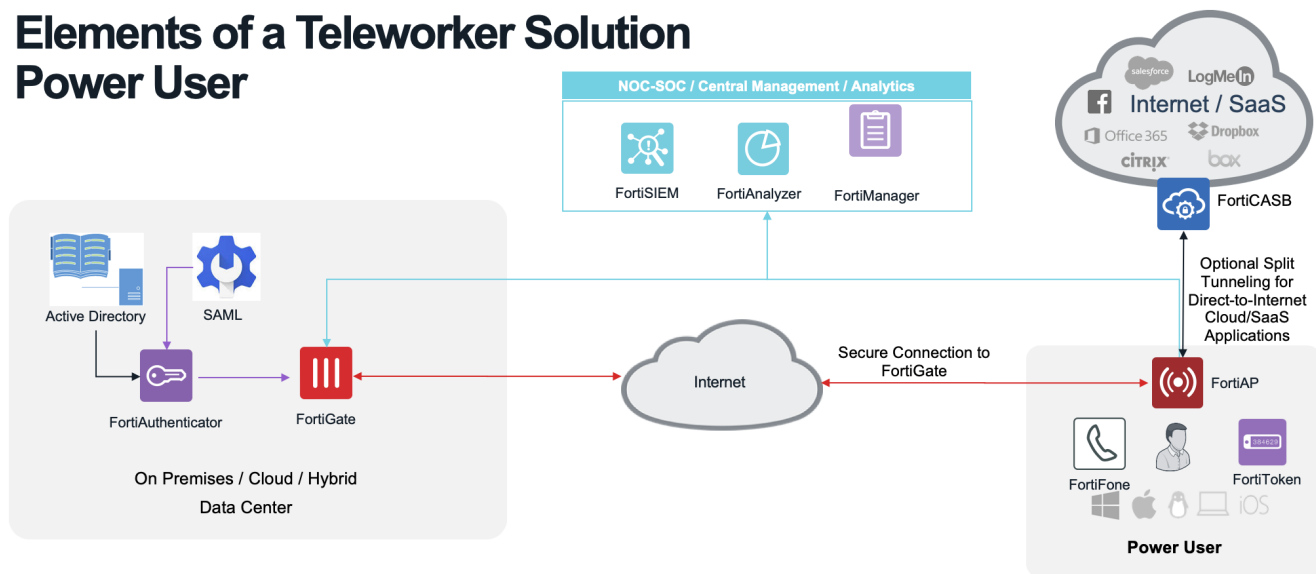
Configuration prerequisites

- Ensure that your FortiGate has an existing wireless SSID configured in tunnel mode.
  - For more information on configuring SSIDs, refer to Defining a wireless network interface (SSID) in the *FortiWiFi and FortiAP Configuration Guide*.
- For the best security practices, set up WPA2/Enterprise for SSIDs used by remote clients. You can use RADIUS Server for PEAP Authentication using MS-CHAPv2 and install a trusted Root CA certificate on all devices that connect to the secure SSIDs.

> For more security, you can use Client Certificates instead of MS-CHAPv2. For more information, refer to the FortiAuthenticator Cookbook.

- If you plan on deploying the FortiAP from FortiAP Cloud, ensure you have a Fortinet Support Account at https://support.fortinet.com.
- Ensure the internet bandwidth at the site where the FortiGate is located can handle the extra load needed for the remote APs.
- Determine if you want to tunnel all traffic from the remote wireless client to the FortiGate or just a select subset of the

internal or corporate networks (Split Tunneling).

> If you are only tunneling a subset of your internal or corporate networks, a security client such as FortiClient with URL Filtering and Anti-malware (or another security product) should be used to protect the remote client from becoming compromised and used to access corporate resources.

- Determine how remote sites will provide IP address to the remote AP once it's deployed.

Reference guides

You can refer to the following guides for using FortiAuthenticator (FAC) or Microsoft NPS Server as a RADIUS server:

- WiFi RADIUS authentication with FortiAuthenticator in the *FortiAuthenticator Cookbook*.
- WiFi with WSSO using Windows NPS and user groups on page 45.

Configuring FortiGate before deploying remote APs

Before you can deploy your remote FortiAPs, you must perform the following actions on your FortiGate:

1. Configuring the FortiGate interface on page 70
2. Creating a FortiAP profile for teleworkers on page 70
3. Enabling split tunneling on SSIDs on page 72
4. Encrypting CAPWAP communication on page 72

Configuring the FortiGate interface

1. On the external facing interface that the FortiAP will connect over the internet to, enable either:
   - CAPWAP on devices running FortiOS 6.2.2 and earlier.

   - Security Fabric Connection on devices running FortiOS 6.2.3 and later.

Creating a FortiAP profile for teleworkers

We recommend creating a separate FortiAP profile for teleworkers so you can apply split tunneling and encryption to devices in that profile.

To enable split tunneling options

By default, split tunneling options are not visible in the FortiGate GUI and must be made visible from the CLI.

1. From the FortiGate CLI, enter the following to display the options on the GUI:

    ```
    config system settings
        set gui-fortiap-split-tunneling enable
    end
    ```
2. Once you enable the split tunneling option, return to the FortiGate GUI and create the FortiAP profile.

To create a FortiAP profile

Once you enable split tunneling options in the GUI, you can create a FortiAP profile for teleworkers and apply it. In the FortiAP profile, you can also specify the SSIDs that the FortiAP will broadcast.

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and create the FortiAP profile for your remote workers.
2. Set an **AP login password** so users at remote sites cannot log in to the unit with default credentials.
3. In the newly visible Split Tunneling section, enable **Include Local Subnet** as needed.

    The behavior for this option varies depending on which split tunnel method you configure. See Configuring split tunnel behavior on page 72 for more details.

4. Enable **Split Tunneling Subnet(s)** and enter IP subnets as needed.

    The behavior for this option varies depending on which split tunnel method you configure. See Configuring split tunnel behavior on page 72 for more details.
5. In **SSIDs**, you can select **Manual** to limit which SSIDs can be used at the remote teleworker's site instead of exposing all corporate SSIDs in a potentially unsecure location.
6. When you are finished configuring the profile, click **OK**.

For more comprehensive instructions on how to create a FortiAP profile, refer to Creating a FortiAP profile in the *FortiWiFi and FortiAP Configuration Guide*.

Configuring split tunnel behavior

Once you enable split tunneling and create a FortiAP profile, you can further configure how split tunneling is handled in each profile.

There are two methods the FortiAP can use to tunnel networks from the remote AP:

- **Tunnel:** Define the subnets in the profile that you *want* to tunnel to the FortiGate. These are usually the IP subnets that contain internal corporate applications such as file shares.

  Uncheck the **Include Local Subet** option in the FortiAP profile if you want the remote wireless client to be able to communicate with internal devices at their home/remote site.

- **Local:** Define the subnets that you *do not* want to be tunneled back to the FortiGate. Use this method if you want all traffic to be inspected by the FortiGate, including traffic destined for the internet. This method is more secure but can add latency to the user's internet browsing.

  Check the **Include Local Subnet** option in the FortiAP profile if you want the remote wireless client to be able to communicate with internal devices at their home/remote site

To configure split tunnel behavior

1. From the FortiGate CLI, enter the following commands to change the split tunneling behavior in a FortiAP profile:

```
config wireless-controller wtp-profile
  edit <teleworker_profile_name>
    set split-tunneling-acl-path {tunnel | local}
  end
end
```

Enabling split tunneling on SSIDs

Once you create your FortiAP profile, you need to enable split tunneling on the SSIDs you want to use on the remote APs.

To enable split tunneling on SSIDs

1. Go to **WiFi & Switch Controller > SSIDs** and edit the SSIDs the remote AP will use.
2. Enable **Split tunneling**.
3. Click **OK**.

Encrypting CAPWAP communication

The default DTLS setting for CAPWAP communication over the internet is `clear-text`, meaning it's non-encrypted. You can enable IPSEC or DTLS for more security. IPSEC is preferred for most modern FortiGates because the NP6 and SOC3/4 SPUs can offload IPSEC data more efficiently than DTLS.

For more information about each encryption method, see Data channel security: clear-text, DTLS, and IPsec VPN on page 19.

To enable encryption

1. From the FortiGate CLI, enter the following commands to edit the FortiAP profile:

```
config wireless-controller wtp-profile
   edit <teleworker_profile_name>
      set dtls-policy {clear-text | dtls-enabled | ipsec-vpn}
   end
end
```

Configuring FortiAPs to connect to FortiGate

Once you finish configuring your FortiGate, you can begin to configure your FortiAPs for deployment.

There are two ways to configure and deploy your FortiAPs:

- Deploying with FortiAP Cloud on page 73
- Deploying without FortiAP Cloud on page 74

Deploying with FortiAP Cloud

1. Log in to your FortiAP Cloud account with your FortiCloud credentials at:

   https://www.fortiapcloud.com

2. In top top-right of the page, click **Inventory**.

The Inventory page loads.

3. Select how you want to import FortiAPs to the Cloud.
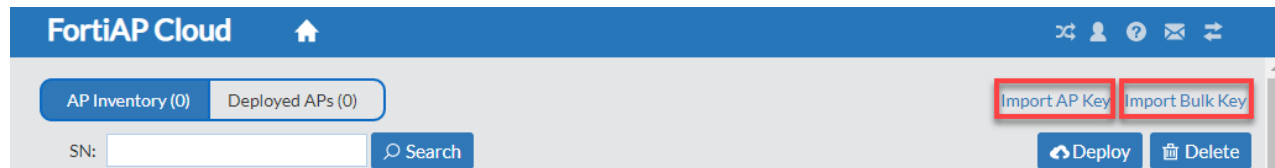
- **Import AP Key:** Import individual FortiAPs by entering their FortiCloud Key
- **Import Bulk Key:** Enter a Bulk key that you've obtained from Fortinet Support, or from purchasing FortiDeploy.

4. Once you've added your devices to FortiAP Cloud, select the FortiAP(s) you want to deploy and click **Deploy**.

5. In the Deploy to AP Network pop up, select **Deploy to External AC**.

6. Enter the Public Facing WAN IP Address (or FQDN that points to the WAN IP Address) of the External AC (FortiGate), then click **Deploy**.

   FortiAP Cloud configures the WTP Profile on the FAP to statically point to the public facing WAN address of the FortiGate.

Deploying without FortiAP Cloud

To configure and deploy your FortiAP

1. Plug the FortiAP you want to deploy into a port or VLAN that has DHCP configured.
   - If no DHCP server is available, the default IP information to log in to the AP is:

     IP Address: 192.168.1.2

     Subnet Mask: 255.255.255.0

     DGW: 192.168.1.1

2. Look for the assigned IP Address on the router or DHCP server.

   If no DHCP server is available, use a cross-over cable to connect your Ethernet port directly to the LAN port on the AP.

    Note: You might need a power adapter for the FortiAP if POE is not available.

3. From a web browser, access your FortiAP at https://<FAP-IP> where <FAP-IP> is the IP address of the FortiAP.

4. Log in with username `admin` and no password.

5. From the FortiAP page, click **Local Configuration**.

6. In the **AC Discovery Type** field, select how you want the FortiAP to discover the controller and complete any required fields:

   This guide only covers the options relevant to setting up a remote AP. For comprehensive information, refer to Advanced WiFi controller discovery in the *FortiWiFi and FortiAP Configuration Guide*.

   - **Auto:** Automatically cycle through all six of the discovery methods until it establishes an AC connection.
   - **Static:** Provide up to three Static IP Addresses (most likely the public facing IP addresses for remote workers).
   - **DHCP:** Use DHCP Option 138.
   - **DNS:** Provide up to three FQDN entries that are resolvable by the FortiAP.
   - **FortiAP Cloud:** Enter your FortiAP Cloud username and password.

7. In the **AP Data Channel Security** field, select **IPsec Enabled**.

8. Click **OK** to save your changes.

Applying configurations to multiple FortiAPs

If you have multiple FortiAPs that you need to configure, you can save a backup configuration file and use the restore function to apply these configurations to other FortiAPs. In order for this method to work, the firmware version of all your FortiAPs must match.

To apply configurations to multiple FortiAPs

1. From your FortiAP page, in the top right corner, click to expand the **admin** menu.
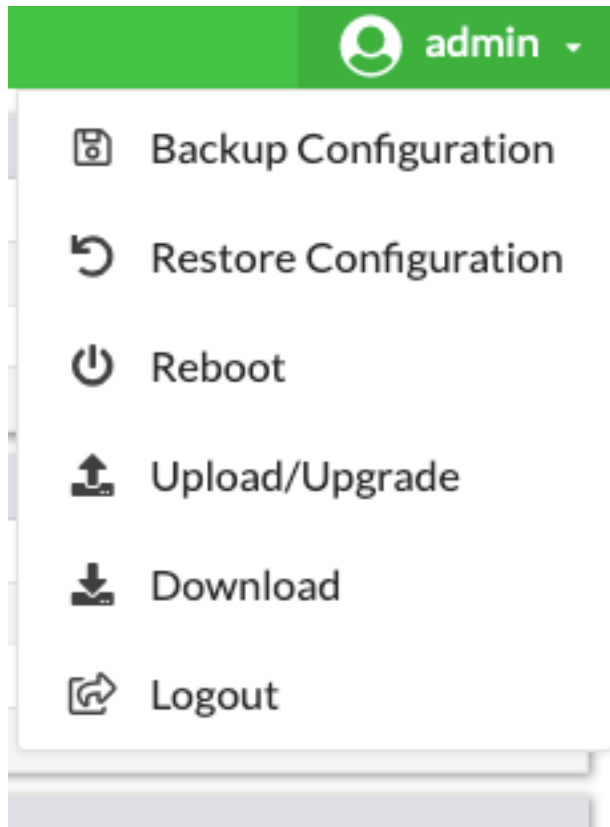
2. Click **Backup Configuration** to save a configuration file.
3. Log in to the FortiAP page that you want to apply to configuration to.
4. Click to expand the **admin** menu.
5. Click **Restore Configuration** and select the configuration file you created.

Final FortiGate configuration tasks

After you set the method for tunneling back to the FortiAP, the remote user needs to plug the FortiAP into their home router that has DHCP enabled. The FortiAP boots up and attempts to discover the FortiGate using the settings applied in under WTP Configuration. If the discovery attempt is successful, the FortiGate shows the FortiAP on the list of Managed FortiAPs with a status of "Waiting for Authorization on the FortiGate".

To authorize and complete remote FortiAP setup

1. From your FortiGate, navigate to **WiFi & Switch Controller > Managed FortiAPs**.
2. Locate and right-click the FortiAP and select **Authorize**.

   Note: If you have Security Fabric configured, navigate first to **Security Fabric > Settings** and the right-click to authorize from the Root FortiGate.

3. Once your FortiAP is authorized, right-click and select **Assign Profile**.
4. Assign the profile you created for your remote FortiAPs.
5. The FortiAP should come online and your remote users can connect to the wireless network through their AP.

> * To keep track of your remote APs, you can rename each FortiAP to identify where it is deployed.
> * To better manage your remote and on-site APs, you can create FortiAP groups and apply a profile to multiple APs of the same model.

Other

This section contains other topics about configuring WiFi:

UTM security profile groups on FortiAP-S

This guide provides instructions for simple configuration of security profile groups for FortiAP, including creating security profile groups and selecting profile groups for the SSID.

> This feature only works for local bridge SSIDs.

To configure UTM security profile groups on the FortiWiFi and FortiAP GUI:

1. Create a security profile group:
   a. Go to *WiFi & Switch Controller > Security Profile Groups*, then click *Create New*.
   b. Enter the desired interface name. Configure logging as desired.
   c. Enable Antivirus, Web Filter, Application, IPS, or Botnet, then select the desired profile.
2. Create a local bridge mode SSID and enable security profile groups:
   a. Go to *WiFi & Switch Controller > SSID*. Select *SSID*, then click *Create New*.
   b. Enter the desired interface name. For *Traffic mode*, select *Bridge*.
   c. In the *SSID* field, enter the desired SSID name. Configure security as desired.
   d. Enable *Security Profile Group*, then select the group created in step 1.
   e. Click *OK*.
3. Select the SSID on a managed FortiAP by editing the FortiAP profile. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C:
   a. Go to *WiFi & Switch Controller > FortiAP Profile*. Select the FAP320C-default profile, then click *Edit*.
   b. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
   c. To broadcast the SSID from 5 G radio, scroll to *Radio 2 > SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
   d. Click *OK*.

To configure UTM security profile groups using the FortiWiFi and FortiAP CLI:

1. Create a security profile group:
```
config wireless-controller utm-profile
    edit "wifi-UTM"
        set ips-sensor "default"
        set application-list "default"
        set antivirus-profile "default"
        set webfilter-profile "default"
        set scan-botnet-connections block
    next
end
```

2. Create a local bridge mode SSID and enable security profile groups:
```
config wireless-controller vap
    edit "wifi-vap"
        set ssid "SSID-UTM"
        set passphrase 12345678
        set local-bridging enable
        set schedule "always"
        set utm-profile "wifi-UTM"
    next
end
```

3. Select the SSID on a managed FortiAP by editing the FortiAP profile. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C:
```
config wireless-controller wtp
    edit "FP320C3X14000640"
        set admin enable
        set wtp-profile "FAP320C-default"
    next
end
config wireless-controller wtp-profile
    edit "FAP320C-default"
        config radio-1
            set vap-all disable
            set vaps "wifi-vap"
        end
        config radio-2
            set vap-all disable
            set vaps "wifi-vap"
        end
    next
end
```

1+1 fast failover between FortiGate WiFi controllers

The following shows a simple network topology for this recipe. The primary and secondary FortiGates must be routed into subnets and NAT must not be done on the traffic. The FortiAP must be able to reach both the primary and secondary FortiGates.
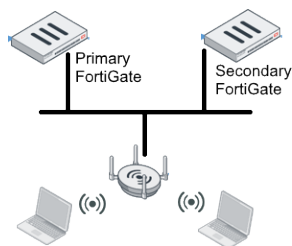
The following takes place in the event of a failover:

1. The primary FortiGate syncs the wireless configuration to the secondary FortiGate.
2. If the primary FortiGate fails, the secondary FortiGate takes over management of the FortiAP. The client can still connect with the SSID from the FortiAP and pass traffic.
3. When the primary FortiGate is back online, it returns to managing the FortiAP.

In the CLI example below, the primary FortiGate has an IP address of 10.43.1.80, and the secondary FortiGate has an IP address of 10.43.1.62.

To configure the primary FortiGate:

```
config wireless-controller inter-controller
   set inter-controller mode 1+1
   set inter-controller key 123456
   config inter-controller-peer
      edit 1
         set peer-ip 10.43.1.62
         set peer-priority secondary
      next
   end
```

To configure the secondary FortiGate:

```
config wireless-controller inter-controller
   set inter-controller mode 1+1
   set inter-controller key 123456
   set inter-controller-pri secondary
   config inter-controller-peer
      edit 1
         set peer-ip 10.43.1.80
      next
   end
```

To run diagnose commands:

1. On the primary FortiGate, run the `diagnose wireless-controller wlac -c ha` command. The output should resemble the following:
   ```
   WC fast failover info
   cfg iter: 1 (age=17995, size=220729, fp=0x5477e28)
   dhcpd_db iter: 123 (age=132, size=1163, fp=0x5435930)
   dhcpd_ipmac iter: 123 (age=132, size=2860, fp=0x587d848)
   mode: 1+1-ffo
   pri: primary
   key csum: 0x9c99
   max: 10
   wait: 10
   ```

```
peer cnt: 1
    FWF60E4Q16027198: 10.43.1.62:5245 secondary UP (age=0)
```

2. On the secondary FortiGate, run the `diagnose wireless-controller wlac -c ha` command. The output should resemble the following:

```
WC fast failover info
mode: 1+1-ffo
status: monitoring
pri: secondary
key csum: 0x43e
max: 10
wait: 10
peer cnt: 1
    FG22E1T919900557: 10.43.1.80:5246 primary UP (age=0)
        dfile 0 iter 1 (age=133, size=1564731/1564731)
        dfile 1 iter 1 (age=163, size=0/0)
        dfile 2 iter 1 (age=163, size=0/0)
```

> ⚠️ You cannot use FortiGate Clustering Protocol and Wireless 1+1 fast failover together. They are two different HA features and cannot be combined.

CAPWAP Offloading (NP6 only)

Simple Network Topology

NP6 offloading over CAPWAP traffic is supported by all high-end and most mid-range FortiGate models.

NP6 offloading over CAPWAP configuration

NP6 offloading over CAPWAP traffic is supported with traffic from tunnel mode virtual APs. The WTP data channel DTLS policy (`dtls-policy`) must be set to `clear-text` or `ipsec-vpn` in the WTP profile (*wireless-controller wtp-profile*). Traffic is not offloaded if it is fragmented.

NP6 session fast path requirements:

1. Enable offloading managed FortiAP and FortiLink CAPWAP sessions:

```
config system npu
    set capwap-offload enable
end
```

2. Enable offloading security profile processing to CP processors in the policy:

```
config firewall policy
    edit 1
        set auto-asic-offload enable
    next
end
```

Verify the system session of NP6 offloading

- Check the system session, when dtls-policy=clear-text to verify npu info: *flag=0x81/0x89, offload=8/8*

```
FG1K2D3I16800192 (vdom1) # diagnose sys session list
    session info: proto=6 proto_state=01 duration=21 expire=3591 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=5
    origin-shaper=
    reply-shaper=
    per_ip_shaper=
    class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
    state=log may_dirty npu f00
    statistic(bytes/packets/allow_err): org=16761744/11708/1 reply=52/1/1 tuples=2
    tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
    orgin->sink: org pre->post, reply pre->post dev=57->37/37->57
gwy=172.16.200.44/10.65.1.2
    hook=post dir=org act=snat 10.65.1.2:50452->172.16.200.44:5001(172.16.200.65:50452)
    hook=pre dir=reply act=dnat 172.16.200.44:5001->172.16.200.65:50452(10.65.1.2:50452)
    pos/(before,after) 0/(0,0), 0/(0,0)
    misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=1
    serial=00009a97 tos=ff/ff app_list=0 app=0 url_cat=0
    rpdb_link_id = 00000000
    dd_type=0 dd_mode=0
    npu_state=0x000c00
    npu info: flag=0x81/0x89, offload=8/8, ips_offload=0/0, epid=158/216, ipid=216/158,
vlan=0x0000/0x0000
    vlifid=216/158, vtag_in=0x0000/0x0000 in_npu=2/2, out_npu=2/2, fwd_en=0/0, qid=4/2
total session 1
```

- Check the system session, when dtls-policy=ipsec-vpn to verify npu info: *flag=0x81/0x82, offload=8/8*

```
FG1K2D3I16800192 (vdom1) # diagnose sys session list
    session info: proto=6 proto_state=01 duration=7 expire=3592 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=5
    origin-shaper=
    reply-shaper=
    per_ip_shaper=
    class_id=0 ha_id=0 policy_dir=0 tunnel=/wlc-004100_0 vlan_cos=0/255
    state=log may_dirty npu f00
    statistic(bytes/packets/allow_err): org=92/2/1 reply=92/2/1 tuples=2
    tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
    orgin->sink: org pre->post, reply pre->post dev=57->37/37->57
gwy=172.16.200.44/10.65.1.2
    hook=post dir=org act=snat 10.65.1.2:50575->172.16.200.44:5001(172.16.200.65:50575)
    hook=pre dir=reply act=dnat 172.16.200.44:5001->172.16.200.65:50575(10.65.1.2:50575)
    pos/(before,after) 0/(0,0), 0/(0,0)
    misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=1
    serial=0000a393 tos=ff/ff app_list=0 app=0 url_cat=0
    rpdb_link_id = 00000000
    dd_type=0 dd_mode=0
    npu_state=0x000c00
    npu info: flag=0x81/0x82, offload=8/8, ips_offload=0/0, epid=158/216, ipid=216/158,
vlan=0x0000/0x0000
    vlifid=216/158, vtag_in=0x0000/0x0000 in_npu=2/2, out_npu=2/2, fwd_en=0/0, qid=0/0
total session 1
```

Airtime fairness

WiFi has a natural tendency for clients farther away or clients at lower data rates to monopolize the airtime and slow down overall performance. Airtime fairness helps to improve the overall network performance in these conditions.

Airtime fairness has these characteristics:

- Only applies to downlink traffic.
- Can be set on both 2.4 GHz and 5 GHz radio bands.
- Can be set per-SSID. Each VAP is granted airtime according to the percentage assigned to the VAP.
- Can apply to all kinds of VAP (Bridge, Tunnel, or Mesh) and all kinds of authentication (Open, PSK, or Enterprise).
- Only applies to data and is not for control or management.

Airtime fairness is balanced from TX side from AP to client since that's the only direction under the control of AP.

Sample topology and usage
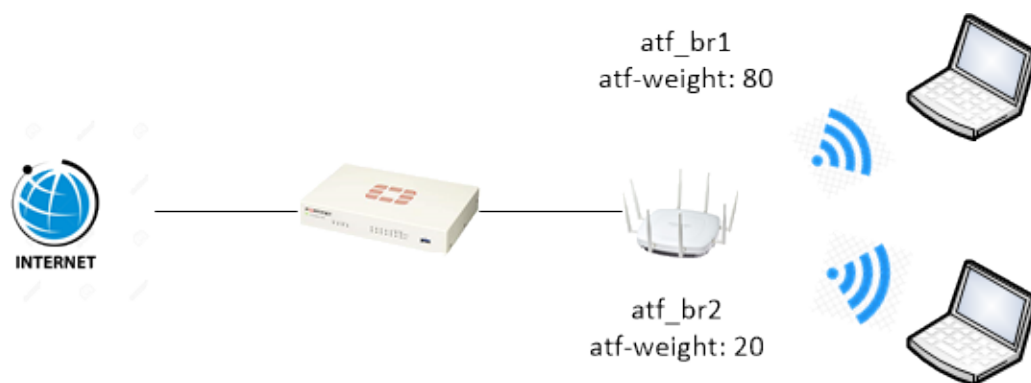
For example, there are two Bridge mode SSIDs with a wireless client and an airtime fairness weight of 80% and 20%. Using WaveDynamix to simulate the same traffic from Ethernet to the wireless client, the traffic for each SSID matches the airtime fairness weight assigned to them.

Airtime fairness is not related to SSID type or authentication type. In this example, it uses Bridge mode SSID and Open Authentication.

You must use the CLI to configure this function.

To set the airtime fairness weight in SSID:

The default `atf-weight` is 20 so there is no need to set this option for `atf_br2`.

```
config wireless-controller vap
    edit "atf_br1"
        set atf-weight 80
        set ssid "atf_br1"
        set security open
        set local-bridging enable
        set schedule "always"
    next
end
```

```
config wireless-controller vap
    edit "atf_br2"
        set ssid "atf_br2"
        set security open
        set local-bridging enable
        set schedule "always"
    next
end
```

To enable airtime fairness in radio:

This example uses one FAP-S423E unit with airtime fairness enabled on the 5 GHz radio band.

```
config wireless-controller wtp-profile
    edit "S423E_atf"
        config platform
            set type S423E
        end
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ac
            set airtime-fairness enable
            set vap-all disable
            set vaps "atf_br1" "atf_br2"
            set channel "149"
        end
        set ext-info-enable enable
    next
end

config wireless-controller wtp
    edit "PS423E3X16000029"
        set admin enable
        set wtp-profile "S423E_atf"
        config radio-2
        end
    next
end
```

To verify the airtime fairness weight from FAP:

```
PS423E3X16000029 # cw_diag -c atf
Airtime Fairness Info:
 interface                        ssid  configured-atf      applied-atf
    Radio 0 ATF disabled
    Radio 1 ATF enabled
    wlan10                    atf_ssid1             80                80
    wlan11                    atf_ssid2             20                20

PS423E3X16000029 # wlanconfig wlan10 showatfinfo
                    SHOW   RADIO   ATF   TABLE
WLAN:SSID/Client(MAC Address)      Air time(%)    Config ATF(%%)    Assoc
 wlan10:atf_ssid1                       80.0            80.0
```

```
  wlan11:atf_ssid2                          20.0              20.0
  ------:Unallocated Airtime                 0.0
```

Verify the airtime fairness weight from real traffic

Using WaveDynamix to create two same clients connected with two SSIDs, downlink traffic is passed from Ethernet to the wireless client with the same bit rate.

This example shows that `tx_bytes` from `atf_br1` is almost four times higher than `atf_br2`.

To view traffic statistics from SSID1:

```
PS423E3X16000029 # cw_diag -d vap 90:6C:AC:8A:66:10
  VAP extension info
Radio 1 VAP 0:
    tx_packets                 : 60543
    tx_bytes                   : 70608777
    tx_data_packets            : 60543
    tx_data_bytes              : 70608777
    tx_datapyld_bytes          : 68308143
    tx_ucast_data_packets      : 57462
    tx_mbcast_data_packets     : 3081
    tx_discard                 : 94193
```

To view traffic statistics from SSID2:

```
PS423E3X16000029 # cw_diag -d vap 90:6C:AC:8A:66:11
  VAP extension info
Radio 1 VAP 1:
    tx_packets                 : 18839
    tx_bytes                   : 19731946
    tx_data_packets            : 18839
    tx_data_bytes              : 19731946
    tx_datapyld_bytes          : 19016064
    tx_ucast_data_packets      : 15760
    tx_mbcast_data_packets     : 3079
    tx_discard                 : 84924
```

Extended logging

Extended logging information in these four key areas help WiFi troubleshooting: Association, Authentication, DHCP, and DNS.

The detailed wireless event logs show client connection procession to help IT administrators troubleshoot WiFi connection problems. The FortiAP can send more detailed events of client connections (such as probe, associate, authentication, 4-way handshake, DHCP), and FortiGate can create associated logs of these event.
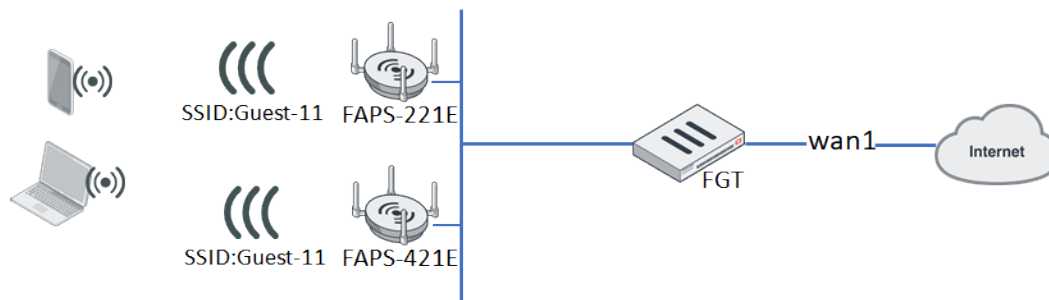
New probe, authentication, and associate logs when wireless clients try to connect a broadcasted SSID with any security-mode

Probe request and response logs

Action	Description	Message	Detail
probe-req	Probe request from wireless station	AP received probe request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:52 logid="0104043681" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Probe request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="probe-req" reason="Reserved 0" msg="AP received probe request frame from client f0:98:9d:76:64:c4" remotewtptime="49.326391"
probe-resp	Probe response to wireless station	AP sent probe response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:52 logid="0104043682" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Probe response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="probe-resp" reason="Reserved 0" msg="AP sent probe response frame to client f0:98:9d:76:64:c4" remotewtptime="49.326459"

Authentication request and response logs

Action	Description	Message	Detail
auth-req	Authentication request from wireless station	AP received authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043675" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Authentication request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="auth-req" reason="Reserved 0" msg="AP received authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="44.902962"
auth-resp	Authentication response to wireless station	AP sent authentication response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043676" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Authentication response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="auth-resp" reason="Reserved 0" msg="AP sent authentication response frame to client f0:98:9d:76:64:c4" remotewtptime="44.903038"

Associate request and response logs

Action	Description	Message	Detail
assoc-req	Association request from wireless station	AP received association request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043677" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Association request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="assoc-req" reason="Reserved 0" msg="AP received association request frame from client f0:98:9d:76:64:c4" remotewtptime="44.915155"
assoc-resp	Association response to wireless station	AP sent association response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043679" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Association response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="assoc-resp" reason="Reserved 0" msg="AP sent association response frame to client f0:98:9d:76:64:c4" remotewtptime="44.916829"

New WPA 4-Way handshake logs when wireless clients try to connect WPA2-Personal/WPA2-Enterprise SSID

Complete WPA 4-Way handshake logs

Action	Description	Message	Detail
WPA-1/4-key-msg	AP sent 1/4 message of 4 way handshake to wireless client	AP sent 1/4 message of 4-way handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043650" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="AP sent 1/4 message of 4 way handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-1/4-key-msg" reason="Reserved 0" msg="AP sent 1/4 message of 4-way handshake to client f0:98:9d:76:64:c4" remotewtptime="44.920791"
WPA-2/4-key-msg	Wireless client sent 2/4 message of 4 way handshake	AP received 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043651" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless client sent 2/4 message of 4 way handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-2/4-key-msg" reason="Reserved 0" msg="AP received 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="44.926647"
WPA-3/4-key-msg	AP sent 3/4 message of 4 way handshake to wireless client	AP sent 3/4 message of 4-way handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043652" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="AP sent 3/4 message of 4 way handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-3/4-key-msg" reason="Reserved 0" msg="AP sent 3/4 message of 4-way handshake to client f0:98:9d:76:64:c4" remotewtptime="44.928406"
WPA-4/4-key-msg	Wireless client sent 4/4 message of 4 way handshake	AP received 4/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043653" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless client sent 4/4 message of 4 way handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-4/4-key-msg" reason="Reserved 0" msg="AP received 4/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="44.933383"

Invalid 2/4 handshake logs with wrong PSK input

Action	Description	Message	Detail
WPA-invalid-2/4-key-msg	Wireless client 4 way handshake failed with invalid 2/4 message	Probably wrong password entered, invalid MIC in 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:41:02 logid="0104043648" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548981661 logdesc="Wireless client 4 way handshake failed with invalid 2/4 message" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=11 security="WPA2 Personal" encryption="AES" action="WPA-invalid-2/4-key-msg" reason="Reserved 0" msg="Probably wrong password entered, invalid MIC in 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="0.0"

New RADIUS authentication logs when clients connect WPA2-Enterprise with User-group or Radius-auth SSID

RADIUS authenticate success log when client pass authentication

Action	Description	Message	Detail
RADIUS-auth-success	Wireless client RADIUS authentication success	Wireless client RADIUS authentication success	date=2019-01-30 time=14:36:09 logid="0104043630" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548887768 logdesc="Wireless client RADIUS authentication success" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="RADIUS-auth-success" reason="Reserved 0" msg="Client f0:98:9d:76:64:c4 RADIUS authentication success" remotewtptime="0.0"

RADIUS authenticate failure log when client fails to pass authentication

Action	Description	Message	Detail
RADIUS-auth-failure	Wireless client RADIUS authentication failure	Client f0:98:9d:76:64:c4 RADIUS authentication failure	date=2019-01-30 time=14:35:51 logid="0104043629" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548887750 logdesc="Wireless client RADIUS authentication failure" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="RADIUS-auth-failure" reason="Reserved 0" msg="Client f0:98:9d:76:64:c4 RADIUS authentication failure" remotewtptime="0.0"

New RADIUS MAC authentication logs when clients try to connect a SSID with radius-mac-auth enabled

RADIUS MAC authenticate success log when client passes RADIUS MAC authentication

Action	Description	Message	Detail
RADIUS-MAC-auth-success	Wireless client RADIUS MAC authentication success	Client b4:ae:2b:cb:d1:72 RADIUS MAC authentication success	date=2019-01-30 time=15:54:40 logid="0104043633" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548892477 logdesc="Wireless client RADIUS MAC authentication success" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="b4:ae:2b:cb:d1:72" channel=6 security="WPA2 Personal" encryption="AES" action="RADIUS-MAC-auth-success" reason="Reserved 0" msg="Client b4:ae:2b:cb:d1:72 RADIUS MAC authentication success" remotewtptime="0.0"

RADIUS MAC authenticate failure log when client fails to pass RADIUS MAC authentication

Action	Description	Message	Detail
RADIUS-MAC-auth-success	Wireless client RADIUS MAC authentication success	Client 1c:87:2c:b6:a8:49 RADIUS MAC authentication failure	date=2019-01-30 time=15:47:42 logid="0104043632" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548892061 logdesc="Wireless client RADIUS MAC authentication failure" sn="FP320C3X17001909" ap="320C-TEST" vap="stability3" ssid="Guest-11" radioid=2 stamac="1c:87:2c:b6:a8:49" channel=40 security="WPA2 Personal" encryption="AES" action="RADIUS-MAC-auth-failure" reason="Reserved 0" msg="Client 1c:87:2c:b6:a8:49 RADIUS MAC authentication failure" remotewtptime="0.0"

New DHCP logs when clients try to acquire IP after connected

Complete DHCP Discover/Offer/Request/ACK logs

Action	Description	Message	Detail
DHCP-DISCOVER	Wireless station sent DHCP DISCOVER	DHCP DISCOVER from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043663" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless station sent DHCP DISCOVER" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-DISCOVER" reason="N/A" msg="DHCP DISCOVER from client f0:98:9d:76:64:c4" remotewtptime="45.123652"
DHCP-OFFER	DHCP server sent DHCP OFFER	DHCP OFFER of IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:49 logid="0104043664" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886189 logdesc="DHCP server sent DHCP OFFER" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-OFFER" reason="N/A" msg="DHCP OFFER of IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4" remotewtptime="46.156969"
DHCP-REQUEST	Wireless station sent DHCP REQUEST	DHCP REQUEST for IP 11.10.80.2 offered by server 11.10.80.1 from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:50 logid="0104043666" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Wireless station sent DHCP REQUEST" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-REQUEST" reason="N/A" msg="DHCP REQUEST for IP 11.10.80.2 offered by server 11.10.80.1 from client f0:98:9d:76:64:c4" remotewtptime="47.243792"
DHCP-ACK	DHCP server sent DHCP ACK	DHCP ACK for IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:50 logid="0104043667" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="DHCP server sent DHCP ACK" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-ACK" reason="N/A" msg="DHCP ACK for IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4" remotewtptime="47.246381"

Error logs when DHCP failure happens

Action	Description	Message	Detail
DHCP-NAK	DHCP server sent DHCP NAK	IP address not assigned, DHCP NAK from server 11.10.80.1 for client b4:ae:2b:cb:d1:72	date=2019-01-30 time=15:22:08 logid="0104043661" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548890528 logdesc="DHCP server sent DHCP NAK" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-NAK" reason="requested address not available" msg="IP address not assigned, DHCP NAK from server 11.10.80.1 for client b4:ae:2b:cb:d1:72" remotewtptime="289.83561"
DHCP-no-response	Wireless station DHCP process failed with no server response	DHCP server not responding for client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:39:07 logid="0104043658" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046347 logdesc="Wireless station DHCP process failed with no server response" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-no-response" reason="N/A" msg="DHCP server not responding for client b4:ae:2b:cb:d1:72" remotewtptime="457.629929"
DHCP-no-ACK	No DHCP ACK from server	No DHCP ACK for IP 11.10.80.3 requested by client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:38:56 logid="0104043660" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046336 logdesc="No DHCP ACK from server" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-no-ACK" reason="N/A" msg="No DHCP ACK for IP 11.10.80.3 requested by client b4:ae:2b:cb:d1:72" remotewtptime="448.236740"
DHCP-self-assigned-IP	Wireless station is using self-assigned IP	Detected self assigned IP 169.254.210.208 of client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:38:51 logid="0104043670" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046330 logdesc="Wireless station is using self-assigned IP" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-self-assigned-IP" reason="N/A" msg="Detected self assigned IP 169.254.210.208 of client b4:ae:2b:cb:d1:72" remotewtptime="441.742363"

New GTK-Rekey logs when clients perform gtk-rekey

Action	Description	Message	Detail
WPA-group-1/2-key-msg	AP sent 1/2 message of group key handshake to wireless client	AP sent 1/2 message of group key handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=15:12:01 logid="0104043654" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548889920 logdesc="AP sent 1/2 message of group key handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="WPA-group-1/2-key-msg" reason="Reserved 0" msg="AP sent 1/2 message of group key handshake to client f0:98:9d:76:64:c4" remotewtptime="3778.128070"
WPA-group-2/2-key-msg	Wireless client sent 2/2 message of group key handshake	AP received 2/2 message of group key handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=15:12:01 logid="0104043655" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548889920 logdesc="Wireless client sent 2/2 message of group key handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="WPA-group-2/2-key-msg" reason="Reserved 0" msg="AP received 2/2 message of group key handshake from client f0:98:9d:76:64:c4" remotewtptime="3778.228253"

New Fast-BSS-Transition (FT) logs when 802.11r clients roam between 2 FAPs

FT logs when clients succeed to roaming

Action	Description	Message	Detail
FT-action-req	Wireless client sent FT action request	AP received FT action request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043642" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="Wireless client sent FT action request" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=1 security="WPA2 Personal" encryption="AES" action="FT-action-req" reason="Reserved 0" msg="AP received FT action request frame from client f0:98:9d:76:64:c4" remotewtptime="146.847041"

Action	Description	Message	Detail
FT-action-resp	FT action response was sent to wireless client	AP sent FT action response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043643" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="FT action response was sent to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=1 security="WPA2 Personal" encryption="AES" action="FT-action-resp" reason="Reserved 0" msg="AP sent FT action response frame to client f0:98:9d:76:64:c4" remotewtptime="146.849137"
FT-reassoc-req	Wireless client sent FT re-association request	AP received FT re-association request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043646" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="Wireless client sent FT reassociation request" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=40 security="WPA2 Personal" encryption="AES" action="FT-reassoc-req" reason="Reserved 0" msg="AP received FT reassociation request frame from client f0:98:9d:76:64:c4" remotewtptime="146.899110"
FT-reassoc-resp	FT re-association response was sent to wireless client	AP sent FT re-association response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043647" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="FT reassociation response was sent to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=40 security="WPA2 Personal" encryption="AES" action="FT-reassoc-resp" reason="Reserved 0" msg="AP sent FT reassociation response frame to client f0:98:9d:76:64:c4" remotewtptime="146.904372"
FT-auth-req	Wireless client sent FT auth request	AP received FT authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043644" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548982158 logdesc="Wireless client sent FT auth request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-auth-req" reason="Reserved 0" msg="AP received FT authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="1805.311496"

Action	Description	Message	Detail
FT-auth-resp	FT auth response was sent to wireless client	AP sent FT authentication response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043645" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548982158 logdesc="FT auth response was sent to wireless client" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-auth-resp" reason="Reserved 0" msg="AP sent FT authentication response frame to client f0:98:9d:76:64:c4" remotewtptime="1805.312777"

Error logs when FT failure

Action	Description	Message	Detail
FT-invalid-action-req	Wireless client sent invalid FT action request	Receive invalid FT request action frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:17 logid="0104043639" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548982157 logdesc="Wireless client sent invalid FT action request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-invalid-action-req" reason="Reserved 0" msg="Receive invalid FT request action frame from client f0:98:9d:76:64:c4" remotewtptime="0.0"
FT-invalid-auth-req	Wireless client sent invalid FT auth request	Receive invalid FT authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043640" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548982157 logdesc="Wireless client sent invalid FT auth request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-invalid-auth-req" reason="Reserved 0" msg="Receive invalid FT authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="0.0"

New DNS error logs in DNS service failure

Action	Description	Message	Detail
DNS-no-domain	Wireless station DNS process failed due to non-existing domain	DNS lookup of uop.umeng.com from client 3c:2e:ff:83:91:33 failed with \"non-existing domain\"	date=2019-02-01 time=09:42:03 logid="0104043673" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549042922 logdesc="Wireless station DNS process failed due to non-existing domain" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="3c:2e:ff:83:91:33" security="WPA2 Personal" encryption="AES" action="DNS-no-domain" reason="Server 100.100.16.172 replied \"non-existing domain\"" msg="DNS lookup of uop.umeng.com from client 3c:2e:ff:83:91:33 failed with \"non-existing domain\"" remotewtptime="1130.445518"