

# Deploying Remote APs

FortiAP 7.0.0



**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](mailto:techdoc@fortinet.com)



Feb 2, 2024

FortiAP 7.0.0 Deploying Remote APs

20-700-623260-20240202

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Deploying secured remote APs for the Teleworker</b> .....	<b>5</b>
<b>Configuring FortiGate before deploying remote APs</b> .....	<b>7</b>
Configuring the FortiGate interface .....	7
Creating a FortiAP profile for teleworkers .....	7
Configuring split tunnel behavior .....	8
Enabling split tunneling on SSIDs .....	9
Encrypting CAPWAP communication .....	9
<b>Final FortiGate configuration tasks</b> .....	<b>10</b>

## Change Log

Date	Change Description
2022-03-23	Initial release.
2024-02-02	Updated <a href="#">Configuring FortiAPs to connect to FortiGate</a> .

# Deploying secured remote APs for the Teleworker

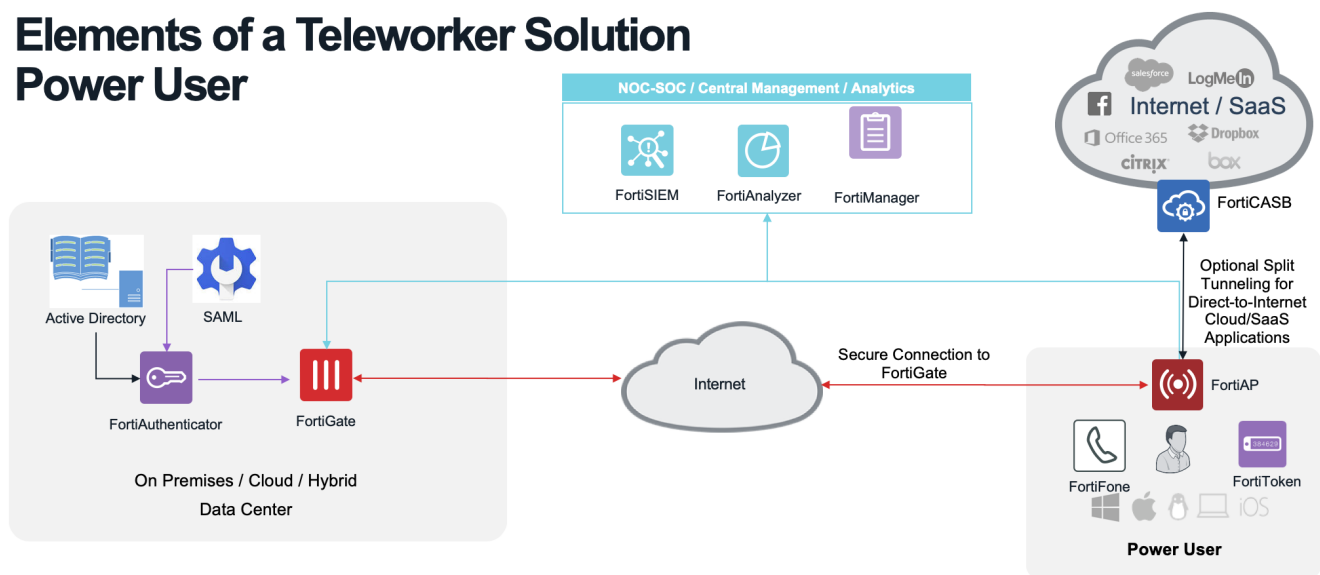
Remote WLAN FortiAP models enable you to provide a pre-configured WiFi access point to a remote or traveling employee. Once plugged in at home or in a hotel room, the FortiAP automatically discovers the enterprise FortiGate WiFi controller over the Internet and broadcasts the same wireless SSID used in the corporate office. Communication between the WiFi controller and the FortiAP is secure, eliminating the need for a VPN.

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

1. [Configuring FortiGate before deploying remote APs on page 7](#)
2. [Configuring FortiAPs to connect to FortiGate](#)
3. [Final FortiGate configuration tasks on page 10](#)

## 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 FortiLAN 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 either 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](#) in the *FortiWiFi and FortiAP Configuration Guide*.

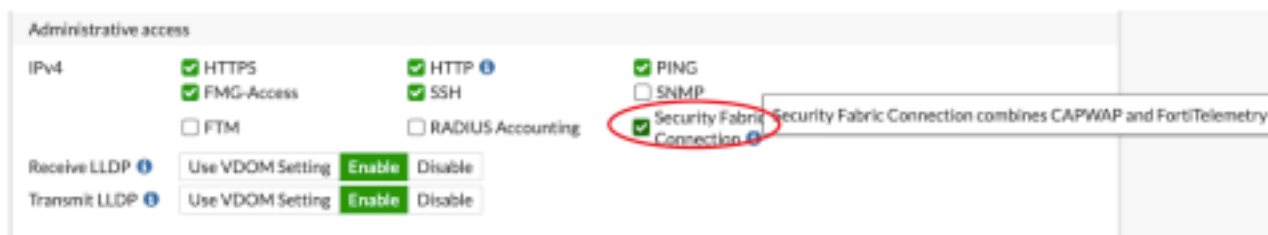
# Configuring FortiGate before deploying remote APs

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

1. [Configuring the FortiGate interface on page 7](#)
2. [Creating a FortiAP profile for teleworkers on page 7](#)
3. [Enabling split tunneling on SSIDs on page 9](#)
4. [Encrypting CAPWAP communication on page 9](#)

## Configuring the FortiGate interface

1. On the external facing interface that the FortiAP will connect over the internet to, enable **Security Fabric Connection**.



## 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 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 8](#) for more details.

The screenshot shows the 'New FortiAP Profile' configuration interface. The 'Split Tunneling' section is highlighted with a red box. It contains two options: 'Include Local Subnet' with an information icon and a toggle switch that is turned on, and 'Split Tunneling Subnet(s)' with a toggle switch that is turned off. Other visible fields include Name, Comments, Platform (FAP221E), Country / Region (Use default (United States)), AP login password (Set, Leave Unchanged), Administrative access (HTTPS, SSH), and Client load balancing (Frequency Handoff, AP Handoff).

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 8](#) 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 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.



- **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 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](#) in the *FortiWiFi and FortiAP Configuration Guide*.

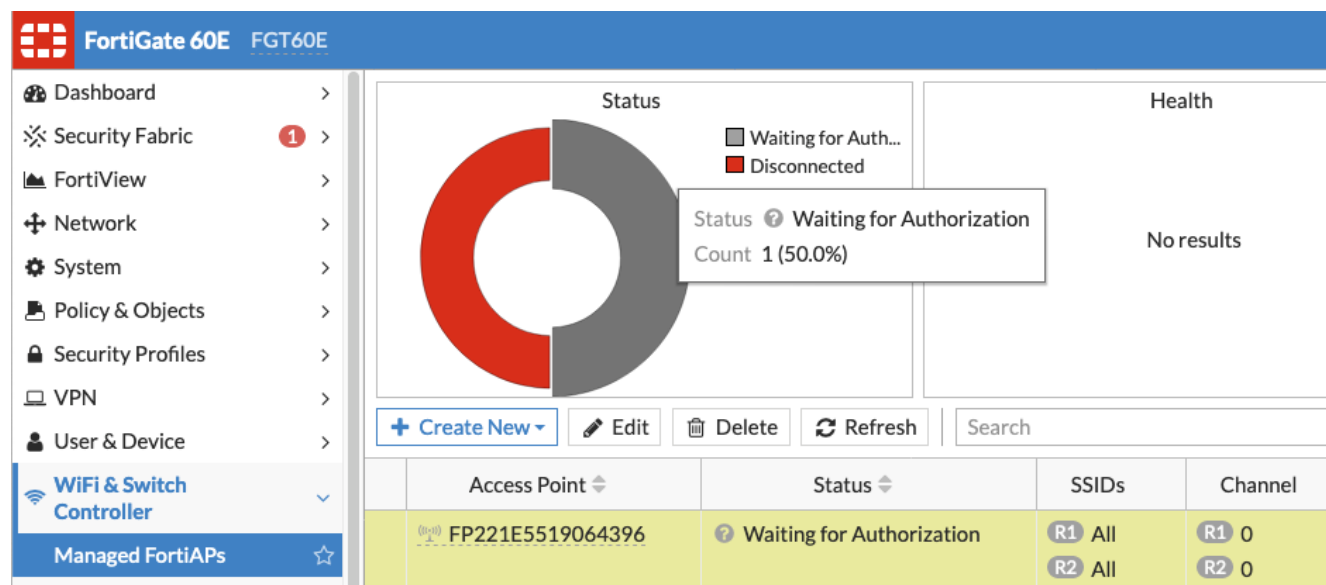
### To enable encryption

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
```

## Final FortiGate configuration tasks

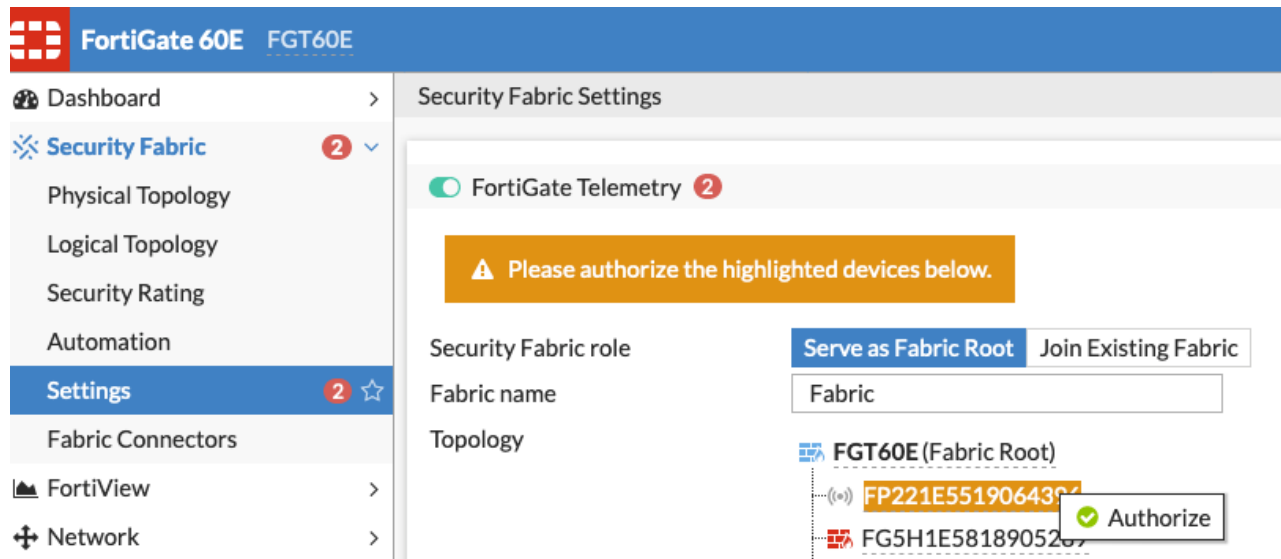
After you set the method for tunneling back to the FortiAP, the remote user needs to plug the FortiAP into their home router that has DHCP enabled. The FortiAP boots up and attempts to discover the FortiGate using the settings applied in under WTP Configuration. If the discovery attempt is successful, 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 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.



FortiGate 60E FGT60E

Dashboard > Security Fabric Settings

Security Fabric 2

Physical Topology

Logical Topology

Security Rating

Automation

Settings 2 ☆

Fabric Connectors

FortiView >

Network >

FortiGate Telemetry 2

Please authorize the highlighted devices below.

Security Fabric role: Serve as Fabric Root | Join Existing Fabric

Fabric name: Fabric

Topology:

- FGT60E (Fabric Root)
- FP221E5519064307 (highlighted)
- FG5H1E5818905207

Authorize

- Once your FortiAP is authorized, right-click and select **Assign Profile**.
- Assign the profile you created for your remote FortiAPs.
- The FortiAP comes 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.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.