



Secure SD-Branch - ZTP Framework with FortiManager

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



March 30, 2022

Secure SD-Branch 6.4 ZTP Framework with FortiManager

02-646-761262-20220330

TABLE OF CONTENTS

Change Log	4
Introduction	5
Intended audience	5
Design overview	6
Uses cases and topologies	6
Design considerations	8
Product versions and models	8
Deployment methods with FortiManager	9
FortiSwitch deployment method	9
FortiAP deployment method	10
FortiExtender deployment method	11
Configuration with FortiManager	12
Creating a FortiGate model device	12
Configuring FortiSwitch	13
Defining VLANs	14
Defining FortiSwitch templates	18
Creating a FortiSwitch model device	20
Assigning FortiSwitch templates	20
Installing FortiSwitch configuration to FortiGate	21
Configuring FortiAP	22
Defining SSIDs	23
Defining AP profiles	28
Creating a model device and assigning a profile	29
Modifying the FortiSwitch template	30
Installing the AP configuration to FortiGate	30
Configuring FortiExtender	31
Configuring FortiExtender with CLI templates	31
Creating a normalized interface for FortiExtender	32
Adding FortiExtender to an SD-WAN template	33
Installing FortiExtender configuration to FortiGate	33
Configuring security policies	34
Editing normalized interfaces for FortiAPs	34
Updating policy packages	35
Deployment verification	38
Verifying FortiGate connectivity with FortiManager	38
Verifying FortiSwitch devices	38
Verifying FortiAP devices	40
Verifying FortiExtender devices	40

Change Log

Date	Change Description
2022-01-12	Initial release.
2022-03-30	Added tip to Creating a FortiGate model device on page 12 .

Introduction

This guide aims to leverage different Fortinet Security Fabric components, such as FortiGate, FortiManager, FortiAP, FortiSwitch, and FortiExtender, in an effort to provide a clearer understanding of reference configurations for real-life use cases.

As mentioned in the [SD-WAN / SD-Branch Architecture for MSSPs](#) document, a fundamental starting point for SD-Branch is the delivery of SD-WAN as-a-service. When it comes to selecting the right SD-Branch solution, service providers have multiple options and need to carefully weigh each option. Factors such as orchestration, management, TCO (total cost of ownership), and security all impact ARPU (average revenue per user) potential over time. Therefore, this guide will focus on delivering architectures that leverage **central management, templates, and zero touch provisioning (ZTP)** while providing a recommended configuration approach.

Intended audience

This design guide has primarily been created for a technical audience, including system architects and design engineers, who want to deploy and configure Fortinet Secure SD-Branch, or even extend their current Fortinet Secure SD-WAN offering.

It assumes the reader is familiar with the basic concepts of applications, networking, routing, security, and high availability and has a basic understanding of network and datacenter architectures. For implementation, a working knowledge of FortiOS networking and policy configuration is ideal.

Design overview

This section contains the following topics:

- [Uses cases and topologies on page 6](#)
- [Design considerations on page 8](#)
- [Product versions and models on page 8](#)

Uses cases and topologies

Fortinet Secure SD-Branch can be defined as a natural extension of an existing Fortinet Secure SD-WAN architecture. As such, this guide will not provide details about SD-WAN configuration. For details about SD-WAN configuration, see the following guides:

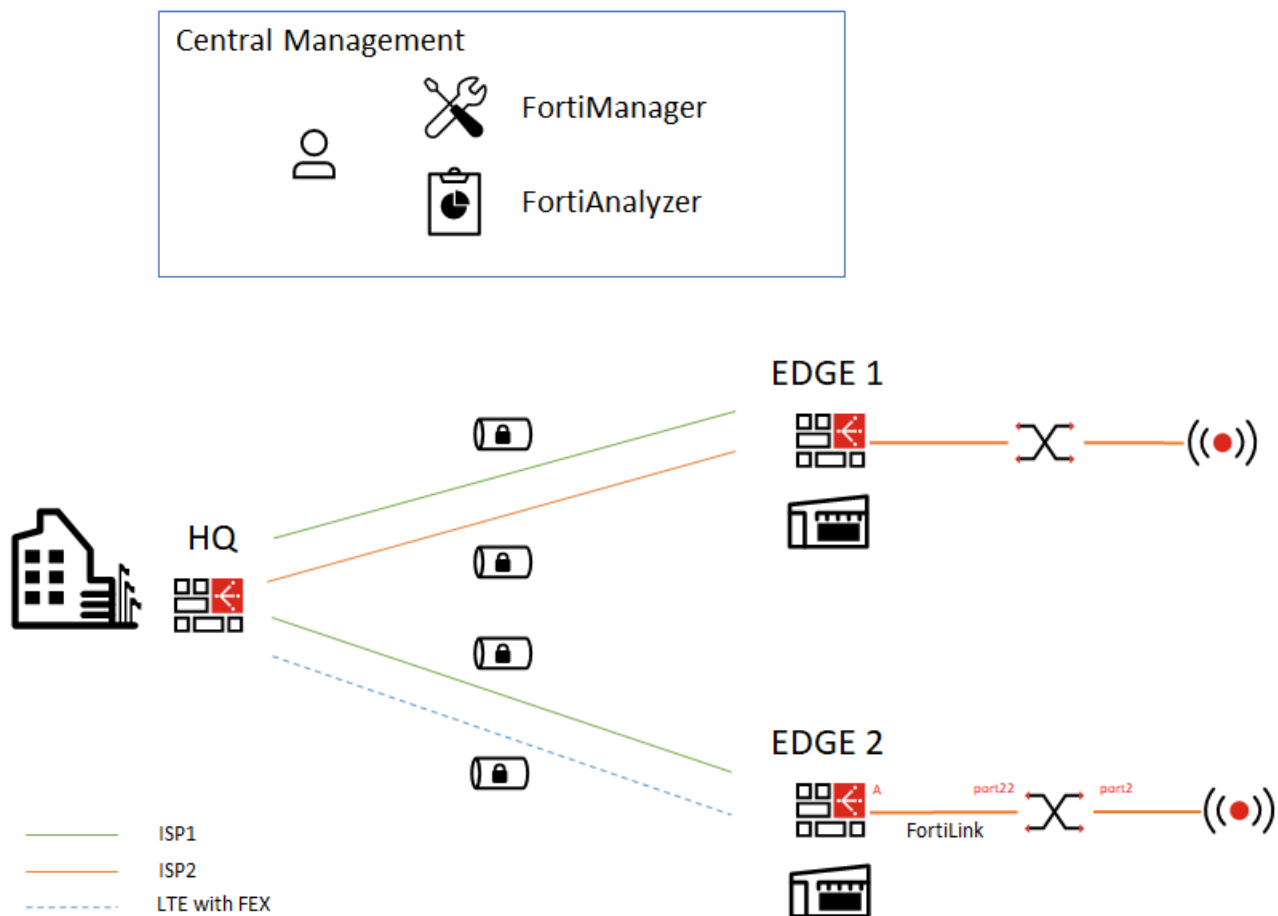
- [SD-WAN Architecture for MSSPs](#)
- [SD-WAN Deployment for MSSPs](#)

Instead this guide will focus on the implementation of remote branches that leverage wireless and wired LAN by using FortiGate as a distributed controller and by using FortiManager/FortiAnalyzer as central management / reporting platforms. Because this guide does not provide details about some parts of the configuration related to routing, overlay, and SD-WAN, it is strongly recommended to read the [SD-WAN Deployment for MSSPs](#) document before reading this guide.

This guide aims to deliver best practice guidelines for deploying a Fortinet Secure SD-Branch architecture that is optimized for ZTP of an entire branch, including wired, wireless, and LTE connectivity. One key requirement of such a deployment is the capability to minimize the number of manual operations while still providing a high degree of flexibility.

The reference topology used in this deployment guide uses the following devices:

- FortiGates
Three FortiGates are used. One FortiGate is used at the headquarter (HQ) office, and the other two FortiGates represent the two branch offices named EDGE1 and EDGE2.
- FortiSwitch
- FortiAP
- FortiExtender



On the HQ and EDGE1 FortiGates, we connected two internet links. On EDGE2, a single internet link is enabled, and we will later add 4G connectivity with a FortiExtender.



The FortiExtender is an appliance that provides [enterprise-class LTE/5G connectivity](#) and can easily be integrated as an extension of the SD-WAN fabric. FortiExtender can be used as a standalone router, or FortiExtender can be managed by FortiGate or FortiCloud. In standalone mode, the FortiExtender must be configured directly from its management interface (GUI or CLI), which may not be ideal for mass deployments. You can also use FortiCloud, which is a SaaS platform that provides fleet management for FortiExtender. However, for the ZTP use case, it is best to use the FortiGate managed mode to have a single management platform for our SD-Branch approach.

Two IPsec overlays are configured on the *HQ* and on *EDGE1*, and BGP is used to exchange routes. We will configure *EDGE2* to build two IPsec overlays on top of ISP1 and a 4G link with the FortiExtender.



The FortiManager is reachable through the Hub and will be used to deploy, manage and monitor all the devices.

Users and devices can then connect to the SD-WAN architecture by using either wired or wireless LAN access.

For wired LAN access, FortiSwitches are available in a variety of models to address needs [from the access layer to the datacenter](#). All models can be managed and configured directly from FortiGate.

For wireless LAN access, FortiAPs are available in a variety of models, from 2x2 to 4x4 or with an internal or external antenna, to address specific use cases and price points.

Design considerations

FortiSwitch, FortiAP, and FortiExtender will be controlled by their respective branch FortiGate, and the configuration will be done exclusively by using FortiManager for central management. The base example will include a single FortiSwitch and a single FortiAP. However, it is possible to use multiple devices on a single branch to provide redundancy, more coverage, and so on.

For more information about the maximum number of devices that a FortiGate can manage, see the [FortiGate Product Matrix](#).

Product versions and models

This document is aligned with the following software releases:

Product	Software release
FortiOS	6.4.6 or later
FortiManager	6.4.6 or later
FortiAnalyzer	6.4.6 or later
FortiAP	6.4.6 or later
FortiSwitch	6.4.6 or later
FortiExtender	4.2.3 or later

This document references the following sites and models:

Site	Model
FortiGate H1	FGT-VM
FortiGate EDGE1	FortiGate 60F
FortiGate EDGE2	FortiGate 40F
FortiAP EDGE2	FortiAP 231F
FortiSwitch EDGE2	FortiSwitch 124F-PoE
FortiExtender EDGE2	FortiExtender 201E

Deployment methods with FortiManager

In this section, we will review each type of branch device along with its recommended method of deployment. While it is entirely possible to configure devices directly by using a FortiGate GUI, we avoid this method because it is inefficient for large deployments, and may lead to misconfiguration and discrepancies between branches. Instead we will use the following FortiManager templates to configure and deploy our devices:

- FortiSwitch templates
- AP templates
- CLI templates

FortiManager supports the following deployment methods, depending on the type of device:

1. **Device discovery:** a device is connected to an already deployed and configured FortiGate, and is then discovered and configured by using FortiManager.
2. **Model device:** a model device is a representation of the final configuration in the FortiManager database that can be provisioned before the device is physically connected. For details, see the [SD-WAN Deployment Guide for MSSPs](#) document.

This section contains the following topics:

- [FortiSwitch deployment method on page 9](#)
- [FortiAP deployment method on page 10](#)
- [FortiExtender deployment method on page 11](#)

FortiSwitch deployment method

FortiGates use FortiLink to control FortiSwitches. FortiLink defines the management interface and the remote management protocol between FortiGate and FortiSwitch. Depending on the model of FortiGate and FortiSwitch, specific ports will be dedicated for use by FortiLink, but you can modify the ports if necessary. For more information on how to configure FortiLink and its options, see the [Device Managed by FortiOS](#) documentation.

For our example, FortiLink is configured by default on the FortiGate 60F named *EDGE2*. FortiLink includes both port *a* and *b* of the FortiGate, so we can connect our FortiSwitch to either port *a* or *b*:

The screenshot shows the FortiGate 60F web interface for 'sdbranch-demo-edge1'. The left sidebar shows the 'Network' menu with 'Interfaces' selected. The main area is 'Edit Interface' for 'fortilink'. The 'Type' is 'FortiLink (802.3ad Aggregate)'. The 'Addressing mode' is 'Dedicated to FortiSwitch'. The 'IP/Netmask' is '169.254.1.1/255.255.255.0'. The 'Connected devices' section shows '1 FortiSwitch(es)'. A blue box with an information icon states 'A DHCP server will be automatically generated.' The 'Status' on the right is 'Up' with MAC address 'e0:23:ff:69:c2:e8'.



By default, FortiLink uses a **non-routable subnet** to assign an IP address to each FortiSwitch. We may want to change the addressing of this interface/DHCP server to later access the FortiSwitch for monitoring purposes (such as monitoring with SNMP).

On the FortiSwitch, we may use any of the dedicated management ports to connect to our FortiGate. In our example we will use *port22* of FortiSwitch 124F-PoE.

FortiAP deployment method

FortiAPs will also be controlled by FortiGate. Contrary to the FortiSwitch device, which is connected to FortiGate, it is more practical to connect FortiAP to FortiSwitch. To manage our FortiAP, we will later use the FortiSwitch Manager module in FortiManager to create a dedicated management VLAN named *AP_Management* along with a DHCP server.

It is not necessary to create a specific management VLAN for our FortiAPs. Instead we can use one of the following options:

1. Use an extra management VLAN that is created on FortiSwitch to manage our FortiAPs.
The extra VLAN runs a DHCP server and can be routed with or without SNMP monitoring. An extra VLAN is useful if we want to completely separate our SSID network from our wired network by using only SSIDs in tunnel mode.
2. Place our FortiAP in the same VLAN as our wired clients.
The FortiAPs will receive an IP address on the LAN network and can have an SSID bridging the wireless clients to the wired network as well as SSIDs in tunnel mode.

In both case, we need to make sure that the *Secure Fabric Connection* option is enabled and that the interface runs a DHCP server.

In our example, we will use the first option and create a dedicated management VLAN with an isolated network.



As this guide focuses on central management and deployment of SD-Branches, we don't configure the advanced options and specific details pertaining to a WiFi deployment. It is **strongly** recommended to perform site surveys, spectrum analysis, and coverage mappings to determine the ideal AP placement.

FortiExtender deployment method

FortiExtender will also be controlled by FortiGate. As this feature might not be enabled by default on the FortiGate, we need to enable it before we can see the menu in FortiGate:

```
config system global
    set fortiextender enable
end
```

By default, the FortiExtender port1, port2, port3 form a LAN virtual switch that runs a DHCP server. The DHCP server provides IP addresses in the 192.168.200.0/24 subnet and offers internet access when LTE is up. This is useful if you want to use FortiExtender for internet access to provide FortiGate ZTP. On the contrary, port4 runs a DHCP client, which means we could select a subnet to address the FortiExtender from the FortiGate.

In our case, we will use port1 to illustrate what should be configured in a ZTP scenario, and we will then manage FortiExtender from FortiGate.

On FortiGate, we need to set an interface to run as DHCP client and enable the *Secure Fabric Connection* option. In our example, we will use *wan2*; however, we may use any physical interface for that purpose. If we are using the second interface of FortiLink (port *b*), we must make sure to add `FortiExtender` to the DHCP `vci-string` to ensure it is discovered by our FortiGate along with the switches:

```
set vci-string "FortiSwitch" "FortiExtender"
```

From the FortiGate perspective, *wan2* will be used as a management interface to interact with and control the FortiExtender (on the control plane), but it will not be used to send data. In order to use FortiExtender WAN access, we must create a virtual interface of type `fext-wan` that can later be included in our SD-WAN configuration.

Other scenarios are possible, such as using two FortiExtenders at a time, in active-backup or active-active mode. For more information, see the [FortiExtender Administration Guide](#).

Configuration with FortiManager

In the section, we will create the necessary templates on FortiManager and prepare the EDGE2 branch for zero touch provisioning of the FortiGate along with a FortiSwitch, a FortiAP and a FortiExtender. We will use model devices to preconfigure our devices before they are connected to FortiManager.

A model device is a virtual representation of a real device in the database of FortiManager. A model device allows an administrator to apply different templates (including but not exclusively limited to system templates, FortiAP templates, FortiSwitch templates, CLI templates, SD-WAN templates, and policy packages) to a device before connecting the device to FortiManager.

In this section, we will do the following by using FortiManager:

1. Use the *Device Manager* module to create a model device for the FortiGate 60F. See [Creating a FortiGate model device on page 12](#).
2. Use the *FortiSwitch Manager* module to configure FortiSwitch. See [Configuring FortiSwitch on page 13](#).
3. Use the *AP Manager* module to configure FortiAP. See [Configuring FortiAP on page 22](#).
4. Prepare a FortiExtender configuration to onboard FortiExtender after ZTP. See [Configuring FortiExtender on page 31](#).
5. Use the *Policy & Objects* module to create security policies. See [Configuring security policies on page 34](#).

Creating a FortiGate model device

In FortiManager, we will start by creating a model device for the FortiGate 60F. After the model device is created, we will use it again later when we assign templates to it for our FortiSwitch, FortiAP, and FortiExtender devices.



Some FortiGate model devices include a default policy to allow inside to outside access using a specified interface, for example WAN1.

As SD-WAN members may not use interfaces that are referenced directly in firewall policies, you must remove this reference by deleting the policy before installing the SD-WAN template.

This can be done manually through the CLI or GUI, or by installing a new policy package to the device that does not contain the default policy.

For more information on how to provision a FortiGate model device and the associated SD-WAN configuration (such as underlay, routing, overlay, SD-WAN and security), see the [SD-WAN Deployment for MSSPs](#) document.

To create a model device:

1. In FortiManager, go to *Device Manager > Device & Groups*.
2. Click *Add Device*. The *Add Device* wizard displays.

3. Click *Add Model Device*, and add a model device for a FortiGate 60F, which we will use as our branch EDGE2:

Add Device

☒ Add Model Device

Name:

Link Device By: ☒ Serial Number ☐ Pre-shared Key

Serial Number:

Device Model:

☒ Enforce Firmware Version:

☒ Add to Device Group: (1 Entry Selected)

☐ Add to Folder:

☒ Assign Policy Package:

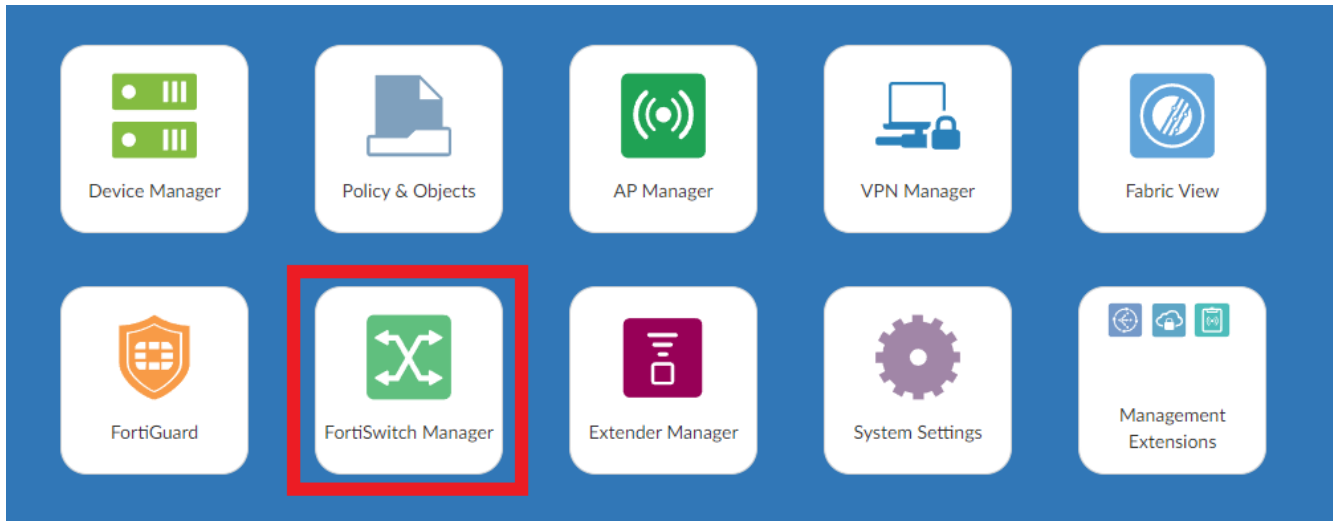
☒ Assign Provisioning Template:

< Previous Next > Cancel

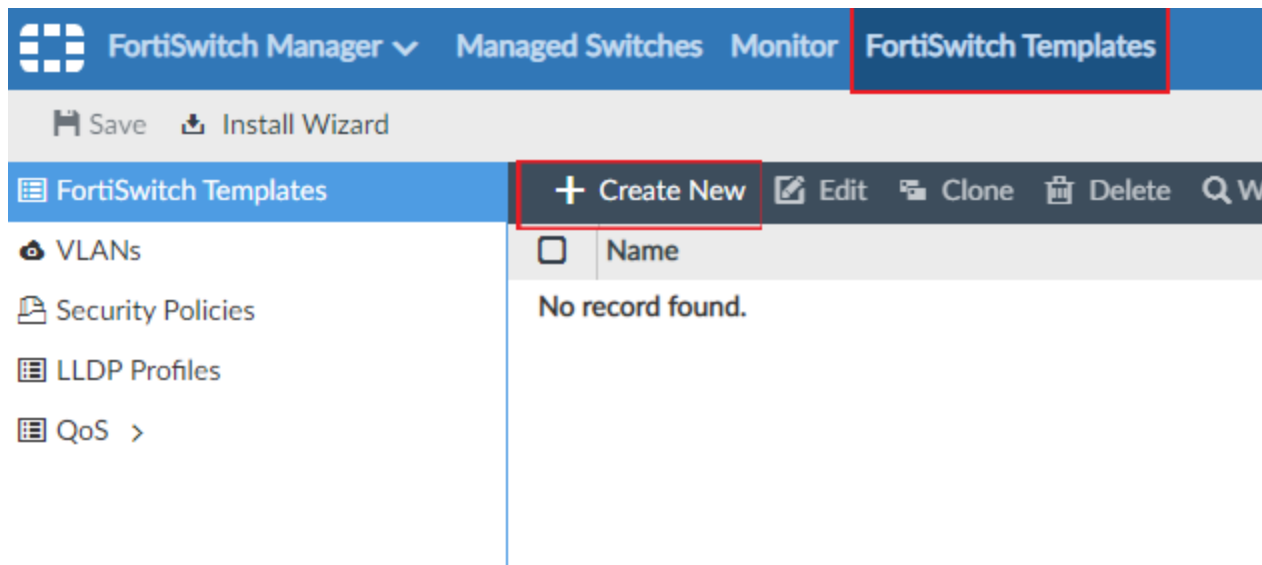
The model device will be used again in the following sections when we assign templates to it for our FortiSwitch, FortiAP, and FortiExtender devices.

Configuring FortiSwitch

In this section, we will use the *FortiSwitch Manager* module in FortiManager to create a template that can be used by our FortiSwitch. Once created, the template can be assigned to a model device or to a connected FortiSwitch, which will then inherit the configuration.



In *FortiSwitch Manager*, each model of FortiSwitch needs a specific template where you can assign your VLANs, define LLDP profiles, QoS profiles, and so on.



Following is an overview of how to use *FortiSwitch Manager* to create FortiSwitch templates:

1. Define VLANs. See [Defining VLANs on page 14](#).
2. Define a FortiSwitch template, and select VLANs. See [Defining FortiSwitch templates on page 18](#).
3. Create a FortiSwitch model device that is associated with FortiGate. See [Creating a FortiSwitch model device on page 20](#).
4. Assign the FortiSwitch template to the FortiSwitch model device. See [Assigning FortiSwitch templates on page 20](#).
5. Install the FortiSwitch configuration to FortiGate. See [Installing FortiSwitch configuration to FortiGate on page 21](#).

Defining VLANs

Before we can select VLANs in a FortiSwitch template, we must define the VLANs. For the sake of simplicity, we will only create a VLAN named *Wired_Lan* for our wired clients. More VLANs can be added to cover different use cases. The

VLAN named *Wired_Lan* will run a DHCP server.

As mentioned in [FortiAP deployment method on page 10](#), we also need to create a VLAN named *AP_Management* that will be assigned to *port2*, where we will connect our FortiAP. We will use the VLAN named *AP_Management* to manage our FortiAPs, and we need to enable *Secure Fabric Connection* on the interface.

Please note that any options defined in the VLAN will be applied to all FortiSwitches that are attached to the template. This may be convenient when we need a VLAN that always has the *same subnet on all branches*. However most deployments need a way to specify a different subnet for each branch. You can specify a different subnet for each branch by using the following methods:

1. Use the per-device mapping feature when you define a VLAN by using the GUI. The per-device mapping feature lets you define a specific subnet, a DHCP server range, or any other relevant setting.
2. Use CLI templates with meta fields to define the subnet, DHCP server range, or any other relevant setting.

While the per-device mapping feature provides some visibility in the GUI, it is not the most practical method for large SD-WAN deployments, as subnets will most probably need to be specified in other templates, such as routing for example.

This topic includes the following sections:

- [Defining the Wired_Lan VLAN with the GUI on page 15](#)
- [Defining the Wired_Lan VLAN with CLI templates on page 17](#)
- [Defining the AP_Management VLAN with the GUI on page 18](#)

Defining the Wired_Lan VLAN with the GUI

In this section we use the FortiManager GUI to create a VLAN named *Wired_Lan* with the per-device mapping feature enabled.

To define the Wired_LAN VLAN with the GUI:

1. In FortiManager, go to *FortiSwitch Manager > FortiSwitch Templates > VLANs*.
2. Click *Create New*, and define a VLAN named *Wired_LAN*.

The screenshot displays the FortiManager GUI for configuring a new VLAN. The left sidebar shows the navigation menu with 'FortiSwitch Templates' selected, and 'VLANs' highlighted under the 'FortiSwitch Manager' tab. The main content area is titled 'Create New VLAN Definition' and contains the following configuration sections:

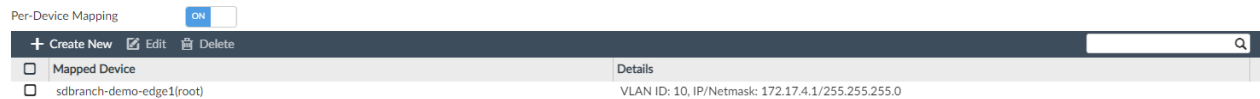
- Interface Name:** Wired_Lan
- VLAN ID:** 10
- Role:** DMZ, LAN (selected), UNDEFINED, WAN
- Address:**
 - Addressing mode: Manual (selected), DHCP, PPPoE
 - IP/Netmask: 0.0.0.0/0.0.0.0
 - IPv6 Addressing mode: Manual (selected), DHCP
 - IPv6 Address/Prefix: ::/0
 - Create address object matching subnet: OFF
- Restrict Access:**
 - Administrative Access:
 - HTTPS, SNMP, FMG-Access, DNP: OFF
 - PING: ON
 - HTTP, RADIUS Accounting, FTM: OFF
 - SSH, TELNET, Probe Response, Security Fabric Connection: OFF
 - IPv6 Administrative Access:
 - HTTPS, SNMP, FMG-Access: OFF
 - PING, HTTP: OFF
 - SSH, TELNET, Security Fabric Connection: OFF
- DHCP Server:** OFF (selected), Server, Relay
- Networked Devices:**
 - Device Detection: ON
 - Active Scanning: OFF
- Admission Control:**
 - Security Mode: CAPTIVE-PORTAL, NONE (selected)
- Miscellaneous:**
 - Secondary IP Address: OFF
- Status:**
 - Description: (empty text box)
 - Interface State: Enabled (selected), Disabled
 - Color: (color picker icon)
- IPv4 Advanced Options >**
- IPv6 Advanced Options >**
- Per-Device Mapping:** OFF



Any options that we define in the VLAN will be applied to all FortiSwitches that are attached to the template. This may be convenient when we need a VLAN that always has the same subnet on all branches.

3. If you want to define a specific subnet, a DHCP server range, or any other relevant setting, set *Per-Device Mapping* to *ON*, and click *Create New* to create a mapped device.

With per-device mapping enabled and configured, we can directly see the list of branches and their assigned subnets on the GUI:



Defining the Wired_Lan VLAN with CLI templates

Below is an example of a CLI template for the VLAN named `Wired_Lan` that uses variables and meta fields. The CLI template is applied directly to the FortiGate. We use the CLI template to modify the subnet of the VLAN on the FortiGate while still using the template to assign it to FortiSwitch ports.

```
config system interface
  edit "Wired_Lan"
    set type vlan
    set vdom "root"
    set ip $(wired_lan_net:4,1) $(wired_lan_netmask)
    set role lan
    set interface "fortilink"
    set vlanid 10
  next
end
config system dhcp server
  edit 1
    set dns-service default
    set ntp-service default
    set default-gateway $(wired_lan_net:4,1)
    set netmask $(wired_lan_netmask)
    set interface "Wired_Lan"
  next
end
config ip-range
  edit 1
    set start-ip $(wired_lan_net:4,10)
    set end-ip $(wired_lan_net:4,250)
  next
end
next
end
```

Please note that we are using CLI template syntax to set and modify our variables. In the CLI template example, `$(wired_lan_net:4,1)` means use the `wired_lan_net` meta-field content, but change the last bytes with the value 1. For example, if `wired_lan_net = 10.0.0.0`, then the IP address of the `Wired_Lan` interface would be `10.0.0.1`.



For more information on CLI template syntax, see the [FortiManager 6.2 New Features Guide](#).

CLI template is the recommended method for large deployments as it allows an admin to configure a list of predefined variables that are necessary to deploy a full branch while streamlining the whole process.

Defining the AP_Management VLAN with the GUI

We will also create our VLAN named *AP_Management*. Again, we could use the VLAN named *Wired_Lan* for our FortiAPs, if we wanted to bridge our wireless clients into the wired network. We may use the same subnet for all our branches, and ensure that you select *Secure Fabric Connection* to allow our FortiAPs to communicate with our FortiGate (on the control plane).

To define the AP_Management VLAN with the GUI:

1. In FortiManager, go to *FortiSwitch Manager > FortiSwitch Templates > VLANs*.
2. Click *Create New*, and define a VLAN named *AP_Management*.

Create New VLAN Definition

Interface Name: AP_Management
 VLAN ID: 999
 Role: DMZ LAN UNDEFINED WAN

Address
 Addressing mode: Manual DHCP PPPoE
 IP/Netmask: 172.31.31.1/255.255.255.0
 IPv6 Addressing mode: Manual DHCP
 IPv6 Address/Prefix: ::0
 Create address object matching subnet: OFF

Restrict Access
 Administrative Access: ☐ HTTPS ☒ PING ☐ SSH
☐ SNMP ☐ HTTP ☐ TELNET
☐ FMG-Access ☐ RADIUS Accounting ☐ Probe Response
☐ DNP ☐ FTM ☒ Security Fabric Connection
 IPv6 Administrative Access: ☐ HTTPS ☐ PING ☐ SSH
☐ SNMP ☐ HTTP ☐ TELNET
☐ FMG-Access ☐ Security Fabric Connection

DHCP Server
 OFF Server Relay

IP Range

Start IP	End IP
172.31.31.10	172.31.31.250

Network Mask: Same as Interface Specify
Default Gateway: Same as Interface Specify
Next Server: 0.0.0.0
DNS Service: Specify Use System DNS Setting (Default) Same as Interface IP (Local)
NTP Service: Specify Use System NTP Setting (Default) Use FortiGate as NTP Server (Local)
FortiClient On-Net Status: ON
Timezone Option: Specify Disable Default

IP Address Assignment Rules

Type	Match Criteria	Action	IP	Description
Implicit	Unknown MAC address	Assign IP		

Advanced... (DNS, WINS, Custom Options, Exclude Ranges.) >
 Networked Devices

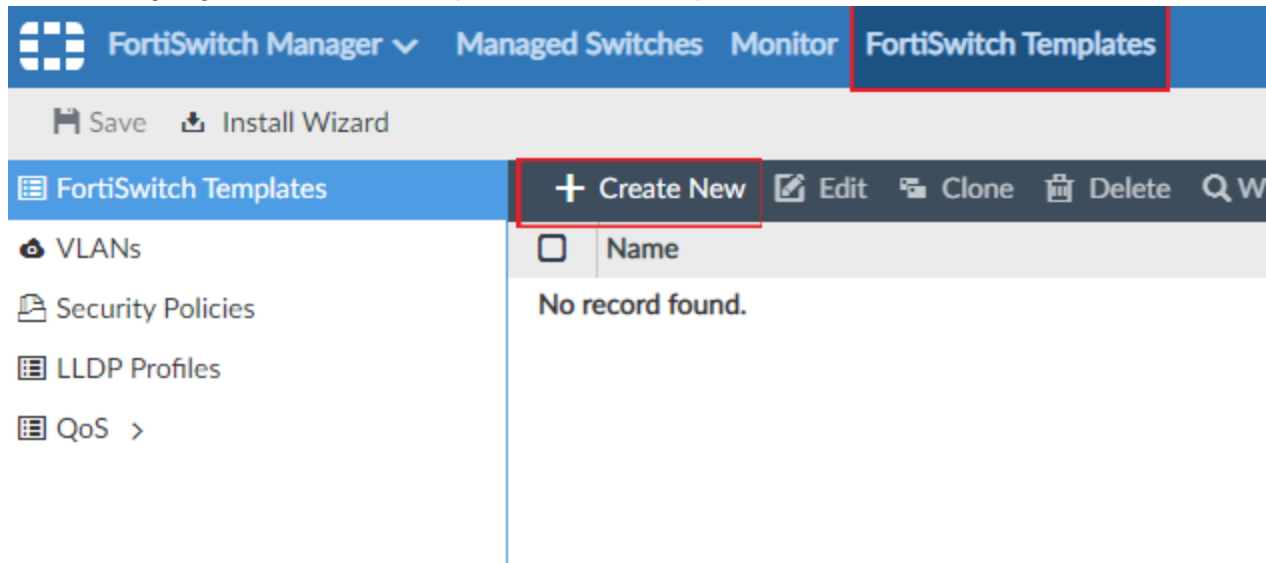
OK Cancel

Defining FortiSwitch templates

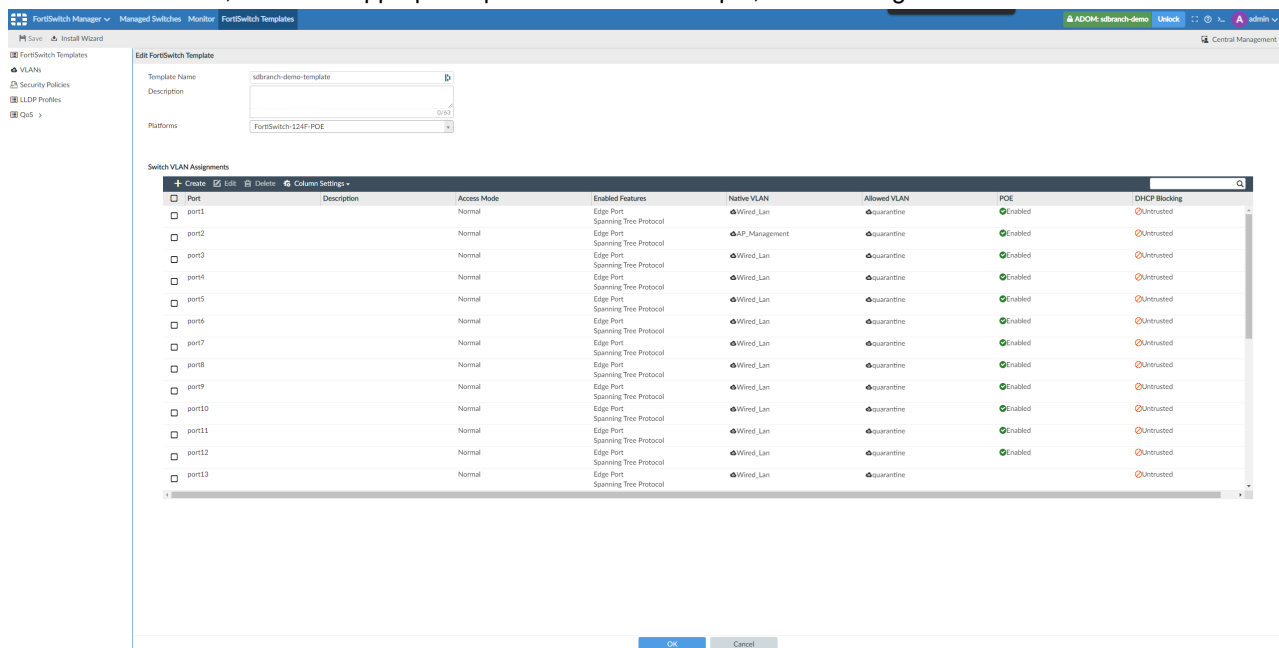
Now that our VLANs are created, we can create a FortiSwitch template, and select our VLANs.

To define FortiSwitch templates:

1. In FortiManager, go to *FortiSwitch Manager > FortiSwitch Templates*, and click *Create New*.



2. In the *Template Name* box, type a name for the template, such as *sdbranch-demo-template*.
3. In the *Platforms* list, select the appropriate platform. In our example, we are using a FortiSwitch-124F-POE.



4. In the *Switch VLAN Assignments* list, we can assign our VLANs to the FortiSwitch ports.
In the example, we assigned the VLAN named *Wired_Lan* as a native VLAN for all ports, except port22. Port22 will be used by FortiLink and is left to the default VLAN. Port2 will be used for the management of our FortiAP, so we assign it the VLAN named *AP_Management*.

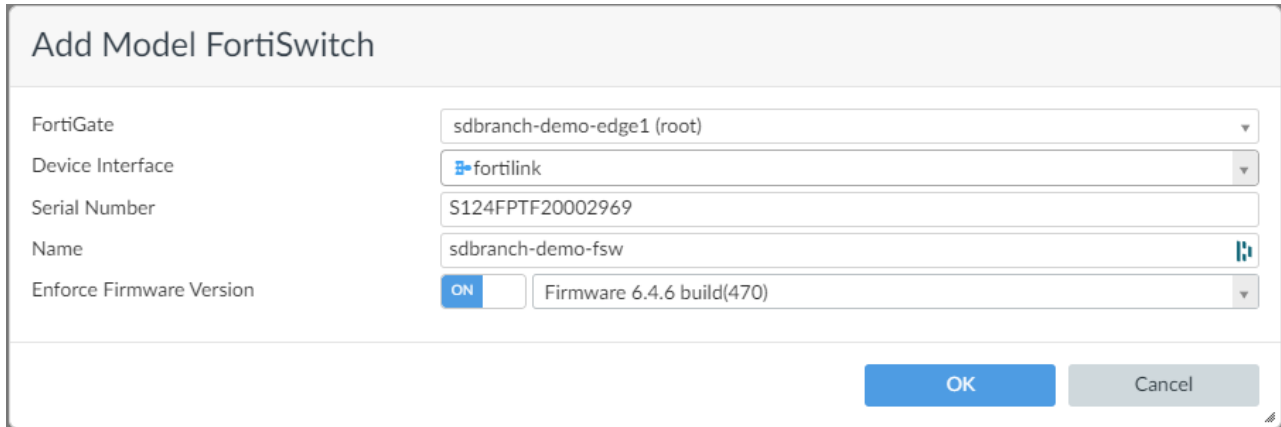
Here we may also add any necessary options depending on the use case (such as enable/disable PoE, Spanning-tree, create MC-LAG interfaces, and so on).

Creating a FortiSwitch model device

Finally, we need to create a FortiSwitch model device. The FortiSwitch model device will represent our end device, and we can assign to it the previously created FortiSwitch template.

To create a FortiSwitch model device:

1. In *FortiSwitch Manager*, go to *Managed Switches*.
2. In the content pane, select the FortiGate, and then click *Create New*. The *Add Model FortiSwitch* dialog box is displayed.

The image shows a dialog box titled "Add Model FortiSwitch". It contains several input fields: "FortiGate" with a dropdown menu showing "sdbranch-demo-edge1 (root)"; "Device Interface" with a dropdown menu showing "fortilink"; "Serial Number" with a text box containing "S124FPTF20002969"; "Name" with a text box containing "sdbranch-demo-fsw"; and "Enforce Firmware Version" with a toggle switch set to "ON" and a dropdown menu showing "Firmware 6.4.6 build(470)". At the bottom right, there are "OK" and "Cancel" buttons.

Add Model FortiSwitch	
FortiGate	sdbranch-demo-edge1 (root)
Device Interface	fortilink
Serial Number	S124FPTF20002969
Name	sdbranch-demo-fsw
Enforce Firmware Version	ON Firmware 6.4.6 build(470)
<div>OK Cancel</div>	

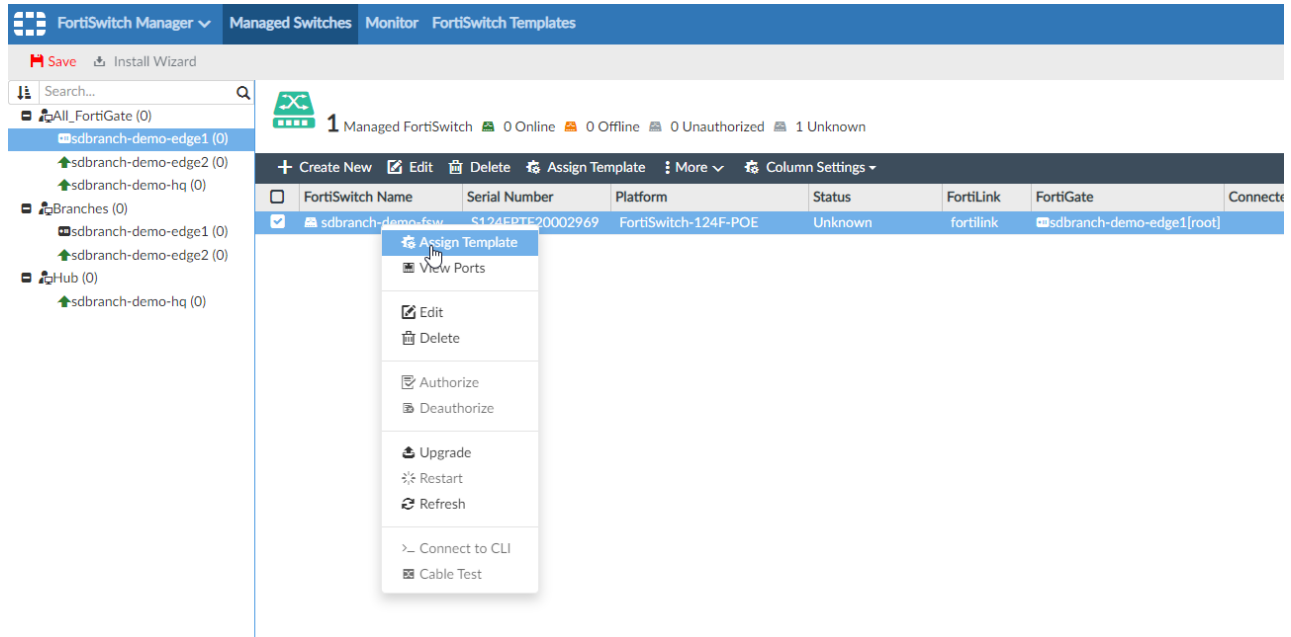
3. In *Serial Number* box, fill in the serial number for the FortiSwitch.
4. From the *Device Interface* list, select the *fortilink* interface.
We will connect FortiSwitch to the fortilink interface.
5. In the *Name* box, type a name.
6. Toggle *Enforce Firmware Version* to *ON* to ensure that the firmware version is the same on all branches.
7. Click *OK* to save the FortiSwitch model device.

Assigning FortiSwitch templates

After we create the FortiSwitch model device, we can select our FortiSwitch model device, and assign our FortiSwitch template to it.

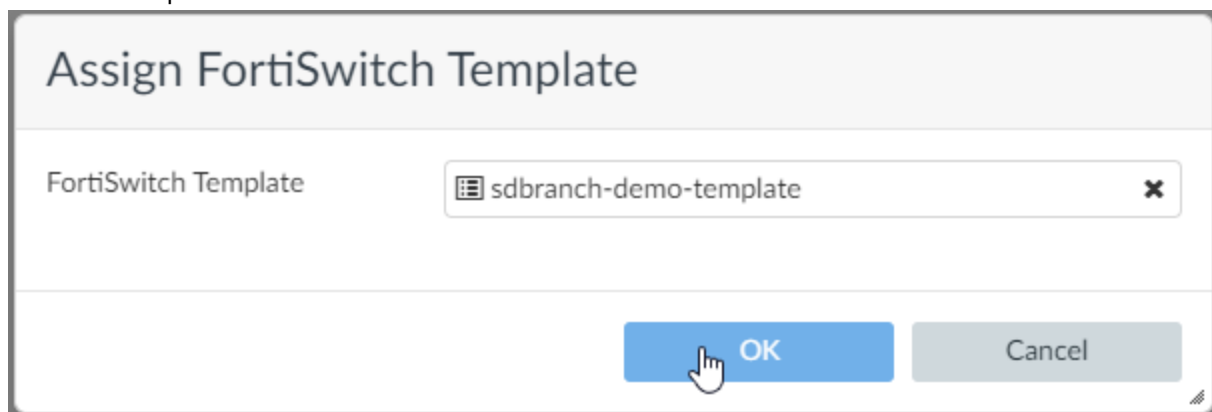
To assign a FortiSwitch templates to a model device:

1. In *FortiSwitch Manager* on the *Managed Switches* tab, right-click the model device, and select *Assign Template*.



The *Assign FortiSwitch Template* dialog box is displayed.

2. Select the template and click *OK*.



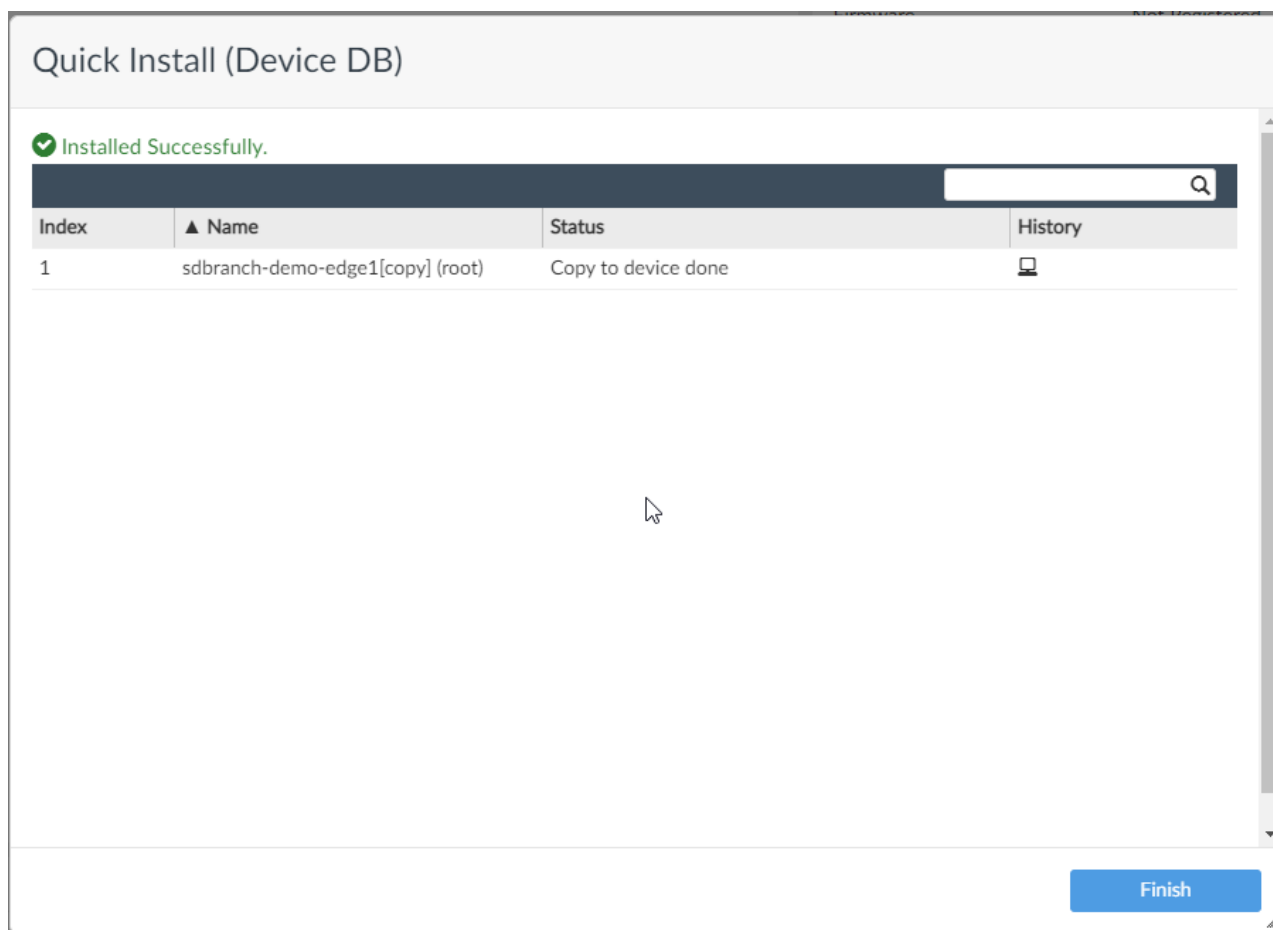
Installing FortiSwitch configuration to FortiGate

After you create the FortiSwitch template is assigned to the FortiSwitch model device, which is associated with FortiGate, you are ready to install the configuration to FortiGate.

It is important to complete this step before you connect FortiSwitch to FortiGate, and turn on FortiSwitch.

To install the FortiSwitch configuration to FortiGate:

1. Go to *Device Manager*.
2. Right-click the FortiGate, and select *Quick Install (Device DB)*.
The quick installation creates the VLANs.



3. Click *Finish*, and you can view the interfaces.

<input type="checkbox"/>	Wired_Lan	VLAN	Wired_Lan
<input type="checkbox"/>	AP_Management	VLAN	AP_Management

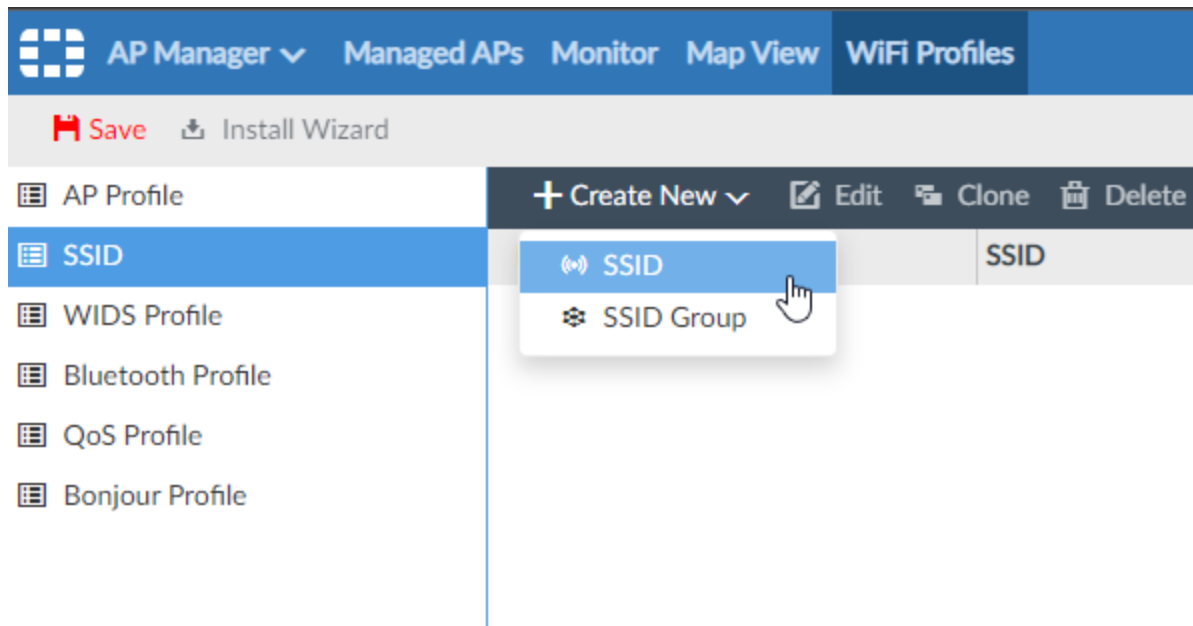
4. After the quick installation is complete, you can connect the FortiSwitch to the FortiGate, and turn on FortiSwitch. Once turned on, our FortiSwitch should now register with our FortiGate, and reboot to load its configuration.



Please note that the previous steps **must** be done prior to connecting the FortiSwitch to the FortiGate if the FortiGate has already been provisioned.

Configuring FortiAP

In this section, we will use the *AP Manager* module in FortiManager to create a template that can be used by our FortiAP. Similar to FortiSwitch, each model of FortiAP needs a specific template where you can assign your SSIDs and set your country. Moreover, other settings, such as the AP country, are to be considered for regulatory purposes. As such, we could end up with several templates for the same FortiAP models, but with different channels and RF bands.



Following is an overview of how to configure FortiAP:

1. Define SSIDs. See [Defining SSIDs on page 23](#).
2. Define AP profiles. See [Defining AP profiles on page 28](#).
3. Create a FortiAP model device that is associated with FortiGate, and select the AP profile. See [Creating a model device and assigning a profile on page 29](#).
4. Modify the FortiSwitch template to add *Wired_Lan* as an *Allowed VLAN*. See [Modifying the FortiSwitch template on page 30](#).
5. Install the AP configuration to FortiGate. See [Installing the AP configuration to FortiGate on page 30](#).

Defining SSIDs

The topic describes how to create the needed SSIDs. Following is a summary of the procedures:

1. Configure an SSID named *Wired_Bridge* that will bridge wireless clients into the VLAN named *Wired_Lan*. See [Defining the Wired_Bridge SSID on page 24](#).
2. Configure an SSID in tunnel mode named *Wireless_Lan* that will be segregated from the *Wired_Lan*. This section describes how to use the GUI and CLI templates.
 - For information about using the GUI, see [Defining the Wireless_Lan SSID with the GUI on page 25](#).
 - For information about using CLI templates, see [Defining the Wireless_Lan SSID with CLI templates on page 26](#).
3. Configure a guest WiFi that will be used for local breakout and will use a simple email collection captive portal. See [Defining the Guest SSID on page 27](#).



FortiAP sends bridge SSID data as VLAN traffic, according to the VLAN ID configured in the SSID menu. In that mode, FortiAP Manager will not configure a VLAN interface on the FortiGate. On the contrary, tunnel SSID data is encapsulated using a CAPWAP tunnel to the FortiGate. As such, FortiAP Manager will generate a VLAN interface with the name and VLAN ID specified in the SSID menu on the FortiGate.

Defining the Wired_Bridge SSID

To define the Wired_Bridge SSID:

1. Go to *AP Manager > WiFi Profiles > SSID*, and click *Create new*.
The *Create New SSID Profile* pane is displayed.
2. In the *Interface Name* box, type *Wired_Bridge*.

The screenshot shows the 'Create New SSID Profile' configuration page in FortiManager. The left sidebar lists 'AP Profile', 'SSID', 'WIDS Profile', 'Bluetooth Profile', 'QoS Profile', and 'Bonjour Profile'. The 'SSID' section is selected. The main area is titled 'Create New SSID Profile' and contains the following settings:

- Interface Name:** Wired_brigde
- Alias:** (empty)
- Traffic Mode:** Tunnel, Bridge (selected), Mesh
- WiFi Settings:**
 - SSID:** demo-wired-brigde
 - Security Mode:** WPA2 Personal
 - Local Standalone:** OFF
 - Local Authentication:** OFF
 - Client Limit:** OFF
 - Pre-shared Key Mode:** Single (selected), Multiple
 - Passphrase:** (empty)
 - Broadcast SSID:** ON
 - Schedule:** Click here to select
 - Block Intra-SSID Traffic:** OFF
 - Optional VLAN ID:** 10
 - Broadcast Suppression:** ON
 - Filter Clients by MAC Address:** OFF
 - RADIUS Server:** OFF
 - VLAN Pooling:** OFF, Managed AP Group, Round Robin, Hash
 - Encrypt:** TKIP, AES (selected), TKIP-AES
 - QoS Profile:** None
 - Advanced Options >**
 - Per-Device Mapping:** OFF

3. Beside *Traffic Mode*, select *Bridge*.
4. In the *SSID* list, select *demo-wired-bridge*.

As mentioned previously, we will use the bridge mode for the SSID named *demo-wired-bridge*. As the FortiAP will bridge the data from this SSID directly as VLAN traffic, we must use the same VLAN ID as the VLAN named *Wired_Lan*, if we want the wireless clients and the wired clients to communicate and to reach the *Wired_Lan* interface on the FortiGate as our default gateway.

5. In the *Security Mode* list, select *WPA2 Personal*.
For the sake of simplicity, we will use the *WPA2 Personal* authentication scheme.
6. In the *Optional VLAN ID* box, type the same VLAN ID as the *Wired_Lan*.
7. Click *OK* to save the SSID.

Defining the Wireless_Lan SSID with the GUI

We will create the *Wireless_Lan* SSID to use tunnel traffic mode. As with the VLAN named *Wired_Lan*, we can choose per-device mapping or create a CLI template to configure the IP address for the interface. See also [Defining VLANs on page 14](#).

To define the Wireless_Lan SSID:

1. Go to *AP Manager > WiFi Profiles > SSID*, and click *Create new*.
The *Create New SSID Profile* pane is displayed.

2. In the *Interface Name* box, type *Wireless_Lan*.

Save Install Wizard

AP Profile

SSID

WIDS Profile

Bluetooth Profile

QoS Profile

Bonjour Profile

Create New SSID Profile

Interface Name: Wireless_Lan

Alias:

Traffic Mode: Tunnel Bridge Mesh

Address

IP/Network Mask: 0.0.0.0/0.0.0.0

IPv6 Address:

Administrative Access

HTTPS PING SSH

SNMP HTTP TELNET

FMG-Access Auto-Ipsec RADIUS Accounting

IPv6 Administrative Access

HTTPS PING SSH

SNMP HTTP TELNET

Any FMG-Access

DHCP Server: OFF Server Relay

Networked Devices

Device Detection: ON

WiFi Settings

SSID: demo-wireless-lan

Security Mode: WPA2 Personal

Client Limit: OFF

Pre-shared Key Mode: Single Multiple

Passphrase: *****

Broadcast SSID: ON

Schedule: Click here to select

Block Intra-SSID Traffic: OFF

Broadcast Suppression: ON

Filter Clients by MAC Address

RADIUS Server: OFF

VLAN Pooling: OFF Managed AP Group Round Robin Hash

Quarantine Host: OFF

Encrypt: TKIP AES TKIP-AES

QoS Profile: None

Advanced Options >

3. Beside *Traffic Mode*, select *Tunnel*.

4. Toggle *Per-Device Mapping* to ON, and click *Create New* to create a mapped device.

Per-Device Mapping: ON

+ Create New Edit Delete

Mapped Device	Details
sdbranch-demo-edge1(root)	IP/Netmask: 172.17.5.1/255.255.255.0

Defining the Wireless_Lan SSID with CLI templates

With CLI templates, we use the following new variables:

- wireless_lan_net
- wireless_lan_netmask

Before you can use the new variables in a CLI template, you must create the variables. Go to *System Settings > Meta Fields > Create New > (Device type)*.

Below is an example of a CLI template that uses variables to define the SSID named *Wireless_Lan*:

```
config system interface
  edit "Wireless_Lan"
    set vdom "root"
    set ip $(wireless_lan_net:4,1) $(wireless_lan_netmask)
    set allowaccess ping
    set type vap-switch
    set alias "demo-wireless-lan"
    set role lan
  next
end
config system dhcp server
  edit 2
    set dns-service default
    set ntp-service default
    set default-gateway $(wireless_lan_net:4,1)
    set netmask $(wireless_lan_netmask)
    set interface "Wireless_Lan"
    config ip-range
      edit 1
        set start-ip $(wireless_lan_net:4,10)
        set end-ip $(wireless_lan_net:4,250)
      next
    end
  next
end
```

Defining the Guest SSID

Finally, we configure our SSID named *Guest*. For the *Guest* SSID, we use tunnel traffic mode and the same subnet for all our branches, as well as a captive portal.

To define the guest SSID:

1. Go to *AP Manager > WiFi Profiles > SSID*, and click *Create new*.
The *Create New SSID Profile* pane is displayed.
2. In the *Interface Name* box, type *Guest*.
3. Beside *Traffic Mode*, select *Tunnel*.

4. Set the remaining options, and click **OK** to create the SSID named *Guest*.

The screenshot displays the 'Create New SSID Profile' configuration window in FortiManager. The left sidebar shows the navigation tree with 'SSID' selected. The main configuration area is divided into several sections:

- Interface Name:** Guest
- Alias:** (empty)
- Traffic Mode:** Tunnel (selected), Bridge, Mesh
- Address:**
 - IP/Network Mask: 192.168.10.1/255.255.255.0
 - IPv6 Address: (empty)
- Administrative Access:**
 - HTTPS, SNMP, FMG-Access (unchecked)
 - PING (checked)
 - SSH, TELNET, RADIUS Accounting (unchecked)
- IPv6 Administrative Access:**
 - HTTPS, SNMP, Any (unchecked)
 - PING, HTTP, FMG-Access (unchecked)
 - SSH, TELNET (unchecked)
- DHCP Server:** OFF, Server (selected), Relay
- IP Range:**
 - Start IP: 192.168.10.2
 - End IP: 192.168.10.254
- Network Mask:** Same as Interface (selected), Specify
- Default Gateway:** Same as Interface (selected), Specify
- Next Server:** 0.0.0.0
- DNS Service:** Specify, Use System DNS Setting (Default) (selected), Same as Interface IP (Local)
- NTP Service:** Specify, Use System NTP Setting (Default) (selected), Use FortiGate as NTP Server (Local)
- FortiClient On-Net Status:** ON (selected)
- Timezone Option:** Specify, Disable (selected), Default
- IP Address Assignment Rules:**

Type	Match Criteria	Action
Implicit	Unknown MAC address	Assign IP
- Advanced... (DNS, WINS, Custom Options, Exclude Ranges) >**
 - Networked Devices:** Device Detection: OFF
 - WiFi Settings:**
 - SSID: demo-guest
 - Security Mode: Captive Portal
 - Client Limit: OFF

At the bottom right, there are **OK** and **Cancel** buttons.

Defining AP profiles

Now that the SSIDs are defined, we can create a FortiAP profile.

When we configure a new profile, we need to select the country and the FortiAP model. The number and type of radios depend on the model. As a result, SSID assignment may vary. As mentioned earlier, selecting the proper RF bands and channels can greatly improve bandwidth and coverage. See also [Configuring FortiAP on page 22](#).

To define AP profiles:

1. Go to **AP Manager > WiFi Profiles > AP Profile**, and click **Create New**. The **Create New AP Profile** pane is displayed.
2. In the **Name** box, type a name for the profile.
3. In the **Platform** list, select the FortiAP model.
4. In the **Country/Region** list, select the country.

5. Set the remaining options, and click **OK**.

The screenshot displays the 'Create New AP Profile' configuration window in FortiManager. The left sidebar shows the 'AP Profile' section with options for SSID, WIDS Profile, Bluetooth Profile, QoS Profile, and Bonjour Profile. The main configuration area is divided into two sections: Radio 1 and Radio 2.

Radio 1 Configuration:

- Platform: FAP231F
- Country/Region: France
- AP Login Password: Set (Leave Unchanged / Set Empty)
- Administrative Access: ☐ HTTPS ☐ SNMP ☐ SSH
- Client Load Balancing: ☒ Frequency Handoff ☐ AP Handoff
- Bluetooth Profile: None
- Mode: Disabled (Access Point / Dedicated Monitor)
- WIDS Profile: OFF
- Radio Resource Provision: OFF
- Band: 2.4 GHz (802.11ax/n/g/b)
- Channel Width: 20MHz (40MHz / 80MHz)
- Short Guard Interval: OFF
- Channels: ☒ 1 ☒ 6 ☒ 11
- TX Power Control: Auto (Manual)
- TX Power: 100 %
- SSIDs: Tunnel Bridge Manual (Search results: demo-wireless-lan (Wireless_Lan), 1 Entry Selected)
- Monitor Channel Utilization: ON

Radio 2 Configuration:

- Mode: Disabled (Access Point / Dedicated Monitor)
- WIDS Profile: OFF
- Radio Resource Provision: OFF
- Band: 5 GHz (802.11ax/ac/n)
- Channel Width: 20MHz (40MHz / 80MHz / 160MHz)
- Short Guard Interval: OFF
- Channels: ☒ 36 ☐ 40 ☒ 44 ☐ 48 ☒ 52* ☐ 56* ☒ 60* ☐ 64* ☒ 100* ☐ 104* ☒ 108* ☐ 112* ☒ 116* ☐ 120* ☒ 124* ☐ 128* ☒ 132* ☐ 136*
- TX Power Control: Auto (Manual)
- TX Power: 100 %
- SSIDs: Tunnel Bridge Manual (Search results: demo-wired-bridge (Wired_bridge), 1 Entry Selected)
- Monitor Channel Utilization: ON

At the bottom right, there are 'OK' and 'Cancel' buttons.

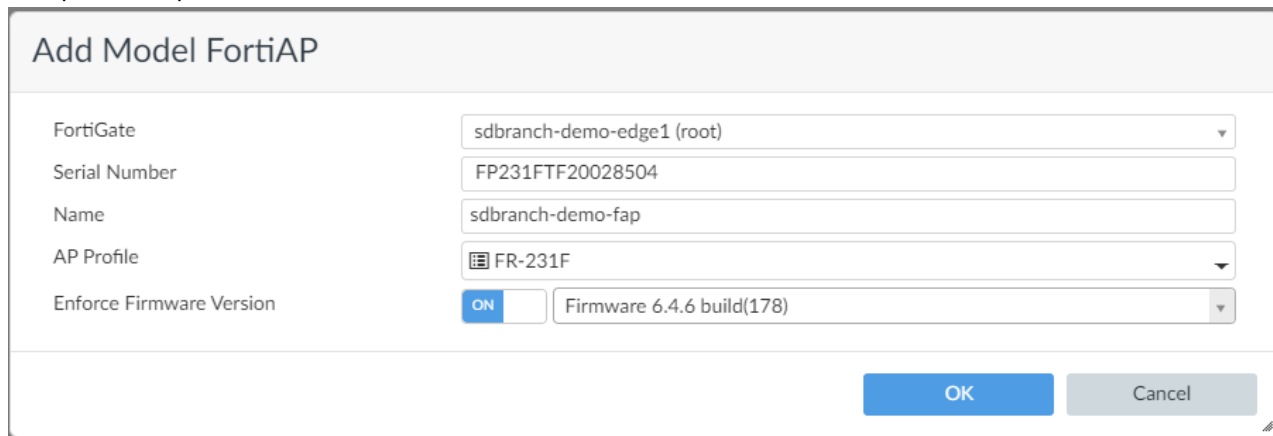
Creating a model device and assigning a profile

In this section, we create a FortiAP model device, select our AP profile, and associate them with our FortiGate.

To create a FortiAP model device:

1. In *AP Manager*, go to *Managed APs*.
2. In the content pane, select the FortiGate, and then click *Create New*. The *Add Model FortiAP* dialog box is displayed.

- Complete the options, and click **OK** to create the model device.



Add Model FortiAP

FortiGate	sdbranch-demo-edge1 (root)
Serial Number	FP231FTF20028504
Name	sdbranch-demo-fap
AP Profile	FR-231F
Enforce Firmware Version	ON Firmware 6.4.6 build(178)

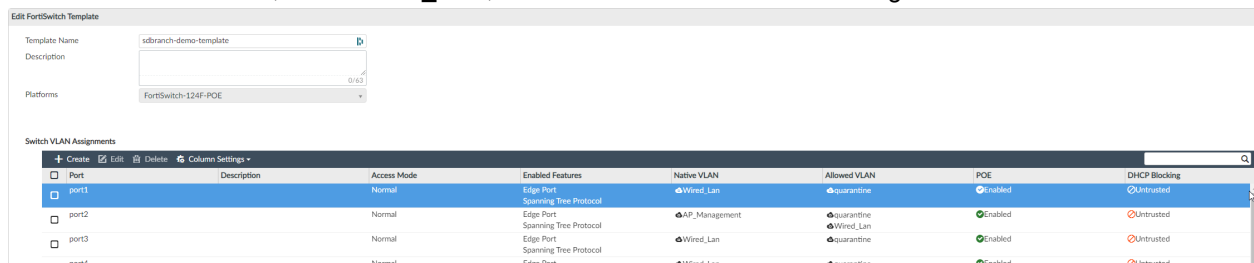
OK **Cancel**

Modifying the FortiSwitch template

As mentioned previously in this section, the bridge SSID named *Wired_Bridge* will be on the same VLAN as the *Wired_Lan*. We need to adapt the FortiSwitch configuration to add *Wired_Lan* as an *Allowed VLAN* so that the FortiAP can trunk the traffic into the FortiSwitch and reach the FortiGate interface named *Wired_Lan*.

To modify the FortiSwitch template:

- Go to *FortiSwitch Manager > FortiSwitch Templates*.
- Double-click the FortiSwitch template to open it for editing.
- Double-click the port to open it for editing. The *Edit VLAN Assignment* dialog box is displayed.
- In the *Allowed VLAN* list, select *Wired_LAN*, and click **OK** to save the VLAN assignment.



Edit FortiSwitch Template

Template Name: sdbranch-demo-template

Description:

Platforms: FortiSwitch-124F-POE

Switch VLAN Assignments

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	DHCP Blocking
port1		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled	Untrusted
port2		Normal	Edge Port Spanning Tree Protocol	AP_Management	quarantine Wired_Lan	Enabled	Untrusted
port3		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled	Untrusted
port4		Normal	Edge Port	Wired_Lan	quarantine	Enabled	Untrusted

- Click **OK** to save the template.

Installing the AP configuration to FortiGate

After modifying the FortiSwitch template to add *Wired_Lan* as an *Allowed VLAN*, we can install the AP configuration to FortiGate.

To install the FortiAP configuration to FortiGate:

- Go to *Device Manager*.
- Right-click the FortiGate, and select *Quick Install (Device DB)*.

Configuring FortiExtender

As mentioned in [Uses cases and topologies on page 6](#), we will manage the FortiExtender with the FortiGate.



In this mode, the FortiGate creates a virtual interface of type *fext-wan* that represents the LTE link and can be added as an SD-WAN interface.

Following is an overview of how to configure FortiExtender:

1. Define the FortiExtender configuration by using a CLI template. See [Configuring FortiExtender with CLI templates on page 31](#).
2. Create a normalized interface for FortiExtender. See [Creating a normalized interface for FortiExtender on page 32](#).
3. Add the FortiExtender interface to an existing SD-WAN template. See [Adding FortiExtender to an SD-WAN template on page 33](#).
4. Install the FortiExtender configuration to FortiGate. See [Installing FortiExtender configuration to FortiGate on page 33](#).

Configuring FortiExtender with CLI templates

As of FortiManager 6.4, FortiExtender units are only *managed per-device* by FortiManager. As such, the best way to configure a FortiExtender in a large SD-WAN deployment is to use CLI templates. In our design, the FortiExtender is connected to *wan2* of the FortiGate. As mentioned in [FortiExtender deployment method on page 11](#), we need to configure the *wan2* interface as a DHCP client in order to retrieve an IP address from our FortiExtender, and we also need to enable the *Secure Fabric Connection* option to make sure we discover it.

We can achieve that by using the following CLI template:

```
config system interface
  edit "wan2"
    set vdom "root"
    set mode dhcp
    set allowaccess ping fabric
    set type physical
  next
end
```

We then need to configure the FortiExtender virtual interface that will be used as part of the SD-WAN to access the mobile network :

```
config system interface
  edit "FEX"
    set vdom "root"
    set mode dhcp
    set type fext-wan
    set role wan
  next
end
```

The last CLI template will map the FortiExtender to the created interface.

```
config extender-controller extender
  edit "FortiExtender1"
```

```

set id "FX201E5920012510"
set authorized enable
config modem1
    set ifname "FEX"
end
end
next
end

```

Creating a normalized interface for FortiExtender

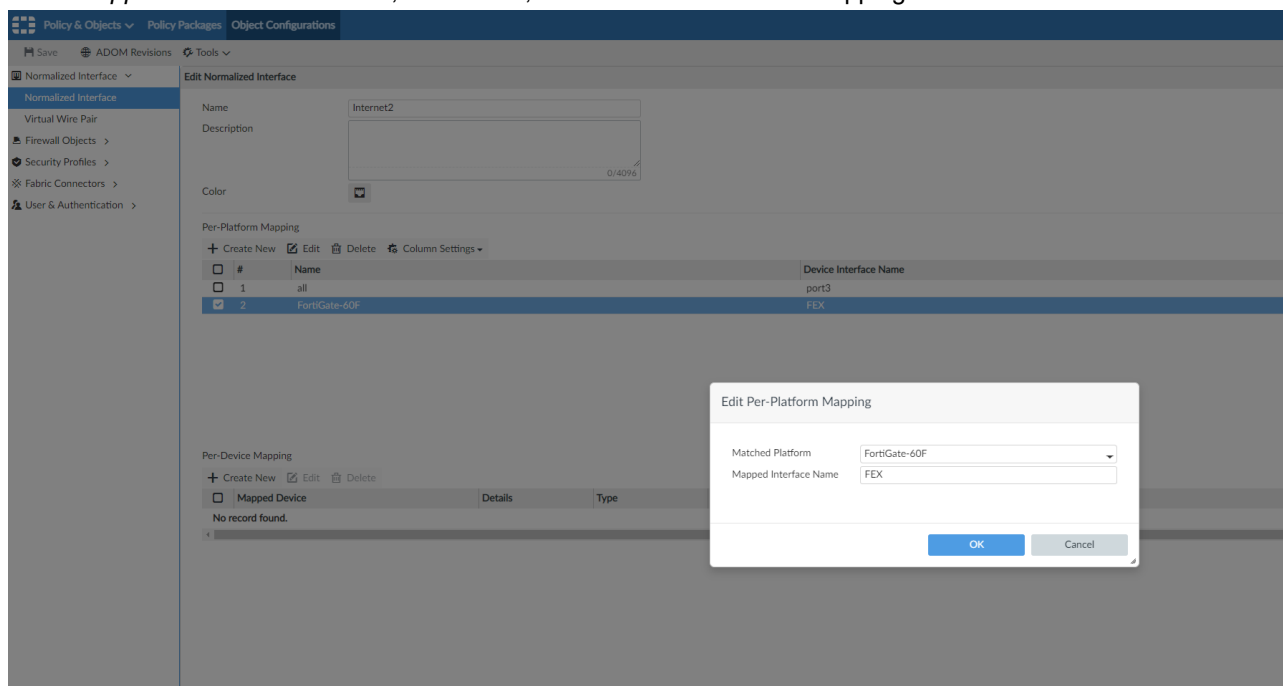
Before we can add FortiExtender to an existing SD-WAN template, we must create a normalized interface. As it will be our second internet link, we named it *Internet2* in the example below.



We are using the name (*FEX*) of the virtual interface (type *fext-wan*) that we previously created in the CLI template.

To create a normalized interface for FortiExtender:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface*, and click *Create New*. The *Create New Normalized Interface* pane is displayed.
2. In the *Name* box, type *Internet2*.
3. Under *Per-Platform Mapping*, click *Create New*. The *Create New Per-Platform Mapping* dialog box is displayed.
4. In the *Matched Platform* list, select *FortiGate-60F*.
5. In the *Mapped Interface Name* box, select *FEX*, and click *OK* to save the mapping.



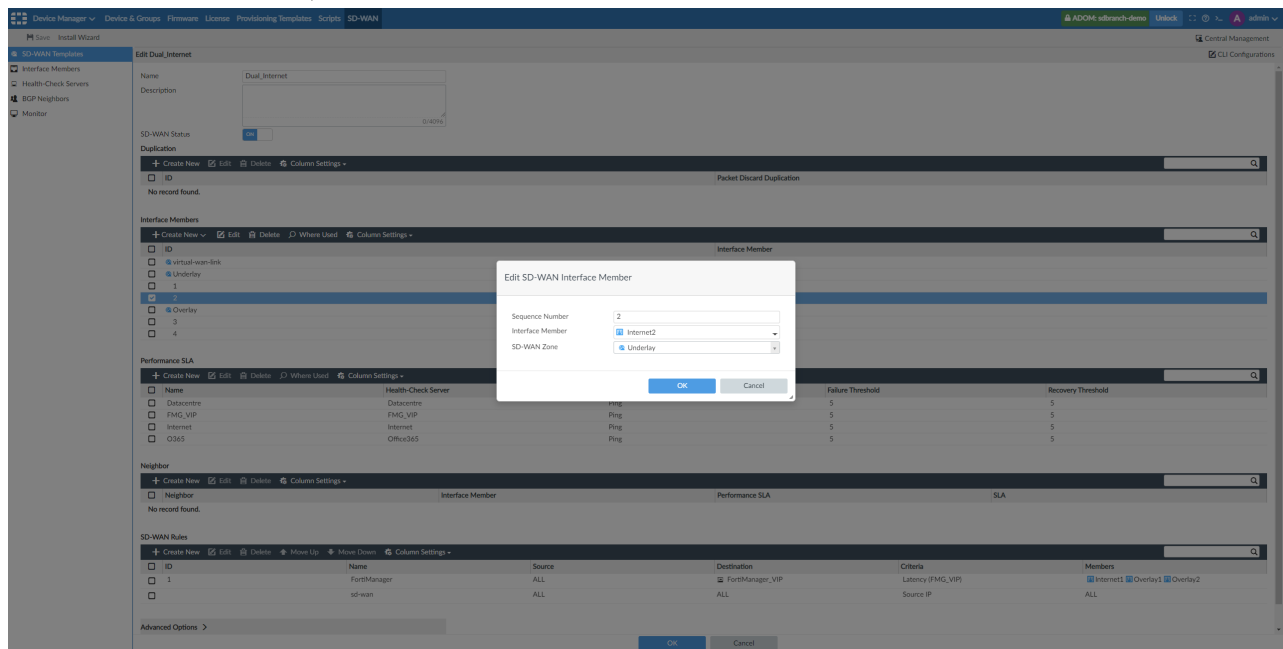
6. Click *OK* to save the normalized interface.

Adding FortiExtender to an SD-WAN template

After creating the normalized interface, we can finally add the FortiExtender interface as a member to an existing SD-WAN template.

To add FortiExtender to an SD-WAN template:

1. Go to *Device Manager > SD-WAN > SD-WAN Templates*.
2. In the content pane, double-click a template to open it for editing.
3. Under *Interface Member*, click *Create New > SD-WAN Member*.
4. In the *Interface Member* list, select *Internet2*.



5. In the *SD-WAN Zone* list, select *Underlay*.
6. Click *OK* to save the changes.

Installing FortiExtender configuration to FortiGate

Lastly we need to apply the FortiExtender changes by installing the configuration on our FortiGate.

To install the FortiExtender configuration to FortiGate:

1. Go to *Device Manager*.
2. Right-click the FortiGate, and select *Quick Install (Device DB)*.

Configuring security policies

Our FortiGate 60F model device is ready along with the SD-Branch extensions. However we still need to create security policies to access network resources. In this section we will:

1. Edit normalized interfaces for FortiAPs that can be used in the branch policy package. See [Editing normalized interfaces for FortiAPs on page 34](#).
2. Create a policy package that includes the FortiSwitch and FortiAP interfaces. See [Updating policy packages on page 35](#).

Editing normalized interfaces for FortiAPs

After configuring the different templates, FortiManager displays the interfaces created on *Policy & Objects > Objects configuration > Normalized Interface* pane:

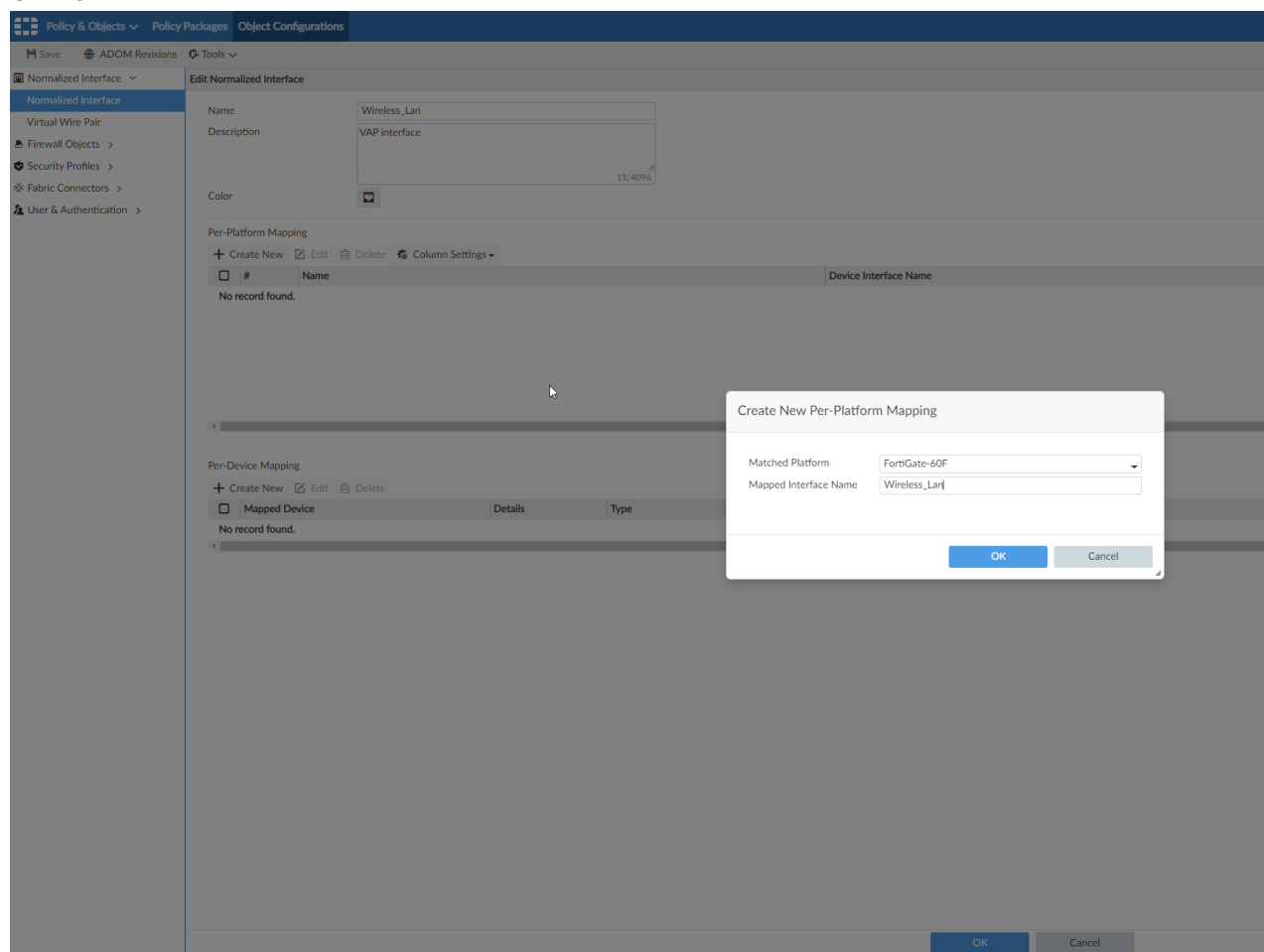
<input type="checkbox"/> <input checked="" type="checkbox"/> Wired_Lan			FortiSwitch VLAN interface
<input type="checkbox"/>	Default	Wired_Lan	
<input type="checkbox"/> <input checked="" type="checkbox"/> Wired_brigde			VAP interface
<input type="checkbox"/> <input checked="" type="checkbox"/> Wireless_Lan			VAP interface

The FortiAP interfaces are created for reference, but have no associated interface name by default. We need to edit the interfaces and apply a *per-platform* or *per-device* mapping. In the following example, we edit the interface named *Wireless_Lan* to add a *per-platform* mapping for the FortiGate 60F model. We need to repeat this operation for all the SSIDs in tunnel mode.

To edit normalized interfaces:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface*.
2. Double-click the interface named *Wireless_Lan* to open it for editing.
3. Under *Per-Platform Mapping*, click *Create New*. The Create New Per-Platform Mapping dialog box is displayed.
4. In the *Matched Platform* list, select *FortiGate-60F*.
5. In the *Mapped Interface Name* box, type *Wireless_Lan*, and click *OK* to save the mapping.

6. Click **OK** to save the normalized interface.



Updating policy packages

After editing normalized interfaces for devices, we can use the interfaces in our firewall policies. For example, we can use the interfaces to allow the Guest network to access to the underlay exclusively with specific security profiles. On the other hand, the wireless and wired networks get access to the overlay/underlay with different security profiles.

This topic contains the following sections:

- [Creating interface subnet objects on page 35](#)
- [Creating policy packages for multiple branches on page 36](#)
- [Installing policy package changes to FortiGate on page 36](#)

Creating interface subnet objects

To map the source networks, we can create new firewall address objects of type *Interface subnet* that will be dynamically mapped to the source interface subnet when FortiManager pushes the policy to the FortiGate.

To create interface subnet objects:

1. Go to *Policy & Objects > Object Configurations > Firewall Objects > Addresses*, and click *Create New*. The *Create New Address* pane is displayed.
2. In the *Address Name* box, type a name for the address, such as *Wireless_Lan_Network*.
3. In the *Type* list, select *Interface Subnet*.
4. Complete the remaining options, and click *OK* to save the object.

The screenshot shows the 'Edit Address' configuration window in FortiManager. The left sidebar contains a tree view with 'Addresses' selected. The main configuration area includes the following fields:

- Address Name:** Wireless_Lan_Network
- Color:** (Color selection icon)
- Type:** Interface Subnet
- IP/Netmask:** 0.0.0.0/255.255.255.255 (with a DNS Lookup button)
- Interface:** Wireless_Lan
- Static Route Configuration:** OFF
- Comments:** (Text area)
- Add To Groups:** Click here to select
- Advanced Options:**
 - Per-Device Mapping:** OFF

Creating policy packages for multiple branches

Below is an example of a simple policy package that can be deployed to multiple branches on the *Policy & Objects > Policy Packages* pane:

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log	NAT	Comments	Install On
1	Guest allow underlay	Guest	Underlay	Guest_net	all	always	ALL		Accept	Guest_AV, Guest_WF, Guest_AC, certificate-inspection, default	Log All Sessions	Enabled		Installation Targets
2	Guest deny all	Guest	any	all	all	always	ALL		Deny		Log Violation Traffic			Installation Targets
3	Internet	Wireless_Lan	Underlay	Wireless_Lan_Network	all	always	ALL		Accept	Branches_AV, Branches_WF, Branches_AC, deep-inspection, default	Log All Sessions	Enabled		Installation Targets
4	DC / Other Branches	Wireless_Lan	Overlay	Wireless_Lan_Network	all	always	ALL		Accept	Branches_AV, Branches_WF, Branches_AC, deep-inspection, default	Log All Sessions	Disabled		Installation Targets
5		Overlay	Wireless_Lan	Wireless_Lan_Network	all	always	ALL		Accept	no-inspection	Log All Sessions	Disabled		Installation Targets
▼ Implicit (5-6 / Total: 1)														
6	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log			Installation Targets

Installing policy package changes to FortiGate

As we selected this policy package while creating the FortiGate model device, we can install the changes using the *Install > Install Wizard > Policy Package*:

Install Wizard - Policy Package (Branches)

✔ Policy package (Branches) is installed successfully.

100%

Total: 2/2, ✔ Success: 2, ⚠ Warning: 0, ✖ Error: 0

[View Installation Log](#) [View Progress Report](#)

#	Name	Time Used	Status
1	sdbranch-demo-edge1	4s	Copy to model device (sdbranch-demo-edge1) done
2	sdbranch-demo-edge2	19s	install and save finished status=OK

The following example shows that the *Branches* policy package was successfully installed to the device.

Edit Delete Import Policy Install More Column Settings						
<input type="checkbox"/>	▲ Device Name	Config Status	Policy Package Status	CLI Template Status	Firmware Version	Host Name
<input type="checkbox"/>	sdbranch-demo-edge1	Unknown	✔ Branches	✔ Edge-Template-Group	Upgrade 6.4 --> 6.4.6-b1879	sdbranch-demo-edge1

Deployment verification

In this section we will verify that the different settings that we configured in the previous sections are correctly applied. This section contains the following topics:

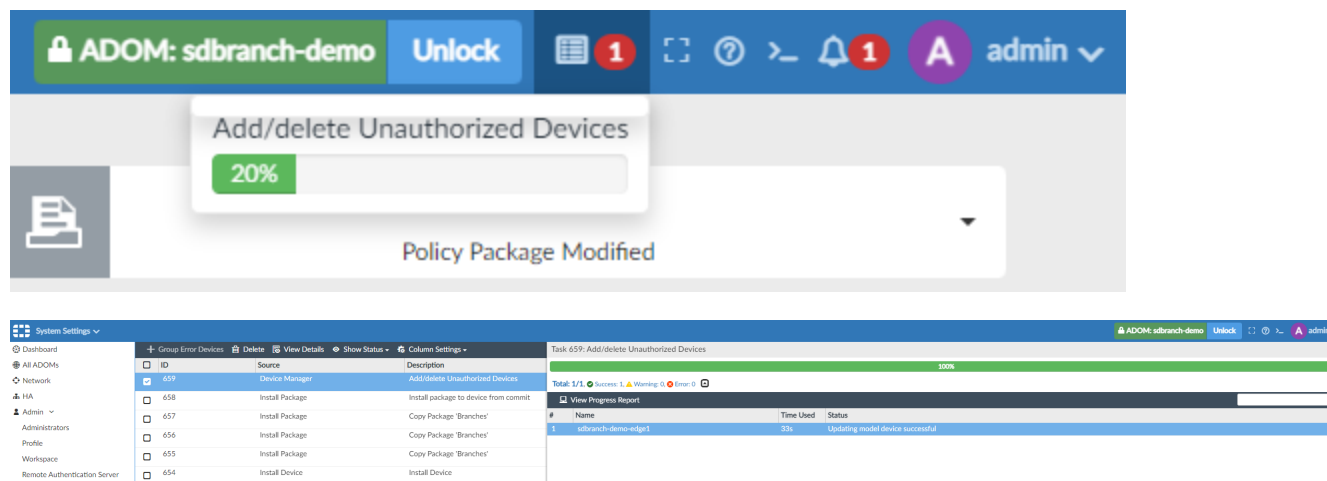
- [Verifying FortiGate connectivity with FortiManager on page 38](#)
- [Verifying FortiSwitch devices on page 38](#)
- [Verifying FortiAP devices on page 40](#)
- [Verifying FortiExtender devices on page 40](#)

Verifying FortiGate connectivity with FortiManager

The first step for verification is to connect our FortiGate to FortiManager. In FortiManager, add FortiGate as a managed device by going to *Device Manager > Device & Groups > Add Device*.

Once our FortiGate reaches FortiManager, FortiManager pushes its configuration that includes all the templates.

We can click on the event at the upper right corner to get more details, or we can go to *System Settings > Task Monitor* to view details of the installation:



At this point, all of the devices should have their complete configuration and be operational.

Verifying FortiSwitch devices

We can verify that our devices have been discovered and authorized by the FortiGate by going to *FortiSwitch Manager > Managed Switches*:

FortiSwitch Manager ▾ Managed Switches Monitor FortiSwitch Templates

Save Install Wizard

Search...

All_FortiGate (1)

sdbranch-demo-edge1 (1)

sdbranch-demo-edge2 (0)

sdbranch-demo-hq (0)

Branches (1)

Hub (0)

Edit Managed FortiSwitch

Serial Number: S124FPTF20002969

Name: sdbranch-demo-fsw

Description: 0/63

Template: sdbranch-demo-template

Managed Switch Status

Status: Online [View Ports](#) [Restart](#)

Connecting From: 169.254.1.2

Join Time: Wed Dec 8 14:20:19 2021

Authorize State: Authorized [Deauthorize](#)

Firmware

FortiSwitch OS Version: S124FP-v6.4.6-build470,210211 (GA) [\[Upgrade\]](#)

Enforce Firmware Version: OFF

The previous image shows that the FortiSwitch 124F-POE model is connected and authorized. We can then view the ports on FortiSwitch by clicking the *View Ports* button.

FortiSwitch Manager ▾ Managed Switches Monitor FortiSwitch Templates

ADOM: sdbranch-demo [Unlock](#) admin ▾

Save Install Wizard

Search...

All_FortiGate (1)

sdbranch-demo-edge1 (1)

sdbranch-demo-edge2 (0)

sdbranch-demo-hq (0)

Branches (1)

Hub (0)

FortiSwitch Ports

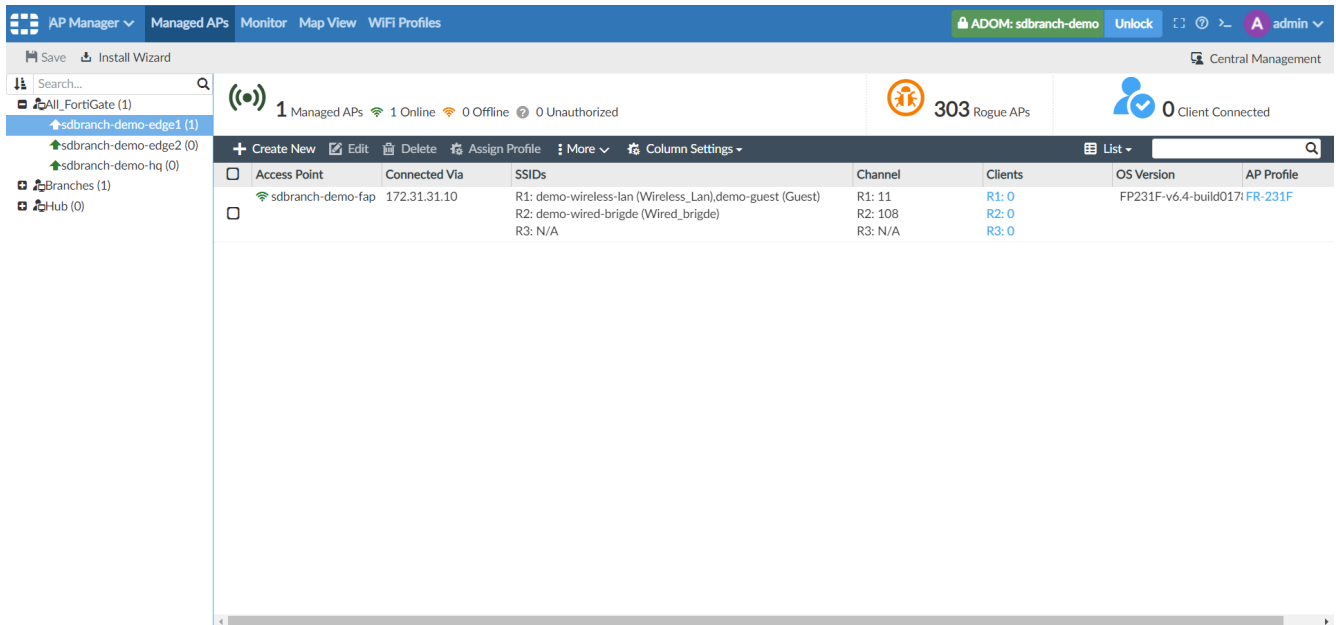
Refresh Column Settings

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	Device Information	DHCP Blocki
port1		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port2		Normal	Edge Port Spanning Tree Protocol	AP_Management	quarantine Wired_Lan	Enabled	sdbranch-demo-fap	Untrust
port3		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port4		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port5		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port6		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port7		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port8		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port9		Normal	Edge Port Spanning Tree Protocol	Wired_Lan	quarantine	Enabled		Untrust
port10		Normal	Edge Port	Wired_Lan	quarantine	Enabled		Untrust

Looking at the ports, we can see that the VLANs are assigned as specified in the template, and we can also get a hint of our connected FortiAP on port2 in the device list.

Verifying FortiAP devices

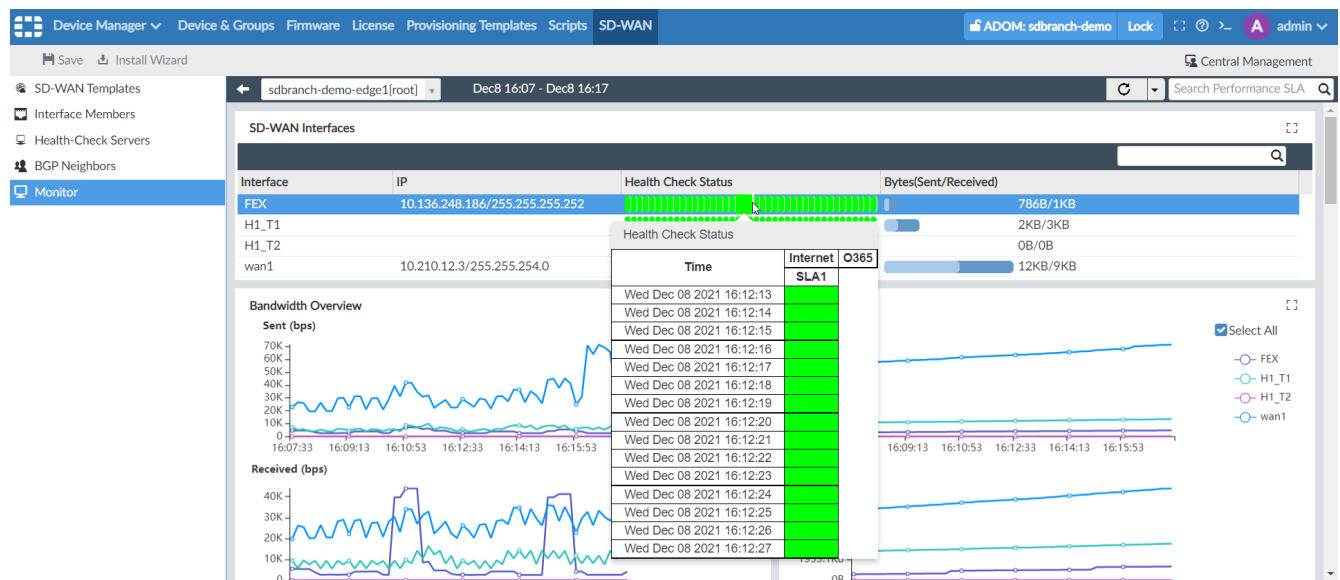
We can also ensure that our FortiAP is properly authorized and connected by going to *AP Manager > Managed APs*.



The previous image shows that the FortiAP 231F model received an IP address on the *AP_Management* VLAN (172.31.31.10), and the device connected and authorized. The two radios are broadcasting the three SSIDs that were configured in the template, and the profile named *FR-231F* is attached to the FortiAP.

Verifying FortiExtender devices

You can verify that the FortiExtender SD-WAN interface has internet access by going to *Device Manager > SD-WAN > Monitor*.





FORTINET®



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.