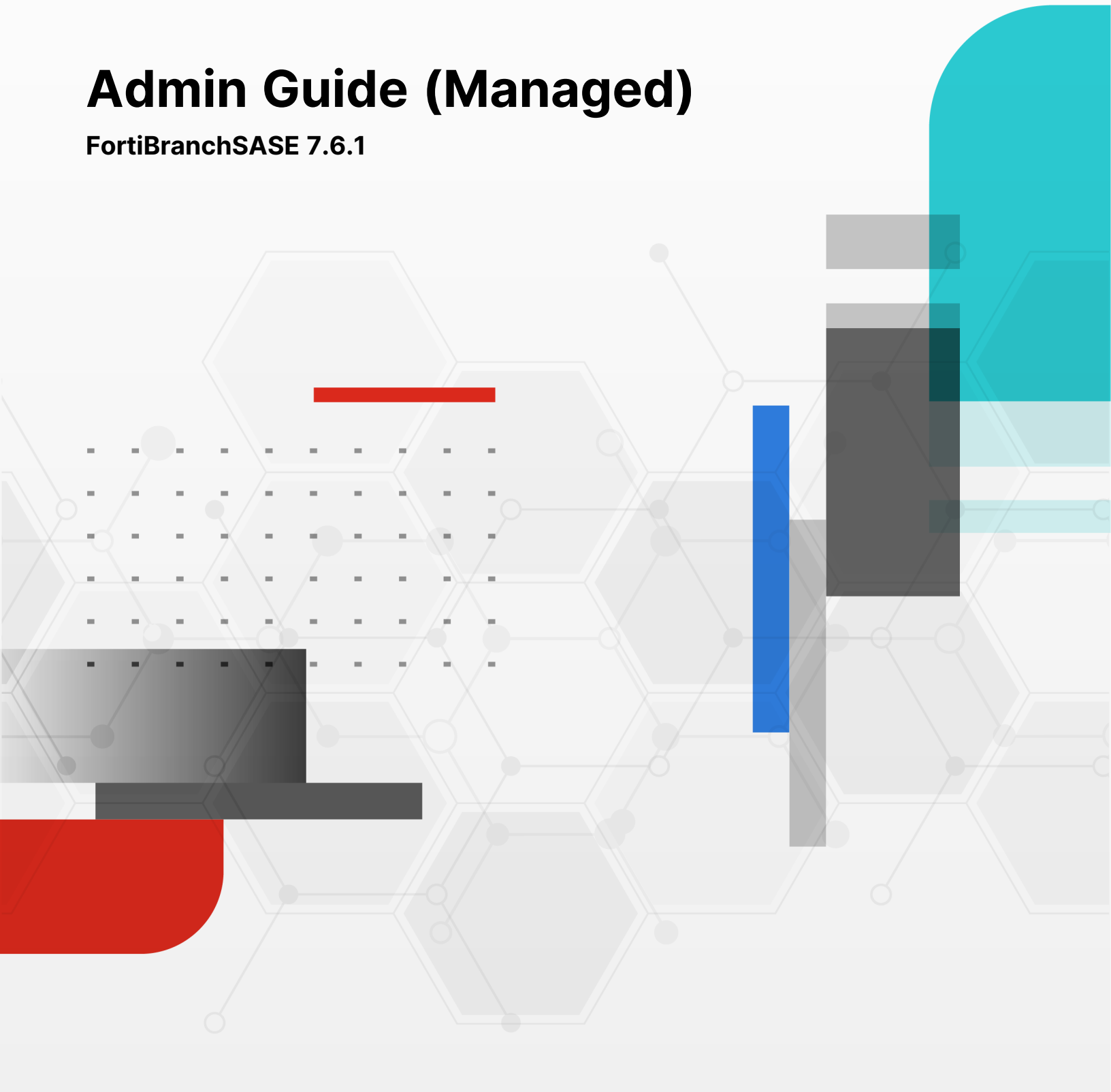
Admin Guide (Managed)

FortiBranchSASE 7.6.1



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

Aug 7, 2025
FortiBranchSASE 7.6.1 Admin Guide (Managed)

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-05-12	Initial release.
2025-08-07	Updated Introduction on page 5.

Introduction

Many enterprises find themselves with locations where a small network exists and needs to be secured, but where it is unnecessary or cost prohibitive to deploy a firewall appliance. In those situations, security can be extended to the site in question from a centralized location, leaving only a "thin edge" of networking equipment at the site, while security actions are performed elsewhere.

The FortiExtender SASE solution, branded as *FortiBranchSASE* (FBS), offers secure and reliable connectivity by integrating with Fortinet's FortiOS through FortiSASE or remote FortiGate devices.

FortiBranchSASE ensures comprehensive connection at the thin edge. As part of the FortiExtender product family, FortiBranchSASE extends the reach of the Fortinet Security Fabric, bringing advanced networking and security capabilities to even the most remote or small office environments.

About this guide

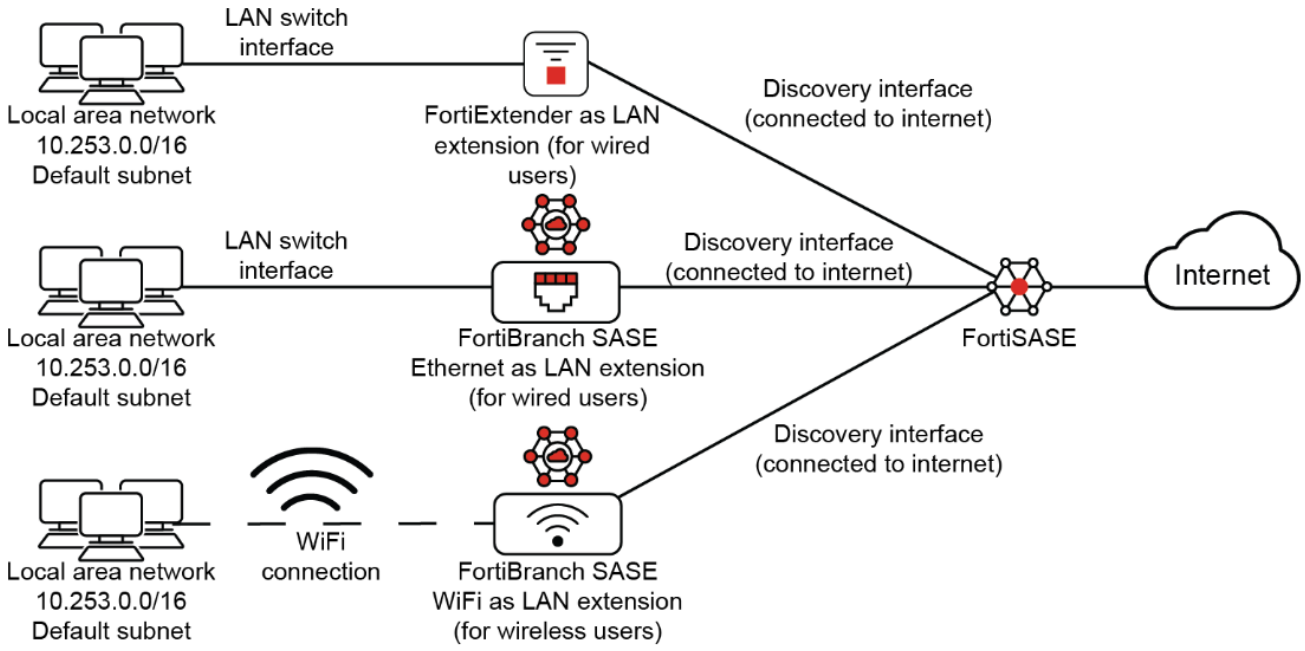
This document outlines the configuration steps required to connect FortiBranchSASE devices to FortiGate or FortiSASE for LAN extension deployments.

- For FortiBranchSASE devices operating in standalone mode, refer to the *FortiExtender Standalone Mode Administration Guide*.
- For FortiBranchSASE devices managed by FortiGate, refer to the FortiGate LAN Extension section in the *FortiOS Administration Guide* for configuration guidance.
- For FortiBranchSASE device working in FortiSASE managed mode, refer to Configuring FortiExtender as FortiSASE LAN Extension in the *FortiSASE Administration Guide*.

Key Features

Managing FortiBranchSASE from FortiSASE or FortiGate offers the following key features:

- FortiBranchSASE provides centralized control and configuration, enabling streamlined connection across the network.
- Split-Tunnel capabilities allow for secure connections to corporate application and direct internet access for personal internet access.
- Flexible zero-touch provisioning for quick deployment, simple enough for users of all technical levels to install on site.
- Unified management console simplifies operations and ensures consistent policy enforcement.



Getting started

This section covers topics to help you get started with setting up your FortiBranchSASE.

Prerequisites

Before you begin, you must complete the following:

1. Before installing, you must register FortiBranchSASE devices using the LAN extension feature to the same FortiCloud account used to log into FortiSASE.
2. To activate FortiBranchSASE management support on FortiSASE, you must purchase and apply a FortiSASE ThinEdge License to each registered FortiBranchSASE device.

Recommended port configurations

Fortinet recommends different port configuration depending on your FortiBranchSASE model.

Model	Recommended configuration
FBS-10F WiFi	The device includes one WAN port and one LAN port. • Use the WAN port as the discovery interface. • Use the LAN port for connecting to the local network.
FBS-20G / FBS-20G WiFi	WAN Interfaces (Port 1 and Port 2): • Both ports are configured as WAN interfaces in DHCP mode by default. • Use one or both ports as discovery interfaces to connect with FortiGate or FortiSASE. LAN Interfaces (Port 4 and Port 5): • These ports are part of the integrated LAN switch. • You can connect local network devices to either Port 4 or Port 5.

Accessing FortiBranchSASE

To access the FortiBranchSASE web GUI from a computer:

1. Using an Ethernet cable, connect your computer to a FortiBranchSASE LAN port.
2. Configure your computer's network settings to the following:

- IP Address: `192.168.200.100`
- Netmask: `255.255.255.0`

3. Open a web browser and navigate to the default FortiBranchSASE web GUI address: `http://192.168.200.99`
4. Enter `admin` as the username.
5. Follow the on-screen CLI prompt to create your new password.

To access FortiBranchSASE using Telnet or SSH:

1. Using an Ethernet cable, connect your computer to Port 4 or Port 5 of the FortiBranchSASE.
2. Manually configure your computer's network settings to the following:
   - IP Address: `192.168.200.100`
   - Subnet Mask: `255.255.255.0`
3. Open a Telnet or SSH client (such as PuTTY or Terminal) and connect to IP address `192.168.200.99`.
   - If using Telnet, use *port 23*.
   - If using SSH, use *port 22*.

Configuring the Discovery Interface

By default FortiBranchSASE models have different ports designated as the discovery interface. These interfaces are used to establish connectivity with FortiGate or FortiSASE for device discovery and onboarding.

Model	Discovery interfaces
FBS-20G / FBS-20G WiFi	Port 1 and Port 2
FBS-10F WiFi	WAN port

To configure the discovery interface on a FortiBranchSASE device - CLI:

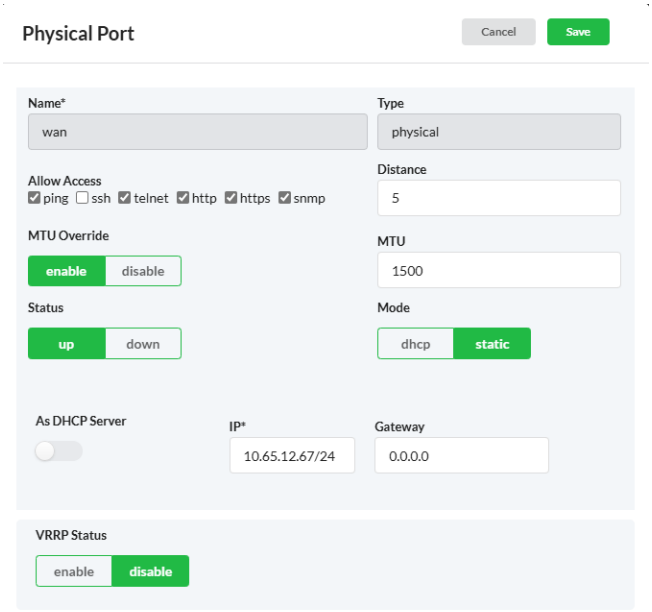
```
config system management
  set discovery-type auto
  config fortigate
    set ac-discovery-type broadcast
    set ac-ctl-port 5246
    set ac-data-port 25246
    set discovery-intf port1 port2
    set ingress-intf
  end
end
```

Configuring the Interface IP Address

You can configure the IP address of an interface using either the FortiBranchSASE GUI or CLI.

To configure the interface IP address - GUI:

1. Navigate to *Networking* > *Interface* > *Edit Physical Ports*.
2. Select an interface (for example, Port 1, Port 2, or WAN depending on your model).
3. Click *Edit*.
4. Depending on your network setup, select a *Mode*.
   You can choose between *static* or *dhcp*.



5. When you are finished, click *Save*.

To configure the interface IP address - CLI:

```
config system interface
  edit <interface_name>
    set mode <dhcp | static>
      # If using static mode:
      set ip <IP_address> <subnet_mask>
  next
end
```

Command	Description
<interface_name>	Enter the interface. For example, port1, port2, or wan.
mode <dhcp | static>	Select a server mode.

Command	Description
set ip <IP_address> <subnet_mask>	If you selected a static server mode, enter a static IP and subnet mask. For example, 192.168.1.99 255.255.255.0.

FortiSASE managed mode

This section contains topics on connecting a FortiBranchSASE to FortiSASE and how to configure it.

Connecting FortiBranchSASE to FortiSASE

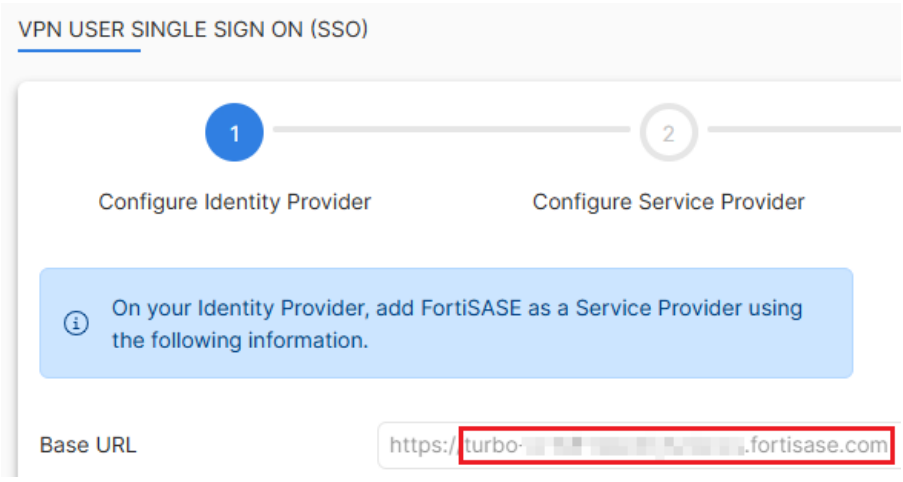
For information on connecting FortiBranchSASE to FortiSASE using FortiZTP, refer to Connecting FortiExtender to FortiSASE using FortiZTP in the *FortiSASE Admin Guide*.

Before connecting your FortiBranchSASE to FortiSASE, perform the following:

1. Ensure you are running the latest FortiBranchSASE OS firmware. If not, update the firmware to ensure compatibility and optimal performance.
2. Ensure that no other configurations have been applied, except for the modifications made to the discovery interface. This ensures that the device is ready for a clean connection to FortiSASE.
3. Obtain the FortiSASE domain name from FortiSASE.

To obtain the FortiSASE domain name from FortiSASE:

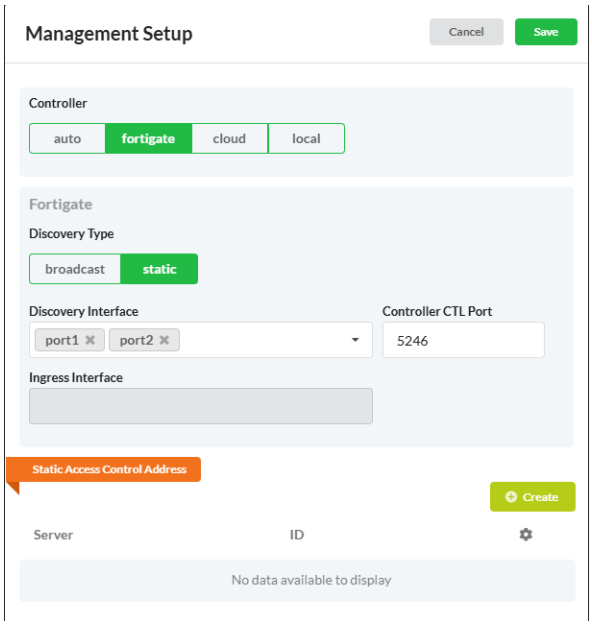
1. From the FortiSASE GUI, go to *Configuration* > *VPN User SSO*.
2. Locate the *Base URL* field. The FortiSASE domain name comes after the `https://` string.
   In the example, the FortiSASE domain name is `turbo...fortisase.com`.



To connect a FortiBranchSASE to a FortiSASE - GUI:

1. Log in to the FortiBranchSASE GUI.
2. Navigate to *Settings* > *Management*.
3. In the *Management Setup* section, click *Edit* to edit settings.
4. Configure the following:

Controller	*fortigate*
Discovery Type	*static*
Discovery Interface	Select the interface connected to the internet.

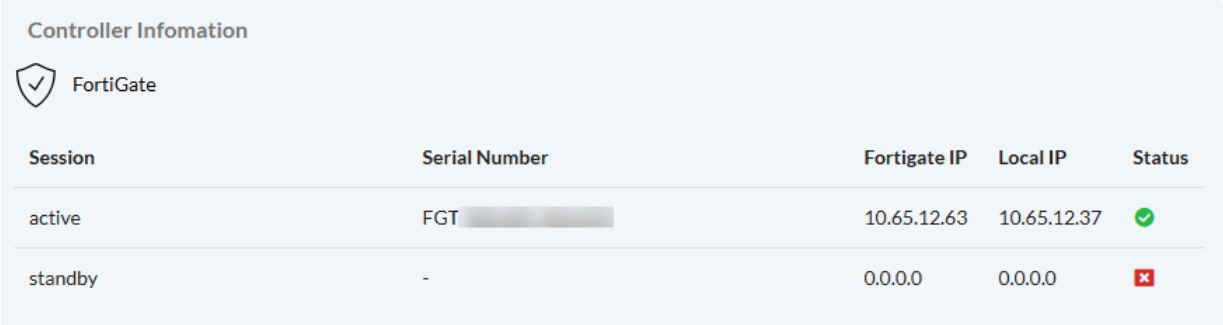


5. Under *Static Access Control Address*, click *Create* and configure the following:
   - *Server*: Enter the FortiSASE domain name. For more information, see To obtain the FortiSASE domain name from FortiSASE: on page 11.
   - *ID*: 1.

   When you are finished, click *Save*.
6. Click *Save* again to apply all settings.
7. When prompted, click *OK* to confirm and reboot the FortiBranchSASE for the changes to take effect.

To verify the connection is successful - GUI:

5. After the FortiBranchSASE finishes rebooting, log back into the FortiBranchSASE GUI.
6. Go to *Dashboard*.
7. Under *Controller Information*, ensure that:
   - *FGT IP* is a non-zero address.
   - *Status* shows as *Connected*.



To connect a FortiBranchSASE to a FortiSASE - CLI:

1. Log in to the FortiBranchSASE CLI.
2. Configure the system management setting and edit the domain name:

```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
        set server <enter the FortiSASE domain name>
      next
    end
    set discovery-intf port1 port2 wan <customize per your FBS model and networking
environment>
  end
end
```

To verify the connection is successful - CLI:

1. From the FortiBranchSASE CLI, run the following command:

```
# get extender status
Extender Status
    name                : BS20GWS224000007
    mode                : CAPWAP
    session             : active
      fext-addr         : 172.XX.XXX.XXX
      ingress-intf      : port1
      controller-addr   : 206.XX.XXX.XXX:5246
      controller-name   : FGXXXXXXXXXXXXX
      uptime            : 3 days, 1 hours, 37 minutes, 52 seconds
      management-state  : CWWS_RUN
    base-mac            : 78:18:EC:C4:86:90
    network-mode        : lan-extension
    fgt-backup-mode     : backup
    discovery-type      : static
    discovery-interval  : 5
    echo-interval       : 30
```

```
    report-interval      : 30
    statistics-interval  : 120
    mdm-fw-server        : fortiextender-firmware.forticloud.com
    os-fw-server         : fortiextender-firmware.forticloud.com
```

Confirm that `controller-addr` is non-zero and `management-state` is `CWWS_RUN`.

Configuring SSIDs and FortiExtender Profiles for FortiBranchSASE

Certain FortiBranchSASE WiFi models, such as FBS-20G-WiFi and FBS-10F-WiFi, support wired, wireless, or both types of connectivity, offering enhanced flexibility and performance for micro branch LAN deployments. They can support both wired and wireless users, helping to extend and optimize your LAN coverage.

You can configure SSIDs, allowing wireless users to connect to the network. IP address management (IPAM) in FortiSASE handles automatic assignment of IP address and subnet mask information for each SSID, streamlining network configuration.

When a FortiBranchSASE device connects to FortiSASE, a default FortiExtender profile is automatically generated. You can either use the default profile or create a custom FortiExtender profile to override and tailor settings for specific devices.

Since FortiBranchSASE is a member of the FortiExtender product family, it also uses FortiExtender profiles.

To configure SSIDs for FortiBranchSASE:

1. Navigate to *Edge Devices* > *FortiExtenders*.
2. Select the *SSIDs* tab and then click *Create*.
3. Enter a *Name*.
4. Under *Wifi Settings*, complete the following settings:

Field	Description
SSID	Enter the name for SSID.
Client Limit	Enable the toggle to specify the limit for number of clients that are allowed to connect to SSID.
Broadcast SSID	Enable SSID broadcast

5. Under *WiFi Security*, complete the following settings:

Field	Description
Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. • *WPA2 Personal*: WPA2 is WiFi Protected Access version 2. Users use a pre-shared key (password) to obtain access. • *WPA2 Enterprise*: similar to WPA2 Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password. • *WPA3 Enterprise Only*: WPA3 enterprise with Protected Management Frames (PMF) mandatory. Best used for enterprise networks. Each user is separately authenticated by user name and password. • *Captive Portal Only*: Captive portal will be enforced based on the security groups selected in the individual FortiExtender configuration. To avoid captive portal, ensure you have a policy for the FortiExtender which exempts captive portal authentication, see Configuring an exemption policy for an edge device.
Pre-shared Key	Available only when *Mode* is *WPA2 Personal*. Preshared key must be 8 to 63 characters long.
Authentication server address	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Enter the IP address or resolvable FQDN of the RADIUS server.
Authentication server port	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Enter the authentication port number used by RADIUS server.
Authentication server secret	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Enter the password used to connect to the RADIUS server.

6. When you are finished, click *OK*.

To configure FortiExtender Profiles for FortiBranchSASE:

1. Go to *Edge Devices* > *FortiExtenders* and select the *FortiExtender Profiles* tab.
2. Select the default FortiExtender profile created by FortiSASE based on the model detected by FortiSASE and click *Edit* or click *Create* for new FortiExtender profile.
3. (Optional) If editing the default profile, click *Change* next to the *Login Password* field to update the default login credentials for the FortiBranchSASE device.
4. For new profiles, click the *Model* dropdown and select the model of your FortiBranchSASE device.
5. For new profiles, enter a new password in the *Login Password* field.
   This will be applied to the FortiBranchSASE device during provisioning.
6. In the *Country/Region* dropdown, select the location where the FortiBranchSASE device is deployed.
   This ensures compliance with local wireless regulations.
7. Under *WiFi Configuration*, select *2.4GHZ Radio* or/and *5GHz Radio* and set the *Status* to *Enable*.
8. Complete the following settings:

Field	Description
Status	Activates the selected radio when set to *Enable*
Operating Standard	Select the wireless protocols to support. The available choices depend on the radio's capabilities. Where multiple protocols are supported, the letter suffixes are combined: "802.11ax/n/g" means 802.11ax and 802.11n and 802.11g.
Extension channel	Specify whether the additional channel for extended bandwidth is placed above or below the primary channel. Options include *Auto*, *Higher*, and *Lower*.
Bandwidth	Select the range of frequency range used by WiFi channels to transmit data.
Guard interval	Choose an appropriate time buffer to mitigate Intersymbol Interference (ISI) based on your microbranch deployment environment. Available options include *Auto*, *400 ns*, and *800 ns*.
Transmit power	Adjust the transmit power by selecting a percentage of the maximum power allowed based on the configured country/region and FortiBranchSASE device. Use the slider to set a suitable percentage.
Channels	Select the specific channel(s) to use. The available options depend on the IEEE wireless protocol selected under Operating Standard.
LAN extension SSID	Select the SSID from the dropdown menu that you want to broadcast on the selected radio.

9. When you are finished, click *OK*.
   Once you finish configuring the FortiExtender profile, you must apply it to a FortiBranchSASE device. See Authorizing and deauthorizing a FortiBranchSASE device on page 16.

Authorizing and deauthorizing a FortiBranchSASE device

Since FortiBranchSASE is a member of the FortiExtender product family, the process to authorize is the same as FortiExtenders.

To authorize a FortiBranchSASE device:

1. Navigate to *Edge Devices* > *FortiExtenders*.
2. Go to the *Managed FortiExtenders* tab and select the FortiBranchSASE device you want to authorize.
3. Perform one of the following actions:
   - Under the *Authorization* column, click *Authorize*; or
   - Right-click the device and select *Authorization* > *Authorize*.

   Once you authorize the FortiBranchSASE, a slide-in panel loads

4. From the *Profile* dropdown, select the profile you want to apply and then click OK.
5. After authorization, the FortiBranchSASE may initially appear as *offline*.
   You can refresh the *FortiExtenders* page. Once the connection is established, the device status changes to *online*.

To deauthorize and remove a FortiBranchSASE device from FortiSASE management:

1. Navigate to *Edge Devices* > *FortiExtenders*.
2. Select the FortiBranchSASE device you want to deauthorize.
3. Perform one of the following actions:
   - Under the *Authorization* column, click *Deauthorize*; or
   - Right-click the device and select *Authorization* > *Deauthorize*.
4. Once deauthorized, *FortiSASE* will update the device's status to *FortiCare Registered*, indicating that it is no longer under FortiSASE management but remains registered to your FortiCare account.

Disconnecting a FortiBranchSASE

If a FortiBranchSASE device has been deregistered from the FortiCloud account, disconnecting it will remove the entry from the FortiSASE console under *Edge Devices* > *FortiExtenders*.

To disconnect a FortiBranchSASE:

1. Navigate to *Edge Devices* > *FortiExtenders*.
2. Select the FortiBranchSASE device you wish to disconnect.
3. Perform one of the following actions:
   - Click the *Disconnect* button; or
   - Right-click the device and select *Disconnect*.

Once disconnected, the device will no longer appear in the FortiExtenders list in FortiSASE.

FortiGate managed mode

LAN Extension is a configuration mode on FortiGate that enables a FortiBranchSASE device to act as a remote thin edge node, extending LAN connectivity over a secure backhaul link.

When you deploy a FortiBranchSASE at a remote site, the FortiBranchSASE performs the following actions:

- Discovers the FortiGate Access Controller (AC).
- Establishes an IPsec tunnel (or multiple tunnels, if multiple WAN links are available).
- Forms a VXLAN over these IPsec tunnels, enabling Layer 2 (L2) connectivity between the FortiGate and the network behind the remote FortiBranchSASE.

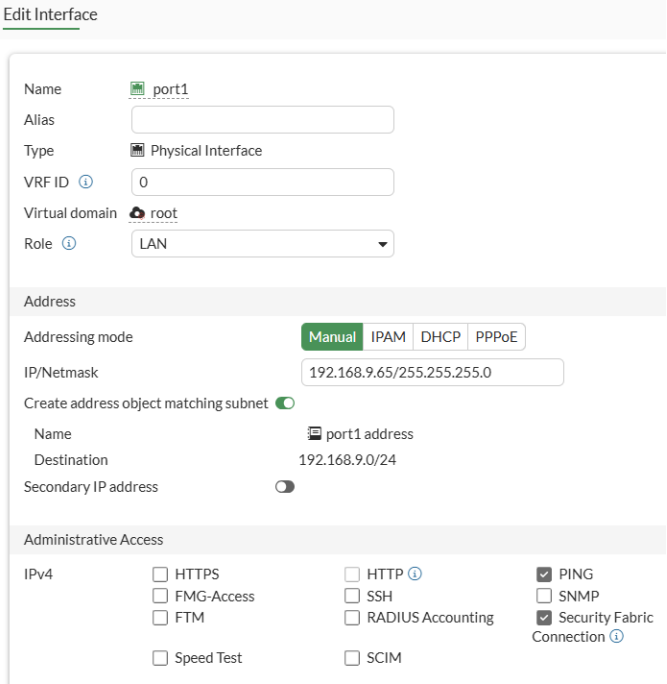
For more information on the LAN-Extension solution, refer to the Using the backhaul IP when the FortiGate access controller is behind NAT in the *FortiExtender (Managed) Administration Guide*.

Configuring a FortiBranchSASE for FortiGate discovery and authorization

Before you can deploy a FortiBranchSASE under FortiGate management, you must first configure your devices so that the FortiGate can discover the FortiBranchSASE.

To configure FortiGate to discover FortiBranchSASE - GUI:

1. From the FortiGate GUI, enable *Security Fabric connection* on the interface (e.g., *port1*) to allow FortiBranchSASE to connect over CAPWAP:
   a. Navigate to *Network* > *Interfaces*.
   b. Edit *port1*.
   c. Under *Administrative Access*, enable *PING* and *Security Fabric Connection*
   d. Click *OK* to save changes.



To configure FortiGate to discover FortiBranchSASE - CLI:

1. From the FortiGate CLI, enable *Security Fabric connection* on the interface (e.g., *port1*) to allow FortiBranchSASE to connect over CAPWAP.

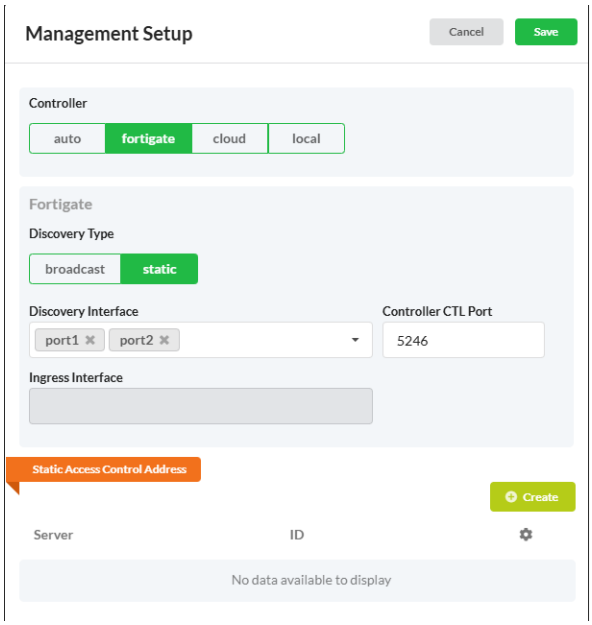
```
config system interface
  edit "port1"
    set vdom "root"
    set ip 192.168.9.65 255.255.255.0
    set allowaccess ping fabric
  next
end
```

To configure FortiBranchSASE so it can be discovered by FortiGate - GUI:

1. Log in to the FortiBranchSASE GUI.
2. Navigate to *Settings* > *Management*.
3. In the *Management Setup* section, click *Edit* to edit settings.
4. Configure the following:

Controller	*fortigate*
Discovery Type	*static*
Discovery Interface	Select the interface that can reach the FortiGate port 1 IP address.
Static Access Control Address > Create	
Server	Enter the FortiGate port 1 IP address.

ID	1



5. When you are finished, click *Save*.
6. Click *Save* to apply all settings.
7. When prompted, click *OK* so the changes to take effect.

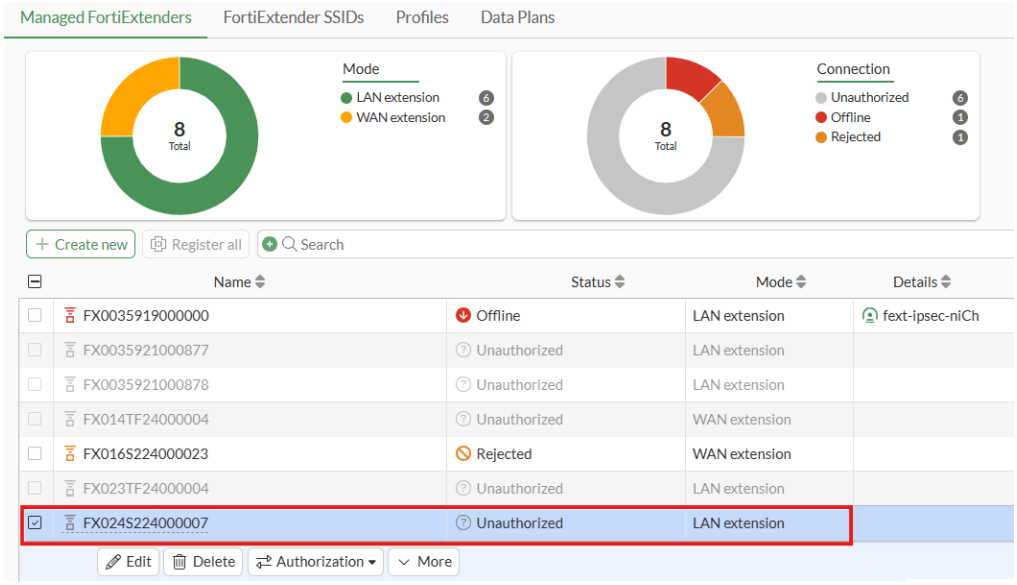
To configure FortiBranchSASE so it can be discovered by FortiGate - CLI:

1. Connect to the FortiBranchSASE CLI via SSH, then set the FortiGate as the static Access Controller (AC) server.

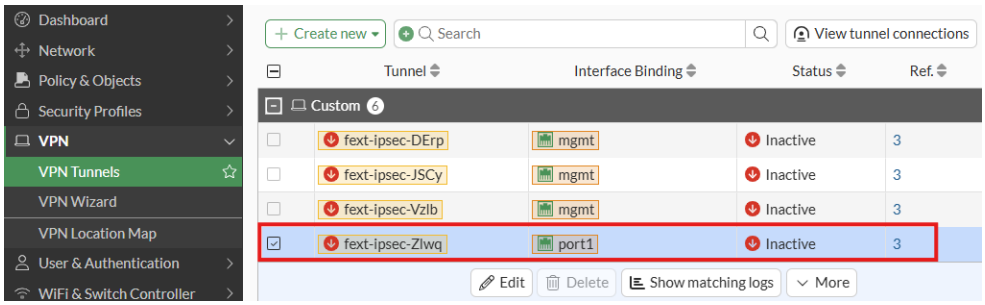
```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
        set server 192.168.9.65     # FortiGate IP from Step 1
      next
    end
    set ac-ctl-port 5246            # CAPWAP Control Port
    set ac-data-port 25246          # CAPWAP Data Port
    set discovery-intf port1 port2  # Discovery interfaces (adjust as needed)
    set ingress-intf
  end
end
```

To verify FortiBranchSASE is discovered by FortiGate - GUI:

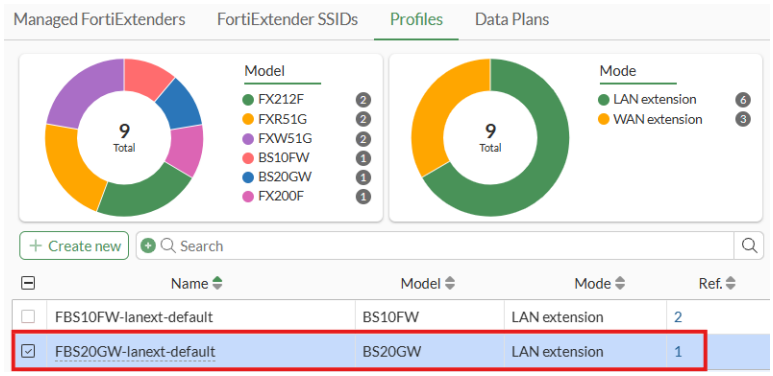
- Once the FortiBranchSASE's discovery packet reaches port1 on the FortiGate, the FortiBranchSASE will appear under the FortiGate GUI's *Network* > *FortiExtenders* with an *Unauthorized* status.



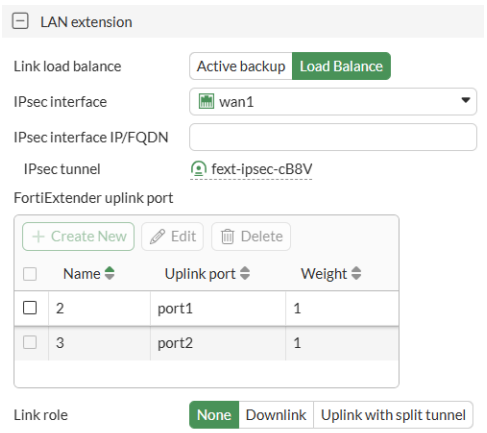
- The FortiGate automatically creates a VPN profile for this FortiBranchSASE in *VPN > IPsec Tunnels*.



- The FortiGate also automatically creates a FortiExtender profile for that model of FortiBranchSASE, which can be found in *Network > FortiExtenders > Profiles*.



By default, the profile selects *Load Balance* as the Link load balance setting and has the IPsec interface and pre-configured tunnel set.



To verify FortiBranchSASE is discovered by FortiGate - CLI:

- When the FortiGate successfully discovers a FortiBranchSASE device, it automatically initializes basic configuration parameters in FortiOS:

```
config extension-controller extender
  edit " FX024S224000007"
    set id " BS20GWS224000007"                    # Device serial or model ID
    set device-id 0                              # Internal identifier
    set extension-type lan-extension             # Configured as LAN extension
    set profile " FBS20GW-lanext-default"          # Default profile assigned
  next
end
```

- The FortiGate automatically creates an IPsec VPN tunnel for the detected FortiBranchSASE:

```
config vpn ipsec phase1-interface
  edit "fext-ipsec-ksKS"
    set type dynamic
    set interface "port1"
    set ike-version 2
    set peertype one
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set localid "localid-5bzuqs54dGni2TT0x2NePg0HexHW2piQ44aZ4NiGe8SVxxBnFuiqZqo"
    set dpd on-idle
    set comments "[ FBS20GW -lanext-default] Do NOT edit. Automatically generated by extender
controller."
    set peerid "peerid-svxVy5bZbPxZdfoIQBNA7YrkSKBA9Ui1vZsvYcVrgp1Uy0aFMCVZzGzh"
    set psksecret ENC <secret>
    set dpd-retryinterval 60
  next
end
config vpn ipsec phase2-interface
  edit "fext-ipsec-ksKS"
    set phase1name "fext-ipsec-ksKS"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
```

```
chacha20poly1305
    set comments "[ FBS20GW -lanext-default] Do NOT edit. Automatically generated by extender
controller."
  next
end
```

- The FortiGate automatically creates a FortiExtender profile based on the FortiBranchSASE model. By default, the Link load balance is set to *Load Balance*. The IPsec interface and pre-configured tunnel are also set.

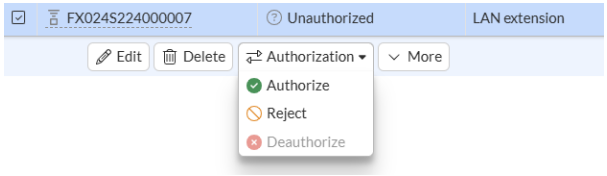
```
config extension-controller extender-profile
  edit "FBS20GW-lanext-default"
    set id 4
    set model BS20GW
    set extension lan-extension
    config wifi
      set country US
      config radio-1
        set mode AP
        set band 2.4GHz
        set status disable
        set operating-standard auto
      end
      config radio-2
        set mode AP
        set band 5GHz
        set status enable
        set operating-standard auto
      end
    end
    config lan-extension
      set link-loadbalance loadbalance
      set ipsec-tunnel "fext-ipsec-a7KH"
      set backhaul-interface "mgmt"
      config backhaul
        edit "2"
          set port port1
        next
        edit "3"
          set port port2
        next
      end
    end
  next
end
```

Authorizing FortiBranchSASE

Once the FortiBranchSASE is discovered by the FortiGate, you can authorize it.

To authorize FortiBranchSASE on FortiGate - GUI:

1. Go to *Network* > *FortiExtenders* > *Managed FortiExtenders* and select the discovered FortiBranchSASE you want to authorize.
2. In the *Authorization* dropdown, select *Authorize*.



3. Click *OK*.
   The device now displays as authorized.

To authorize FortiBranchSASE on FortiGate - GUI:

```
config extension-controller extender
  edit "FX024S224000007"
    set authorized enable
  next
end
```

www.fortinet.com