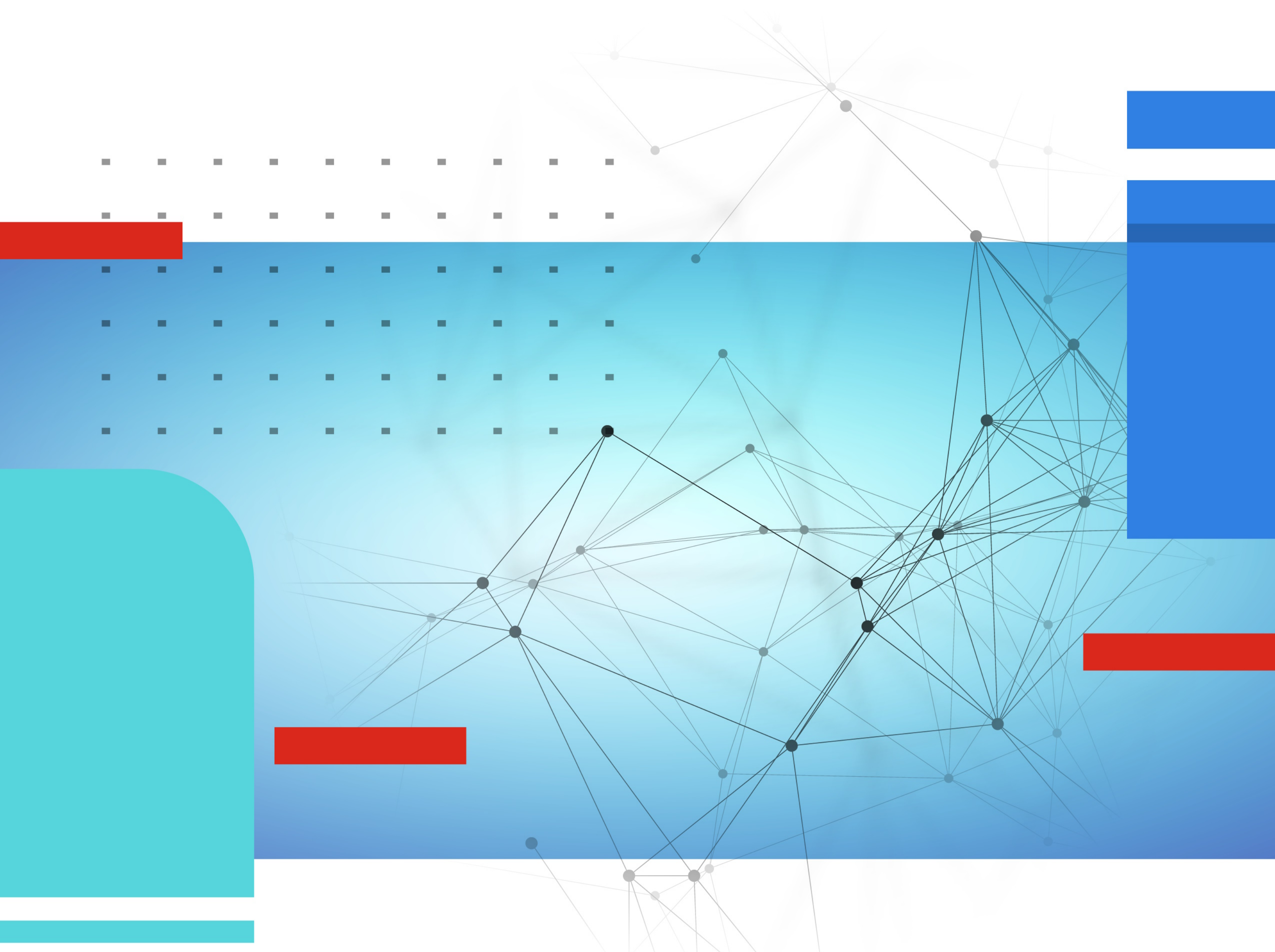
Administration Guide

FortiExtender Cloud 24.1



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

March 15, 2024
FortiExtender Cloud 24.1 Administration Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-03-15	FortiExtender Cloud 24.1 Administration Guide initial release.

Introduction

FortiExtender Cloud is a Cloud-based Web application for deploying and managing FortiExtender devices over distributed LTE networks. With FortiExtender Cloud, you can remotely deploy and manage your devices. FortiExtender Cloud helps you improve productivity, reduce cost of ownership, and ensure the reliability and intelligence of your business operations.

Main features and benefits

FortiExtender Cloud offers the following features and benefits:

Support for unlimited number of devices

FortiExtender Cloud can support an unlimited number of devices across the globe, making it easy to scale up or down based on your business needs.

Centralized management

Create and update configuration profiles, device groups, and mobile service plans, all from a single portal.

Zero-touch deployment

Remotely configure and deploy your devices from anywhere.

SSO authentication

FortiExtender Cloud provides single sign-on (SSO) authentication for all applications running on its platform, not only ensuring the security and integrity of your devices on the Cloud but also enhancing user experience. We monitor each and every log in and access attempt to prevent malicious actors from gaining access to your devices using compromised credentials.

Device access control

FortiExtender Cloud lets you manage user access by assigning ReadWrite or a ReadOnly permissions to user accounts. This ensures that only authorized users can access your devices through FortiExtender Cloud. For more information, see Manage users on page 74.

Automatic SIM switching

Each FortiExtender unit can support up to two or four SIM cards depending on the model. While one card is in use, the other stands by as a backup. If a certain event happens such as the SIM card disconnecting multiple times or the plan data capacity is hit, the system automatically switches over to the other card to ensure uninterrupted service.

Configuration profile

Profiles are configurations templates that can be applied to devices. FortiExtender Cloud makes it easy to create, update, clone, and apply profiles to devices. For more information, see Profile on page 10.

Device group

Grouping devices together can greatly improve your operational efficiency because it lets you apply or update the same configuration profile to all devices in a group. For more information, see Group on page 9.

Carrier plan management

FortiExtender Cloud makes it easy to view and monitor the usage of your existing mobile service plans. You can continue to add or clone new carrier plans as your business evolves. For more information, see Carrier plan on page 10.

Remote OS and modem firmware upgrades

You can easily schedule upgrades to the OS or modem firmware on your device from FortiExtender Cloud.

Event logs

FortiExtender Cloud captures user, device, and system events in the Log page. This lets you keep track of device activities and device status 24/7. For more information, see View event logs on page 80.

Dashboard

The Dashboard page provides an overview of device location, user activity, and device status data critical to your business operations. For more information, see The Dashboard on page 19.

Key concepts

This section discusses the key product concepts used in FortiExtender Cloud.

- Group
- In Service
- Inventory
- Offline
- Online
- Carrier plan
- Profile

Device State

Once a device is deployed and In Service, they are sorted into one of the following states:

Device States	Description
⟳ Deploying	The device is in the process of being deployed.
✓ Deployed	The device is fully installed and synced with the firmware configurations from FortiExtender Cloud.
○ Syncing	The device is currently syncing its configurations with FortiExtender Cloud. The device will reboot during the syncing process.

Group

A *group* is a virtual container that contains one or more devices. You can add up to two profiles for each group, one profile per device model category. Each device can join only one group. When adding a device to a group, you can decide whether to keep the device's own profile or override it with that of the group. If you elect to keep the device's profile, it will take priority over the group profile.

Grouping makes it easy to keep track of and manage your devices by letting you upgrade the device firmware by group. For more information, see Manage device groups on page 40.

In Service

A device is categorized as *In Service* when it is deployed on FortiExtender Cloud. When a device is In Service, you can edit its configurations and manage it remotely from FortiExtender Cloud.

In Service devices all have a device state. For more information, see Device State on page 8.

Inventory

A device is categorized as *Inventory* after it is registered in FortiCare, but before it is deployed.

Offline

An In Service device has an *offline* availability status when it is not connected to FortiExtender Cloud.

A device can be offline for the following reasons:

- The device is down.
- The SIM card has been removed from its slot or has exceeded its subscribed data plan (if it connects to FortiExtender Cloud through a SIM card).
- The device has been unplugged from the LAN (if it connects to FortiExtender Cloud through an Ethernet connection).

Online

An In Service device has an *online* availability status when it is deployed and connected to FortiExtender Cloud.

Carrier plan

A *carrier plan* refers to a service plan that you have signed up or subscribed from a mobile phone service provider or carrier. It identifies your mobile phone service provider, and contains information such as your allowed data usage and billing cycle.

Profile

A *profile* is a configuration object that specifies the various settings that can be applied to a device or group of devices. Before you can deploy a device, you must first choose a profile and apply it to the device. No device can be deployed without a profile. Because profiles are associated with devices, any change made to a profile will affect the associated devices and cause them to reboot. After a profile is applied to a FortiExtender, it will overwrite any existing configuration on the device.

A profile contains all configuration information except the OS and modem firmware, which must be installed or updated either through FortiExtender Cloud or your LAN.

Note: The Device Detail page (under the In Service page) lets you change a device's configuration. Changes made on that page will override both the individual profile or group profile (see Group on page 9) associated with the device.

Licensing

As of March 29, 2020, the FortiExtender Cloud free tier licenses are no longer offered. This service allowed you to register and manage 3 FortiExtender units, free of charge, in FortiExtender Cloud. The units that have been managed for free previously will continue to work with their last uploaded configurations.

To add more devices, you must purchase a license for each new device through authorized Fortinet resellers and distributors. For licensing information, contact your primary Fortinet service provider.

Supported devices and OS firmware versions

FortiExtender Cloud supports the following FortiExtender models and OS firmware versions:

Supported Models

- FEX-40D-AMEU, FEX-40D-NAM, FEX-40D-INTL, FEX-201E, FEX-211E
- FEX-101F-AM, FEX-101F-EA
- FEX-200F, FEX-201F-AM, FEX-201F-EA, FEX-202F-AM, FEX-202F-EA, FEX-212F
- FEX-311F, FEX-511F
- FEV-211F, FEV211F-AM

Supported OS firmware versions

- 4.1.1, 4.1.2, 4.1.3, 4.1.4
- 4.2.0, 4.2.1, 4.2.2
- 7.0.0, 7.0.1, 7.0.2, 7.0.3
- 7.2.0, 7.2.1, 7.2.2, 7.2.3
- 7.4.0, 7.4.1, 7.4.3

Getting started

This section gets you started with instructions on how to register your FortiExtender device, access and navigate FortiExtender Cloud, and push configurations from FortiExtender Cloud to your devices.

- Step 1: Register and add your devices
- Step 2: Access FortiExtender Cloud
- Step 3: Configure device profiles or groups
- Step 4: Select a device to deploy
- Step 5: Synchronize and install your device

Step 1: Register and add your devices

To add devices to FortiExtender Cloud, you must first register your FortiExtender devices through your FortiCare account. After your devices are registered, they are automatically added to FortiExtender Cloud.

To register and add your FortiExtender devices:

1. Log into your account at https://support.fortinet.com.
   If you do not have an existing FortiCare account, click *Register* and complete the registration process.
2. Click *Register Now* to register your FortiExtender to the FortiExtender Cloud platform.
   The Register Product page loads.
3. In the *Registration Code* field, enter your device's FortiCloud Key or serial number.
4. Select your end user type, and then click *Next*.
5. Follow the on-screen instructions and complete the appropriate fields to finish registering your device.
   Once your device is registered, it is automatically added into FortiExtender Cloud.

Step 2: Access FortiExtender Cloud

Before you can access FortiExtender Cloud, you must have either:

- A FortiCare/FortiCloud account, or
- A FortiGate account.

To access FortiExtender Cloud:

1. Log into your account at https://fortiextender.forticloud.com.
2. Enter your Account ID/Email and password, and then click *Login*.
   The FortiExtender Cloud home page opens.

We recommend that you use the following browsers to access FortiExtender Cloud:

- Google Chrome
- Firefox
- Microsoft Edge

FortiExtender Cloud UI

The FortiExtender Cloud UI has two main parts:

- A navigation bar
- An information pane

Navigation bar

The navigation bar is located on the left of each page and contains links to the main pages of FortiExtender Cloud.

Navigation bar links	Link description
Dashboard (home page)	Monitor device usage statistics and see your device's geographical locations on a map.
Device	Expand to manage your devices. • *In Service*: Manage your active devices. • *Inventory*: Deploy registered devices.
Scheduled Upgrade	Manage your scheduled OS and Modem firmware upgrades.
Group	Manage your groups.
Plan	Expand to manage your plans. • *Carrier*: Manage your carrier plans. • *Credential*: Manage your account credential plans. • *Network*: Manage your network plans. • *VPN*: Manage your VPN plans. • *DNS Database*: Manage your DNS Database plans.
Customized Carrier	Lists all your customized carriers in one location for ease of management.
Profile	Manage your device profiles.
Certificates	Expand to manage your certificates. • *VPN Local*: Upload local certificates to specific devices. • *VPN Ca*: Upload Certificate Authority (CA) to apply to multiple devices. You can assign these certificates from VPN Plan if you select a signature authentication method.
Log	See user, device, and system event logs.
Notification	Create notifications to send email or SMS alerts when there are changes to a device's availability status or health.
Feedback	Leave feedback about FortiExtender Cloud.

Navigation bar links	Link description
Questions	Links to the FortiExtender Cloud documentation page.
Account	Expand to access account settings. • *Settings*: Manage device heartbeat interval and email notifications for users. • *License Information*: View license status and subscription information. • *API Token*: Opens a window containing your API token. • *Sub Users*: View your sub users who have access to FortiExtender Cloud. • *IAM Users*: View the Identity and Access Management Portal Users who have access to FortiExtender Cloud.

Information pane

The information pane displays the contents of the selected page.

Step 3: Configure device profiles or groups

Before you can deploy a device, you must first configure a profile or group for your device. There are two steps to the configuration process:

1. (Optional) Create a carrier plan for the profile.
2. Create a device profile or device group.

Configuring a carrier plan

Before you configure your profile's general settings, you have the option to create a carrier plan to add to the profile.

A *carrier plan* refers to a service plan that you have signed up or subscribed from a mobile phone service provider or carrier. It identifies your mobile phone service provider, and contains information such as your allowed data usage and billing cycle.

- If you do not want to create a plan for your profile, skip to Create a device profile or device group on page 15.

Before creating your plan, you must know:

- The name of your carrier company
- Your Access Point Name (APN)
- Your Authentication type (None, CHAP, PAP)
- Your plan's billing date
- Your plan's total capacity (in MB)
- If your plan is an individual plan or a pooled plan
- Your plan's overage limits (if any)
- Your plan's security mode (NAT or IP PASS)

1. In the navigation bar, go to *Plan* > *Carrier*.

   The Carrier Plan page loads.
2. In the upper-left corner of the page, click *Add Carrier Plan*.

   The Add Carrier Plan window loads.
3. In the Plan Name field, enter a plan name.

   Note: Valid characters are: alphanumeric characters and special characters (. -_). Spaces are not permitted.
4. Click *Add*.

   The Carrier Plan Detail page loads.
5. Make the required entries or selections. For more information about each configuration option, see Profile configuration fields on page 23.
6. Click *Save*.

   The new carrier plan is created. You can return to the Carrier Plan page to see it.

Create a device profile or device group

Before you can deploy a device, you must create a profile or group.

- Profiles contain configuration specifications that you can apply to multiple devices.
- Groups are a way to manage and group together different devices under one profile.

For more information on device profiles and groups, see Key concepts on page 8.

Before deploying a device, consider the following:

- How many SIM cards will you use? Depending on your FortiExtender model, it can support either two or four SIM cards.
- If you have multiple SIM cards, do you want to automatically switch between the cards to maintain connection quality?
- Do your SIM cards have a PIN code?
- How do you want to organize your devices? By group or by profiles? For more information on the differences between groups and profiles, see Group on page 9 and Profile on page 10.
- What is your data plan?

To create a device profile:

1. From the Navigation bar, go to *Profile*.
2. Click *Add Profile* to create a new profile.

   The Add Profile window loads.
3. Complete the following fields:

Field Name	Description
Profile Name	Enter a name for the profile. **Note:** Valid characters are: alphanumeric characters and special characters (. -_). Spaces are not permitted.
Hardware Platform	Select the hardware platform/model you want to apply the profile to.

4. Click *Add*.

   The Profile Settings page loads.
5. Make your profile configuration selections. For more information about each configuration option, see Profile configuration fields on page 23.
6. Click *Save* to save the profile.

   The new profile is created. You can return to the Profile page to see it.

To create a group:

1. From the Navigation bar, go to *Group*.

   The Group page loads.
2. Click *Add Group* to create a new group

   The Add Group window loads.
3. Complete the following fields:

Field Name	Description
Group Name	Enter a name for the group. **Note:** Valid characters are: alphanumeric characters and special characters (. -_). Spaces are not permitted.
Profile for Single Modem	Select a profile that applies to devices with a single modem.
Profile for Dual Modem	Select a profile that applies to devices with a dual modem.

4. Click *Apply*.

   The Group Settings page loads.
5. Verify that your group settings are correct.

Step 4: Select a device to deploy

Adding devices

You cannot add devices into FortiExtender Cloud directly. Your registered devices are automatically pulled from your FortiCare account and listed in the Inventory page.

If you do not see your devices in the Inventory page, log into your FortiCare account at https://support.fortinet.com and go to *Asset* > *Register/Activate* to register your FortiExtender devices. After your devices are registered, refresh your FortiExtender Cloud session to update your device list.

For more information, see Step 1: Register and add your devices on page 12.

FortiExtender Cloud automatically pulls your devices from your FortiCare account and lists them in the Inventory page. When you log into FortiExtender Cloud, you can view all your registered FortiExtender devices and select which device to deploy. After you deploy a device, you can push configurations to it and manage it from FortiExtender Cloud.

To find and select a device to deploy:

1. From the navigation bar, go to *Device* > *Inventory*.

   The Inventory page loads, showing all your registered devices.

   Note: If you do not see your devices, log into your FortiCare account at https://support.fortinet.com and make sure your FortiExtender devices are registered. After your devices are registered, refresh your FortiExtender Cloud session to update your device list.
2. From the list of devices, select the device you want to deploy.
3. From the top of the page, click either *Deploy with Profile* or *Deploy with Group*.
4. Select the Profile or Group you want, and then click *Apply*.

   The system deploys your device and consumes a license. During the deployment process, FortiExtender Cloud moves the device from the Inventory page to In Service page, and begins applying your configurations.

You can see the current state of your devices in the In Service page. All devices fall into one of the following states:

- *Deploying*: The device is in the process of being deployed.
- *Deployed*: The device is fully installed and synced with the firmware configurations from FortiExtender Cloud.
- *Syncing*: The device is currently syncing its configurations with FortiExtender Cloud. The device will reboot during the syncing process.

Step 5: Synchronize and install your device

After you deploy your device in FortiExtender Cloud, you must synchronize the configurations from FortiExtender Cloud to the physical device.

To synchronize device configurations:

1. Ensure the FortiExtender device is assembled and set up according to the QuickStart Guide.
2. Connect the FortiExtender device to the internet using its Ethernet port.

   This triggers zero-touch provision (ZTP), enabling the device to synchronize with its assigned profile from FortiExtender Cloud.
3. When the device state changes from deploying to deployed, the device is fully synchronized.

   The deployment process causes the device to reboot.
4. Disconnect the device and install it on-site.

   After the device is connected and activated, it will provide cellular internet access over its Ethernet port, enabling it to be managed from FortiExtender Cloud.

   When installing your device on-site, place the device near windows and away from metal and solid objects to reduce signal obstructions.

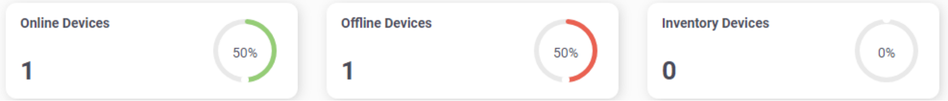
The Dashboard

The Dashboard is the default home page of FortiExtender Cloud and has multiple widgets that provide an overview of your FortiExtender's data usage.

The Dashboard contains the following widgets:

Device summary

The top of the Dashboard page shows the number of devices under each availability status.



Online Devices 50% 1

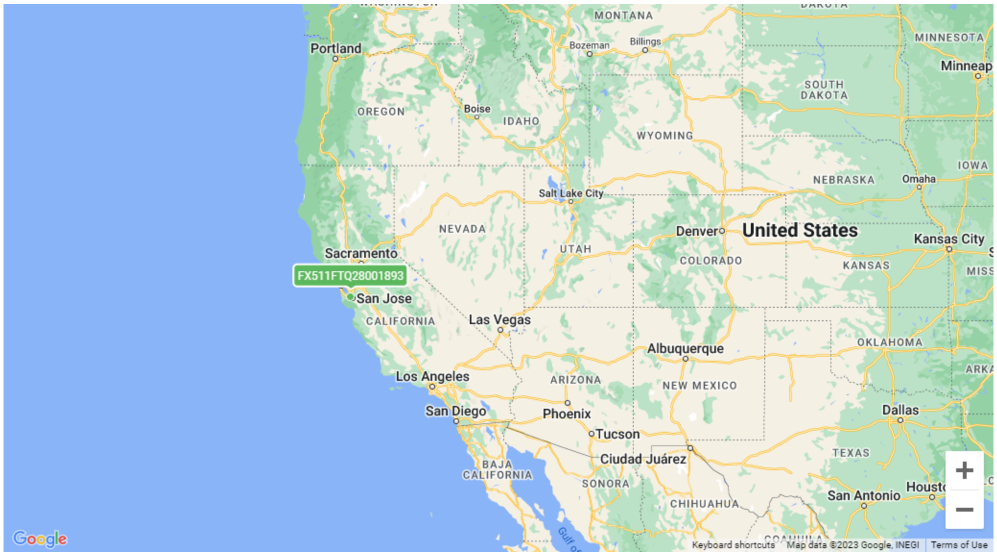
Offline Devices 50% 1

Inventory Devices 0% 0

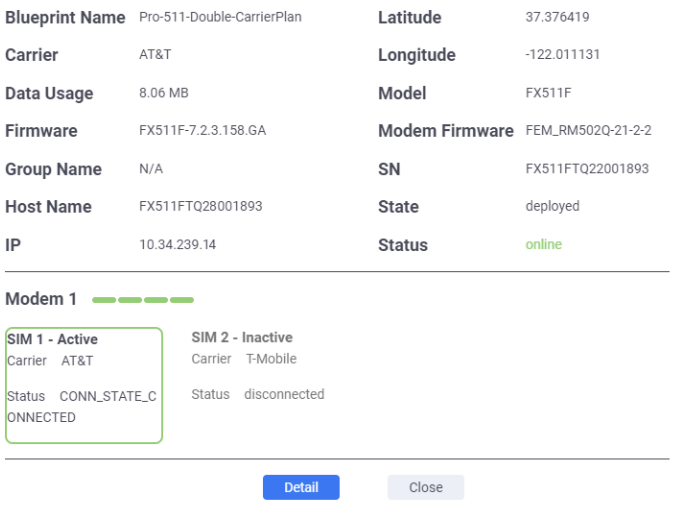
Device Status	Description
Online Devices	The device is connected to FortiExtender Cloud.
Offline Devices	The device is deployed but not connected to FortiExtender Cloud.
Inventory Devices	The device is registered in FortiCare but not deployed in FortiExtender Cloud.

Device map

The Device map page shows a world map that has the locations of your deployed devices plotted via their GPS coordinates. For devices that are offline, the map logs the last known GPS location.



When multiple devices are located in the same location, they are clustered under one location marker with a green and red ring denoting the ratio of online and offline devices. You can click on the location markers to see more information about the device.



Blueprint Name	Pro-511-Double-CarrierPlan	**Latitude**	37.376419
Carrier	AT&T	**Longitude**	-122.011131
Data Usage	8.06 MB	**Model**	FX511F
Firmware	FX511F-7.2.3.158.GA	**Modem Firmware**	FEM_RM502Q-21-2-2
Group Name	N/A	**SN**	FX511FTQ22001893
Host Name	FX511FTQ28001893	**State**	deployed
IP	10.34.239.14	**Status**	online

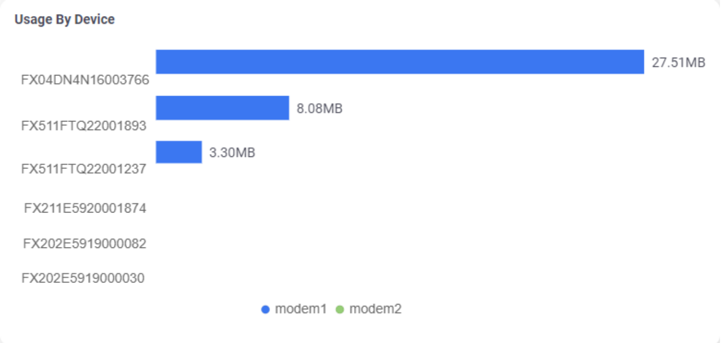
Modem 1

SIM 1 - Active	**SIM 2 - Inactive**
Carrier AT&T	Carrier T-Mobile
Status CONN_STATE_CONNECTED	Status disconnected

To go directly to that device's detail page, click *Detail*.

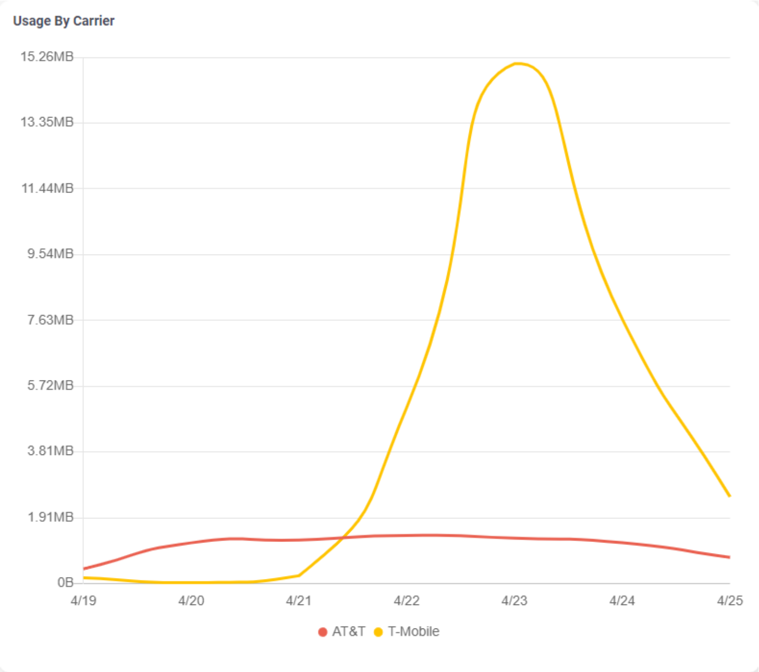
Usage by Device

This bar graph shows the top 10 devices that have consumed the most data in terms of MB.



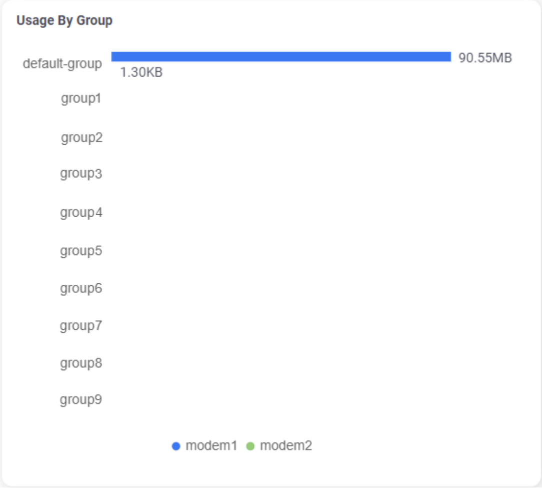
Usage by Carrier

This line graph shows the amount of data used by each carrier over time. Hold the pointer over a specific day to see the exact amount of data used by each carrier on that day.



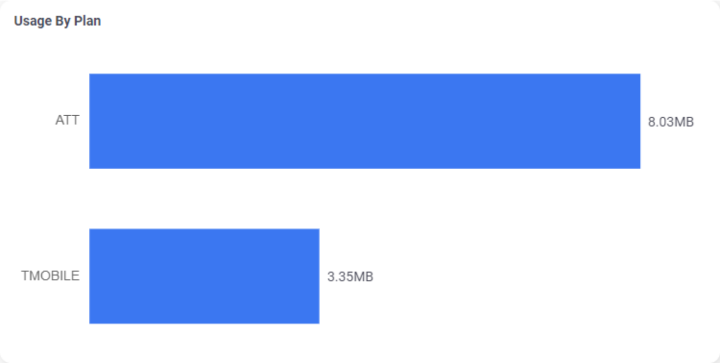
Usage by Group

This bar graph shows the amount of data used by the devices in each device group.



Usage by Plan

This bar graph shows the amount of data used by each plan.


Usage By Plan
ATT
8.03MB
TMOBILE
3.35MB

Manage profiles

Profiles are templates that contain general configuration settings and carrier plans that can be applied to multiple devices. All devices must be associated with a profile before they can be deployed.

The Profile page lets you:

- Create profiles
- View and modify profile configurations
- Delete profiles
- Clone an existing profile on page 36

Create profiles

You must create and apply profiles to devices before you can deploy them.

To create a profile:

1. From the Navigation bar, go to *Profile*.
2. Click *Add Profile* to create a new profile.

   The Add Profile window loads.
3. Complete the following fields:

Field Name	Description
Profile Name	Enter a name for the profile. **Note:** Valid characters are: alphanumeric characters and special characters (. -_). Spaces are not permitted.
Hardware Platform	Select the hardware platform/model you want to apply the profile to.

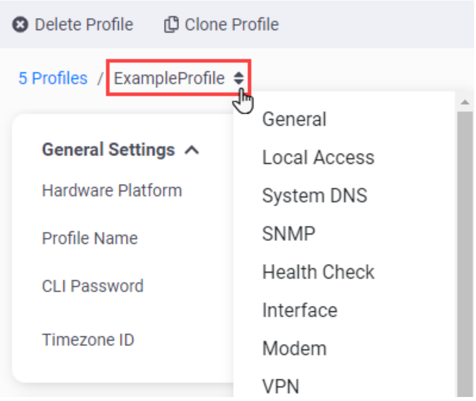
4. Click *Add*.

   The Profile Settings page loads.
5. Make your profile configuration selections. For more information about each configuration option, see Profile configuration fields on page 23.
6. Click *Save* to save the profile.

   The new profile is created. You can return to the Profile page to see it.

Profile configuration fields

The Profile page has multiple fields you can configure. To navigate to each field directly, click the index dropdown list and select which section you want to jump to.



The following sections can be configured:

- General Settings on page 24
- Local Access Settings on page 25
- System DNS Settings on page 25
- SNMP Settings on page 25
- Health Check Settings on page 26
- Interface Settings - lan/loopback/lte1/sfp/wan on page 27
- Interface Settings - Dynamic interfaces on page 30
- Modem1 Settings/Modem2 Settings on page 31
- VPN Settings on page 32
- Carrier Plan Settings on page 32
- DNS Database Plan Settings on page 32
- Credential Plan Settings on page 32
- Services on page 32
- Firewall Settings on page 32
- Static Routing Settings on page 33
- Multicast Routing Settings on page 33
- Policy Routing Settings on page 33
- NTP Settings on page 33
- Firmware Settings on page 34
- SSIDs on page 34
- WiFi-Configuration on page 34
- Radio on page 34

General Settings

Profile Name	Change the profile name if needed.
CLI Username	Enter a username for accessing the device through out-of-band management (OBM). For more information, see OBM Console on page 71.
CLI Password	Enter a password for accessing the device through out-of-band management (OBM). For more information, see OBM Console on page 71.

Work Mode	Select a work mode. • *NAT* — The FortiExtender device works as a gateway of the subnet behind it, forwarding all the traffic between the LAN and LTE WAN. • *IP PASS* — The FortiExtender distributes the WAN IP address provided by the Network Service Provider to the device behind it.
Timezone ID	Select a timezone for your FortiExtenders.

Local Access Settings

http https ssh telnet	FortiExtender and FortiGate share the same LTE IP in WAN-extension mode. To distinguish local services from FortiGate services, you must configure FortiExtender to use different ports. Otherwise, all traffic to these default services will be sent to FortiExtender locally instead of FortiGate.
idle-timeout	Set an idle time.

System DNS Settings

Primary	Input a primary DNS address.
Secondary	Input a secondary DNS address.
Search Order Options	Drag and reorder DNS search order options.

SNMP Settings

Status	Select if you want to Enable or Disable SNMP.
Description	Enter a description for the SNMP setting.
Contact Info	Set the contact info.
Location	Set the location.
Hosts	Click *Add Host* to add a hosts
Name	Enter the host name.
IP	Enter the IPv4 address of the SNMP manager (host), syntax: X.X.X.X/24.
Type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both: • any • query • trap
Communities	Click *Add Community* to add a community. As an SNMP agent, FortiExtender responds to SNMP managers query on v1/v2c and v3 protocol. It supports the SNMP trap events which can be configured in both SNMP community and user events.

	Name	Enter the community name.
	Status	Select if you want to Enable or Disable this SNMP community.
	Queries V Status	Select if you want to Enable or Disable an SNMP v queries
	Queries V Port	Enter an SNMP v query port (default = 161).
	Trap V Status	Select if you want to Enable or Disable an SNMP v traps
	Trap V Local Port	Enter an SNMP v trap local port (default = 162).
	Trap V Remote Port	Enter an SNMP v trap remote port (default = 162).
	Hosts	Select a IPv4 SNMP manager (host).
	Events	Select SNMP trap events.
Users		Click *Add User* to add a user.
	Name	Enter a User name.
	Status	Select if you want to Enable or Disable traps for this SNMP user
	Notify Hosts	Select which SNMP managers to send notifications (traps) to.
	Events	Select SNMP trap events.
	Trap Status	Select if you want to Enable or Disable Trap.
	Trap Local Port	Enter an SNMPv3 local trap port (default = 162).
	Trap Remote Port	Enter an SNMPv3 trap remote port (default = 162)
	Queries Status	Select if you want to Enable or Disable SNMP queries for this user.
	Query Port	Enter an SNMPv3 query port (default = 161).
	Security Level	Select a Security level for message authentication and encryption: • No Authentication No Private • Authentication No Private • Authentication Private

Health Check Settings

Name	Enter a Health Check name.
Interface	Select the outgoing interface to be monitored. Some interfaces, such as loopback, cannot be selected. If you configure a VWAN interface, this interface must be the same as the VWAN member's Target Interface on page 30.
Protocol	Select which protocol to use for status checks: • *ping* — Use PING to test the link with the probe-target. • *http* — Use HTTP-GET to test the link with the probe-target. Adds new field: port, HTTP URL • *dns* — Use DNS-Query to test the link with the probe-target

Port	Only available if Protocol is set to *http*. Enter the port number used to communicate with the server
HTTL URL	Only available if Protocol is set to *http*. Enter the URL used to communicate with the server.
Interval	Enter the monitoring interval in seconds.
Probe Count	Enter the number of probes sent within an interval.
Probe Timeout	Enter the timeout for a probe in seconds.
Probe Target	Enter the target (ipv4-address) to which a probe is sent.
Source Type	The way to set the source address for probes. • *none* — Do not set the source address. • *interface* — Set the source address as the address derived from a specific interface. • *ip* — Set the source address as a specific IP.

Interface Settings - lan/loopback/lte1/sfp/wan

Add Interface	(Optional) Click *Add Interfaces* to add a dynamic interface to the Profile. See Interface Settings - Dynamic interfaces on page 30.
Status	Select the status you want for your interface: • Up • Down
Mode	Select the interface IP addressing mode: • *dhcp* — FortiExtender will work in DHCP client mode. • *static* — FortiExtender will use a fixed IP address to connect to the Internet.
Allowaccess	Select the types of management traffic allowed to access the interface: • http • ssh • telnet • snmp • https • ping • capwap
Override MTU	Select if you want to be able to override the MTU value.
STP	Select enable to activate Spanning Tree Protocol (STP) for the built-in LAN Switch on applicable FortiExtender models.
MTU	Enter the interface's MTU value for the interface.
Distance	Enter the route metric of the interface gateway.
Virtual Wire Pair	When the Work Mode is IP PASS, you can configure the Virtual Wan Interface of a particular port to FortiGate.

VRRP Setting	Add and configure VRRP settings. • *Backup* — Select enable to configure the device's `fortigate-backup.vrrp-interface` and `fortigate-backup.status`. • *Status* — Select enable to activate the VRRP. • *Mode* — Select how you want to assign an IP. ◦ plan: FortiExtender Cloud automatically assigns the `vrrp_setting.virtual_router_ip` based on your network plan. ◦ manual: Manually enter the `virtual_router_ip`.
DNS Server Setting	Add and configure DNS Server settings. • *Name* — Enter the name of the DNS Server. • *Mode* — Select the DNS server mode, which can be one of the following: ◦ recursive: Is for the shadow DNS database and forward. In this mode, FortiExtender looks up the local shadow DNS database first. If no DNS RR (resource record) is found, the DNS request will be forwarded to the configured system DNS server. ◦ non-recursive: Is for the public DNS database only. In this mode, FortiExtender only looks up the local public DNS database. If no DNS RR (resource record) is found, it will reply with an error status of NXDOMAIN. ◦ forward-only: Is for forwarding to the system DNS server only. In this mode, FortiExtender will forward DNS requests directly to the configured system DNS servers.
PPPoE Interface Setting	Add and configure a Point-to-Point Protocol over Ethernet (PPPoE) Interface. This is only supported on FEX311F and FEX511F models. • *Name* — Enter the name of the PPPoE interface. • *Status* — Select if you want to bring the PPPoE up or down. • *Username* — Enter the username of the PPPoE account, this is provided by the ISP. • *Password* — Enter the password of the PPPoE account.
SFP DSL Setting	Add and configure DSL configuration in SFP interface settings. This is only supported on FEX311F and FEX511F models. • *Status* — Enable or Disable the use of vdsl or adsl for SFP. • *Physical Mode* — Select the DSL physical mode you want to use, vdsl or adsl. • *Auto Detect* — Enable or Disable sfp-dsl autodetect. ◦ If you disable *Auto Detect*, you must enter the MAC address of the sfp-dsl module. If you set the Physical Mode as *adsl*, you can configure the following options: • *Virtual Path Identifier (vpi)* — SFP-DSL ADSL Fallback virtual path identifier. • *Virtual Channel Identifier (vci)* — SFP-DSL ADSL Fallback virtual channel identifier • *Multiplexer Type* — SFP-DSL ADSL Fallback Multiplexer type. • *PVC VLAN Id* — SFP-DSL ADSL Fallback Permanent Virtual Circuit VLAN ID. • *PVC VLAN TX Id* — SFP-DSL ADSL Fallback PVC VLAN ID tx. • *PVC VLAN RX Id* —SFP-DSL ADSL Fallback PVC VLAN ID rx. • *PVC VLAN TX Op* —SFP-DSL ADSL Fallback PVC VLAN TX op.

	• *PVC VLAN RX Op* —SFP-DSL ADSL Fallback PVC VLAN RX op • *PVC CRC* —SFP-DSL ADSL Fallback PVC CRC option (bit0 = sar LLC preserve, bit1 = ream LLC preserve, bit2 = ream VC-MUX has crc). • *PVC ATM QoS* —SFP-DSL ADSL Fallback PVC ATM QoS. • *PVC Packet Cell Rate* —SFP-DSL ADSL Fallback PVC packet cell rate (0 - 5500 cells per second, default = 0). • *PVC Sustainable Cell Rate* —SFP-DSL ADSL Fallback PVC sustainable cell rate (0 - 5500 cells per second, default = 0).
Network Plan	Select which network plan you want to apply to the interface. Devices associated with this profile will be automatically assigned a subnet based on the network plan. A default subnet 192.168.2.0/24 will be assigned for all devices if no network plan is selected.
DHCP Setting	Configure DHCP Server and Relay settings.
Server Setting	Add and configure a DHCP server for other clients to obtain an IP. • *Name* — Specify the name of the DHCP server. • *Status* — Select if you want to enable, disable, or set the DHCP server status to backup. • *Mode* — Select if you want to use information from the Network plan or if you want to manually input the information. • *Lease Time* — Specify the DHCP address lease time in seconds. The valid range is 300–8640000. 0 means unlimited. • *MTU* — Enter the interface's MTU value • *NTP Service* — The NTP service is automatically set to *specify*. • *NTP Server 1-3* — Specify the IP address of each NTP Server. • *DNS Service* — Select one of the options for assigning a DNS server to DHCP clients. ◦ default: Clients are assigned the FortiExtender configured DNS server. ◦ specify: Specify up to three DNS servers in the DHCP server configuration. ◦ wan-dns: The DNS of the WAN interface that is added becomes clients' DNS server IP address. • *Reserved Addresses* — Add a MAC addresses and select if you want to block or assign it a reserved IP address. ◦ Reserved: Reserve an IP address for the specified client. ◦ Block: Block a specific MAC address.
Relay Setting	When running in static mode, you can configure DHCP relay functionality. • *Name* — Specify the name of the relay setting. • *Status* — Select if you want to enable or disable the relay. • *Server Interface* — Select the server interface. • *Mode* — Select if you want to run in plan or manual mode. • *Server IP* — Enter the server IP. • *Client Interfaces* — Select which interface you want to relay.
Virtual IP Settings	When running in static mode, you can configure how your Virtual IPs direct traffic. • *IP Mapping* — Enter the IP address you want to forward traffic to.

	• *Protocol* — Select which protocol you want to use. • *Port Forward* —Select if you want to enable port forwarding. • *Port* — Enter the port number you want to forward traffic from. • *Port Mapping* — Enter the port number you want to forward traffic to.

Interface Settings - Dynamic interfaces

Virtual-Wan	
	VWAN Interface configurations only apply to devices running FEXTOS 7.4.0 and later.
Name	Specify the name of the VWAN interface.
Status	Select the status you want for your interface: • Up • Down
Algorithm	Select the Load-Balancing algorithm: • *redundant* — Targets work in primary-secondary mode • *WRR* — Targets work in Weighted Round Robin mode. For more information, refer to the FortiExtender (Standalone) Admin Guide.
Redundant By	Only available if Algorithm is set to *redundant*. Redundant algorithm using a VWAN member for data transmission based on: • priority • cost
FEC	Only available if you select *WRR* as the Algorithm. Select a LLB metric to denote how to distribute traffic: • *source_ip* — Traffic from the same source IP is forwarded to the same target. • *dest*_ip — Traffic to the same destination IP is forwarded to the same target. • *source_dest_ip_pair* — Traffic from the same source IP and to the same destination IP is forwarded to the same target. • *connection* — Traffic with the same 5 tuples (i.e., a source IP address/port number, destination IP address/port number and the protocol) is forwarded to the same target
Session Timeout	Specify the session timeout threshold in seconds. The default is 60. This is used to time out a VWAN session. A LLB session is created for each traffic stream. However, when a session times out, it is deleted.
Grace Period	Specify the grace period in seconds to delay fail-back.
Member Setting	Add VWAN members to the VWAN interface.
Name	Specify the name of the VWAN member.
Target Interface	Specify the target to which traffic is forwarded. Must be the same interface as the Interface on page 26.

Priority	Specify the priority of the link member. The lower the value, the higher the priority. The valid value range is 1—7.
Weight	Specify the weight of the member.
Health Check Fail Threshold	Specify the number of consecutive failed probes before the member is considered dead. **Note:** The valid value range is 1—10; the default is 5.
Health Check	Specify a link health check you configured in Health Check Settings.
Link Cost Factor	Select which constraints you want enabled: • *packet-loss* • *latency* • *jitter*
Latency Threshold	Set the Latency Threshold in millisecond.
Jitter Threshold	Set the Jitter Threshold in millisecond.
Packet Loss Threshold	Set the Packet Loss Threshold in percentage.

Modem1 Settings/Modem2 Settings

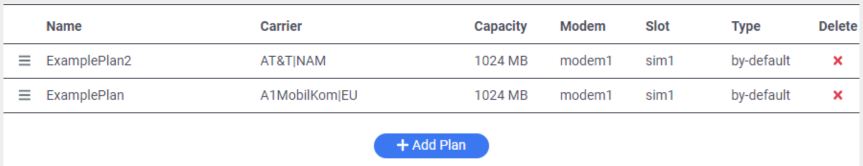
Sim1 PIN	Enter a pin code for your Sim1 card (if applicable).
Sim2 PIN	Enter a pin code for your Sim2 card (if applicable).
Report Interval	Specify a desired report interval in seconds.
Default SIM	If there are two SIM cards, select how you want to define the default SIM card: • *By Carrier* — Select the SIM card with the preferred carrier. You can define the preferred carrier by arranging the order of plans under the Add Plan section in the Profile page. • *By Cost* — Select the SIM card with the lowest Monthly fee. You can specify the Monthly fee from the Carrier plan page. • *SIM 1* — Select the SIM card in the SIM1 slot. • *SIM 2* — Select the SIM card in the SIM2 slot.
Auto Switch	Select which event triggers automatic switching between SIM cards. You can select more than one event: • *Plan Capacity* — Switch when your data plan hits your specified data limit and overage is disabled. You can specify data limit from the Carrier plan page. • *SIM Signal* — Switch when the Received Signal Strength Indicator (RSSI) value drops below -100 for 600 seconds. You can configure the default values from the Carrier plan page. • *SIM Disconnect* — Switch when a SIM card disconnects a certain number of times in a specified time period. ◦ SIM Disconnect Threshold: Enter the number of times a SIM card can disconnect. ◦ SIM Disconnect Period: Enter the time period in seconds. • *Switch Back by Time* — Switch at a certain time of the day.

	◦ Switch Back Time: Enter the time (hh:mm) for when you want to switch SIM cards. • *Switch Back By Period* — Switch after a certain amount of time has elapsed. ◦ Switch Back Period: Enter the time in seconds. **Note:** Automatic switching will not occur if you enable the overage function under Plan configuration and also exceed the specified data limit.

VPN Settings

Add VPN	Add existing VPN plans to your profile.

Carrier Plan Settings

Add Plan	Add existing carrier plans to your profile. **Note:** If you select the By Carrier option for defining a Default SIM, you can define the preferred carrier by dragging and rearranging the Plans in this section. Plans are prioritized based on their order, with the top plan being the most preferred. 

	Name	Carrier	Capacity	Modem	Slot	Type	Delete
☰	ExamplePlan2	AT&T|NAM	1024 MB	modem1	sim1	by-default	✕
☰	ExamplePlan	A1MobilKom|EU	1024 MB	modem1	sim1	by-default	✕

DNS Database Plan Settings

Add DNS Database Plan	Add existing DNS plans to your profile.

Credential Plan Settings

Add Credential	Add existing credential plans to your profile.

Services

Edit Services	Edit the services and ports associated with the profile.

Firewall Settings

Mode	Select a mode type: • *manual* — Manually configure firewall policies. Note: FortiExtender Cloud only includes a base all-pass policy, all other policies need to be manually entered. • *plan* — FortiExtender Cloud automatically assigns default policies based on the VPN plan's Phase 1 name, Phase 2 Source/Destination subnets and the Interface plan's IP addresses.

Policies	If you select the manual mode type, you can add up to 96 firewall policies to your profile. **Note**: You must define two ACCEPT firewall polices to permit communications between the source and destination addresses.

Static Routing Settings

Name	Enter the name of the static route.
Interface	Select the interface type.
Gateway	Enter the IP address of the gateway.
Status	Set the status of the static route: • *enable* — Enable the static route. • *disable* — Disable the static route.
Destination Subnet	Specify the destination IP address and netmask of the static route.
Distance	Specify the administrative distance. The range is 1–255.

Multicast Routing Settings

Join Prune Interval	Set the period of time between sending periodic PIM join/prune messages in seconds.
Hello Interval	Set the period of time between sending PIM hello messages in seconds.
PIM Interface	Select a PIM Interface type: • lan • lte1 • loopback • wan
RP Address	Click *Add RP Address* and enter the following: • *Name* —Enter the name for the Rendezvous Point (RP) address. • *Group* —Enter the groups to use this RP. • *Address* — Enter the RP router address.

Policy Routing Settings

Mode	Select a mode type: • *manual* — Manually configure routing policies. • *plan* — FortiExtender Cloud automatically assigns default policies based on the VPN plan's Phase 1 name, Phase 2 Source/Destination subnets and the Interface plan's IP addresses.
Policy Routes	You can add up to 20 policy routes.

NTP Settings

Type	Select a Network Time Protocol (NTP) server to use:

	• *fortiguard* • *custom* ○ Enter the Name of your custom NTP server. ○ Enter the IP address or hostname of the custom NTP server.

Firmware Settings

OS Firmware	Select or upload the OS firmware you want to apply to each FortiExtender model associated with this profile.
Modem Firmware	Select the modem firmware you want to apply to each FortiExtender model associated with this profile.

SSIDs

Add SSIDs	Add SSIDs to the profile.
ID	Enter an ID or name for the SSID plan.
SSID	Enter the name you want your SSID to show during broadcast.
Broadcast SSID	Select if you want to broadcast the SSID.
Wlan Members	Enter the WLAN members.
Security Mode	Set the security encryption mode of the SSID.
Passphrase	Enter a password for the SSID.

WiFi-Configuration

Add WiFi-Config	Add Wi-Fi Configurations to the profile.
ID	Enter an ID or name for the Configuration plan.
SSID	Enter the name of an SSID.
Security Mode	Set the security mode of the SSID.
Passphrase	Enter a passphrase for the SSID.
Country Code	Set a country code.

Radio

Add Radio	Add Radio configurations to the profile.
ID	Enter an ID or name for the Radio plan.
Role	Set the Radio role: • lan • wan

Band	Select the frequency band you want to broadcast: • 2GHz • 5GHz
Bandwidth	Select the channel width you want to broadcast: • auto • 20MHz • 40MHz
Channel	Select the channel or channels to include.
Status	Set the status of the radio: • enable • disable
Extension Channel	Select the radio extension channel: • auto • higher • lower
Guard Interval	Select the radio guard interval: • auto • 800ns • 400ns
Operating Standards	Select the radio operating standards.
Power Mode	Set the power mode for your radio: • auto • percentage • dBm
VAP	Select the Virtual APs you want to apply radio configurations to.

View and modify profile configurations

After you create a profile, you can view the profile's configurations and modify them if necessary. You can also see which devices or groups your profile is applied to.

To modify a profile's configurations:

1. In the navigation bar, click *Profile*.
   The Profile page loads.
2. In the list of profiles, locate and click the profile you want to view.
   The Profile Settings page loads, letting you see and modify the profile's configurations.
3. Click *Save* to confirm your changes.
   FortiExtender Cloud saves the profile changes.

1. Modifying a profile causes the devices associated with it to reboot.

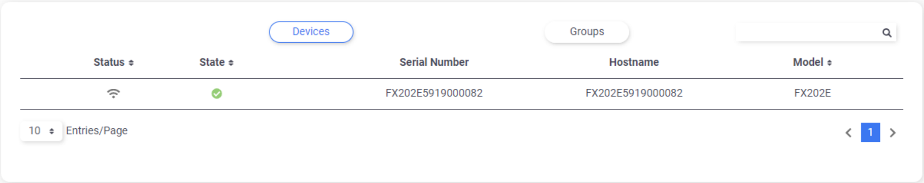
Delete profiles

FortiExtender Cloud lets you delete profiles you no longer need.

You cannot delete profiles that are associated with a device or group. You must first reassign each device or group to a new profile before you can delete the old profile (for more information, see Change a device's profile on page 64 and Change a group's profile on page 41).

To delete a profile:

1. In the navigation bar, click *Profile*.
   The Profile page loads.
2. In the list of profiles, locate and click the profile you want to delete.
   The Profile General Settings page loads.
3. At the bottom of the page, check to ensure there are no devices or groups associated with the profile.



Status ⇕	State ⇕	Serial Number	Hostname	Model ⇕
ᯤ	✓	FX202E5919000082	FX202E5919000082	FX202E

   If there are devices or groups associated with the profile, you must reassign each device/group to a new profile. You cannot delete a profile until all affected devices/groups have a new profile (for more information, see Change a device's profile on page 64 and Change a group's profile on page 41).
4. In the upper-left of the page, click *Delete Profile*.
   A Confirm Profile Deletion window loads.
5. Click *Yes*.
   FortiExtender Cloud deletes the profile.

Clone an existing profile

After you create a profile, you can clone the profile to make multiple identical profiles, and then adjust the configuration settings as needed.

To clone an existing profile:

1. In the navigation bar, click *Profile*.
   The Profile page loads.
2. In the list of profiles, locate and click the profile you want to clone.
   The Profile Settings page loads.
3. Click *Clone Profile*.
   The Clone Profile window loads.
4. Enter a name for the new profile, and then click *Clone*.
   FortiExtender Cloud clones the profile.
5. Click *Close* to finish.
   You can find the newly cloned profile in the Profile page.

Virtual IPs

Virtual IP (VIP) can be used to implement Destination Network Address Translation (DNAT), which is used to map an external IP address to an IP address. This address does not have to be an individual host, it can also be an address range. This mapping can include all TCP/UDP ports or, if Port Forwarding is enabled, it only refers to the configured ports. Because, the Central NAT table is disabled by default, the term Virtual IP address or VIP is predominantly used.

You can configure VIPs from FortiExtender Cloud profiles under Interface Settings (see Create profiles on page 23).

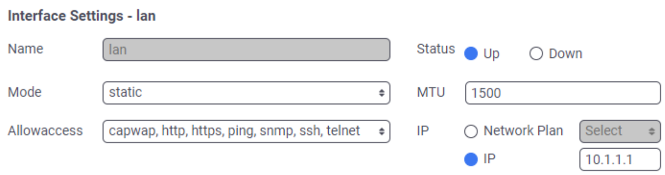
FortiExtender only supports static NAT, and does not support mapping of an address range or port range.

The external or public IP addresses must be configured on FortiExtender because FortiExtender does not support the ARP-Reply function which responds to ARP requests for the external address that is not actually configured on FortiExtender.

Configuring DNAT for all protocols and ports on one IP

In the following configuration example, all packets arriving on the FortiExtender with a destination of 10.1.1.1 and port 8081 will depart from the device with a destination of 192.168.200.100 and port 7071.

1. From the navigation bar, click *Profile* and select the profile associated with the FortiExtender you want to configure DNAT for.
2. Under Interface Settings, set the *Mode* to static.
3. In the *IP field*, enter 10.1.1.1.



Interface Settings - lan

Name	lan	Status	● Up ○ Down
Mode	static	MTU	1500
Allowaccess	capwap, http, https, ping, snmp, ssh, telnet	IP	○ Network Plan Select ● IP 10.1.1.1

When you enter an IP address, all interfaces using this profile will receive the same IP. If you select a network plan instead, interfaces will recieve planned IPs that are different for each device. For example, if you set LAN interface IP to 10.1.1.1, every device on the LAN interface will receive an IP of 10.1.1.1. If you select a network plan, each device's LAN interface will receive a different IP assigned by the network plan.

4. Go to the Interface Settings of the interface you want to expose and click + *Virtual IP Settings* to create a VIP.
5. Populate the Virtual IP Settings fields with the following example information:

IP Mapping	192.168.200.100
Protocol	tcp
Port Forward	On
Port	8081
Port Mapping	7071

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

Configuring DNAT for a single port

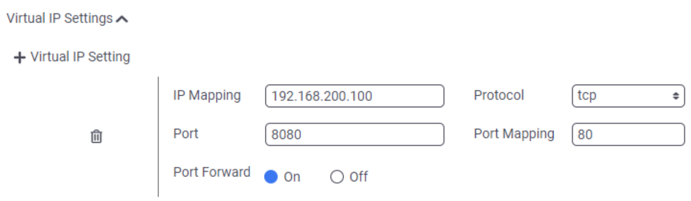
In the following example, all TCP packets arriving on the FortiExtender with a destination of 10.1.1.1:8080 will depart from the device with a destination of 192.168.200.100:80.

You will need a VPN plan before you begin (see Add VPN plans on page 53).

FortiExtender Cloud automatically creates a tunnel interface when you add a VPN setting to a Profile. The tunnel interface name created by FortiExtender Cloud follow the following template: <VPN_name>.phase1.

1. From the navigation bar, click *Profile* and select the profile associated with the FortiExtender you want to configure DNAT for.
2. Under Interface Settings, set the *Mode* to static.
3. In the *IP field*, enter 10.1.1.1.
4. Go to the Interface Settings of the interface you want to expose and click + *Virtual IP Settings* to create a VIP.
5. Populate the Virtual IP Settings field with the following example information:

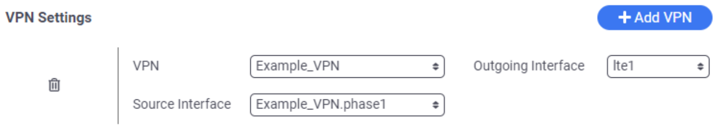
IP Mapping	192.168.200.100
Protocol	tcp
Port Forward	On
Port	8080
Port Mapping	80


Virtual IP Settings

IP Mapping: 192.168.200.100
Protocol: tcp
Port: 8080
Port Mapping: 80
Port Forward: ● On ○ Off

6. Go to *VPN Settings* and click + *Add VPN*.
7. Populate the VPN Settings fields with the following example information:

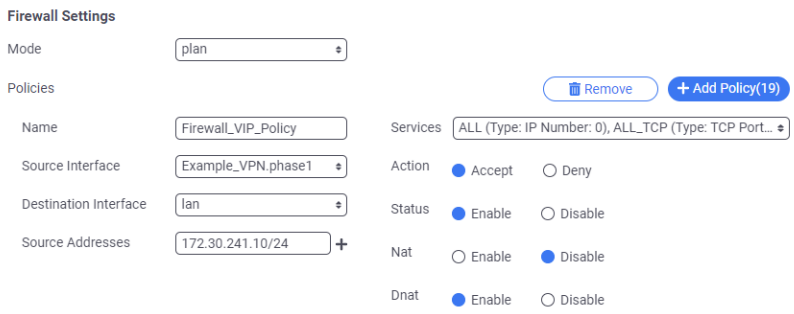
VPN	Enter a VPN plan ("Example_VPN")
Outgoing Interface	lte1
Source Interface	Select the automatically created tunnel interface ("Example_VPN.phase1")


VPN Settings

VPN: Example_VPN
Outgoing Interface: lte1
Source Interface: Example_VPN.phase1

8. Go to *Firewall Settings*, and click + *Add Policy*.
9. Populate the Firewall Settings field with the following example information:

Name	Enter a name for the Firewall policy
Services	Use the default value
Source Interface	Select the tunnel interface from before ("Example_VPN.phase1")
Action	Accept
Destination Interface	lan
Status	Enable
Source Addresses	Enter the IP of the client that is trying to connect to machines behind FortiExtender, for example, 172.30.241.10/24
Nat	Disable
Dnat	Enable


Firewall Settings

Mode: plan

Policies

Name: Firewall_VIP_Policy
Services: ALL (Type: IP Number: 0), ALL_TCP (Type: TCP Port...
Source Interface: Example_VPN.phase1
Action: ● Accept ○ Deny
Destination Interface: lan
Status: ● Enable ○ Disable
Source Addresses: 172.30.241.10/24 +
Nat: ○ Enable ● Disable
Dnat: ● Enable ○ Disable

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

Manage device groups

FortiExtender Cloud lets you sort devices into groups. You can use groups to organize your devices by department, region, data plan, wireless carrier, or in any other category. After grouping them, you can choose to upgrade the firmware for the devices in each group. A device can only be placed into one group at a time and each group must have at least one profile.

The Group page lets you:

- Create groups
- Add a device to a group
- View group details
- Change a group's profile
- Upgrade device firmware by groups
- Export grouped devices
- Delete a group

Create groups

FortiExtender Cloud lets you create groups before you deploy your devices.

To create a group:

1. From the Navigation bar, go to *Group*.
   The Group page loads.
2. Click *Add Group* to create a new group
   The Add Group window loads.
3. Complete the following fields:

Field Name	Description
Group Name	Enter a name for the group. **Note:** Valid characters are: alphanumeric characters and special characters (. -_). Spaces are not permitted.
Profile for Single Modem	Select a profile that applies to devices with a single modem.
Profile for Dual Modem	Select a profile that applies to devices with a dual modem.

4. Click *Apply*.
   The Group Settings page loads.
5. Verify that your group settings are correct.

Add a device to a group

After creating a group, you can add devices to it.

To add a device to a group:

1. In the navigation bar, click *Group*.
   The Group page loads.
2. In the list of groups, click the group that you want to add a device to.
   The Group Detail page loads.
3. At the top of the page, click *Add Devices*.
   The Add devices to group window loads.
4. In the Device SN field, enter the serial number of the device you want to add.
   You can add multiple devices to the group by separating the device serial numbers with a comma.
5. Click *Add*.
   FortiExtender Cloud adds the device to the group.

View group details

You can view information about a group from the Group page. The Group page lists all your groups, displays the number of devices in each group, the profile of each group, and enables you to export a list of devices in each group (see Export grouped devices on page 43). You can also use the search field to search for a specific group.

To view a group's details:

1. In the navigation bar, click *Group*.
   The Group page loads.
   Note: You can search for specific groups by entering the group name into the search field, and then clicking *Search* 🔍.
2. In the list of groups, locate and click the group you want to view.
   The Group Details page loads, displaying all the devices in that group, their status, state, serial number, hostname, and device model. You can see and change the profile for that group (see Change a group's profile on page 41), as well as upgrade the firmware for devices in that group (see Upgrade device firmware by groups on page 42).

Change a group's profile

After you create a group, you can check the group's current profile or profiles, and change them if necessary.

To change a group's profile:

1. In the navigation bar, click *Group*.
   The Group page loads.
2. In the list of groups, click the group you want to change profiles for.
   The Group Detail page loads.
3. Click *Edit Group*.
   The Edit Group window loads.
4. Select the profile you want to apply to the group.
5. Click *Apply*.
   The new profile is applied to the group.

Modifying a group's profile causes the devices associated with the group to reboot.

Upgrade device firmware by groups

You can use groups to organize devices and determine which devices need firmware upgrades. This gives you more insight and control when managing a large number of devices.

To upgrade the firmware for a grouped device:

1. In the navigation bar, click *Group*.
   The Group page loads.
2. In the list of groups, click the group you want to upgrade the device firmware for.
   The Group Detail page loads.
3. From the list of devices in the group, select the checkbox for each device you want to upgrade.
   You can select multiple devices at once.
4. At the top of the page, click *Upgrade*.
   The Upgrade Configuration window loads.
5. Select when you want to apply the upgrade.
   - Now: Upgrade the device now.
   - Scheduled date and time: Select a later time to schedule your upgrade. You can view and edit your scheduled upgrade from the Scheduled Upgrade tab.
6. From the drop-down lists, select which OS or modem firmware you want to upgrade the device to. You can also a upload a firmware file from your local machine.
7. Click *Upgrade*.
   FortiExtender Cloud schedules the upgrades of the selected devices.

Upgrading a device's OS or modem firmware causes the device to reboot.

Export grouped devices

Using the Export Groups option, you can export a list of grouped devices in a CSV file.

To export your grouped devices:

1. In the navigation bar, click *Group*.
   The Group page loads.
2. Click *Export Groups*.
3. Save the CSV file.

Delete a group

FortiExtender Cloud lets you delete groups you no longer need.

⚠ You cannot delete groups that contain devices. You must first remove all the devices before you can delete the group.

To delete a group:

1. In the navigation bar, click *Group*.
   The Group page loads.
2. In the list of groups, locate and click the group you want to delete.
   The Group Detail page loads.
3. Ensure that there are no devices in the group.
   Note: You cannot delete a group until all associated devices are removed from the group.
   - If there are devices in the group, select the checkbox by each device and click *Remove Devices*, and then confirm.
4. At the top of the page, click *Remove Group*.
   A Confirm Group Deletion window loads.
5. Click *Yes.*
   FortiExtender Cloud deletes the group and reloads the Group page.

Manage plans

FortiExtender Cloud consolidates all your plans in the Plans page. From the navigation bar, expand *Plans* to manage your carrier, credential, network, VPN, and DNS Database plans.

- Manage carrier plans on page 44
- Manage credential plans on page 48
- Manage network plans on page 50
- Manage VPN plans on page 53
- Manage DNS Database plans on page 56
- Clone an existing plan on page 59

Manage carrier plans

The FortiExtender Cloud Carrier Plan page lets you create data plans and apply them to profiles and individual devices.

The Carrier Plan page displays information about each plan's carrier company, data capacity, as well as the plan fee and billing date. You can export this information in a CSV file. You can also see which plans have permission to exceed your allotted data limits.

The Carrier Plan page lets you:

- Add carrier plans
- View and modify carrier plan configurations
- Delete carrier plans
- Export carrier plans on page 47

You can manage customized carriers from the Customized Carrier tab (see Manage customized carriers on page 60).

Add carrier plans

FortiExtender Cloud lets you create carrier plans to specify your data provider and the limits of your data plan. After creating a carrier plan, you can add it to a profile to push it onto a device.

Before creating your carrier plan, you must have the following information ready:

- The name of your carrier or data provider
- Your Access Point Name (APN)
- Your authentication type (None, CHAP, PAP)
- Your plan's billing date
- Your plan's total capacity (in MB)
- If your plan is an individual plan or a pooled plan
- Your plan's overage limits (if any)
- Your plan's security mode (NAT or IP PASS)

To add a carrier plan:

1. In the navigation bar, go to *Plan > Carrier*.

   The Carrier Plan page loads.
2. In the upper-left corner of the page, click *Add Carrier Plan*.

   The Add Carrier Plan window loads.
3. In the Plan Name field, enter a plan name.

   Note: Valid characters are: alphanumeric characters and special characters (. -_). Spaces are not permitted.
4. Click *Add*.

   The Carrier Plan Detail page loads.
5. Make the required entries or selections as described in the following table:

Field Name	Description
General Plan Settings	
Plan Name	Enter a name for the carrier plan.
Mode	Select how your modem chooses a wireless network standard: • *AUTO* — Automatically select the wireless network standard. • *AUTO_3G* — Automatically select the wireless network standard with 3G having the highest priority. • *FORCE_2G* — Select the 2G wireless network standard. • *FORCE_3G* — Select the 3G wireless network standard. • *FORCE_LTE* — Select the LTE wireless network standard.
Modem	Select which modems on the device that this plan will be associated with.
Slot	Select which SIM slot you want to apply the plan to.
Type	Select how a plan applies configurations to a SIM: • *By-default* — This plan will apply to any SIM card inserted. • *By-carrier* — This plan will apply to the SIM card with the plan's specified carrier. • *By-slot* — This plan will apply to the SIM inserted the plan's specified slot. • *By-iccid* — This plan will apply to the SIM card with the provided ICCID. **Note:** Assigning a type only applies to devices running OS 4.2.0 and later.
Carrier Settings	
Type	Select a carrier setting type: • *Built-In* — Select from a list of commonly used mobile phone service carriers. • *Customized* — Lets you add your own carrier. To add your own carrier, click the + *Add New Carrier* button and complete the fields, and then click *APPLY*. You can view all your customized carriers from the Customized Carrier tab (see Manage customized carriers on page 60).
Region	Select the region where your device is to be deployed.
Carrier	If you selected the Built-In type, select your carrier. If you do not find your carrier, you can select "Generic".

Field Name		Description
Authentication Settings		
	APN	Enter the Access Point Name of your plan.
	Type	Select your plan's authentication type: • *CHAP* — Challenge-Handshake Authentication Protocol, authenticated with a unique challenge phrase. • *PAP* — Password Authentication Protocol, authenticated with a static user name and password combination. • *None* — No authentication.
	Username	Enter your username. **Note:** This field is only enabled if you have CHAP or PAP authentication selected.
	Password	Enter your authentication password. **Note:** This field is only enabled if you have CHAP or PAP authentication selected.
Billing Settings		
	Billing Date	Enter the plan's monthly billing date.
	Pooled	Enable if your plan is a group plan.
	Monthly Fee	Enter how much the plan costs per month
	Overage	Enableif you want to allow your plan to exceed its data usage limit. **Note:** Enabling the overage function prevents Smart Switch from automatically switching to the secondary SIM card after the first card hits its data limit
Auto Switch		
	Capacity	Enter your plan's data capacity in MB.
	Signal Threshold	Enter a threshold for an allowable Received Signal Strength Indicator (RSSI) value. If the RSSI value drops below this amount for a specified time period, this can trigger Automatic SIM switching.
	Signal Period	Enter the allowable length of time in seconds in which an RSSI value can drop below the specified threshold. If the RSSI value is below the threshold for more than this time period, this can trigger Automatic SIM switching.

6. Click *Save*.

   The new carrier plan is created. You can return to the Carrier Plan page to see it.

View and modify carrier plan configurations

After you create a carrier plan, you can view the carrier plan's configurations and modify them if necessary. You can also see which devices or profiles your carrier plan is applied to.

To modify a carrier plan's configurations:

1. In the navigation bar, go to *Plan* > *Carrier*.
   The Carrier Plan page loads.
2. In the list of carrier plans, locate and click the plan you want to view.
   The Carrier Plan Detail page loads, letting you see and modify the plan's configurations
3. Click *Save* to confirm your changes.
   A Confirm Plan Changes window loads.
4. Click *Close*.
   FortiExtender Cloud saves the modified plan.

Modifying a carrier plan causes the devices associated with it to reboot.

Delete carrier plans

FortiExtender Cloud lets you delete carrier plans you no longer need.

You cannot delete carrier plans that are associated with a device or profile. You must first reassign each device or profile to a new carrier plan before you can delete the old plan.

To delete a carrier plan:

1. In the navigation bar, go to *Plan* > *Carrier*.
   The Carrier Plan page loads.
2. Click *Remove Carrier Plan*.
   The Remove Carrier Plan window loads.
3. Select the plans you want to delete, and then click *Remove*.
   If you do not see the plan, it means there are profiles or devices associated with it. You must reassign each profile/device to a new plan. You cannot delete a plan until all affected profiles and devices have a new plan. You can check the Affected Devices and Affected Profiles section in the plan's detail page to see which profiles or devices are associated with the plan.
4. To confirm the removal, click *Yes*.
   FortiExtender Cloud deletes the carrier plan and reloads the Carrier Plan page.

Export carrier plans

You can export you carrier plans in a CSV file.

To export your carrier plans:

1. In the navigation bar, click *Plan* > *Carrier*.
   The Carrier Plan page loads.
2. Click *Export*.
3. Save the CSV file.

Manage credential plans

The FortiExtender Cloud Credential Plan page lets you create credential plans to configure device account credentials and apply them to profiles and individual devices. This allows to you add additional users and allow admin access to the CLI and GUI of the FortiExtender if it is reachable on the internet or across the network. You can use credential plans to assign a username, password, and account profile types.

The Credential Plan page displays information about each plan's account profile type.

The Credential Plan page lets you:

- Add credential plans
- View and modify credential plan configurations
- Delete credential plans

Add credential plans

FortiExtender Cloud lets you create credential plans to set a device account profile with username and password permissions. After creating a credential plan, you can apply it to a profile or individual device.

To create a credential plan:

1. In the navigation bar, go to *Plan* > *Credential*.
   The Credential plan page loads.
2. In the upper-left corner of the page, click *Add Credential Plan*.
   The Add Credential Plan window loads.
3. Complete the following fields:

Field Name	Description
Plan Name	Enter a username for accessing FortiExtender devices associated with the credential plan. This allows you to access the device CLI console and local GUI.
Plan Password	Enter a password for accessing FortiExtender devices associated with the credential plan. This allows you to access the device CLI console and local GUI.
AccProfile Type	Select the Account Profile type you want. • *built-in* — Use a pre-built Account Profile. • *customized* — Manually customize the Account Profile.
AccProfile Name	Select the type of access you want to grant to the plan.

Field Name	Description
	If you selected a *built-in* Account Profile type, you can select between: • *no_access* — No access is granted. • *super_admin* — Grant super administrator access. If you selected a *customized* Account profile type, you must select an existing Account Profile name or use the default ACCPROFILENAME and then create a new Account Profile name later.

4. Click *Add*.

   The Credential Plan Detail page loads.

5. Complete the following fields:

Field Name	Description
General Credential Plan Settings	
Credential Plan Name	Change the Credential plan name if necessary. This is the username used for access FortiExtender devices associated with the credential plan.
Password	Change the Credential plan password if necessary. This is the username used for access FortiExtender devices associated with the credential plan.
AccProfile Settings	
AccProfile Type	Change the AccProfile Type if necessary.
AccProfile Name	Change the AccProfile if necessary. If you are using a *customized* AccProfile Type, you can add a new AccProfile or edit the selected AccProfile.
Add/Edit AccProfile	Only available if you are using a *customized* AccProfile Type. Configure the AccProfile permissions for the following: • header • firewall • lte • router • system • snmp • hmon • vpn • network
Trusted Hosts Settings	
Trusted Host 1	Edit the address of your Trusted Hosts. Administrators of the hosts can connect to the FortiExtender device via the IP/network. You can specify any IPv4 address or subnet address and netmask from which an administrator can connect to the FortiExtender. Click *Add Trusted Host* to add more.

6. Click *Save*.

   The new Credential plan is created. You can return to the Credential Plan page to see it.

View and modify credential plan configurations

After you create a credential plan, you can view the credential plan's configurations and modify them if necessary. You can also see which devices or profiles your carrier plan is applied to.

To modify a credential plan's configurations:

1. In the navigation bar, go to *Plan* > *Credential*.
   The Credential Plan page loads.
2. In the list of credential plans, locate and click the plan you want to view.
   The Credential Plan Detail page loads, letting you see and modify the plan's configurations
3. Click *Save* to confirm your changes.
   FortiExtender Cloud saves the modified plan.
4. Click *Close*.

Delete credential plans

You can delete credential plans you no longer need.

> ⚠ You cannot delete credential plans that are associated with a device or profile. You must first reassign each device or profile to a new credential plan before you can delete the old plan.

To delete a credential plan:

1. In the navigation bar, go to *Plan* > *Credential*.
   The credential Plan page loads.
2. In the list of credential plans, locate and click the plan you want to delete.
   The credential Plan Detail page loads.
3. At the bottom of the page, check the Affected Devices and Affected Profiles section to ensure there are no profiles or devices associated with the plan.
   If there are profiles or devices associated with the plan, you must reassign each profile/device to a new plan. You cannot delete a plan until all affected profiles and devices have a new plan.
4. At the top of the page, click *Delete Credential Plan*.
   A Confirm Plan Deletion window loads.
5. Click *Yes.*
   FortiExtender Cloud deletes the credential plan and reloads the Credential Plan page.

Manage network plans

FortiExtender Cloud enables you to define a network and apply it to a device profile. Through Network Plans, you can choose if you want to use a predefined plan to configure your network, or manually configure your own.

The Network Plan page enables you to:

- Add network plans on page 51
- View and modify network plan configurations on page 52
- Delete network plans on page 52

Add network plans

FortiExtender Cloud lets you create network plans to configure your system interface. After creating a network plan, you can add it to a profile to push it onto a device.

From Network Plans, you can create a subnet pool by using network IP and subnet mask. Each device's interface automatically receives an IP from the subnet pool as long as there are enough subnets.

When you define the Source IP, Source Subnet, and Destination IP, you are defining a network pool with subnets. Subnets are assigned to the device that joins the network. For each subnet, there will be a number of IPs that can be used for the device's hosts.

You must select an integer to define how each subnet device uses those IPs. Once you select an integer and click Save, the reserved index graph updates to visually reflect your selection.

To create a network plan:

1. In the navigation bar, go to *Plan* > *Network*.
   The Network plan page loads.
2. In the upper-left corner of the page, click *Add Network Plan*.
   The Add Network Plan window loads.
3. In the Plan Name field, enter a unique network name.
4. Click *Add*.
   The Network Plan Detail page loads.
5. Complete the following fields:

Field Name	Description
General Settings	
Name	Change the network name if necessary.
Destination IP	Enter the Destination IP of your plan.
Source IP	Enter the Source IP of your plan.
Source Subnet Mask	Select if you want to subnet your plan. If you choose to subnet your plan, select how many.
Interface IP DHCP Server Default Gateway IP DHCP Server Start IP DHCP Server End IP VRRP Virtual Router IP	Select an integer for each IP to define how each subnet device uses those IPs. You can select a customized number from 0-4096. For example, if a device is assigned a subnet from 192.168.2.1/24 to 192.168.2.35/24, choosing **First** means they get an IP of 192.168.2.**1**. **Second** means 192.168.2.**2**, and so on.

6. Click *Save*.

   The new network plan is created. You can return to the Network Plan page to see it.

View and modify network plan configurations

After you create a network plan, you can view the plan's configurations and modify them if necessary. You can also see which devices or profiles your plan is applied to.

To modify a network plan's configurations:

1. In the navigation bar, go to *Plan* > *Network*.

   The Network Plan page loads.
2. In the list of network plans, locate and click the plan you want to view.

   The Network Plan Detail page loads, letting you see and modify the plan's configurations
3. Click *Save* to confirm your changes.

   A Confirm Plan Changes window loads.
4. Click *Close*.

   FortiExtender Cloud saves the modified plan.

Modifying a network plan causes the devices associated with it to reboot.

Delete network plans

You can delete network plans you no longer need.

You cannot delete network plans that are associated with a device or profile. You must first reassign each device or profile to a new network plan before you can delete the old plan.

To delete a network plan:

1. In the navigation bar, go to *Plan* > *Network*.

   The Network Plan page loads.
2. In the list of network plans, locate and click the plan you want to delete.

   The Network Plan Detail page loads.
3. At the bottom of the page, check the Affected Devices and Affected Profiles section to ensure there are no profiles or devices associated with the plan.

   If there are profiles or devices associated with the plan, you must reassign each profile/device to a new plan. You cannot delete a plan until all affected profiles and devices have a new plan.
4. At the top of the page, click *Delete Network Plan*.

   A Confirm Plan Deletion window loads.

5. Click *Yes.*
   FortiExtender Cloud deletes the network plan and reloads the Network Plan page.

Manage VPN plans

FortiExtender uses IPsec VPN to connect branch offices to each other. Currently, only site-to-site VPN tunnel mode is supported. Through VPN Plans, you can choose if you want to use a predefined plan to configure your VPN, or manually configure your own.

FortiExtender Cloud enables you to define a VPN plan and apply it to a device profile.

The VPN Plan page enables you to:

- Add VPN plans on page 53
- View and modify VPN plan configurations on page 55
- Delete VPN plans on page 56

Add VPN plans

FortiExtender Cloud lets you create IPsec VPN plans to connect branch offices to each other. After creating a VPN plan, you can add it to a profile to push it onto a device.

An IPsec VPN is established in two phases: Phase 1 and Phase 2.

Several parameters determine how this is done, except for IP addresses, the settings simply need to match at both VPN gateways.

There are defaults that are applicable for most cases.

When a FortiExtender unit receives a connection request from a remote VPN peer, it uses IPsec Phase-1 parameters to establish a secure connection and authenticate that VPN peer. Then, the FortiExtender unit establishes the tunnel using IPsec Phase-2 parameters. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

To support these functions, the following general configuration steps must be performed on both units:

- Define the Phase-1 parameters that the FortiExtender unit needs to authenticate the remote peer and establish a secure connection.
- Define the Phase-2 parameters that the FortiExtender unit needs to create a VPN tunnel with the remote peer.
- Create firewall policies to control the permitted services and permitted direction of traffic between the IP source and destination addresses. See Create profiles on page 23
- Create a route to direct traffic to the tunnel interface.

To create a VPN plan:

1. In the navigation bar, go to *Plan* > *VPN*.
   The VPN plan page loads.
2. In the upper-left corner of the page, click *Add VPN Plan*.
   The Add VPN Plan window loads.
3. In the Plan Name field, enter a unique VPN plan name.

4. Click *Add*.
   The VPN Plan Detail page loads.
5. Complete the following fields:

Field Name	Description
General Settings	
Name	Change the VPN name if necessary.
Mode	Select which mode you want your VPN plan to run in. • *plan* — The VPN's source subnet destination subnet is automatically assigned based on the interface's network situation. • *manual* — Manually configure the source and destination subnet.
Phase 1	
Name (manual mode)	Enter a name for the Phase 1.
Authentication Method	Select an authentication method. • *psk* — Authenticate using a pre-shared key. • *signature* — Authenticate using a CA certificate. You can upload certificate from the VPN Ca page (see Upload certificates for VPN plans on page 77
Key Life	Specify the time (in seconds) to wait before the Phase-1 encryption key expires. The valid range is 20 –172800.
Ike Version	Specify the IKE protocol version: 1 or 2.
Certificates (signature authentication)	Select a Certificate Authentication that you've uploaded (see Upload certificates for VPN plans on page 77.
PSK-Secret (psk authentication)	Specify the pre-shared secret created when configuring the VPN client.
Proposal	Select a Phase-1 proposal.
Dhgrp	Select one of the following DH groups: • 1 • 2 • 5 • 14
Type	Select a remote gateway type: • static • ddns
Remote Gateway	Specify the IPv4 address of the remote gateway’s external interface.
Phase 2	
Name (manual mode)	Enter a name for the Phase 2.
Proposal	Select a Phase-2 proposal.

Field Name	Description
PFS	Enable or Disable PFS.
Source Subnet (manual mode)	Enter the local proxy ID subnet.
Source Subnet Port	Enter the quick mode source port. Note: The valid range is 1—65535. 0 means for all.
Destination Subnet (manual mode)	Enter the remote proxy ID subnet.
Destination Subnet Port	Enter the quick mode destination port. **Note**: The valid range is 1—65535. 0 means for all.
Key Life Type	Select how you want to define the key life type: • seconds • kbs
Encapsulation	Select the ESP encapsulation mode: • tunnel-mode • transport-mode
Key Life Seconds	Define the Phase-2 key life time in seconds. **Note**: The valid range is 120—172800.
Protocol	Quick mode protocol selector. **Note**: The valid range is 1—255. 0 means for all.
Key Life Kbs	Define the Phase-2 key life time in Kbs.
Add Phase	You can add up to 10 phases as needed.

6. Click *Save*.
   The new VPN plan is created. You can return to the VPN Plan page to see it.

View and modify VPN plan configurations

After you create a VPN plan, you can view the plan's configurations and modify them if necessary. You can also see which devices or profiles your plan is applied to.

To modify a VPN plan's configurations:

1. In the navigation bar, go to *Plan* > *VPN*.
   The VPN Plan page loads.
2. In the list of VPN plans, locate and click the plan you want to view.
   The VPN Plan Detail page loads, letting you see and modify the plan's configurations
3. Click *Save* to confirm your changes.
   A Confirm Plan Changes window loads.

4. Click *Close*.

   FortiExtender Cloud saves the modified plan.

Modifying a VPN plan causes the devices associated with it to reboot.

Delete VPN plans

You can delete VPN plans you no longer need.

You cannot delete VPN plans that are associated with a device or profile. You must first reassign each device or profile to a new VPN plan before you can delete the old plan.

To delete a VPN plan:

1. In the navigation bar, go to *Plan* > *VPN*.

   The VPN Plan page loads.
2. In the list of VPN plans, locate and click the plan you want to delete.

   The VPN Plan Detail page loads.
3. At the bottom of the page, check the Affected Devices and Affected Profiles section to ensure there are no profiles or devices associated with the plan.

   If there are profiles or devices associated with the plan, you must reassign each profile/device to a new plan. You cannot delete a plan until all affected profiles and devices have a new plan.
4. At the top of the page, click *Delete VPN Plan*.

   A Confirm Plan Deletion window loads.
5. Click *Yes.*

   FortiExtender Cloud deletes the VPN plan and reloads the VPN Plan page.

Manage DNS Database plans

The FortiExtender Cloud DNS Database Plan page lets you create DNS Database plans to configure a FortiExtender as a DNS server. For more information about configuring FortiExtenders as DNS servers, refer to DNS Service in the FortiExtender Admin Guide (Standalone).

The DNS Database Plan page lets you:

- Add DNS Database plan
- View and modify DNS Database plan configurations
- Delete DNS Database plans

Add DNS Database plan

FortiExtender Cloud lets you create DNS Database plans to configure your FortiExtender as a DNS server. After creating a DNS Database plan, you can apply it to a profile or individual device.

To create a DNS Database plan:

1. In the navigation bar, go to *Plan* > *DNS Database*.
   The DNS Database plan page loads.
2. In the upper-left corner of the page, click *Add DNS Database Plan*.
   The Add DNS Plan window loads.
3. Complete the following fields:

Field Name	Description
Zone Name	Enter a unique zone name.
Domain Name	Enter the name of the domain.

4. Click *Add*.
   The DNS Database Plan Detail page loads.
5. Complete the following fields:

Field Name	Description
General Settings	
Zone Name	Change the zone name if necessary.
Domain Name	Change the domain name if necessary.
Authoritative	Select the status of the authoritative zone.
Status	Select the status of the DNS zone.
Contact (Host Name)	Enter the email address of the zone administrator. You can specify either the username (e.g., admin) or the full email address (e.g., admin@test.com). When using a simple username, the domain of the email will be this zone.
Primary Name	Enter the domain name of the default DNS server for this zone.
Source IP	Enter the source IP for forwarding to the DNS server.
Zone Type	Select the DNS zone to manage entries directly.
Zone View	Select the zone view: • shadow: Shadow DNS zone to serve internal clients. • public: Public DNS zone to serve public clients.
TTL	Enter the time-to-live value for the entries of this DNS zone. Note: The value ranges from 0 to 2147483647. The default is 86400.
Forwarder Settings	
Forwarder	Click *Add Forwarder* to enter the DNS zone forwarder IP address.

Field Name			Description
DNS Entries			
	DNS Entry		Click *Add DNS Entry* to add a DNS Entry.
		Hostname	Name of the host.
		TTL	Time-to-live for this entry.
		Type	Resource record type: • A — Host type. • NS — Name server type • CNAME — Canonical name type • MX — Mail exchange type • PTR — Pointer type
		Status	Select the resource record status.
		IP	Enter the IPv4 address of the host. **Note:** Applicable to A and PTR(types) only.
		Canonical name	Canonical name of the host. **Note:** Applicable to CNAME (type) only.
		Preference	DNS entry preference, 0 is the highest preference. **Note:** Applicable to MX (type) only.

6. Click *Save*.
   The new DNS Database plan is created. You can return to the DNS Database Plan page to see it.

View and modify DNS Database plan configurations

After you create a DNS Database plan, you can view the plan's configurations and modify them if necessary.

To modify a DNS Database plan's configurations:

1. In the navigation bar, go to *Plan* > *DNS Database*.
   The DNS Database Plan page loads.
2. In the list of DNS Database plans, locate and click the plan you want to view.
   The DNS Database Plan Detail page loads, letting you see and modify the plan's configurations
3. Click *Save* to confirm your changes.
   FortiExtender Cloud saves the modified plan.
4. Click *Close*.

Delete DNS Database plans

You can delete DNS Database plans you no longer need.

You cannot delete plans that are associated with a device or profile. You must first reassign each device or profile to a new plan before you can delete the old plan.

To delete a DNS Database plan:

1. In the navigation bar, go to *Plan* > *DNS Database*.
   The DNS Database Plan page loads.
2. In the list of DNS Database plans, locate and click the plan you want to delete.
   The DNS Database Plan Detail page loads.
3. At the top of the page, click *Delete DNS Database Plan*.
   A Confirm Plan Deletion window loads.
4. Click *Yes.*
   FortiExtender Cloud deletes the DNS Database plan and reloads the DNS Database Plan page.

Clone an existing plan

After you create a carrier, network, or VPN plan, you can clone the plan to make multiple identical plans, and then adjust the configuration settings as needed.

To clone an existing plan:

1. From the navigation bar, navigate to the Plan type you want to clone (*Plan* > *Carrier/Network/VPN*).
   The Plan page for the respective plan type loads.
2. In the list of plans, locate and click the plan you want to clone.
   The Plan Settings page loads.
3. Click *Clone Carrier/Network/VPN Plan* .
   The Clone Plan window loads.
4. Enter a name for the new plan, and then click *Clone*.
   FortiExtender Cloud clones the plan.
5. Click *Close* to finish.
   You can find the newly cloned plan in its respective Plan page.

Manage customized carriers

The Customized Carrier page lists all the custom carriers you have created for ease of management. You can also create new customized carriers directly from this page.

To create a Customized Carrier:

1. In the navigation bar, go to *Customized Carrier*.
   The Customized Carrier page loads.
2. In the upper-left corner of the page, click *Add Customized Carrier*.
   The Add Carrier Plan window loads.
3. Make the required entries or selections as described in the following table:

Field Name	Description
Name	Enter a name for the custom carrier.
MCC	Enter the Mobile Country Code for the carrier.
MNC	Enter the Mobile Network Code for the carrier.
Region	Select the region for the carrier.
Country	Enter the country for the carrier.
Modem Firmware Version	Select the modem firmware on the device that this carrier will be associated with.

4. Click *Save*.
   The new custom carrier is created. You can return to the Customized Carrier page to see it.

Manage devices

FortiExtender Cloud enables you to manage all your devices from the Device section. Undeployed devices are listed in the Inventory page while deployed devices are listed in the In Service page.

From the In Service page, you can see your device's availability status, deployment state, signal strength, and manage your device configurations. Through the In Service page, you can change your device groups and profiles, modify individual device configurations, undeploy active devices, and sync device configurations with the cloud.

From the In Service page, you can:

- View your devices
- Change a device's profile
- Change a device's group
- Undeploy devices
- Remove a device
- Upgrade OS and modem firmware
- Edit a device's configuration
- Sync devices
- Export device information
- Monitor and manage a deployed device

From the Inventory page, you can:

- Deploy FortiExtenders on page 63

View your devices

The In Service page and Inventory page contains all the FortiExtender devices associated with your account.

In Service devices

The In Service page contains FortiExtenders that have been deployed, but not necessarily fully installed or synced.

To access the In Service page:

1. From the navigation bar, go to *Device* > *In Service*.
   The In Service page loads with all your deployed devices.

These devices are categorized into the following states:

Device States	Description
🔄 Deploying	The device is in the process of being deployed.

Device States	Description
✓ Deployed	The device is fully installed and synced with the firmware configurations from FortiExtender Cloud.
○ Syncing	The device is currently syncing its configurations with FortiExtender Cloud. The device will reboot during the syncing process.

You can use *Filters* to filter your deployed devices by their availability status, device state, carrier, model, profile, group, modem version, and OS version.

Under the Signal Strength column, you can view the relative signal strength of each device.

Signal Strength Icons	Description
📶 📶	Good signal strength.
📶 📶	Low signal strength.
📶	No signal strength.
🟥	No SIM card detected.

Under the Data Usage column, you can see the amount of data used by each device over the past month.

Under the OnlineIP column, you can see the IP address of the FortiExtender. If the FortiExtender has more than one modem, it will show the IP for each modem.

Inventory devices

The Inventory page contains FortiExtenders that are registered in FortiCare, but not yet deployed.

To access the Inventory page:

1. From the navigation bar, go to *Device* > *Inventory*.
   The Inventory page loads with all your undeployed devices.

From the Inventory page, you can see when your devices were first shipped out, when they were registered, and how they were registered.

Adding devices

You cannot add devices into FortiExtender Cloud directly. Your registered devices are automatically pulled from your FortiCare account and listed in the Inventory page.

If you do not see your devices in the Inventory page, log into your FortiCare account at https://support.fortinet.com and go to *Asset* > *Register/Activate* to register your FortiExtender devices. After your devices are registered, refresh your FortiExtender Cloud session to update your device list.

For more information, see Step 1: Register and add your devices on page 12.

Deploy FortiExtenders

Adding devices

You cannot add devices into FortiExtender Cloud directly. Your registered devices are automatically pulled from your FortiCare account and listed in the Inventory page.

If you do not see your devices in the Inventory page, log into your FortiCare account at https://support.fortinet.com and go to *Asset* > *Register/Activate* to register your FortiExtender devices. After your devices are registered, refresh your FortiExtender Cloud session to update your device list.

For more information, see Step 1: Register and add your devices on page 12.

FortiExtender Cloud automatically pulls your devices from your FortiCare account and lists them in the Inventory page. When you log into FortiExtender Cloud, you can view all your registered FortiExtender devices and select which device to deploy. After you deploy a device, you can push configurations to it and manage it from FortiExtender Cloud.

- You can deploy FortiExtenders with settings pre-configured from a Profile or Group.
- You can also choose to deploy a FortiExtender as a replacement device. This applies the exact configurations from the existing device to the one you are trying to deploy, and then automatically undeploys the existing device.

To find and select a device to deploy:

1. From the navigation bar, go to *Device* > *Inventory*.

   The Inventory page loads, showing all your registered devices.

   Note: If you do not see your devices, log into your FortiCare account at https://support.fortinet.com and make sure your FortiExtender devices are registered. After your devices are registered, refresh your FortiExtender Cloud session to update your device list.
2. From the list of devices, select the device you want to deploy.
3. From the top of the page, click either *Deploy with Profile*, *Deploy with Group*, or *Deploy as Replacement*.
4. Select the Profile, Group, or individual device you want to apply configurations from, and then click *Apply*.

   The system deploys your device and consumes a license. During the deployment process, FortiExtender Cloud moves the device from the Inventory page to In Service page, and begins applying your configurations.

You can see the current state of your devices in the In Service page. All devices fall into one of the following states:

- *Deploying*: The device is in the process of being deployed.
- *Deployed*: The device is fully installed and synced with the firmware configurations from FortiExtender Cloud.
- *Syncing*: The device is currently syncing its configurations with FortiExtender Cloud. The device will reboot during the syncing process.

Change a device's profile

The In Service page lets you change the profile of deployed devices.

To change a device's profile:

1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, locate the device that you want to change profiles for.
3. Select the checkbox for your device, and click *Swap Profile*.

   You can select multiple checkboxes to change the profile of multiple devices.

   The Swap Profile window loads.
4. From the list of profiles, select the profile you want to swap to, and click *Apply*.
   FortiExtender Cloud applies the new profile to the device.

   Changing a device's profile causes the device to reboot.

Change a device's group

The In Service page lets you change the group of deployed devices.

To change a device's group:

1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, locate the device that you want to change groups for.
3. Check the checkbox for your device, and click *Re-Group*.

You can select multiple checkboxes to change the group of multiple devices.

The Re-Group window loads.

4. From the list of groups, select the group you want to change to, and click *Apply*.
   A Confirm Discard Profile window loads, asking if you want to keep or discard the existing device's profile.
5. Select the profile option you want for your device.
   - *Keep* — Keep your device's current profile.
   - *Discard* — Discard your device's current profile and apply the profile from the selected group.

Device profiles are given precedence over group profiles.

FortiExtender Cloud assigns your device to the new group.

Modifying a device's group causes the devices associated with it to reboot.

Undeploy devices

When a device is no longer needed, you can undeploy the device and move it to the Inventory page.

To undeploy a device:

1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, locate the device that you want to undeploy.
3. Check the checkbox for your selected device, and click *Un-Deploy*.

You can check multiple checkboxes to undeploy multiple devices.

A Confirm Undeployment window loads.

4. Click *Yes*.
   FortiExtender Cloud begins the undeployment process and moves the device to the Inventory page.

Remove a device

You can remove devices from the Inventory page if they were added to FortiExtender Cloud with a Cloud Key. You cannot remove the devices that have been pulled from your FortiCare account. If you have accidentally added a device to the wrong FortiCare account, contact support at https://support.fortinet.com.

To remove a device:

1. From the navigation bar, click *Device* > *Inventory*.
   The Inventory page loads.
2. Locate the device that you want to remove.
3. Check the checkbox for the device, and click *Remove Device*.

   You can select multiple checkboxes to remove multiple devices.

   A Confirm Remove window loads.
4. Click *Yes.*
   FortiExtender Cloud removes the device from your account.

Upgrade OS and modem firmware

Once you deploy a device, you can upgrade the device OS and modem firmware from (1) the In Service page, and (2) from the device's details page. You can also update the OS and modem firmware from the Group page (see Upgrade device firmware by groups on page 42).

To upgrade a device's firmware from the In Service page:

1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, locate the device that you want to upgrade.
   You can select multiple devices at once.
3. Check the checkbox for your selected device, and click *Upgrade*.
   An Upgrade Configuration window loads.
4. Select when you want to apply the upgrade.
   - Now: Upgrade the device now.
   - Scheduled date and time: Select a later time to schedule your upgrade. You can view and edit your scheduled upgrade from the Scheduled Upgrade tab.
5. From the drop-down lists, select which OS or modem firmware you want to upgrade the device to. You can also a upload a firmware file from your local machine.
6. Click *Upgrade*.
   FortiExtender Cloud schedules the upgrades of the selected devices.

Upgrading a device's OS or modem firmware causes the device to reboot.

Edit a device's configuration

After you deploy a device, you can override the set configurations through the Device Detail page. The configurations made directly to an individual device take higher priority over the configurations set by a profile or group.

To edit a device's configuration:

1. From the navigation bar, click *Device* > *In service*.
   The In Service page loads.
2. From the list of deployed devices, click the device that you want to view.
   The Device Detail page loads.
3. On the upper-left corner of the page, click *Edit*.
   The Edit Device Configuration window loads, letting you override existing profile settings. For information about each profile settings, see Create profiles on page 23.
4. When you finish editing the device's configuration, click *Apply*.
   FortiExtender Cloud applies the new configurations to the device.

Editing a device's configuration causes the device to reboot.

Sync devices

If you have made local modifications to your device and want to overwrite those local changes, you can manually push configurations from FortiExtender Cloud to your devices to sync them.

To sync devices:

1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, locate the device that you want to sync.
3. Check the checkbox for your selected device, and click *Sync*.
   A Confirm Sync Device window loads.
4. Click *Yes* to confirm.
   FortiExtender Cloud syncs the device.

Syncing a device causes the device to reboot.

Export device information

You can export device information of individual devices in a CSV file.

To export device information:

1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, select the device that you want to export information for.
3. Click *Export.*
4. From the list of possible information to export, select what information you want.
5. Click *Export*.
6. Save the CSV file.

To export device usage statistics:

1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, click device that you want to export usage information for and go to the Device Detail page.
3. Scroll down to the SIM History chart and click *Export*.
4. Save the CSV file.

Monitor and manage a deployed device

After you deploy a device, you can access the Device details page to monitor its usage statistics and status information, remotely manage the device, and download device debug logs.

- View device details
- Download device debug log
- Manage a remote device on page 71

Device details

Each device has a details page containing information specific to that device.

To view device details:

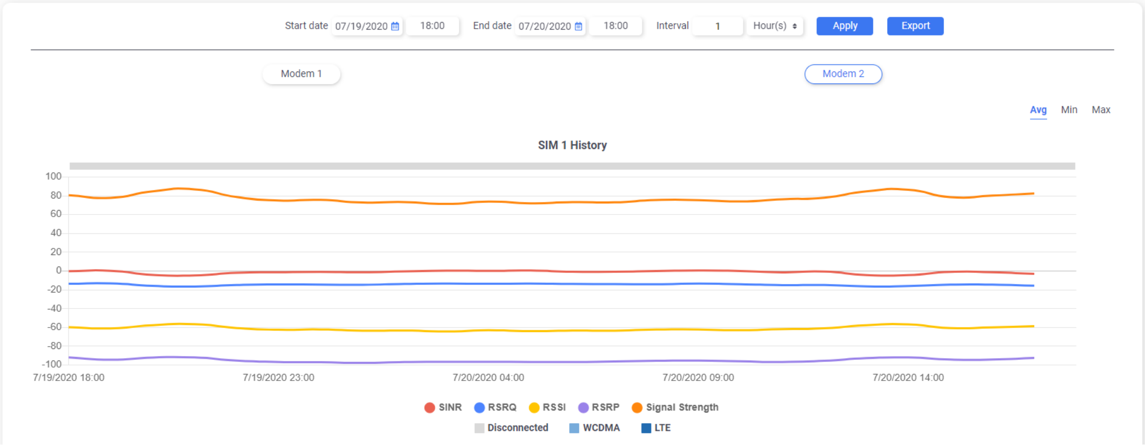
1. From the navigation bar, click *Device* > *In Service*.
   The In Service page loads.
2. From the list of In Service devices, click the device that you want to view.
   The Device Detail page loads, displaying details about the device.

SIM History graph

The Device Detail page contains an interactive chart of your SIM signal strength and throughput history, allowing you to monitor and save your device's usage statistics. You can sort the graph by date and time as well as set a time interval to breakdown the data. You can also click *Export* to export the usage statistics in a CSV file.

Use the Avg, Min, and Max filters to display data based the average, maximum, or minimum values in that set time interval.

If your device has multiple modems, you can toggle between Modem 1 and Modem 2.



Start date 07/19/2020 18:00 End date 07/20/2020 18:00 Interval 1 Hour(s)

SIM History key

Acronym	Definition	Signal Quality values*
SINR	Signal-to-Interference-plus-Noise Ratio • Used to measure 4G (LTE) services.	• > 12.5 dB: Excellent • 10 dB to 12.5 dB: Good • 7 dB to 10 dB: Fair • < 7 dB: Poor • 0 dB: No Signal
RSRQ	Reference Signal Received Quality • Used to measure 4G (LTE) services.	• > -5 dB: Excellent • -5 dB to -9 dB: Good • -9 dB to -12 dB: Fair • < -12 dB: Poor
RSSI	Received Signal Strength Indicator • Used to measure both 3G and 4G (LTE) services.	• > -65 dBm: Excellent • -65 dBm to -75 dBm: Good • -75 dBm to -85 dBm: Fair • < -85 dBm: Poor • -110 dBm: No signal
RSRP	Reference Signal Received Power • Used to measure 4G (LTE) services.	• > -84 dBm: Excellent • -84 dBm to -102 dBm: Good • -102 dBm to -111 dBm: Fair • < -111 dBm: Poor

*These Signal Quality values are Fortinet approximations; your actual quality will vary depending on your carrier. Contact your carrier for more accurate measurements.

Throughput key

Acronym	Definition
RX	Received data
TX	Transmitted data
RX+TX	Received and Transmitted data

Download device debug log

From the Device Detail page, you can download the device debug log for individual devices.

To download the debug log

1. From the navigation bar, click *Device* > *In Service*
   The In Service page loads.

2. From the list of In Service devices, click the device that you want to view.

   The Device Detail page loads, displaying details about the device.
3. At the top of the page, click *Debug*.
4. Save the TGZ file.

Manage a remote device

From the Device Detail page, you can remotely access the FortiExtender command-line interface (CLI), Out-of-Band Management (OBM) console, as well as edit, upgrade, reboot, and reset the device.

Button Name	Description
Upgrade	Upgrade the OS and modem firmware of the device. You can choose from a list of recommended firmware versions, or upload a firmware file from your computer. **Note:** Upgrading a device's OS or modem firmware causes the device to reboot.
Reboot	Reboot the device.
Edit	Edit the configurations of the device. See Edit a device's configuration on page 67
Factory Reset	Reset the device to default factory settings.
Console	Access the CLI of the device.
OBM Console	Access the Out-of-Band Management (OBM) console of the FortiExtender to connect to the console port of any device connected to the FortiExtender via its USB port. For more information on OBM, see OBM management in the FortiExtender Admin Guide (Standalone).

Common CLI commands

This section contains a list of common CLI commands for your FortiExtender device. For a full list of CLI commands, refer to the FortiExtender Administration Guide.

Changing the administrative password

When you first access the CLI of your FortiExtender device, the default password is blank. We strongly recommend that you create a new password to secure your FortiExtender.

`execute shell`
`~ passwd`
	Execute the device shell and enter "passwd" to change the password on your FortiExtender.
	Note: This is the only way to change the password on a FortiExtender running OS firmware 4.0 and earlier.

`execute change-password`	Change the password on a FortiExtender running OS firmware 4.1 and later.

Troubleshooting commands

You can use the following status and debug commands to check the device status and debug accordingly.

Status CLI Commands

`get system version`	Shows the device's hardware and software versions.
`get extender status`	Displays the device's synchronization status with FortiExtender Cloud.
`get cpm status`	Provides the device's SSL tunnel information and connectivity status.
`get modem status`	Details the cellular modem's status.

Logging and Debugging

`execute debug log-to-console on`	Displays logs on telnet or the cloud console terminal.
`execute debug log-to-console off`	Turns off logs on telnet or the cloud console terminal.
`execute debug clear`	Turns off all enabled logging.
`execute debug EXTD info on`	Turns on extender information logging.
`execute debug EXTD info off`	Turns off extender information logging.
`execute debug CPM info on`	Turns on cpm information logging.
`execute debug CPM info off`	Turns off cpm information logging.
`execute debug CONNMGR info on`	Turns on modem's information logging.
`execute debug CONNMGR info off`	Turns off modem's information logging.

Log-to-console commands are not required while accessing the device over the serial console port. They are only applicable to telnet or cloud console terminals.

Manage scheduled upgrades

FortiExtender Cloud lets you schedule device firmware upgrades for a later time. Once you've scheduled your upgrade, you can view and edit the scheduled upgrade from the Scheduled Upgrade page.

To view or modify a scheduled upgrade:

1. From the navigation bar, click *Scheduled Upgrade*.

   The Scheduled Upgrade page loads with all your scheduled upgrades.
2. From the *Status* column, you can click the toggle to enable or disable each upgrade.
   - *On*: Enable the upgrade.
   - *Off*: Disable the upgrade.
3. Click on the scheduled upgrade to see which devices are included in the batch.

   From this section, you can perform multiple actions:
   - Edit: Change the upgrade time or selected firmware version.
   - Delete: Delete the scheduled upgrade.
   - Add Devices: Add devices to the scheduled upgrade.
   - Remove Devices: Select and remove devices from the scheduled upgrade.
4. When you are finished, click *Apply* to save your changes.

Manage users

FortiExtender Cloud features Role Based Access Control (RBAC), which lets administrators add users to FortiExtender Cloud and assign them permission roles. You cannot add users into FortiExtender Cloud directly; new users must be added through the administrator's FortiCare or Identity and Access Management (IAM) account.

This topic contains instructions for:

- Adding a new user
- Assigning a user role
- Removing a user

Add a user

FortiExtender Cloud administrators can add new users to FortiExtender Cloud via FortiCare or the IAM portal. You can add two different kinds of users:

- Sub Users
- Identity and Access Management (IAM) Users. For more information, refer to the Identity and Access Management Administration Guide.

When users are added via the FortiCare portal, administrators can assign them permission roles from FortiExtender Cloud. IAM users must have their permissions assigned from the IAM portal.

To add a Sub User to your FortiExtender Cloud account:

1. Log into https://support.fortinet.com.
2. In the top-right corner of the Home page, click your account name to expand the drop down menu and select *My Account*.

   The Account Profile page loads.
3. In the side bar, click *Manage User*.

   The Manage User view loads.
4. Click the *Add New User* 👤+ icon.

   The Add User view loads.
5. Enter the user's information into the required fields.
6. Select the desired permissions for your user.

   You can select if the user has access to Customer Service support, begin an RMA process, accesses Technical Assistance, and more.
7. Select the Access level you want the user to have.
   - To grant the user Admin privileges, select *Full Access*.
   - To limit a user's privileges, select *Limit Access* and specify which FortiExtender devices you want to limit your user to seeing. You can also assign either a ReadWrite or ReadOnly role to the user from FortiExtender Cloud, see Assigning sub user permissions on page 75.

8. When you are finished, click *Save*
   The user will automatically be added into FortiExtender Cloud.

Assigning sub user permissions

After you add a sub user with limited access levels from FortiCare (see Add a user on page 74), you must assign a role to the sub user. You can assign either ReadWrite or ReadOnly permissions to each sub user.

You can only assign permissions from FortiExtender Cloud to sub users. IAM users must have their permissions updated from the IAM portal.

To assign permissions to a sub user:

1. From the navigation bar, go to *Account* > *Sub Users*.
   The Users page loads, displaying a table with all your users.
2. Locate the sub user you want to assign permissions to.
3. Under the Action column, click the *Edit* ✎ icon for the selected user.
   The Edit Permission window loads.
4. In the Role drop-down, select either ReadWrite or ReadOnly.
5. Click *Save*.
   FortiExtender Cloud assigns permissions to the sub user.

Remove a user

When a user no long requires access to your FortiExtender Cloud account, you can remove their access via FortiCare or the IAM portal depending on their user type.

IAM users must be removed from the IAM portal. For more information, refer to the Identity and Access Management Administration Guide.

To remove a Sub User:

1. Log into https://support.fortinet.com.
2. In the top-right corner of the Home page, click the *Account* 👤 icon.
   The Account Profile page loads.
3. In the side bar, click *Manage User*.
   The Manage User view loads, loading all your current users.
4. In the Current Users table, locate the user that you want to remove.

5. In the Action column, click the *Delete* 🗑 icon for the selected user.

   A delete user confirmation window loads.

6. Click *OK*.

   FortiCare removes the user.

Certificates

FortiExtender Cloud enables you to upload and manage Certificate Authorities for your devices. From the navigation bar, expand *Certificates* to upload and assign certificates to individual devices or VPN plans.

- Assign certificates to individual devices on page 77
- Upload certificates for VPN plans on page 77

Assign certificates to individual devices

From the VPN Local page, you can upload certificates to individual devices.

To upload a certificate to a specific device:

1. From the navigation bar, go to *Certificates* > *VPN Local*.
2. Locate the device you want to attach a VPN certificate to, and click the *Add* ⊕ icon.
   The Add VPN Certificate window loads.
3. Select and upload the VPN certificate.
4. Enter a *Name* and *Password* for the certificate.
5. When you are finished, click *Add*.

Upload certificates for VPN plans

From the VPN Ca, you can upload certificates to FortiExtender Cloud and apply them to multiple devices from the VPN Plan page.

To upload a certificate to FortiExtender Cloud:

1. From the navigation bar, go to *Certificates* > *VPN Ca*.
2. Click *Upload*.
   The Add VPN Certificate window loads.
3. Select and upload the VPN certificate.
4. Enter a *Name* for the certificate.
5. When you are finished, click *Add*.

Once you upload the certificate, you can apply them to a VPN plan that has a signature Authentication Method.

API

FortiExtender Cloud has public APIs that allow you to access event logs, device information, and apply configurations to your devices. To access the APIs, you must present either a FortiExtender Cloud token or a FAC OAuth token.

API Schema and documentation

To see the FortiExtender Cloud API schema, you will need a Fortinet Developer Network account.

Once you have an account, you can access the FortiExtender Cloud API documentation.

API Tokens

FortiExtender Cloud tokens can be generated by users who can access the FortiExtender Cloud portal. The permission roles (Admin, ReadWrite, ReadOnly) granted by a FortiExtender Cloud token matches the role of the user who generated it.

FAC OAuth tokens can be generated when you create an API User in the Identity and Access Management (IAM) portal. You can modify the permissions from the IAM portal. Users who use OAuth tokens can only access services by calling APIs, they cannot log into FortiExtender Cloud.

Keep your API token confidential.

To generate a FortiExtender Cloud API token:

1. From the navigation bar, click *Account* > *API Token*.
   A window loads with your specific API token.

You can invalidate the previous token and generate a new API token by clicking *Reset* .

To generate a FAC OAuth token:

For instructions on how to generate a FAC OAuth token, refer to "API users" in the Identity and Access Management Administration Guide.

FortiExtender Cloud tokens do not expire while FAC OAuth tokens do. The expiration time for FAC OAuth tokens are returned in the response when you init or refresh a FAC OAuth token. You should init a new FAC OAuth token or refresh the token before it expires to ensure that you can access the APIs.

Using the API

Example FortiExtender Cloud token.

The keyword is 'token'.

```
response = requests.get(url, headers = {'Authorization': 'token <your_api_token>'})
```

Example FAC OAuth token

The keyword is 'Bearer'.

```
response = requests.get(url, headers = {'Authorization': 'Bearer <your_fac_token>'})
```

Response status codes

Status Code	Description
200	The request is successful.
403	The server understood the request but refuses to authorize it.
404	Unable to find the specified resource.
500	Internal server error.

If you are unable to connect, contact support at https://support.fortinet.com.

View event logs

FortiExtender Cloud logs user, device, and system events so you know what is happening within FortiExtender Cloud. These events can be viewed and downloaded from the Log page and filtered by event types and time range.

From the logs page, you can:

- Filter by event types
- Filter by time range
- Search for specific events
- Downloading event logs on page 81

To access the Log page:

1. In the navigation bar, click *Log*.
   The Log page loads with all logged events displayed in a table.

The logs table truncates longer text with ellipses to prevent overflow. To see the full text, hold your pointer over each cell until a tooltip containing the full text appears.

Filtering by event types

FortiExtender Cloud categorizes each event into one of three event types:

Event Type	Description
User	Events made by users on FortiExtender Cloud. These user events include: • Adding and deleting plans and profiles • Updating device firmware • Deploying and undeploying devices
Device	Events associated with devices. These device events include: • Connection attempts and failures • SIM card insertions • Successful connections
System	Events associated with the FortiCare system. These system events include: • Removing a device from FortiCare • Upgrading the firmware of a FortiExtender device • Pushing new configurations from FortiCare to a FortiExtender device.

To filter by event types:

1. At the top of the Log page, click *Filters*.
2. Select the event type checkbox you want to filter for and click *Apply Filters*.
   The logs table reloads and displays only the event type you selected.

Filtering by time range

You can figure the event logs by selecting a specific time range.

To filter by time range:

1. At the top of the Log page, click *Time*.
   A date picker loads.
2. Select a Start and End time range that you want to filter for and click *Apply*.
   The logs table reloads and displays only the events that occurred during your selected time range.

Searching for specific events

You can search the Log page for specific events by using the search tool.

To search for specific events:

1. At the top of the Log page, locate the search field.
2. Enter a keyword into the search field and click *Search* 🔍.
   The logs table reloads and displays results containing the keyword.
3. To redisplay all log entries, delete all text from the search field, and then click *Search* 🔍 again.

Downloading event logs

You can download even logs CSV format.

To download event logs:

1. At the top of the Log page, click *Export*.
   The Export Logs window loads.
2. Click *Yes* to save the logs.

Notifications

FortiExtender Cloud enables you to manage and view notifications from the Notifications section. From the navigation bar, expand *Notification* to create notification rules and view notifications.

- Create notification rules on page 82
- View notification messages on page 82

Create notification rules

From the Notification Rules page, you can create notifications to send email or SMS alerts when there are changes to a device's availability status or health. You can also create notifications for when licenses are about to expire. Users must be added in your FortiCare account to receive notifications (see Add a user on page 74).

To create a notification:

1. From the navigation bar, go to *Notification* > *Rules*.
2. In the upper-left corner, click *Add Notification Rule.*

   The Add Notification window loads.
3. In the Category field, select the type of notification you want to create.
   - *fext_device*: Notifications relating to a device's availability status.
   - *fext_system*: Notifications relating to a device's health (CPU, temperature, memory).
   - *fext_license_expiration*: Notifications related to FortiExtender Cloud license status changes
4. Once you select a category, fill in the Condition fields to create a notification.
5. In the Email Recipients field, select which email accounts will receive a notification when the specified conditions are met.
6. In the SMS Recipients field, add the phone numbers that will receive an SMS alert when the specified conditions are met.
7. When you are finished, click *Add*.

View notification messages

You can see your notification massages from FortiExtender Cloud. From the navigation bar, click to expand *Notifications* and go to *Messages*.

From the Notification Message page, you can see all your notifications as well as filter your notifications by category type and level of urgency.

Manage account settings

Configure heartbeat interval

Administrators can change the heartbeat interval on all devices in the account from the Settings page.

By default, the system heartbeat interval is set to 30 seconds, however some certification carriers have specified requirements so FortiExtender Cloud sets the heartbeat interval to meet their standards. For example, T-Mobile requires 28 minutes intervals.

To change the heartbeat interval:

1. From the navigation bar, go to *Account* > *Settings*.
   The Settings page loads.
2. In the *Heartbeat Interval* field, enter the time you want in seconds.
3. Click *Save*.

View license information

From the License Information page, you can view the number of FortiExtender Cloud Management subscriptions associated with your account. You can see the total number of license you have, the number of licenses used, and the number of licenses available.

To view license information:

1. From the navigation bar, go to *Account* > *License Information*.
   The License Information page loads with a list of your devices, their current subscription status, as well as their license start and end date.

Troubleshooting

This section contains troubleshooting tips for issues you might encounter when deploying and managing your devices in FortiExtender Cloud.

Issue	Troubleshooting tip
I cannot deploy my FortiExtender; it is stuck in the deploying state.	Make sure your FortiExtender device is running a supported OS firmware version. • To find out which versions are supported, see Supported devices and OS firmware versions on page 11. • For instructions on finding your version number and upgrading firmware, see the FortiExtender Administration Guide. Note that it can take several hours for a FortiExtender to deploy. If the device has not successfully deployed after 24 hours, contact support at https://support.fortinet.com.
My FortiExtender cannot detect the SIM card.	**1.** Check that the SIM card is properly inserted in the SIM slot. **2.** Ensure the SIM card works by testing it in a known working device. **3.** If the SIM card is working and the device is still unable to detect the SIM card, contact support at https://support.fortinet.com.
How can I check the FortiExtender Cloud Service Status?	You can check the status of the FortiExtender Cloud service at: https://status.fortistatus.com/guest-portal/fortiextender/incident/overview

www.fortinet.com