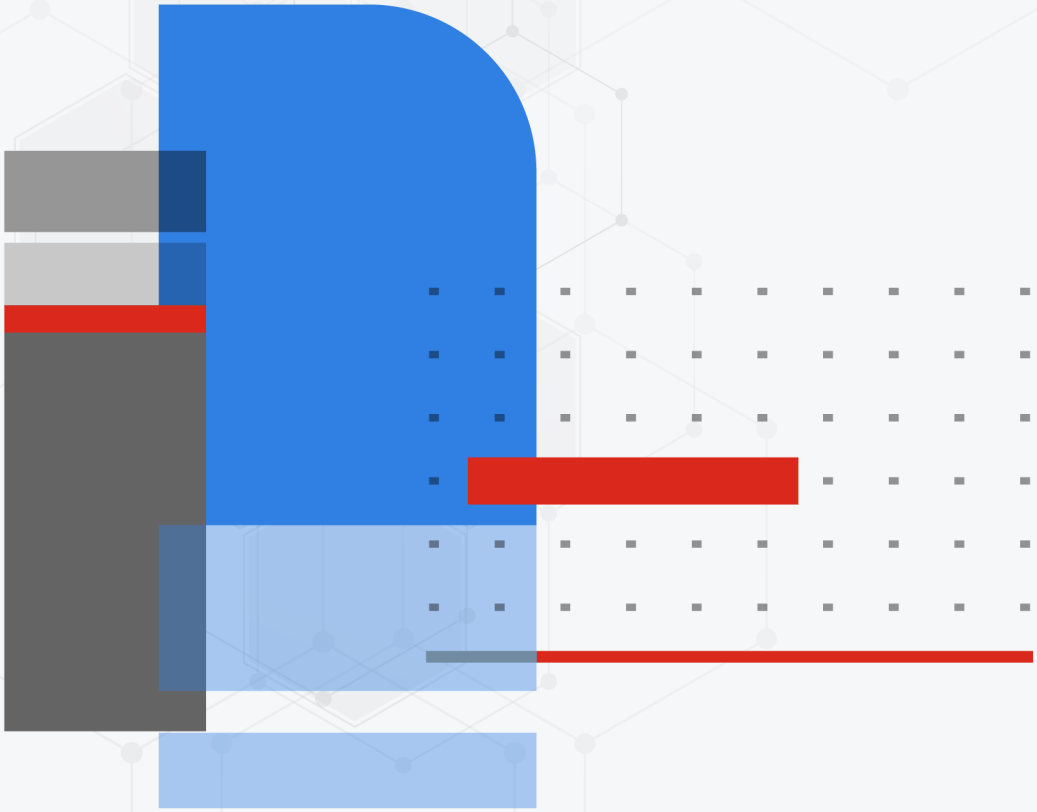
Administration Guide

FortiFlex (Formerly Flex-VM) 24.1.1



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 26, 2024
FortiFlex (Formerly Flex-VM) 24.1.1 Administration Guide
82-241-996900-20240326

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
FortiFlex v24.1.1 release information **7**
New features and updates in v24.1.1 7
Access the points calculator through an API endpoint 7
FortiEDR MSSP updates 7
Getting started **8**
Program requirements 8
Version and feature support 8
Registering FortiFlex 9
FortiFlex Portal 10
Accessing the portal 10
Adding a secondary user 10
Dashboard 10
Program guide **12**
Program renewal 12
Points 13
Prepaid points 13
Postpaid points 14
Point calculation 14
Roll-Over points 14
Service offerings 14
Virtual Machines 15
Hardware Appliances 18
Cloud Services 19
Email notifications 21
Reports 22
Deploying FortiFlex **24**
Flex Entitlements 24
My Assets 25
Decommissioned units 26
Creating entitlements 26
Injecting the FortiFlex license 31
Confirming the license token is injected 35
Configuring web proxy tunneling for FDN 36
Managing Flex Entitlements 36
Creating a license pool group 39
Configurations 39
Creating configurations 40
Configuration details 45
Deployment examples and scripts 53
Manual deployment on KVM 53
Automatic deployments 60

Automation **61**
FortiFlex API 61
FortiFlexVM Terraform provider 63
Ansible Collection 63
Tools **64**
Points calculator 64
Daily points 65

Change Log

Date	Change Description
2024-03-08	Initial release.
2024-03-26	Updated Getting started on page 8, Program guide on page 12, and Deploying FortiFlex on page 24.

Introduction

FortiFlex allows you to easily manage VM usage entitlements. You can use the FortiFlex portal to create VM configurations, generate licensing tokens, and monitor resource consumption in the form of points.

FortiFlex subscribers can create multiple sets of a single VM entitlement that corresponds to a licensed virtual machine. Resource consumption is based upon predefined points that are calculated on a daily basis (PST/PDT time zone).

Virtual Machines with usage entitlements require a per-VM unique token to be installed on every VM. These tokens can be injected into the VM once the configurations and vCPU quantities are defined in the FortiFlex portal, and the VMs are deployed on the customer-managed platform in supported clouds and hypervisors.

FortiFlex v24.1.1 release information

New features and updates in v24.1.1

Access the points calculator through an API endpoint

The points calculator can now be accessed through an API endpoint, providing the current price, latest price, and the effective date for the latest price.

See Points calculator on page 64.

FortiEDR MSSP updates

The FortiEDR MSSP product type now includes XDR as an add-on. The number of EDR and XDR endpoints are the same when creating a configuration.

See Configuration details on page 45.

Getting started

Review the following content when getting started with FortiFlex:

- Program requirements on page 8
- Registering FortiFlex on page 9
- FortiFlex Portal on page 10

Program requirements

The FortiFlex program requires the following items:

- A primary FortiCloud account or IAM user account.
- FortiFlex Program SKU (either Enterprise/prepaid or MSSP/postpaid) purchased from Fortinet's resellers and distributors.
- FortiFlex Point Pack SKU (only applicable to Enterprise/prepaid) purchased from Fortinet's resellers and distributors.

Version and feature support

FortiFlex is supported in the following Fortinet solutions.

Product support

FortiFlex can be used to create VM usage entitlements for the following products:

- FortiOS 6.4.3 and higher
- FortiWeb 7.0.1 and higher
- FortiManager 7.2.1 and higher
- FortiAnalyzer 7.2.2 and higher
- FortiPortal-VM 7.0.3 and higher
- FortiADC 7.4.0 and higher
- FortiClient EMS 7.2.2 and higher
- FortiWeb Cloud 23.3.a and higher

Version support

FortiFlex licensed devices are supported in the physical and virtual versions of FortiManager and FortiAnalyzer.

- FortiManager 6.4.3 and higher
- FortiAnalyzer 6.4.3 and higher

VDOMs

FortiFlex natively supports VDOMs and no longer requires perpetual licenses.

You can add and stack up to 500 VDOMs to FortiGate-VM regardless of its CPU capacity. The number of VDOMs to be added is determined by VDOM license you purchased.

FortiFlex supported VDOMs in the following products:

- FortiOS 6.4.9 and higher

FortiToken

FortiToken is supported on FortiFlex FortiGate-VMs.

Registering FortiFlex

FortiFlex is an annually contracted program that can be registered through the FortiCloud Asset Management portal.

FortiFlex program-related SKUs are available for purchase from Fortinet's resellers and distributors. There may be certain conditions to be eligible to join the program. Consult your Fortinet sales representatives.

To register FortiFlex:

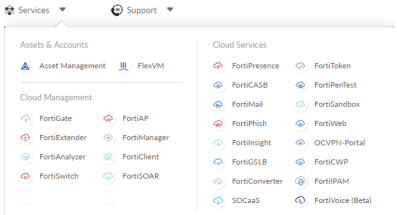
1. Log into your FortiCare account. The *Asset Management* portal opens.
2. Go to *Products* > *Product List*.
3. Click *Register More* and follow the steps in the registration wizard.
4. Log out of your account after the registration is complete.

For information about product registration, see *Registering products* in *Asset Management Administration Guide*.

The program begins on the date of registration. It may take up to four hours for the registration to validate in FortiCloud.

To access the FortiFlex portal:

1. Log in to your FortiCare account. The *Asset Management* portal opens.
2. In the banner, click *Services* > *Assets & Accounts* > *FlexVM*.



To view your FortiFlex license:

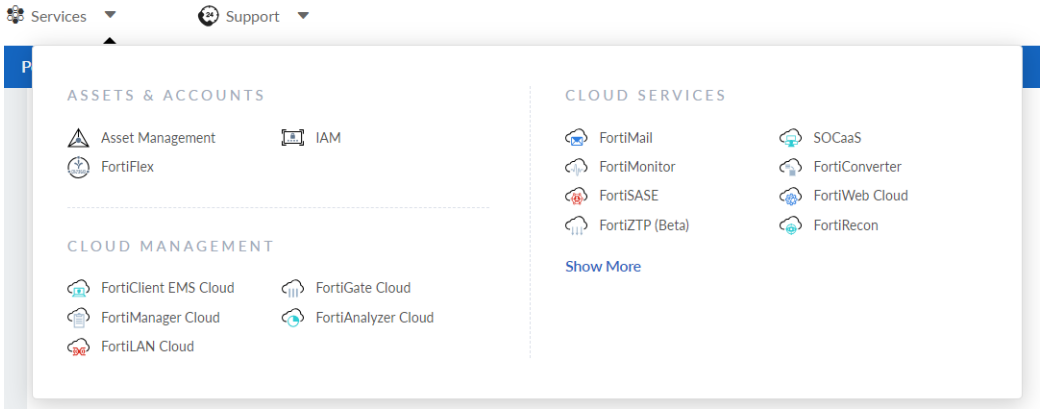
1. Log into your FortiCare account. The *Asset Management* portal opens.
2. Click *Account Services*.

FortiFlex Portal

The FortiFlex portal allows you to monitor point consumption, configure virtual machine entitlements, create licensing tokens, and run reports.

Accessing the portal

You can access the FortiFlex portal from the *Services* menu in Asset Management. The FortiFlex option appears in the *Asset & Accounts* section when there is a valid FortiFlex license.



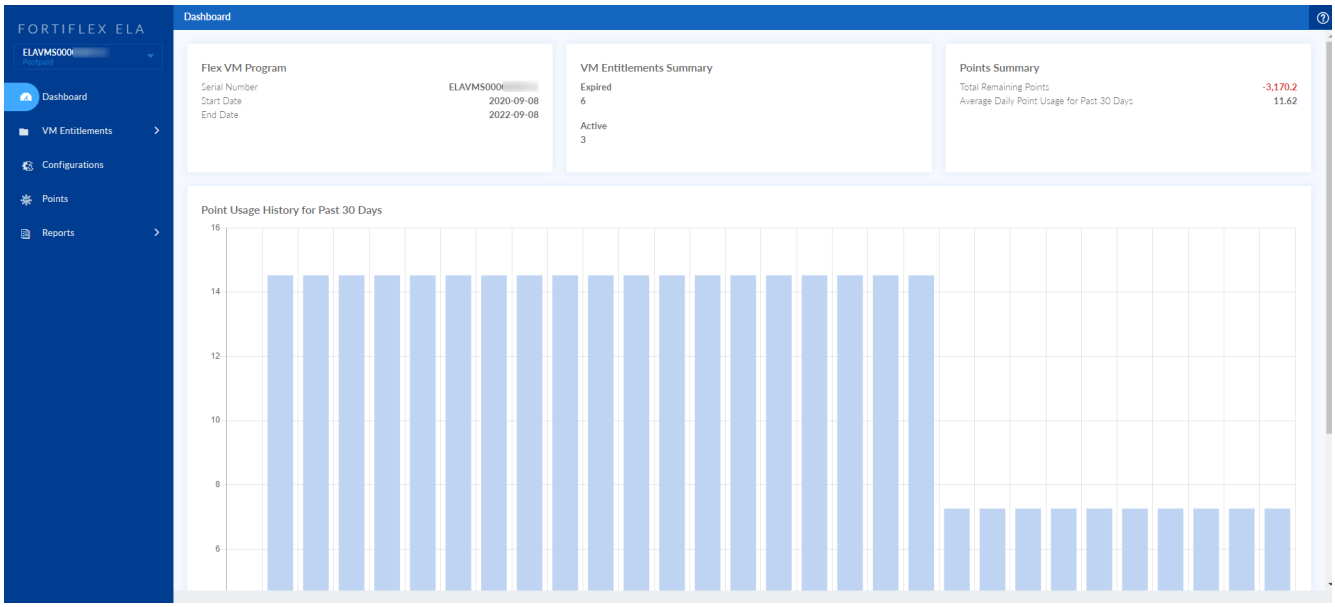
Adding a secondary user

The FortiFlex portal supports the Master account in FortiCloud. To add secondary accounts, create an IAM user. For information, see Adding IAM users.

The FortiFlex portal does not support FortiCloud sub user accounts. To grant access to a FortiCloud sub user, migrate the user in the IAM portal. See Migrating sub users.

Dashboard

The *Dashboard* view provides an overview of activity in your FortiFlex account. Use the dashboard to quickly monitor active and expired virtual machines, as well points consumed.



The *Dashboard* contains the following monitors:

Monitor	Description
Flex VM Program(s)	Displays the program serial number and the program start and end dates.
VM Entitlements Summary	Displays the number of *Active*, *Stopped* and *Expired* virtual machines.
Points Summary	For Prepaid programs, this field displays the *Total Remaining Points* and *Average Daily Point Usage for Past 30 Days*. For Postpaid and Evaluation programs, this field displays the *Current Period* month and a positive value for the *Total Consumed Points in the Period*.
Point Usage History for Past 30 Days	Displays the daily point usage for the past thirty days as a chart. Hover over a bar in the chart to see the points used for a specific day.

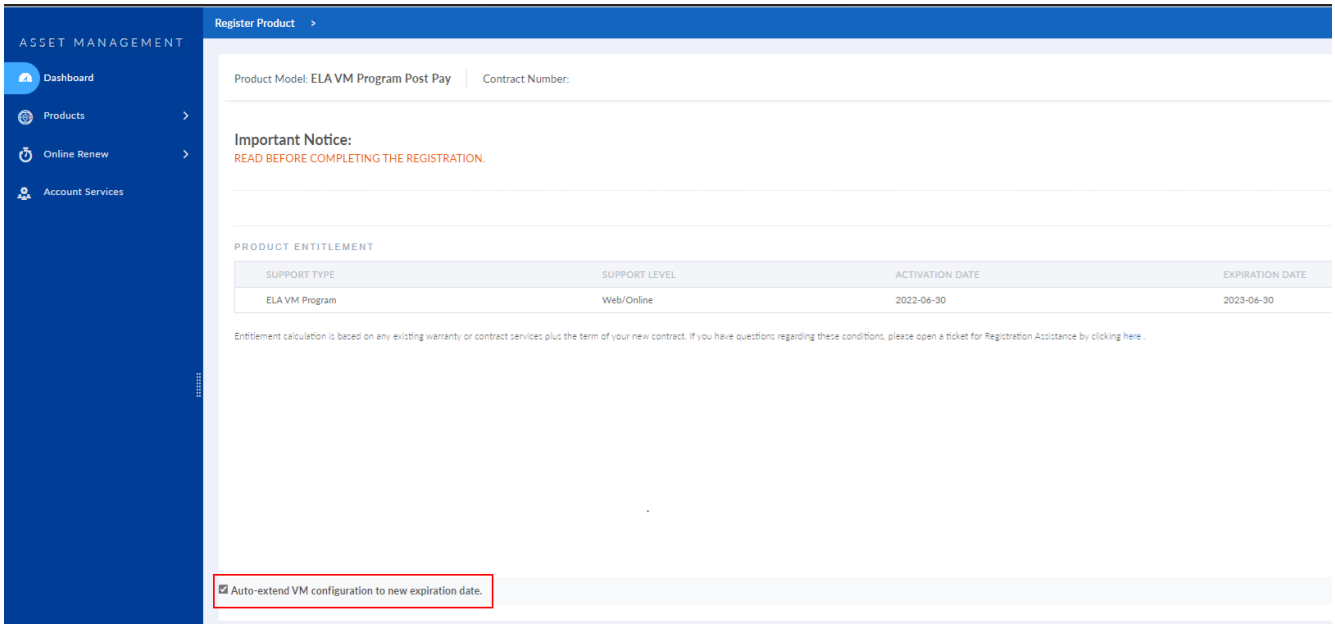
Program guide

The topics in this section provide information about the FortiFlex program.

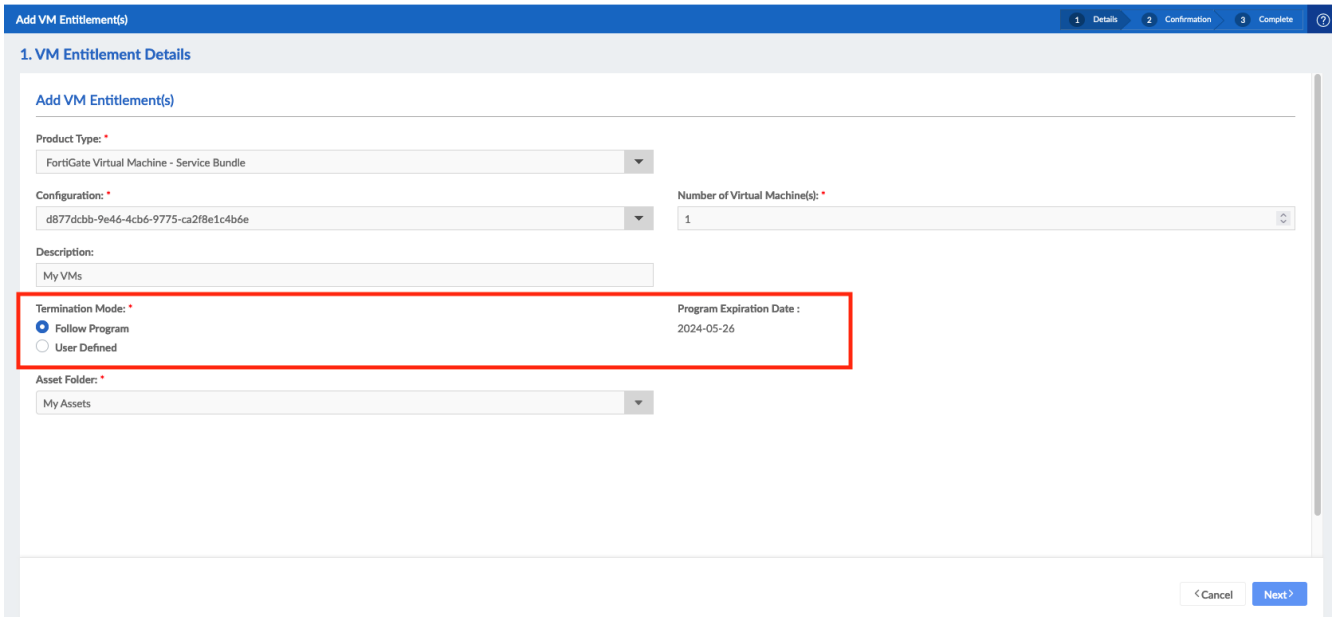
- Program renewal on page 12
- Points on page 13
- Service offerings on page 14
- Email notifications on page 21
- Reports on page 22

Program renewal

When you register a new FortiFlex contract for renewal, you have the option of selecting *Auto-extend VM configuration*.



This tells FortiFlex to update the expiration date of all VM entitlements that have the *Termination Mode* set to *Follow Program*, to the expiration date of the new contract that is being registered.



Points

Resource consumption is based upon predefined points that are calculated on a daily basis (PST/PDT time zone). Points can be purchased in advance or billed on a month basis based on the number of CPUs and service package.

Prepaid points

Prepaid points are available for Enterprise customers. Points are purchased in units of 10,000 and 50,000 points and are deducted on a daily basis based on resource consumption. Unused points can be rolled over upon the program registration anniversary date. See Roll-over points.

One account can have only one Prepaid FortiFlex program. Multiple registrations can be performed to extend the existing program period.

FortiFlex Points can also be converted from FortiCloud FortiPoints in the Asset Management portal's *Marketplace*. This is only available for Prepaid programs at the root account level. See FortiFlex in the FortiCloud Asset Management guide.

Grace Period for negative points

The negative points grace period is applicable only to Prepaid accounts and is activated whenever the points balances becomes negative. Customers have 90 days to bring the balance back to positive otherwise the account may be suspended.

Postpaid points

Points are calculated based on resource consumption and billed on a monthly basis. The detailed payment terms may be specified in your individual purchase agreements.

One account can have only one Postpaid FortiFlex program. Multiple registrations can be performed to extend the existing program period.

A FortiFlex account can only accommodate one prepaid program and one postpaid program at the same time.

Point calculation

Points are calculated daily based on PST/PDT time zones. Calculations are based on the number of CPUs and service package. You can change the per-VM entitlements as many time as you like in a day. The largest CPU size and service package for the day will be charged based on the PST/PDT time zone day count. It may take up to three hours for the change to be updated in FortiCloud.

Points are not calculated during a VM entitlement stoppage, even though the VM may still be running on the customer-managed environment.

Roll-Over points

Pre-paid points can be rolled-over on the service registration anniversary date. Unused points will be rolled over to the next year with the following conditions:

Program	Description
12 months	• Unused points that existed and were added before the 180th day in the year will be rolled over in half to the next year. • Unused points that were added on or after the 180th day in the year will be rolled over as the full amount.
36 months	• Unused points will be rolled over as the full amount.
60 months	• Unused points will be rolled over as the full amount.

Roll-over points do not apply to the post-paid program.

Service offerings

The following table provides an overview of the available service packages.

For detailed information, see the FortiGate™ Virtual Appliances.

Virtual Machines

FortiGate Virtual Machine - Service Bundle

Bundles	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	FortiCare Only
FortiCare Premium	24x7	24x7	24x7	24x7
FortiGuard App Control Service	✓	✓	✓	✓
IPS	✓	✓	✓	
Application Control	✓	✓	✓	
Advanced Malware Protection	✓	✓	✓	
URL, DNS, & Video Filtering	✓	✓		
Anti-spam Service	✓	✓		
DLP	✓			
Inline CASB Database	✓			
AI-based Inline Malware Prevention	✓			
Attack Surface Security	✓			
Converter Service	✓			

Entitlement Limits			
vCPUS		**VDOMs**	
Minimum	1	VM01	10
Maximum	96	VM02 - VM03	25
Increments	1	VM04 - VM07	50
		VM08 - VM96	500

FortiGate Virtual Machine - A La Carte Services

The A La Carte Service package allows you to pick and choose the services you want use.

Service Type	Services
FortiGuard Services	Intrusion Prevention

Service Type	Services
	Advanced Malware Protection
	FortiGuard Attack Surface Security Service
	FortiGuard OT Security Service
	DLP
	AI-Based InLine Sandbox
	Web, DNS, & Video Filtering
	FortiConverter Service
Cloud Services	FortiGate Cloud
	SD-WAN Underlay
	FortiAnalyzer Cloud with SOCaaS
	FortiAnalyzer Cloud
	SD-WAN Connector for FortiSASE
	Cloud-based Overlay-as-a-Service
Support Services	FortiCare Premium
	FortiCare Elite

Entitlement Limits			
vCPUS		**VDOMs**	
Minimum	1	VM01	10
Maximum	96	VM02 - VM03	25
Increments	1	VM04 - VM07	50
		VM08 - VM96	500

FortiWeb Virtual Machine - Service Bundle

Service type	Advanced Bundle	Standard Bundle
24 x 7 FortiCare plus AV	✓	✓
FortiWeb Security Service	✓	✓
IP Reputation	✓	✓
FortiWeb Cloud Sandbox	✓	
Crential Stuffing Defense Service	✓	

FortiManager Virtual Machine

The FortiManager Virtual Machine allows you to set the number of managed devices and ADOMs.

Service Type	Included in bundle
FortiCare Premium support	✓

Entitlement Limits			
Devices		**ADOMs**	
Minimum	1	Minimum	0
Maximum	100 000	Maximum	100 000
Increments	1	Increments	1

FortiClient EMS On-Prem

Service Type	Services
Support Services	FortiCare Premium
	FortiCare Best Practice
Service Packages	ZTNA/VPN
	EPP/ATP + ZTNA/VPN
	Chromebook

Entitlement Limits	
All Endpoints	
Minimum	25
Maximum	25 000
Increments	25

FortiAnalyzer Virtual Machine

The FortiAnalyzer Virtual Machine allows you to set the daily storage (GB) and ADOMs.

Service Type	Included in bundle
FortiCare Premium support	✓
FortiGuard IOC (Indicators Of Compromise)	✓
Security Automation Service	✓
FortiGuard Outbreak Detection Service	✓

Entitlement Limits			
Storage (GB)		**ADOMs**	
Minimum	5	Minimum	0
Maximum	8 300	Maximum	1 200
Increments	1	Increments	1

FortiPortal Virtual Machine

Service Type	Included in bundle
FortiCare Premium support	✓

Entitlement Limits	
Devices	
Minimum	0
Maximum	100 000
Increments	1

Hardware Appliances

FortiGate Hardware

The hardware device is purchased and owned by customers. However, only hardware that does not have any services already attached can be added to FortiFlex. If the hardware has any services attached, contact customer service to detach the services before configuring on FortiFlex.

The Continuous Service Policy is not applicable to FortiFlex entitlements.

Service Type	Services
Support Services	FortiCare Premium
	FortiCare Elite
	FortiCare Elite Upgrade
	ATP
	UTP
	Enterprise

The FortiCare Elite Upgrade can only be combined with one of the FortiGuard Service Bundles (ATP, UTP, or Enterprise).

FortiGate Hardware is only available for postpaid and select prepaid accounts. See Points on page 13 for more information.

Cloud Services

FortiWeb Cloud - Private

Service Type	Services
Average Throughput	Average throughput measured by the 95th percentile, between 10 Mbps and 10 Gbps
Web Applications	Number of web applications, between 1 and 2000

Entitlement Limits			
Throughput		**Web Apps**	
Minimum	10	Minimum	1
Maximum	10 000	Maximum	2 000
Increments	25	Increments	1

FortiWeb Cloud - Public

Service Type	Services
Average Throughput	Average throughput measured by the 95th percentile, between 10 Mbps and 10 Gbps
Web Applications	Number of web applications, between 1 and 2000

Entitlement Limits			
Throughput		**Web Apps**	
Minimum	10	Minimum	1
Maximum	10 000	Maximum	2 000
Increments	25	Increments	1

FortiClient EMS Cloud

Service Type	Services
Support Services	FortiCare Best Practice
Service Packages	ZTNA/VPN
	ZTNA/VPN + FortiGuard Forensics
	EPP/ATP + ZTNA/VPN
	EPP/ATP + ZTNA/VPN + FortiGuard Forensics
	Chromebook

Entitlement Limits	
All Endpoints	
Minimum	25
Maximum	25 000
Increments	25

FortiSASE

Service Type	Services
Number of users	Number of users of the service
Service Packages	Standard
	Advanced
Bandwidth (Mbps)	Total required bandwidth
Dedicated IPs	Number of dedicated IP addresses

Entitlement Limits					
Users		**Bandwidth**		**Dedicated IP**	
Minimum	50	Minimum	25	Minimum	4
Maximum	50 000	Maximum	10 000	Maximum	65 534
Increments	25	Increments	25	Increments	1

FortiEDR MSSP

Service Type	Services
Service Package	Discover/Protect/Respond

Entitlement Limits	
Endpoints	
Minimum	0
Maximum	50 000
Increments	1

Email notifications

Email notifications are sent to provide updates on the current status of registered FortiFlex programs and points balances. When certain conditions are triggered, an email is sent by FortiFlex to notify you of the event that triggered the email.

Email notification types include:

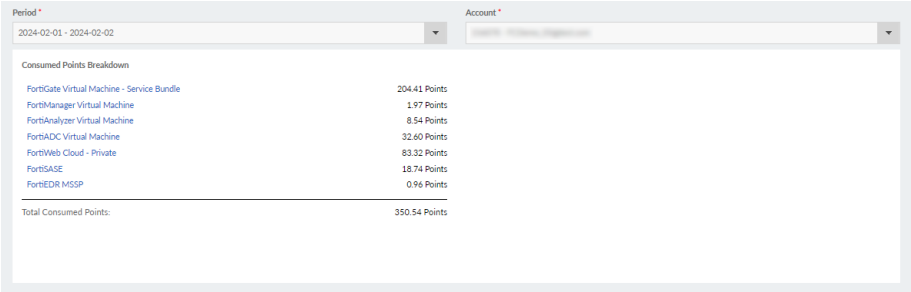
Notification Type	Description
Low Balance	This email is used to notify users that the current point balance is less than the average consumption in the last 30 days multiplied by the number of days until it runs out. The email is triggered if the points balance is not high enough to maintain the current average points consumption for 90, 60, 30, 15, or seven days. This email is part of the Pre-paid program. For example, if the average points consumption in the last 30 days is 1000 points per day, FortiFlex will anticipate that the same average points consumption rate will be maintained for the next 90 days (1000 points per day * 90 days = 90 000 points consumed). However, if the current points balance is less than 90 000, FortiFlex will send an email alert to notify users that the points will run out in 90 days time.
Negative Balance	This email is used to notify users when the point balance becomes negative. This email is part of the Pre-paid program.
Program Anniversary	This email is used to mark how many days are left until the anniversary of program registration. The email is sent when there are 60, 30, 21, 15, seven, and three days left until the anniversary. This email is part of the Pre-paid program.
Program End	This email is used to notify users when the expiry of the program is approaching. The email is sent when there are 90, 60, 30, 21, 15, seven, and three days left until the program expires. This email is part of the Pre-paid and Post-paid programs.
Program Expired	This email is used to notify users about how many days have passed since the program expired. The email is sent when three, seven, 11, 15, 21, 26, and 30 days have passed since the program expired. This email is part of the Pre-paid and Post-paid programs.

Reports

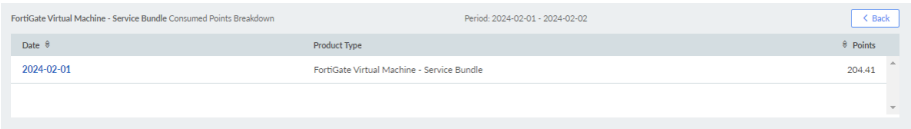
The *Reports* tab contains the *Point Usage Summary*, *Point Usage Detail*, and *Point Pack Summary*. You can run a report for a specified time period, and then export it as a CSV, XLXS, or XML file.

To run the Point Usage Summary:

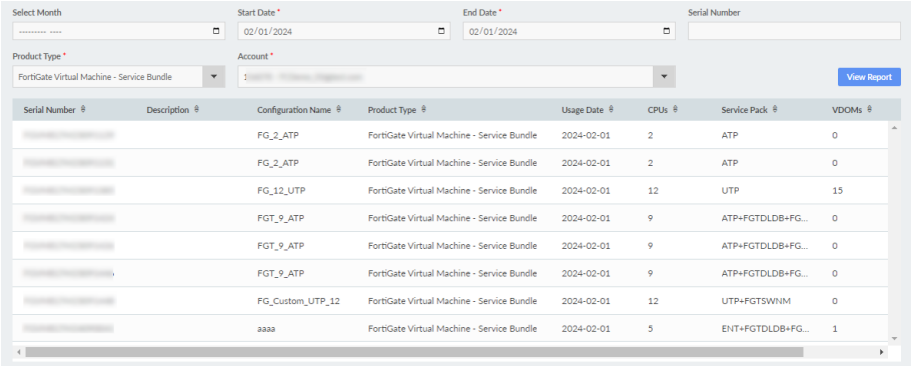
1. Go to *Reports* > *Point Usage Summary*.
2. Select the *Period* and *Account*. The *Consumed Points Breakdown* is displayed.



3. Select the product type. The breakdown of point usage for that product time in displayed.



4. Select a date. The *Point Usage Detail* for that date is displayed.



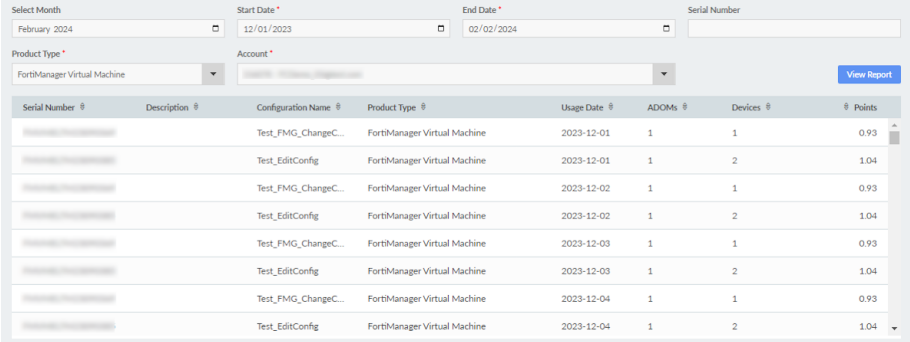
To run the Point Usage Detail Report:

1. Go to *Reports* > *Point Usage Detail*.
2. Select the desired filters.

The *Start Date* cannot be more than 90 days ago.

If FortiFlex is used in an Organization, the *OU/Account* dropdown menu will show options based on the user's permission scope. When in the root account, all accessible accounts will be displayed. When in a member account, only the current account will be displayed.

3. Click *View Report*. The report results are displayed.



4. (Optional) Right-click the report and click *Export* to download the report as a CSV or XLSX file.

To view the Point Pack Summary:

1. Go *Reports* > *Point Pack Summary*.
   The FortiFlex point licenses that were registered are displayed. If there are no point packs registered, the report will be empty.

2. (Optional) Right-click the report, and click *Export* to download the report as a CSV or XLSX file.

Deploying FortiFlex

To deploy FortiFlex, create a VM configuration and use it to create a new VM entitlement. After the entitlement is created, inject the licensing token into the virtual machine. This will trigger the VM to download the corresponding license file.

To deploy Flex VM:

1. Create a VM configuration.
2. Create VM entitlements.
3. Inject the FortiFlex license.
4. Monitor the points consumed.
5. Run reports to manage points and serial numbers.

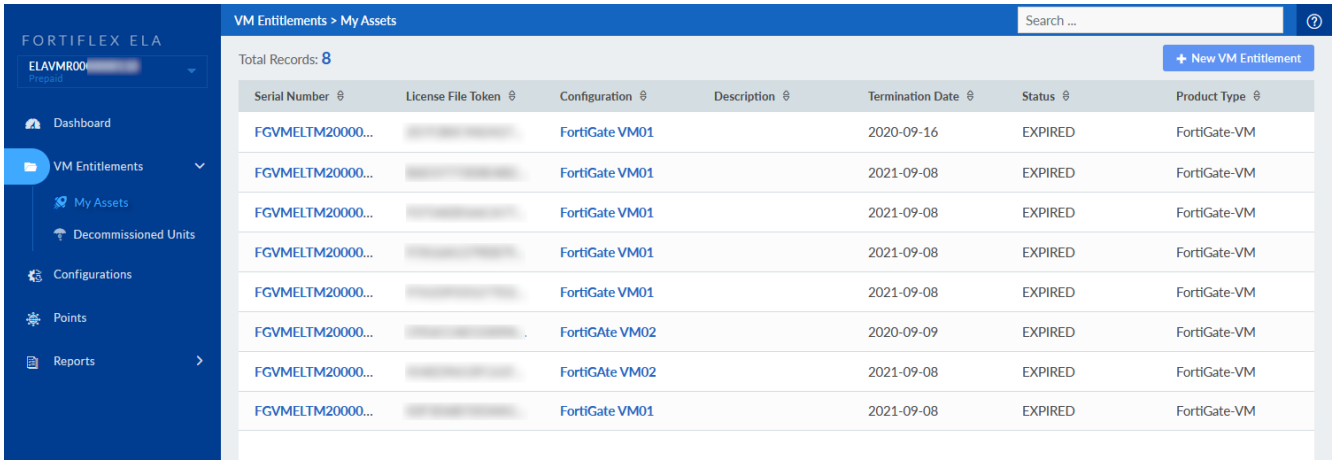
This section includes the following information:

- Flex Entitlements on page 24
- Configurations on page 39
- Deployment examples and scripts on page 53

Flex Entitlements

Use the *Flex Entitlements* page to create and manage VM license entitlements which are consumed via the license tokens. You can also disable compromised license entitlements or change the configuration of a virtual machine.

A License Token is a one-time code used to activate a VM instance. A new token must be re-generated if the VM needs to be re-activated. See Managing Flex Entitlements on page 36.

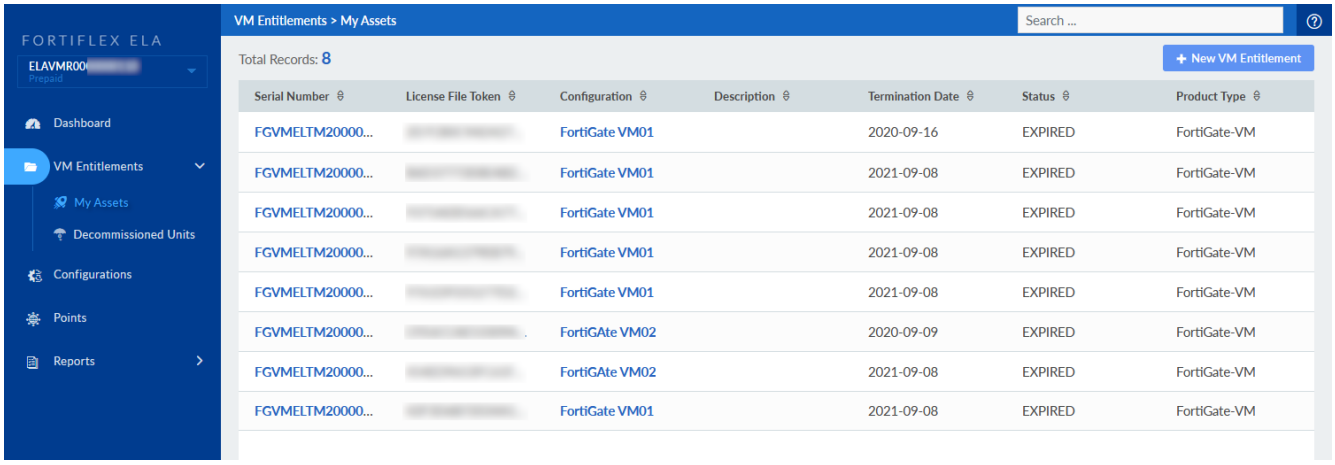


The table displays the following information:

Serial Number	The serial numbers generated when you configure a VM.
License File Token	The available License File Tokens that can be injected into a VM to leverage consumption entitlements.
Configuration	The VM configuration assigned to the serial number.
Description	The description of the entitlement you entered when the VM was created.
Termination Date	The expiry date for the token. The token can be stopped, edited, or reactivated.
Status	The status of the VM entitlement. • *PENDING*: The entitlement is created but not activated. The VM is not being charged for daily consumption. • *ACTIVE*: The entitlement is activated and the VM is being charged for daily consumption (PST/PDT time zone). • ~~*ACTIVE*~~: The entitlement is in use. • *STOPPED*: When the entitlement is stopped for the entire day, the VM will not be charged for the day. • *EXPIRED*: The entitlement has exceeded the *Termination Date*. • *GRACE_PERIOD*: The entitlement is *ACTIVE* but has a negative balance or a program expiration that has triggered the activation of the grace period. Once all grace period events have been cleared, it may take a full day for the status to change back from *GRACE_PERIOD* to *ACTIVE*. *PENDING*, *ACTIVE*, and *STOPPED* entitlements can be edited to update the *Configuration* and *Description*. *PENDING* and *ACTIVE* entitlements can also be edited to have a new *Termination Date*.

My Assets

The *My Assets* view shows the Asset Folders assigned to a VM entitlement. You will only see the asset folders you have permission to view. Asset folders are created in the Asset Management portal. FortiFlex only shows VMs inside each folder except for when creating new VMs. For information about creating Asset Folders in Asset Management, see *Asset Management > Creating custom views*.



Asset folder permissions

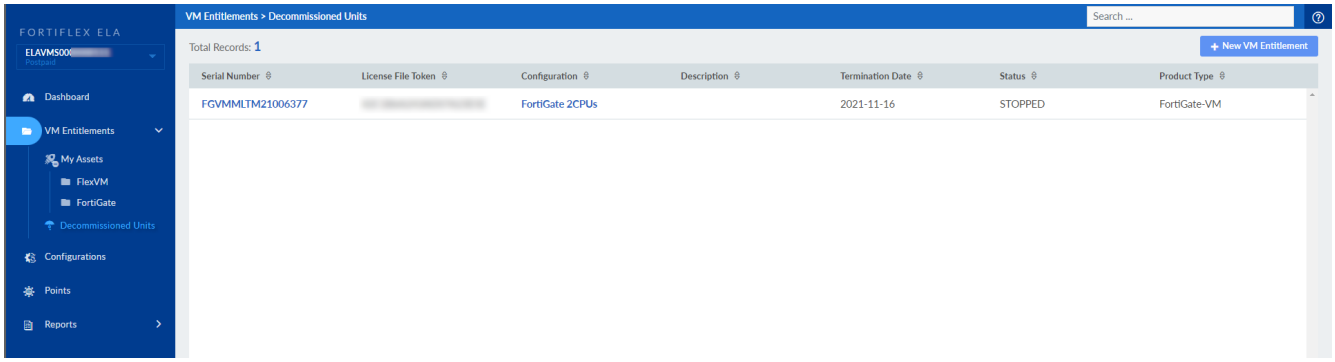
Asset folder permissions are assigned in the Identity & Access Management (IAM) portal. For more information about Asset Folder permissions, see *Identity & Access Management (IAM) > Asset and portal permissions*.

You can use an asset folder to request the next available serial number with the API. See Creating a license pool group on page 39.

Decommissioned units

The *Decommissioned Units* view shows the VM serial numbers that were decommissioned in the Asset Management portal. When decommissioning an active VM serial number in the Asset Management portal, you must stop the entitlement before it can be decommissioned. Attempting to decommission the serial number while it is still active will return an error. See Managing Flex Entitlements on page 36 for information on stopping VM entitlements.

For information about decommissioning units in Asset Management, see Asset Management > Viewing decommissioned units.



Creating entitlements

Entitlements can be created for virtual machines (VMs), hardware devices, and cloud services. The program requires a positive point balance to create entitlements.

This section includes:

- Creating VM entitlements on page 26
- Creating hardware device entitlements on page 28
- Creating Cloud service entitlements on page 29

Creating VM entitlements

Create a VM entitlement to be used with various VM products, including FortiGate-VM or FortiWeb-VM.

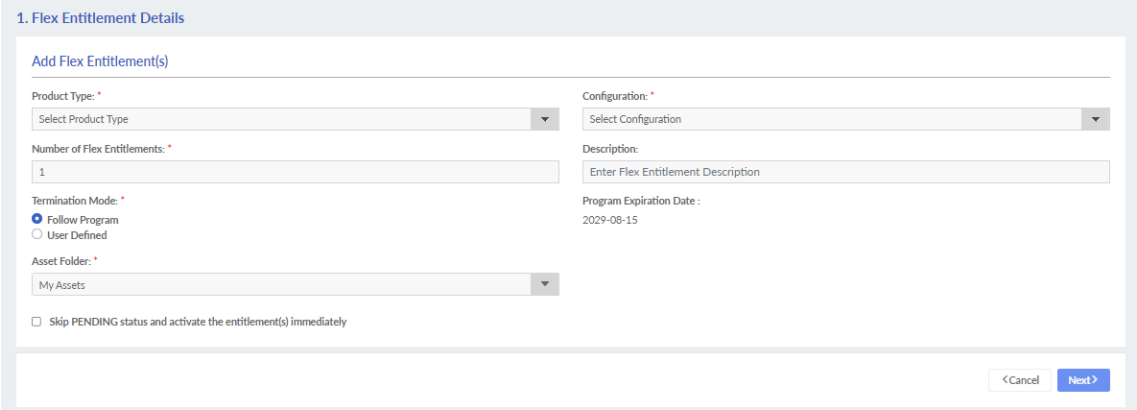
When you create a VM on FortiFlex the consumption for the VM starts when the entitlement is activated for the first time.

All newly created entitlements will be set to *PENDING* and will be changed to *ACTIVE* when the entitlement is activated by the VM instance, which triggers the start of charges.

You cannot add purchased VMs or pre-existing Trial or Evaluation services to FortiFlex. You must create a new VM entitlement.

To create a VM entitlement:

1. Go to *Flex Entitlements*, and click *New Flex Entitlement*. The *Add Flex Entitlement(s)* page opens.

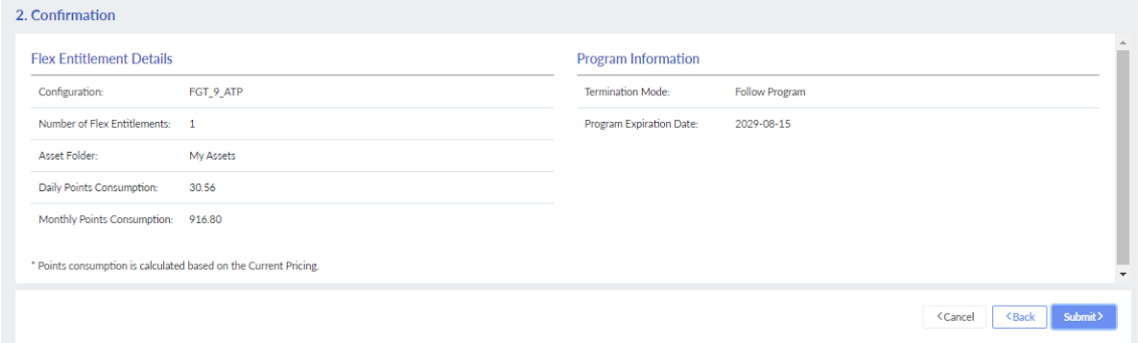


2. Configure the VM Entitlement.

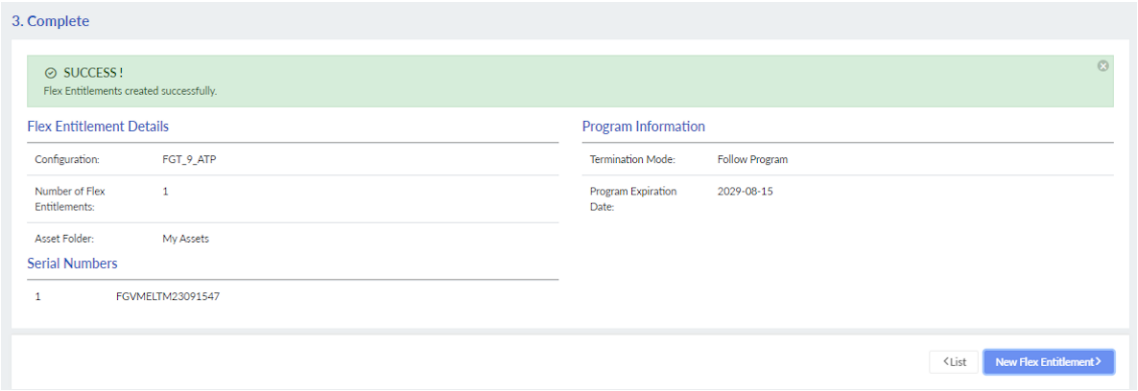
Product Type	Select one of the following service bundles from the dropdown: • *FortiGate Virtual Machine - Service Bundle* • *FortiGate Virtual Machine - A La Carte Services* • *FortiWeb Virtual Machine - Service Bundle* • *FortiManager Virtual Machine* • *FortiClient EMS On-Prem* • *FortiAnalyzer Virtual Machine* • *FortiPortal Virtual Machine* • *FortiADC Virtual Machine* For information about the product types, see Service offerings on page 14.
Configuration	Select a VM configuration from the list. See Creating a VM configuration on page 40.
Number of Flex Entitlements	Enter the number of entitlements. See Creating a VM configuration on page 40.
Description	Enter a description of the VM.
Termination Mode	• Select *Follow Program* to terminate the machine when the program expires.

	• Select *User Defined*, and select a date in the calendar to specify the termination date.
Asset Folder	Assign the VM to a folder in *My Assets*. For more information about Asset Folders, see Asset Management > Creating custom views. You can use an asset folder to request the next available serial number with the API. See Creating a license pool group on page 39.
Skip PENDING status and activate the entitlement(s) immediately	Select this option to immediately set you VM entitlement to *ACTIVE* instead of *PENDING* upon creation.

3. Click *Next*.
4. Review the *Flex Entitlement Details* and *Program Information*, and click *Submit*.



The *Serial Numbers(s)* are displayed.

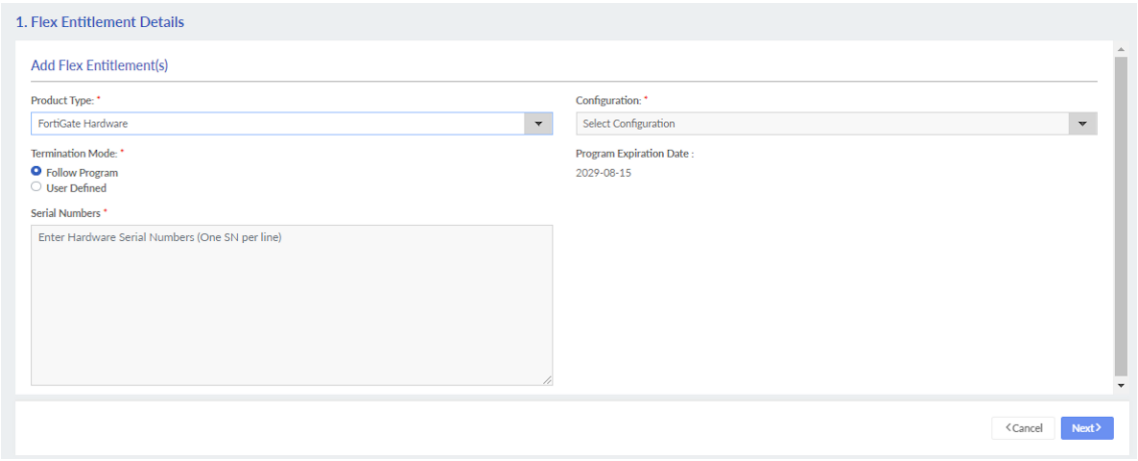


Creating hardware device entitlements

Create a hardware device entitlement to be used with FortiGate products. License tokens are not applicable for hardware devices.

To create a hardware device entitlement:

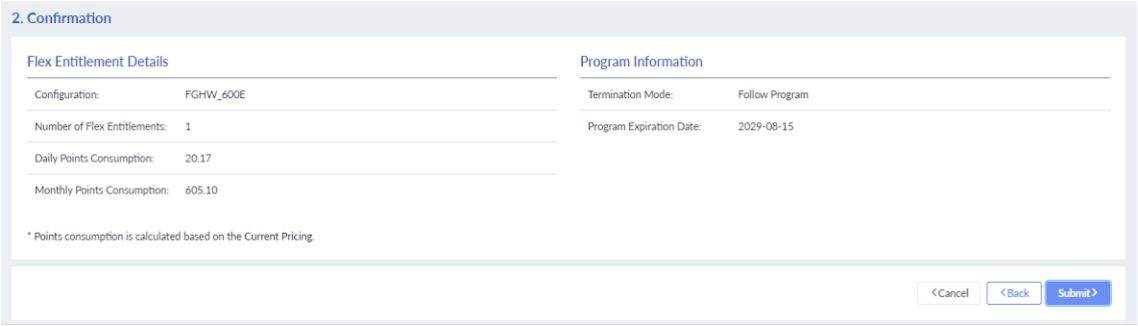
1. Go to *Flex Entitlements*, and click *New Flex Entitlement*. The *Add Flex Entitlement(s)* page opens.



2. Configure the VM Entitlement. Creating configurations on page 40.

Product Type	Select one of the following service bundles from the dropdown: • *FortiGate Hardware* For information about the product types, see Service offerings on page 14.
Configuration	Select a configuration from the list. See Creating a hardware appliance configuration on page 42.
Termination Mode	• Select *Follow Program* to terminate the machine when the program expires. • Select *User Defined*, and select a date in the calendar to specify the termination date.
Serial Numbers	Enter the device serial numbers.

3. Click *Next*.
4. Review the *Flex Entitlement Details* and *Program Information*, and click *Submit*.



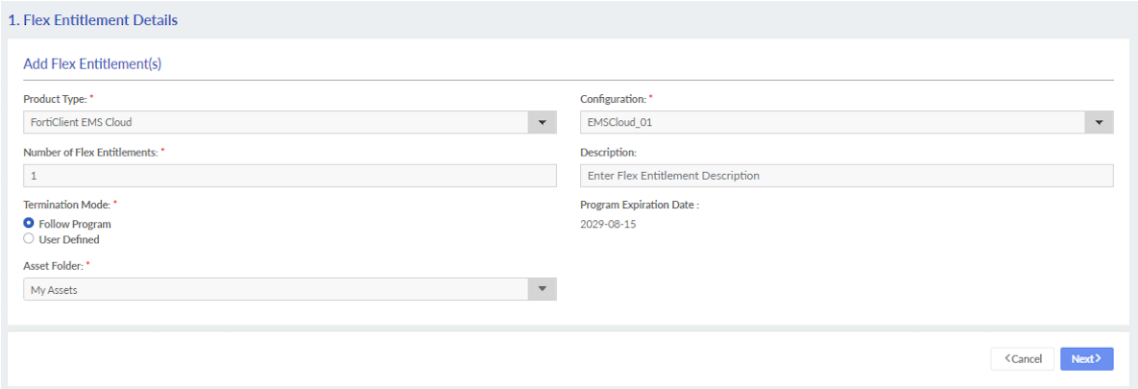
Creating Cloud service entitlements

Create a Cloud service entitlement to be used with various products, including FortiWeb Cloud or FortiSASE. License tokens are not applicable for Cloud services.

You cannot add purchased Cloud services or pre-existing Trial or Evaluation services to FortiFlex. You must create a new Cloud service entitlement.

To create a Cloud service entitlement:

1. Go to *Flex Entitlements*, and click *New Flex Entitlement*. The *Add Flex Entitlement(s)* page opens.

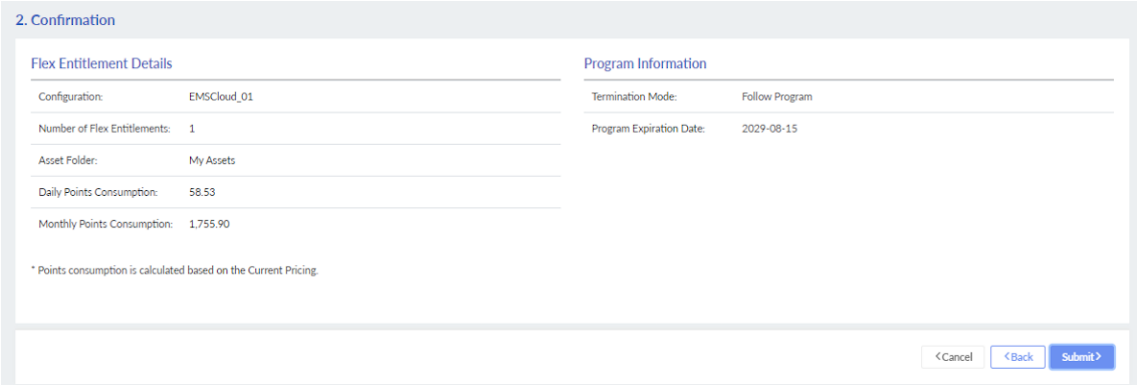


2. Configure the Cloud entitlement.

Product Type	Select one of the following service bundles from the dropdown: • *FortiWeb Cloud* • *FortiClient EMS Cloud* • *FortiSASE* • *FortiEDR MSSP* For information about the product types, see Service offerings on page 14.
Configuration	Select a configuration from the list. See Creating a Cloud service configuration on page 43.
Number of Flex Entitlements	Enter the number of entitlements. See Creating a Cloud service configuration on page 43.
Description	Enter a description.
Termination Mode	• Select *Follow Program* to terminate the machine when the program expires. • Select *User Defined*, and select a date in the calendar to specify the termination date.
Asset Folder	Assign the service to a folder in *My Assets*. For more information about Asset Folders, see Asset Management > Creating custom views. You can use an asset folder to request the next available serial number with the API. See Creating a license pool group on page 39.

3. Click *Next*.

4. Review the *Flex Entitlement Details* and *Program Information*, and click *Submit*.



Injecting the FortiFlex license

You can inject a FortiFlex license into a VM instance via the CLI or during the VM bootstrapping via Cloud-Init (KVM) or OVF template (ESXi).

The commands `execute vm-license-options count` and `execute vm-license-options interval` allow for the customization of license token activation retry parameters. See VM license in the FortiOS Administration Guide for more information.

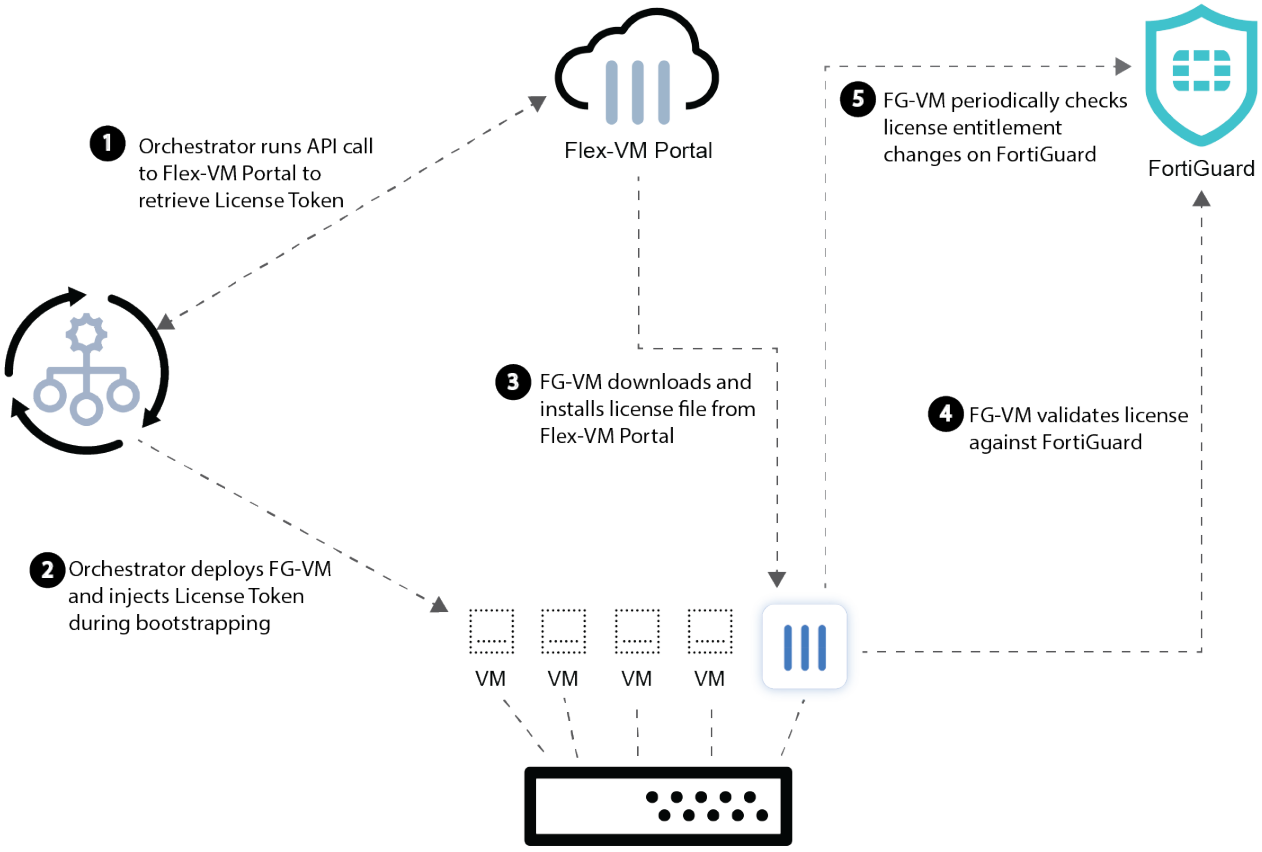
Requisites:

- Create the VM configuration

Injecting the FortiFlex license consists of the following steps:

1. Ensure that the VM has Internet connectivity properly configured.
2. Inject the FortiFlex License Token into the VM using one of the following methods:
   - CLI
   - OVF Template (FGT-64VM only)
   - Cloud-init
   - FortiOS API
3. Confirm that the license token is injected
4. Configuring web proxy tunneling for FDN

FortiFlex License Activation Workflow



Inject a FortiFlex license with the CLI

Use of the following commands to inject a FortiFlex license into a VM instance:

To inject a FortiFlex license with the FortiFlex CLI:

To inject a FortiFlex license into a VM instance with the CLI:

```
execute vm-license <license_token>
```

Example:

```
exec vm-license 58923569A3FFB7F46879
```

To inject a FortiFlex license via web proxy:

```
execute vm-license <license_token> <proxy>
```

The following are examples of the syntax for `<proxy>`:

```
http://user:password@proxyip:proxyport
```

```
user:password@proxyip:proxyport
```

The following shows examples for each command:

```
exec vm-license 58923569A3FFB7F46879 http://qa:123456@10.1.100.74:8080
exec vm-license 95D87F50C075C6F20EE7 hazel:123456@10.1.100.74:8080
```

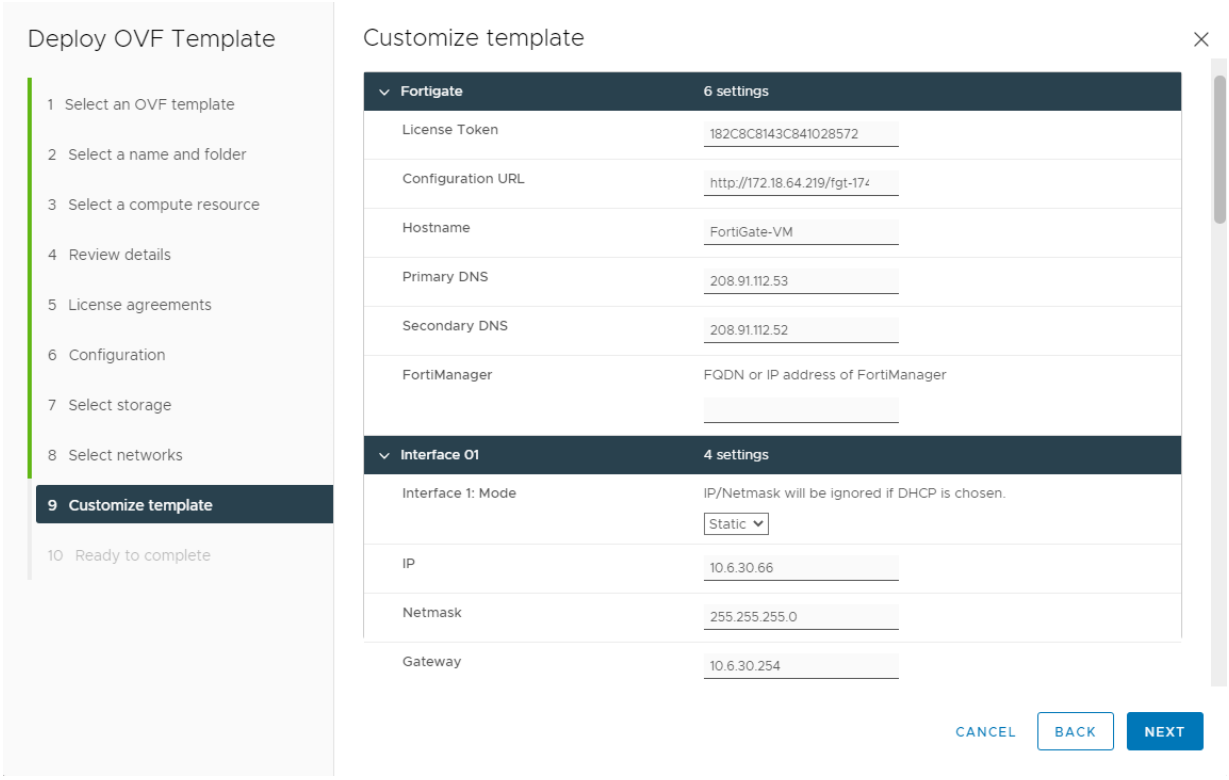
Inject a license token with an OVF template

The custom OVF template contains a *License Token* and *Configuration URL* fields where a bootstrap configuration for the FortiGate is stored.

This option is only available for VMware vCenter.

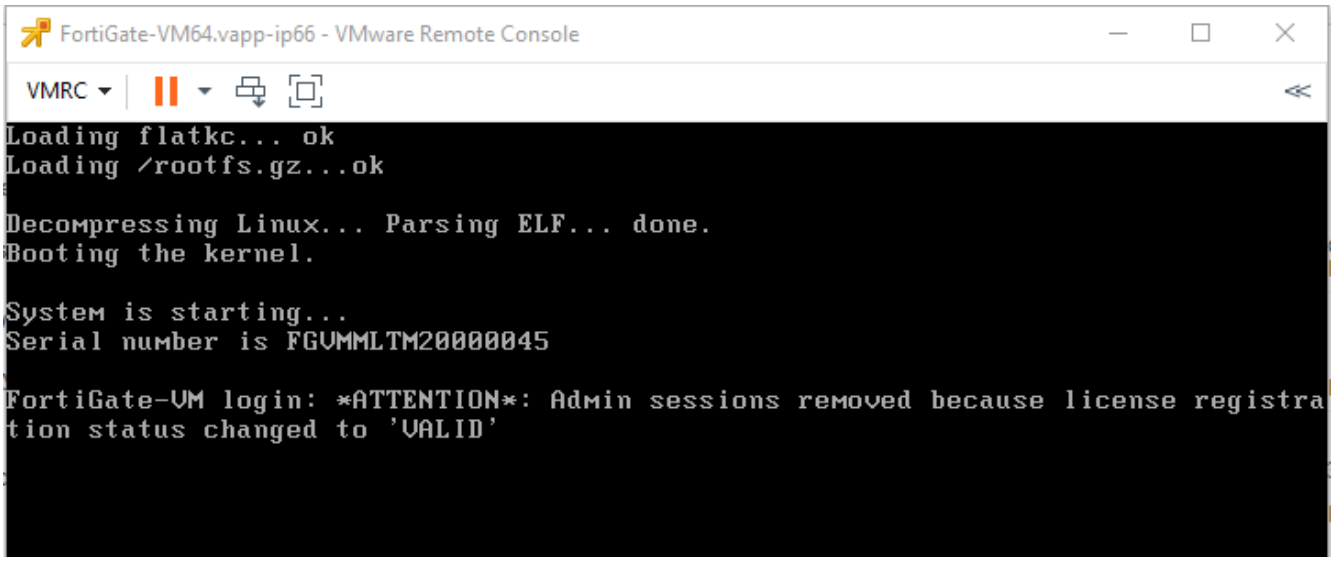
To inject a license token with a custom OVF template:

1. Create a new FGT-VM64 from the vCenter web UI with the extracted files in *FGT_VM64-v7-buildxxxx-FORTINET.out.ovf.zip*.
2. Deploy an OVF Template.
3. In the *Customize template* step:
   a. Enter the License Token in the *License Token* field.
   b. Enter the Configuration URL in the *Configuration URL* field.



4. Restart the VM instance.

After the FGT-VM64 is started, it will activate VM license and load the configuration automatically



Inject a FortiFlex license via cloud-init

The following are the MIME files that you can use to inject a FortiFlex license into a FortiGate-VM instance using cloud-init. See cloud-init Documentation for details.

Configuration information for the FortiGate-VM

```
Content-Type: multipart/mixed; boundary="===============0740947994048919689=="
MIME-Version: 1.0
----------------0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"
config sys glo
set hostname FGT-MSSP-MIME
set admintimeout 480
end
......
```

License token information

```
----------------0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"
LICENSE-TOKEN:FF69500C90C1604F71EE
----------------0740947994048919689==--
```

Injecting with the FortiOS API

The FortiOS API method is useful for automating the migration of existing FortiGate-VM instances into FortiFlex. The FortiFlex API and documentation are available on the Fortinet Developer Network website.

Example: Inject a license via HTTP method:

```
<user_email>:~# curl -k --request POST 'http://<IP_
address>/api/v2/monitor/system/vmlicense/download?token=<token_ID>&access_token=<access_
token>'
{
  "http_method":"POST",
  "status":"success",
  "http_status":200,
  "vdom":"root",
  "path":"system",
  "name":"vmlicense",
  "action":"download",
  "serial":"<serial_number>",
  "version":"v7.2.0",
  "build":1157
```

Example: Inject a license via proxy URL:

```
<user_email>:~# curl -k --request POST 'https://<IP_
address>/api/v2/monitor/system/vmlicense/download?token=<token_ID>&proxy_url=<proxy_
URL>&access_token=<token>'
{
  "http_method":"POST",
  "status":"success",
  "http_status":200,
  "vdom":"root",
  "path":"system",
  "name":"vmlicense",
  "action":"download",
  "serial":"<serial_number>",
  "version":"v7.2.0",
  "build":1157
}<user_email>:~#
```

Confirming the license token is injected

To confirm that the license token is injected:

```
diagnose debug cloudinit show
>> Checking metadata source ovf
>> Found metadata source: ovf
>> Trying to install vmlicense ...
>> License-token:95D87F50C075C6F20EE7 http://qa:123456@10.1.100.74:8080
>> Config script is not available

get system status
Version: FortiGate-VM64 v7.0.4,build0292,220115 (interim)
Serial-Number: FGVMMLTM111111
```

Configuring web proxy tunneling for FDN

After the FortiFlex license has been installed, the FortiGate-VM must validate the license on FDN servers. You can also configure a proxy to accomplish this.

To configure web proxy tunneling for FDN:

```
config system autoupdate tunneling
   set status enable
   set address "<web proxy IP address or FQDN>"
   set port <web proxy port>
   set username "<username>"
   set password <password>
end
```

It may take a while for FortiGate-VM to be able to validate the VM license and update UTM signatures from FortiGuard.

The following shows the output from `get system status` when the FortiGate-VM has completed the validation and update:

```
Version: FortiGate-VM64 v7.0.4,build0292,220115 (interim)
Virus-DB: 89.08825(2022-01-18 21:26)
Extended DB: 89.08825(2022-01-18 21:26)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 2.04168(2022-01-18 18:45)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 19.00243(2022-01-18 01:30)
APP-DB: 19.00243(2022-01-18 01:30)
INDUSTRIAL-DB: 19.00243(2022-01-18 01:30)
IPS Malicious URL Database: 3.00246(2022-01-18 20:50)
Serial-Number: FGVMMLTM111111
License Status: Valid
License Expiration Date: 2022-10-31
VM Resources: 1 CPU/2 allowed, 2007 MB RAM
Log hard disk: Available
Hostname: FGT-DEMO
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 1
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0292
Release Version Information: interim
FortiOS x86-64: Yes
System time: Tue Jan 18 21:46:36 2022
Last reboot reason: warm reboot
```

Managing Flex Entitlements

You can stop and regenerate a license token if it is stolen or compromised. After the token is regenerated, it must be re-injected into your VM to revoke the old token. You can also export a list of tokens to parse them in scripts.

Modifying FortiGate-VM configurations

We recommend rebooting the FortiGate-VM after you change the configuration. To verify the configuration is in effect, run the following CLI command:

```
get system status
```

- A reboot is required if you are lowering the vCPU size.
- A reboot is recommended when adding more vCPU.
  If you do not want to reboot the VM, run the following CLI command:
  ```
  exec cpu add X
  ```
  Where `X` is the number of vCPU to be hot-added on top of the existing number.

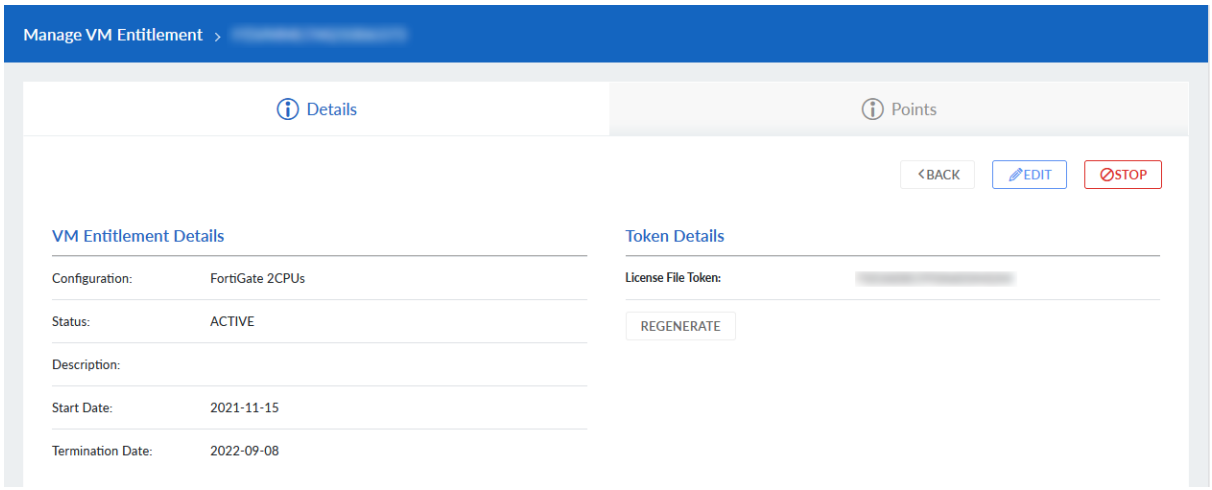
  Example:

  A reboot is not required if the FortiGate-VM currently consumes 4 vCPUs out of the entitled 16 vCPUs which can be seen as `VM Resources: 4 CPU/16 Allowed` in the `get system status` output, and you run `exec cpu add 12` to consume 12 more vCPUs.

Starting in FortiOS 7.2.4, vCPU changes in the FortiFlex licenses are automatically handled by the FortiGate-VM instances. Running `exec cpu add X` is no longer required if you are running FortiOS v7.2.4.

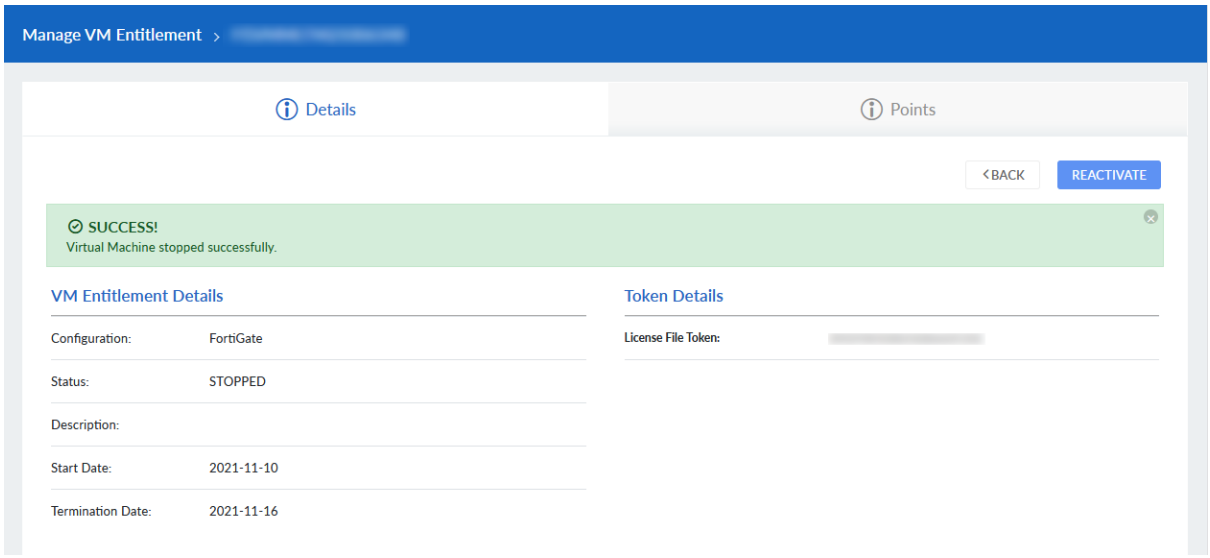
To stop a VM Entitlement:

1. Go to *Flex Entitlements*, and click the serial number you want to stop.
2. Click *Stop*. The *Stop VM Entitlement* dialog opens.



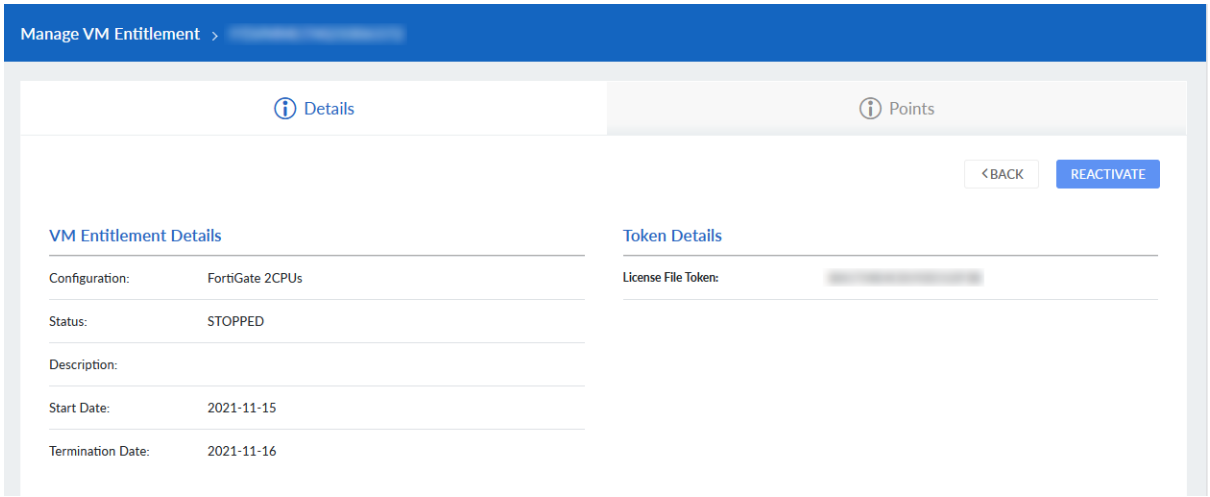
3. Click *Confirm*. The VM status changes to *STOPPED*. Point consumption will stop from the next day even while your

managed VM may be still running.

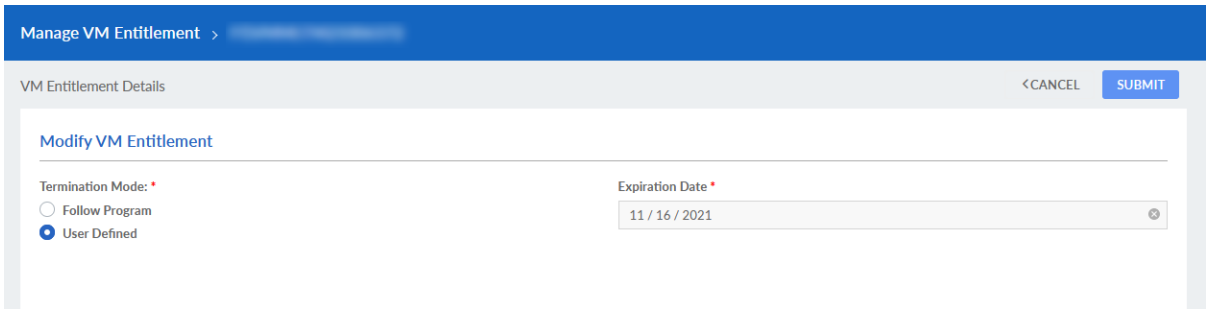


To reactivate a VM Entitlement:

1. Go to *Flex Entitlements* and click a serial number with a status of *STOPPED*.
2. Click *Reactivate*. The *Virtual Machine Details* page opens.



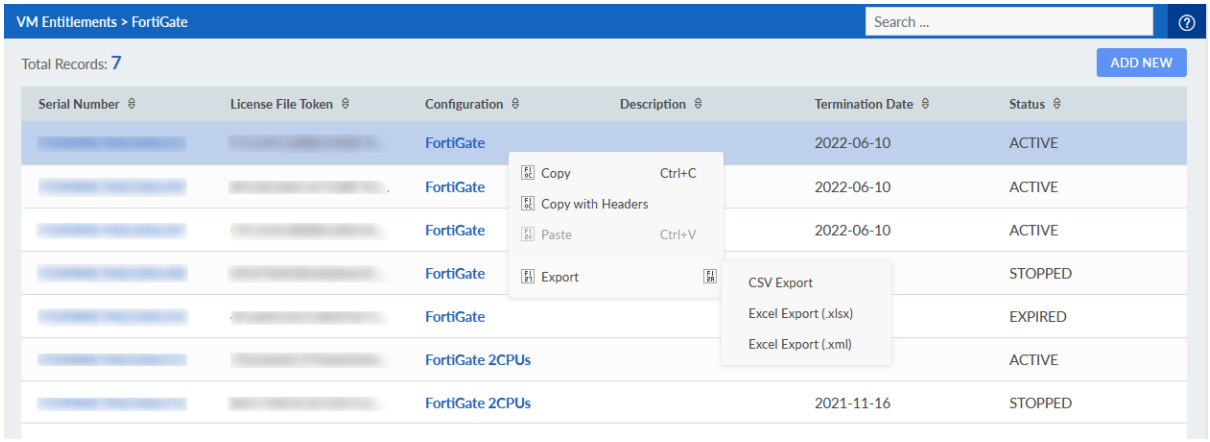
3. (Optional) Modify the VM Entitlement details.



4. Click *Submit*. The serial number *Status* changes to *Active*. Point consumption will restart from the day you make this change even though you may still have not rerun your managed VM.

To export a list of serial numbers and tokens:

1. Go to *Flex Entitlements*.
2. Right-click the table, and click *Export*.
3. Select *CSV Export*, *Excel Export (xlsx)*, or *Excel Export (.xml)*. The file is saved to your computer.



Creating a license pool group

A licence pool group allows you to request the next availble serial number in the pool. When a VM is decomissioned, the license is returned to the pool.

Requirements:

- Access to Asset Management
- Fortinet Developer Network membership

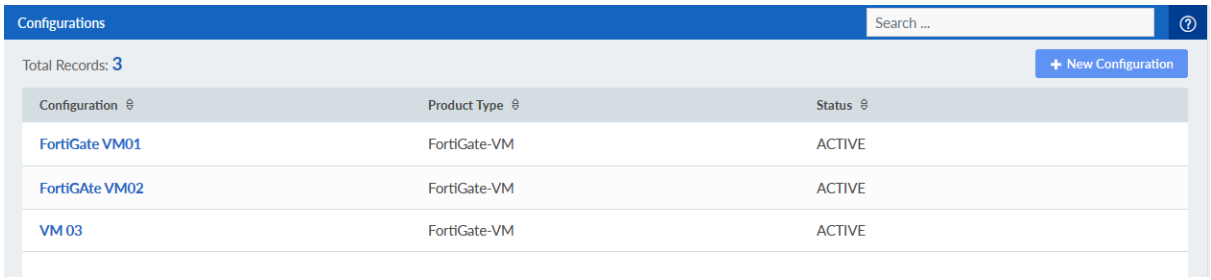
To create a license pool group:

1. In Asset Management, create an Asset Folder for the asset pool group. See Creating custom views.
2. Create a VM Entitlement and select a folder for the group. See, Creating entitlements on page 26.
3. Use the Virtual Machines API to `create` and add a `folderpath` to the asset folder in *My Assets*.
4. Create a new endpoint to return the group information.
5. Create a new endpoint to return the next available token.

Configurations

The *Configurations* tab is used to create and manage configurations. You can set the number of vCPUs in a virtual machine, and select a service package. After the configuration is created, it can be assigned to a entitlement. See Creating configurations on page 40.

When you disable a configuration, the entitlements that are using the configuration are no longer entitled to consume points. Use caution when disabling configurations or stopping entitlements, as this will impact the performance of the virtual machines, devices, or services. Disabled configurations can be re-enabled.



Creating configurations

Create configurations to be used in VM, hardware device, and cloud service entitlements.

This section includes:

- Creating a VM configuration on page 40
- Creating a hardware appliance configuration on page 42
- Creating a Cloud service configuration on page 43

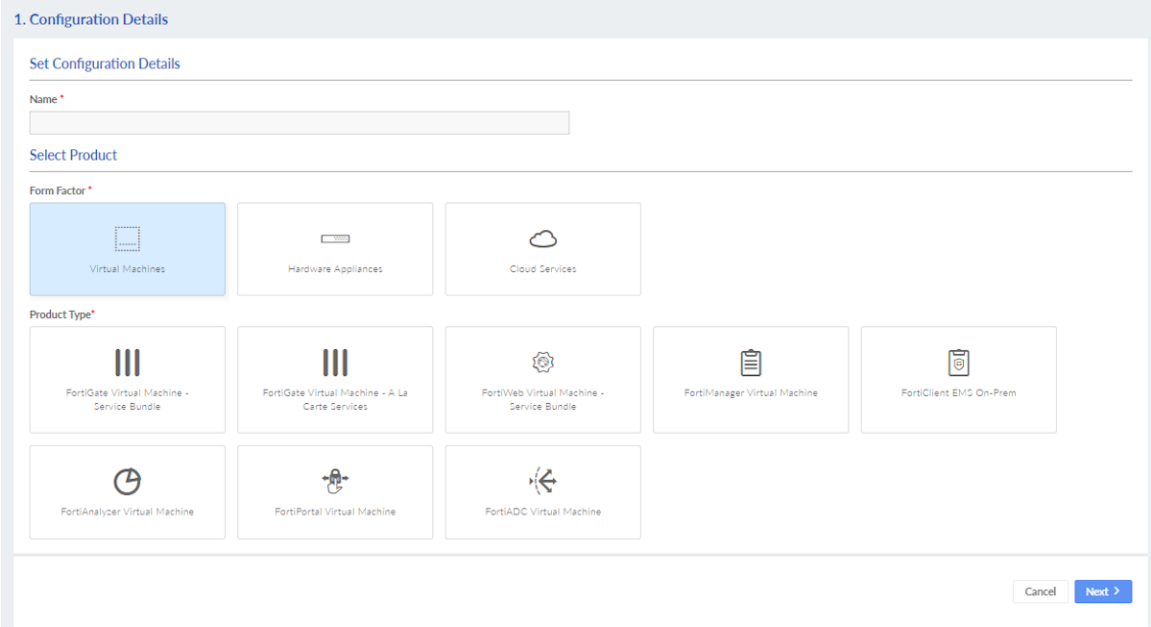
Creating a VM configuration

Specify the number of vCPUs and service package to use in a VM entitlement. See Creating VM entitlements on page 26.

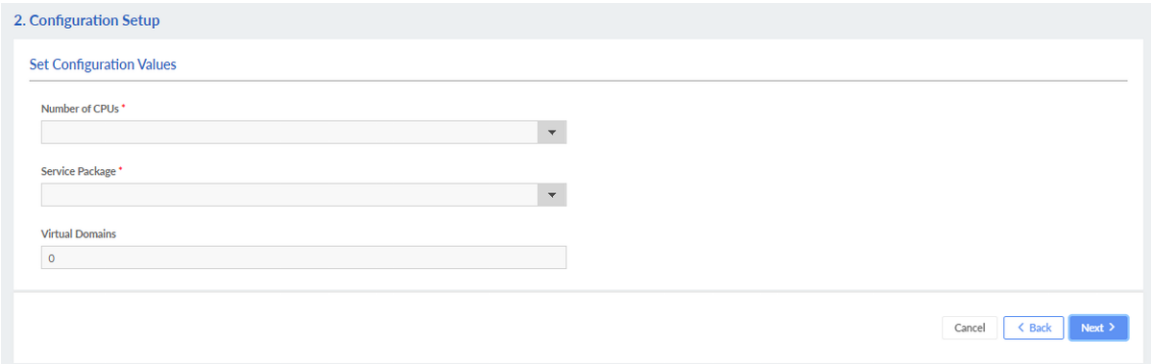
To create a VM configuration:

1. Go to *Configurations*, and click *New Configuration*.
2. In the *Configuration Details* page, set the configuration details and click *Next*.

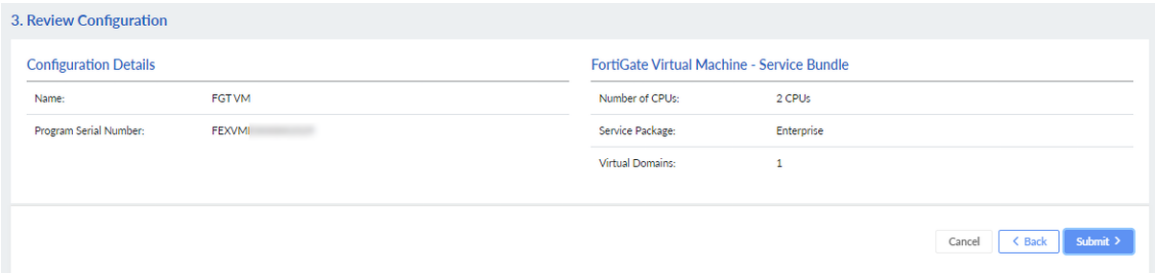
Name	Enter a configuration name.
Form Factor	*Virtual Machines*
Product Type	Select one of the following options: • *FortiGate Virtual Machine - Service Bundle* • *FortiGate Virtual Machine - A La Carte Services* • *FortiWeb Virtual Machine - Service Bundle* • *FortiManager Virtual Machine* • *FortiClient EMS On-Prem* • *FortiAnalyzer Virtual Machine* • *FortiPortal Virtual Machine* • *FortiADC Virtual Machine* For information, see Service offerings on page 14.



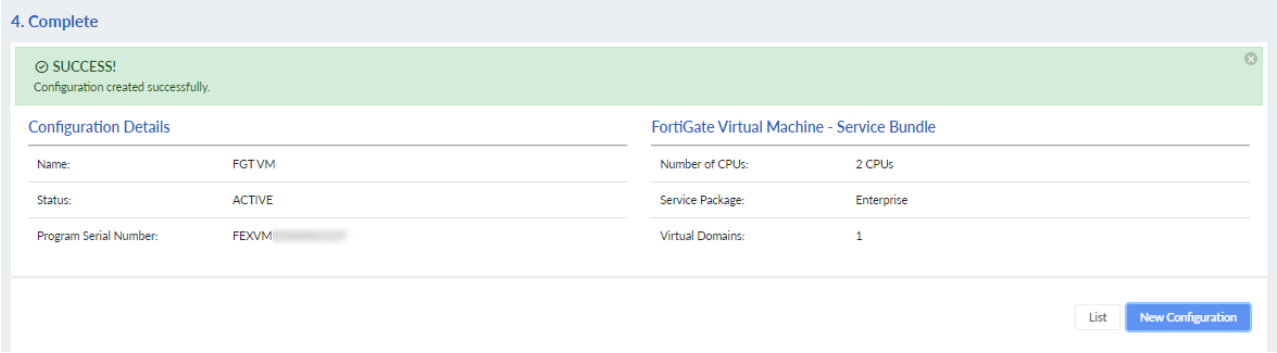
3. In the *Configuration Setup* page, set the service details and click *Next*. For more information, see Configuration details on page 45.



4. Review the configuration details, and click *Submit*.



The configuration is created. Points start to be consumed on the same day even though your managed VM may still not be created or running.



5. Click *List* to view the configuration in the *Configurations* tab.

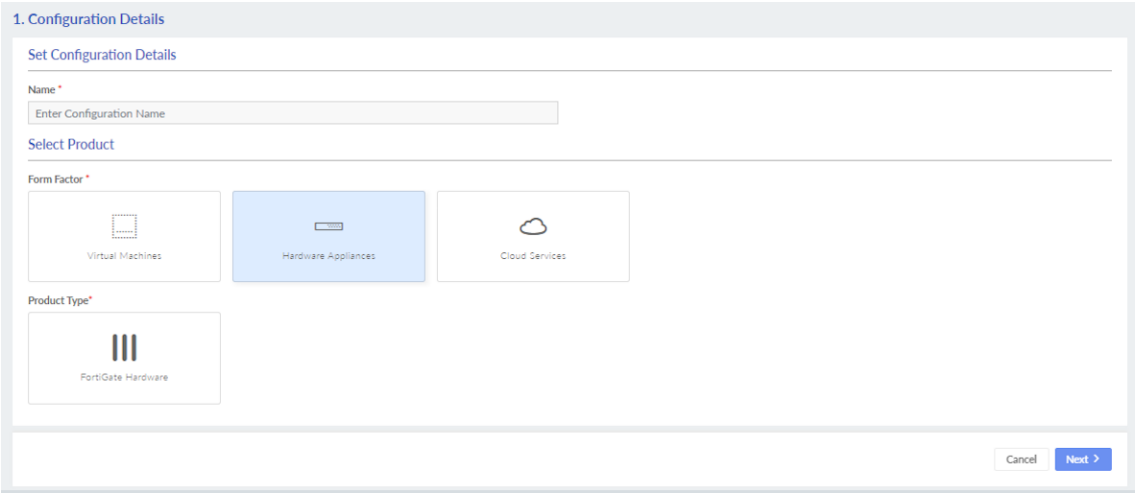
Creating a hardware appliance configuration

Specify the device model and service package to use in a hardware device entitlement. See Creating hardware device entitlements on page 28.

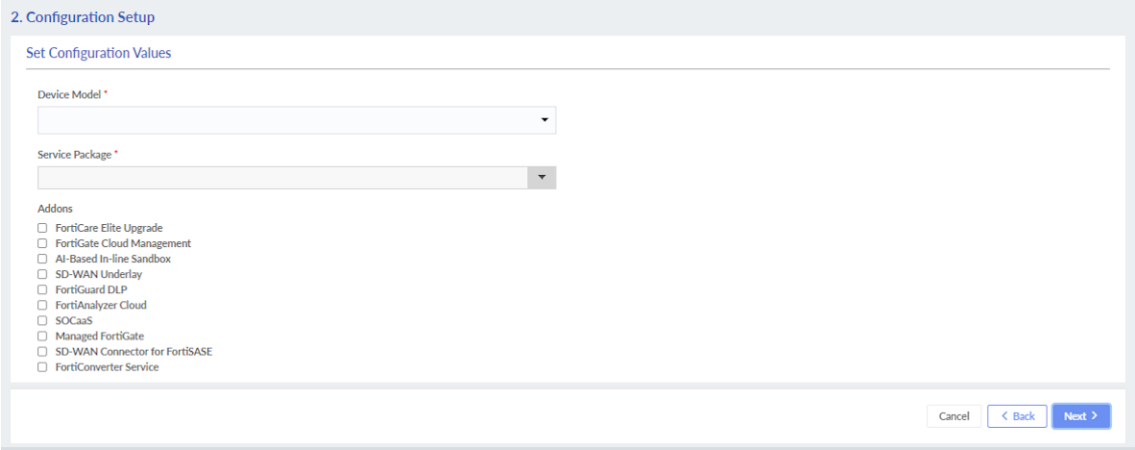
To create a hardware appliance configuration:

1. Go to *Configurations*, and click *New Configuration*.
2. In the *Configuration Details* page, set the configuration details and click *Next*.

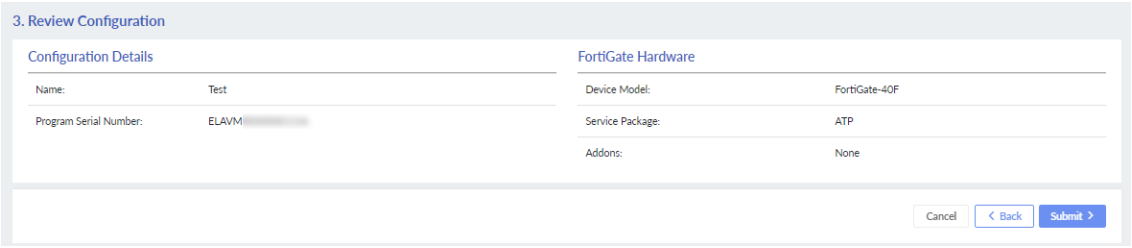
Name	Enter a configuration name.
Form Factor	*Hardware Appliances*
Product Type	Select the following option: • *FortiGate Hardware* For information, see Service offerings on page 14.



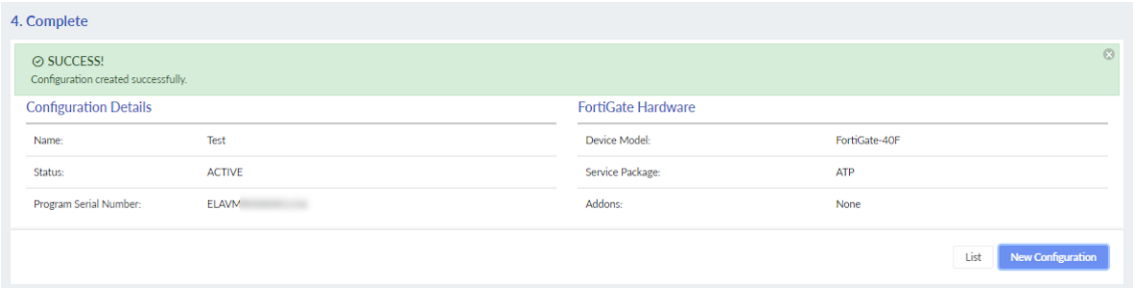
3. In the *Configuration Setup* page, set the service details and click *Next*. For more information, see Configuration details on page 45.



4. Review the configuration details, and click *Submit*.



The configuration is created. Points start to be consumed on the same day even though your managed hardware may still not be running.



5. Click *List* to view the configuration in the *Configurations* tab.

Creating a Cloud service configuration

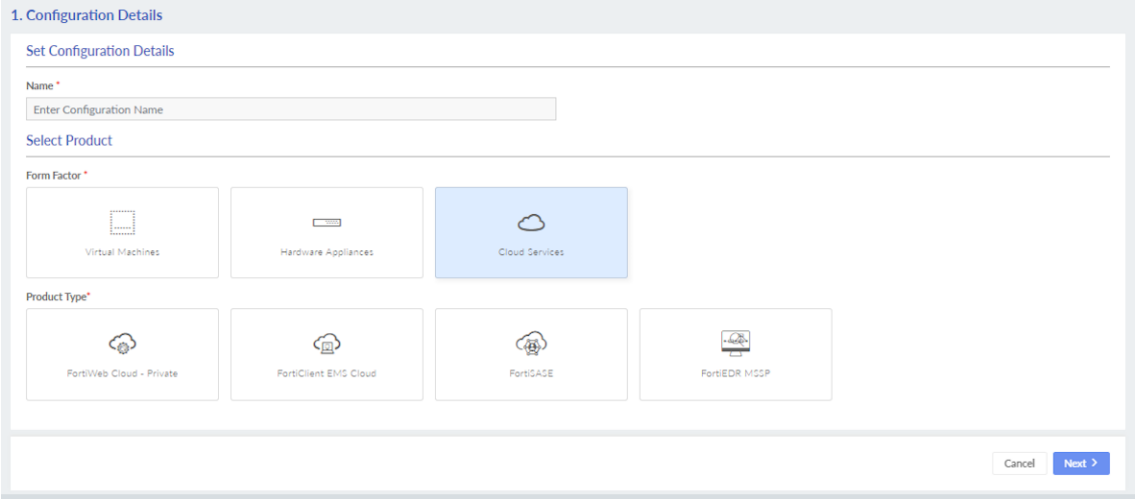
Specify the users, endpoints, service package, and bandwidth for a Cloud service entitlement. See Creating Cloud service entitlements on page 29.

To create a Cloud service configuration:

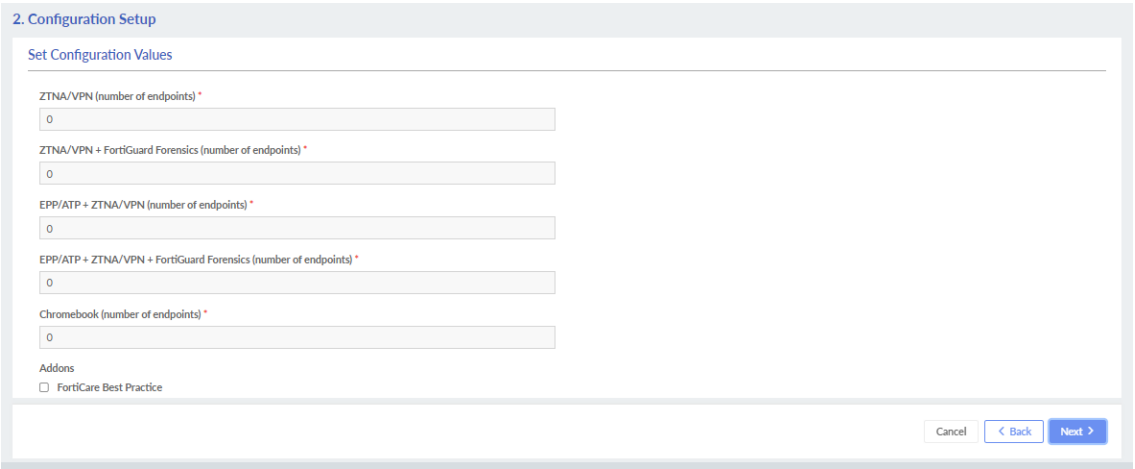
1. Go to *Configurations*, and click *New Configuration*.
2. In the *Configuration Details* page, set the configuration details and click *Next*.

Name	Enter a configuration name.
Form Factor	*Cloud Services*

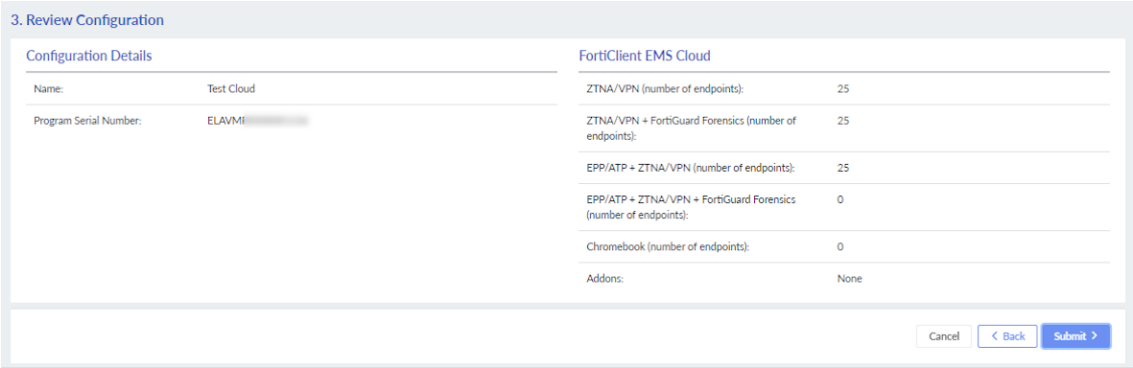
Product Type	Select one of the following options: • *FortiWeb Cloud* • *FortiClient EMS Cloud* • *FortiSASE* • *FortiEDR MSSP* For information, see Service offerings on page 14.



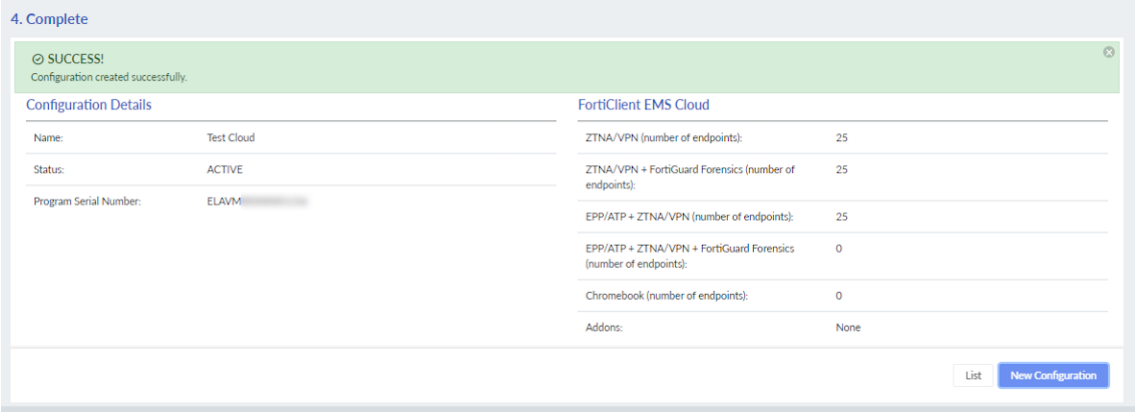
3. In the *Configuration Setup* page, set the service details and click *Next*. For more information, see Configuration details on page 45.



4. Review the configuration details, and click *Submit*.



The configuration is created. Points start to be consumed on the same day even though your managed cloud service may still not be running.



5. Click *List* to view the configuration in the *Configurations* tab.

Configuration details

This topic includes configuration details of the following:

- Virtual Machines on page 45
- Hardware Appliances on page 48
- Cloud Services on page 52

Virtual Machines

FortiGate Virtual Machine - Service Bundle

Number of CPUs	Enter the number of CPUs.
Service Package	Select one of the following options: • *FortiCare Premium* • *UTM* • *Enterprise* • *ATP*

Virtual Domains	Enter the number of virtual domains.
FortiGuard Services	Select from the following options: • *Advanced Malware Protection* • *AI-Based In-line Sandbox* • *FortiGuard OT Security Service* • *FortiGuard DLP* • *FortiGuard Attack Surface Security Service* • *FortiConverter Service*
Cloud Services	Select from the following options: • *FortiGate Cloud Management* • *SD-WAN Underlay* • *SOCaaS* • *FortiAnalyzer Cloud* • *Cloud-based Overlay-as-a-Service* • *SD-WAN Connector for FortiSASE*
Support Services	Select one of the following options: • *FC Elite Upgrade*
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

FortiGate Virtual Machine - A La Carte Services

Number of CPUs	Enter the number of CPUs.
FortiGuard Services	Select from the following options: • *Intrusion Prevention* • *Advanced Malware Protection* • *FortiGuard Attack Surface Security Service* • *FortiGuard OT Security Service* • *DLP* • *AI-Based InLine Sandbox* • *Web, DNS & Video Filtering* • *FortiConverter Service*
Cloud Services	Select from the following options: • *FortiGate Cloud* • *SD-WAN Underlay* • *FortiAnalyzer Cloud with SOCaaS* • *FortiAnalyzer Cloud* • *SD-WAN Connector for FortiSASE* • *Cloud-based Overlay-as-a-Service*
Support Services	Select one of the following options: • *FortiCare Premium* • *FortiCare Elite*
Virtual Domains	Enter the number of Virtual Domains.

	The FortiGate VM will report two Virtual Domains (VDOMs) due to its native ability to create an admin VDOM. The number of VDOMs added in FortiFlex is in addition to these two VDOMs. For example, if you add one VDOM in FortiFlex, the VM will report three VDOMs.
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

FortiWeb Virtual Machine - Service Bundle

Number of CPUs	Select the number of CPUs from the dropdown.
Service Package	Select *Standard* or *Advanced*.
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

FortiManager Virtual Machine

Number of managed devices	Enter the number of managed devices.
Number of ADOMs	Enter the number of ADOMs. FortiManager comes with a base of five ADOMs, per a normal subscription. Therefore, the number of ADOMs is additional to this base. For example, if you add one ADOM in FortiFlex, the FortiManager VM is capable of six.
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

After creating an entitlement which contains any of the Cloud Services, you can refer to the following on-boarding guides for further instructions:

- FortiGate Cloud
- FortiManager Cloud
- FortiAnalyzer Cloud

FortiClient EMS On-Prem

ZTNA/VPN	Enter the number of endpoints.
EPP/ATP + ZTNA/VPN	Enter the number of endpoints.
Chromebook	Enter the number of endpoints.
Support Services	Select a support service: • *FortiCare Premium*
Addons	Select an add on: • *FortiCare Best Practice*
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

FortiAnalyzer Virtual Machine

Daily Storage (GB)	Use the toggle to set the select the number of GB of daily storage.
Number of ADOMs	Use the toggle to set the select the number of ADOMS. FortiAnalyzer comes with a base of five ADOMs, per a normal subscription. Therefore, the number of ADOMs is additional to this base. For example, if you add one ADOM in FortiFlex, the FortiAnalyzer VM is capable of six.
Support Services	Select a support service: • *FortiCare Premium*
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

FortiAnalyzer comes with IOC, the Security Automation Service, and the FortiGuard Outbreak Detection Service. These additional services cannot be detached or purchased a-la-carte.

FortiPortal Virtual Machine

Number of managed devices	Use the toggle to set the select the number of managed devices.
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

FortiADC Virtual Machine

Number of CPUs	Select the number of CPUs from the dropdown.
Service Package	Select the service package from the dropdown: • *Standard* • *Advanced* • *FortiCare Premium*
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

Hardware Appliances

FortiGate Hardware

Device Model	Select one of the device models from the dropdown: • *FortiWifi-40F* • *FortiWifi-40F-3G4G* • *FortiWifi-60F* • *FortiWifi-61F* • *FortiWifi-80F-2R*

- *FortiWifi-80F-2R-3G4G-DSL*
- *FortiWifi-81F-2R*
- *FortiWifi-81F-2R-3G4G-DSL*
- *FortiWifi-81F-2R-3G4G-PoE*
- *FortiWifi-81F-2R-POE*
- *FortiGateRugged-35D*
- *FortiGateRugged-60F*
- *FortiGateRugged-60F-3G4G*
- *FortiGateRugged-70F*
- *FortiGateRugged-70F-3G4G*
- *FortiGate-40F*
- *FortiGate-40F-3G4G*
- *FortiGate-60E*
- *FortiGate-60E-DSL*
- *FortiGate-60E-POE*
- *FortiGate-60F*
- *FortiGate-61E*
- *FortiGate-61F*
- *FortiGate-70F*
- *FortiGate-71F*
- *FortiGate-80E*
- *FortiGate-80E-POE*
- *FortiGate-80F*
- *FortiGate-80F-PoE*
- *FortiGate-80F-Bypass*
- *FortiGate-80F-DSL*
- *FortiGate-81E*
- *FortiGate-81E-POE*
- *FortiGate-81F*
- *FortiGate-81F-PoE*
- *FortiGate-90E*
- *FortiGate-90G*
- *FortiGate-91E*
- *FortiGate-91G*
- *FortiGate-100E*
- *FortiGate-100F*
- *FortiGate-101E*
- *FortiGate-101F*
- *FortiGate-200E*
- *FortiGate-200F*
- *FortiGate-201E*

- *FortiGate-201F*
- *FortiGate-300E*
- *FortiGate-301E*
- *FortiGate-400E*
- *FortiGate-400E-BYPASS*
- *FortiGate-400F*
- *FortiGate-401E*
- *FortiGate-401E-DC*
- *FortiGate-401F*
- *FortiGate-600E*
- *FortiGate-600F*
- *FortiGate-601E*
- *FortiGate-601F*
- *FortiGate-900G*
- *FortiGate-901G*
- *FortiGate-1000F*
- *FortiGate-1001F*
- *FortiGate-1100E*
- *FortiGate-1100E-DC*
- *FortiGate-1101E*
- *FortiGate-1800F*
- *FortiGate-1800F-DC*
- *FortiGate-1801F*
- *FortiGate-1801F-DC*
- *FortiGate-2000E*
- *FortiGate-2200E*
- *FortiGate-2201E*
- *FortiGate-2500E*
- *FortiGate-2600F*
- *FortiGate-2600F-DC*
- *FortiGate-2601F*
- *FortiGate-2601F-DC*
- *FortiGate-3000F*
- *FortiGate-3000F-DC*
- *FortiGate-3001F*
- *FortiGate-3001F0DC*
- *FortiGate-3200F*
- *FortiGate-3201F*
- *FortiGate-3300E*
- *FortiGate-3301E*
- *FortiGate-3400E*

	• *FortiGate-3400E-DC* • *FortiGate-3500F* • *FortiGate-3501F* • *FortiGate-3600E* • *FortiGate-3600E-DC* • *FortiGate-3601E* • *FortiGate-3700F* • *FortiGate-3701F* • *FortiGate-3960E* • *FortiGate-3980E* • *FortiGate-3980E-DC* • *FortiGate-4200F* • *FortiGate-4200F-DC* • *FortiGate-4400F* • *FortiGate-4400F-DC* • *FortiGate-4401F* • *FortiGate-4800F* • *FortiGate-4800F-DC* • *FortiGate-4801F* • *FortiGate-4801F-DC*
Service Package	Select one of the following options: • *FortiCare Premium* • *FortiCare Elite* • *ATP* • *UTP* • *Enterprise*
Addons	Select an add on: • *FortiCare Elite Upgrade* • *FortiGate Cloud Management* • *AI-Based In-line Sandbox* • *SD-WAN Underlay* • *FortiGuard DLP* • *FortiAnalyzer Cloud* • *SOCaaS* • *Managed FortiGate* • *SD-WAN Connector for FortiSASE* • *FortiConverter Service* • *FortiGuard OT Security Service* • *SD-WAN Overlay-as-a-Service*
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

Hardware entitlements cannot be applied to a hardware FortiGate with an active license. You must either:

- Wait for the FortiGate to expire and then apply the FortiFlex license. There is a 48-hour grace period after the license expires where security subscriptions and FortiGuard will continue to work.
- Request Customer Service to de-register the device. This option does not grant the 48-hour grace period. Once it is de-registered, the FortiGate will be unable to receive security updates or utilize FortiGuard services.

Cloud Services

FortiWeb Cloud - Private

Average Throughput	Select average throughput measured by the 95th percentile from the dropdown, between 10 Mbps to 10 Gbps.
Web Applications	Enter the number of web applications, between 1 and 2000.

FortiWeb Cloud - Public

Average Throughput	Select average throughput measured by the 95th percentile from the dropdown, between 10 Mbps to 10 Gbps.
Web Applications	Enter the number of web applications, between 1 and 2000.

FortiClient EMS Cloud

ZTNA/VPN	Enter the number of endpoints.
ZTNA/VPN + FortiGuard Forensics	Enter the number of endpoints.
EPP/ATP + ZTNA/VPN	Enter the number of endpoints.
EPP/ATP + ZTNA/VPN + FortiGuard Forensics	Enter the number of endpoints.
Chromebook	Enter the number of endpoints.
Addons	Select an add on: • *FortiCare Best Practice*
Number of Flex Entitlements	Enter the number of FortiFlex entitlements.

FortiSASE

Number of users	Enter the number of users.
Service Package	Select a service package: • *Standard*

	• *Advanced*
Bandwidth (Mbps)	Enter amount of bandwidth required.
Dedicated IPs	Enter the number of dedicated IP addresses.

FortiEDR MSSP

Service Package	Select a service package: • *Discover/Protect/Respond*
Addons	Select an add on: • *XDR* The number of EDR and XDR endpoints will be the same when creating a configuration.

Deployment examples and scripts

The following section provides an example of a manual deployment for KVM as well as links to sample scripts to automate deployments for KVM.

- Manual deployment on KVM on page 53
- Automatic deployments on page 60

Manual deployment on KVM

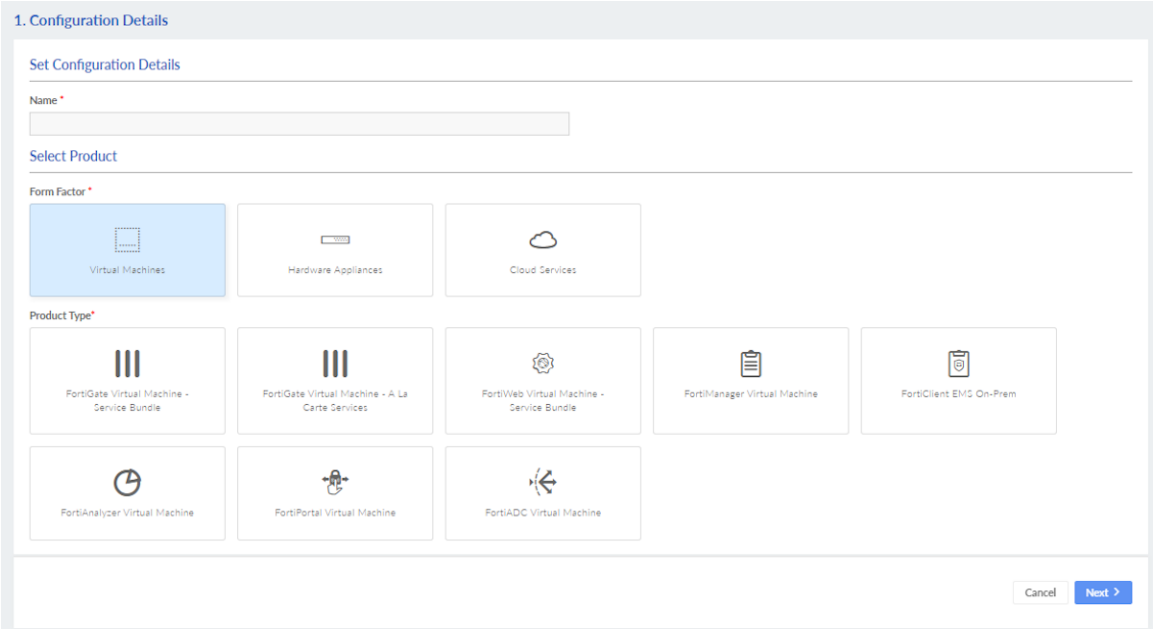
Activate a FortiGate VM using a FortiFlex license. FortiFlex allows for adhoc license via its portal.

Step 1. Create the FortiFlex configuration.

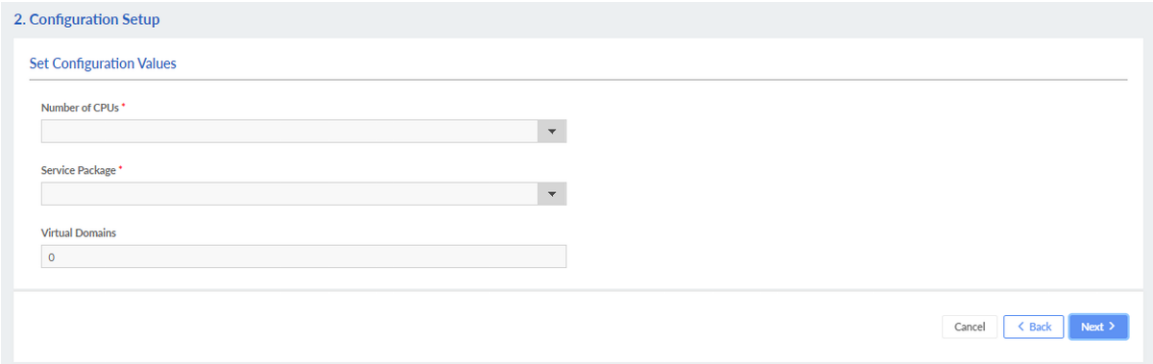
To create a FortiFlex configuration:

1. Open the FortiFlex portal.
2. Go to *Configurations* and click *New configuration*.

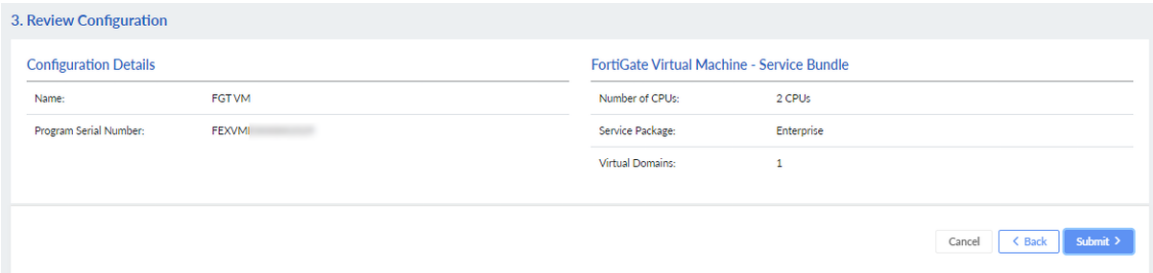
3. In the *Configuration Details* page, enter a name for the configuration and the product type and click *Next*.



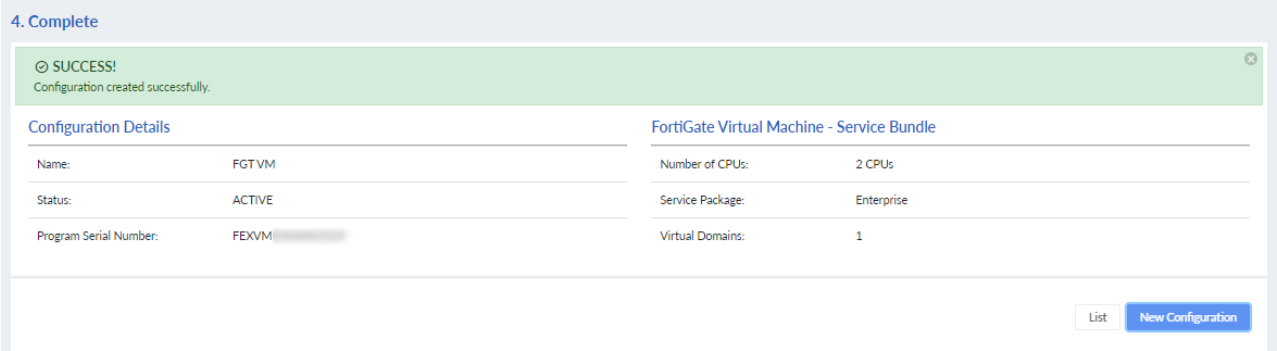
4. Set the configuration values and click *Next*.



5. On the *Review configuration* page, click *Submit*.



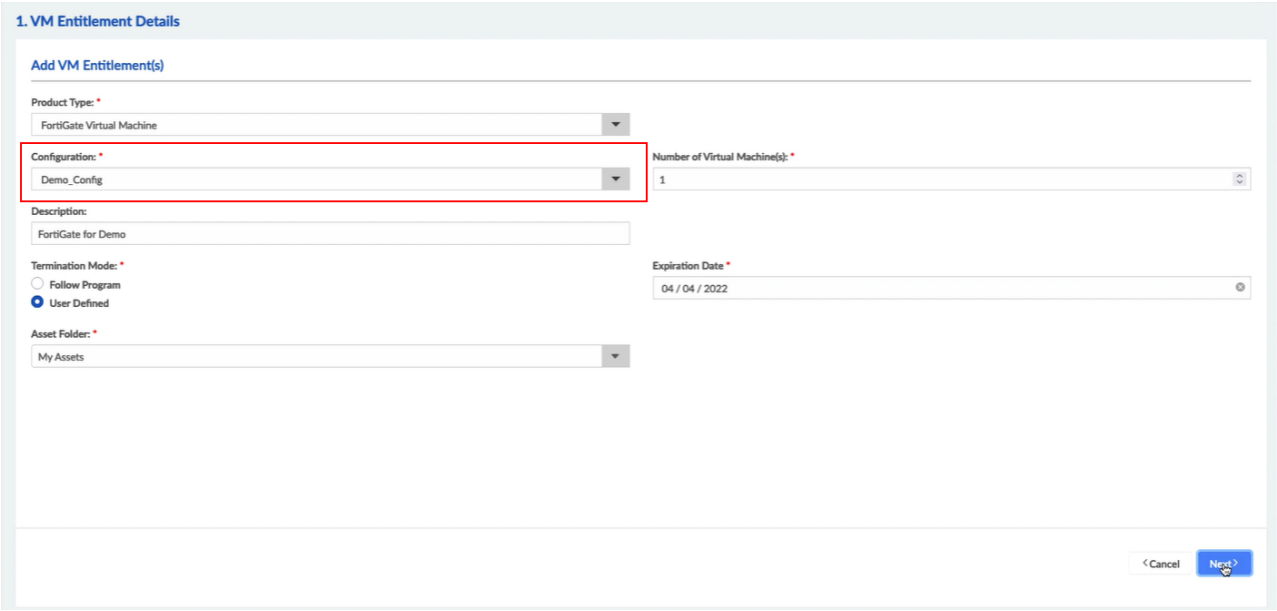
The configuration is complete.



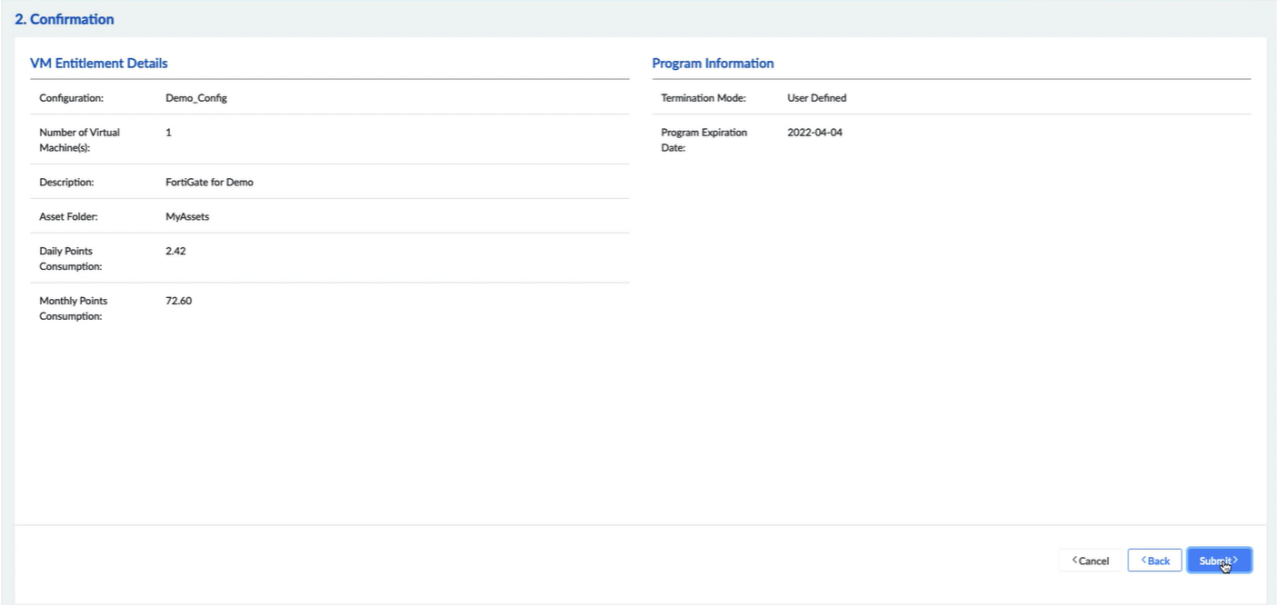
Step 2. Create the license entitlement

To create a license entitlement:

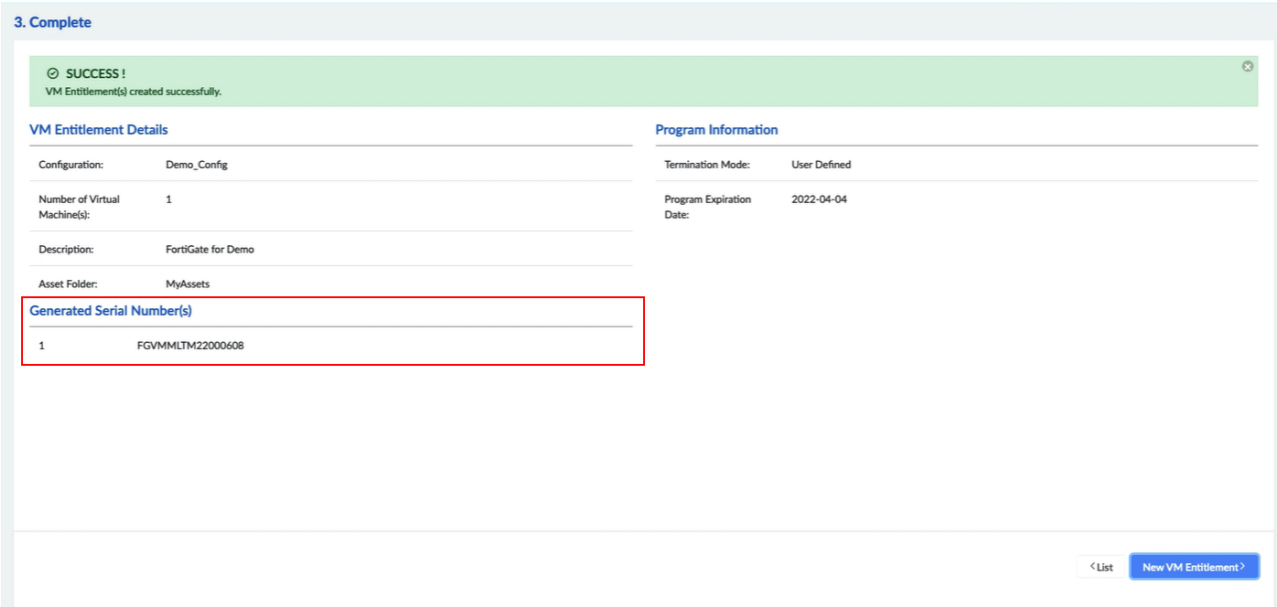
1. Go to *VM Entitlements* and click *New VM Entitlement*.
2. In the *VM Entitlement Details* page, from the *Configuration* list, select the configuration you created in Step 1 and click *Next*.



3. On the *Confirmation* page, click *Submit*.

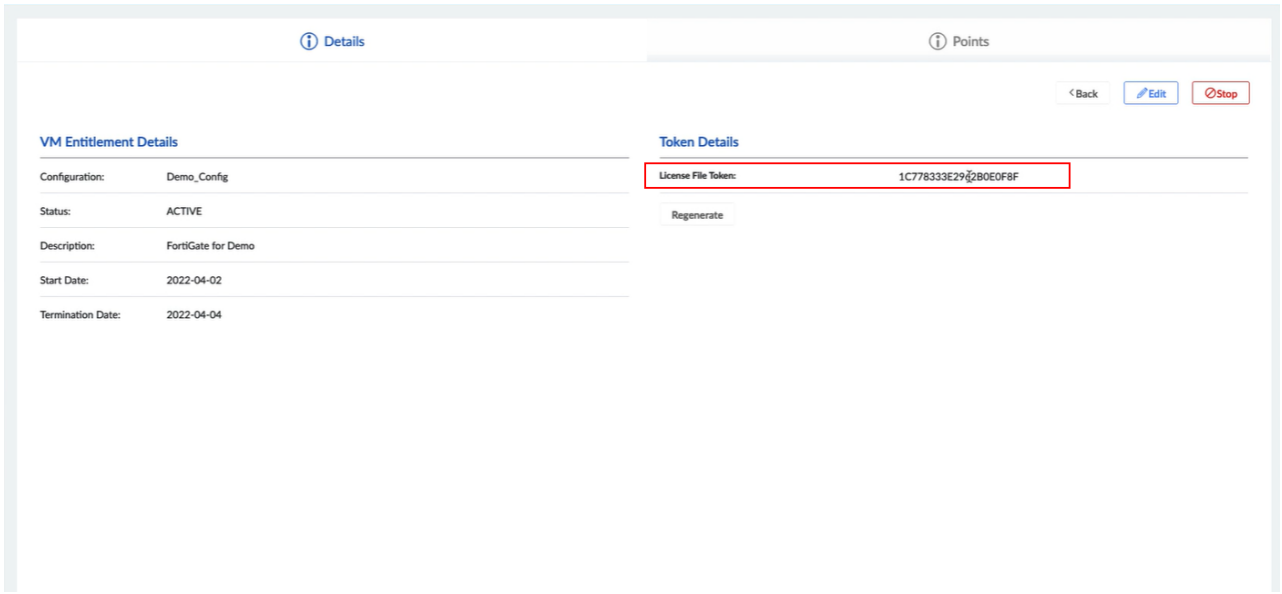


The license entitlement is created. The serial number is displayed under *Generated Serial Number(s)*.



4. Go to *VM Entitlements* and search for the Serial Number you generated. Click the Serial Number to view the Product details.

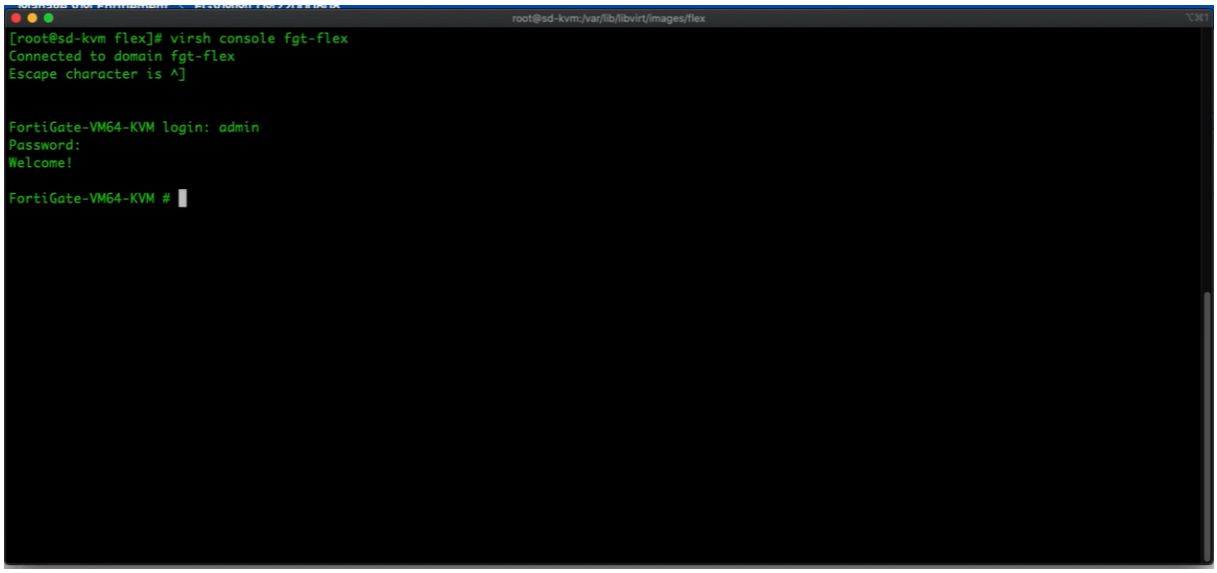
5. In the *Details* page, copy the *License File Token*. You will need this token to activate the FortiGate VM instance.



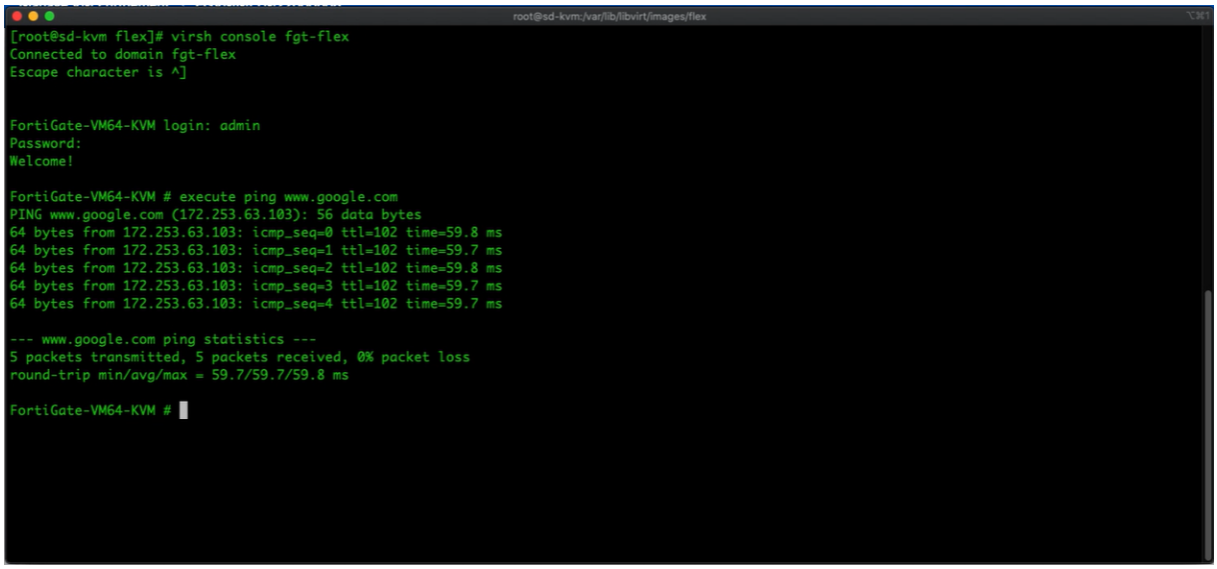
Step 3: Configure the VM

To configure the VM:

1. Open the KVM host which has already deployed the FortiGate VM and connect to it.

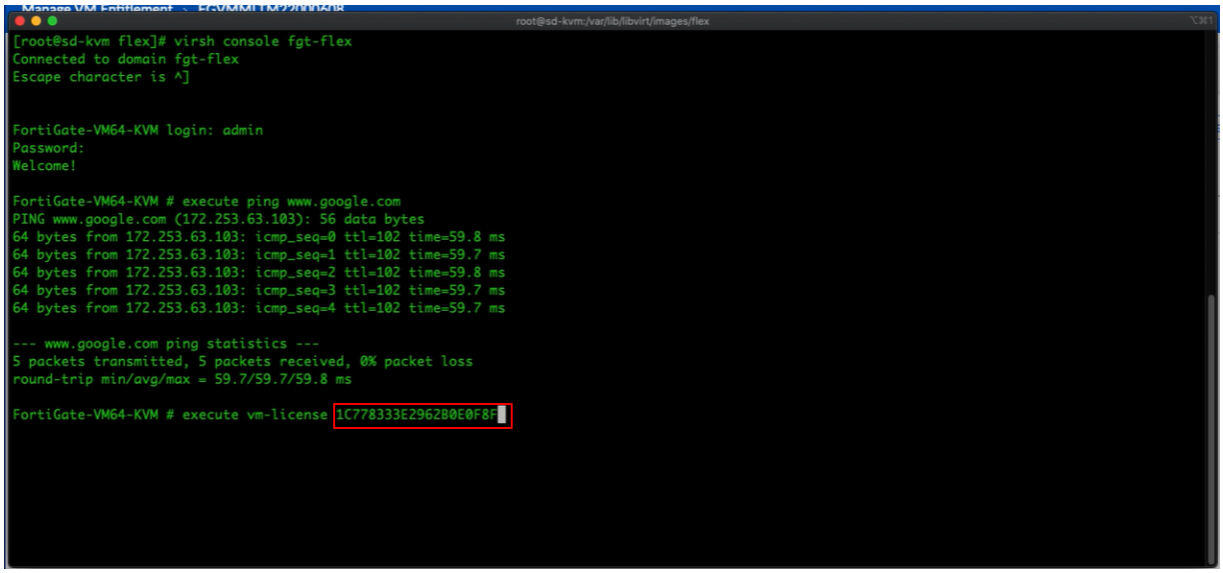


2. Confirm the VM is connected to the Internet.

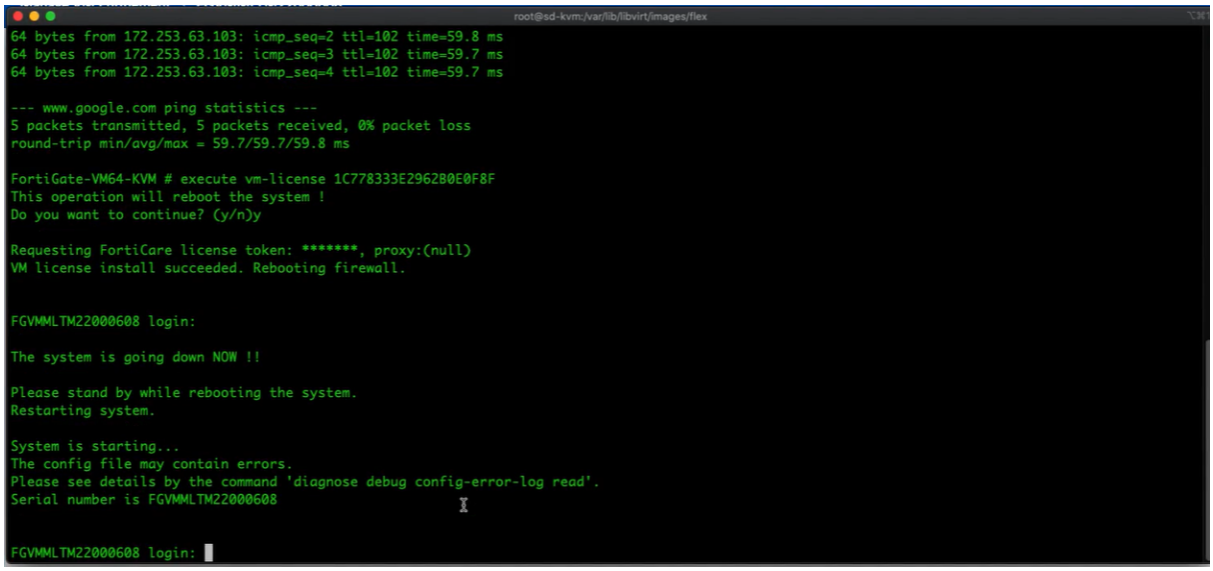


3. Activate the license with the following command:

```
execute vm-license <license_token>
```

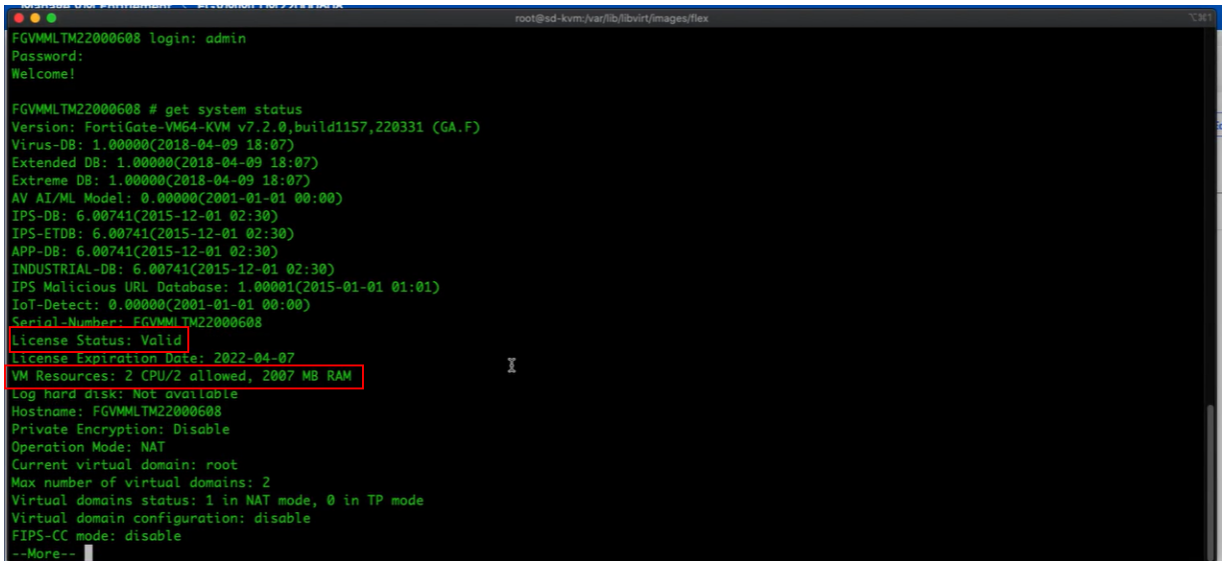


4. When prompted enter `y` to allow the VM to reboot to activate the new license. The VM reboots and the license is validated against the FortiGaurd servers.



5. To confirm the license and configuration, run the following command:

```
get system status
```



Automatic deployments

Customers with access to Orchestrator tools can the use FortiFlex API to automate the FortiGate deployment and activation.

Automatic deployment on KVM

Automate the FortiGate deployment and activation on HyperVisor using a python script and the KVM cloud-init capabilities.

A Python script with examples of the basic calls for the FortiFlex API is available in the Fortinet Developer Network (FNDN). To view the script, log in to FNDN and search for the following article: *Sample Python Script for Flex-VM API*.

Automation

The topics in this section provide information about automation and the FortiFlex API:

- FortiFlex API on page 61
- FortiFlexVM Terraform provider on page 63
- Ansible Collection on page 63

FortiFlex API

Instead of making changes to your FortiFlex objects in the FortiCloud portal, you can automate tasks, such as creating VMs and entitlements, with an API when integrating with cloud orchestration platforms.

FortiFlex API information can also be found on the Fortinet Developer Network along with sample Python script.

When implementing the FortiFlex API, you can follow this general process:

1. Create an API user.
2. Acquire the API token.
3. Run API calls against the FortiFlex portal to view, create, or modify objects.

Before you begin, ensure that you have a FortiCloud account and have FortiFlex activated.

To create an API user:

1. Go to https://support.fortinet.com.
2. Go to *Services* > *IAM*.
3. Create an active permission profile that includes the FortiFlex portal. See Creating a permission profile in the Identity & Access Management (IAM) guide.

   Actions that involve changing or creating data, such as creating a new configuration or updating a VM, will require read and write permissions or above.

4. Create an API user with the permission profile from the previous step applied. See Adding an API user in the Identity & Access Management (IAM) guide.
5. Click *Download Credentials* and set a password. A CSV file with the API user's credentials is downloaded that can only be opened with the password. See Adding an API user in the Identity & Access Management (IAM) guide.

Downloading API user credentials will reset the user's security credentials each time you perform this action. Any previous password will become invalid.

To acquire the API token:

1. Open the Postman app.

The Postman API Toolkit can be found at https://www.postman.com. FortiFlex Postman collections can also be found on GitHub.

2. Click *Create a request*.
3. Enter the following information:

Method	POST
URL	https://customerapiauth.fortinet.com/api/v1/oauth/token/

4. Click *Body*.
5. Select *raw* and *JSON*.
6. Enter the following content:

```
{
    "username":"<username of your API user>",
    "password":"<password of your API user>",
    "client_id":"flexvm",
    "grant_type":"password"
}
```

7. Click *Send*. If authentication is successful, you should receive a 200 response code with the following information:
   - `access_token`: The API token that will be used to run API calls against the FortiFlex portal.
   - `expires_in`: The token expiration time in seconds. The default value is 1440 seconds.
8. Copy the `access_token` value.

To run API calls:

1. Click on the + to open a new tab in the Postman app.
2. Click *Authorization*.
3. Set *Type* to *Bearer Token*.
4. Paste the `access_token` value in the *Token* field.

The URL for the API calls is https://support.fortinet.com.

FortiFlexVM Terraform provider

The FortiFlexVM Terraform provider is used to interact with the resources supported by FortiFlexVM. The provider must be configured with the proper credentials before it can be used. See the FortiFlexVM Documentation on the Terraform Registry for information on available resources, data sources, and so on.

The FortiFlexVM provider requires:

- A FortiCloud account.
- FortiFlex registered.
- An API token. See FortiFlex API on page 61.

Ansible Collection

The FortiFlex Ansible Collection can be used to run playbooks to interact with FortiFlex. The FortiFlex Ansible Collection can be found on GitHub and Ansible Galaxy. See the Ansible Galaxy FortiFlexVM Collection Documentation for more information on using Ansible Galaxy, running a playbook, available modules, and so on.

You can get support from the Fortinet Inc. Technical Assistance Center or from the community engineering team by filing an issue in the GitHub issues page. For support with common Ansible issues, you can get support from the Ansible community.

Tools

The topics in this section provide information about the points calculator tool:

- Points calculator on page 64
- Daily points on page 65

The points calculator in the FortiFlex portal should be used to calculate points consumption for existing FortiFlex programs only. It should not be used for new deals.

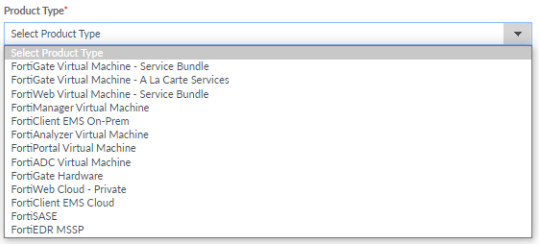
Points calculator

Use the points calculator to calculate how many points will be consumed before you create a new VM configuration.

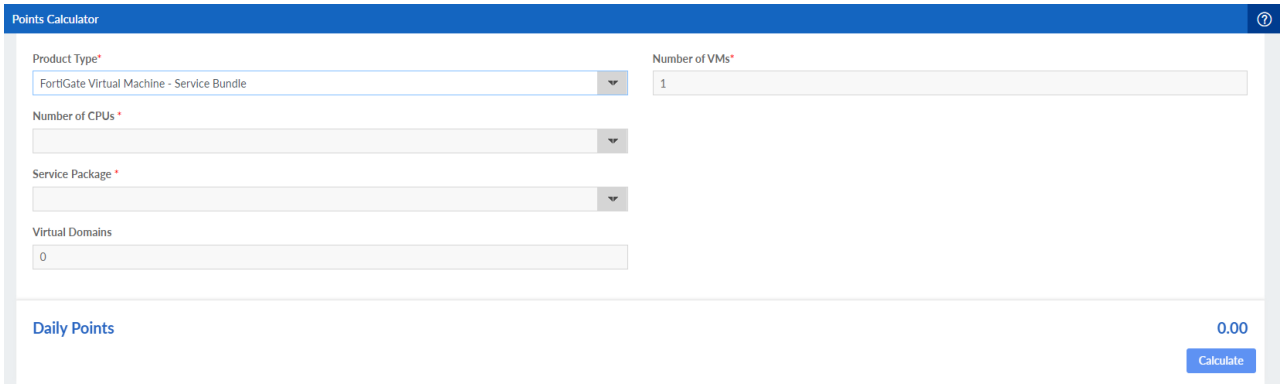
The points calculator can be found in the *Tools* > *Points Calculator* page, on the Fortinet Developer Network (https://fndn.fortinet.net/index.php?/tools/fortiflex/) or accessed through an API endpoint. Accessing the calculator through an API endpoint provides the current price, latest price, and effective date for the latest price.

To calculate points for a VM configuration:

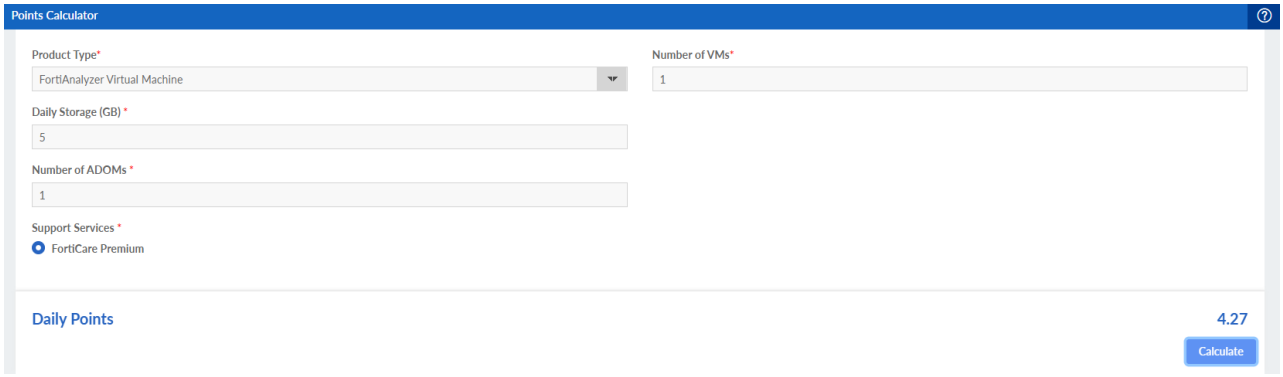
1. Go to *Tools* > *Points Calculator*.
2. From the list select on of the following options.
   - *FortiGate Virtual Machine - Service Bundle*
   - *FortiGate Virtual Machine - A La Carte Services*
   - *FortiWeb Virtual Machine - Service Bundle*
   - *FortiManager Virtual Machine*
   - *FortiClient EMS On-Prem*
   - *FortiAnalyzer Virtual Machine*
   - *FortiPortal Virtual Machine*
   - *FortiADC Virtual Machine*
   - *FortiGate Hardware*
   - *FortiWeb Cloud - Private*
   - *FortiClient EMS Cloud*
   - *FortiSASE*
   - *FortiEDR-MSSP*



3. Configure the VM based on the service you selected. The configuration settings will vary depending on the service. For more information, see Service offerings on page 14



4. From the number of *Number of VMs* dropdown, select the number of VMs.
5. Click *Calculate*. The number of points is displayed.

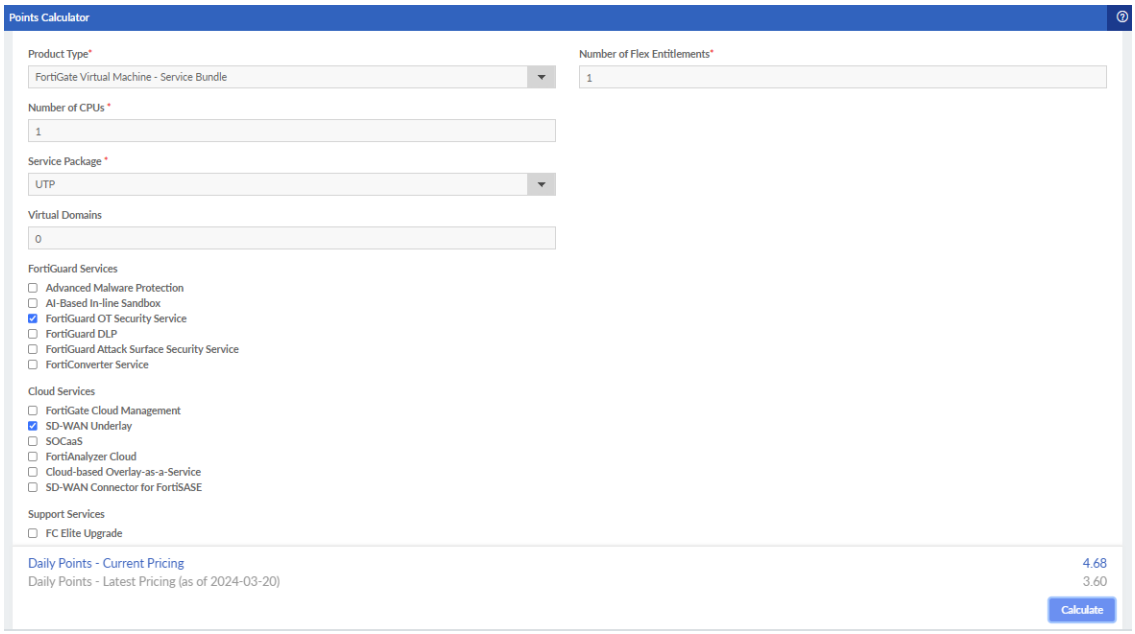


The *Daily Points* may display both current and latest pricing. See Daily points on page 65 for more information.

Daily points

When the daily rates of a product are updated, the *Daily Points* will display both the *Current Pricing* and *Latest Pricing* for the points calculator:

- *Current Pricing*: Displays the daily point cost for the total entitlements configured. This is calculated using the fixed ratings from when the program was registered. This fixed rating is valid for up to one year and is not subject to fluctuations in program ratings.
- *Latest Pricing (as of YYYY-MM-DD)*: Displays the cost based on the latest pricing as of the date that the points calculator tool is used. This rate is the new rate that will be applied to the configured entitlements after the next anniversary date, beginning on the date displayed. This rate is an estimate based on current rates and is subject to fluctuations.



www.fortinet.com

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