FortiFlex Automation and API

Deployment Guide 26.2

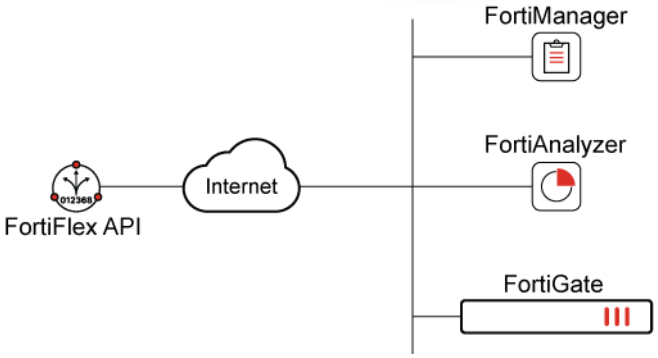
DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Deployment overview

The FortiFlex API fully automates program management operations, such as creating and managing configurations and entitlements. Direct access to the FortiFlex API is ideal for scripts and cloud orchestration platforms and can be directly interacted with by using an API toolkit solution, such as Postman. By leveraging FortiManager's FortiFlex connector along with the FortiFlex API, a FortiGate VM entitlement can be deployed.

In this document, deployment procedure to create FortiGate, FortiManager, and FortiAnalyzer configurations and entitlements using the FortiFlex API are discussed. Readers will be introduced to the available features of FortiFlex API and automation. Guidance is then provided on injecting the entitlement tokens in the CLI to successfully license the devices for further deployment of the FortiGate VM in FortiManager.



For more information on FortiFlex automation, see the FortiFlex Automation and API Brief.

Intended audience

This guide assumes the reader has a good understanding of FortiFlex and FortiCloud Services, including at least a high-level knowledge of FortiFlex deployment procedures and FortiCloud account permissions. For FortiFlex API implementation, the reader should have a working knowledge of Postman and understanding of JSON API calls, request body components, and responses.

About this guide

This deployment guide serves the purpose of going through connecting the FortiFlex API with Postman and performing standard FortiFlex API procedures, including creating configurations and entitlements without the use of the FortiFlex portal UI.

Prerequisites

The following prerequisites are assumed for this deployment:

- A FortiCloud API user credentials with Read/Write permissions for FortiFlex services. See API users in the FortiCloud Identity & Access Management guide.
- A registered FortiFlex program SKU in the same FortiCloud account as the API user. See the FortiFlex Getting Started guide.
- FortiFlex points available to support the device entitlements once they are configured and active. See the FortiFlex Getting Started guide.
- Access to Postman and the Fortinet Developer Network (FNDN).

Deployment plan

When performing this deployment, we will connect and use Postman and the FortiFlex API to configure FortiGate, FortiManager, and FortiAnalyzer VM configurations and entitlements. Once the FortiManager and FortiAnalyzer entitlements are activated, FortiManager will be used to install the FortiGate VM license.

The deployment is organized into the following steps:

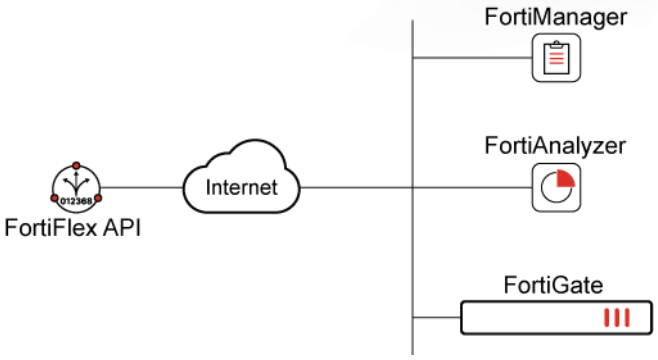
1. Configuring Postman to interact with the FortiFlex API on page 5
2. Creating FortiFlex configurations and entitlements using the API on page 6
3. Executing basic VM licensing on page 11
4. Preparing FortiManager for device registration on page 12
5. Registering and licensing the FortiGate VM on page 13

You will need API user credentials from your FortiCloud account to complete this deployment. See API users in the FortiCloud Identity & Access Management guide.

Deployment procedures

In this deployment example, we will demonstrate creating configurations and entitlements in Postman using the FortiFlex API and using them to register a FortiGate VM with FortiManager.

This deployment guide does not cover the configuration of the FortiManager or FortiAnalyzer instances apart from that which relates to the FortiFlex configurations. For information on configuring these devices, see the FortiManager Administration Guide and the FortiAnalyzer Administration Guide.



The following deployment plan is an overview of the procedure:

1. Connect Postman and the FortiFlex API using your FortiCloud API user credentials. See Configuring Postman to interact with the FortiFlex API on page 5.
2. Create configurations for FortiGate, FortiManager, and FortiAnalyzer VMs. These configurations will then be used to create entitlements for the device instances. See Creating FortiFlex configurations and entitlements using the API on page 6.
3. Inject the entitlement tokens to activate FortiManager and FortiAnalyzer VMs. See Executing basic VM licensing on page 11.
4. Create a FortiFlex connector and configure the FortiManager instance for the FortiGate device. See Preparing FortiManager for device registration on page 12.
5. Configure the FortiGate for central management using FortiManager and then install the FortiGate VM license on the FortiManager. See Registering and licensing the FortiGate VM on page 13.

Configuring Postman to interact with the FortiFlex API

In this step, you will use Postman to interact with the FortiFlex API in order to create the configurations and entitlements.

To configure Postman to interact with the FortiFlex API:

1. Open Postman.
2. Create a new HTTP POST request for listing program details. See Request basics in the Postman documentation.
3. In the *Authorization* tab, add the token details to the *Configure New Token* fields:

Field	Value
Token Name	`FortiFlex API Token`
Grant Type	*Password Credentials*
Access Token URL	`https://customerapiauth.fortinet.com/api/v1/oauth/token/`
Client ID	`flexvm`
Username	Copy and paste the *apiId* value from your API user credentials.
Password	Copy and paste the *password* value from your API user credentials.
Client Authentication	*Send client credentials in body*

4. Click *Get New Access Token*. The *Token Details* are displayed.
5. Click *Use Token*.
6. Insert the following in the request URL field: https://support.fortinet.com/ES/api/fortiflex/v2/programs/list
   This URL is the endpoint in the FortiFlex API used to obtain a list of the FortiFlex programs associated with your FortiCloud account.
7. Click *Send*. Verify that you received a HTTP response with a status code of *200 OK*.
8. Copy the response and save it for later use.

Creating FortiFlex configurations and entitlements using the API

In this step, you will create FortiFlex configurations and entitlements for the following product VMs:

- FortiGate on page 6
- FortiManager on page 8
- FortiAnalyzer on page 10

FortiGate

The following procedures demonstrate how to create FortiGate VM configurations and entitlements using the FortiFlex API in Postman.

To create a FortiGate VM configuration using the API:

1. Open Postman.
2. Create a new HTTP POST request for configurations. See Request basics in the Postman documentation.
3. In the *Authorization* tab, select *Available Tokens*.
4. Select *FortiFlex API Token*.
5. Insert the following in the request URL field: https://support.fortinet.com/ES/api/fortiflex/v2/configs/create
6. In the *Body* tab, select *raw* and *JSON*.
7. Copy and paste the following query:

```
{
    "programSerialNumber": "ELAVMS000000XXXX",
```

```
    "accountId": 1234567,
    "name": "configName",
    "productTypeId": 1,
    "parameters": [
        {
            "id": 1,
            "value": "maxCpu"
        },
        {
            "id": 2,
            "value": "ENT"
        }
    ]
}
```

The value `1` in the `productType` field indicates the product is FortiGate VM.

The parameter with ID `1` determines the maximum number of maximum number of SPU that can be allocated to the FortiGate VM using this configuration.

The parameter with ID `2` determines the service pack to be applied. In this case, the value `ENT` determines the enterprise service pack bundle.

For information on FortiFlex API base URLs, product types, endpoints, and so on, see the FNDN FortiFlex API documentation.

8. Replace the following values:

Parameter	Current value	New value
`programSerialNumber`	`ELAVMS000000XXXX`	The `serialNumber` value obtained from the first FortiFlex API request
`accountId`	`1234567`	Your account ID
`name`	`configName`	`Flex-FGT-1CPU`
`value` under parameter `"id": 1`	`maxCPU`	`1`

9. Click *Send*.
10. Verify the response status is *200 OK* and the response body reflects the desired configuration. Scroll down to the end of the response body and verify there were no errors and the request was processed successfully.
11. Copy the *config id* and *name* from the response body for future reference.

To create the FortiGate VM entitlement using the API:

1. Create a new HTTP POST request for entitlements. See Request basics in the Postman documentation.
2. In the *Authorization* tab, select *Available Tokens*.
3. Select *FortiFlex API Token*.
4. Insert the following in the request URL field:
https://support.fortinet.com/ES/api/fortiflex/v2/entitlements/vm/create
5. In the *Body* tab, copy and paste the following query:

```
{
    "configId": 12345,
```

```
    "count": 1,
    "description": "FortiGate VM 1 CPU entitlement created for DC",
    "endDate": null,
    "folderPath": "My Assets",
    "skipPending": false
}
```

By setting `"endDate": null`, the entitlements' `endDate` will be set automatically to the same value as that of the program's end date.

6. Replace the *configID* value with the configuration *id* value from the *Flex-FGT-1CPU* configuration.
7. Click *Send*.
8. Verify the response code is *200 OK* and the response body contains the appropriate entitlements.

FortiManager

The following procedures demonstrate how to create FortiManager VM configurations and entitlements using the FortiFlex API in Postman.

To create a FortiManager VM configuration using the API:

1. Open Postman.
2. Create a new HTTP POST request for configurations. See Request basics in the Postman documentation.
3. In the *Authorization* tab, select *Available Tokens*.
4. Select *FortiFlex API Token*.
5. Insert the following in the request URL field: https://support.fortinet.com/ES/api/fortiflex/v2/configs/create
6. In the *Body* tab, select *raw* and *JSON*.
7. Copy and paste the following query:

```
{
    "programSerialNumber": "ELAVMS000000XXXX",
    "accountId": 1234567,
    "name": "configName",
    "productTypeId": 2,
    "parameters": [
        {
            "id": 30,
            "value": "managedDevices"
        },
        {
            "id": 9,
            "value": "adoms"
        }
    ]
}
```

The value `2` in the `productType` field indicates the product is FortiManager VM.

The parameter with ID `30` determines the maximum number of managed devices that can be added to FortiManager VM using this configuration.

The parameter with ID `9` determines the maximum number of ADOMs supported by FortiManager VM using this configuration.

For information on FortiFlex API base URLs, product types, endpoints, and so on, see the FNDN FortiFlex API documentation.

8. Replace the following values:

Parameter	Current value	New value
`programSerialNumber`	`ELAVMS000000XXXX`	The `serialNumber` value obtained from the first FortiFlex API request
`accountId`	`1234567`	Your account ID
`name`	`configName`	`Flex-FMG`
`value` under parameter `"id": 30`	`managedDevices`	`10`
`value` under parameter `"id": 9`	`adoms`	`5`

9. Click *Send*.
10. Verify the response status is *200 OK* and the response body reflects the desired configuration.
11. Copy the *config id* and *name* from the response body for future reference.

To create the FortiManager VM entitlement using the API:

1. Create a new HTTP POST request for entitlements. See Request basics in the Postman documentation.
2. In the *Authorization* tab, select *Available Tokens*.
3. Select *FortiFlex API Token*.
4. Insert the following in the request URL field:
https://support.fortinet.com/ES/api/fortiflex/v2/entitlements/vm/create
5. In the *Body* tab, copy and paste the following query:

```
{
    "configId": 12345,
    "count": 1,
    "description": "FortiManager VM entitlement created for DC",
    "endDate": null,
    "folderPath": "My Assets",
    "skipPending": false
}
```

6. Replace the *configID* value with the configuration *id* value from the FortiManager configuration.
7. Click *Send*.
8. Verify the response code is *200 OK* and the response body contains the appropriate entitlements.
9. Copy the entire response body for future reference. You will need the token value.

FortiAnalyzer

The following procedures demonstrate how to create FortiAnalyzer VM configurations and entitlements using the FortiFlex API in Postman.

To create a FortiAnalyzer VM configuration using the API:

1. Open Postman.
2. Create a new HTTP POST request for configurations. See Request basics in the Postman documentation.
3. In the *Authorization* tab, select *Available Tokens*.
4. Select *FortiFlex API Token*.
5. Insert the following in the request URL field: https://support.fortinet.com/ES/api/fortiflex/v2/configs/create
6. In the *Body* tab, select *raw* and *JSON*.
7. Copy and paste the following query:

```
{
    "programSerialNumber": "ELAVMS000000XXXX",
    "accountId": 1234567,
    "name": "Flex-FAZ",
    "productTypeId": 7,
    "parameters": [
        {
            "id": 21,
            "value": "dailyStorage"
        },
        {
            "id": 22,
            "value": "adoms"
        },
        {
            "id": 23,
            "value": "FAZFC247"
        }
    ]
}
```

The value `7` in the `productType` field indicates the product is FortiAnalyzer VM.

The parameter with ID `21` determines the daily storage limit in GB of the FortiAnalyzer VM using this configuration.

The parameter with ID `22` determines the maximum number of ADOMs supported by the FortiAnalyzer VM using this configuration.

The parameter with ID `23` indicates the support services for entitlements using this configuration. In this case, the value `FAZFC247` determines the FortiCare Premium support.

For information on FortiFlex API base URLs, product types, endpoints, and so on, see the FNDN FortiFlex API documentation.

8. Replace the following values:

Parameter	Current value	New value
`programSerialNumber`	`ELAVMS000000XXXX`	The `serialNumber` value obtained

Parameter	Current value	New value
		from the first FortiFlex API request
accountId	1234567	Your account ID
name	configName	Flex-FAZ
value under parameter "id": 30	managedDevices	20
value under parameter "id": 9	adoms	5

9. Click *Send*.
10. Verify the response status is *200 OK* and the response body reflects the desired configuration.
11. Copy the *config id* and *name* from the response body for future reference.

To create the FortiAnalyzer VM entitlement using the API:

1. Create a new HTTP POST request for entitlements. See Request basics in the Postman documentation.
2. In the *Authorization* tab, select *Available Tokens*.
3. Select *FortiFlex API Token*.
4. Insert the following in the request URL field:
https://support.fortinet.com/ES/api/fortiflex/v2/entitlements/vm/create
5. In the *Body* tab, copy and paste the following query:

```
{
    "configId": 12345,
    "count": 1,
    "description": "FortiAnalyzer VM entitlement created for DC",
    "endDate": null,
    "folderPath": "My Assets",
    "skipPending": false
}
```

6. Replace the *configID* value with the configuration *id* value from the FortiAnalyzer configuration.
7. Click *Send*.
8. Verify the response code is *200 OK* and the response body contains the appropriate entitlements.
9. Copy the entire response body for future reference. You will need the token value.

Executing basic VM licensing

In this step, you will use the CLI to inject the FortiFlex entitlement tokens into the devices for FortiManager and FortiAnalyzer.

To inject a FortiFlex token into the VMs using the CLI:

1. Copy the FortiFlex token generated when you created the FortiManager VM entitlement.
2. In the command line, execute the following CLI command to inject the token, replacing <token_value> with the token valued you copied:

```
execute vm-license <token_value>
```

The FortiManager will automatically reboot once the `execute vm-license` command successfully runs.

3. Once the VM has completed the reboot process, connect to CLI and execute the following command:

```
get sys status
```

The `License Status` should be `Valid`.

4. Repeat these steps for the FortiAnalyzer VM.

Preparing FortiManager for device registration

In this step, you will prepare the FortiManager for registration of the FortiGate VM device.

> This deployment guide does not cover the configuration of the FortiManager or FortiAnalyzer instances apart from that which relates to the FortiFlex configurations. For information on configuring these devices, see the FortiManager Administration Guide and the FortiAnalyzer Administration Guide.

To configure the FortiFlex connector in FortiManager:

1. Log into the FortiManager instance.
2. Select the root ADOM.
3. In the *Dashboard*, verify that FortiManager is properly licensed using FortiFlex.
4. Go to *Policy & Objects* > *Security Fabric*.
5. In the *Endpoint/Identity* tab, select *Create New* > *FortiFlex Connector*.
6. Configure the following *Connector Settings*:

Field	Value
Name	`Flex-Deployment`
Status	Enabled
API User	Copy and paste the *apiId* value from your API user credentials.
API Password	Copy and paste the *password* value from your API user credentials.
Program SN	The `serialNumber` value obtained from the first FortiFlex API request

7. Click *Apply & Refresh*.
8. Verify that the FortiFlex configuration is listed. This means the connector was properly configured and was able to retrieve the configurations using the FortiFlex API and the credentials provided.
9. Click *OK*.

To configure FortiManager for registration of the FortiGate:

1. Go to *Device Manager* > *Devices & Groups*.
2. Click *Add Device*.
3. Add the FortiGate VM instance using the *Add Model Device* method using the Pre-Shared Key (PSK) option. See Adding offline model devices in the FortiManager Administration Guide for more information.
4. For the FortiGate device added, create a metadata variable for the FortiAnalyzer instance where the *Default Value* is the FortiAnalyzer serial number. See ADOM-level metadata variables in the FortiManager Administration Guide for more information.
5. Right-click the FortiGate managed device and click *Quick Install (Device DB)*. A confirmation dialog is displayed.

6. Click *OK*.
7. Verify the installation was successful and click *Finish*.
8. Go to *Policy & Objects* > *Normalized Interface*.
9. Configure the normalized interface mappings and policy package. See Normalized interface and Create new policy packages in the FortiManager Administration Guide for more information.
10. Click *Install Wizard*.
11. Select *Install Policy Package & Device Settings*.
12. Set the *Policy Package* to the FortiGate device.
13. Click *Next*.
14. Select the device and click *Next*.
15. Verify the installation was successful and click *Finish*.

Registering and licensing the FortiGate VM

In this step, you will configure central management options on the FortiGate VM and register it on FortiManager. You will then use FortiManager to install a FortiFlex VM license on the FortiGate.

To configure and register the FortiGate for central management using FortiManager:

1. In the FortiGate CLI, execute the following commands:

```
config system central-management
    set type fortimanager
    set fmg "<ip-address>"
    set serial-number <FortiManager serial number>
end
execute central-magmt register-device <FortiManager serial number> <password>
```

> The `<password>` is the pre-shared key that was used in the FortiManager instance when registering the model device using the PSK method.

This will configure the central management and send a device registration request to FortiManager.

2. In the FortiManager instance, Go to *Device Manager* > *Device & Groups*.
3. Verify that the FortiGate device appears as *Synchronized* in the *Config Status* column.

> If the device is not yet fully synchronized once you access FortiManager, go to *System Settings* > *Task Monitor* to monitor the progress of the *Autolinking Device* and *Push config to device* tasks until they are completed successfully.

To install a FortiFlex FortiGate VM license on the FortiGate instance using FortiManager:

1. In the FortiManager instance, Go to *Device Manager* > *Device & Groups*.
2. Right-click the FortiGate managed device and click *Install VM License*.
3. Set *From* to *FortiFlex*.
4. Set *FortiFlex Connector* to the *Flex-Deployment* connector that you created previously.
5. Set *FortiFlex Configuration* to the FortiGate VM configuration that you created previously.
6. Click *OK*.

7. Verify the license installation task finished successfully and click *Finish*. The FortiGate VM will reboot to apply the new FortiFlex license.
8. Log into the FortiGate VM instance to verify the licensing information and *Serial number*.

More Information

Products used in this guide

This guide uses the following product models and firmware:

Product	Model	Firmware
FortiFlex	N/A	25.2

Documentation references

Feature documentation

- FortiFlex Administration Guide
- FortiFlex Automation and API Brief

Solution hub

- FortiCloud

Change log

Date	Change description
2026-05-25	Initial release.

www.fortinet.com

82-252-1118411-20260525