

Air-Gapped Mode

FortiSandbox 4.0.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



September 09, 2021

FortiSandbox 4.0.0 Air-Gapped Mode

00-400-000000-20210909

TABLE OF CONTENTS

Change Log	4
Introduction	5
Topology	6
Step 1: Offline Licenses	7
Request the Offline Licenses	7
Prepare and Install the licenses on FortiManager	8
License FortiGate from FortiManager	11
Step 2: Licensing FortiSandbox	15
Enable SIMNET	15
Point FortiSandbox to the FortiManager as License Server	15
Validate FortiSandbox License	19
Step 3: FortiManager Security Updates (FortiGate)	23
Prepare FortiManager as the update server	23
Install offline FortiGate security updates on FortiManager	24
Verify FortiGate is receiving offline updates	25
Step 4: FortiManager Security Updates (FortiSandbox)	28
Install Offline FortiSandbox Security Updates on FortiManager	28
Verify FortiSandbox is receiving offline updates	29
Install Web Filtering DB on FortiManager	30
Verifying Web Filtering Queries on FortiGate and FortiSandbox	31
Step 5: FortiSandbox Microsoft Windows/Office Offline Activation	35
Microsoft Windows VMs Offline Installation	35
Offline Microsoft Windows VMs Activation	37
Offline Microsoft Office Licenses Activation	38
Step 6: FortiSandbox File Query DB	42
Verify File Query DB on the Online FortiManager	42
Export File Query DB	42
Import File Query DB into FortiManager	43
Configure and Verify FortiSandbox can query file DB	43

Change Log

Date	Change Description
2021-09-09	Initial release.

Introduction

This document explains the process to run FortiSandbox in air-gapped (or closed) network mode where internet connectivity is not available. The process includes the FortiGate and FortiManager devices and explains the following:

- Devices offline licensing
- Offline updates
- Initializing Microsoft VMs including Microsoft office licenses

The firmware version used for the devices are the following:

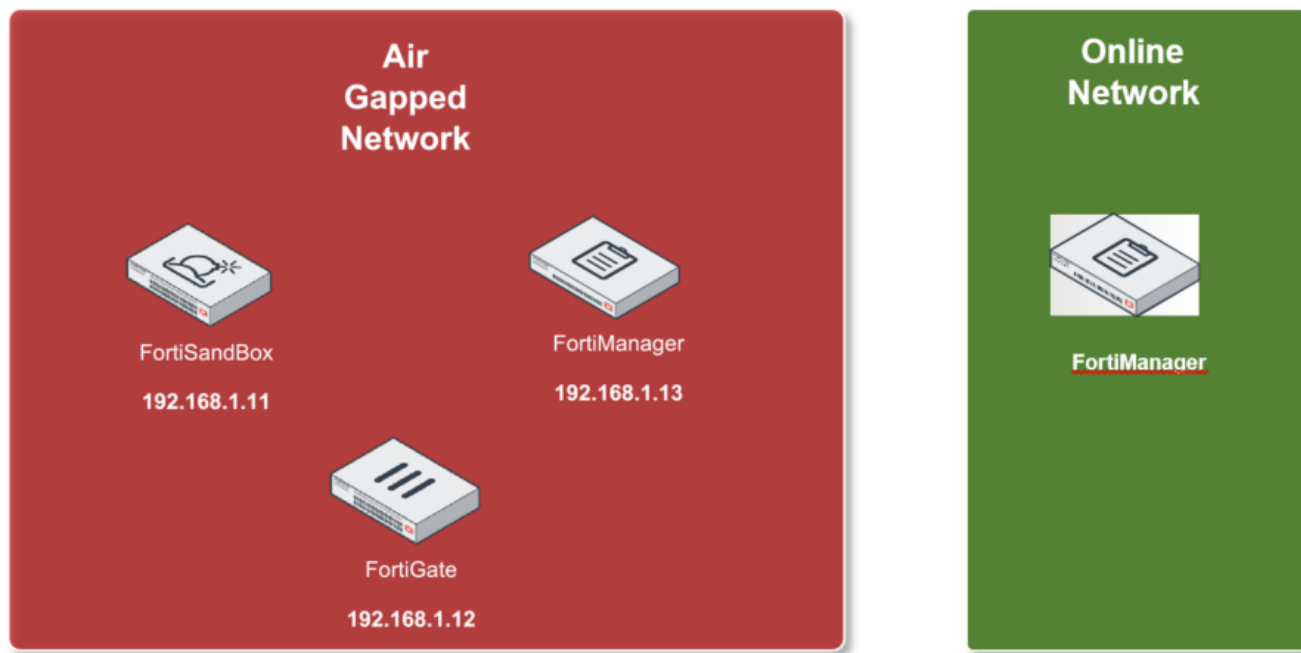
Device/Platform	Version Number and Build
FortiSandbox VM	V3.1.0 GA build 0124
FortiManager VM	V6.2.2 GA build 1183
FortiGate VM	V6.2.2 GA build 1010



Please refer to the respective [Release Notes](#) when using a newer firmware version of FortiSandbox. For example, FortiSandbox v4.0.0 is only compatible to FortiManager v 6.4.6 or later.

Topology

The diagram below shows the basic topology to setup an air-gapped network.



Step 1: Offline Licenses

Obtain an Entitlement File from FortiCloud that includes the licenses for the registered devices and Install the licenses on FortiManager. After the installation, you will use FortiManager to license FortiGate.

To install offline licenses:

1. [Request the Offline Licenses on page 7](#)
2. [Prepare and Install the licenses on FortiManager on page 8](#)
3. [License FortiGate from FortiManager on page 11](#)

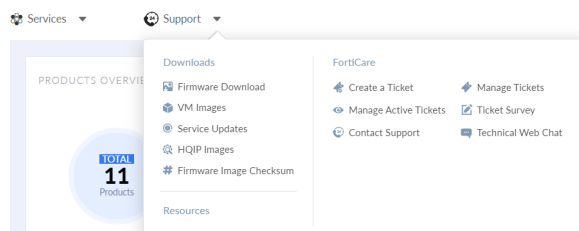
Request the Offline Licenses

Create a support ticket to obtain an *Entitlement File* that includes the licenses for the registered devices.

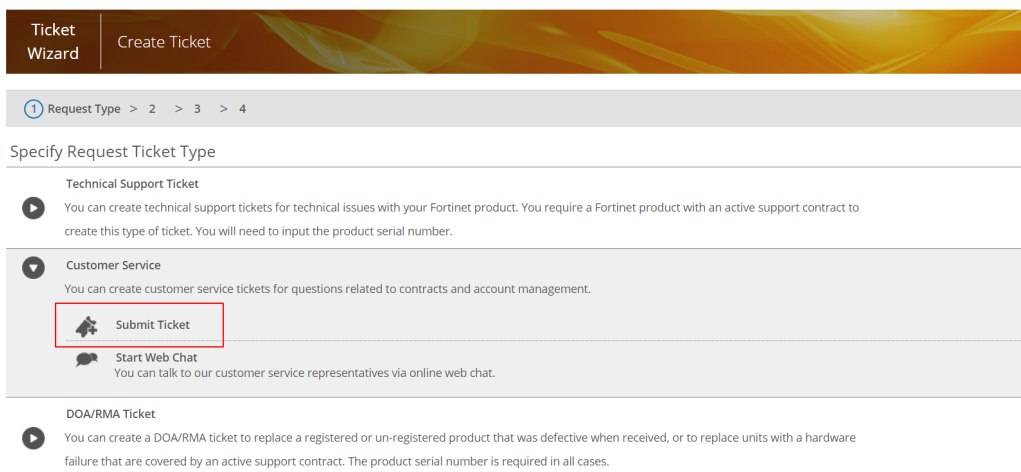
You will need to create a support ticket to obtain an *Entitlement File* that includes the licenses for the registered devices.

To obtain an entitlement File:

1. Log in to [FortiCloud](#). The Asset Management (AM) portal opens.
2. In the toolbar, go to *Support > FortiCare > Create a Ticket*.



3. Click *Customer Service > Submit Ticket*.



4. Provide the requested ticket info. Specify the Category as *CS Contract/License*.

Ticket Wizard

CS Ticket
Serial Number: N/A

1 Request Type > 2 Basic Info > 3 Comment > 4 Completion

Specify Ticket Information

Serial Number:

Contact Information

Name:* Tony Correia

Email:* tcorreia@fortinet.com

Telephone: +1 7783295001

Mobile Phone:

Ticket Information

Subject:* Entitlement File

Category:* CS Contract/License

PreviousNext

5. Use the Add Comment form to request the entitlement file for your account and click Next. The confirmation message opens. An email with entitlement file will be sent to your address.

Ticket Wizard

CS Ticket
Serial Number: N/A

1 Request Type > 2 Basic Info > 3 Comment > 4 Completion

Add Comment

Note: The maximum characters system allow to be entered here is 8000.

Hello,

Can I please have the entitlement file for my account?

Thank you!

Attachments

Log File

Configuration

Virus Sample File (Temp)

Other

PreviousNext

Prepare and Install the licenses on FortiManager

To prepare and install the licenses:

1. On FortiManager, install the FortiManager license file. FortiManager will reboot.
2. After rebooting, log in to FortiManager again.
3. Go to *System Settings > Network*. The *System Network Management Interface* pane opens.
4. On *port1* interface, enable *HTTPS*, *PING*, *SSH*, *FortiGate Updates*, *Web filtering* and its corresponding IP addresses.

System Settings ▾

- Dashboard
- All ADOMs
- Network**
- HA
- Admin ▾
 - Administrators
 - Profile
 - Remote Authentication Server
 - Admin Settings
 - SAML SSO
- Certificates ▾
 - Local Certificates
 - CA Certificates
 - CRL
 - Remote Certificates
- Event Log

System Network Management Interface

Name: port1

IP Address/Netmask: 192.168.1.13/255.255.255.0

IPv6 Address: ::/0

Administrative Access: ☒ HTTPS ☐ HTTP ☒ PING ☒ SSH ☐ SNMP ☐ Web Service

IPv6 Administrative Access: ☐ HTTPS ☐ HTTP ☐ PING ☐ SSH ☐ SNMP ☐ Web Service

Service Access: ☒ FortiGate Updates

Bind to IP Address ⓘ: 192.168.1.20/255.255.255.0

Web Filtering: ☒ Web Filtering

Bind to IP Address ⓘ: 192.168.1.21/255.255.255.0

Default Gateway:

Primary DNS Server: 208.91.112.52

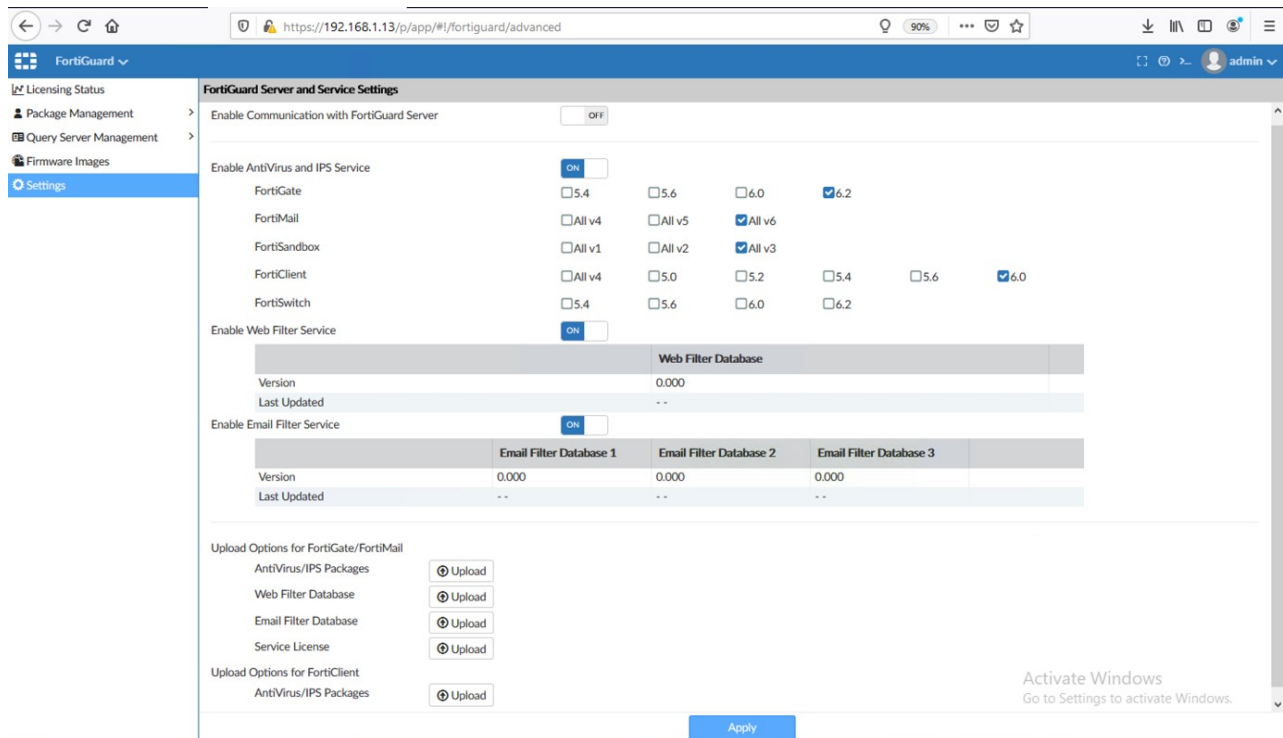
Secondary DNS Server: 208.91.112.53

Buttons: All Interfaces, Routing Table, IPv6 Routing Table, Packet Capture

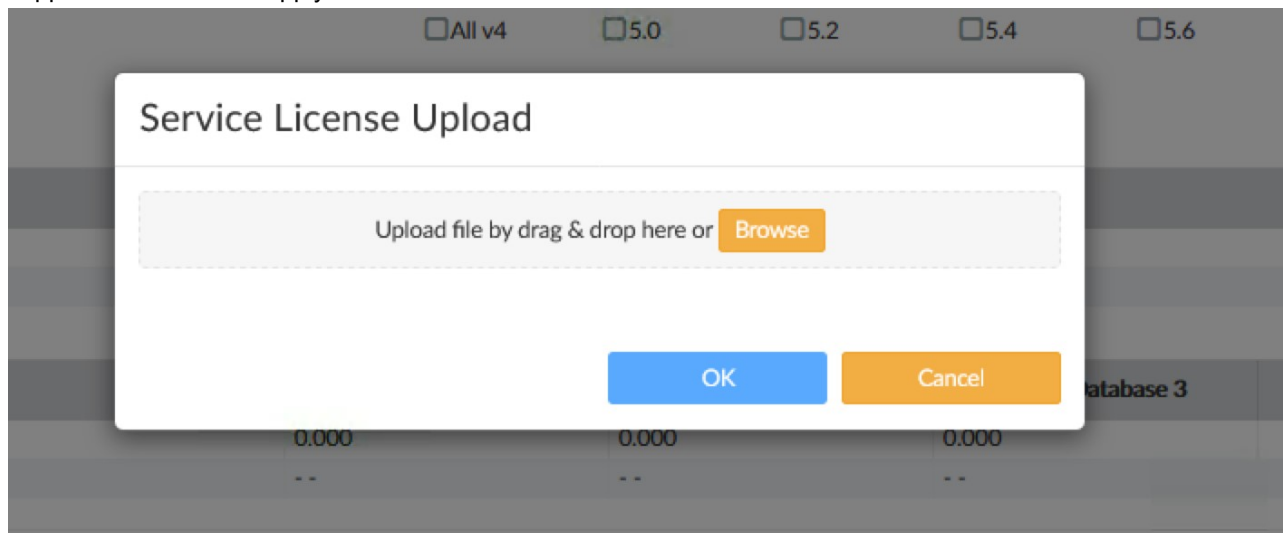
5. Go to *FortiGuard* > *Settings*. Configure the following settings and click *Apply*.

Enable Communication with FortiGuard Server	Set to OFF
Enable Antivirus and IPS Service	Set to ON Select the FortiGate, FortiMail, FortiSandbox and FortiClient versions that you need FortiManager to support as FDS for AV and IPS.
Web Filter Service	Enable if required.
Email Filter Service	Enable if required.

Step 1: Offline Licenses



- On the Settings page, FortiGate/FortiMail > Service License. Upload the entitlement file you received from the support team and click Apply.



- Open FortiManager's CLI console, and execute the following command:

```
config system admin setting
set unreg_dev_opt add_allow_service
end
```
- Reboot FortiManager.
- After FortiManager reboots, verify the serial number(s) for your devices are available in the FortiManager DB.

```
#diagnose fupdate dbcontract fgd.
```

The following is an example of the output.

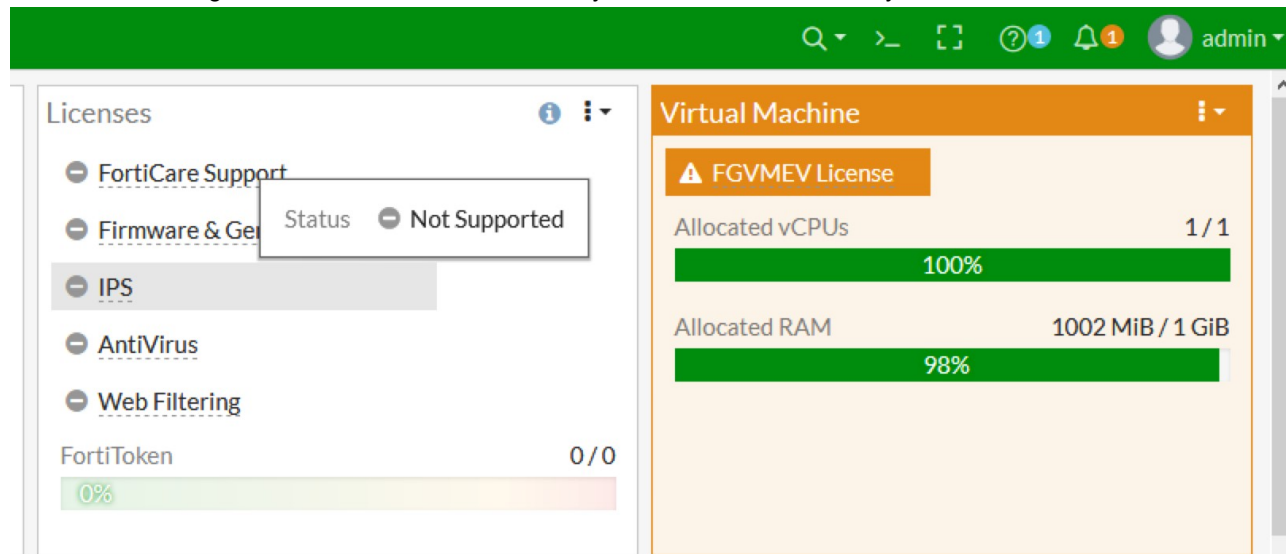
```

FSAVM0000000000000000 [SERIAL-NO]
Contract: 10
AVDB-1-06-20210113
COMP-1-20-20210113
ENHN-1-20-20210113
FQDB-1-20-20210113
FMWR-1-06-20210113
FURL-1-06-20210113
ISSS-1-06-20210113
NIDS-1-06-20210113
SBEN-1-06-20210113
SPRT-1-20-20210113
    
```

License FortiGate from FortiManager

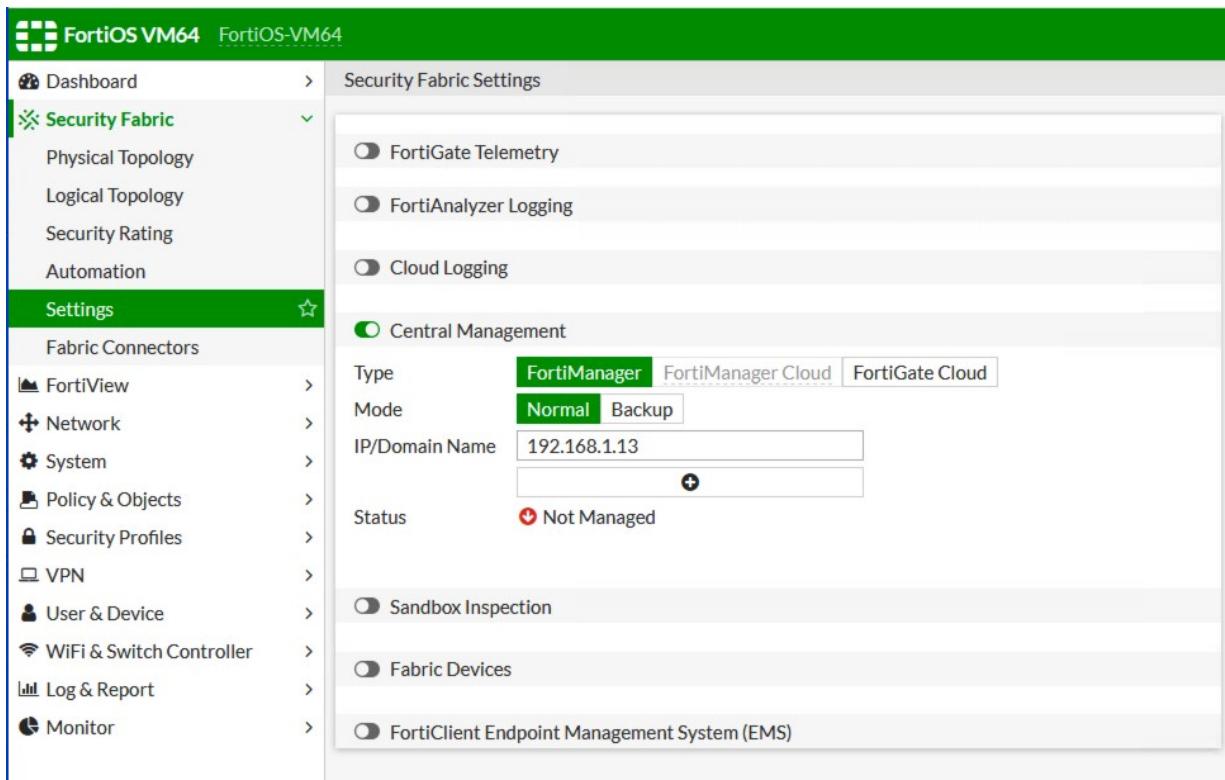
To license FortiGate from FortiManager:

1. On the FortiGate, go to *Dashboard > Status* and verify FortiGate is not licensed yet.

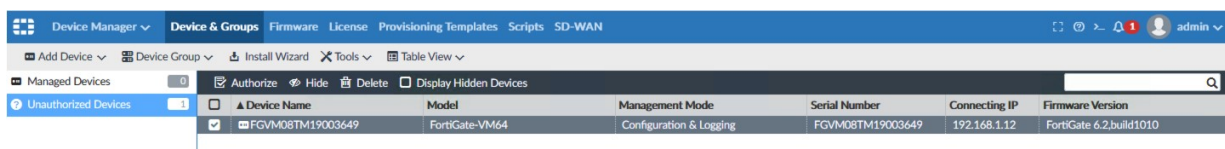


2. On FortiGate, set the FortiManager as *Central Management*.
 - a. Go to *Dashboard > Security Fabric > Settings*.
 - b. Enable *Central Management*, and configure the following settings:

Type	FortiManager
Mode	Normal
IP/Domain Name	Set the IP address of the FortiManager in your network.



- c. Click *Apply*.
3. Upload the license of the FortiGate-VM.
 - a. Go to support.fortinet.com and download the FortiGate-VM license. See, [Viewing product details](#).
 - b. Go to *Dashboard > Licenses*.
 - c. Upload the FortiGate-VM license you downloaded from support.fortinet.com. Once the license is uploaded, FortiGate will reboot.
4. Add the FortiGate to FortiManager
 - a. On FortiManager, go to *Device Manager > Device & Groups*. You will see a new unregistered device request notification.



If you did not get the request, you can add the FortiGate manually.


- b. Go to *Device Manager > Unauthorized Devices*.










- c. Select the FortiGate and click *Add Device*. The *Import Wizard* launches and adds the device.


Add Device

Name FGVM08TM19003649

IP Address 192.168.1.12







Status  Device is added successfully

-  Discovering device
-  Creating device database
-  Initializing configuration database
-  Retrieving configuration
-  Retrieving support data
-  Retrieving HA configuration
-  Updating group membership
-  Successfully add device
-  Check Device Status

 To manage policies and objects of this device, you need to import them into FortiManager database.

[Import Now](#) [Import Later](#)

5. After the FortiGate is added to FortiManager, go to *Device Manager > Managed Devices*.

Device Manager	Device & Groups	Firmware	License	Provisioning Templates	Scripts	SD-WAN	admin
Add Device	Device Group	Install Wizard	Tools	Table View			
Managed Devices	1 Devices Total	0 Devices Connection Down	0 Devices Device Config Modified	0 Devices Policy Package Modified			
<div>       </div>							
Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	
FortiOS-VM64	Synchronized	Never installed	FortiGate 6.2.2.build1010 (GA)	FortiOS-VM64	192.168.1.12	FortiOS-VM64	

6. If you have synced the policy with FortiGate, you will see the policy package status change.

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform
FGVM08TM19003649	Synchronized	FGVM08TM19003649_root	FortiGate 6.2.2.build1010 (GA)	FGVM08TM19003649	192.168.1.12	FortiGate-VM64

7. FortiGate validates the license from FortiManager. Please allow some time for the validation process to complete. If the process takes too long, you can try to upload the entitlement file again.

Device Name	Serial Number	Platform	ADOM	AntiVirus	IPS	Email Filtering	Web Filtering	Outbreak Protect	Industrial DB	Support
FGVM08TM19003649	FGVM08TM1900	FortiGate-VM64	root	2020-12-10	2020-12-10	2020-12-10	2020-12-10	2020-12-10	2020-12-10	2020-12-10

Step 2: Licensing FortiSandbox

Ensure that SIMNET is enabled and then point FortiSandbox to the FortiManager as the License Server. Once FortiManager is designated as the license server, validate the FortiSandbox license.

To license FortiSandbox:

1. [Enable SIMNET on page 15](#)
2. [Validate FortiSandbox License on page 19](#)
3. [Point FortiSandbox to the FortiManager as License Server on page 15](#)

Enable SIMNET

On FortiSandbox, ensure that SIMNET is enabled to prevent FortiSandbox from sending requests through port3 (optimization).

To enable SIMNET:

1. Log in to FortiSandbox.
2. Go to *Scan Policy > General*.
3. Deselect 'Allow Virtual Machines to access external network through outgoing port3'.
4. In the *System Information* dashboard, verify the status of *SIMNET* is *ON*.

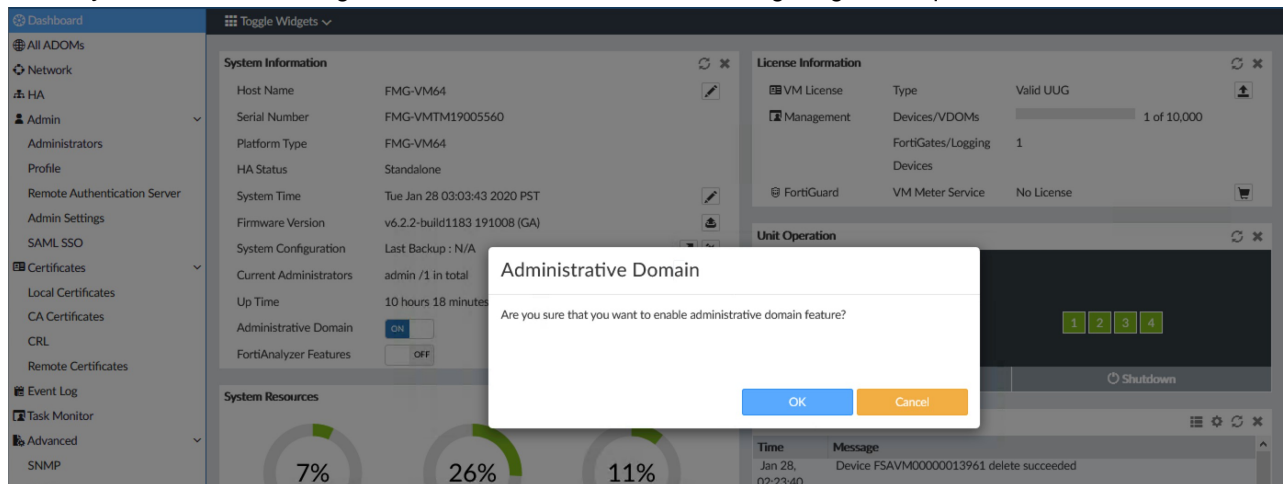


Point FortiSandbox to the FortiManager as License Server

To point FortiSandbox to FortiManager as License Server:

1. Log in to FortiManager.
2. Go to *System Settings*.

3. In the *System Information* widget, enable *Administrative Domains*. Log in again if required.



4. Go to system SSettings > ADOMs.

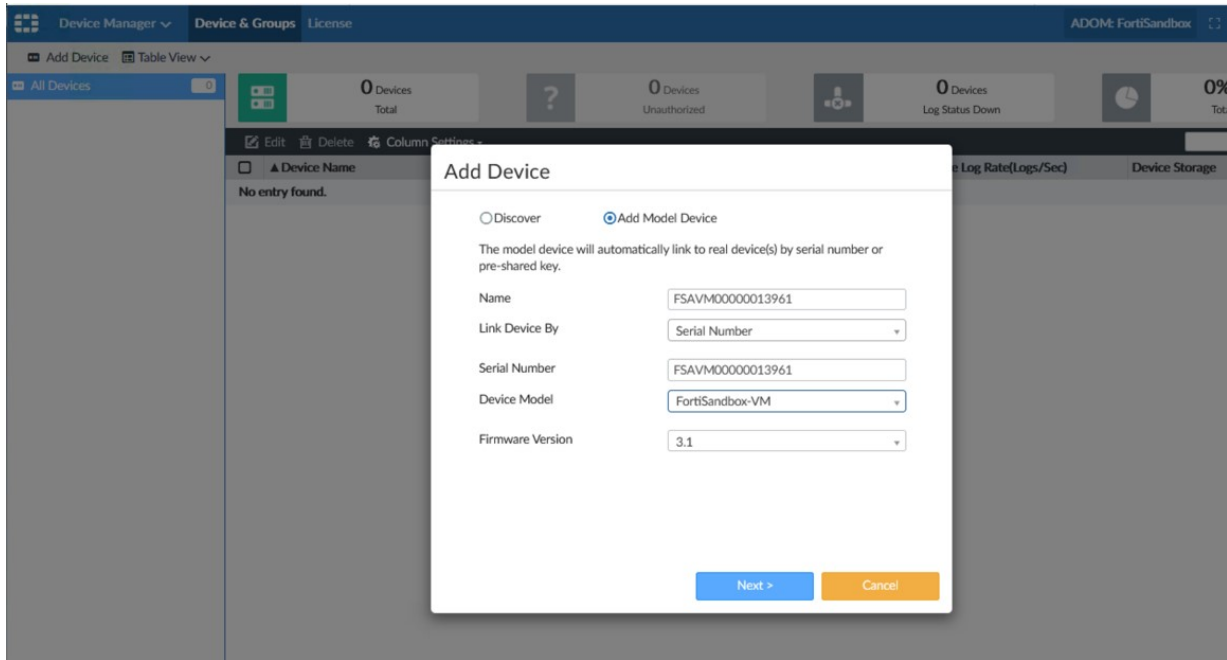
5. Right-click the FortiSandbox ADOM, and click *Enter ADOM > Device Manager*.

	Name	Firmware Version
▼ Central Management (3)		
<input type="checkbox"/>	FortiCarrier	FortiCarrier 6.2
<input type="checkbox"/>	root	FortiGate 6.2
<input type="checkbox"/>	Global Database	Global 6.2
▼ Other Device Types (13)		
<input type="checkbox"/>	FortiAnalyzer	FortiAnalyzer
<input type="checkbox"/>	FortiAuthenticator	FortiAuthenticator
<input type="checkbox"/>	FortiCache	FortiCache
<input type="checkbox"/>	FortiClient	FortiClient
<input type="checkbox"/>	FortiDDoS	FortiDDoS
<input type="checkbox"/>	FortiMail	FortiMail
<input type="checkbox"/>	FortiManager	FortiManager
<input type="checkbox"/>	FortiNAC	FortiNAC
<input type="checkbox"/>	FortiProxy	FortiProxy
<input checked="" type="checkbox"/>	FortiSandbox	FortiSandbox
<input type="checkbox"/>	FortiWeb	FortiWeb
<input type="checkbox"/>	Syslog	Syslog
<input type="checkbox"/>	Chassis	-

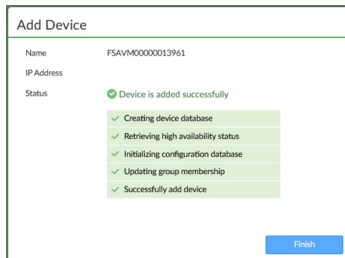
6. Once inside the FortiSandbox ADOM, click *ADD Device* at the top left-side of the page. The *Add Device* dialog opens.

- Click 'Add Model Device'.
- Type the device *Name* and *Serial Number* and then select the *Device Model* (FortSandbox-VM) and *Firmware Version*.
- From the *Link Device By* dropdown, select *Serial Number*.

- d. Click *Next*. The *Add Device* wizard launches.



7. Wait for the wizard to create the required database for the FortiSandbox, and click *Finish*.



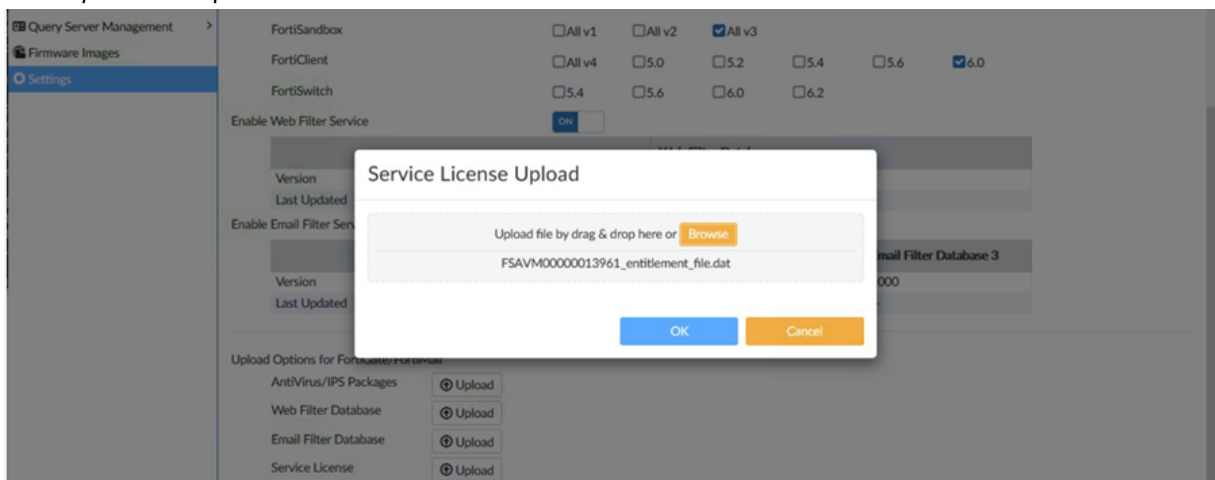
8. On FortiManager, upload the FortiSandbox entitlement file that you received from the support team if you have a separate entitlement file for FortiSandbox.



If you have entitlement file for the entire account, FortiSandbox will be included in the account entitlement file.

- a. Go to *FortiGuard > Settings > Upload Options for FortiGate/FortiMail*. The *Service License Upload* dialog opens.

- b. Click *Upload* and upload the FortiSandbox entitlement file.



Validate FortiSandbox License

FortiSandbox needs to point to FortiManager as License Server. The initial status of the FortiSandbox license should be unlicensed (*Upload License*) in the *System Information* dashboard.

FortiSandbox VM

What are you looking for? 🔍

- Dashboard
- FortiView
- Network
- System
- Virtual Machine
- Scan Policy
- Scan Input
- File Detection
- Network Alerts
- URL Detection
- Log & Report

System Information

Unit Type	Standalone
Host Name	FSA-VM0000000000 [Change]
Serial Number	FSA-VM0000000000
System Time	Thu Dec 26 06:10:47 2019 UTC [Change]
Firmware Version	v3.1.2.build0125 (Interim) [All firmwares]
VM License	⚠️ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 7 hour(s) 0 minute(s)
Windows VM	⚠️
Microsoft Office	⚠️ [Upload License]
VM Internet Access	⚠️ [(SIMNET ON)]
FDN Download Server	⚠️
Community Cloud Server	⚠️
Web Filtering Server	⚠️

To validate a FortiSandbox license:

1. Log in to FortiSandbox.
2. Go to *FortiGuard* and configure the following settings and click *Apply*.

FortiGuard Server Location	Nearest
FortiGuard Server Settings	Select <i>Use override FDN server to download module updates</i> and enter the FortiManager's IP address.

FortiSandbox Community Cloud & Threat Intelligence Settings

Select *Use override server for community cloud server query (address or address: port)* and enter the FortiManager's IP address.

FortiGuard Server Location

FDN Server Location

Nearest US Region

FortiGuard Server Settings

☒ Use override FDN server to download module updates

192.168.1.13

☐ Use Proxy

Connect FDN Now

FortiGuard Web Filter Settings

☐ Secure Connection

☒ Use override server for web filtering query (address or address:port)

192.168.1.13

53 8888

☐ Use Proxy

VM Image Download Proxy Settings

☐ Use Proxy

FortiSandbox Community Cloud & Threat Intelligence Settings

☒ Use override server for community cloud server query (address or address:port)

192.168.1.13

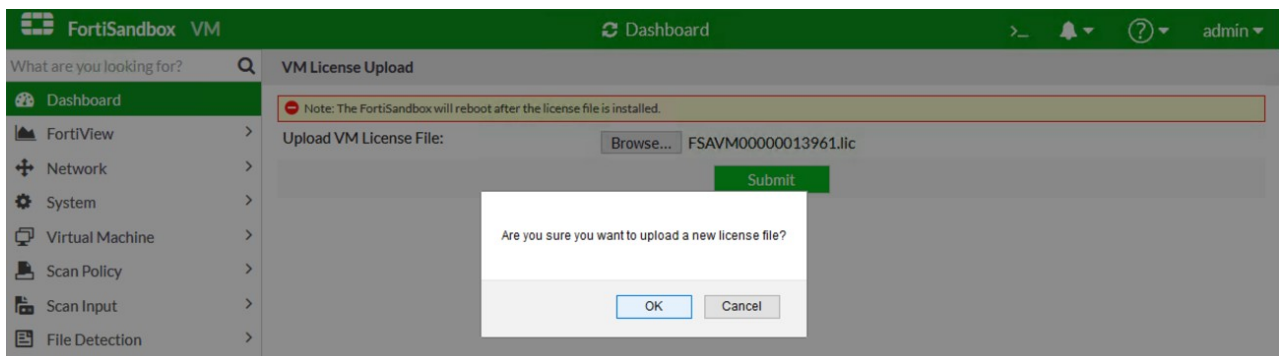
53 8888

☐ Use Proxy

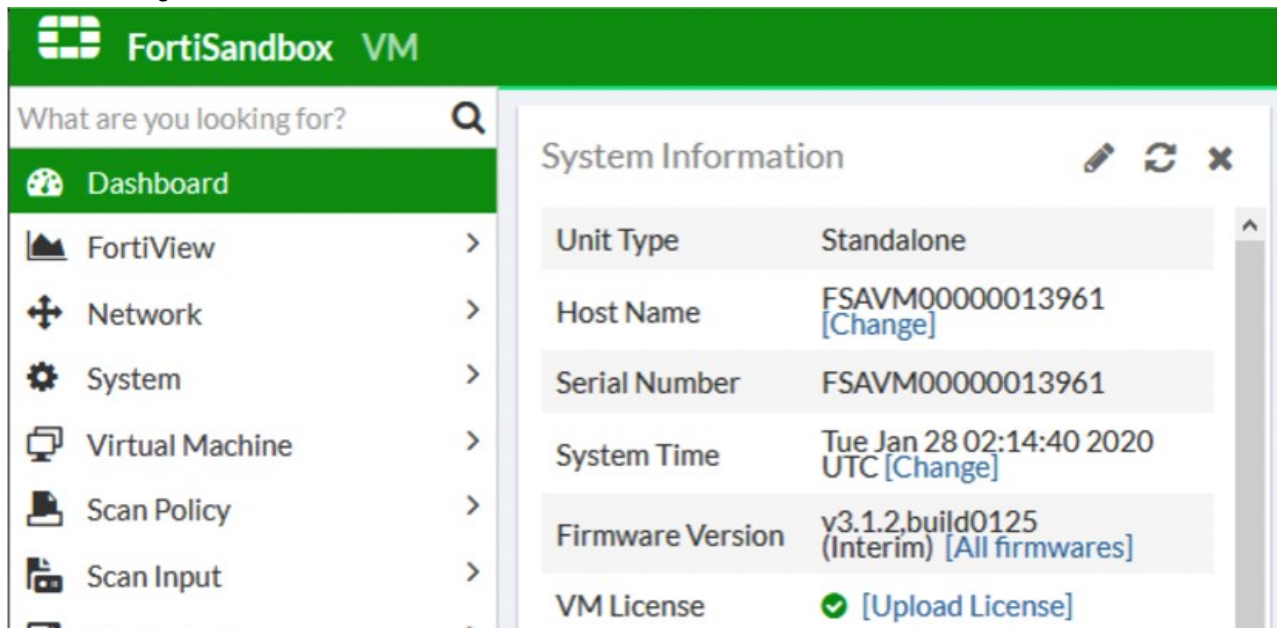
Apply

Activate Windows
Go to Settings to activate Wi

- Click *Connect FDN Now*.
- Download the FortiSandbox license file from the product page on support.fortinet.com. See, *Asset Management Admin Guide > Viewing product details*.
- Log in to FortiSandbox.
- Go to *Dashboard > System Information > Upload License*. Select the (.lic) file for FortiSandbox. FortiSandbox will reboot.



- After rebooting, issue a test-network on FortiSandbox to confirm the license status.



- Log in to FortiManager.
- Go to *FortiGuard > Licensing Status*. Verify that FortiSandbox is licensed. You should see the license dates of FortiSandbox.

The screenshot shows the FortiGuard Licensing Status page. The table lists the following devices:

Device Name	Serial Number	Platform	ADOM	AntiVirus	IPS	Email Filtering	Web Filtering	Outbreak Protect	Industrial DB	Support
FGVM08TM19	FGVM08TM190C	FortiGate-VM64	root	2020-12-10	2020-12-10	2020-12-10	2020-12-10		2020-12-10	2020-12-10
FSAVM000000	FSAVM00000001	FortiSandbox-VM	FortiSandbox	2021-01-14	2021-01-14		2021-01-14		2021-01-14	2021-01-14

Step 3: FortiManager Security Updates (FortiGate)

Prepare FortiManager as the update server and then install the offline FortiGate security updates on FortiManager. After the installation is complete, verify FortiGate is receiving the offline updates.

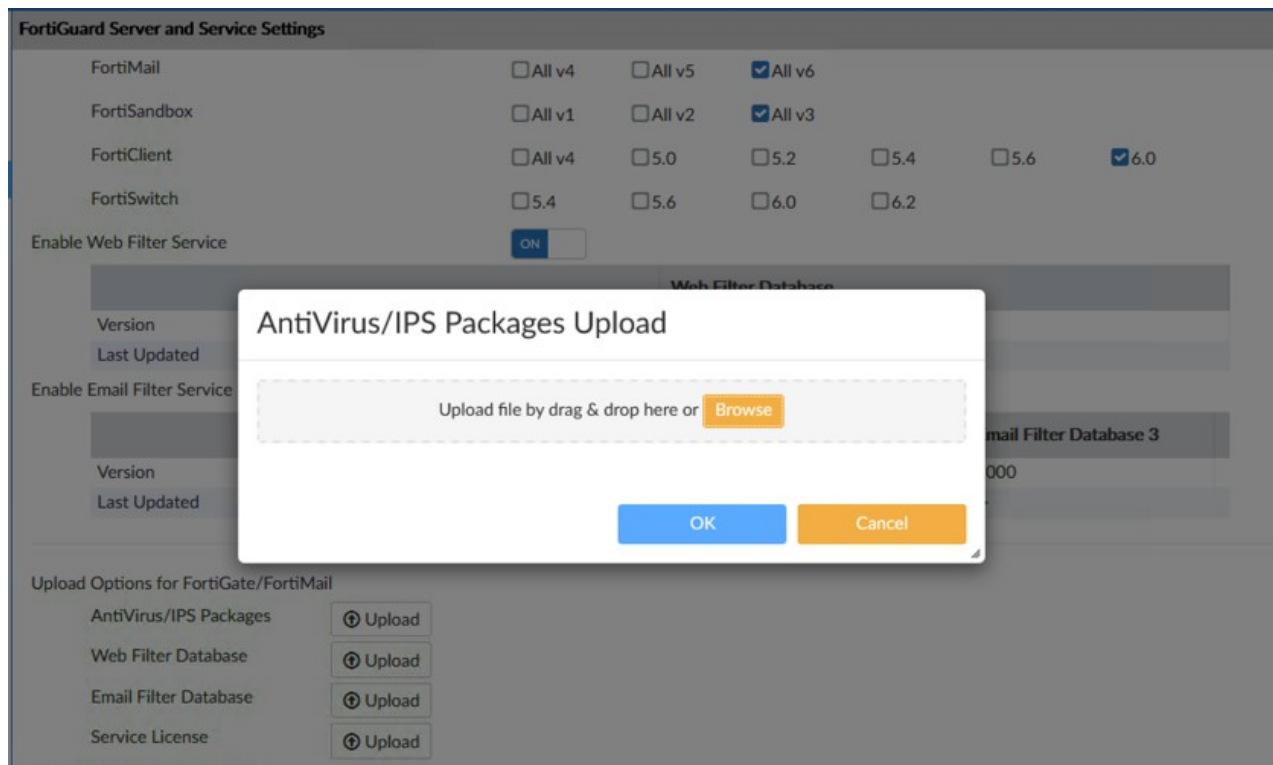
To use FortiManager as the update server:

1. Prepare FortiManager as the update server on page 23
2. Install offline FortiGate security updates on FortiManager on page 24
3. Verify FortiGate is receiving offline updates on page 25

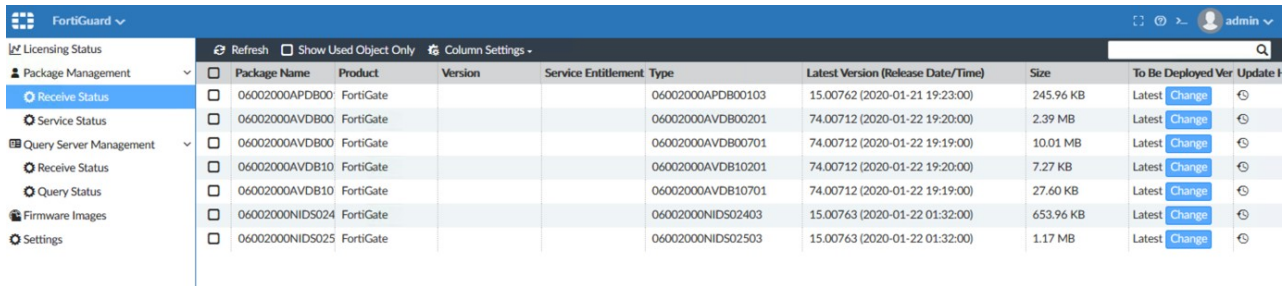
Prepare FortiManager as the update server

To prepare FortiManager as the update server:

1. Log in to FortiManager.
 2. Go to *FortiGuard > Settings*.
 3. Go to *Upload Options for FortiGate/FortiMail > Antivirus/IPS Packages*, and click *Upload*.
 4. Select the packages downloaded and available on removable media, and install them on FortiManager.
- After the installation is complete, all the required packages should be available on FortiManager.



5. Go to *FortiGuard > Package Management > Receive Status*. You should see the packages with the corresponding installation date.

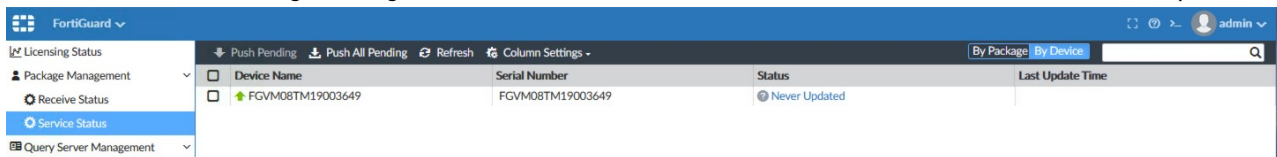


Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Ver	Update
06002000APDB00	FortiGate			06002000APDB00103	15.00762 (2020-01-21 19:23:00)	245.96 KB	Latest	Change
06002000AVDB00	FortiGate			06002000AVDB00201	74.00712 (2020-01-22 19:20:00)	2.39 MB	Latest	Change
06002000AVDB00	FortiGate			06002000AVDB00701	74.00712 (2020-01-22 19:19:00)	10.01 MB	Latest	Change
06002000AVDB10	FortiGate			06002000AVDB10201	74.00712 (2020-01-22 19:20:00)	7.27 KB	Latest	Change
06002000AVDB10	FortiGate			06002000AVDB10701	74.00712 (2020-01-22 19:19:00)	27.60 KB	Latest	Change
06002000NIDS024	FortiGate			06002000NIDS02403	15.00763 (2020-01-22 01:32:00)	653.96 KB	Latest	Change
06002000NIDS025	FortiGate			06002000NIDS02503	15.00763 (2020-01-22 01:32:00)	1.17 MB	Latest	Change

Install offline FortiGate security updates on FortiManager

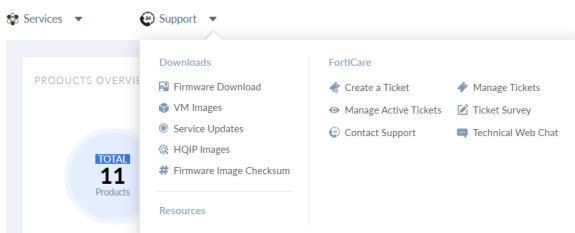
To install offline FortiGate security updates:

1. Log in to FortiManager.
2. Go to *FortiGuard > Package Management > Service Status*. You will see that FortiGate's *Status* is *Never Updated*.



Device Name	Serial Number	Status	Last Update Time
FGVM08TM19003649	FGVM08TM19003649	Never Updated	

3. Log in to [FortiCloud](#). The Asset Management portal opens.
4. Go to *Support > Download > FortiGuard Service Updates*.



5. Select the FortiGate from the list.

6. Select the version you want to use and download the packages.



Select a version that is supported by FortiManager.

We recommend storing the packages on removable media (for example) to install on FortiManager.

FortiGuard Updates

Download FortiGuard Service Updates

FortiGate

VCM FortiGate

FortiSandBox

FortiGate

OS Version:

v6.2.0

Product Model

FortiGate VM02

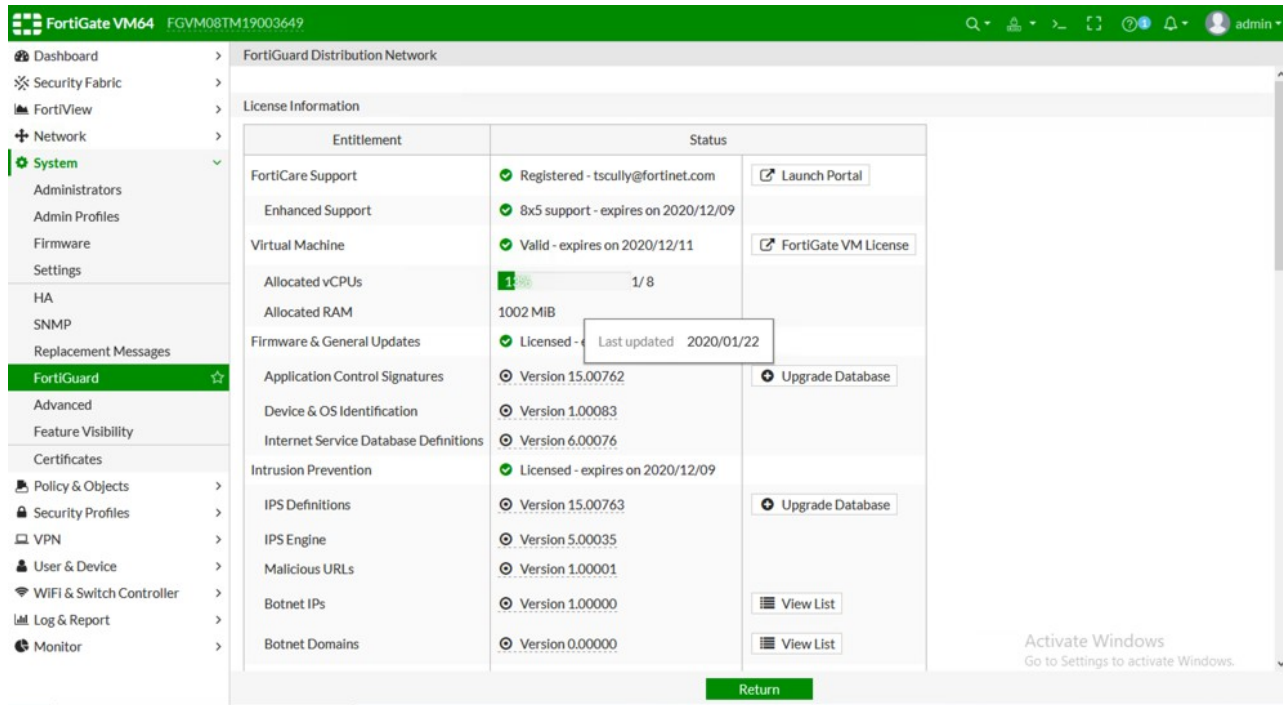
Type	File	Creation Date
Virus Definition	OS6.2.0_75.01617.ETDB (MD5)	2020-02-24
Attack Definition	OS6.2.0_15.00785.NIDS (MD5)	2020-02-24
Industrial Definition	OS6.2.0_15.00784.ISDB (MD5)	2020-02-24
Application Definition	OS6.2.0_15.00785.APDB (MD5)	2020-02-24
Internet Service Definition	fos62_00007.00494 (MD5)	2020-02-24
Botnet IP database	OS6.2.0_4.631 (MD5)	2020-02-24

Verify FortiGate is receiving offline updates

To verify FortiGate is receiving updates:

1. Log in to FortiGate and go to *System > FortiGuard*.
 - If FortiGate is not receiving updates (as in the figure below) proceed to Step 2.
 - If FortiGate is receiving updates proceed to Step 3.

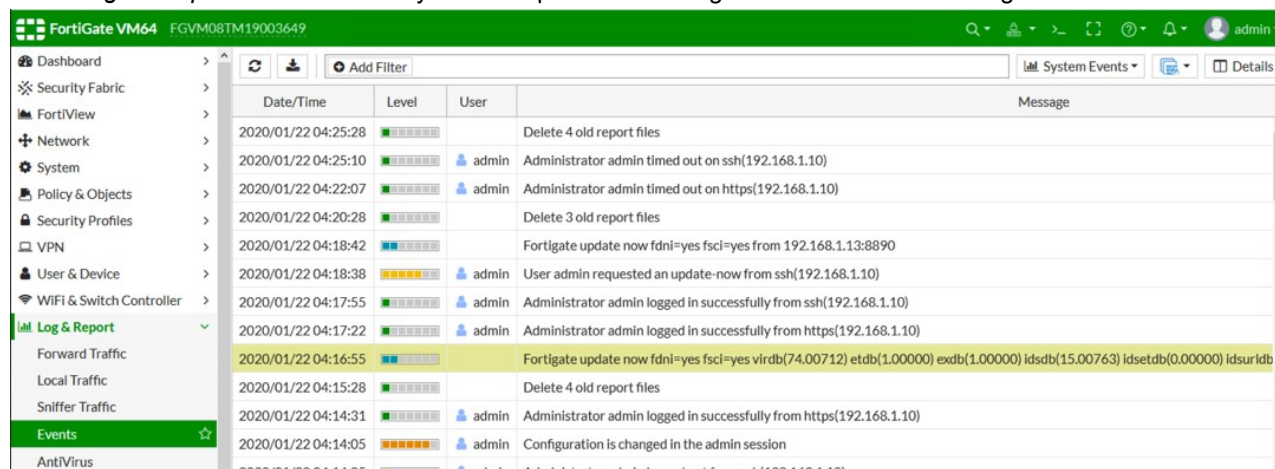
Step 3: FortiManager Security Updates (FortiGate)



2. Update the configuration to disable the default update servers. The complete central management config should be:

```
config system central-management
  set type fortimanager
  set fmg "192.168.1.13"
  config server-list
    edit 1
      set server-type update
      set server-address 192.168.1.13
    next
    edit 2
      set server-type rating
      set server-address 192.168.1.21
    next
  end
  set include-default-servers disable
end
```

- Go to *Logs & Reports > Events*. Verify that the updates are being received from FortiManager.



Date/Time	Level	User	Message
2020/01/22 04:25:28	Information		Delete 4 old report files
2020/01/22 04:25:10	Warning	admin	Administrator admin timed out on ssh(192.168.1.10)
2020/01/22 04:22:07	Warning	admin	Administrator admin timed out on https(192.168.1.10)
2020/01/22 04:20:28	Information		Delete 3 old report files
2020/01/22 04:18:42	Information		Fortigate update now fdni=yes fsci=yes from 192.168.1.13:8890
2020/01/22 04:18:38	Warning	admin	User admin requested an update-now from ssh(192.168.1.10)
2020/01/22 04:17:55	Information	admin	Administrator admin logged in successfully from ssh(192.168.1.10)
2020/01/22 04:17:22	Information	admin	Administrator admin logged in successfully from https(192.168.1.10)
2020/01/22 04:16:55	Information		Fortigate update now fdni=yes fsci=yes virdb(74.00712) etdb(1.00000) exdb(1.00000) idbdb(15.00763) idsetdb(0.00000) idsurldb(0.00000)
2020/01/22 04:15:28	Information		Delete 4 old report files
2020/01/22 04:14:31	Information	admin	Administrator admin logged in successfully from https(192.168.1.10)
2020/01/22 04:14:05	Warning	admin	Configuration is changed in the admin session
2020/01/22 04:14:05	Warning	admin	Administrator admin logged out from ssh(192.168.1.10)

Step 4: FortiManager Security Updates (FortiSandbox)

Install the offline FortiSandbox security updates on FortiManager and verify FortiSandbox is receiving the updates. Install Web Filtering DB on FortiManager and then verify the Web Filtering Queries on FortiGate and FortiSandbox.

Requirements:

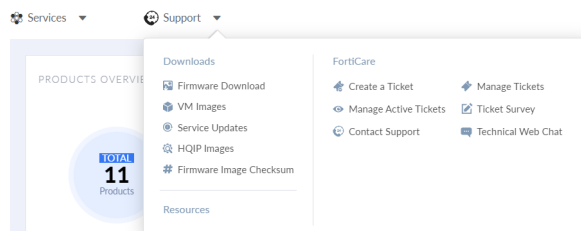
If you have not completed [Install offline FortiGate security updates on FortiManager on page 24](#), please do so now. This will set FortiManager as the update server for FortiSandbox.

To receive offline security updates on FortiSandbox:

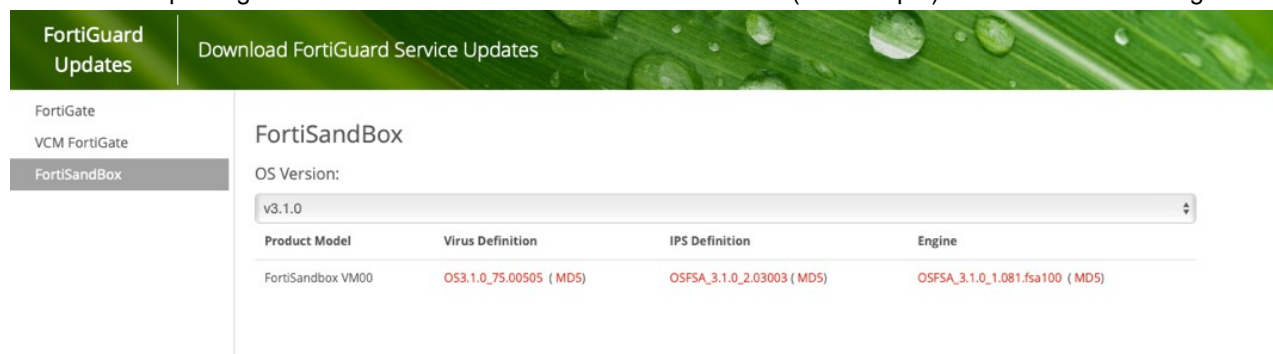
1. [Install Offline FortiSandbox Security Updates on FortiManager on page 28](#)
2. [Verify FortiSandbox is receiving offline updates on page 1](#)
3. [Install Web Filtering DB on FortiManager on page 30](#)
4. [Verifying Web Filtering Queries on FortiGate and FortiSandbox on page 31](#)

Install Offline FortiSandbox Security Updates on FortiManager

1. Log in to [FortiCloud](#). The Asset Management portal opens.
2. Go to *Support > Download > FortiGuard Service Updates*.

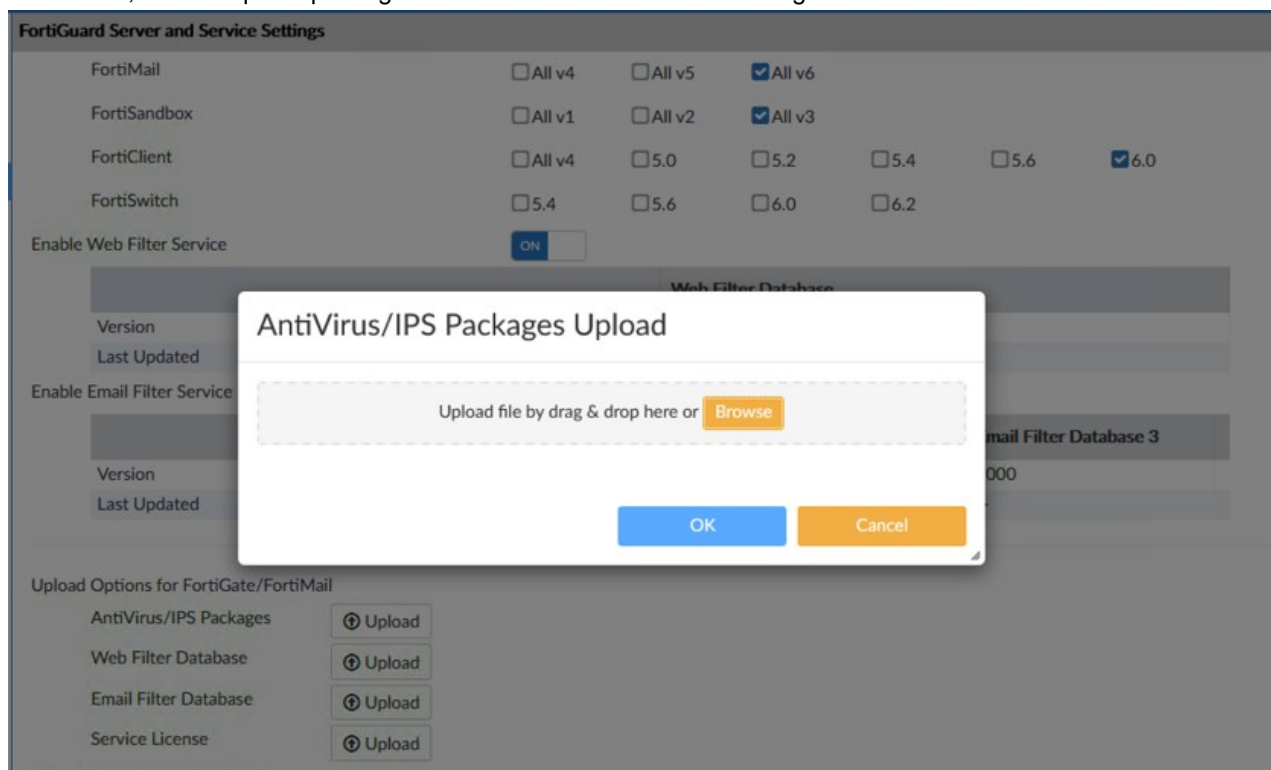


3. Locate the FortiSandbox in the list.
4. Select the version that you would like to use that is supported by FortiManager.
5. Download the packages and have them available on removable media (for example) to install on FortiManager.



6. Log in to FortiManager.
7. Go to *FortiGuard > Settings*.

8. Go to *Upload Options for FortiGate/FortiMail > Antivirus/IPS Packages*, and click *Upload*.
9. Select the packages you downloaded and stored on removable media, and install them on FortiManager. After the installation, all the required packages should be available on FortiManager.



10. Open the CLI console and verify the output of `diagnose fmupdate fds-getobject`.

```

FSA object version information
ObjectID      Description      Version      Size      Created
Date Time
-----
03000000SBDB00100  FortiSandbox AVDB  00076.00212  13 MB  20/03/25 08:20
03000000SBDB00100  FortiSandbox AVDB  00076.00213  13 MB  20/03/25 09:20
03000000SBDB00100  FortiSandbox AVDB  00076.00214  13 MB  20/03/25 10:20
03000000SBDB00100  FortiSandbox AVDB  00076.00215  13 MB  20/03/25 11:20
03000000SBDB00100  FortiSandbox AVDB  00076.00216  13 MB  20/03/25 12:20
03000000SBDB00100  FortiSandbox AVDB  00076.00217  13 MB  20/03/25 13:20
03000000SBDB00100  FortiSandbox AVDB  00076.00218  13 MB  20/03/25
  
```

Verify FortiSandbox is receiving offline updates

On FortiManager, go to *System Settings > Event Log*. Verify the update requests from FortiSandbox.

Remote Certificates	FortiGuard service event	Object update request from device or FortiClient received	Send new version object to device (sn:FSAVM00000013961, ip=127.0.0.1): objid=03001002SBEN01000, curr_ver=03001.00063 new_ver=03001.00081
Event Log	FortiGuard service event	Object update request from device or FortiClient received	Send new version object to device (sn:FSAVM00000013961, ip=127.0.0.1): objid=03001002SBEN00900, curr_ver=03001.00153 new_ver=03001.00177
Task Monitor	FortiGuard service event	Object update request from device or FortiClient received	Send new version object to device (sn:FSAVM00000013961, ip=127.0.0.1): objid=03001000SBD00400, curr_ver=00002.02806 new_ver=00002.03018
Advanced	FortiGuard service event	Object update request from device or FortiClient received	Send new version object to device (sn:FSAVM00000013961, ip=127.0.0.1): objid=03001000SBD00300, curr_ver=00000.00000 new_ver=00076.00222
SNMP	FortiGuard service event	Object update request from device or FortiClient received	Send new version object to device (sn:FSAVM00000013961, ip=127.0.0.1): objid=03001000SBD00200, curr_ver=00000.00000 new_ver=00076.00198
Mail Server	FortiGuard service event	Object update request from device or FortiClient received	Send new version object to device (sn:FSAVM00000013961, ip=127.0.0.1): objid=03001000SBD00100, curr_ver=00001.00000 new_ver=00076.00230
Syslog Server	FortiGuard service event	Object update request from device or FortiClient received	
Meta Fields	FortiGuard service event	Object update request from device or FortiClient received	
Advanced Settings	FortiGuard service event	Object update request from device or FortiClient received	

Install Web Filtering DB on FortiManager

Web filtering DB is not available for download from support.fortinet.com. To download the DB, you need an online FortiManager to download the DB, and then export it to the offline FortiManager.

To install Web Filtering DB on FortiManager:

1. Log in to FortiManager.
2. Go to **FortiGuard > Query Server Management > Receive Status**. Verify that you have the Database FURL.

Package Received	Latest Version (Release Date/Time)	Size	Update History
Web Filter Database 1	22.51748(2020-01-21 19:55:08)	4.98 GB	
Email Filter Database 1	101.54921(2020-01-23 08:30:01)	769.95 MB	
Email Filter Database 2	92.32775(2019-09-27 00:38:01)	44.01 MB	
Email Filter Database 4	78.60521(2019-09-29 03:26:01)	30.71 MB	

3. Prepare an external FTP/SCP/TFTP server on the network to export the DB. Expect the DB to be multiple GBs. To do this, open the FortiManager CLI console and execute the following command:

```
execute fupdate {ftp | scp | tftp} export <type> <remote_file>
<ip> <port> <remote_path><user> <password>
```

The following images shows an example of how exporting the DB to an external FTP server should look.

```
[FMG-VM64 # execute fupdate ftp export url url.db 192.168.3.80 / ahmad fortinet
Package backup is in process... This could take some time.
lcclient command result:Response=202]

Start sending file to FTP Server...
Transferred 6853.073M of 6853.073M in 0:00:33s (202.794M/s)
FTP transfer is successful.
Backup successfully.

FMG-VM64 #
```

4. Copy the DB to a USB stick/CD-DVD Drive and move it to the offline network.
5. Setup the FTP/SCP/TFTP server to import the DB onto the offline FortiManager.
6. Log in to the offline FortiManager.

7. Go to *FortiGuard > Query Server Management > Receive Status*. Verify *FURL* is not selected to ensure there is no URL filter Database.

History	Package Received	Latest Version (Release Date/Time)	Size	Update History
<input type="checkbox"/>	Web Filter Database	0.000(-)	0B	
<input type="checkbox"/>	Email Filter Database 1	0.000(-)	0B	
<input type="checkbox"/>	Email Filter Database 2	0.000(-)	0B	
<input type="checkbox"/>	Email Filter Database 4	0.000(-)	0B	

8. Using the offline FortiManager's CLI console, import the URL filter DB using FortiManager CLI:

```
execute fupdate {ftp | scp | tftp} import <type> <remote_file>
<ip> <port> <remote_path><user> <password>
```

The following images shows an example of importing the DB using an FTP server.

```
FMG-VM64 # execute fupdate ftp import url url.db 192.168.1.10 / ahmad fortinet
This operation will replace the current <url> package!
Do you want to continue? (y/n)y

Start getting file from FTP Server...
Transferred 6853.073M of 6853.073M in 0:00:39s (173.280M/s)
FTP transfer is successful.
Package installation is in process... This could take some time.
locllient command result:Response=202|

Update successfully

FMG-VM64 #
```

9. Go to *FortiGuard > Query Server Management > Receive Status*.
- Ensure you have the Database *FURL*.
 - Double-check the DB Size.

History	Package Received	Latest Version (Release Date/Time)	Size	Update History
<input checked="" type="checkbox"/>	Web Filter Database	22.51748(2020-01-21 19:55:08)	6.38 GB	
<input type="checkbox"/>	Email Filter Database 1	0.000(-)	0B	
<input type="checkbox"/>	Email Filter Database 2	0.000(-)	0B	
<input type="checkbox"/>	Email Filter Database 4	0.000(-)	0B	

Verifying Web Filtering Queries on FortiGate and FortiSandbox

To Verify Web Filtering Queries on FortiGate and FortiSandbox:

1. Log in to FortiGate and enable web filter service and choose *any location* for the location.

```
#config system fortiguard
(fortiguard) # set update-server-location any
(fortiguard) # set webfilter-force-off disable
(fortiguard) # end
```

2. Update the server location on FortiGate.
 - a. Go to *System > FortiGuard*.
 - b. Set the following configurations.

Update server location		<i>Lowest latency locations.</i>
Filtering		
	Web Filter Cache	Enable
	Anti-Spam Cache	Enable
	FortiGuard Filtering Protocol	UDP
	FortiGuard Filtering Port	8888
	Filtering Service Availability	Click <i>Check Again</i> . Verify <i>Web Filtering</i> and <i>Anti-Spam</i> are <i>Up</i> .
Override FortiGuard Servers	Click <i>Create New</i> to add the <i>Server Address</i> and select the <i>Server Type</i> .	

Update Server Location

US only

Lowest latency locations

Filtering

Web Filter Cache

Clear cache after

60

Minutes

Anti-Spam Cache

Clear cache after

30

Minutes

FortiGuard Filtering Protocol

HTTPS

UDP

FortiGuard Filtering Port

443

53

8888

Filtering Services Availability

Check Again

Web Filtering

↑

Anti-Spam

↑

Request re-evaluation of a URL's category

Override FortiGuard Servers

+ Create New

Edit

Delete

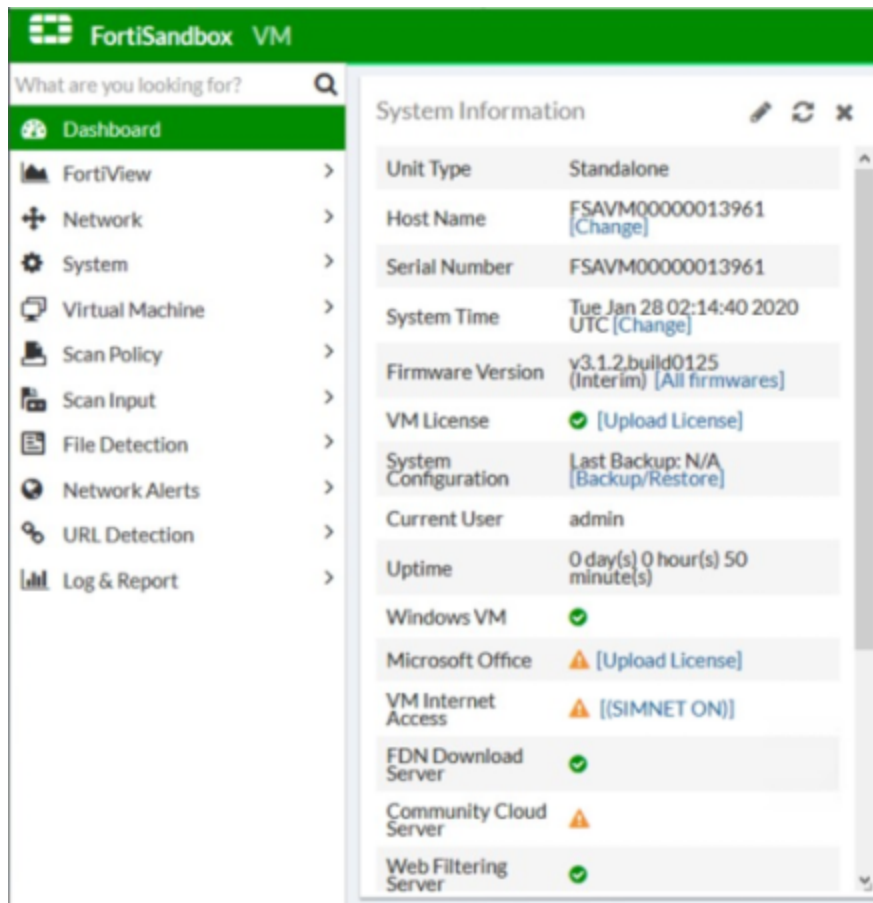
Server Address	Server Type
<div>✓</div> <div>192.168.1.13</div>	Both
Fall back to public FortiGuard servers	Disable

Apply

- c. Click *Apply*.
3. Log in to FortiSandbox.
4. Open the CLI console and issue the command `test-network`. The Web filtering service should turn *ON* in both the CLI output and the *Dashboard*.

FortiSandbox 4.0.0 Air-Gapped Mode
Fortinet Technologies Inc.

33



Step 5: FortiSandbox Microsoft Windows/Office Offline Activation

Install offline Microsoft Windows VMs and then activate the Windows licenses. After the VM licenses are activated, activate the offline Microsoft Office licenses.

To activate the Microsoft Office licenses:

1. [Microsoft Windows VMs Offline Installation on page 35](#)
2. [Offline Microsoft Windows VMs Activation on page 37](#)
3. [Offline Microsoft Office Licenses Activation on page 38](#)

Microsoft Windows VMs Offline Installation

To install MS Windows VMs offline:

1. Log in to [FortiCloud](#). The Asset Management portal opens.
2. Locate the FortiSandbox in the Product List and download the VM package file. For more information, see *Asset Portal Admin Guide* > [Viewing product details](#).



The VM package includes built-in VMs for FortiSandbox. If you need to download additional optional OSs, please ask the Fortinet sales team where to download the required VM package.

3. Copy the VM package to an offline FTP/SCP/HTTPS server and install it to FortiSandbox using *fw-upgrade* command. This process will take some time after reboot.

Example using ftp server:

```
# fw-upgrade -b -v -tftp -sFTP_Server_IP -uuser_name -f/VM00_base.pkg
```

```

> fw-upgrade -b -v -tftp -s192.168.1.10 -uahmad -f/VM00_base.pkg
Password:
You are about to upload and install a new set of VM image. Please do not interrupt
the process. The unit will reboot later.
After reboot, the system will re-activate Microsoft Windows OS if there is any.
Note: One OS license can only be used for activation for a limited number of times.
Do you want to continue? (y/n)y
--2020-01-29 02:12:53-- ftp://192.168.1.10/VM00_base.pkg
      => '/drive0/tmp/vmimage.tmp'
Connecting to 192.168.1.10:21... connected.
Logging in as ahmad ... Logged in!
==> SYST ... done.      ==> PWD ... done.
==> TYPE I ... done.    ==> CWD not needed.
==> SIZE VM00_base.pkg ... 12281379032
==> PASV ... done.      ==> RETR VM00_base.pkg ... done.
Length: 12281379032 (11G) (unauthoritative)

VM00_base.pkg      100%[=====>]  11.44G  56.0MB/s   in 94s

2020-01-29 02:14:26 (125 MB/s) - '/drive0/tmp/vmimage.tmp' saved [12281379032]

Start installing VM image file VM00_base.pkg
Reboot system!
>

```

4. Log in to FortiSandbox after the reboot.
5. Go to *Virtual Machine* > *VM Images* and verify the VM package is available. The package will be disabled by default.

FortiSandbox VM VM Images

What are you looking for?

VM Images

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Default VMs (1/1)						
WIN10X64VM	3	installed	✖	0	0	
Remote VMs (2)						
MACOSX	0	installed	✖	0	0	mac dmg
WindowsCloudVM	0	installed	✖	0	0	exe htm ppsx ppt pptx xls xlam potx sldx pptm ppsl pps pot upx WEBLink Ink

Offline Microsoft Windows VMs Activation

Microsoft Windows activation offline activation is described in Best Practices Guide > [Revalidating Windows license key](#).

Only one key needs to be activated for each Windows VM Type.

To activate offline MS Windows VMs:

1. Log in FortiSandbox.
2. Go to *Log & Report > VM Events*.
3. Record one Product Key and its corresponding installation ID for each OS you want to activate.

Network Alerts	>	19	2020-01-29 03:41:4...	information	system	VMINIT: WIN10X64VM Start activating Windows 10 online with key RNP2-BV4M2-F4Q69-X3KGG-XXXXX
URL Detection	>	20	2020-01-29 03:41:4...	information	system	VMINIT: WIN10X64VM No internet access to activate Windows 10 online
Log & Report	✓	21	2020-01-29 03:41:4...	error	system	VMINIT: WIN10X64VM Failed to activate Windows 10 online with key T9PDN-6JVJ7-8V4RQ-J76RX-XXXXX
All Events		22	2020-01-29 03:41:4...	information	system	VMINIT: WIN10X64VM Windows activation error message: Failed to activate Windows with key T9PDN-6JVJ7-8V4RQ-J76RX-XXXXX
System Events		23	2020-01-29 03:34:5...	information	system	VMINIT: WIN10X64VM Start activating Windows 10 online with key T9PDN-6JVJ7-8V4RQ-J76RX-XXXXX
VM Events		24	2020-01-29 03:34:5...	information	system	VMINIT: WIN10X64VM No internet access to activate Windows 10 online
Job Events		25	2020-01-29 03:34:5...	error	system	VMINIT: WIN10X64VM Failed to activate Windows 10 online with key RNYTD-FQWVH-4MXVF-HB2Y7-XXXXX
Notification Events						
Log Servers						
Local Log						
Dagnostic Logs						
Summary Report						

First Previous Pages: 1 / 4 Next Last Total Logs: 50/196

#	22	Date/Time	2020-01-29 03:41:40
Level	information	User	system
User Interface	system	Action	log
Status	success	Message	VMINIT: WIN10X64VM Windows activation error message: Failed to activate Windows with key T9PDN-6JVJ7-8V4RQ-J76RX-XXXXX: 08538820899540530538562964829374500267209143352910113300009365, 0x80072EE2 On a computer running Microsoft Windows n on-core edition, run 'slui.exe 0x2a 0x80072EE2' to display the error text. activate Windows.
Log ID	0106000001	Sub Type	system
Reason	none	Log Type	event

4. Open the FortiSandbox CLI console and Install the confirmation ID along with its corresponding product Key using the following command:

```
confirm-id.
```

```
> confirm-id -a -kT9PDN-6JVJ7-8V4RQ-J76RX-XXXXX -c202880514405106514054092865234
000460416924240073
Confirmation ID has been added.
```

5. Ensure the confirm-id has been added successfully using the following command:

```
confirm-id -l.
```

```
> confirm-id -l
GTHXH-2NXDM-D4KRR-TD9R9-XXXXX 168846571604113273095393917351166636445324904940
T9PDN-6JVJ7-8V4RQ-J76RX-XXXXX 202880514405106514054092865234000460416924240073
T9V33-NCGV4-MTG7R-RFM6W-XXXXX 217212975595682346920043261151649980320310887266
```


6. Reboot FortiSandbox. After the reboot, go to *Dashboard* to verify the Windows VMs were initialized.

The screenshot displays the FortiSandbox VM interface. On the left is a navigation menu with options: Dashboard (selected), FortiView, Network, System, Virtual Machine, Scan Policy, Scan Input, File Detection, Network Alerts, URL Detection, and Log & Report. The main panel is titled 'System Information' and contains the following details:

Unit Type	Standalone
Host Name	FSAVM00000013961 [Change]
Serial Number	FSAVM00000013961
System Time	Tue Jan 28 02:14:40 2020 UTC [Change]
Firmware Version	v3.1.2,build0125 (Interim) [All firmwares]
VM License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 0 hour(s) 50 minute(s)
Windows VM	✓
Microsoft Office	⚠ [Upload License]
VM Internet Access	⚠ [(SIMNET ON)]
FDN Download Server	✓
Community Cloud Server	⚠
Web Filtering Server	✓

Offline Microsoft Office Licenses Activation

Microsoft Windows activation offline activation is described in Best Practices Guide > [Revalidating Windows license key](#).

Only one key needs to be activated for each Windows VM Type.

To activate offline MS Office licenses:

1. Log in FortiSandbox.
2. Go to *Log & Report > VM Events*.
3. Find the log that reports *office activation failure*, and record the office key and its corresponding installation ID.

The screenshot shows the FortiSandbox interface with the 'Log & Report' section expanded to 'VM Events'. A search filter 'office' is applied. The log table shows several entries, with entry #9 highlighted. Below the table, the details for entry #9 are displayed:

#	9	Date/Time	2020-01-29 09:28:48
Level	information	User	system
User Interface	system	Action	log
Status	success	Message	VMINIT: WIN10X64VMO16 Office activation error message: Failed to activate Office with key GJDBX-N76WD-3X628-XR866-XXXXX: 222238303140420245880592345312532912317060330363679757365598645, 0xC004F017, The Software Licensing Service reported that the license is not installed.
Log ID	0106000001	Sub Type	system
Reason	none	Log Type	event

4. Install the confirmation ID along with its corresponding product Key using the following CLI command:

```
confirm-id -K
```

```
> confirm-id -K GTHXH-2NXDM-D4KRR-TD9R9-XXXXXX -c168846571604113273095393917351166636445324904940
```

5. Ensure the `confirm-id` has been added successfully using the following CLI command:

```
confirm-id -l.
```

```
> confirm-id -l
GTHXH-2NXDM-D4KRR-TD9R9-XXXXXX 168846571604113273095393917351166636445324904940
T9PDN-6JVJ7-8V4RQ-J76RX-XXXXXX 202880514405106514054092865234000460416924240073
T9V33-NCGV4-MTG7R-RFM6W-XXXXXX 217212975595682346920043261151649980320310887266
```

6. Reboot FortiSandbox.

- After FortiSandbox reboots, the Windows and Office Licenses should be activated and initialized.

```

# End of keyboard-interactive prompts from server
> vm-status -l
activated and initialized
Virtual Hosts Initialization ..... Passed

Installed VM Images:
Name           Ver      Type      License      Activation      (App Status)
              Clone   Load   Clone   Load   ImageMD5
WIN10X64VM      3        Local    Permanent    Activated
              0         0
WIN10X64VM016   3        Local    Permanent    Activated      Office 2016(
activated)      1         1
WIN7X86SP1016   2        Local    NoKey        N/A            Office 2016(
installed) 7 keys available 0         0
MACOSX          0        Remote   NoContract   N/A
              0         0
WindowsCloudVM 0        Remote   NoContract   N/A            Office (activ
ated)          0         0
>

















```


System Information

Unit Type	Standalone
Host Name	FSAVM00000013961 [Change]
Serial Number	FSAVM00000013961
System Time	Wed Jan 29 10:09:54 2020 UTC [Change]
Firmware Version	v3.1.2,build0125 (Interim) [All firmwares]
VM License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 0 hour(s) 16 minute(s)
Windows VM	✓
Microsoft Office	✓ [Upload License]
VM Internet Access	⚠ [(SIMNET ON)]
FDN Download Server	✓
Community Cloud Server	⚠
Web Filtering Server	✓

8. Go to **System > Virtual Machine > VM Images** the FortiSandbox Scan profile:

- Assign the Office files to the VM that has Office installed.
- Assign *Clone #* a value greater than or equal to 1.

System	>		Name	Version	Status	Enabled	Clone #	Load #	Extensions
Virtual Machine	>	- Default VMs (1/1)							
VM Status			 WIN10X64VM	3	 activated		0	0	
VM Images		- Optional VMs (1/1)							
Scan Policy	>		 WIN10X64VMO16	3	 activated		1	1	
Scan Input	>	- Remote VMs (2)							
File Detection	>		 MACOSX	0	 installed		0	0	mac dmg
Network Alerts	>		 WindowsCloudVM	0	 installed		0	0	exe htm ppsx ppt pptx xls xlsx dll doc docx rtf pdf swf jar dotx docm dotm xltb xltm xlsx xlam potx sldx pptm ppsm potm ppam sldm onetoc thmx bat cmd vbs ps1 js msi msg url dot xlt pps pot upx WEBLink Ink wsf eml lqy jse scr
URL Detection	>								
Log & Report	>								
<div>Apply</div>									

Step 6: FortiSandbox File Query DB

Verify File Query DB on the Online FortiManager and then Export File Query DB. After you export the query DB, verify FortiSandbox can query the DB.

To query the DB with FortiSandbox:

1. [Verify File Query DB on the Online FortiManager on page 42](#)
2. [Export File Query DB on page 42](#)
3. [Import File Query DB into FortiManager on page 43](#)
4. [Configure and Verify FortiSandbox can query file DB on page 43](#)

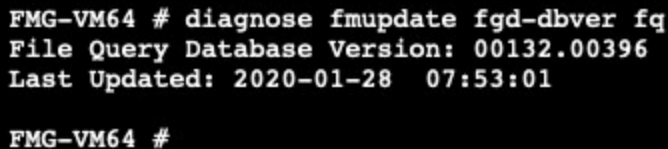
Verify File Query DB on the Online FortiManager

To verify File Query DB on the online FortiManager:

1. Verify File Query DB on the Online FortiManager using the following CLI command:

```
config fmupdate service
set query-filequery enable
end
```
2. Allow time for the file query DB to update. Ensure the file query DB is available and up-to-date using the following CLI command:

```
diagnose fmupdate fgd-dbver fq
```



```
FMG-VM64 # diagnose fmupdate fgd-dbver fq
File Query Database Version: 00132.00396
Last Updated: 2020-01-28 07:53:01
FMG-VM64 #
```

Export File Query DB

Once the DB update is verified on the online FortiManager, export the file query DB to a FTP/SCP/TFTP Server using the command:

```
execute fmupdate
```

The following example shows the export file query DB using FTP server.

```
FMG-VM64 # execute fmupdate ftp export file-query file.md5 192.168.3.80 / ahmad fortinet
Package backup is in process... This could take some time.
lcclient command result:Response=202|

Start sending file to FTP Server...
Transferred 4867.516M of 4867.516M in 0:00:20s (231.986M/s)
FTP transfer is successful.
Backup successfully.

FMG-VM64 #
```

Import File Query DB into FortiManager

Using USB Stick or CD/DVD Drive, copy the file to a FTP server inside the closed network. Import the file query DB into the offline FortiManager using the following CLI command:

```
execute fmupdate
```

```
FMG-VM64 # execute fmupdate ftp import file-query file.md5 192.168.1.10 / ahmad fortinet
This operation will replace the current <file-query> package!
Do you want to continue? (y/n)y

Start getting file from FTP Server...
Transferred 4867.516M of 4867.516M in 0:00:23s (206.192M/s)
FTP transfer is successful.
Package installation is in process... This could take some time.
lcclient command result:Response=202|

Update successfully

FMG-VM64 #
```

Configure and Verify FortiSandbox can query file DB

To verify FortiSandbox can query file DB:

1. Verify the file query DB is successfully imported and available in the offline FortiManager using the following CLI command:

```
diagnose fmupdate.
```

2. Enable file query service on the offline FortiManager so FortiSandbox can query the service.

```

FMG-VM64 # config fmupdate service

(service)# set query-filequery enable

(service)# end

FMG-VM64 #

```

3. Configure FortiManager to log all the service query events using `config fmupdate` command line.

```

FMG-VM64 # config fmupdate web-spam fgd-setting

(fgd-setting)# set fq-log all

(fgd-setting)# end

```

4. On FortiSandbox, issue the command line `test-network` to verify the file query service status. The service status should be *Success*.

```

Testing FSA community cloud service ++++++
Access FGD cloud server: Failed
Connect to FGD file server: Success

```

5. On FortiManager shell, verify the file query request is received from FortiSandbox by checking the `fgdsvr.log` under `/var/log`.

```

2020/03/01_00:25:58.866 debug   FGDSVR(FileQuery)[974]: FQ2->FileQuery: req{ip:1
92.168.1.11, devid:FSAVM00000013961, subver:0, fsig:sig[0].dig:6c623fe8fc451cfc6
9e5e036aaebe55912feea879caab485ff56fba9c8e67f78 .flen:0} resp{dbver:132.397, num
info:1, info[0].fid=0x191653ef,flag=0x4}

```

```

FMG-VM64 # diagnose fmupdate fgd-dbver fq
File Query Database Version: 00132.00397
Last Updated: 2020-01-28 08:49:53

FMG-VM64 #

```



www.fortinet.com

Copyright© 2021 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 General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. 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.