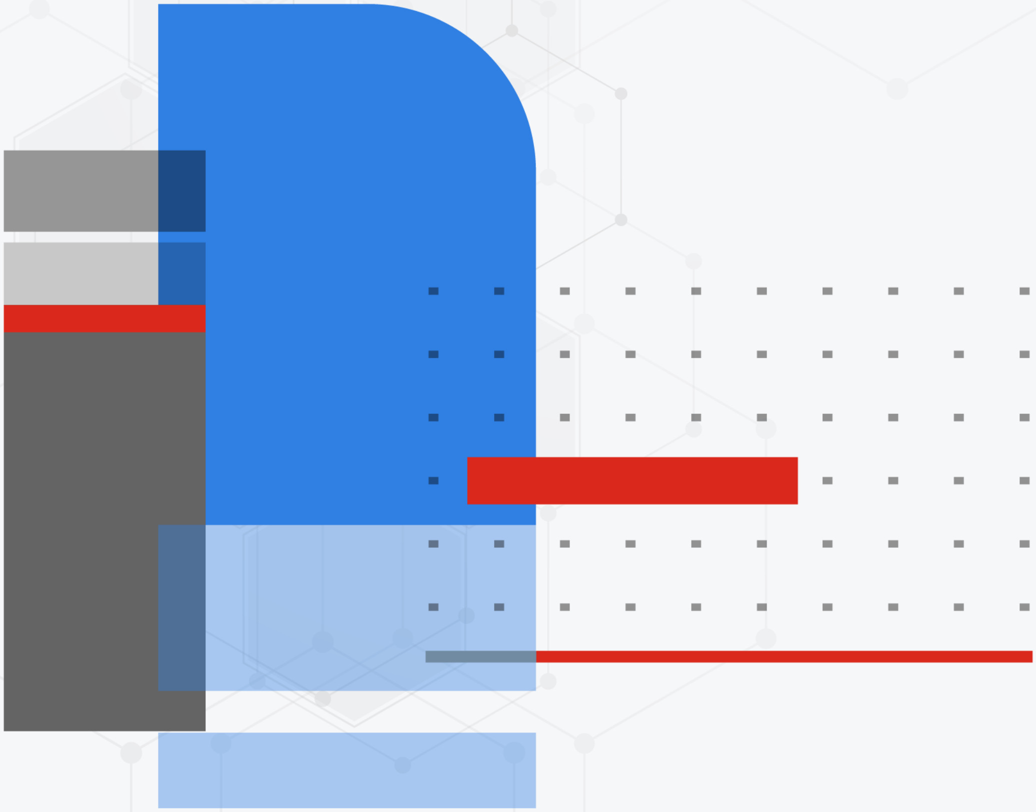
KVM Administration Guide

FortiPAM 1.2.0



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

FORTINET®

March 6, 2024
FortiPAM 1.2.0 KVM Administration Guide
74-120-936954-20240306

TABLE OF CONTENTS

Change Log 4
Introduction 5
FortiPAM-VM Overview 6
Licensing 6
System requirements 7
VM requirements 7
FortiPAM-VM sizing guidelines 8
Log and video disk size guidelines 8
Register FortiPAM-VM on FortiCloud 8
Download the FortiPAM-VM software 9
KVM deployment package contents 9
Unlicensed FortiPAM-VM 10
FortiPAM-VM Deployment 12
Deploying FortiPAM-VM on KVM 12
Installing vTPM package on KVM and adding vTPM to FortiPAM-VM 14
Power on your FortiPAM-VM 15
Initial Configuration 16
FortiPAM-VM GUI access 16
Upload the FortiPAM-VM license file 19
Enable vTPM 20
Configure your FortiPAM-VM 21

Change Log

Date	Change Description
2023-12-15	Initial release.
2024-01-15	Updated FortiPAM-VM GUI access on page 16.
2024-03-06	Updated System requirements on page 7.

Introduction

FortiPAM is a privileged access management solution. FortiPAM solutions are an important part of an enterprise network, providing role-based access, auditing, and security options for privileged users (users that have system access beyond that of a regular user).

For information on FortiPAM features, see the *FortiPAM Administration Guide* on the Fortinet Docs Library.

This document includes an overview of the FortiPAM-VM, its deployment with KVM, and information on how to perform an initial configuration.

FortiPAM-VM Overview

This section provides an overview of FortiPAM-VM.

The following topics are included in this section:

- Licensing on page 6
- System requirements on page 7
- Register FortiPAM-VM on FortiCloud on page 8
- Download the FortiPAM-VM software on page 9
- Unlicensed FortiPAM-VM on page 10

Licensing

Fortinet offers FortiPAM in a yearly user subscription model.

Contact your Fortinet Authorized Reseller for more information.

Virtualization environment supported:

- KVM

FortiPAM-VM support options:

SKU	Description
FC1-10-PAVUL-591-02	One year subscription for one FortiPAM Virtual Machine seat for 5 to 9 users. • Includes FortiClient VRS agent for FortiPAM. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC2-10-PAVUL-591-02	One year subscription for one FortiPAM Virtual Machine seat for 10 to 24 users. • Includes FortiClient VRS agent for FortiPAM. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC3-10-PAVUL-591-02	One year subscription for one FortiPAM Virtual Machine seat for 25 to 49 users. • Includes FortiClient VRS agent for FortiPAM. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC4-10-PAVUL-591-02	One year subscription for one FortiPAM Virtual Machine seat for 50 to 99 users. • Includes FortiClient VRS agent for FortiPAM. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.

SKU	Description
FC5-10-PAVUL-591-02	One year subscription for one FortiPAM Virtual Machine seat for 100 to 249 users. • Includes FortiClient VRS agent for FortiPAM. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC6-10-PAVUL-591-02	One year subscription for one FortiPAM Virtual Machine seat for 250 or more users. • Includes FortiClient VRS agent for FortiPAM. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.

Note: The SKUs are user license/seats for different pricing level.

After placing an order for FortiPAM-VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiPAM-VM with FortiCloud.

Upon registration, you can download the license file. You will need this file to activate your FortiPAM-VM. For more information on configuring basic network settings and applying your license, see the *FortiPAM Administration Guide*.

System requirements

Prior to deploying the FortiPAM-VM virtual appliance, your virtual machine manager must be installed and configured. The installation instructions for FortiPAM-VM assume you are familiar with both VM platforms and their related terminology. FortiPAM-VM includes support for:

- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0

For the latest information on virtualization software support, see the corresponding *FortiPAM Release Notes* on the Fortinet Docs Library.

Upgrade to the latest stable server update and patch release.

VM requirements

The following table provides a detailed summary on FortiPAM virtual machine (VM) system requirements. Installing FortiPAM-VM requires that you have already installed a supported VM environment.

Virtual machine	Requirement
Virtual CPUs supported (maximum)	256
Virtual NICs supported (maximum)	10

Virtual machine	Requirement
Storage support (maximum)	16 TB
Memory support (minimum)	2 GB
High Availability (HA) support	Yes (Active-Passive HA)

FortiPAM-VM sizing guidelines

The following table provides FortiPAM-VM sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

Users	Virtual CPUs	Memory	Storage
20 - 1000	4 - 64	16 GB to 256 GB	2 TB to 16 TB

Log and video disk size guidelines

The following tables provide FortiPAM log and video disk sizing guidelines.

Disk	Requirement
Log (minimum)	10 GB
Video (minimum)	10 GB

Video length	Video file size
1 hour	250 MB

Video disk size should be planned according to the number of video recording sessions and the duration of each session.

For example: If, on average, there are 100 one-hour launching sessions with video recording enabled every day, 25 GB (250 MB x 100) video files are added to the video disk.

For the log disk size, we recommend log and video disk ratio should be 1:3. For example, if the video disk size is 2 TB, log disk size should be 700 GB.

If the disk size is more than 2 TB, you must use RAID. See RAID.

Register FortiPAM-VM on FortiCloud

To obtain the FortiPAM-VM license file you must first register your FortiPAM-VM on FortiCloud.

To register your FortiPAM-VM:

1. Go to the FortiCloud portal and create a new account or log in with an existing account.
   The *Asset Management* portal opens.
2. In *Asset Management*, select *Register Now* to register FortiPAM.
3. Provide your registration code:
   a. Enter your product serial number, service contract registration code, or license certificate number.
   b. Choose your end user type as either a government or non-government user.
   c. Click *Next*.
4. The *Fortinet Product Registration Agreement* page displays. Select the check box to indicate that you have read, understood, and accepted the service contract. Click *Next*.
5. The *Verification* page displays. Select the checkbox to indicate that you accept the terms. Click *Confirm*.
   Registration is now complete and your registration summary is displayed.
6. On the *Registration Complete* page, download the license file (`.lic`) to your computer.
   You will upload this license to activate the FortiPAM-VM.

⚠ After registering a license, Fortinet servers can take up to 30 minutes to fully recognize the new license. When you upload the license file to activate the FortiPAM-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Download the FortiPAM-VM software

Fortinet provides the FortiPAM-VM software for 64-bit environments in two formats:

Upgrades: Download this firmware image to upgrade your existing FortiPAM-VM installation.

- FPA_KVM-v1xx-build0xxx-FORTINET.out

New Installations: Download for a new FortiPAM-VM installation.

- FPA_KVM-v1xx-build0xxx-FORTINET.out.kvm.zip

For more information see the FortiPAM product datasheet available on the Fortinet web site.

KVM deployment package contents

The **FPA_KVM-v1xx-build0xxx-FORTINET.out.kvm.zip** file contains the following QCOW2 file:

- fortipam.qcow2

FortiPAM-VM firmware images in the FortiCloud FTP directory are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FPA_VMWARE-v100-build0012-FORTINET.out.ovf.zip image found in the v1.0 directory is specific to the FortiPAM-VM VMware environment.

You can download the *FortiPAM Release Notes* available on the Fortinet web site.

To download the FortiPAM-VM .zip package:

1. Log into FortiCloud.
2. Go to *Support* > *Downloads*, and select *Firmware Download* from the dropdown list.
   The *Firmware Images* page opens.
3. In the *Firmware Images* page, select *FortiPAM*.
4. On the *Download* tab, browse to the appropriate directory in the FTP site for the version that you would like to download.
5. Download the `kvm.zip` file and *FortiPAM Release Notes*, and save these files to your management computer.
   Select the `.zip` file on your management computer and extract the files to a new file folder.

Unlicensed FortiPAM-VM

FortiPAM platforms work in evaluation mode until licensed.

In the evaluation mode:

1. A maximum of 2 users are allowed; a default *Super Administrator* and an additional user.
2. You can log in to the firewall VIP using `https`.
3. The evaluation license expires after 15 days.
4. All the features are available. You can create secret and launch secrets for a target server.
5. FortiPAM does not have a valid serial number.
6. No FortiCare support is available.

FortiPAM configured with no more than 2 CPUs and 2048 MB of RAM works in the evaluation mode until licensed. Otherwise, a valid license is required.

DLP is available for secret launching only when you have a valid Advanced Malware Protection (`AVDB & DLP`) license.

A FortiPAM-VM is unlicensed until the administrator uploads a Fortinet-issued license file.

No activation is required for the unlicensed FortiPAM-VM.

Technical support is not included with the unlicensed FortiPAM-VM.

Please contact your Fortinet Reseller should you require an extended evaluation.

For information on registering and downloading a FortiPAM license, license expiry, and license renewal, see Licensing in the latest *FortiPAM Administration Guide*.

FortiPAM-VM Deployment

For best performance, it is recommended that FortiPAM-VM is installed on a “bare metal” hypervisor. Hypervisors that are installed as applications on top of a general purpose operating system (such as Microsoft Windows, Mac OS X, or Linux) will have fewer computing resources available due to the host OS’s own overhead.

The following sections detail deployments for KVM:

- Deploying FortiPAM-VM on KVM
- Installing vTPM package on KVM and adding vTPM to FortiPAM-VM on page 14
- Power on your FortiPAM-VM

Deploying FortiPAM-VM on KVM

Once you have downloaded the `out.kvm.zip` file and extracted the virtual hard drive image file fortipam.qcow2, you can create the virtual machine in your KVM environment.

To deploy the FortiPAM-VM virtual machine:

1. Launch *Virtual Machine Manager* on your KVM host server.
2. From the Virtual Machine Manager (VMM) home page, select *Create a new virtual machine*.
3. Select *Import existing disk image* and select *Forward*.
4. Select *Browse*.
   If you saved the `fortipam.qcow2` file to */var/lib/libvirt/images*, it will be visible on the right. If you saved it somewhere else on your server, select *Browse Local*, find it, and select *Open*.
5. Select the *OS type* as *Generic default* and select *Forward*.
6. Specify the amount of memory and the number of CPUs to allocate to this virtual machine.
   You can set the memory as 4GB and the CPUs to 4.

   Select *Forward*.
7. Enter the name for the VM.
   A new VM includes one network adapter by default.
8. Check *Customize configuration* before installation, and select *Finish*.

To add additional hard disks:

Before opening your virtual machine for the first time you will need to configure two additional hard disks: one for the log disk and the other for the video disk.

1. Click *Add Hardware* in the Virt-manager application, and select the option to add an additional storage disk.
2. For the *Storage size*, select a size according to the disk sizing guidelines. See System requirements on page 7.
3. For *Bus type* select *VirtIO*.
4. Click *Finish*.

To add ethernet interfaces:

Before opening your virtual machine for the first time you will need to configure two ethernet interfaces.

1. In the Virtual Machine Manager, locate the VM name, then select *Open* from the toolbar.
2. Select `NIC:xxxx`; the default network adapter.
3. In Network source dropdown, select `Host device enxxxx: macvtap`.
4. In the *Device model* dropdown, select *virtio*.
5. Click *Apply*.
6. Click *Add Hardware*, and select the option to add an additional interface.
7. In the *Device model* dropdown, select *virtio*.
8. Select *Finish*.
9. Click *Begin Installation* to start installing the new VM.

To add log/video disks or modify disk sizes after first powering up FortiPAM-VM:

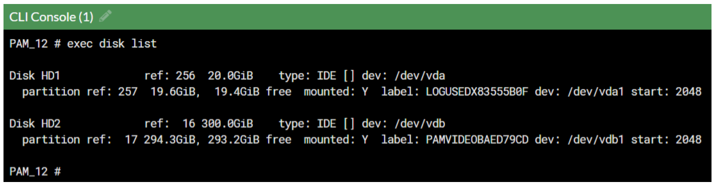
1. In the CLI console, enter `sh sys storage` to verify that the disk size change was successful:

   ```
   config system storage
      edit "HD1"
         set status enable
         set media-status enable
         set order 1
         set partition "LOGUSEDX83555B0F"
         set device "/dev/vda1"
         set size 20029
         set usage log
      next
      edit "HD2"
         set status enable
         set media-status enable
         set order 2
         set partition "PAMVIDEOBAED79CD"
         set device "/dev/vdb1"
         set size 301354
         set usage video
      next
      edit "HD3"
         set status enable
         set media-status disable
         set order 3
         set partition ''
         set device ''
   ```

   If the displayed disk size is not what you had configured, enter the following command to format the log and the video disk:

   ```
      execute disk format <disk_ref>
   ```

   Note: `<disk_ref>` can be checked using the command execute disk list.

   CLI Console (1)

   ```
   PAM_12 # exec disk list

   Disk HD1            ref: 256  20.0GiB    type: IDE [] dev: /dev/vda
     partition ref: 257  19.6GiB,  19.4GiB free  mounted: Y  label: LOGUSEDX83555B0F dev: /dev/vda1 start: 2048

   Disk HD2            ref:  16 300.0GiB    type: IDE [] dev: /dev/vdb
     partition ref:  17 294.3GiB, 293.2GiB free  mounted: Y  label: PAMVIDEOBAED79CD dev: /dev/vdb1 start: 2048

   PAM_12 #
   ```

   HD1 is used for the log disk and the disk_ref is 256.

HD2 is used for the video disk and the disk_ref is 16.

In the above example, disks can be formatted by entering the following commands:

```
execute disk format 256 #HD1
execute disk format 16 #HD2
```

Disk formatting results in the loss of all existing logs and videos.

Installing vTPM package on KVM and adding vTPM to FortiPAM-VM

For added security when installing FortiPAM on KVM, vTPM package must be installed, and vTPM added to the FortiPAM-VM.

To install vTPM package on KVM (Ubuntu):

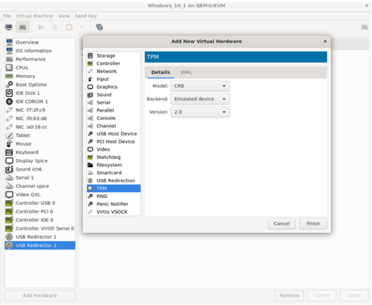
1. In the command line, enter the following commands:

```
mkdir TPM_WorkSpace
cd TPM_WorkSpace/
git clone https://git.seabios.org/seabios.git
git clone https://github.com/stefanberger/libtpms.git
ls
cd libtpms
sudo apt-get -y install automake autoconf libtool gcc build-essential libssl-dev dh-
     exec pkg-config gawk
./autogen.sh --with-openssl --with-tpm2
make dist
dpkg-buildpackage -us -uc -j$(nproc)
cd ..
ls
sudo dpkg -i libtpms0_0.10.0~dev1_amd64.deb libtpms-dev_0.10.0~dev1_amd64.deb
git clone https://github.com/stefanberger/swtpm.git
cd swtpm
sudo su
ln -s /dev/null /etc/systemd/system/trousers.service
exit
sudo apt-get -y install libfuse-dev libglib2.0-dev libgmp-dev expect libtasn1-dev
     socat tpm-tools python3-twisted gnutls-dev gnutls-bin softhsm2 libseccomp-dev
     dh-apparmor libjson-glib-dev
dpkg-buildpackage -us -uc -j$(nproc)
dpkg -i swtpm_0.8.0~dev1_amd64.deb swtpm-dev_0.8.0~dev1_amd64.deb swtpm-libs_
     0.8.0~dev1_amd64.deb swtpm-tools_0.8.0~dev1_amd64.deb
```

To add vTPM when creating a FortiPAM-VM:

1. Deploy FortiPAM, see Deploying FortiPAM-VM on KVM on page 12.
2. Before opening the virtual machine for the first time, in the Virt-manager application, click *Add Hardware*.
3. From the menu, select *TPM*.

4. In the *Details* tab:
   a. In *Model*, select *CRB*.
   b. In *Backend*, select *Emulated device*.
   c. In *Version*, select *2.0*.
   d. Click *Finish*.



Model: CRB
Backend: Emulated device
Version: 2.0

This adds *TPM v2.0* to the list of hardware devices on the left.

Power on your FortiPAM-VM

You can now power on your FortiPAM-VM.

Initial Configuration

Before you can connect to the FortiPAM-VM GUI you must configure basic network settings via the console in your client. Once configured, you can connect to the FortiPAM-VM GUI and upload the FortiPAM-VM license file that you downloaded from FortiCloud.

The following topics are included in this section:

- FortiPAM-VM GUI access on page 16
- Upload the FortiPAM-VM license file on page 19
- Enable vTPM on page 20
- Configure your FortiPAM-VM on page 21

FortiPAM-VM GUI access

To enable GUI access to the FortiPAM-VM you must configure basic network settings of the FortiPAM-VM in the client console.

To configure basic settings in FortiPAM-VM:

1. Power on your virtual machine, and enter the VM *Console*.
2. At the FortiPAM-VM login prompt enter the username `admin` and password.
   The default password is no password. You will be prompted to create a new password.
3. At the CLI prompt, enter `show system storage` to verify the disk usage type for the two added hard disks. The output looks like the following:

   Administrators need to configure a dedicated FortiPAM video disk for video recording.

   Two hard disks and two virtual network interface cards need to be added to the VM in VM manager before FortiPAM image installation.
   See Deploying FortiPAM-VM on KVM on page 12.

```
config system storage
  edit "HD1"
    set status enable
    set media-status enable
    set order 1
    set partition "LOGUSEDXDE8326F6"
    set device "/dev/vda1"
    set size 20023
    set usage log
  next
  edit "HD2"
    set status enable
```

```
      set media-status enable
      set order 2
      set partition "PAMVIDEOB471724F"
      set device "/dev/vdb1"
      set size 20029
      set usage video
   next
end
```

4. Enter the following CLI commands to set up FortiPAM:

```
config system interface
   edit "port1"
      set ip 172.16.x.x/x #Depending on your network setting
      set type physical
      set snmp-index 1
   next
   edit "port2"
      set ip x.x.x.x/x
      set type physical
      set snmp-index 2
   next
end
config router static
   edit 1
      set gateway x.x.x.x
      set device "port1"
   next
end
```

The IP address set here is automatically copied to VIP.

5. FortiPAM requires license. To upload a license, see Upload the FortiPAM-VM license file on page 19.
If the network layout is unable to resolve the correct external FortiGuard server after an external DNS server is set, enter the following commands:

```
config system fortiguard
   set fortiguard-anycast disable
   unset update-server-location
   unset sdns-server-ip
end
```

Optionally, enter the following commands to use the external FortiGuard server in case the FortiGuard server cannot be correctly resolved:

```
config system central-management
   config server-list
      edit 1
         set server-type update rating
         set server-address <addr>
      next
   end
   set include-default-servers disable
end
```

6. On a web browser, go to `https://172.16.xxx.xxx` to access FortiPAM GUI.

FortiCloud currently does not support IPv6 for FortiPAM-VM license validation. You must specify an IPv4 address in both the support portal and the port1 management interface.

Glass breaking mode

Glass breaking in FortiPAM means extending the user permission to access data that the user is not authorized to access. Typically, user access is controlled by permission defined in every secret and folder. In a rare situation, such as a network outage or the remote authentication server becoming unreachable, glass breaking allows you to temporarily access important secrets and target servers to resolve issues.

As a best practice, only a few administrators should have access to the glass breaking mode. Further, the glass breaking mode should only be activated under exceptional situations and for disaster recovery. Email notifications can also be configured to send alerts whenever someone enters glass breaking mode.

To enable glass breaking alert email notifications:

1. Ensure that *Email Service* is set up in *System* > *Settings*.
2. Go to *Log & Report* > *Email Alert Settings*, and select *Enable email notification*.
3. In the *Glassbreaking Notification* tab:
    a. In *From*, enter the email address of the sender.
    b. In *To*, enter the email address of the receiver.
4. Click *Apply*.

Setting up an email alert for glass breaking excludes other important notifications, e.g., administrative change (configuration and HA status) and security (virus detection).

To update firmware image:

1. You can only upload a firmware when in maintenance mode. See Maintenance mode.
2. In the user dropdown on the top-right, go to *System* > *Firmware*.
   The *Firmware Management* window opens.
3. Go to *File Upload*:
    a. Select *Browse*, then locate the `image.out` FortiPAM firmware image on your local computer.
    b. Click *Open*.
4. Click *Confirm and Backup Config*.
   The firmware image uploads from your local computer to the device, which will then reboot. For a short period of time during this reboot, the device is offline and unavailable.

To enter maintenance mode:

1. From the user dropdrown, select *Activate Maintenance Mode* in *System*.
2. In the *Warning* dialog:
    a. Enter the maximum duration, in minutes.
    b. Enter a reason for activating the maintenance mode.
    c. Click *OK*.

Upload the FortiPAM-VM license file

Before using the FortiPAM-VM you must enter the license file that you downloaded from FortiCloud upon registration.

Plan a maintenance window to apply the FortiPAM-VM license as the VM will reboot.

As your organization grows, you can simply either allocate more resources or migrate your virtual appliance to a physical server with more power, then upgrade your FortiPAM-VM license to support your needs.

There are two methods to upload the license file to FortiPAM-VM.

To upload the FortiPAM-VM license file via the GUI:

You must be in maintenance mode to be able to upload a license. See Maintenance mode.

1. Log in to the FortiPAM-VM from a browser.
   Access FortiPAM by using the IP address configured on FortiPAM port1.

   The *Upload License File* pane appears immediately after you log in.

   If FortiPAM is in evaluation mode, go to *Dashboard* > *Status*, click the *Virtual Machine* widget, and click *FortiPAM VM License*.

   Use the `https` prefix with the FortiPAM IP address to access the FortiPAM-VM GUI.
2. In the *Upload License File* pane, select *Upload* and browse to the license file on your management computer.
3. Click *OK*.
4. After the boot up, the license status changes to valid.

   Use the CLI command `get system status` to verify the license status.

To upload the license through the public IP address using SCP:

Use the following command:

```
scp <license_file> admin@<public_ip_address>:vmlicense
```

For example:

```
$ scp FPAVULTM23000007.lic admin@52.52.143.64:vmlicense
```

```
admin@52.52.143.64's password:
FPAVULTM23000xxx.lic 100% 9128 344.0KB/s 00:00
100-install VM license completed
```

Enable vTPM

TPM should be enabled when you initially install FortiPAM.

If you enable TPM after secrets have been configured on FortiPAM, secret credentials may be corrupted.

On FortiPAM-VM, TPM can only be enabled after enabling vTPM. See Installing vTPM package on KVM and adding vTPM to FortiPAM-VM on page 14.

To enable vTPM on FortiPAM-VM:

1. In the CLI console, enter the following commands:

```
config system global
  set v-tpm enable
end
```

To enable TPM on FortiPAM-VM:

FortiPAM must be in maintenance mode to change TPM settings.

1. In the CLI console, enter the following commands:

```
  config sys maintenance
    set mode enable
  end
  config system global
    set private-data-encryption enable
  end
Be carefull!!!This operation will refresh all ciphered data!
Backup the current configuration file at first!
Do you want to continue? (y/n)y
Please type your private data encryption key (32 hexadecimal numbers):
0123456789abcdef0123456789abcdef
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0123456789abcdef0123456789abcdef
Your private data encryption key is accepted.
```

The key must be the same for data restoration between source FortiPAM and destination FortiPAM.

To disable TPM:

1. In the CLI console, enter the following commands:
   ```
     config sys maintenance
       set mode enable
     end
     config system global
       set private-data-encryption disable
     end
   Be carefull!!!This operation will refresh all ciphered data!
   +Backup the current configuration file at first!
   +Do you want to continue? (y/n)y
   ```
   For FortiPAM-VM, vTPM should be disabled after disabling TPM.

To disable vTPM for FortiPAM-VM:

1. In the CLI console, enter the following commands:
   ```
     config system global
       set v-tpm disable
     end
   This operation will stop using vTPM module
   Do you want to continue? (y/n)y
   ```

Configure your FortiPAM-VM

Once the FortiPAM-VM license has been validated you can begin to configure your device. For more information on configuring your FortiPAM-VM see the *FortiPAM Administration Guide* on the Fortinet Document Library.

www.fortinet.com