FortiSIEM - ESX Installation Guide

Version 5.2.6

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

11/20/2019
FortiSIEM 5.2.6 ESX Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
09/05/2018	Initial version of FortiSIEM - ESX Installation Guide.
03/29/2019	Revision 1: updated the instructions for registering the Collector on the Supervisor node.
05/22/2019	Revision 2: added a note regarding VMotion support.
11/20/2019	Release of FortiSIEM - ESX Installation Guide for 5.2.6.

Installing FortiSIEM on VMware ESX

This document provides instructions to install FortiSIEM on VMware ESX.

FortiSIEM Virtual Appliance supports VMotion subject to the limitations of maximum CPU cores supported by VMotion. As an example, VMWare with Enterprise Plus license will allow the movement of up to 4 VMs with 4vCPUs, each using vMotion and DRS.

A change to the configuration file of VMWare will allow movement of up to 16vCPUs in one go. You can't move more than 16vCPUs in one go so you should consider a maximum of 16 vCPUs of FortiSIEM infrastructure in each ESXi host. This could be 1 Super with 8vCPUs, 1 x Worker with 8vCPUs on ESXi #1 and 2 x Workers with 8 vCPUSs each on ESXi#2, then the Virtual Appliances can be moved to ESXi #3 and/or ESXi #4 in one go.

Please ensure that you refer to the VMware documentation as these limitations are subject to change by VMware, and clarification should be sought as needed from VMware.

Pre-installation check-list

Step A: Determine your FortiSIEM hardware needs and deployment type

Before you begin, check the following:

1. Number of Workers needed, if any.
2. Number of Collectors needed, if any.
3. Hardware specification of Supervisor, Worker and Collectors (CPU, RAM, Local Storage)

If Elasticsearch is chosen as the Event Database, the Supervisor needs an additional 8 GB RAM - in this case, the minimum requirement of the Supervisor is 32 GB RAM.

4. Event Database Storage – Local or Remote (For Remote - NFS or Elasticsearch)
   Note: The Remote option is required if you are deploying Workers. If you are going to add Workers in the future, then it is recommended to choose a Remote database option to avoid data migration.
5. Deployment type – Enterprise or Service Provider

Step B: Deploy Remote Storage

Before you install FortiSIEM virtual appliance in ESX, you should decide whether to use NFS storage, local or Elasticsearch storage to store event information in EventDB. If you decide to use a 'Local' disk, you can add a data disk of appropriate size. For 'Local' and 'NFS' storage, refer to the Sizing Guide here. Typically, this will be named as `/dev/sdd` if it is the 4th disk.

If required, install and configure NFS or Elasticsearch before beginning the installation below:

- *For NFS deployment, see FortiSIEM - NFS Storage Guide here.*
- *For Elasticsearch deployment, see FortiSIEM - Elasticsearch Storage Guide here.*

Installation FortiSIEM Virtual Appliance on VMware ESX

Follow the steps below to install the FortiSIEM Virtual Appliance on VMware ESX:

Step 1: Set Network Time Protocol (NTP) for ESX

1. Log in to your VMware ESX server.
2. Select your ESX host server.
3. Click the **Configuration** tab.
4. Under **Software**, select **Time Configuration**.
5. Click **Properties**.
6. Select **NTP Client Enabled**.
7. Click **Options**.
8. Under **General**, select **Start automatically**.
9. Under **NTP Setting**, click **Add...**.
10. Enter the IP address of the NTP servers to use.
    If you don't have an internal NTP server, you can access a publicly available one at http://tf.nist.gov/tf-cgi/servers.cgi
11. Click **Restart NTP service**.
12. Click **OK** to apply the changes.

Step 2: Import FortiSIEM Virtual Appliance into ESX

1. Go to the Fortinet Support website https://support.fortinet.com to download the ESX package. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Download and uncompress the packages for Super/Worker and Collector (using 7-Zip tool) to the location where you want to install the image.
3. Log in to the VMware vSphere Client.
4. In the **File** menu, select **Deploy OVF Template**.
5. **Browse** to the .ova file (example: FortiSIEM-VA-5.0.0.1201.ova) and select it.
   On the OVF Details page you will see the product and file size information.

6. Click **Next**.
7. Click **Accept** to accept the 'End User Licensing Agreement' and click **Next**.
8. Enter a **Name** for the Supervisor or Worker, and then click **Next**.
9. Select a **Storage** location for the installed file, and then click **Next**.
10. Select a **Disk Format**, and then click **Next**.
    Note that FortiSIEM recommends using *Thick Provision Lazy Zeroed*.
11. Review the **Deployment Settings**, and then click **Finish**.
12. Do not turn off or reboot the system during deployment, which may take 7 to 10 minutes to complete. When the deployment completes, click **Close**.

Running on VMware ESX 6.0: If you are importing FortiSIEM VA or Collector images for VMware on an ESXi 6.0 host, you must also 'Upgrade VM Compatibility' to ESXi 6.0. If the VM is already started, you must shutdown the VM, and use the **Actions** menu to do this. Sometimes, due to the incompatibility created by the VMware, the Collector VM processes restart and the Collector may not register with the Supervisor. Similar problems are also likely to occur on Supervisor or Worker, so make sure that the VM compatibilities are upgraded as well. More information about VM compatibility is available in the VMware KB below: https://kb.vmware.com/s/article/1010675

Step 3: Edit FortiSIEM Virtual Appliance Hardware Settings

The default network adapter is of type E1000 whose performance will max out at 1Gbps. If your ESX environment supports 10Gbps, it is better to use VMXNet3 network adapter. Before powering on the VM, replace E1000 by VMXnet3. Remove the existing network adapters, then add a new network adapter of type VMXnet3. More information about network adapters is available in the VMWare KB.

Before you start the Supervisor, Worker, or Collector for the first time, you must make a few changes to its hardware settings.

1. In the VMware vSphere client, select the imported Supervisor, Worker, or Collector.
2. Right-click on the node to open the **Virtual Appliance Options** menu, and then select **Edit** settings.
3. Select the **Hardware** tab, and check that CPU and Memory according to need. See Step A.

Step 4: Start and Configure the FortiSIEM Virtual Appliance from the VMware Console

Do not press any control keys (for example - **Ctrl**-C or **Ctrl**-Z) while configuring the virtual appliances, as this may cause the installation process to stop. If this happens, you must erase the virtual appliance and start the installation process again.

1. In the VMware vSphere client, select the Supervisor, Worker, or Collector virtual appliance.
2. Right-click to open the **Virtual Appliance Options** menu, and then select **Power** > **Power On**.
3. In the **Virtual Appliance Options** menu, select **Open Console**.
   Network Failure Message: When the console starts up for the first time you may see a "Network eth0 Failed message", but this is expected behavior.
4. In VM console, select **Set Timezone** and then press **Enter**.

5. Select your **Location**, and press **Enter**.
6. Select your **Country**, and press **Enter**.
7. Select your **Timezone**, and press **Enter**.
8. Review your **Timezone** information, select **1**, and press **Enter**.
9. When the **Configuration** screen reloads, select **Login**, and press **Enter**.
10. Enter the default login credentials – user: 'root' and Password: 'ProspectHills'.
11. Run the `vami_config_net` script to configure the network:
`/opt/vmware/share/vami/vami_config_net`
12. Based on your network type, enter one of the options below:
    - **1** for **IPv6 Network Only**
      - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
    - **2** for **IPv4 Network Only**
      - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
    - **3** for **Both Networks**
      i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
      ii. Follow Step 13 below to turn off the proxy server and continue with step c.
      iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).
13. Enter **n**. **Note**: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the ESX host.
14. Enter **y** to accept the network configuration settings.
15. Enter the **Host name**, and press **Enter**.
16. For Supervisor and Worker: You will be prompted to choose Supervisor [s] or Worker [w].
Choose accordingly:
    a. For Supervisor, the system will initialize the PostGreSQL database which will take around 20 minutes and then reboot the system. A few minutes after reboot, the system GUI will be ready to upload license and configure the Event Database Storage option. For a Worker node, the system will reboot quickly and a few minutes after reboot, it will be ready to be added as a Worker from the Supervisor GUI.
    b. For a Worker node, the system will reboot quickly and a few minutes after reboot, it will be ready to be added as a Worker from the Supervisor GUI.
17. For Collector, the system will reboot and after a few minutes it will be ready.

Step 5: Upload FortiSIEM License on Supervisor

You will now be asked to input a license.

1. Click **Browse** and upload the license file.
Make sure that the 'Hardware ID' shown in the **License Upload** page matches the license.
2. For **User ID** and **Password**, choose any 'Full Admin' credentials.
For the first time, install by choosing user as 'admin' and password as 'admin*1'
3. Choose **License type** as 'Enterprise' or 'Service Provider'.
This option is available only on first install. Once the database is configured, this option will not be available.

Step 6: Choose FortiSIEM Event Database Storage

For fresh installation, you will be taken to the Event Database Storage page. Based on Step-B, you will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options.

For more details about configuring storage, see here.

Step 7: (Optional) Install Workers and Add to Supervisor Node

Follow Steps 1 and 4 to configure a Worker.

Add the Worker node to the Supervisor by visiting **ADMIN** > **License** > **Nodes** > **Add**.

See **ADMIN** > **Health** > **Cloud Health** to ensure that the Workers are up, healthy and properly added to the system.

Step 8: (Optional) Install Collectors

Collectors can be installed as Virtual Appliances or Hardware appliances (FSM-500F).

For ESX based Virtual Appliances, set up the Collector by following Steps 1 to 4 above.

Step 9: (Optional) Register Collectors to Supervisor Node

For Enterprise deployments, follow these steps.

1. Login to Supervisor with 'Admin' privileges.
2. Go to **ADMIN** > **Setup** > **Collectors** and add a Collector by entering:
   a. **Name** – Collector Name
   b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set 'Unlimited'.
3. SSH to the Collector and run following script to register Collectors:
   `phProvisionCollector --add <user> <password> <Super IP or Host> <Organization> <CollectorName>`
   a. Set **User** and **Password** use the admin User Name and password for the Supervisor
   b. Set **IP Address** as 'Supervisor IP'.
   c. Set **Organization** as 'Super'.
   d. Set **Name** from Step 2a.
   The Collector will reboot during the Registration
4. Go to **ADMIN** > **Health** > **Collector Health** and see the status.

For Service Provider deployments, follow these steps.

1. Login to Supervisor with 'Admin' privileges.
2. Go to **ADMIN** > **Setup** > **Organizations** and add an Organization.
3. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
4. Under **Collectors**, click **New**.

5. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**. The last two values could be set as 'Unlimited'. Guaranteed EPS is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
6. SSH to the Collector and run following script to register Collectors:
   `phProvisionCollector --add <user> <password> <Super IP or Host> <Organization> <CollectorName>`
   a. Set **User** and **Password** use the admin User Name and password for the Supervisor
   b. Set **IP Address** as 'Supervisor IP'.
   c. Set **Organization** as 'Super'.
   d. Set **CollectorName** from Step 2a.
   The Collector will reboot during the Registration
7. Go to **ADMIN** > **Health** > **Collector Health** and check the status.

Installing FortiSIEM Report Server on VMware ESX

Follow the steps below to install FortiSIEM Report Server on VMware ESX:

Step 1: Set Network Time Protocol (NTP) for ESX

- Follow the instructions in Step 1.

Step 2: Import FortiSIEM Report Server into ESX

1. Go to the Fortinet Support website https://support.fortinet.com to download the ESX package. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Download and uncompress the packages for Report Server (using 7-Zip tool) to the location where you want to install the image.
3. Log in to the VMware vSphere Client.
4. In the **File** menu, select **Deploy OVF Template**.
5. **Browse** to the .ova file (example: FortiSIEM-ReportServer-5.0.0.1201.ova) and select it.
   On the OVF Details page you will see the product and file size information.
6. Click **Next**.
7. Click **Accept** to accept the 'End User Licensing Agreement' and click **Next**.
8. Enter a **Name** for the Report Server, and then click **Next**.
9. Select a **Storage** location for the installed file, and then click **Next**.
10. Select a **Disk Format**, and then click **Next**.
    Note that FortiSIEM recommends using *Thick Provision Lazy Zeroed*.
11. Review the **Deployment Settings**, and then click **Finish**.
12. Do not turn off or reboot the system during deployment, which may take 7 to 10 minutes to complete. When the deployment completes, click **Close**.

Running on VMware ESX 6.0: If you are importing FortiSIEM Report Server images for VMware on an ESXi 6.0 host, you must also 'Upgrade VM Compatibility' to ESXi 6.0. If the VM is already started, you must shutdown the VM, and use the **Actions** menu to do this. Sometimes, due to the incompatibility created by the VMware, the Collector VM processes restart and the Collector may not register with the Supervisor. Similar problems are also likely to occur on Report server, so make sure that the VM compatibilities are upgraded as well. More information about VM compatibility is available in the VMware KB below: https://kb.vmware.com/s/article/1010675.

Step 3: Edit FortiSIEM Virtual Appliance Hardware Settings

The default network adapter is of type E1000 whose performance will max out at 1Gbps. If your ESX environment supports 10Gbps, it is better to use VMXNet3 network adapter. Before powering on the VM, replace E1000 by VMXnet3. Remove the existing network adapters, then add a new network adapter of type VMXnet3. More information about network adapters is available in the VMWare KB.

Before you start the Report Server for the first time, you must make few changes to its hardware settings.

1. In the VMware vSphere client, select the imported Report Server.
2. Right-click on the node to open the **Virtual Appliance Options** menu, and then select **Edit** settings.
3. Select the **Hardware** tab and check that the memory is set to at least 16 GB and CPUs is set to 8.
4. Install the Report Server using either native ESX storage or NFS storage. These instructions are for creating native ESX storage. For NFS deployment, see the *FortiSIEM - NFS Storage Guide* here.
   a. On the **Hardware** tab, click **Add**.
   b. In the 'Add Hardware' dialog box, select **Hard Disk**, and then click **Next**.
   c. Select **Create a new virtual disk**, and then click **Next**.
   d. Check that these selections are made in the 'Create a Disk' dialog box: Disk Size 300GB
   e. In the 'Advanced Options' dialog box, make sure that the Independent option for Mode is not selected.
   f. Check all the options for creating the virtual disk, and then click **Finish**.
   g. In the 'Virtual Machine Properties' dialog box, click **OK**. The Reconfigure virtual machine task will launch.
5. For Local storage, add the data disk. Use the command `fdisk -l` to get the disk name.

Step 4: Start and Configure the Report Server from the VMware Console

Do not press any control keys (for example - **Ctrl**-C or **Ctrl**-Z) while configuring the virtual appliances, as this may cause the installation process to stop. If this happens, you must erase the virtual appliance and start the installation process again.

1. In the VMware vSphere client, select the Report Server virtual appliance.
2. Right-click to open the **Virtual Appliance Options** menu, and then select **Power** > **Power On**.
3. In the **Virtual Appliance Options** menu, select **Open Console**.
   Network Failure Message: When the console starts up for the first time you may see a "`Network eth0 Failed message`", but this is expected behavior.
4. In VM console, select **Set Timezone** and then press **Enter**.
5. Select your **Location**, and then press **Enter**.
6. Select your **Country**, and then press **Enter**.
7. Select your **Timezone**, and then press **Enter**.
8. Review your **Timezone** information, select **1**, and then press **Enter**.
9. When the **Configuration** screen reloads, select **Login**, and then press **Enter**.
10. Enter the default login credentials – user: 'root' and Password: 'ProspectHills'.
11. Based on your network type, enter one of the options below:
    - **1** for **IPv6 Network Only**
      - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
    - **2** for **IPv4 Network Only**
      - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
    - **3** for **Both Networks**
      i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
      ii. Follow Step 12 below to turn off the proxy server and continue with step c.

iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).

12. Enter **n**. **Note**: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the ESX host.
13. Enter the **Host name**, and then press **Enter**.
14. Enter the mount point for your data. Set one of the following:
    - 'Local' (`/dev/<disk_name>`)
      Use the `disk_name` from Step 3 - #5.
    - 'NFS' storage mount point
      Note: Do not use the same mount point as EventDB on Supervisor. This should be a different mount point/storage path.

    After you set the mount point, the Report Server will automatically reboot, and in 10 to 15 minutes the Report Server will be successfully configured.

Step 5: Register FortiSIEM Report Server to Supervisor

1. Log in to your Supervisor node.
2. Open the 'License Management' page on:
   - Flash GUI: Go to **Admin** > **License Management**. Under 'Report Server Information', click **Add**.
   - HTML5 GUI: Go to **ADMIN** > **License** > **Nodes** tab. Click **Add** and select '**Report Server**' from the **Type** drop-down.
3. Enter the **Report Server IP Address**, **Database Username** and **Database Password** of the Report Server you want to use to administer.
   You will use the same credentials to set up the Visual Analytics Server for reading data from the Report Server.
4. Click **Run in Background** if you want Report Server registration to run in the background for larger installations. When CMDB size is below 1 GB, registration takes approximately three minutes to complete.
5. When the registration is complete, click **OK** in the confirmation dialog.
6. Make sure the Report Server is up and running by navigating to:
   - Flash GUI: **Admin** > **Cloud Health**
   - HTML5 GUI: **ADMIN** > **Health** > **Cloud Health**

Step 6: Sync Reports from FortiSIEM Supervisor to the Report Server

1. Log in to your Supervisor node.
2. Select **Synced Reports** from:
   - Flash GUI: **RESOURCE > Reports** > **Synced Reports**
   - HTML5 GUI: **RESOURCES** > **Reports** > **Synced Reports**
3. Select a Report.
   Currently, only reports that contain a 'Group By' condition can be synced. Both system and user-created reports can be synched as long as it contain a 'Group By' condition.
4. Select **Sync**.
   When the sync process initiates, the Supervisor node dynamically creates a table within the Report Server reportdb database. When the sync is established, it will run every five minutes, and the last five minutes of data in the synced report will be pushed to the corresponding table. This lets you run Visual Analytics on event data stored in the Report Server reportdb database.