

# Deployment Guide

**FortiSOAR 7.2.2**



**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](mailto:techdoc@fortinet.com)



August, 2022

FortiSOAR 7.2.2 Deployment Guide

00-400-000000-20210113

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>Introduction</b>	<b>7</b>
Purpose	7
Prerequisites	7
Browser Compatibility	7
<b>Deploying FortiSOAR</b>	<b>8</b>
Planning	9
Recommended Resource Requirements	9
Credentials	10
Requirements	11
Port Requirements	11
Importing the FortiSOAR Virtual Appliance	12
Downloading the FortiSOAR Virtual Appliance from the Support Portal	12
Deploying the FortiSOAR Virtual Appliance	14
Deploying the FortiSOAR Virtual Appliance using vSphere or vCenter	14
Deploying the FortiSOAR Virtual Appliance using AWS	15
Deploying FortiSOAR using KVM	15
Installing FortiSOAR 7.2.2 using the FortiSOAR installer	20
Prerequisites	20
Procedure	21
Installing the secure message exchange	22
Installing FortiSOAR on RHEL using the FortiSOAR installer	23
FortiSOAR Configuration Wizard	23
Interactive VM configuration	23
Non-interactive VM configuration	25
Pointing the ntpd service to a valid ntp server	26
Editing the VM configuration	26
Setting a static IP	27
Determining your DHCP IP address	29
Deploying FSR Agents	30
Architecture	31
Recommended Resource Requirements for Virtual Machines (VM)	31
Prerequisites for installing a FSR agent	31
Process of setting up a FSR agent	32
Adding a FSR agent	35
Installing a FSR agent	38
Deboarding FSR Agents	38
Moving a FSR agent to a new secure message exchange	39
Adding multiple disks and partitioning disks in your FortiSOAR VM	39
Recovering data	40
<b>Deploying FortiSOAR using offline repositories</b>	<b>43</b>
Prerequisites	43
Setting up the Offline Repository	43

Deploying FortiSOAR using the Offline Repository .....	44
Upgrading FortiSOAR using the Offline Repository .....	45
Troubleshooting .....	45
Peer Certificate issue not recognized error .....	45
<b>Licensing FortiSOAR .....</b>	<b>46</b>
FortiSOAR licensing process .....	47
FortiSOAR licensing using FortiManager .....	48
Process to deploy the FortiSOAR license when you are in a complete air-gapped environment .....	48
Process to deploy the FortiSOAR license when you are not in a complete air-gapped environment .....	50
Retrieving the FortiSOAR Device UUID .....	51
Deploying the FortiSOAR license .....	51
Deploying the FortiSOAR license using the FortiSOAR UI .....	51
Deploying the FortiSOAR license using the FortiSOAR Admin CLI .....	55
Activating the FortiCare Trial license for FortiSOAR .....	55
License Manager Page .....	56
User Seat Support in FortiSOAR .....	59
Updating your license using the FortiSOAR UI .....	60
Troubleshooting licensing issues .....	60
Troubleshooting issues while deploying the FortiSOAR license in a proxy environment .....	61
<b>Configuring FortiSOAR .....</b>	<b>62</b>
Logging on to FortiSOAR for the first time .....	62
Configuring SMTP for FortiSOAR .....	64
Creating your first user and record .....	64
<b>Additional configuration settings for FortiSOAR .....</b>	<b>65</b>
Changing the hostname .....	65
Regenerating self-signed certificates .....	66
Updating the SSL certificates .....	66
Adding self-signed CA certificates in CentOS as trusted certificates .....	67
Exporting the CA certificate using a browser .....	67
Adding the self-signed CA cert in the OS .....	81
Verifying that the self-signed CA certificates are added as trusted certificates in CentOS .....	82
Setting up monitoring for your FortiSOAR system .....	82
Setting up system monitoring .....	82
Setting up purging for audit and playbook logs .....	82
Configuring High Availability or Disaster Recovery options .....	83
Starting and stopping FortiSOAR Services .....	83
Changing the FortiSOAR default database passwords .....	83
Setting up a proxy server to service all requests from FortiSOAR .....	84
Configuring Proxy Settings and environment variables .....	85
Backing up the data encryption keys .....	85
Configuring a reverse proxy (Apache proxy server) .....	86

---

<b>Troubleshooting FortiSOAR Issues</b>	<b>87</b>
Troubleshooting issues occurring in FortiSOAR due to insufficient space	87
Increasing the disk space for record storage in case of AWS AMI deployment	91
Troubleshooting Deployment Issues	91
The FortiSOAR Virtual Appliance deployment on ESX is failing	91
Cannot access the FortiSOAR portal	91
Cannot login to the FortiSOAR platform	91
Getting a 502 error when you click on the Reports tab	91
Troubleshooting Upgrade Issues	92
Post license renewal you cannot log into FortiSOAR	92
Failure to upgrade FortiSOAR	92
Post-upgrade your playbooks fail to execute, and the playbooks are also not listed in the executed playbooks log	93
Login and logout events are not audited after you have upgraded your FortiSOAR version	93
Issues occurring when you have restored data on a FortiSOAR 6.0+ system with data backed up from a system prior to 6.0.0	94

## Change Log

Date	Change Description
2022-09-08	Updated commands in the 'Recovering Data' topic in the <a href="#">Deploying FortiSOAR</a> chapter.
2022-08-10	Initial release of 7.2.2

# Introduction

Fortinet Security Orchestration Platform™ (FortiSOAR™) is a scalable, awareness-driven, and encrypted security management intelligence platform. FortiSOAR is a centralized hub for your security operations and dramatically improves the effectiveness and efficiency of your security operations teams, by providing automation and customizable mechanisms for prevention, detection, and response to cybersecurity threats.

## Purpose

Use the deployment guide to deploy the FortiSOAR virtual appliance using VMware, the ESX/ESXi server and AWS.



This document provides you with all the procedures for setting up FortiSOAR in your environment, including deploying FortiSOAR, the initial configuration for FortiSOAR, and troubleshooting of FortiSOAR.

---

## Prerequisites

Before you deploy FortiSOAR, ensure you have the done the following:

- Provision to import FortiSOAR virtual appliance into VMware or AWS. You can also install FortiSOAR on your existing VM.
- Hostname and IP address if you want to change or assign them.
- DNS server should be configured for the appliance if it is not picked up automatically from the network.
- Company-specific SSL certificate, if you want to change the default certificate.
- Optionally configure an SMTP server and an NTP server. The SMTP server is used for outgoing notifications once the system is configured. The NTP server is used to synchronize the machine time after deployment.

## Browser Compatibility

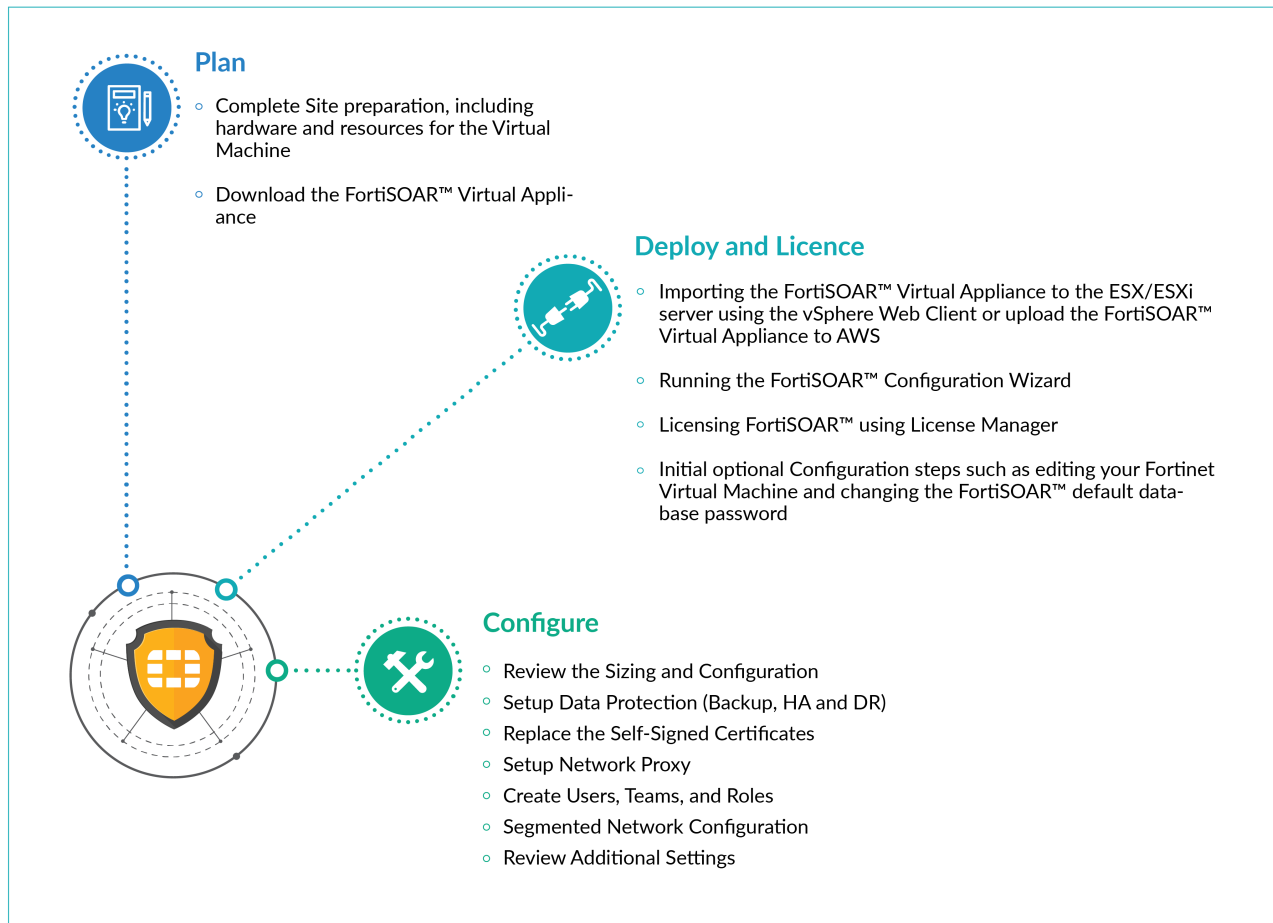
FortiSOAR 7.2.2 User Interface has been tested on the following browsers:

- Google Chrome version 103.0.5060.134
- Mozilla Firefox version 103.0.1 (64-bit)
- Microsoft Edge version 103.0.1264.77 (Official build) (64-bit)
- Safari version 15.5 (17613.2.7.1.8)

# Deploying FortiSOAR

This chapter covers the process of deploying FortiSOAR, and the initial configuration required for FortiSOAR. You can perform the initial configuration for FortiSOAR using the FortiSOAR Configuration Wizard.

The following image displays the high-level tasks for deploying FortiSOAR:



You can also install FortiSOAR 7.2.2 using the FortiSOAR installer (.bin file). For more information, see [Installing FortiSOAR 7.2.2 using the FortiSOAR installer](#).

You can also deploy FortiSOAR using the offline repositories. For more information, see the [Deploying FortiSOAR using offline repositories](#) chapter.

## Planning

### Recommended Resource Requirements

---



The maximum hard drive or physical volume size for FortiSOAR must be limited to 2 TB.

---

### Virtual Machine (VM)

#### Minimum Specifications

- 8 available vCPUs
- 20 GB available RAM
- 500 GB available disk space: Recommended to have high-performance storage, preferably SSDs.
- 1 vNIC

#### Recommended Specifications

- 8 available vCPUs
  - 32 GB available RAM
  - 1 TB available disk space: Recommended to have high-performance storage, preferably SSDs.
  - 1 vNIC
- 



In case of multi-tenant configurations, contact FortiSOAR Support for sizing requirements.

---

The disk space that you require largely depends on your usage and audit and workflow retention policies. So, for a more precise prediction of the database usage, you can check the current disk sizes using the following command:

```
csadm db --getsize
```

The `csadm db --getsize` command returns the sizes of the workflow logs, audit, and primary data. Based on the current usage, and your retention policies, you can extrapolate the usage for these databases. ElasticSearch disk usage would be the same as the primary database sizes. For some examples, see the 'Sizing Guide' available on <https://docs.fortinet.com/product/fortisoar>.

### Supported Hypervisors

- AWS Cloud
- Fortinet-FortiCloud
- VMware ESXi versions 5.5, 6.0, and 6.5
- Redhat KVM



For any other virtualization or cloud hosting environment, you can install CentOS 7.x and then install FortiSOAR using CLI. For more information, see the [Installing FortiSOAR 7.2.2 using the FortiSOAR installer](#) topic.

---

## VM Inbound Networking

Enable the following ports for the VM within your VM network:

- 22 Management (ssh)
- 443 User Interface (https)

## VM Outbound Networking

For FortiSOAR to correctly interact with your network, you must provide access between the FortiSOAR VM and the third-party products and services configured within your network.

To accomplish this, enable the following ports for SSH, SMTP, and HTTPs access:

- 22 Management (ssh)
- 25 Email SMTP relay server. This port can be different based on your environment.
- 443 User Interface (https)



Depending on the type of connectors used in Playbooks, you might require to open other ports or services.

---

## Credentials

Credentials to access SSH management and the FortiSOAR User Interface are:

Username: csadmin

Password: changeme

From FortiSOAR 6.0.0 onwards, the UI password of the 'csadmin' user for AWS is set to the "instance\_id" of your instance.

To know the instance ID of your FortiSOAR AWS instance, you can SSH and run the `cloud-init query instance_id` command.



From version 7.0.2 onwards, first FortiSOAR SSH login, password change is mandated for the 'csadmin' users, thereby enhancing the security of your csadmin account and preventing unauthorized parties from accessing the FortiSOAR administration account.

---

## Requirements

It is highly recommended that Internet access is provided for a FortiSOAR upgrade, license deployment, and also for installing new out-of-the-box connectors.

Add the following URLs in the allowlist of your Firewall or Proxy servers:

For upgrading FortiSOAR, installing connectors, and accessing the widget library:

<https://repo.fortisoar.fortinet.com/>

**Note:** In release 7.2.0 [update.cybersponse.com](https://update.cybersponse.com) has been renamed to <https://repo.fortisoar.fortinet.com/>.

Both these repositories will be available for a while to allow users who are on a release prior to FortiSOAR release 7.2.0 to access connectors and widgets. However, in time, only <https://repo.fortisoar.fortinet.com/> will be available.

For Connector Dependencies: <https://pypi.python.org>

For synchronization of FortiSOAR license details: <https://globalupdate.fortinet.net>

## Port Requirements

The following ports require to be locally open for various services, i.e., all these ports do not require to be open on the firewall for external access, they are used only inter-service communication within the appliance:

Service	Port Number
elasticsearch (Elasticsearch service uses this port for REST communication). Port needs to be opened in case of high availability (HA) environments.	9200
elasticsearch (Elasticsearch service uses this port for communication between nodes)	9300
rabbitmqserver	5672
cyops routing agent through nginx postman	7575
cyops workflow (celery) through nginx /sealab	8888
postgresql Port needs to be opened in case of HA environments.	5432
cyops auth server through nginx	8443
cyops integration (uwsgi) through nginx	9595
cyops-tomcat (hosts cyops-gateway, cyops-notifier)	8080
MQ TCP traffic Port needs to be opened in case of HA environments.	5671
cyops-api (crud-hub) [php-fpm is used to host]	443
rabbitmq service	25672, 4389

If you need to access ssh or start a terminal session from outside your network to troubleshoot or manage services or databases, then port "22/tcp open ssh" should be opened on the firewall for external access. Port 443/tcp open https must always be opened on the firewall for external access.

## Importing the FortiSOAR Virtual Appliance

Use a vSphere Client or a viciant to import the Virtual Appliance into the ESX/ESXi server. See the VMware documentation for steps on how to import a Virtual Appliance.



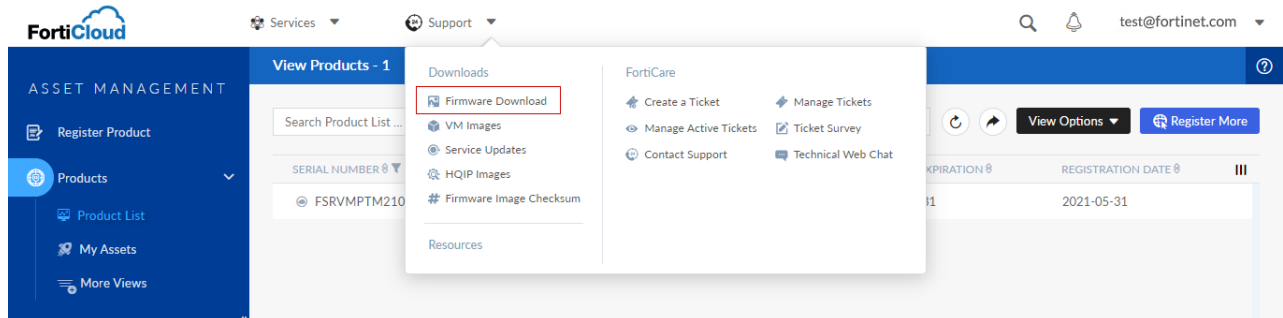
After you import the FortiSOAR Virtual Appliance and the FortiSOAR system boots up, the IP address of the system is displayed on the command prompt. You can share this IP address with users who require to configure FortiSOAR using the FortiSOAR Configuration Wizard.

## Downloading the FortiSOAR Virtual Appliance from the Support Portal

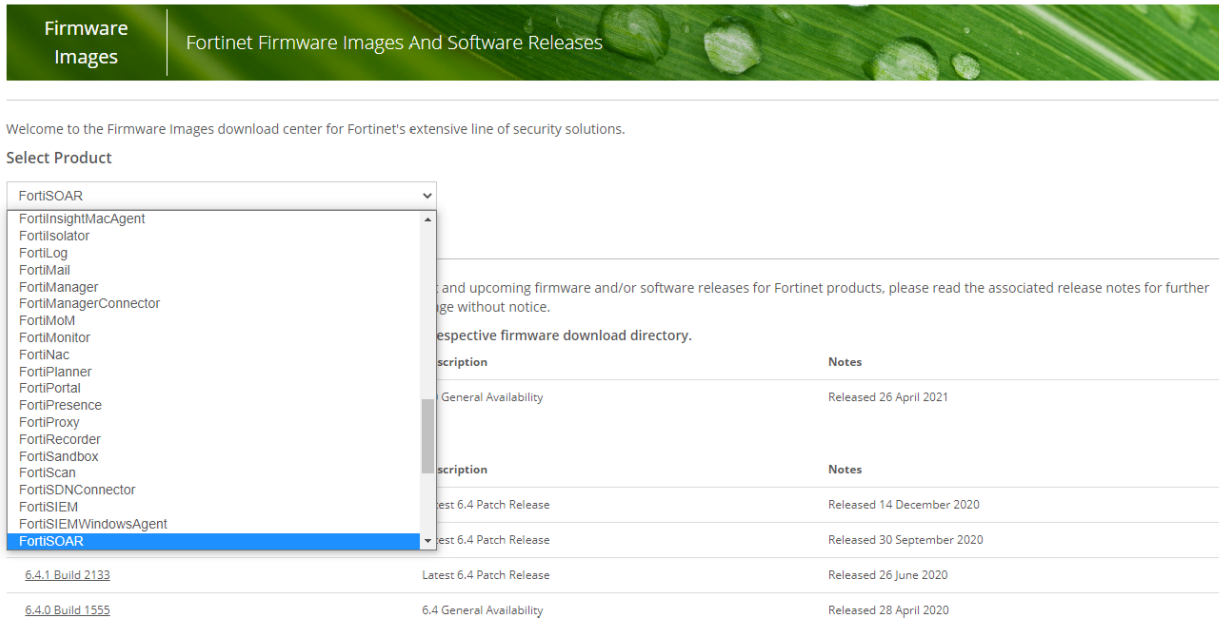
You can download the required FortiSOAR Virtual Appliance image from the support portal, which contains images for AWS, KVM-Supported QCOW2 and VMware. You will need these images to be downloaded before you can begin deploying FortiSOAR using vSphere or vCenter, or KVM. In case of AWS, you can directly launch an instance using the images present on the AWS Marketplace images.

To download the FortiSOAR Virtual Appliance do the following:

1. Log onto [support.fortinet.com](https://support.fortinet.com).
2. Click **Support > Firmware Download**.



3. On the Fortinet Firmware Images And Software Releases page from the **Select Product** drop-down list select **FortiSOAR**.



Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiSOAR

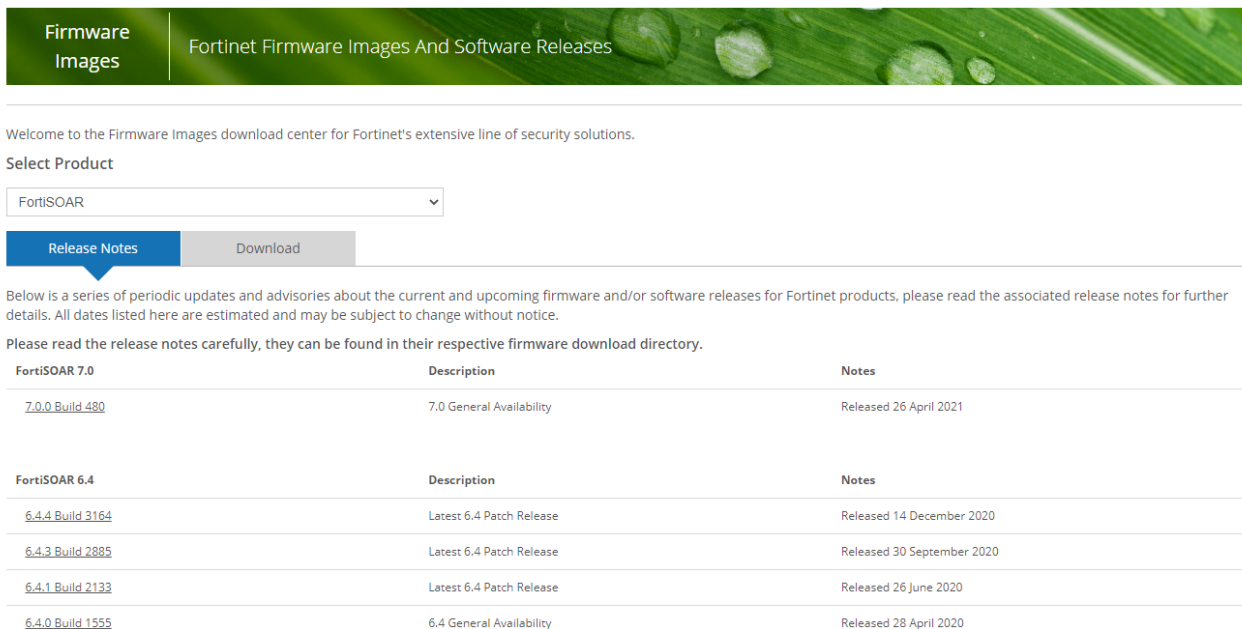
FortiInsightMacAgent  
FortiIsolator  
FortiLog  
FortiMail  
FortiManager  
FortiManagerConnector  
FortiMoM  
FortiMonitor  
FortiNac  
FortiPlanner  
FortiPortal  
FortiPresence  
FortiProxy  
FortiRecorder  
FortiSandbox  
FortiScan  
FortiSDNConnector  
FortiSIEM  
FortiSIEMWindowsAgent  
FortiSOAR

and upcoming firmware and/or software releases for Fortinet products, please read the associated release notes for further details. All dates listed here are estimated and may be subject to change without notice.

Please read the release notes carefully, they can be found in their respective firmware download directory.

Description	Notes
General Availability	Released 26 April 2021
Latest 6.4 Patch Release	Released 14 December 2020
Latest 6.4 Patch Release	Released 30 September 2020
Latest 6.4 Patch Release	Released 26 June 2020
6.4 General Availability	Released 28 April 2020

The page displays various released versions of FortiSOAR , and contains two tabs: **Release Notes** and **Downloads**.



Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiSOAR

Release Notes Download

Below is a series of periodic updates and advisories about the current and upcoming firmware and/or software releases for Fortinet products, please read the associated release notes for further details. All dates listed here are estimated and may be subject to change without notice.

Please read the release notes carefully, they can be found in their respective firmware download directory.

FortiSOAR 7.0	Description	Notes
<a href="#">7.0.0 Build 480</a>	7.0 General Availability	Released 26 April 2021

FortiSOAR 6.4	Description	Notes
<a href="#">6.4.4 Build 3164</a>	Latest 6.4 Patch Release	Released 14 December 2020
<a href="#">6.4.3 Build 2885</a>	Latest 6.4 Patch Release	Released 30 September 2020
<a href="#">6.4.1 Build 2133</a>	Latest 6.4 Patch Release	Released 26 June 2020
<a href="#">6.4.0 Build 1555</a>	6.4 General Availability	Released 28 April 2020

To download the Release Notes for a particular version, click the version and build number link, which opens the FortiSOAR Document Library, from where you can download the release notes for that particular version.

4. To download a firmware image do the following:
  - a. Click the **Download** tab
  - b. Navigate through the directory structure to open the page containing the required images. For example, to download a firmware image for version 7.0.0, click **v7.0.0 > 7.0 > 7.0.0** and locate the firmware image you

require.

Firmware Images

Fortinet Firmware Images And Software Releases

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiSOAR

Release Notes

Download

Image File Path

/ FortiSOAR/ v7.00/ 7.0/ 7.0.0/

Image Folders/Files

[Up to higher level directory](#)

Name	Size (KB)	Date Created	Date Modified	
checksum-7.0.0-480.txt	2	2021-04-26 18:04:44	2021-04-26 18:04:44	<a href="#">HTTPS Checksum</a>
fortisoar-aws-enterprise-7.0.0-480.ova	3,912,416	2021-04-26 17:04:47	2021-04-26 17:04:39	<a href="#">HTTPS Checksum</a>
fortisoar-aws-secure-message-exchange-7.0.0-480.ova	1,463,097	2021-04-26 17:04:40	2021-04-26 18:04:08	<a href="#">HTTPS Checksum</a>
fortisoar-kvm-enterprise-7.0.0-480.qcow2	4,295,880	2021-04-26 18:04:57	2021-04-26 18:04:43	<a href="#">HTTPS Checksum</a>
fortisoar-kvm-secure-message-exchange-7.0.0-480.qcow2	1,427,385	2021-04-26 17:04:41	2021-04-26 17:04:46	<a href="#">HTTPS Checksum</a>

- Download the firmware image by clicking the **HTTPS** link.  
An HTTPS connection is used to download the firmware image.
- Click the **Checksum** link for the image that you downloaded.  
The image file name and checksum code are displayed in the `Get Checksum Code` dialog box.
- Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.

## Deploying the FortiSOAR Virtual Appliance

Download the required FortiSOAR Virtual Appliance image from the Support Portal, which contains images for AWS, KVM-Supported QCOW2 and VMware. You will need these images to be downloaded before you can begin deploying FortiSOAR using vSphere or vCenter, or KVM. In case of AWS, you can directly launch an instance using the images present on the AWS Marketplace images. For information on how to download images from the support portal, see the [Downloading the FortiSOAR Virtual Appliance from the Support Portal](#) section. Also, ensure that your VM is configured as per the specifications outlined in the [Planning](#) section.

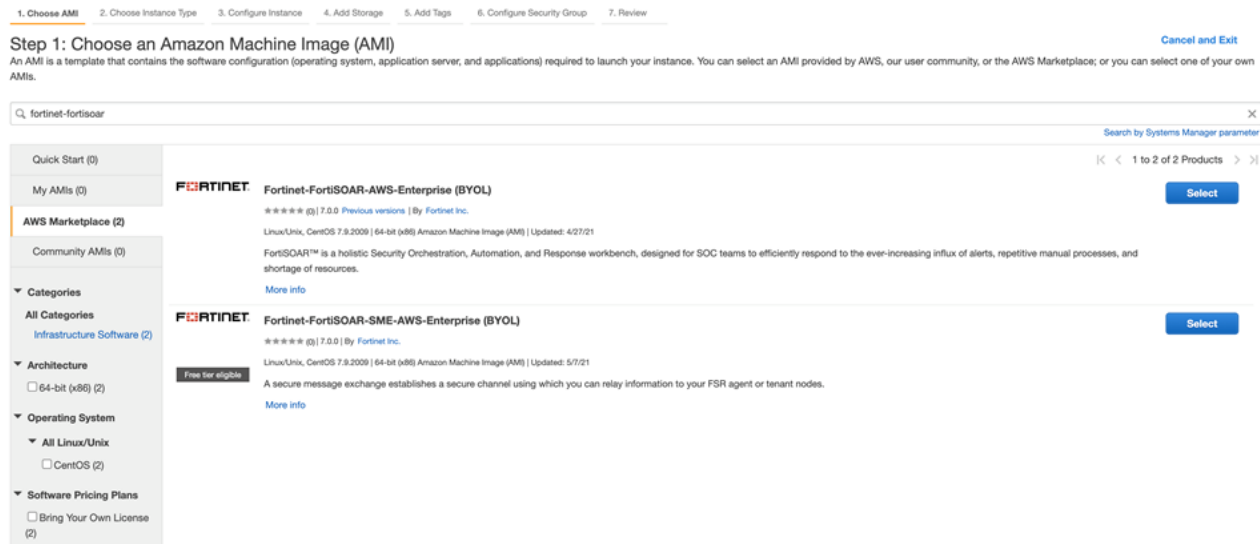
### Deploying the FortiSOAR Virtual Appliance using vSphere or vCenter

Download the VMware enterprise and secure message exchange images as outlined in the [Downloading the FortiSOAR Virtual Appliance from the Support Portal](#) section. Then once you have ensured that you have met all the specifications, deploy the FortiSOAR Virtual Appliance using vSphere or vCenter. See the VMware documentation for steps on how to deploy a Virtual Appliance.

## Deploying the FortiSOAR Virtual Appliance using AWS

Once you have ensured that you have met all the specifications, perform the following steps to deploy the FortiSOAR Virtual Appliance on Amazon Web Services (AWS):

1. Log into your AWS account and from the Amazon EC2 console dashboard, choose **Launch Instance**, to launch the FortiSOAR instance.
2. On the **Choose an Amazon Machine Image (AMI)** page, enter `fortinet-fortisoar` in the search bar to find the latest version of the FortiSOAR Enterprise and SME (secure message exchange) AMIs in the AWS Marketplace. Choose the AMI and start configuring the instance. Following is a reference screenshot:



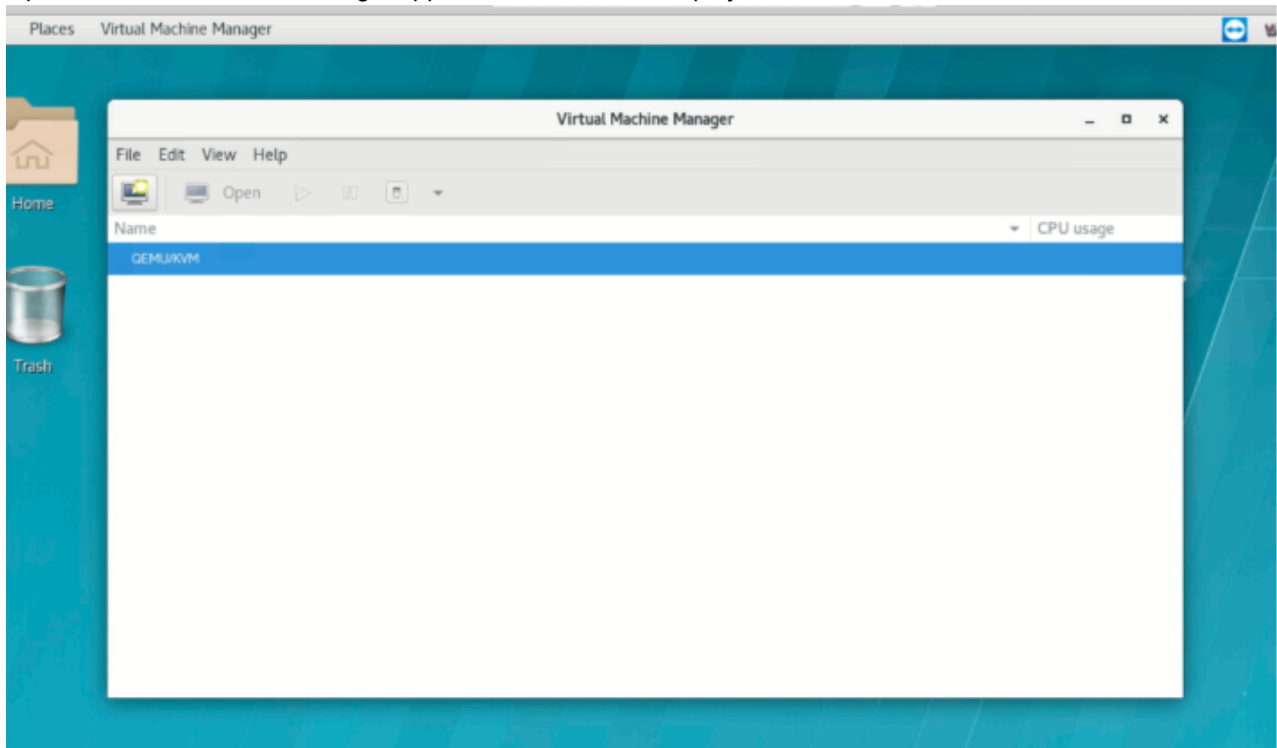
After you complete deploying your FortiSOAR and you connect the first time to your FortiSOAR VM, the EULA agreement page is displayed. You must accept the EULA to continue with your FortiSOAR configuration. If you do not accept the EULA, then the OS will halt, and you have to restart your FortiSOAR VM (power off-power on) and reconnect to the FortiSOAR VM and accept EULA to continue with your FortiSOAR configuration.

## Deploying FortiSOAR using KVM

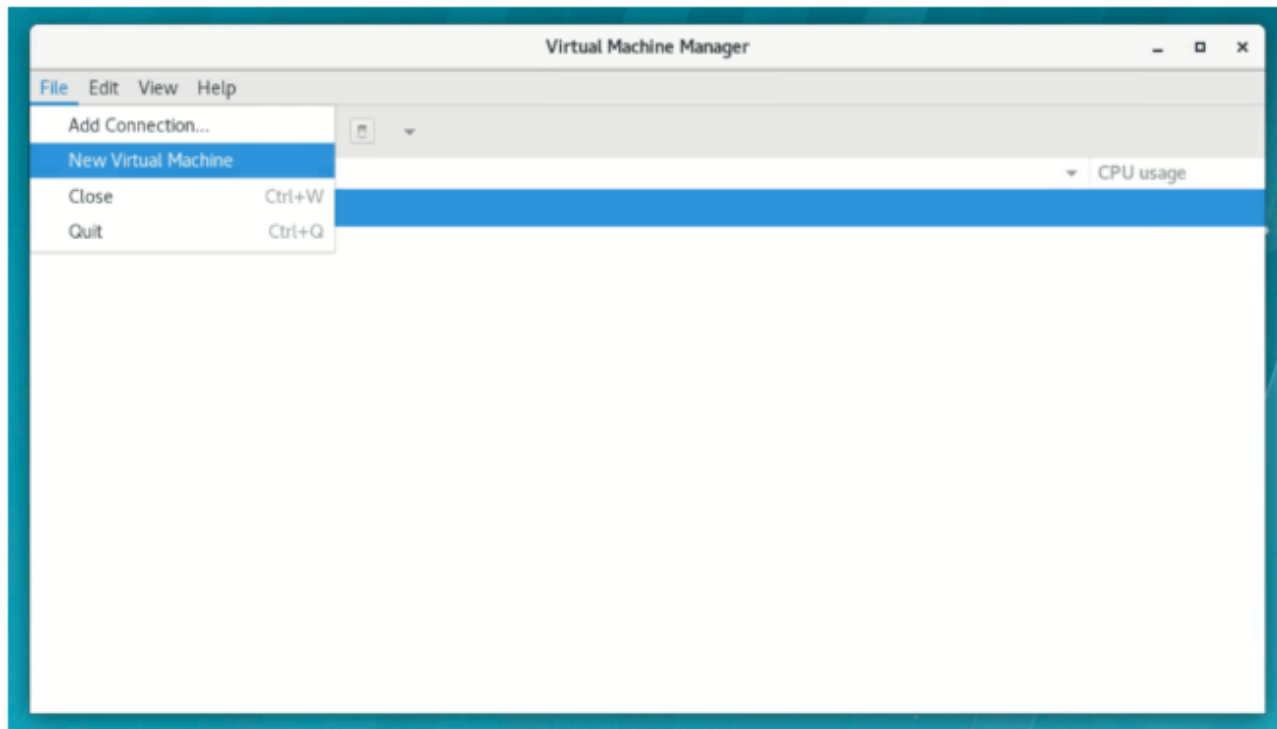
Once you have ensured that you have met all the specifications, perform the following steps to deploy the FortiSOAR QCOW2 on KVM:

1. Download the KVM-Supported QCOW2 images as outlined in the [Downloading the FortiSOAR Virtual Appliance from the Support Portal](#) section.
2. Copy the FortiSOAR QCOW2 image to the VM Image Datastore.

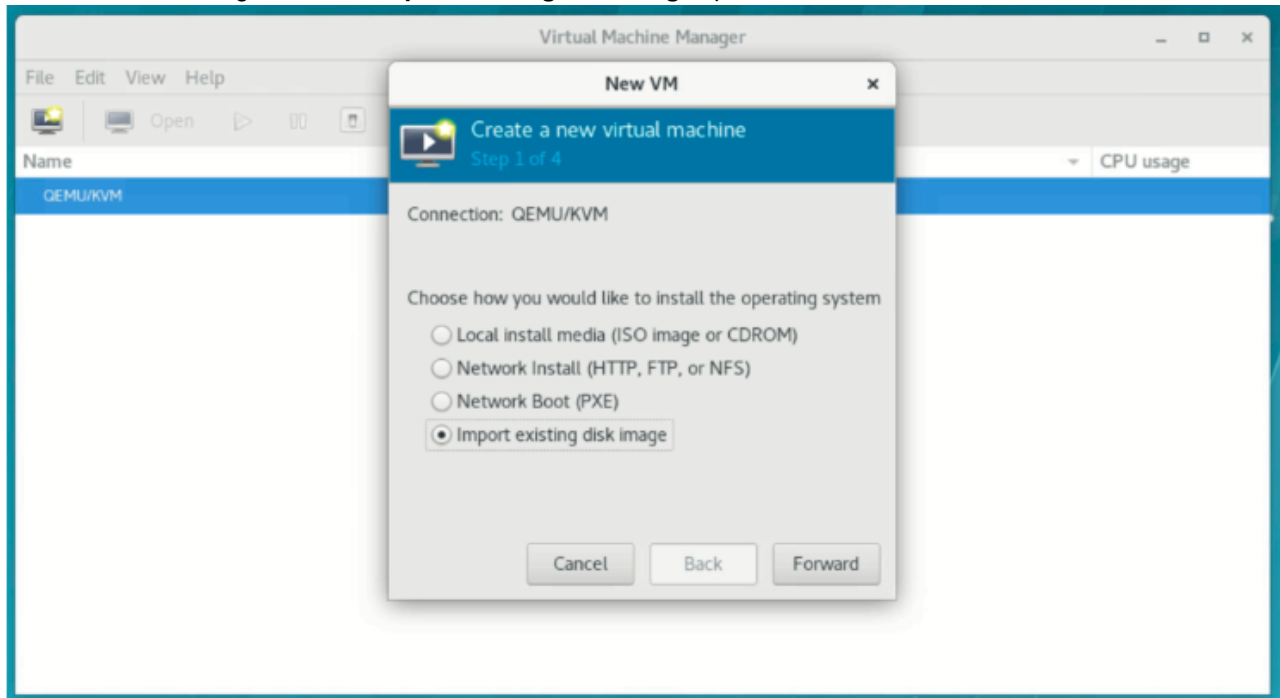
3. Open the Virtual Machine Manager application for KVM VM deployment.



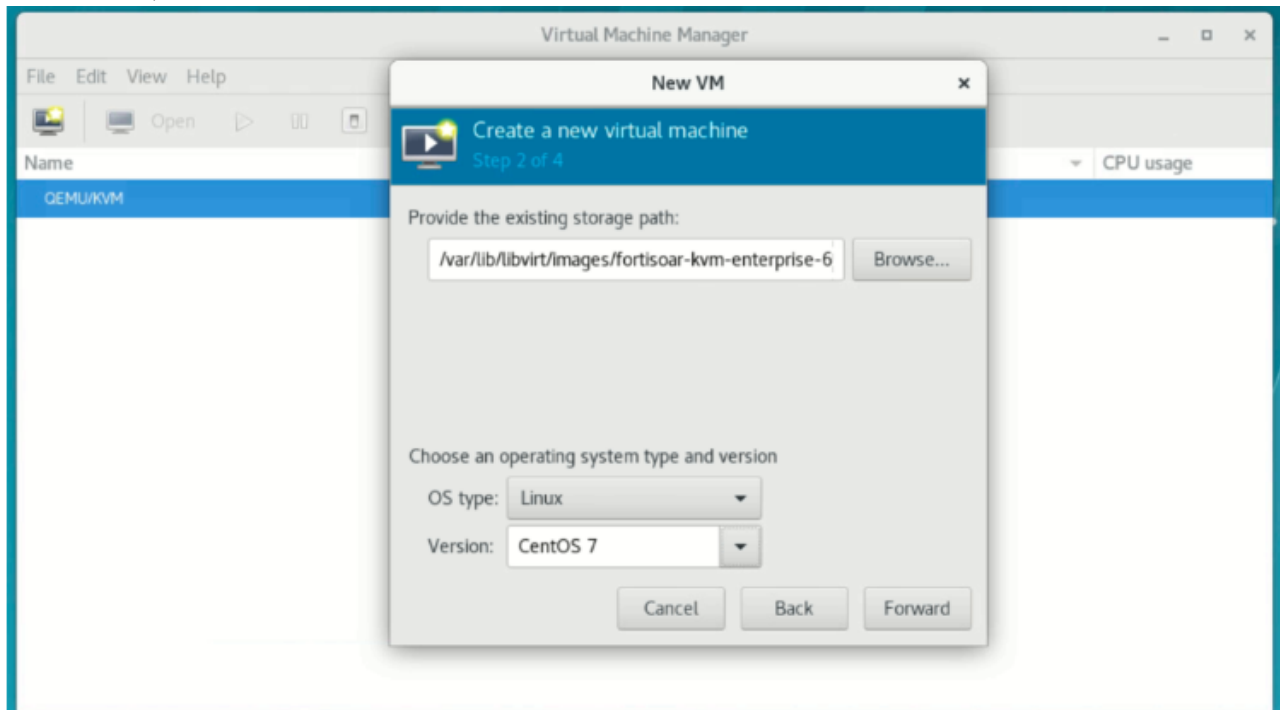
4. Click **File > New Virtual Machine**.



5. On the **New VM** dialog, select the **Import existing disk image** option and click **Forward**.

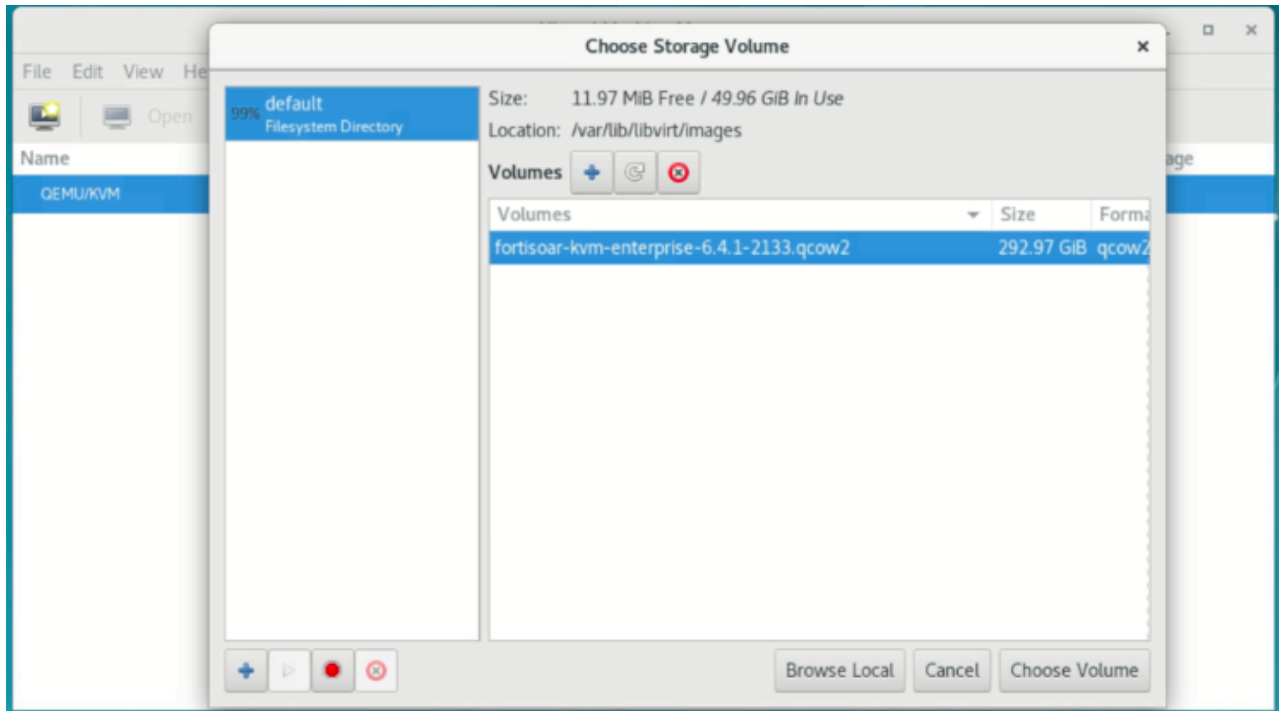


6. Click **Browse** and select the FortiSOAR image from the Image Datastore, select the **OS type** as **Linux** and **Version** as **CentOS 7**, and click **Forward**.

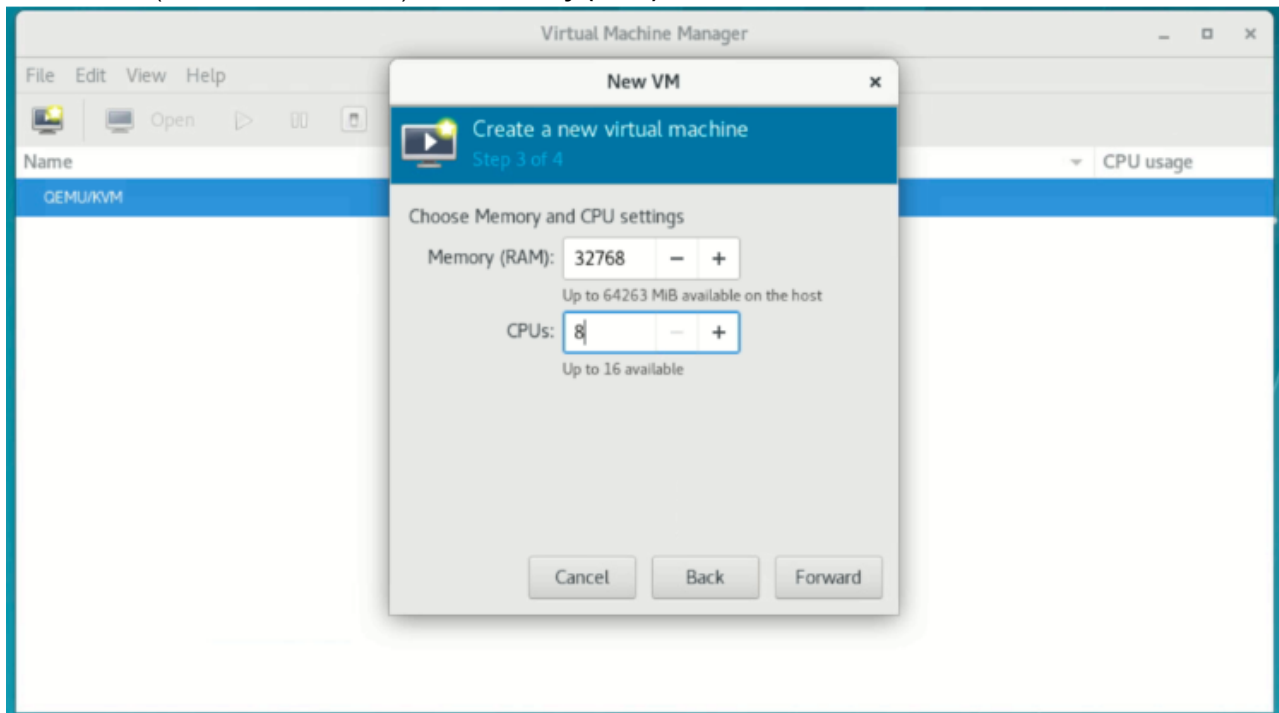


This displays the **Storage Volume** screen, where you can choose the storage volume, or click **Cancel** to keep as

default:



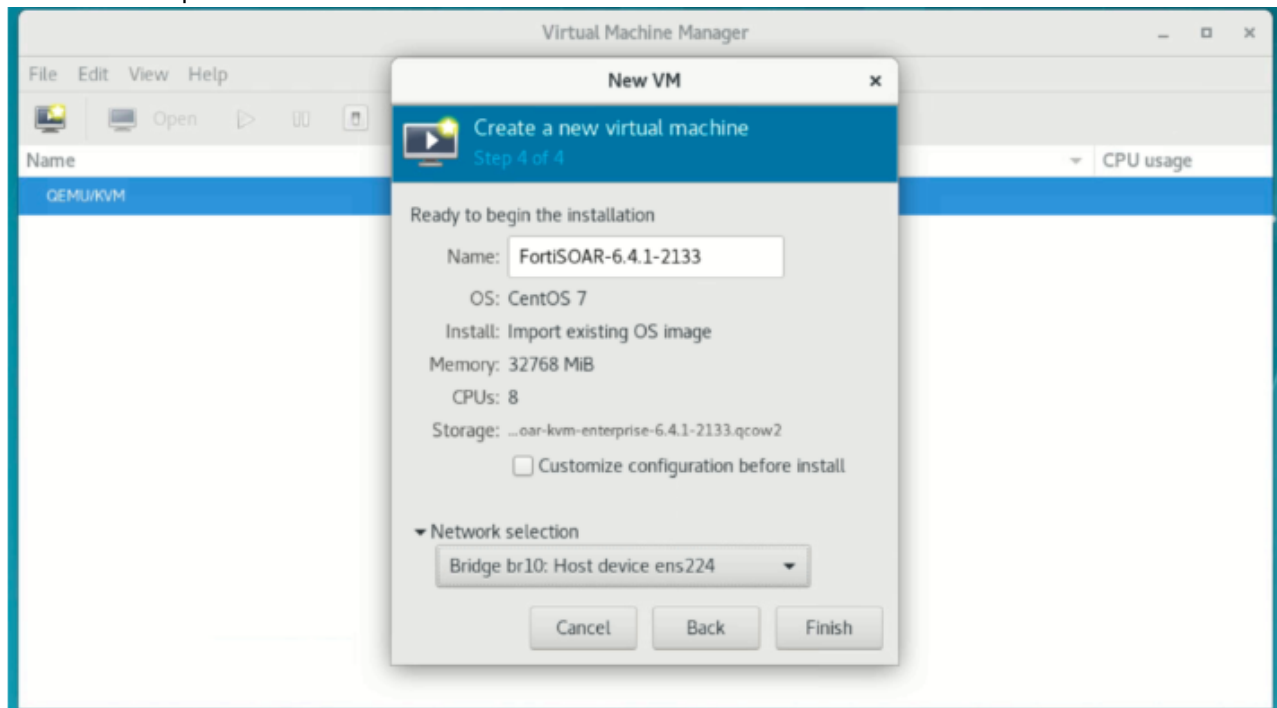
7. Enter 32768 (i.e. 32768 MB=32 GB) in the **Memory (RAM)** field and 8 in the **CPUs** field and click **Forward**.



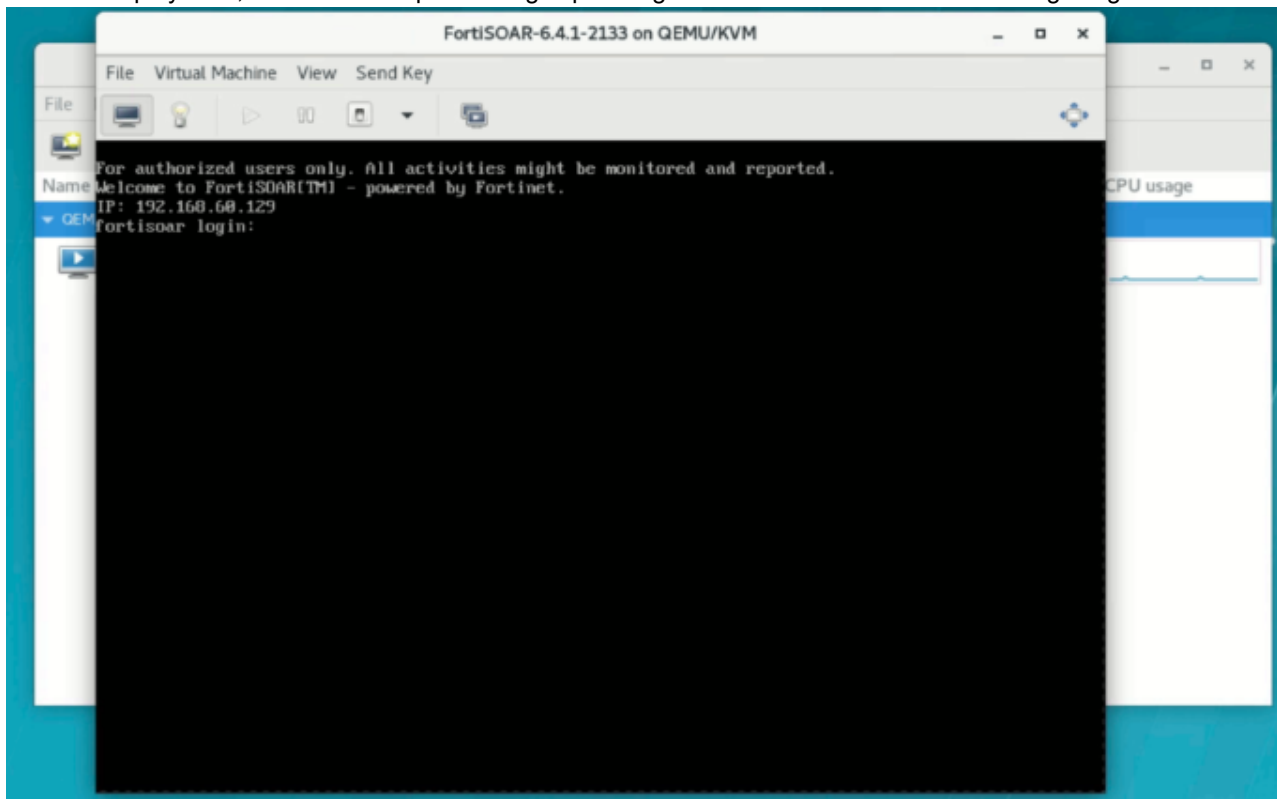
8. Enter the name that you want to specify for the new virtual machine in the **Name** field, select the correct network adapter for this new virtual machine from the **Network Selection** field, and click **Finish** to complete the deployment.

**Note:** The network adapter type would change depending upon your KVM environment. As an example, in the following image the "Bridge adapter.." is selected. You must select the proper network adapter as per your

environment requirements.



9. Post VM deployment, the VM boots up and brings up the login console as shown in the following image:



## CLI Deployment

If you want to deploy the FortiSOAR QCOW2 image (of version 6.4.1 for example) on KVM using the CLI, then use the following command:

```
virt-install --memory 32768 --vcpus 8 --import --os-type=linux --os-variant centos7.0 -
-name <virtual machine name> --disk </path/to/qcow2/image/.qcow2> --network <network
type=kvm network name>
```

Following is an example using the above CLI command:

```
virt-install --memory 32768 --vcpus 8 --import --os-type=linux --os-variant centos7.0 -
-name FortiSOAR-Enterprise-6.4.1 --disk /var/lib/libvirt/fortisoar/fortisoar-kvm-
enterprise-6.4.1-2133.qcow2 --network bridge=virbr0
```

Post deployment, perform the initial configuration steps using the [FortiSOAR Configuration Wizard](#).

## Installing FortiSOAR 7.2.2 using the FortiSOAR installer

This section describes the steps that you require to follow to install FortiSOAR 7.2.2 on a plain CentOS system that has minimal skew selected while installing CentOS.

### Prerequisites

Before you begin this procedure, ensure that you can access [repo.fortisoar.fortinet.com](https://repo.fortisoar.fortinet.com). In case you have configured proxies, then ensure that you have added your proxy settings in the following files:

- /etc/environment
- /etc/yum.conf
- /etc/pip.conf

Following is an example of adding proxy settings to the above-mentioned files:

- **/etc/environment**  

```
product_yum_server=repo.fortisoar.fortinet.com
http_proxy='http://username:password@10.1.1.0:8080'
no_proxy='127.0.0.1','localhost'
https_proxy='http://username:password@10.1.1.0:8080'
```
- **/etc/yum.conf**  

```
proxy=http://10.1.1.0:8080
proxy_username=username
proxy_password=password
```
- **Create the /etc/pip.conf file as follows:**  

```
[global]
extra-index-url= https://repo.fortisoar.fortinet.com/connectors/deps/simple/
proxy='http://username:password@10.1.1.0:8080'
```

The following packages must be installed before you begin installing FortiSOAR using the FortiSOAR installer:

- policycoreutils-python
- gcc
- java-11-openjdk

- `yum-utils`
- `ntp`

## Procedure

The following procedure describes the steps that you require to run for installing FortiSOAR 7.2.2 Enterprise Edition and Secure Message Exchange:

1. Provision a CentOS 7 (minimal) VM [recommended version 7.9.2009 (Core)], with the `wget` package.
2. Ensure your VM has disk space of 500 GB. If you have a large volume of data being ingested daily, it is recommended to have a disk space of 1 TB. It is recommended to have a thin provisioned disk.  
You can add three more disks to your Virtual Machine (VM) and create separate Logical Volume Management (LVM) partitioning for PostgreSQL, Elasticsearch and FortiSOAR RPM data. For more information about multiple disk support, see the [Multidisk Support](#) article present in the Fortinet Knowledge Base.  
**Note:** The database disk requires most volume is required for the database disk. So if you are provisioning the volume with multiple disks, the size of the data disk is the most important and should be sufficiently large. Refer to the table that is present at the end of this procedure for the minimum and recommended disk sizes.

3. To ensure that your `ssh` session does not timeout execute the `screen` command.  
For more information on how to handle session timeouts, see the [Handle session timeouts while running the FortiSOAR upgrade](#) article present in the Fortinet Knowledge Base.

4. To download the installer for FortiSOAR 7.2.2:

```
# wget https://repo.fortisoar.fortinet.com/7.2.2/install-fortisoar-7.2.2.bin
```

5. To install FortiSOAR 7.2.2 run the following command as a `root` user:

```
# sh install-fortisoar-7.2.2.bin
OR
chmod +x install-fortisoar-7.2.2.bin
./install-fortisoar-7.2.2.bin
```

The installer will display the following installation options:

**Enterprise**

OR

**Secure Message Exchange**

Choose **Enterprise** in this case and complete the installation.

**Note:** If you are installing FortiSOAR in a closed or air-gapped environment, you will see a message such as "The system does not have connectivity to `https://globalupdate.fortinet.net`. Connectivity...", ignore these warning messages and proceed with the installation as there is no requirement to check the check connectivity to `globalupdate.fortinet.com` in case of an air-gapped environment. For information on licensing in the case of closed environments, see the *FortiSOAR licensing using FortiManager* topic in the [Licensing FortiSOAR](#) chapter.

6. Once the installation is complete, exit the terminal session and log back in using the following default credentials:  
Username: `csadmin`  
Password: `changeme`  
After entering the default credentials, you will immediately be prompted to change the default password. Only after you have changed the default password can you log into FortiSOAR.
7. Once you have logged into FortiSOAR, you will be asked to accept the **EULA**. You must accept the EULA before you can proceed to the FortiSOAR Configuration Wizard.
8. Retrieve your FortiSOAR Device UUID, which is created automatically by the FortiSOAR installation. This Device UUID is used to identify each unique FortiSOAR environment. A `root` user can directly run the following command to retrieve the Device UUID:  
`csadm license --get-device-uuid`  
Use this Device UUID to get your FortiSOAR license using the process detailed in the [Licensing FortiSOAR](#) chapter.

9. Before you deploy your FortiSOAR license, ensure that you can connect to <https://globalupdate.fortinet.net>, else the license deployment will fail. Connectivity to this address is required for fetching the license entitlements and product functioning post-upgrade.  
You can deploy your FortiSOAR license using the FortiSOAR UI or using the FortiSOAR Admin CLI. For more information on deploying the FortiSOAR license, see the [Licensing FortiSOAR](#) chapter.
10. Once your system is licensed, you can log on to the FortiSOAR UI using the default credentials:  
Username: `csadmin`  
Password: `changeme`  
After you enter the default credentials you will be prompted to change the password. Once you have specified the new password, you can log onto FortiSOAR.

Following is a table that contains the minimum and recommended disk sizes:

Mount Point	Recommended Size	Minimum Size
/	6 GB	-
/boot	1.5 GB	-
/tmp	2 GB	1 GB
/opt	9.5 GB	-
/var	4 GB	-
/var/lib/pgsql	500 GB	20 GB
/var/lib/elasticsearch	150 GB	-
/var/lib/rabbitmq	11.5 GB	-
/var/log	5 GB	2 GB
/var/log/audit	1 GB	
/var/log/cyops/coredump	49 GB	-
/home	10 GB	-

## Installing the secure message exchange

A secure message exchange establishes a secure channel that is used to relay information to the agents or tenant nodes. To create a dedicated secure channel, you are required to add the reference of the installed and configured secure message exchange, when you add agent or tenant nodes to your environment. A default "self" secure message exchange configuration is available and can be enabled. However, for a production setup, we recommend that you configure a separate secure message exchange. For more information, see the [Enabling the secure message exchange](#) and [Adding a secure message exchange](#) sections.

Steps for installing the secure message exchange are as follows:

1. Provision a CentOS 7 (minimal) VM [recommended version 7.9.2009 (Core)], with the `wget` package.
2. Ensure your VM has disk space of minimum 50 GB, recommended is 100 GB. It is recommended to have a thin provisioned disk.
3. To ensure that your `ssh` session does not timeout execute the `screen` command.  
For more information on how to handle session timeouts, see the [Handle session timeouts while running the FortiSOAR upgrade](#) article present in the Fortinet Knowledge Base.

4. To download the installer for FortiSOAR 7.2.2 secure message exchange:  

```
wget https://repo.fortisoar.fortinet.com/7.2.2/install-fortisoar-7.2.2.bin
```
5. To install FortiSOAR 7.2.2 secure message exchange run the following command as a root user:  

```
# sh install-fortisoar-7.2.2.bin
```

OR  

```
chmod +x install-fortisoar-7.2.2.bin
```

```
./install-fortisoar-7.2.2.bin
```

The installer will display the following installation options:  
**Enterprise**  
OR  
**Secure Message Exchange**  
Choose **Secure Message Exchange** in this case and complete the installation.

Once you have installed the secure message exchange, a FortiSOAR Secure Message Exchange Configuration Wizard similar to the [FortiSOAR Configuration Wizard](#) is automatically run on the first `ssh` login by the `csadmin` user and it performs the initial configuration steps that are required for the Secure Message Exchange. In the FortiSOAR Secure Message Exchange Configuration Wizard you require to provide certain inputs such as the hostname of the Secure Message Exchange VM, port numbers to be used for the API and TCP connections to the Secure Message Exchange, etc., which are required to complete the initial configuration steps for the Secure Message Exchange.

## Installing FortiSOAR on RHEL using the FortiSOAR installer

This section describes the steps that you require to follow to install FortiSOAR on a Red Hat Enterprise Linux (RHEL) system.

1. Register your RHEL instance:  

```
subscription-manager register --username <username> --password <password>--auto-attach --force
```
2. Enable the optional repositories:  

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```
3. Install the required packages:  

```
yum install policycoreutils-python gcc java-11-openjdk yum-utils -y && yum install wget screen vim -y
```
4. Follow the steps outlined in the [Installing FortiSOAR 7.2.2 using the FortiSOAR installer](#) topic to install FortiSOAR on your RHEL instance.

## FortiSOAR Configuration Wizard

### Interactive VM configuration

A configuration wizard runs automatically on the first `ssh` login by the `csadmin` user and performs the initial configuration steps that are required for FortiSOAR. The wizard guides you through the configuration process with appropriate instructions so that you can efficiently perform the initial configuration required for FortiSOAR. To begin running the configuration wizard, you must accept the Fortinet End User License Agreement.

The wizard performs the following configuration steps:

1. **Change hostname and refresh the MQ node name:** (Optional) You can change the hostname for your FortiSOAR VM and refresh the node name of your MQ. Ensure that the hostname that you provide is resolvable. If the hostname gets resolved by a DNS server, ensure that you provide only the node name and not the complete FQDN. The wizard checks if the hostname is valid or not; and throws an error in case of an invalid hostname. FortiSOAR optionally also asks for additional DNS servers.  
In an environment where DHCP is not enabled, i.e., in case of a static IP environment, the configuration wizard fails since it cannot get the network. Therefore, from version 6.4.1 onwards, the configuration wizard detects whether the FortiSOAR VM has an IP; if the wizard cannot detect an IP, a `Static IP` page is displayed where you can add the Static IP, Gateway, Netmask, DNS1 and DNS2, ensuring that the configuration wizard completes without failure. This also provides users with the flexibility of changing their environment from DHCP to Static without worrying that the configuration wizard will fail since it cannot get the network.  
If the configuration wizard detects an IP, i.e. in case of a DHCP enabled system, the `DNS servers` input page is displayed.  
Also, if you change the hostname, the configuration wizard automatically updates the `HOSTNAME` variable in `/etc/profile`.
2. **Get DNS:** Gets the DNS for your FortiSOAR system
3. **Configure Proxy:** (Optional) You can configure an https/http proxy server to serve all https/http requests from FortiSOAR. To configure an https or http proxy, you must specify the username and password, and the hostname and the port number of the HTTPS or HTTP proxy server. For example to configure an HTTPS proxy, enter the proxy details in the following format: `https://user:password@[ip/fqdn]:port`. You can also configure a comma-separated list of hostnames that do not require to be routed through a proxy server. For example, `[ip1/fqdn1], [ip2/fqdn2]`
4. **Update network configuration:** This is an automatic process.
5. **Set up intra-service authentication:** This is an automatic process to generate new appliance keys unique to your instance for communication to the FortiSOAR services.
6. **Generate certificates:** This is an automatic process; you do not require to provide any inputs.
7. **Generate Device UUID:** This is an automatic process; you do not require to provide any inputs. The wizard also saves the Device UUID in the `/home/csadmin/device_uuid` file.  
This Device UUID is required for when you are generating your license for FortiSOAR. For more information, see the [Licensing FortiSOAR](#) chapter.  
**Important:** You get logged out after the FortiSOAR VM is configured, so that the changes can take effect. Therefore, you require to `ssh` again to the FortiSOAR VM.
8. **Reset database passwords:** This is an automatic process to reset database password to a new password unique to your instance.
9. **Restart services:** This is an automatic process to reset all FortiSOAR services.
10. **Configure default HA cluster:** This is an automatic process that creates the default single-node HA cluster. This FortiSOAR server is created as a primary-active node.
11. **Install python libraries:** This is an automatic process to install some python libraries required by FortiSOAR. From release 7.2.0, the Content Hub data is also synced automatically by the VM Configuration Wizard.
12. **Install default widgets:** This is an automatic process to install some default widgets as part of FortiSOAR.
13. **Search index initialization:** This is an automatic process.
14. **Refresh SSH keys:** This is an automatic process that refreshes the SSH keys and generates the default encryption keys.
15. **Refresh data identifiers:** This is an automatic process.
16. **Post-configuration tasks:** This is an automatic process and includes installing the SOAR Framework Solution pack for your FortiSOAR instance.

After the FortiSOAR Configuration Wizard is run, it displays the following:

- Device UUID
- Path where the Device UUID is saved

- Path of the Configuration Wizard log



If your FortiSOAR Configuration Wizard displays errors when it is being run, then you can troubleshoot the FortiSOAR Configuration Wizard errors by checking its logs, which are located at `/var/log/cyops/install/config_vm_<timestamp>`. For example, `/var/log/cyops/install/config-vm-09_Nov_2018_05h_37m_36s.log`.



If you want to replace the Self-Signed Certificates with your own signed certificates, see the [Updating the SSL certificates](#) topic in the [Additional Configurations](#) chapter.

## Non-interactive VM configuration

The FortiSOAR Configuration Wizard also has a non-interactive mode that automatically performs the initial configuration steps (as mentioned in the [Interactive VM Configuration](#) section) that are required for FortiSOAR, without any inputs from the user. A non-interactive VM configuration is useful when users are expecting a ready-to-use appliance.

The configuration in this case can be done by using the default inputs from the configuration file that is shipped along with the FortiSOAR appliance. To run the FortiSOAR Configuration Wizard in the non-interactive mode, use the following command:

```
/opt/cyops/scripts/config-vm.sh --non-interactive
```

The default configuration file is:

- For the Enterprise edition: `/opt/cyops/scripts/config-vm-enterprise-default.conf` and
- For the Secure Message Exchange: `/opt/cyops/scripts/config-vm-sme-default.conf`

You can customize the non-interactive VM configuration by either updating the existing default configuration file or providing a custom configuration file.

If you have updated the existing default configuration file, then the updated values are considered during the VM configuration when you run the following command:

```
/opt/cyops/scripts/config-vm.sh --non-interactive
```

If you have provided a custom configuration file, then the values provided in the custom configuration file override the ones mentioned in the default configuration file. When you have provided a custom configuration file, use the following command to run the FortiSOAR Configuration Wizard in the non-interactive mode:

```
/opt/cyops/scripts/config-vm.sh --non-interactive --conf <absolute path of the custom configuration file>
```

A configuration file has the following format:

```
key=value
```

Following is a list of supported key names with their sample values:

- `hostname=sample_hostname`
- `dns=sample_dns_name`
- `proxy_https=https://userid:password@www.sample-https.com:9999`
- `proxy_http=http://userid:password@www.sample-http.com:9999`

- `proxy_noproxy=127.0.0.1,sample-no-proxy`
- `static_ip=192.168.51.181`
- `gateway=192.168.51.1`
- `netmask=255.255.255.0`
- `dns1=192.168.60.100`
- `dns2=8.8.8.8`
- `message_queue_user_id=admin`
- `message_queue_password=changeme`
- `message_queue_api_port=15671`
- `message_queue_tcp_port=5671`

### Guidelines for creating custom configuration files:

- Empty keys are ignored. For example: `hostname=`.
- The `userid` and `password` parameters are optional in the `proxy_http` and `proxy_https` keys. The format of the URL is: `proxy_https=https://www.sample-https.com:9999`  
Also note that `proxy_http`, `proxy_https`, and `proxy_noproxy` apply to only the 'Enterprise' edition
- The `static_ip`, `gateway`, `netmask`, `dns1`, and `dns2` keys are considered only in the case of a 'non-dhcp environment'.  
The `static_ip`, `gateway`, `netmask`, and `dns1` keys are mandatory. The `dns2` key is optional.
- The `message_queue_user_id`, `message_queue_password`, `message_queue_api_port`, and `message_queue_tcp_port` keys are applicable to only the 'Secure Message Exchange' edition
- Keys that do not apply to a particular edition are ignored. For example, if you add the `proxy_http` to the 'Secure Message Exchange' edition, the `proxy_http` will be ignored.

## Pointing the ntpd service to a valid ntp server

If the time on the FortiSOAR server is not correct, you might see issues such as ingestion workflows not pulling the latest data from an external source. It is highly recommended to keep the time in sync with an NTP server. Therefore, if you require to change the system time on your FortiSOAR instance, then perform this step immediately after running the FortiSOAR Configuration Wizard.

The `ntpd` service runs on your FortiSOAR instance, and it requires to be pointed to a valid ntp server. If the `/etc/ntp.conf` file contains entries to ntp server(s) that are not valid; then you might face **Invalid System Time** issues where you might not be able to log on to your FortiSOAR instance. Edit the `/etc/ntp.conf` file to add details of a valid ntp server(s). For a list of common NTP servers, go to <https://www.ntppool.org/en/>.

In case your FortiSOAR VM does not have access to the internet, then you must edit the `/etc/ntp.conf` to add details of a valid ntp server within your datacenter.

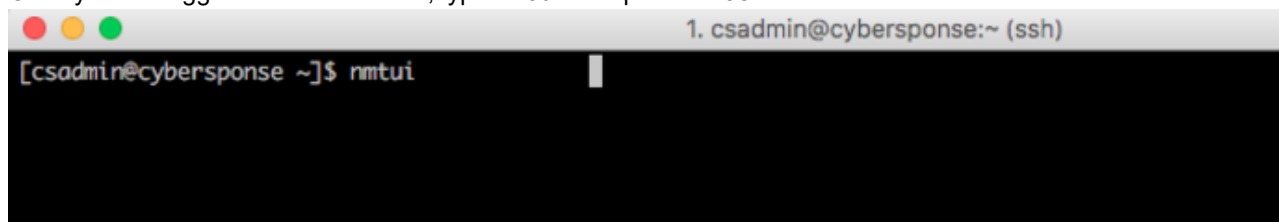
## Editing the VM configuration

It is not necessary to perform the following steps, but they can quickly assist you to get access to the FortiSOAR VM:

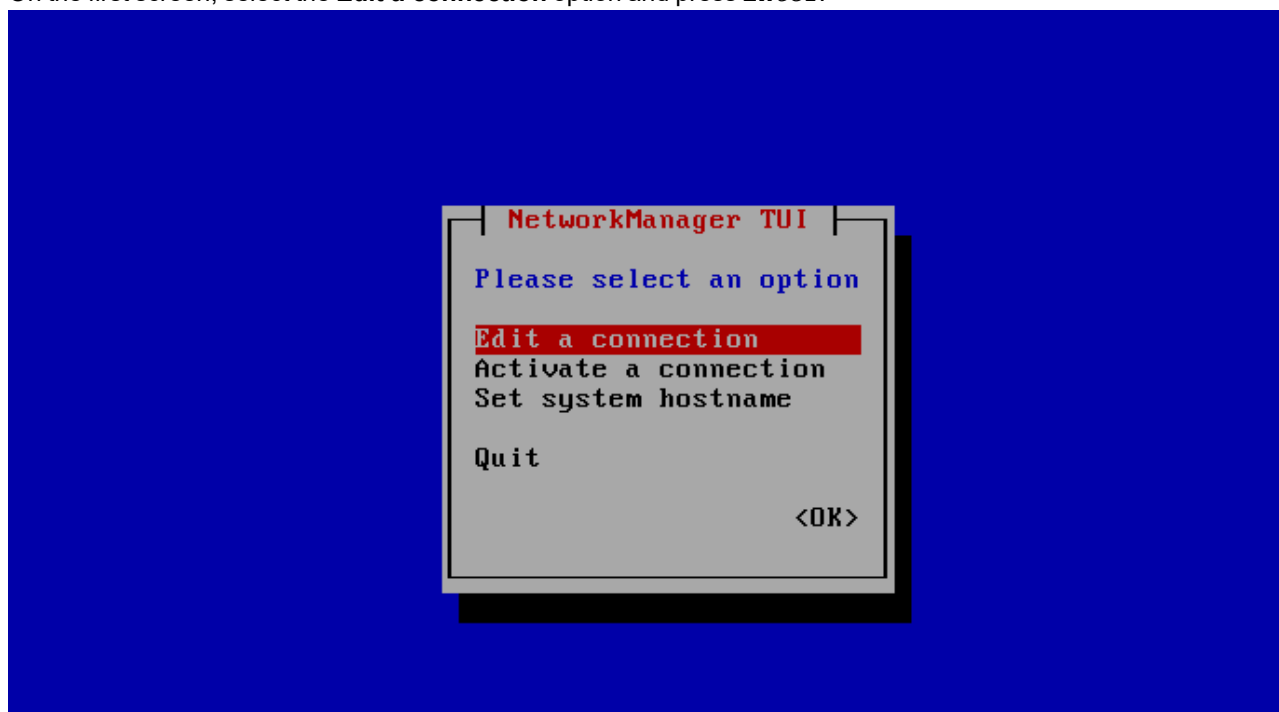
1. Setting a static IP
2. Determining your DHCP IP Address

## Setting a static IP

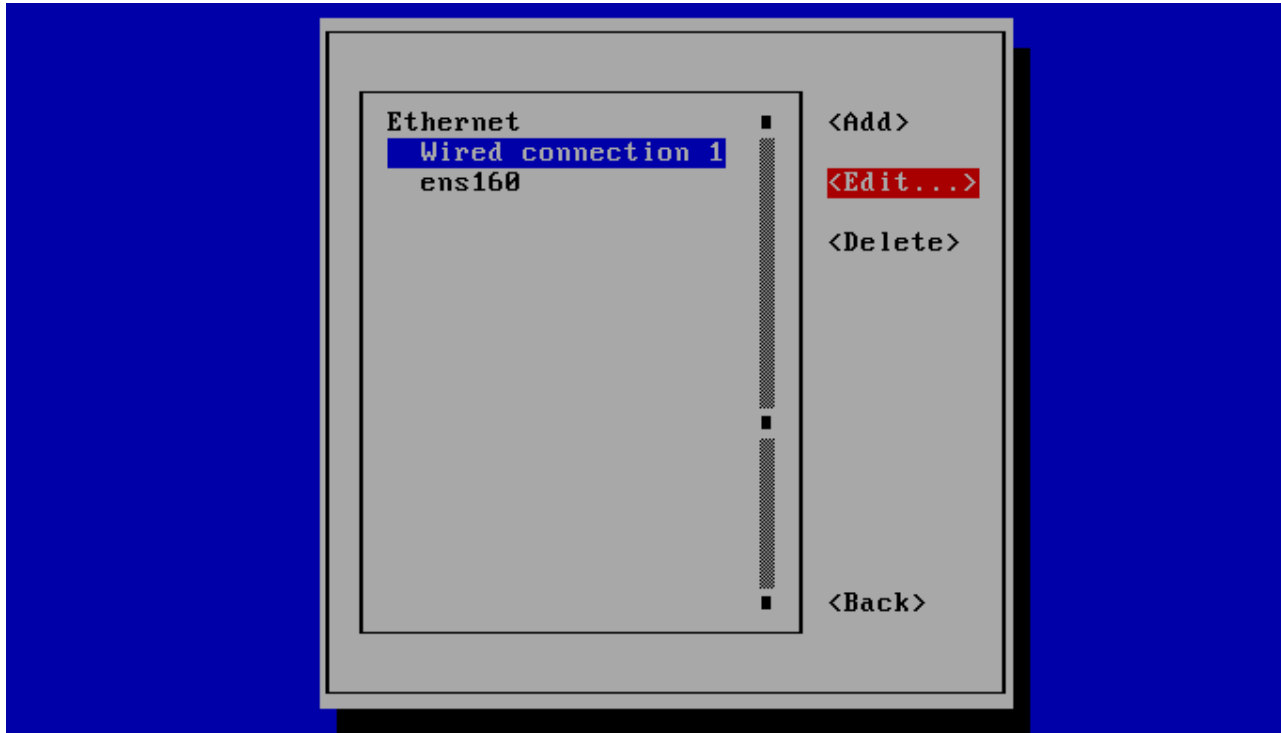
1. On the ESX console for your FortiSOAR VM, login to the VM as the `csadmin` user.
2. Type `sudo -i` in the terminal and press `Enter` to become a root user.
3. Once you are logged in to the terminal, type `nmtui` and press `Enter`.



4. On the first screen, select the **Edit a connection** option and press `Enter`.



5. On the second screen, select the connection listed under Ethernet, which is **Wired connection 1** and select **<Edit...>**.

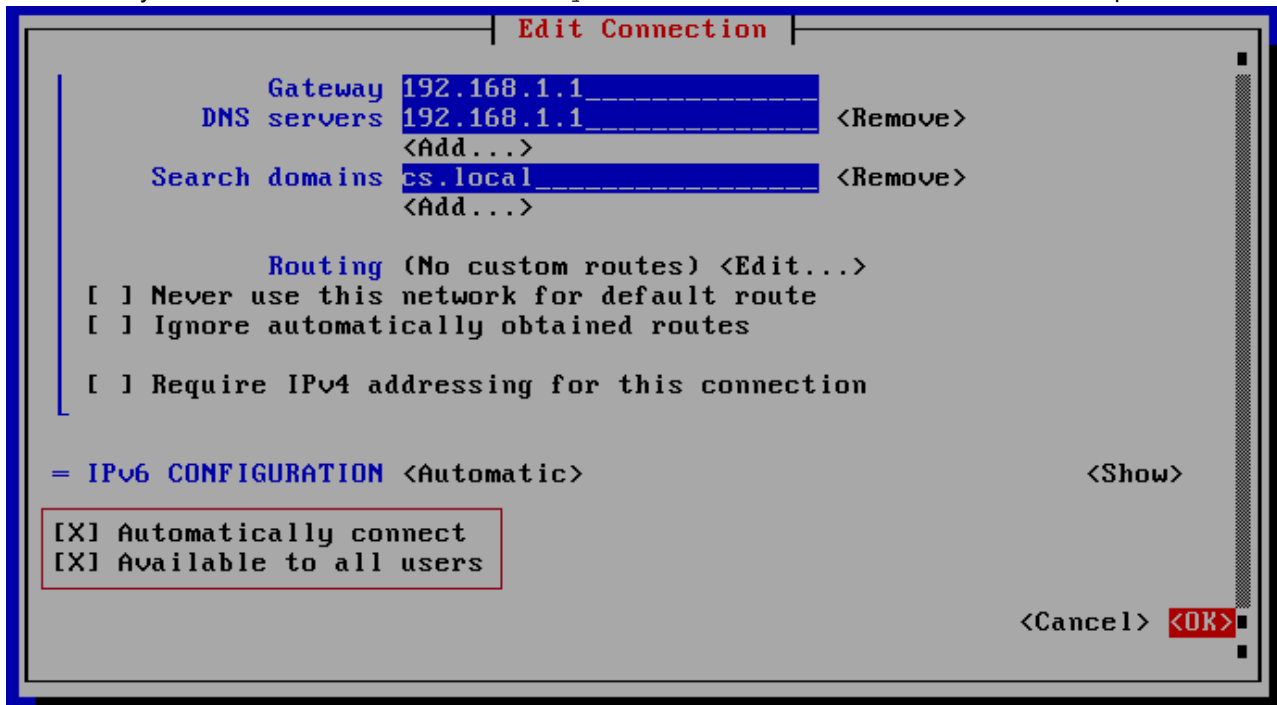


6. Use the arrow keys to select **<Show>** that appears to the right of the IPv4 Configuration option and press **Enter**.
7. Enter the required information for your network. You must enter all the information, such as IP Address, Gateway, DNS servers address, on this screen:

The screenshot shows the 'Edit Connection' screen. At the top, the title 'Edit Connection' is in red. Below it, the 'Profile name' is 'Wired connection 1' and the 'Device' is '00:0C:29:EE:75:35 (ens160)'. The configuration is organized into sections:

- = ETHERNET** with a '<Show>' button on the right.
- = IPv4 CONFIGURATION** with '<Manual>' and '<Hide>' buttons on the right.
  - Addresses:** '192.168.1.10/32' with a '<Remove>' button and a '<Add...>' button below it.
  - Gateway:** '192.168.1.1' with a '<Remove>' button.
  - DNS servers:** '192.168.1.1' with a '<Remove>' button and a '<Add...>' button below it.
  - Search domains:** 'cs.local' with a '<Remove>' button and a '<Add...>' button below it.
  - Routing:** '(No custom routes) <Edit...>'
  - Checkboxes:
    - [ ] Never use this network for default route
    - [ ] Ignore automatically obtained routes
    - [ ] Ignore automatically obtained DNS parameters
    - [ ] Require IPv4 addressing for this connection

8. (Optional) If you want to configure IPv6, repeat steps 5 and 6 and then enter the required information, such as IPv6 Address, for your network.
9. Ensure that you have selected the `Automatically connect` and `Available to all users` options.



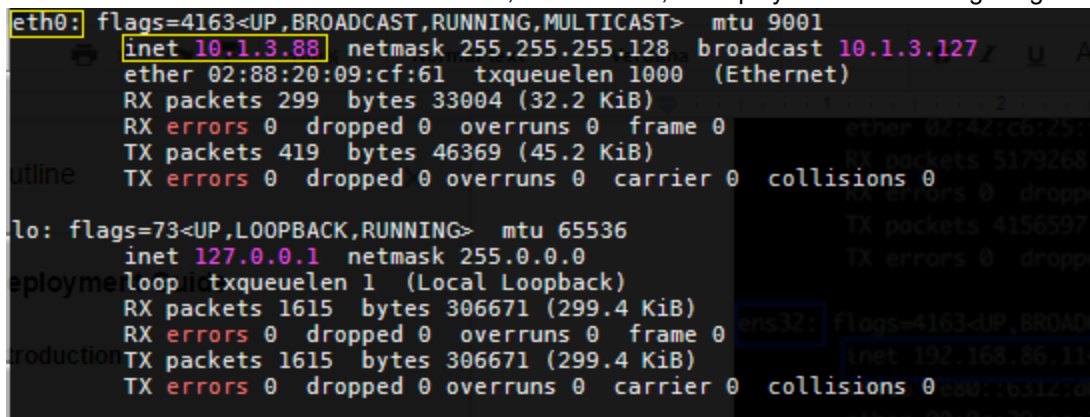
10. Select `<OK>` and press `Enter`.
11. Select `<Back>` and press `Enter`.
12. Select `<OK>` and press `Enter`.
13. Restart the network service using the `systemctl restart network` command.

Once the network service restarts, you can use the assigned static IP.

## Determining your DHCP IP address

1. On the ESX console for your FortiSOAR VM, login to the FortiSOAR VM as the root user.
2. Type `ifconfig | more` in the terminal and press `Enter`.

Your IP address is listed in the `eth**` section, next to `inet`, as displayed in the following image:





Once you have completed configuring the hostname and IP address ensure that the default inbound ports mentioned in the 'VM Inbound Networking' section are open and accessible.

---

Now you must follow the licensing process required for FortiSOAR and then you can use this IP address to log on to the FortiSOAR UI and begin the configuring the system. See the [Licensing FortiSOAR](#) chapter for more information.

## Deploying FSR Agents

FortiSOAR supports segmented networks, which facilitates investigation in a multi-segmented network by allowing secure remote execution of connector actions. If your requirement is to be able to remotely run connector actions, then you can use the "FSR Agent".

Automated ingestion, enrichment, or triage actions using a SOAR platform require network connectivity to various endpoints on which you want to run connector actions. These devices or endpoints, can at times, be in a different network segment than the one where the FortiSOAR node is deployed. To connect to such endpoints in segmented networks, FortiSOAR provides a lightweight component, called the "FSR Agent". A FSR Agent can be deployed in a network segment and configured to receive and execute connector actions from a FortiSOAR node using its secure message exchange. The FSR Agent only needs an outbound network connectivity to the secure message exchange server on its TCP port. It does not need a VPN setup or an inbound network connectivity.

---



You do not require any additional licensing for the FortiSOAR secure message exchange.

---

From version 7.0.2 onwards, you can use client certificate based authentication to create connections between the FSR agent and secure message exchange. Prior to the 7.0.2 release, basic authentication using username and password was used to create connections between FSR agent and secure message exchange. Going forward, you can configure the following types of authentications to connect FSR agent and secure message exchange:

- **Basic Authentication:** Uses username and password to create connections between FSR agent and secure message exchange.
- **Basic Authentication with Peer Verification:** Uses username and password to create connections between FSR agent and secure message exchange, and also performs 'Certificate Verification'. This process will verify that the clients which are attempting to connect can be trusted by presenting a certificate that is signed by a CA and trusted by the server; thereby ensuring that only trusted clients can connect to the secure message exchange.
- **Client Certificate Authentication:** Presents a certificate to the server which is signed by a trusted CA. It is recommended that you create the certificate with the common name as the name of your agent or tenant. This provides enhanced security as this gives the facility to connect only to trusted clients.

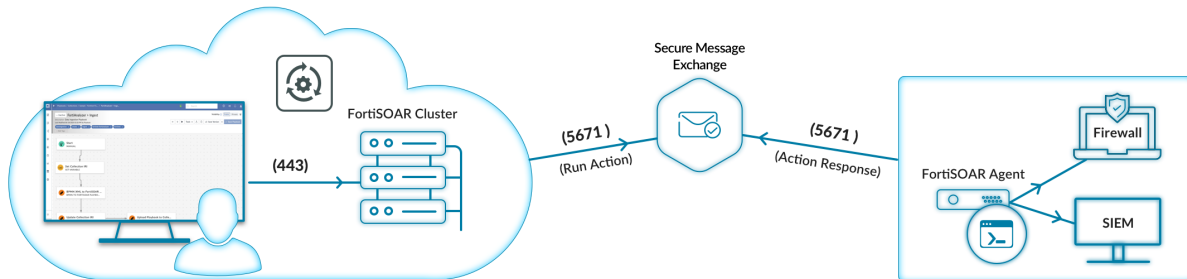
To enable client certificate authentication, you can specify the authentication type as '**Certificate Auth**' while adding a FSR agent.

To enforce client certificate verification, you must provide a pair of exchange event listener client certificates and exchange event listener client key when you are adding a secure message exchange. Client verification ensures that whenever any client wants to connect to secure message exchange that client must present the client certificate to the secure message exchange for verification. You must also provide the pair of exchange event listener client certificates and exchange event listener client key, if you have enabled mutual TLS (mTLS). Use the `csadm mq mTLS` command to

enable or disable mTLS. For more information on `csadm`, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."

## Architecture

### Agents for Segmented Network Support



## Recommended Resource Requirements for Virtual Machines (VM)

### Recommended specifications for Secure Message Exchange

- 8 available vCPUs
- 16 GB available RAM
- 100 GB available disk space: Recommended to have high-performance storage, preferably SSDs.
- 1 vNIC

### Recommended specifications for FSR agents

- 4 GB available RAM
- CentOS Linux release 7.9.2009 (kernel-3.10.0-1160.6.1.el7.x86\_64) or Red Hat Enterprise Linux (RHEL) Server release 7.9 (Maipo) (Kernel - 3.10.0-1160.el7)

## Prerequisites for installing a FSR agent

- Ensure that the VM on which you want to install the FSR agent matches the recommended specifications, see [Recommended specifications for FSR agents](#).
- Ensure that [repo.fortisoar.fortinet.com](https://repo.fortisoar.fortinet.com) is reachable or resolvable from the VM on which you want to install the FSR agent.
- Ensure that the secure message exchange that you have specified when you have added the FSR agent is reachable or resolvable from the VM.

- Ensure that the following packages are installed on the instance where you are going to install the FSR agent:
  - **Python36-devel:** The FSR agent runtime needs "python36-devel". During FSR agent installation, the installer looks for an existing installation, and in the case, it is not installed, tries to install it using `yum install`. If this package is not found, the FSR agent installation will fail.
  - **GCC:** Some connectors have a dependency on GCC. Therefore, the FSR agent installer looks for an existing installation, and tries to install it using `yum install`. If this package is not found, the FSR agent installation will display a "warning" and will not fail the installation. You can install GCC later on a FSR agent using the `yum install gcc` command, if you want to use a connector that is dependent on GCC.

You can either keep these packages pre-installed on the FSR agent's system, or along with the default repos ensure that the following repos are enabled, so that they get installed during agent binary installation:

For CentOS: `CentOS-Base.repo`  
 For RHEL: `rhel-7-server-optional-rpm` and `rhel-7-server-rhsc1-7-rpms` for RHEL

**Note:** If the connector has dependency on any other package or application to work then that package or application will require to be separately installed on the FSR agent. For example, the nmap connector requires the nmap application to be installed, therefore you would require to install this application separately on the agent.

## Process of setting up a FSR agent

1. Add a secure message exchange.  
 A Secure Message server is used for communication with FSR Agents or dedicated tenant nodes. You can add both externally deployed secure message exchange or the Default (Embedded) secure message exchange.  
 If you want to use the local i.e., Default (Embedded) secure message exchange to connect to external FSR agents and run remote actions on various segments of your network or in case of a dedicated tenant, then you must enable the secure message exchange as described in the [Enabling the secure message exchange](#) section. In case of an external secure message exchange, then add the secure message exchange as described in the [Adding a Secure Message Exchange](#) section.
2. Add FSR agents to your FortiSOAR instance. See the [Adding a FSR agent](#) section.
3. Install FSR agents. See the [Installing a FSR agent](#) section.

## Minimal permissions required

To configure and install FSR agents:

- Create, Read, and Update permissions on Agents.
- Read permissions on Application and Secure Message Exchange.



A role named "FortiSOAR SNS" is created on upgrade with the permissions listed above. Upgraded users can assign this role to the admin users to start configuring and using agents for various actions. The "FortiSOAR SNS" role must be added to the `Agent` and `Playbook` appliance roles.

## Enabling the secure message exchange

A secure message exchange establishes a secure channel using which you can relay information to your FSR agent or tenant nodes. A Default (Embedded) secure message exchange configuration is available on every FortiSOAR node that can be enabled as explained in this section.

To use the Default (Embedded) secure message exchange to connect to external FSR agents, you must enable the secure message exchange using the `csadm secure-message-exchange enable` command. For more information on `csadm`, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."



For a production setup, it is recommended that you add and configure an external secure message exchange for handling scale and high availability.

## Adding a Secure Message Exchange

Install a [secure message exchange](#) and then adding the reference of this secure message exchange in the tenant or FSR agent node(s) creates a dedicated secure channel of communication. You can have more than one secure message exchange in the configuration. You can distribute tenants across secure message exchanges based on the geographical locations, scale, or compliance policies of the respective customers.

To add a secure message exchange, do the following:

1. Log on to FortiSOAR as an administrator.  
**Note:** Administrator role must have `Create`, `Update`, and `Delete` permissions on Secure Message Exchange.
2. Click the **Settings** (⚙️) icon to open the `System` page.
3. On the `System` page, you will see the `Agent Configurations` section. Click the **Secure Message Exchange** item in the left menu, to configure the secure message exchange.

**Agent Configurations / Secure Message Exchanges**

Add and manage your secure message exchanges

A secure message exchange establishes a secure channel which is used to relay information to your agent/tenant nodes. Add secure message exchange(s) configurations below and refer them when adding agent/tenant nodes to create a dedicated secure channel. A default self message exchange configuration is available and can be enabled, however for production setup, it is recommended that separate ones are used. Refer to the Segmented Network Configuration section in the FortiSOAR Help guide for more details.

2 Items [+ Add Secure Message Exchange](#)

<input type="checkbox"/>	Name	Address	API Port	TCP Port	User Name	Certificate	Configuration Status	Actions
<input type="checkbox"/>	Dev Router	secure.router.dev	15671	5671	admin	-----BEGIN CERTIFI...	Configured	<a href="#">Refresh</a> <a href="#">Delete</a>
<input type="checkbox"/>	Localhost router	localhost	15671	5671	admin	-----BEGIN CERTIFI...	Configured	<a href="#">Refresh</a> <a href="#">Delete</a>

Items Per Page: 30

4. Click **Add Secure Message Exchange** on the `Secure Message Exchanges` page.  
**Important:** To add a secure message exchange and configure tenants, you must have a role that has a minimum of `Create` and `Read` permissions on the **Secure Message Exchange** and **Tenants** modules. To update the details of the secure message exchange you additionally require `Update` permissions on the **Secure Message Exchange** and **Tenants** modules.  
To edit the configuration of an existing secure message exchange, click the secure message exchange row whose configuration you want to update. This displays the `Edit Secure Message Exchange` dialog. Update the configuration parameters, as required, in the dialog and click **Update**.
5. In the `Add New Secure Message Exchange` dialog, configure the following parameters:
  - a. In the **Name** field, enter the name of the secure message exchange that you have configured to act as a secure channel of data replication between the FortiSOAR node and tenant or FSR agent nodes.

- b. In the **Address** field, enter the FQHN (Fully Qualified Host Name) of the secure message exchange.  
**Important:** Ensure that the FQHN matches the Certificate Name (CN) or the Subject Alternative Name (SAN) provided in the SSL certificate used to configure the secure message exchange.
- c. In the **Username** field, enter the username you will use to login to your secure message exchange as an administrator.  
By default, it is set as `admin`.
- d. In the **Password** field, enter the password you will use to login to your secure message exchange as an administrator.
- e. In the **Server Name Indication** field, enter the Server Name Indication (SNI) address for the Secure Message Exchange. You must specify the SNI address when the Secure Message Exchange is behind a reverse proxy or in a cluster behind a load balancer such as FortiADC.
- f. In the **API Port** field, enter the RabbitMQ Management port number that you had specified while configuring the secure message exchange, and ensure that the FortiSOAR node has outbound connectivity to the secure message exchange at this port.  
By default, it is set as `15671`.
- g. In the **TCP Port** field, enter the TCP port number that you had specified while configuring the secure message exchange, and ensure that the FortiSOAR node has outbound connectivity to the secure message exchange at this port.  
By default, it is set as `5671`.
- h. In the **CA Certificate** field, copy-paste the certificate text of the Certificate Authority (CA) that has signed the secure message exchange certificate in the `pem` format. You can also upload the certificate file. If it is a chain, then the complete chain must be provided.  
By default, the CA certificate for the FortiSOAR self-signed certificate is present at the following location:  
`/opt/cyops/configs/rabbitmq/ssl/cyopsca/cacert.pem`.  
**Important:** If in the future, your secure message exchange certificate expires, and you need to deploy a new certificate, then the new certificate must be copied back to the master node as well as the tenant's router entry. Client certificate can be opted from Certificate Authority in case CA signed certificates are deployed on secure message exchange or if there are no external CA signed certificates deployed. Client certificates can be generated using the following command:  

```
csadm mq client-certs generate --common-name MQ_CLIENT_CERT_COMMON_NAME [--target-dir MQ_CLIENT_CERT_TARGET_DIR]
```

  
Once the certificates are generated, the same can be used in the **Exchange Event Listener Client Cert** and **Exchange Event Listener Client Key** fields. For more information, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."  
**Note:** The default self-signed certificates shipped with FortiSOAR are valid for one year from the inception of your FortiSOAR instance. It is recommended to regenerate these certificates before the end of one year. Steps for this are mentioned in the `Regenerating self-signed certifications` topic in the [Additional Configurations](#) chapter.
- i. (Optional) If you have enabled the mTLS, i.e., you require that clients that want to connect to secure message exchange must present their client certificate to the secure message exchange for verification, then you must also provide a pair of exchange event listener client certificates and exchange event listener client key, as follows:
  - i. In the **Exchange Event Listener Client Cert** field, copy-paste the client certificate text or you can also upload the client certificate file.
  - ii. In the **Exchange Event Listener Client Key** field, copy-paste the client key text or you can also upload the client key file.
- j. To save the configuration for the secure message exchange on the FortiSOAR node, click **Save**.



After you have updated your secure message exchange configuration, the updated configurations might take some time to get reflected.

## Adding a FSR agent

To add a FSR agent, do the following:

1. Log on to your base FortiSOAR node as an administrator and click the **Settings** icon to open the *System* page.
2. To add FSR agents, in the *Agent Configurations* section, click **Agents** in the left menu and click **Add**.  
To edit the configuration of an existing FSR agent, click the FSR agent whose configuration you want to update, which opens the FSR agent record in the detail view. Update the configuration parameters as required.  
If you no longer require an existing FSR agent, you can deactivate or deboard an FSR agent. To deactivate an agent, clear the **Enabled** checkbox in the FSR agent record.  
Deboarding a FSR agent is an irreversible operation which also deletes all data related to that FSR agent from the FortiSOAR node. For more information, see [Deboarding FSR Agents](#).
3. On the *Agent* page, click **Add** to open the *Add New Agent* dialog and configure the following parameters for the FSR agent:
  - a. In the **Name** field, enter the name of the FSR agent.
  - b. From the **Secure Message Exchange** drop-down list, choose the secure message exchange that you have configured as the secure channel using which you can relay information to your FSR agent.
  - c. (Optional) In the **Description** field, enter the description of the FSR agent.
  - d. If you have selected **Certificate Auth** from the **Auth Type** drop-down list, then in the **Client Certificate** field, copy-paste the client certificate text of the Certificate Authority (CA) that has signed the secure message exchange certificate in the *pem* format. You can also upload the client certificate file.  
If you want to enforce client certificate verification with **Basic Auth** then also you must provide client certificate in this field, so that the secure message exchange will verify the certificate before allowing connection to any client.  
**Note:** If you are using CA signed certificates on secure message exchange, you must add these certificates to the truststore using the following command:  

```
csadm mq truststore add --ca-cert CA_CERT_PATH
```

 For more information, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."
  - e. Similarly, in the **Client Key** field, copy-paste the client key text or you can also upload the client key file.  
Client certificate and key can be opted from Certificate Authority if CA signed certificates are deployed on secure message exchange or if there are no external CA signed certificates deployed. Client certificates can be generated using the following command:  

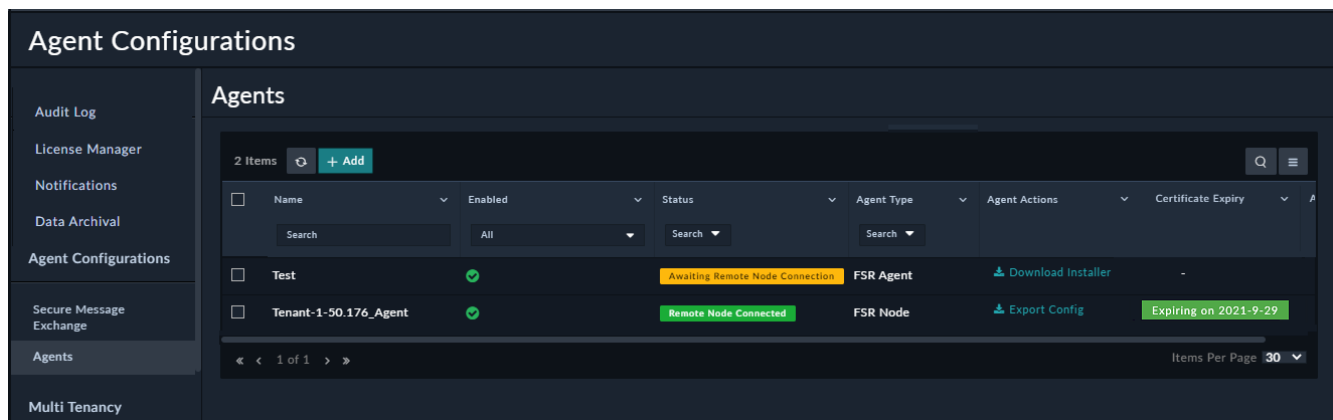
```
csadm mq client-certs generate --common-name MQ_CLIENT_CERT_COMMON_NAME [--target-dir MQ_CLIENT_CERT_TARGET_DIR]
```

 Once the certificates are generated, the same can be used in the **Client Certificate** and **Client Key** fields. For more information, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."
  - f. From the **Auth Type** drop-down list, select the type of authentication you want to enforce for agents or clients to connect to the secure message exchange.
  - g. From the **Owners** drop-down list, select the teams that you want to add as owners of the FSR agent and click **Link Team**.  
If you do not select any team, then the teams that the user who adds the FSR agent belongs to will be associated as owners of the agent. Teams help in governing RBAC for the FSR agent. While running connector actions using FSR agents, users will only see FSR agents that are associated with their teams.
  - h. To complete adding the FSR agent, click **Create**.

Once you have completed adding the FSR agent, you will see the status for the FSR agent. Following is the list of statuses that can be displayed:

- **Configuration In Progress:** Process of configuring the FSR agent has begun.
- **Awaiting Remote Node Connection:** Connection between the FortiSOAR node and secure message exchange is established and awaiting the connection to the FSR agent.
- **Remote Node Connected:** FSR Agent has been connected to the FortiSOAR node using secure message exchange.
- **Configuration Failed:** FSR Agent failed to be added on the secure message exchange.
- **Message Exchange Unreachable:** Secure message exchange is unreachable.
- **Remote Node Unreachable:** FSR Agent is unreachable from the FortiSOAR node.

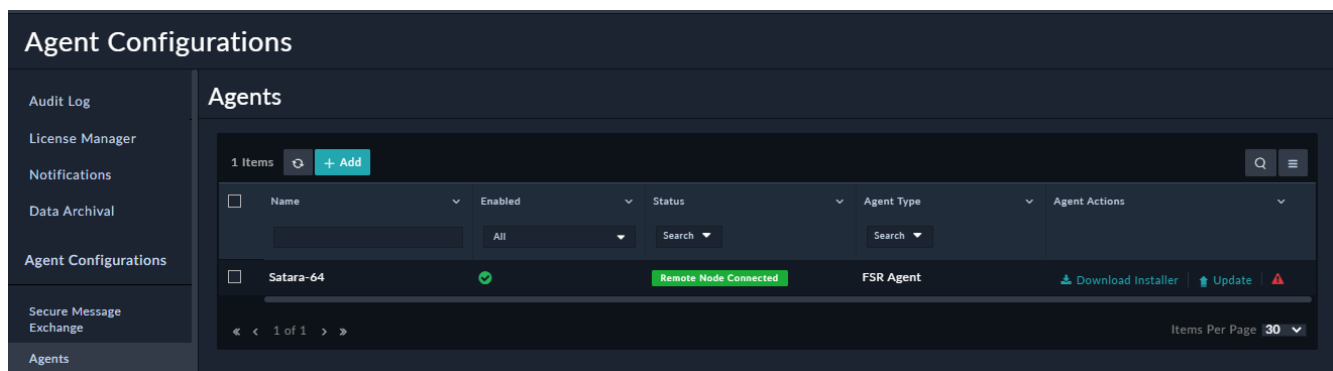
If the connection between the FortiSOAR node and secure message exchange is established, then the `Status` column displays "Awaiting Remote Node Connection" along a **Download Installer** link. Now, you are required to download the FSR agent installer and install the FSR agent as described in the following section.



In the `Agent Actions` column, you will see either the **Export Config** link or the **Download Installer** link. The **Download Installer** link represents a "FSR Agent" and you can use this link to install the agent at a specified endpoint. The **Export Config** link represents a "FSR Node", i.e., in this case the agent represents a dedicated tenant and you can use this link to export the configuration of the dedicated tenant.

If the `Status` column displays statuses like "Message Exchange Unreachable" or "Remote Node Unreachable", the `Agent Actions` column will also display a **Retry** link that allows you to again perform the operation.

From FortiSOAR version 6.4.4 onwards, you might also see a **Warning** symbol in the `Agents Action` column as shown in the following image:



The **Warning** symbol indicates that the master cannot remotely execute or manage connector actions on the FSR agent. Prior to version 6.4.4., the FortiSOAR UI did not provide any indication of remote connector management, and if remote connector management was disabled at the FSR agent, then the master was not notified. Due to this if the master triggers any remote request, then that would get ignored by the FSR agent since the remote operation had been disallowed. Therefore, in version 6.4.4, the **Warning** icon is introduced to indicate when remote connector management is disabled.

To enable or disable remote connector management on the FSR agent, you must have a minimum of **Upgrade** permission on the **Agent** module, and to disallow the master from remotely executing connector actions on an FSR agent, ensure that the FSR agent's version must be 6.4.4 and later.

Then, ssh to the FSR agent's VM and edit the `/opt/cyops-integrations/integrations/configs/config.ini` file and set the value of the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter:

- To enable remote connector management, set the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter to `true`.
- To disable remote connector management, set the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter to `false`.

Once you have completed editing the `config.ini` file and setting the value of the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter, restart the `cyops-integrations-agent` service. Restarting the `cyops-integrations-agent` service notifies these changes to the master node.

From version 7.0.2 onwards, the agent grid will also contain an **Auth Type** column which displays whether the agent will use **Basic Auth** or **Certificate Auth** to connect to the secure message exchange. It also contains a **Certificate Expiry** column, which displays when the client certificate will expire in case of Certificate Authentication or Basic Authentication with Peer Verification. In the case of **Basic Auth**, if you provide certificates while adding agents, then the certificate expiry will be displayed; however, if you do not provide any certificates while adding agents, then a blank will be displayed in the Certificate Expiry column shown in the following image:

Agent Configurations							
<ul style="list-style-type: none"> <li>Audit Log</li> <li>License Manager</li> <li>Notifications</li> <li>Data Archival</li> <li>Agent Configurations</li> <li>Secure Message Exchange</li> <li>Agents</li> <li>Multi Tenancy</li> </ul>	Agents						
	3 Items <span>+ Add</span> <span>Q</span> <span>≡</span>						
	<input type="checkbox"/>	Name	Agent Type	Enabled	Status	Agent Actions	Certificate Expiry
		<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="All"/>	<input type="text" value="Search"/>		<input type="text" value="Search"/>
	<input type="checkbox"/>	tenant77	FSR Agent	✓	Awaiting Remote No	Download Installer	-
	<input type="checkbox"/>	agentDemo	FSR Node	✓	Remote Node Conne	Export Config	Expiring on 2021-9-29
	<input type="checkbox"/>	agentDemo7	FSR Agent	✓	Awaiting Remote No	Download Installer	Expiring on 2021-9-29
	< < 1 of 1 > >						
	Items Per Page: 30						



If you have enabled mTLS on secure message exchange, and you have added the secure message exchange client certificate and key after the FSR agent is added or if you have updated the secure message exchange client certificate and key after they have expired, then you require to first disable and again enable the agent to re-trigger the event listener and update agent status correctly.

## Installing a FSR agent

Before you install a FSR agent, ensure that you meet all the prerequisites to installing an FSR agent. For more information, see [Prerequisites for installing a FSR agent](#).

To install a FSR agent, do the following:

1. Click the **Download installer** link on the `Agents` page.
2. On the `Prepare and Download Agent Installer` dialog, from the **Include Specified Connectors to install on Agent** drop-down list, choose which connectors you want to include while installing the FSR agent. You can choose from the following options: Do not install connectors by default, Custom, All connectors installed on Master, or Include pre-existing connectors on agent.  
 FSR Agents use connectors to remotely run actions on a remote network. If you select **Do not install connectors by default**, then connectors are not installed on the FSR agent, except for the "Utilities" connector that is installed, by default, on the FSR agent.  
 If you select **Custom**, then from the **Select Connectors** drop-down list you have to select the connectors that you want to install on the FSR agent. Note that only connectors that are installed on FortiSOAR (master) node can be installed on the agent. If you select **All connectors installed on Master**, then all the connectors that are installed on FortiSOAR are installed on the FSR agent.  
 If you had an FSR agent system on which you had configured some connectors, which you required to re-provision, if for example, there were some issues with the FSR agent's system, then you can download the FSR agent installer again, and select the **Include pre-existing connectors on agent** option. Selecting the **Include pre-existing connectors on agent** bundles up the connectors and their configurations of those connectors that were previously installed and configured on the FSR agent.
3. Click **Download Installer**.

Once you click **Download Installer**, the installer file named as `<agent-name>-install.bin` is downloaded on your VM. Copy-paste this installer to the FSR agent VM and install the FSR agent.

The installer installs the following for the FSR agent:

- PostgreSQL database.
- `cyops-integrations-agent`

After the installation is complete, you should check the status of the `cyops-integrations-agent` service. Also, note that the password for PostgreSQL is the ID of the FSR Agent.

Once you have completed installing the FSR agent, you can begin to run connector actions on FSR agents, install and configure custom connectors, and perform other administrative functions. For information on all these functions, upgrading the FSR agent, see the *Segmented Network Support* chapter in the "Administration Guide."

## Deboarding FSR Agents

To deboard existing FSR agents, you require to have `Read` and `Delete` permissions on the `Agents` module. Deboarding agents not only deletes the FSR agent, but also removes the list of connectors installed and all the configurations of the connectors that have been installed on the specific FSR agent from the FortiSOAR node. Once you delete a FSR agent, you cannot retrieve any information related to that FSR agent, therefore you must be careful while performing this operation.

To deboard a FSR agent, log on to FortiSOAR as an administrator and click the **Settings** icon to open the `System` page. Click **Agents** in the left menu and on the `Agents` page, click **Delete**. FortiSOAR will display a warning dialog, click **Confirm** on the warning dialog to deboard the FSR agent.

## Moving a FSR agent to a new secure message exchange

If you have added a new secure message in your environment, and you want to move your FSR agent to the new secure message exchange, do the following on the FortiSOAR system:

1. Add the new secure message on your FortiSOAR system. For more information, see the [Adding a Secure Message Exchange](#) section.
2. Log on to your FortiSOAR node, master node in case of a distributed multi-tenant configuration, as an administrator and click the **Settings** icon to open the *System* page.
3. In the *Agent Configurations* section, click **Agents** in the left menu.
4. Click to open the FSR agent record that you want to move to the new secure message exchange.
5. In the FSR agent record, from the **Secure Message Exchange** drop-down list, select the secure message exchange on which you want to move the FSR agent.
6. Restart the `cyops-postman`, `uwsgi`, and `cyops-integrations-agent` services on the master node, using the following command:

```
systemctl restart cyops-postman uwsgi cyops-integrations-agent
```

After you have completed updating the router information and restarting the services, you must download the FSR agent installer again and reinstall the FSR agent on the FSR agent VM.

## Adding multiple disks and partitioning disks in your FortiSOAR VM

Multiple disks are supported for the FortiSOAR installation. Having multiple disks for the FortiSOAR installation has the advantage of being able to detach the disks that contain data and recover data, in the event of a FortiSOAR system crash. For the procedure for recovering data see the [Recovering Data](#) topic. For the procedure for extending existing disks, see the Troubleshooting issues occurring in FortiSOAR due to insufficient space topic in the [Troubleshooting FortiSOAR](#) chapter.

You can add three more disks to your Virtual Machine (VM) and create separate Logical Volume Management (LVM) partitions for PostgreSQL and Elasticsearch data.

For example, you have added the following new disks:

- `/dev/sdb`: Recommended to have a thin provisioned disk for PostgreSQL data whose disk size is 500GB.
- `/dev/sdc`: Recommended to have a thin provisioned disk for Elasticsearch data whose disk size is 150GB.
- `/dev/sdd`: Recommended to have a thin provisioned disk for FortiSOAR™ RPM data whose disk size is 20GB.

### Partitioning the disks



The steps mentioned in this topic are for a fresh installation of FortiSOAR that has been installed using the `.bin` file.

To partition the `/dev/sdb`, which is the disk for PostgreSQL data, run the following commands as a *root* user:

1. `pvcreate /dev/sdb`
2. `vgcreate vgdata /dev/sdb`
3. `mkdir -p /var/lib/pgsql`
4. `lvcreate -l 100%VG -n relations vgdata`
5. `mkfs.xfs /dev/mapper/vgdata-relations`

6. `mount /dev/mapper/vgdata-relations /var/lib/pgsql`
7. `echo "/dev/mapper/vgdata-relations /var/lib/pgsql xfs defaults 0 0" >> /etc/fstab`

To partition the `/dev/sdc`, which is the disk for Elasticsearch data, run the following commands as a *root* user:

1. `pvcreate /dev/sdc`
2. `vgcreate vgdata /dev/sdc`
3. `mkdir -p /var/lib/elasticsearch`
4. `lvcreate -l 100%VG -n search vgsearch`
5. `mkfs.xfs /dev/mapper/vgsearch-search`
6. `mount /dev/mapper/vgsearch-search /var/lib/elasticsearch`
7. `echo "/dev/mapper/vgsearch-search /var/lib/elasticsearch xfs defaults 0 0" >> /etc/fstab`

To partition the `/dev/sdd`, which is the disk for FortiSOAR RPM data, run the following commands as a *root* user:

1. `pvcreate /dev/sdd`
2. `vgcreate vgdata /dev/sdd`
3. `mkdir -p /opt`
4. `lvcreate -l 100%VG -n csapps vgapp`
5. `mkfs.xfs /dev/mapper/vgapp-csapps`
6. `mount /dev/mapper/vgapp-csapps /opt`
7. `echo "/dev/mapper/vgapp-csapps /opt xfs defaults 0 0" >> /etc/fstab`

## Recovering data



Commands for recovery of data must be run as a *root* user.

Following is the procedure for recovering data from the disks:

1. Deploy the recovery VM that has the same version of FortiSOAR installed (OVA or AMI) and power it **ON**.
2. In the `/etc/fstab` file, comment out the lines that contain the word `vgdata` or `vgapp`.
3. Rename the `vgdata` and `vgapp` volume groups using the following command:
 

```
vgrename vgdata old_vgdata
vgrename vgapp old_vgapp
```
4. Stop all FortiSOAR™ services using the following command:
 

```
csadm services --stop
```
5. Run the `umount /var/lib/pgsql/ && umount /opt` command.
6. Deactivate the volume group using the following command:
 

```
vgchange -a n old_vgdata old_vgapp
```
7. Find out which disks contain the `vgdata` and `vgapp` volume groups using the `'pvs'` command.  
 For example, if `vgdata` is on `/dev/sdb` and `vgapp` is on `/dev/sdd`, you require to skip these disks from `lvm` scanning. To skip the disks from `lvm` scanning add the 'skip' filter in the `/etc/lvm/lvm.conf` file as follows:
  - a. Open the `/etc/lvm/lvm.conf` file using the `vi /etc/lvm/lvm.conf` command.
  - b. In the "devices {" section in the `lvm.conf` file, add the following line:
 

```
filter = ["r|/dev/sdb|", "r|/dev/sdd|"]
```

8. Stop the source VM and attach the existing PostgreSQL and RPM disks from the source VM to the recovery VM. The PostgreSQL disk will have the size of 150GB and the RPM disk will have the size of 10GB.
9. Run the `vgs` command, which should display the `vgdata` and `vgapp` volume groups.
10. In the `/etc/fstab` file, uncomment the lines that contain the word `vgdata` or `vgapp` that we had commented out in step 2.
11. Reboot your recovery VM.
12. Truncate the `envc` and `cascade` tables using the following command:
 

```
psql -U cyberpgsql -d das -c "truncate envc cascade;"
```
13. Update the cluster table using the following shell script. You can also create a temporary shell script using the following contents and run the same. For example,
 

```
sh temp_script_for_cluster_table_updatation.sh: hardware_key=`csadm license --get-hkey`
current_hostname=`hostname`
#First findout the number of nodes available in cluster table
number_of_nodes_in_cluster_table=`psql -U cyberpgsql -d das -tAc "select COUNT(*)
from cluster;
if [ $number_of_nodes_in_cluster_table -eq 1 ]; then
    # Only single node is available in cluster, hence directly update the nodeid.
    psql -U cyberpgsql -d das -c "UPDATE cluster SET nodeid='${hardware_key}';"
    csadm ha set-node-name $current_hostname
elif [ $number_of_nodes_in_cluster_table -gt 1 ]; then
    # More than one node is available. Now update the nodeid where nodename in
    cluster table matches with current hostname
    psql -U cyberpgsql -d das -c "UPDATE cluster SET nodeid='${hardware_key}'
where nodename='${current_hostname}';"
else
    echo "Not able to update the cluster table"
fi
```
14. Change the *rabbitmq* password using the following commands:
 

```
systemctl start rabbitmq-server
rabbitmq_password=`grep "cyops.rabbitmq.password"
/opt/cyops/configs/rabbitmq/rabbitmq_users.conf | cut -d"=" -f2`
rabbitmqctl change_password cyops $rabbitmq_password
```
15. Change the *elasticsearch* password using the following commands:
 

```
elasticsearch_password=`csadm license --get-hkey`

printf $elasticsearch_password | /usr/share/elasticsearch/bin/elasticsearch-
keystore add "bootstrap.password" -f
elasticsearch_password=`/opt/cyops-auth/.env/bin/python
/opt/cyops/scripts/manage_passwords.py --encrypt $elasticsearch_password`

/opt/cyops-auth/.env/bin/python /opt/cyops/scripts/confUtil.py -f
/opt/cyops/configs/database/db_config.yml -k "secret" -v $elasticsearch_password
```
16. Clear the API cache using the following commands. If any command fails, rerun that command:
 

```
systemctl start php-fpm
rm -rf /opt/cyops-api/var/cache/prod/
cd /opt/cyops-api
"sudo -u nginx php bin/console cache:clear --env=prod --no-interaction"
```
17. Refresh the keys using the following command:
 

```
csadm certs --skip-hmac
```

- 18.** Update the system using the following command:

```
cd /opt/cyops-api/  
sudo -u nginx php bin/console cybersponse:system:update -la --env=prod --force
```

- 19.** For FortiSOAR release 7.2.0 onwards:

Change the hostname using the following command:

```
sudo csadm hostname --set <source-machine-hostname>
```

For FortiSOAR releases prior to 7.2.0:

Restart the services using the following command:

```
sudo csadm services --restart
```

- 20.** Reindex elasticsearch using the following command:

```
sudo -u nginx php /opt/cyops-api/bin/console cybersponse:elastic:create --env=prod
```

- 21.** (Optional) If you do not remember the FortiSOAR UI password of your source instance and want to reset it to the default, which is 'changeme' for non-AWS instances and the 'instance\_id' for AWS instances, run the following command:

```
/opt/cyops-auth/.env/bin/python -c "import sys; sys.path.append(\"/opt/cyops-auth\"); import utilities.reset_user as reset_user; reset_user.start()"
```

- 22.** Redeploy your FortiSOAR license.

For the embedded Secure Message Exchange, do the following:

- 1.** Delete the existing embedded Secure Message Exchange using the following command:

```
/opt/cyops/scripts/api_caller.py --method DELETE --endpoint  
https://localhost/api/3/routers/52c5cee8-5c28-4ed2-a886-ec8bf4dc5993
```

- 2.** Enable the embedded Secure Message Exchange again using the following command:

```
sudo csadm secure-message-exchange enable
```

- 3.** Reconfigure all your FSR agents. For information on FSR agents, see the *Segmented Network Support* chapter in the "Administration Guide."

# Deploying FortiSOAR using offline repositories

This chapter describes the steps that you need to follow to deploy FortiSOAR using offline repositories.

## Prerequisites

- Virtual machine with CentOS 7.0.0 or RHEL 7.0.0 with minimal install option.
- Access to [repo.fortisoar.fortinet.com](https://repo.fortisoar.fortinet.com).
- Minimum disk size: 500 GB.
- Ensure that the SSL certificates that you are using for the offline repository are authorized by a Certificate Authority (CA). If however, you are using custom certificates such as open-source certificates, then you must ensure that you add these SSL certificates to the truststore of FortiSOAR and offline repository using the following command:

```
cp <SSL_certificate>.cert /etc/pki/ca-trust/source/anchors/
update-ca-trust extract
```

## Setting up the Offline Repository

1. To ensure that your ssh session does not timeout, run the `screen` command:

```
[root@localhost ~]# screen -S repo
```

2. Download `setup-fsr-offline-yum-repo.bin`:

```
wget --no-check-certificate
https://repo.fortisoar.fortinet.com/7.2.2/setup-fsr-offline-yum-repo.bin
```

3. Run the `setup-fsr-offline-yum-repo.bin` file as follows, where the `release_version` is FortiSOAR version that you want to synchronize:

```
[root@localhost ~]# sh /root/setup-fsr-offline-yum-repo.bin --release_version
<release_version>
```

For example, to synchronize FortiSOAR version 7.2.2 use the following command:

```
[root@localhost ~]# sh /root/setup-fsr-offline-yum-repo.bin --release_version 7.2.2
```

**Note:** This script file creates a user whose ID and password are set to `yum`. This ID is used to assign ownership to the content in the `'/repos'` directory.

4. Check the default server certificate and server private key in the `/etc/httpd/conf.d/ssl.conf` file, and if required they should be replaced.

```
# Section Server Certificate
SSLCertificateFile "/<path_to_cert>/<ssl_Certificate>.cert"
# Section Server Private Key
SSLCertificateKeyFile "/<path_to_cert>/<ssl_Certificate>.key"
```

```
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/localhost.crt

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

After you have updated the certificates, restart the 'httpd' service:

```
[root@localhost ~]# systemctl restart httpd
```

5. The `setup-fsr-offline-yum-repo.bin` script file synchronizes the repo. Therefore, if you want to resynchronize the repo, you must rerun the script. If you do not want to rerun the script manually, you can set up a cron job to perform this task. Use the following script to set up a cron job that will run daily at 00:00 hrs and synchronize the offline repo with the prod repo:

```
#!/bin/sh
#write out current crontab
crontab -l > mycron
#echo new cron into cron file
echo "0 0 * * * sh /root/setup-fsr-offline-yum-repo.bin --release_version 7.2.2" >> mycron
#install new cron file
crontab mycron
rm mycron
```

**Note:** You can change the time of running the cron job as per your convenience.

## Deploying FortiSOAR using the Offline Repository

1. Ensure that the offline repository host is accessible from the FortiSOAR appliance and ensure that your ssh session does not timeout, run the `screen` command:  

```
[root@localhost ~]# screen -S repo
```
2. From version 7.0.2 onwards, if you are using your private repository to install or upgrade FortiSOAR, then use the following command to export the "custom\_yum\_url" variable before running the fresh install or upgrade script:  

```
export custom_yum_url=<"custom_yum_url_name">
```

For example, `export custom_yum_url="offline-repo.fortisoar.in"`
3. Download the installer for FortiSOAR 7.2.2 using the following command:  

```
[root@localhost ~]# wget https://<offline_repo>/7.2.2/install-fortisoar-7.2.2.bin
```
4. To install FortiSOAR 7.2.2, run the following command as a *root* user:  

```
[root@localhost ~]# sh install-fortisoar-7.2.2.bin
```

If you have not deployed an SSL certificate on your offline repo or you have a self-signed certificate deployed on your offline repo, then run the following command on plain CentOS, to ignore the SSL check while installing FortiSOAR:  

```
[root@localhost ~]# sh install-fortisoar-7.2.2.bin ignore-ssl-check
```
5. Login as the 'csadmin' user to the FortiSOAR CLI and continue to configure FortiSOAR or Secure Message Exchange (SME) and add your FortiSOAR license. For more information, see the [Deploying FortiSOAR](#) chapter.  
**Note:** You can add self-signed CA certificates in OS as a trusted certificate using the steps mentioned in the

Adding self-signed CA certificates in Centos as trusted certificates topic in the [Additional Configurations](#) chapter.

## Upgrading FortiSOAR using the Offline Repository

1. Ensure that the offline repository host is accessible from the FortiSOAR appliance and ensure that your ssh session does not timeout, run the `screen` command:  

```
[root@localhost ~]# screen -S repo
```
2. From version 7.0.2 onward, if you are using your private repository to install or upgrade FortiSOAR, then use the following command to export the "custom\_yum\_url" variable before running the fresh install or upgrade script:  

```
export custom_yum_url=<"custom_yum_url_name">
```
3. Download the upgrade installer for FortiSOAR 7.2.2 using the following command:  

```
[root@localhost ~]# wget https://<offline_repo>/7.2.2/upgrade-fortisoar-7.2.2.bin
```
4. To upgrade to FortiSOAR 7.2.2, run the following command as a `root` user:  

```
[root@localhost ~]# sh upgrade-fortisoar-7.2.2.bin
```

If you have not deployed an SSL certificate on your offline repo or you have a self-signed certificate deployed on your offline repo, then run the following command on plain CentOS, to ignore the SSL check while upgrading FortiSOAR:

```
[root@localhost ~]# sh upgrade-fortisoar-7.2.2.bin --ignore-ssl-check
```

## Troubleshooting

### Peer Certificate issue not recognized error

If you have not deployed an SSL certificate on your offline repo or you have a self-signed certificate deployed on your offline repo, then run the following command on plain CentOS if you are installing version 7.2.2:

```
# sh install-fortisoar-7.2.2.bin ignore-ssl-check
```

If you are upgrading to version 7.2.2, then use the following command:

```
# sh upgrade-fortisoar-7.2.2.bin --ignore-ssl-check
```

This command ignores the SSL check while installing FortiSOAR. However, you can get the following error while installing FortiSOAR on plain CentOS:

```
"[Errno 14] curl#60 - "Peer's Certificate issuer is not recognized."
```

#### Resolution

Add the `sslverify=false` entry in the `/etc/yum.conf` file on the plain CentOS system, and then restart the installation.

# Licensing FortiSOAR

From version 6.4.0 onwards, FortiSOAR integrates with FortiGuard Distribution Network (FDN) to retrieve updated contract details.



You must be connected to FDN while you are deploying your license. If there is no connectivity to FDN, then your FortiSOAR UI access will be blocked after some hours. If any error occurs while deploying your license, see the [Troubleshooting licensing issues](#) section for some tips on how to resolve the issue.

---

FortiSOAR enforces licensing and restricts the usage of FortiSOAR by specifying the following:

- The maximum number of active users in FortiSOAR at any point in time.
- The type and edition of the license.
- The expiration date of the license.

For a fresh install of FortiSOAR, see [FortiSOAR licensing process](#). To retrieve your Device UUID, see [Retrieving the FortiSOAR Device UUID](#).

## FortiSOAR licensing process

1. You must have an account in FortiCare.
2. Contact FortiSOAR Support to obtain FortiSOAR product SKU. You will require to provide the following information to be able to get the license for FortiSOAR™:
  - The license type that you want for FortiSOAR. For information on the different license types, see [License Manager Page](#).
  - The license edition that you want for FortiSOAR. For information on the different license editions, see [License Manager Page](#).
  - The number of licensed users required for FortiSOAR.

Once you complete purchasing FortiSOAR, you will be sent a service contract registration code to your registered email address.

If a customer wants additional users, then the customer has to also register the contract for additional users. A separate registration code will be sent for the contract of additional users.

**Note:** If you have opted for a "Perpetual" or "Evaluation" license, you should download the license file only after the additional user contract, if any, is registered.
3. Login to your FortiCare account and click **Asset > Register/Activate** to register your FortiSOAR product. You can register your FortiSOAR product using the instructions provided in the FortiCare registration wizard. You will require to copy-paste the service contract registration code from your email to register FortiSOAR. Once you have verified the registration, click **Complete** to complete the registration.
4. Once you click **Complete** you are taken to the **Product Information** page. To generate the license file, click **Edit** on the [Product Information](#) page.  
 On the [Edit Product Information](#) page, in the **UUID** field, enter the Device UUID of your FortiSOAR installation and click **Save**.  
**Important:** The license issued against one device UUID can later be used on another FortiSOAR virtual machine with a difference device UUID, as well in case of disaster recovery (DR). However, the same license cannot be active simultaneously on more than one node.  
 To retrieve your Device UUID, see [Retrieving the FortiSOAR Device UUID](#).  
 The license file is generated after you enter the Device UUID. You can now download and deploy the FortiSOAR license, using the steps mentioned in [Deploying the FortiSOAR license](#).

If you are an existing customer, then your entitlements would have already been imported into FortiCare and you would have received an email with respect to your FortiCare account. Also, your FortiSOAR product would already have been registered. However, you do require to update your Device UUID.

To update your Device UUID, do the following:

1. Login to your FortiCare account and click **Asset > Manage/View Products > Basic View**.
2. Click the row that contains the FortiSOAR (FSR) product to view the [Product Information](#) page.
3. On the [Edit Product Information](#) page, in the **UUID** field, enter the Device UUID of your FortiSOAR installation and click **Save**.  
**Important:** The license issued against one device UUID can later be used on another FortiSOAR virtual machine with a difference device UUID, as well in case of disaster recovery (DR). However, the same license cannot be active simultaneously on more than one node.  
 To retrieve your Device UUID, see [Retrieving the FortiSOAR Device UUID](#).  
 The license file is generated after you enter the Device UUID. You can now download and deploy the FortiSOAR license, using the steps mentioned in [Deploying the FortiSOAR license](#).

## FortiSOAR licensing using FortiManager

A closed or air-gapped environment is an environment where FortiSOAR does not have access to the internet and therefore cannot access the FDN servers. In such cases, FortiManager (FMG) can be used as an intermediary so that FMG provides license validation and FDN updates to FortiSOAR with limited or no internet connectivity. You can configure FMG for the following environments:

- Complete air-gapped environment where FMG also does not have connectivity to FortiGuard Distribution Servers (FDS) and manual synchronization is required for customer entitlements.
- FMG has network connectivity to FDS servers and can automatically synchronize customer entitlements. For more details on FMG and troubleshooting information, see the [FortiManager](#) documentation.

### Process to deploy the FortiSOAR license when you are in a complete air-gapped environment

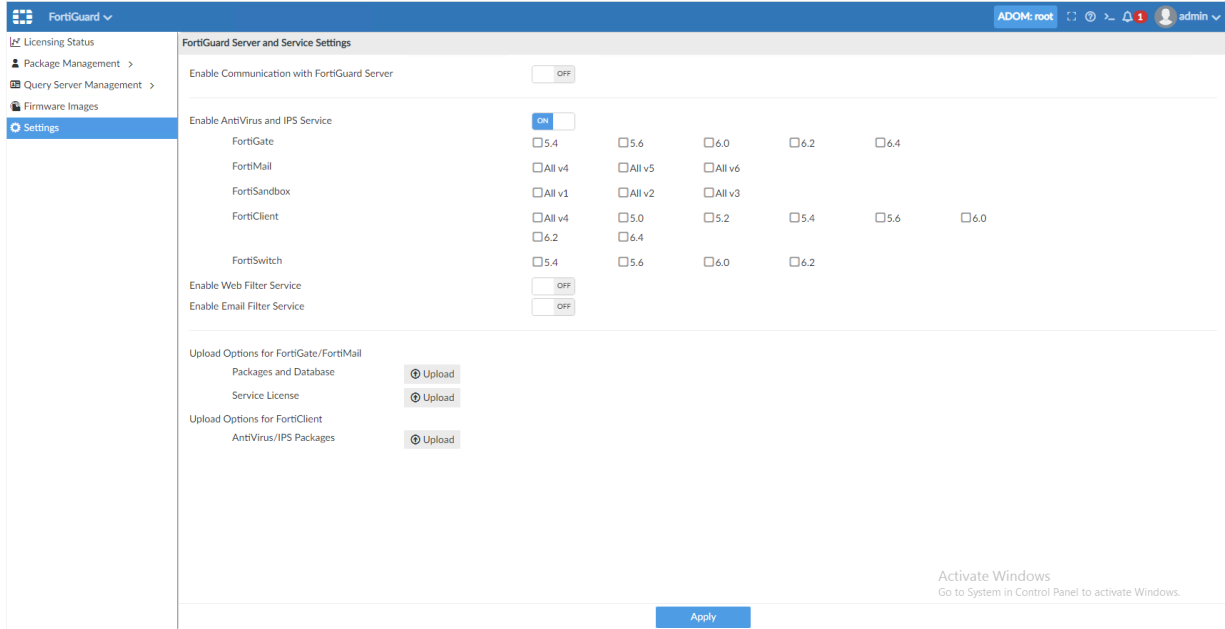
1. You must have an account in FortiManager (FMG).
2. Contact FortiSOAR Customer Support to obtain an entitlement file, which contains all the contract details.
3. Log onto FMG and navigate to FortiGuard.
4. Select the **FortiGate Updates** checkbox for the NIC that is active on FMG, as shown in the following image:

The screenshot shows the 'Edit Network Interface' configuration page in FortiManager. The interface is titled 'Edit Network Interface' at the top. The configuration fields are as follows:

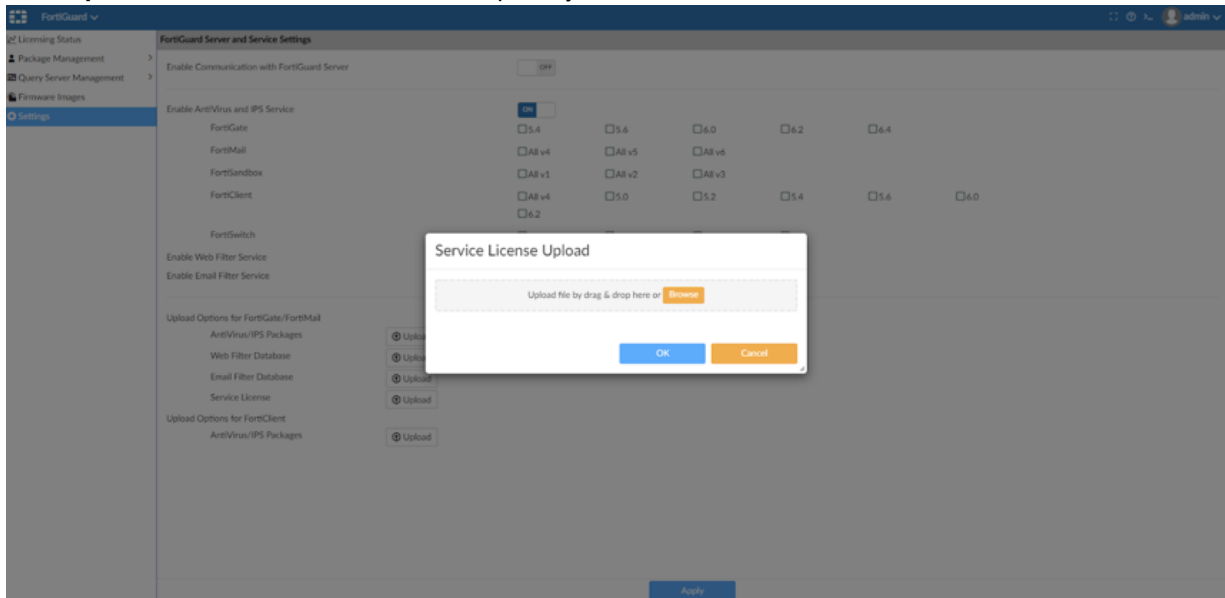
- Name:** port2
- Alias:** Private\_Network
- IP Address/Netmask:** 192.168.80.11/255.255.255.0
- IPv6 Address:** ::/0
- Administrative Access:**
  - ☒ HTTPS ☐ HTTP ☐ PING ☒ SSH ☐ SNMP
  - ☐ Web Service
- IPv6 Administrative Access:**
  - ☐ HTTPS ☐ HTTP ☐ PING ☐ SSH ☐ SNMP
  - ☐ Web Service
- Service Access:**
  - ☒ FortiGate Updates (highlighted with a red box)
- Bind to IP Address:** 0.0.0.0/0.0.0.0 (with an information icon)
- Web Filtering:** ☐
- Status:** Enable (selected) Disable

5. On the left-menu, click **Settings**, and apply the following settings:

a. "Toggle OFF" the **Enable Communication with FortiGuard Server** setting.



b. Click **Upload** beside **Service License** and upload your entitlement file, and then click **OK**.



c. Click **Apply** to apply the above settings.

6. Ensure that FMG is reachable or resolvable from your FortiSOAR instance.

7. Modify your FortiSOAR config to connect to FMG by adding the following entry in the `/opt/cyops-auth/utilities/das.ini` file:

```
[FDN]
host = https://<FMG Hostname>:8890
```

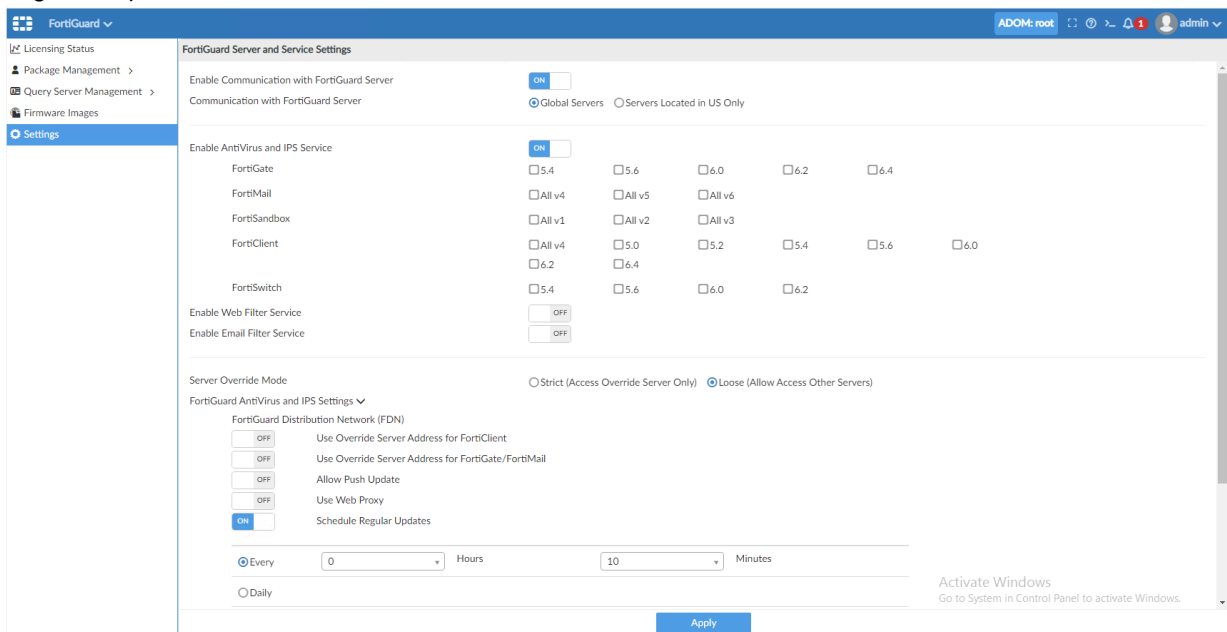
8. Restart the `cyops-auth` service.

9. Deploy your FortiSOAR license using the steps mentioned in [Deploying the FortiSOAR license](#).

## Process to deploy the FortiSOAR license when you are not in a complete air-gapped environment

You might choose to deploy the license using FMG even if you are not in an air-gapped environment. In such cases do the following:

1. You must have an account in FortiManager (FMG).
2. Contact FortiSOAR Customer Support to obtain an entitlement file, which contains all the contract details.
3. Log onto FMG and navigate to FortiGuard.
4. On the left-menu, click **Settings**, and apply the following settings:
  - a. "Toggle ON" the **Enable Communication with FortiGuard Server** setting.
  - b. For the **Communication with FortiGuard Server** settings, select **Global Servers**.
  - c. For the **Server Override Mode** settings, select **Loose (Allow Access Other Servers)**.
  - d. Expand "FortiGuard AntiVirus and IPS Setting", and "Turn ON" the **Schedule Regular Updates** setting.
 Once you turn on the Schedule Regular Updates settings, you need to define the frequency at which you want to get the updates:



- e. Click **Apply** to apply the above settings.
5. Ensure that FMG is reachable or resolvable from your FortiSOAR instance and ensure that FMG has access to the Internet.
6. Modify your FortiSOAR config to connect to FMG by adding the following entry in the `/opt/cyops-auth/utilities/das.ini` file:
 

```
[FDN]
host = https://<FMG Hostname>:8890
```
7. Restart the `cyops-auth` service.
8. Deploy your FortiSOAR license using the steps mentioned in [Deploying the FortiSOAR license](#).
 

**Important:** In case of a non-closed environment, license deployment from FortiSOAR does not work at the first attempt since FMG is unable to send contracts that are required for license deployment. Therefore, users need to retry deploying the license on the FortiSOAR environment. This happens only when FMG is not a part of the air-gapped environment.

## Retrieving the FortiSOAR Device UUID

Your FortiSOAR installation generates a Device UUID for your installation. This key is used to identify each unique FortiSOAR environment.

When you provision a new instance, a configuration wizard runs automatically on the first `ssh` login by the `csadmin` user. This wizard automatically generates your Device UUID and saves the Device UUID in the `/home/csadmin/device_uuid` file from which you can retrieve your device UUID. For more information, see the *FortiSOAR Configuration Wizard* topic. However, if you require the device UUID in the future, you can use the FortiSOAR Admin CLI (`csadm`) or from the see [License Manager Page](#).

You can retrieve the FortiSOAR Device UUID using `csadm`. A `root` user can directly run the `csadm license --get-device-uuid` command to print the Device UUID on the CLI. For more information on the FortiSOAR Admin CLI, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."

## Deploying the FortiSOAR license



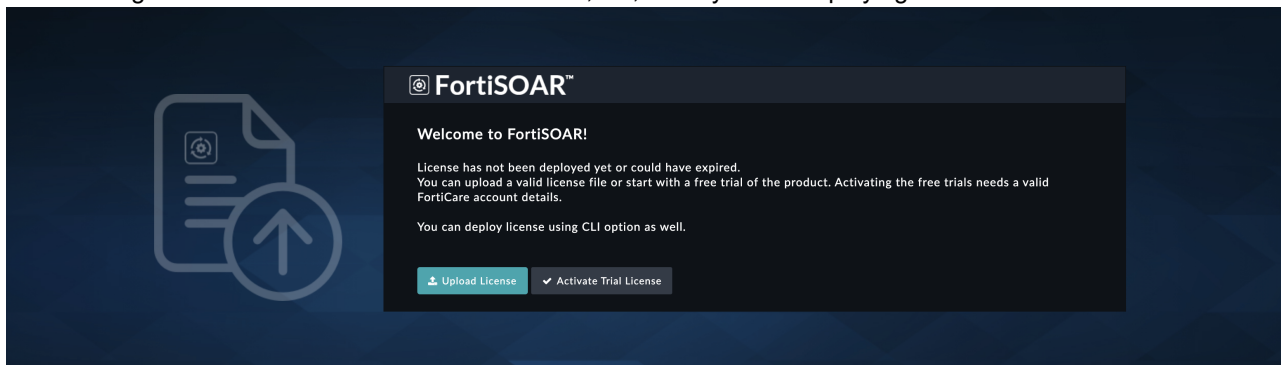
Before you start deploying your FortiSOAR license, you must ensure that you can connect to <https://globalupdate.fortinet.net>, else the license deployment will fail. Connectivity to this address is required for fetching the license entitlements and product functioning post-upgrade.

## Deploying the FortiSOAR license using the FortiSOAR UI

From version 7.0.0 onwards, you can deploy your FortiSOAR license from the FortiSOAR UI itself, without the need to SSH to your FortiSOAR machine. This is extremely useful if the administration does not have `ssh` access to the FortiSOAR machine.

To deploy the initial FortiSOAR license or to upload a new license, if your FortiSOAR license has expired, you can use the FortiSOAR login screen and do the following:

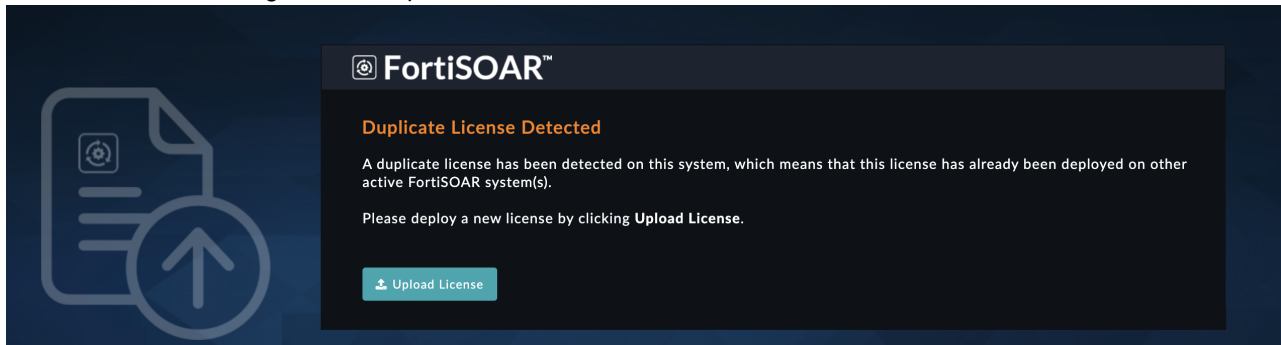
1. In the browser type `https://<YourFortisoarHostname>/login` to open your FortiSOAR UI. This will display the following screen in the case of a fresh installation, i.e., when you are deploying an initial FortiSOAR license:



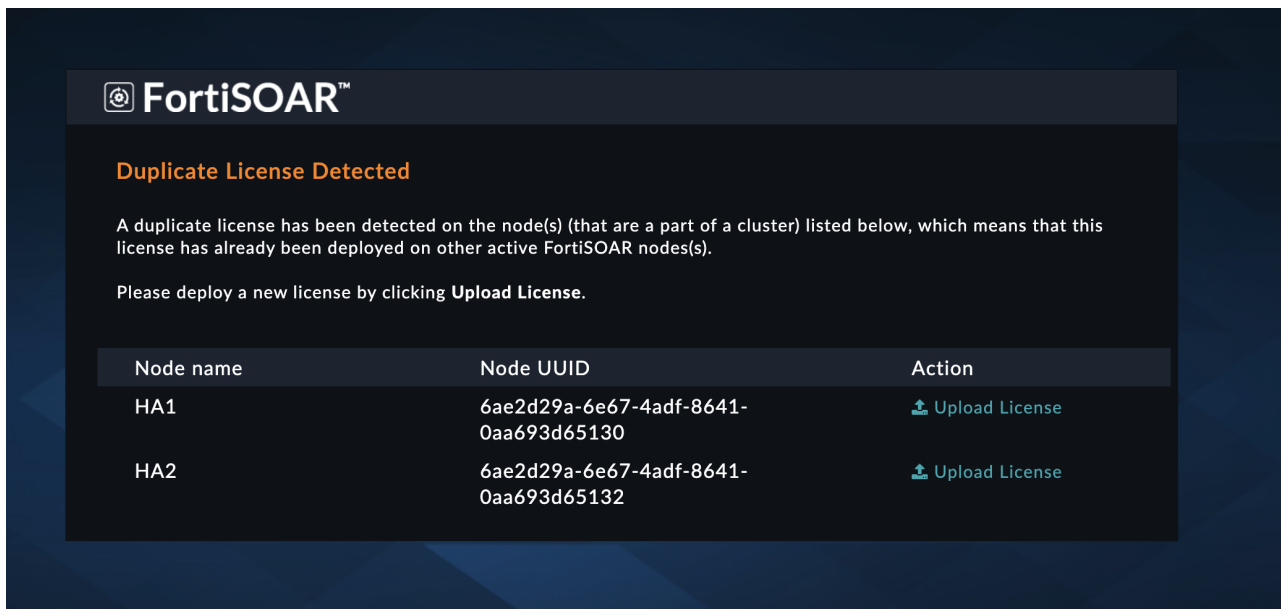
**Note:** In case your FortiSOAR license has expired, then you will see only the Upload License button and not the Activate Trial License button.

From version 7.0.2 onwards, if FortiSOAR detects that a duplicate license has been deployed on the current node, i.e., the same license has already been deployed on another active FortiSOAR node, then you can click **Upload**

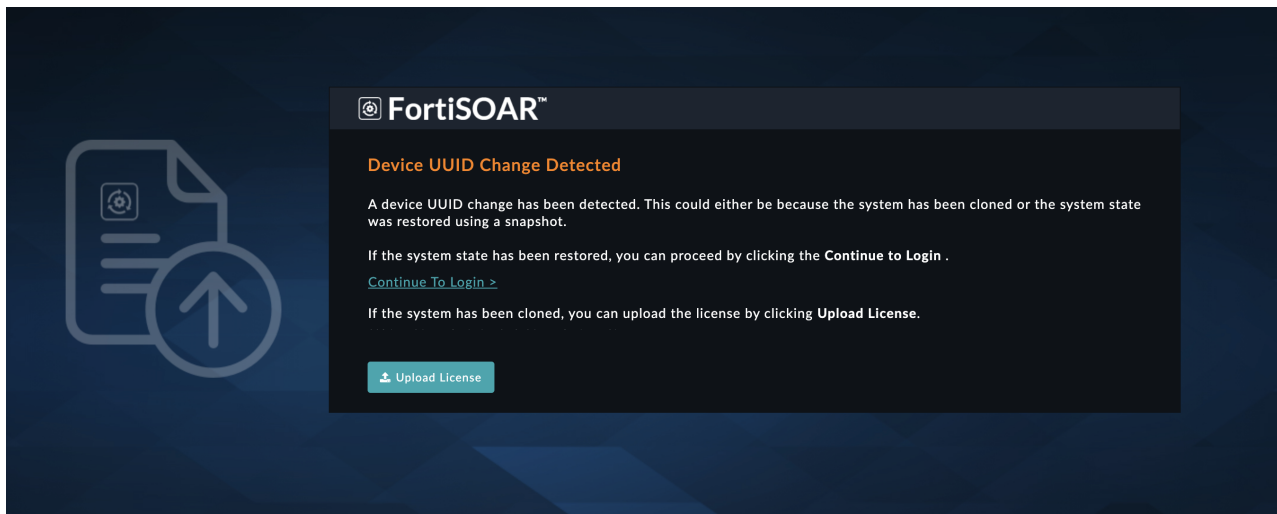
**License** on the following screen to upload a new license on one of the two nodes:



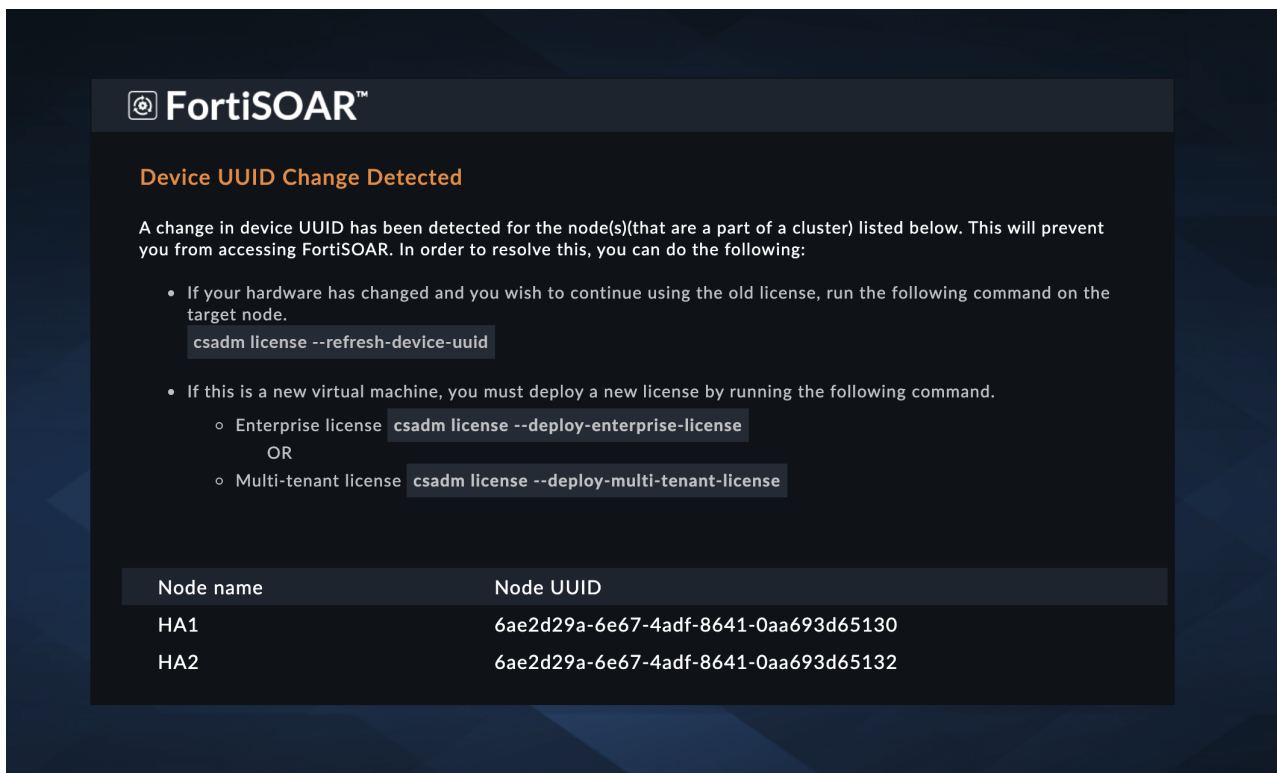
If FortiSOAR detects that a duplicate license has been deployed in an HA cluster, i.e., the same license has already been deployed on another active FortiSOAR node in the HA cluster, then you can click **Upload License** in the row of any of the nodes in the HA cluster as shown in the following screen to upload a new license on one of the two nodes:



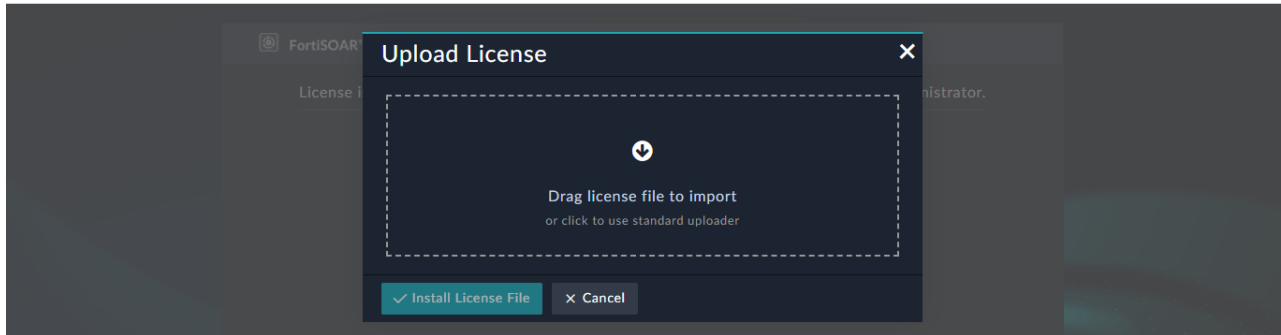
From version 7.0.2 onwards, if FortiSOAR detects a 'Device UUID change', generally due to restoring a snapshot of a FortiSOAR instance, or cloning of a FortiSOAR instance. In case a snapshot is restored on the instance, you can continue to log in by clicking **Continue to Login**. In case of a cloned instance, click **Upload License** to upload a new valid license:



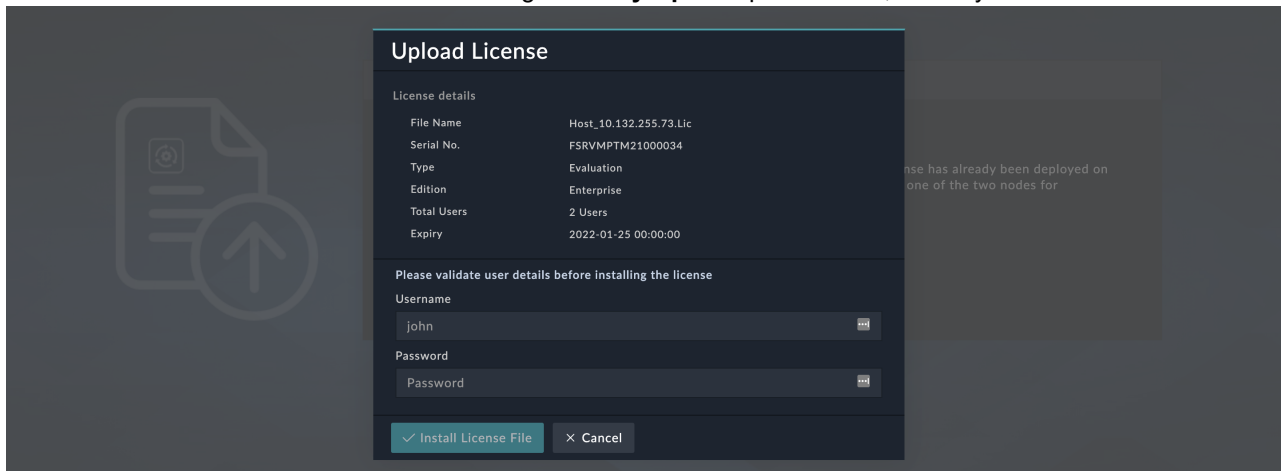
If FortiSOAR detects a 'Device UUID change' for node(s) that are part of an HA cluster, it will list the nodes on which the device UUID changes is detected. In the case of a hardware change, and if you want to continue using the old license, you can run the `csadm license --refresh-device-uuid` command on the specific node of the HA cluster, and then continue to log in to the system. In the case of new virtual machine, you can run the `csadm license --deploy-enterprise-license` (for enterprise systems) or the `csadm license --deploy-multi-tenant-license` command (for MSSP systems) to deploy the new valid license for the specific node of the HA cluster:



- Click **Upload License** to display the following "Upload License" dialog, In case you are deploying the license for the first time:



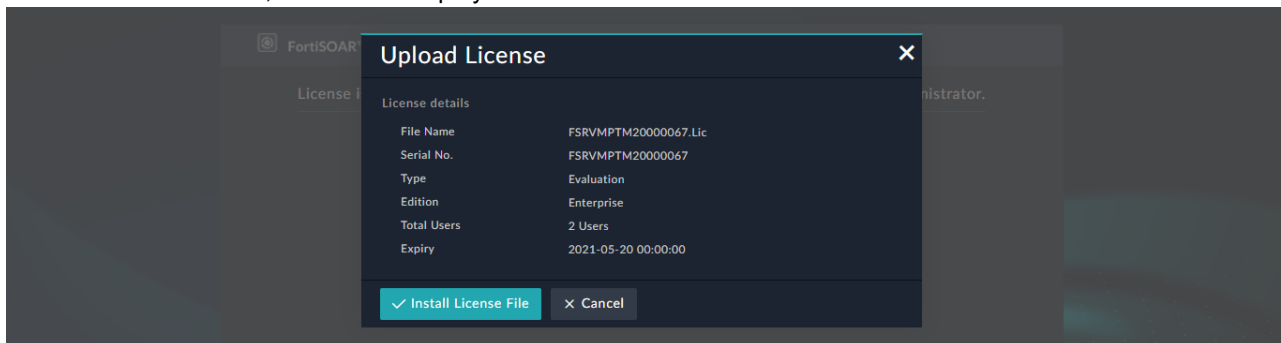
In case you are deploying a new license after the expiration of your FortiSOAR license, in the case of duplicate license detection, or in the case of deploying a new license for a new virtual machine, you also need to provide valid credentials of a FortiSOAR administrator having '**Security Update**' permissions, before you can install the license:



3. Drag and drop your FortiSOAR License file, or click the **Upload** icon and browse to the license file and import your FortiSOAR license.

If the license file is invalid, FortiSOAR displays an error message and the license is not installed.

If the license file is valid, FortiSOAR displays the license details:



4. Click **Install License File** to install your FortiSOAR license. Once the license is successfully installed, FortiSOAR displays a License imported successfully message and the EULA is displayed. Once you accept the EULA, you can log on to the FortiSOAR UI and begin configuring the system.

## Deploying the FortiSOAR license using the FortiSOAR Admin CLI



Ensure that you have copied the FortiSOAR license file, using SCP or other methods, to your FortiSOAR VM. **Do not copy** the contents of the license file and paste it into a new file; this will cause license validation to fail.

You can deploy the FortiSOAR license using the FortiSOAR Admin CLI. A `root` user can directly run the `csadm license --deploy-enterprise-license <License File Path>` command. For example, `csadm license --deploy-enterprise-license temp/<Serial_No>.lic`.

If your license is enabled for multitenancy, then run the `csadm license --deploy-multi-tenant-license <License File Path>` command. For more information on `csadm`, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."

The license path that you provide can either be relative to the current working directory or can be an absolute path. Once you have entered the license path, the `csadm` checks the license file for validity and whether you have selected the appropriate license type (enabled or not enabled for multi-tenancy).

When you deploy a license on FortiSOAR the license entitlements are fetched from FDN.

**Note:** If you deploy a license that does not match with the system UUID, then you will get a warning on CLI while deploying license. If you deploy the same license in more than one environment then the license is detected as duplicate and you require to correct the license, else your FortiSOAR UI will be blocked in 2 hours.

The FortiSOAR Admin CLI displays a `Success` message, if your license file is deployed successfully, or an `Error` message that contains the reason for the failure.

Once your system is licensed, you can log on to the FortiSOAR UI and begin configuring the system.

## Activating the FortiCare Trial license for FortiSOAR

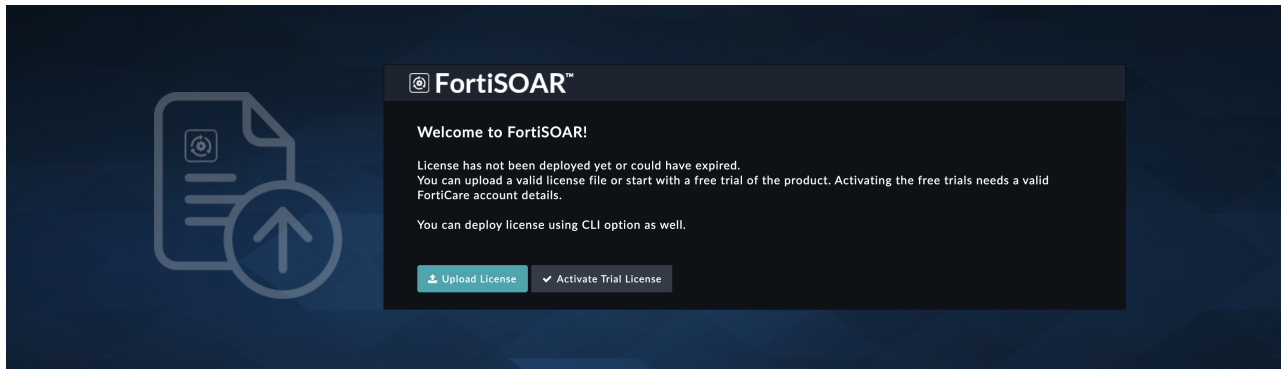
From version 7.0.0 onwards, you get a free trial license for an unlimited time for FortiSOAR per FortiCare account, i.e., if you have a FortiCare account, you can get FortiSOAR for free and for an unlimited time, but in a limited context. This license is an "Enterprise" type license and is restricted to 3 users using FortiSOAR for a maximum of 200 actions a day.



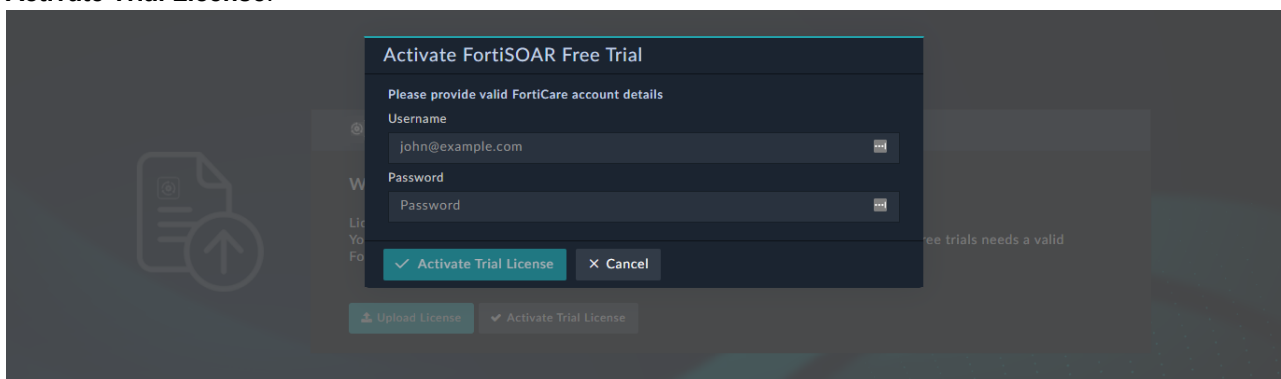
Important steps such as "Create Records", "Update Records", "Find Records", "Connection Actions", etc., are counted towards the maximum action count limit of 200. However, steps used for data manipulation such as "Wait", "Approval", "Loops", "Reference a Playbook", etc. are not counted towards the action count restriction.

To activate the FortiCare trial license for FortiSOAR, do the following:

1. In the browser type `https://<YourFortisoarHostname>/login` to open your FortiSOAR UI. This will display the following screen:



2. Click **Activate Trial License**.
3. In the Activate FortiSOAR Free Trial dialog, enter your FortiCare username (email address) and password and click **Activate Trial License**.



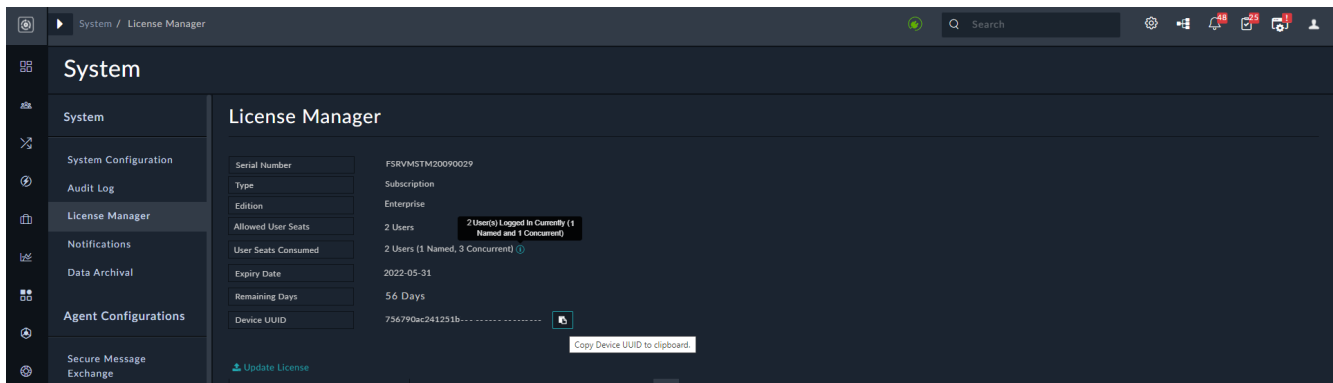
If the email address and password provided are correct, then your FortiCare trial license for FortiSOAR is activated.

You can always update this trial license into a full-fledged production license at any time, by purchasing a FortiSOAR license and then updating it using either the FortiSOAR CLI or UI.

## License Manager Page

In release 7.0.1, FortiSOAR introduced the concept of 'Concurrent User Seats', thereby supporting both 'Named' and 'Concurrent' users. Concurrent user seats enable sharing of a fixed number of user seats among unlimited number of users restricted by the number of users simultaneously accessing FortiSOAR. This particularly is useful for a shift-oriented SOC environment where, for example, a 30-member team only has 10 members working in a given shift and therefore, in this scenario, administrators can create 10 concurrent users and re-use the seats across all shifts effectively. For more information, see the [User Seat Support in FortiSOAR](#) section.

Click **Settings > License Manager** to open the `License Manager` page as shown in the following image:



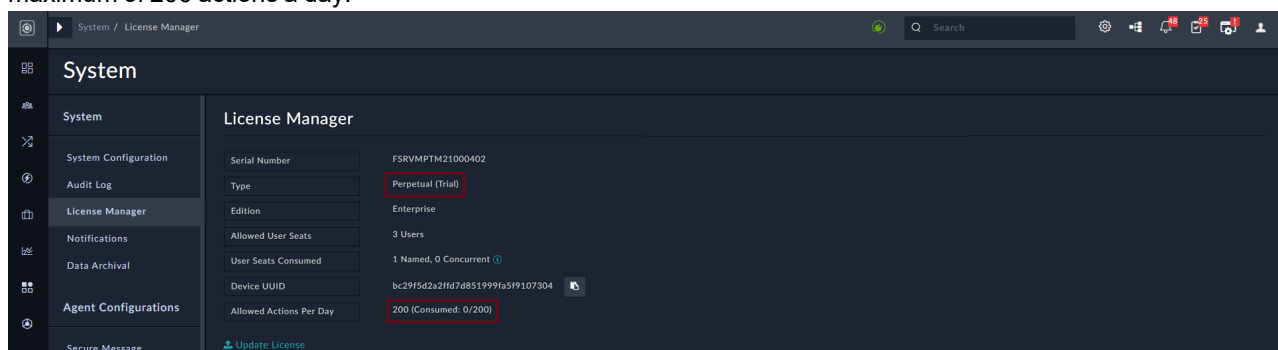
The **License Manager** page displays the serial number, type and edition of the license issued, the total number of users FortiSOAR is licensed for, the number of users created on the system per access type, the number of users who are currently logged into FortiSOAR, the date when the FortiSOAR license will expire, the number of days till the expiry of the FortiSOAR license, and your Device UUID. You can click the **Copy Device UUID** button to copy your Device UUID.

If your license is about to expire, you can update your license by clicking **Update License** and either dragging-and-dropping your updated license or by clicking and browsing to the location where your license file is located, then select the file and click **Open**. Now, if the user count is reduced in updated license and if the logged in users are more than the new count then the logged in users will get logged out at the time of session refresh one by one till the count becomes equal or less. Similarly, If the 'Named' user count in the system is more than the new user count in license, then no named user *apart* from the 'Super Admin' user will be able to log into system. For more information about named users, see the [User Seat Support in FortiSOAR](#) section. For more information about a 'Super Admin' user, see the *Security Management* chapter in the "Administration Guide."

**Serial Number:** The serial number is a unique ID that is created by the FortiCare portal when you register your FortiSOAR product.

The FortiSOAR license can be of the following types:

- **Perpetual:** This type of license provides you with a license for an unlimited time for FortiSOAR.
- **Perpetual (Trial):** This type of license provides you with a free trial license an unlimited time for FortiSOAR, but in a limited context, i.e., with restrictions on the number of users and actions that can be performed in FortiSOAR in a day. By default, this license is an "Enterprise" type license and is restricted to 3 users using FortiSOAR for a maximum of 200 actions a day.



For more information on the trial license, see the [Activating the FortiCare Trial license for FortiSOAR](#) topic.

- **Subscription:** This type of license is a regular license that gives you subscription to FortiSOAR for a particular number of users and a specific timeframe. You can renew your subscription and change the number of users as per your requirements. FortiSOAR will synchronize with the FDN server and retrieve the latest subscription.

- **Evaluation:** This type of license allows you to evaluate FortiSOAR. The evaluation license is shipped with a predefined user count and expiry date.

The FortiSOAR license can have the following editions:

- **Enterprise:** This edition enables a regular "enterprise" production license.
- **MT :** This edition enables multi-tenancy; both shared and distributed multi-tenancy are supported. The instance where this license is deployed would serve as a "master" node in a distributed deployment. For more information of what multi-tenancy is and what master nodes are, see the "Multi-tenancy support in FortiSOAR Guide."
- **MT\_Tenant:** This edition enables the node as a tenant in a multi-tenant deployment. This is the license to be deployed for a "customer" node of a Managed Security Services Provider (MSSP). The node can then be configured as a "tenant" to the MSSP server for syncing data and actions to and from the MSSP "master" server. The "MT\_Tenant" license has only one user.
- **MT\_RegionalSOC:** This edition enables the node as a "Regional SOC" deployment at an organization having a distributed SOC. It is enabled as a complete SOAR platform by the regional SOC team. At the same time, it can be configured as "tenants" to the global SOC where the "MT" license is deployed and sync data and actions from the Global SOC FortiSOAR server.

**Allowed User Seats** displays the number of user seats that you have purchased for FortiSOAR. You cannot create more named active users, in your FortiSOAR environment, than the value specified as in this field. For example, if the Allowed User Seats field is set to five, then you can create a maximum of five named users, and an unlimited number of concurrent users; however, if all five named users are active, then no concurrent user will be able to log into FortiSOAR. Also, note that if a user is logging in from multiple places, then it is counted as a single user. For more information, see the [User Seat Support in FortiSOAR](#) section.

**User Seats Consumed** displays the number of active users, named and concurrent, who have consumed the FortiSOAR user seats. To view the number of users, named and concurrent, who are currently logged into FortiSOAR, you can hover over the tooltip.

**Expiry Date** displays the date at which your FortiSOAR license will expire and **Remaining Days** displays the number of days left for your license to expire.

FortiSOAR version 6.4.4 and later does not mandate 'Additional Users' entitlement to be the same across all cluster nodes. User count entitlement will now always be validated from the primary node. The secondary nodes can have the basic two-user entitlement. The HA cluster shares the user count details from primary node of the cluster. Hence, all 'Concurrent Users' count restrictions apply as per the primary node. If a node leaves the cluster, the restriction will apply as per its own original license.

In case your FortiSOAR instance is part of a High Availability (HA) cluster, then the [License Manager](#) page also displays information about the nodes in the cluster, if you have added secondary node(s) as shown in the following image:

As shown in the above image, the primary node is Node 2 and that node is licensed with 7 users, therefore the Allowed User Seats count displays as 7 users. For more information on licensing of nodes in an HA cluster, see the *High Availability support in FortiSOAR* chapter in the "Administration Guide."

You can update the license for each node by clicking **Update License** and uploading the license for that node as described in the following section.



If you update a license that does not match with the system UUID, you will get a warning on UI while updating the license. If you update the same license in more than one environment then the license is detected duplicate and you require to correct the license, else your FortiSOAR UI will be blocked in 2 hours.

## User Seat Support in FortiSOAR

FortiSOAR supports 'Named' and 'Concurrent' users for licensing. User access details are used to calculate the number of concurrent users that can simultaneously log onto FortiSOAR.

### Named Users

'Named' users are users for whom a seat is permanently reserved, i.e., such a user can always log onto FortiSOAR except in case of a license violation.

### Concurrent Users

The ability to designate a user seat as a 'concurrent user seat' allows system administrators to create a floating seat that can be shared by unlimited users (only limited by the user seat limit). A 'Named' user has a FortiSOAR seat permanently reserved, i.e., such a user can always log onto FortiSOAR except in case of a license violation. However, a concurrent user can log in only when there is a concurrent seat available. Note that if a user is logging in from multiple places, it is counted as a single user.

For example, if you have purchased a five-user license, then a maximum of 5 named active users can be present in the system at a given time. However, there is no limit to concurrent user creation, i.e., you can create as many concurrent users as you want. Therefore, if out of five user seats that you have purchased, you have created two Named users, then those users can log into FortiSOAR at any time, and the other three seats are reserved for Concurrent users, who can log into FortiSOAR when concurrent seats are available. However, if the you create five Named users, then only those users will be able to log into FortiSOAR and Concurrent users will not be able to log into the system.

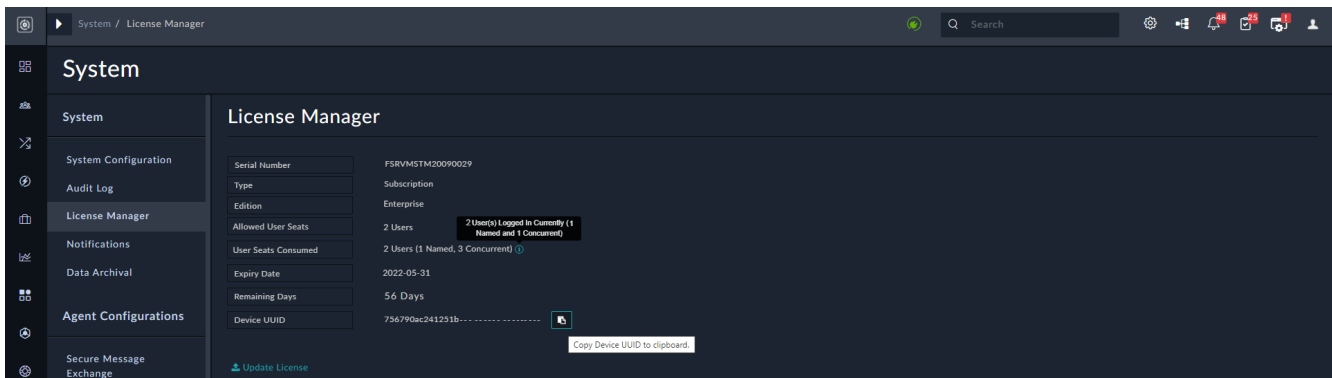


Administrators, i.e., users with `Security` and `People Update` access, can selectively change users' access type, i.e., Concurrent users to Named users, and vice-versa, at any time, or they can also bulk change users access type from Named to Concurrent. For more information, see the *Security Management* chapter in the "Administration Guide." They also have the privilege to forcefully log out selective 'Concurrent' users. When the administrators logs out a user from any instance, that user is notified before being logged out.

The default access type set for all SSO and MSSP users is 'Concurrent'. You can change the access type for the user later, if needed.

## Updating your license using the FortiSOAR UI

You can update your license using your FortiSOAR UI. Click **Settings > License Manager** to open the `License Manager` page.



You can use the `License Manager` page to view your license details and to update your license. FortiSOAR displays a message about the expiration of your license 15 days prior to the date your license is going to expire. If your license type is **Evaluation** or **Perpetual**, then you must update your license within 15 days, if you want to keep using FortiSOAR. To update your license, click **Update License** and either drag-and-drop your updated license or click and browse to the location where your license file is located, then select the file and click **Open**. If your license type is **Subscription**, you must renew your subscription.

## Troubleshooting licensing issues

FortiSOAR displays meaningful messages and troubleshooting tips during the license deployment process, and also validates your FortiSOAR license, making it easier for you to debug licensing issues, as shown in the following image:

```
[root@cybersponse csadmin]# csadm license --deploy-enterprise-license 5d15a571b69d1732e47eb5a439976987.lic
=====
License deployment may take few minutes, please do not stop the process..
=====
Validating license before deployment..
=====
FSR-Auth-026: License deployment failed. This license file is for Multi-Tenancy setups only. Refer documentation for exact steps to deploy this license or get in touch with customer support.
=====
[root@cybersponse csadmin]#
```

Also, note that if your connection to FDN is via a proxy, you must update the proxy settings.

If any error occurs while deploying your license, following are some troubleshooting steps:

- If the license type is "Subscription", then the number of users and expiry date are not present inside the license. They require to be synced from FDN after the installation. The "License has expired issue after installation" issue occurs due to the following two reasons:
  - Sync with FDN failed
  - Sync was successful but we got wrong contract information.  
To verify the above-mentioned cases run the following command: `java -jar <jar_path> <serial_no> <device_uuid> <globalupdate_url>`  
For example, `java -jar /opt/cyops-auth/bin/fdnclient.jar <serial_no> <device_uuid> https://globalupdate.fortinet.net`
- If the license type is "Evaluation" or "Perpetual", then the number of users and expiry date are present inside the license. If a license deployment failure occurs for these types of licenses, then check the license information using the `csadm license -show-details <lic_file>` command.
- After deploying the license if the system is yet not reachable, restart the `cyops-auth` service and then monitor the `fdn.log` and `das.log` files. If you continue to face issues, contact FortiSOAR support.

## Troubleshooting issues while deploying the FortiSOAR license in a proxy environment

You might get the following error, when you are deploying your FortiSOAR license in a proxy environment:

```
FSR-Auth-003: License Entitlement Sync Failed. Ensure that [https://globalupdate.fort]
(https://globalupdate.fort/) is accessible from your environment. If the issue still
persists, contact support."
```

This issue might occur due to some proxies doing the SSL decryption, which means that these proxies can intercept the https connection by modifying the peer certificate and changing the issuer of the certificate to itself. This can cause the license deployment or synchronization to fail as the new issuer is not trusted.

To identify this issue, check the PKIX path building failed error message in the `fdn.log` file:  
# `/var/log/cyops/cyops-auth/fdn.log` file

### Resolution

You can use the following two solutions to solve this issue.

**Method 1:** Do not use SSL decryption for `globalupdate.fortinet.net`.

**Method 2:** Import the proxy issuer certificate into truststore using the following command:

```
keytool -import -alias proxy_issuer_cert -keystore /opt/cyops-auth/certs/fdn_server_
truststore.p12 -file<cert_file> -storepass MXakK2bj6vAteC47 -noprompt
```

# Configuring FortiSOAR

This chapter describes the initial configuration steps required for setting up your FortiSOAR system.

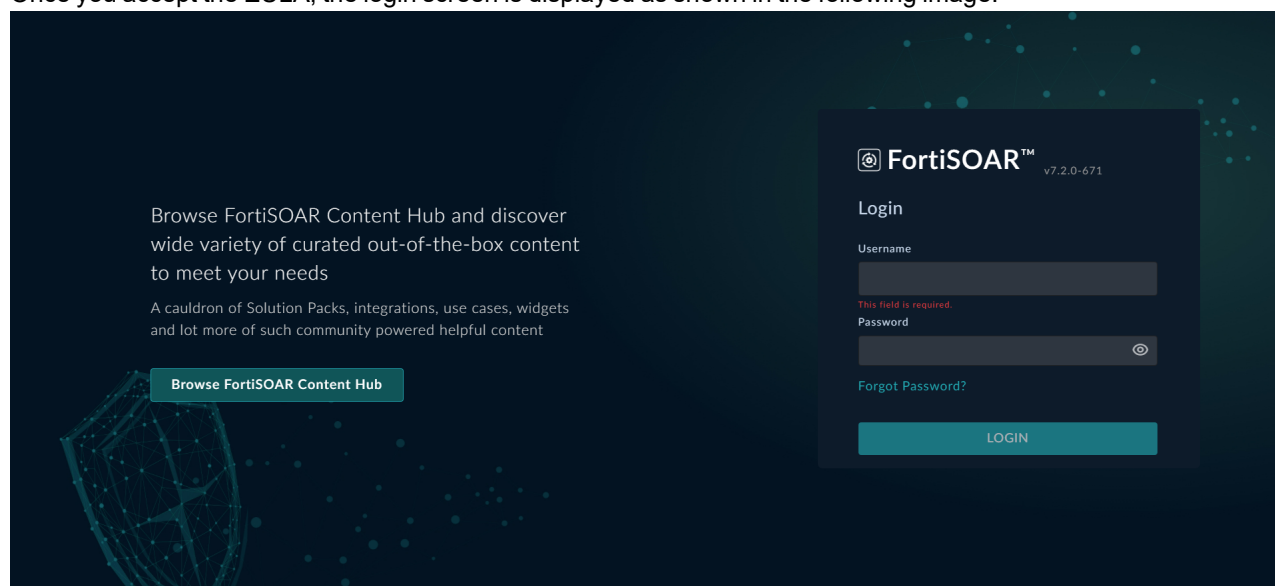
## Logging on to FortiSOAR for the first time

1. In a browser, enter the IP address that you had identified using the steps mentioned in the *Determining your DHCP IP address* section as and press `Enter`.

For example, `https://{Your_FortiSOAR_IP}`

This will display the Fortinet End-User License Agreement (EULA). You must accept the EULA before you can log onto FortiSOAR.

Once you accept the EULA; the login screen is displayed as shown in the following image:



2. Login using the following credentials:

Username: csadmin

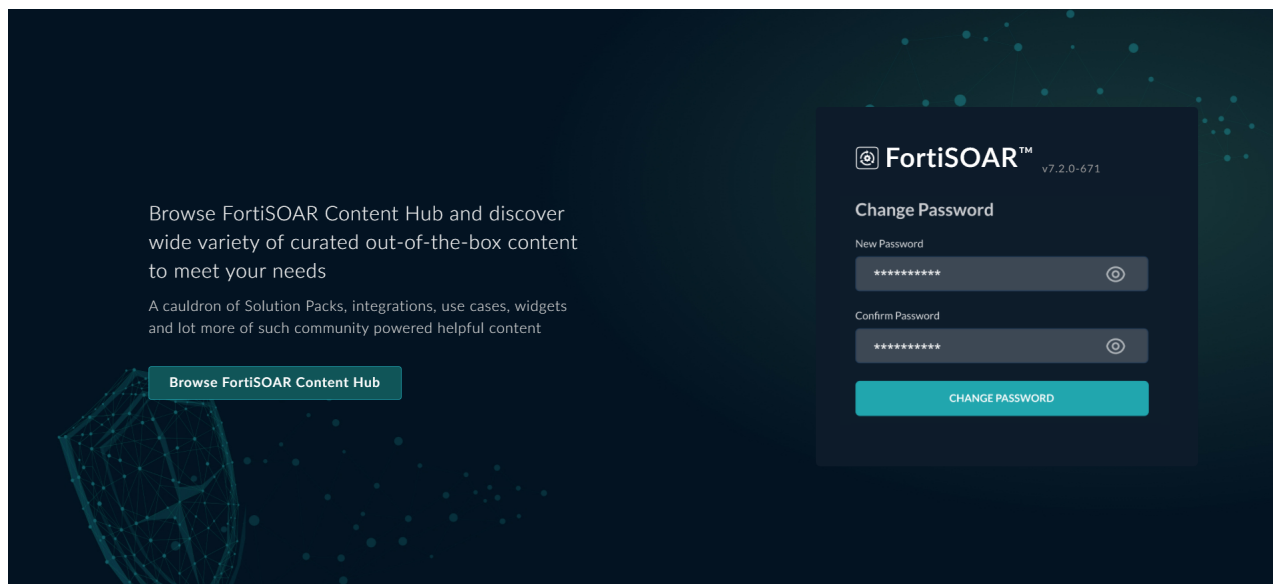
Password: changeme


The UI password of the 'csadmin' user for AWS is set to the "instance\_id" of your instance. To know the instance ID of your FortiSOAR AWS instance, you can SSH and run the `cloud-init query instance_id` command.

If you are a 'csadmin' user, and you are logging into FortiSOAR for the first time, you will be mandated to change the *default password*. This enhances the security of your csadmin account and prevents unauthorized parties from accessing the administration account for FortiSOAR.

New passwords that are set must contain at least 8 characters, one lower-case alphabet, one upper-case alphabet, one digit, and any one of the following special characters `~ ! @ # $ % ^ & * | ? _`

Once you enter the 'csadmin' username and default password the following screen is displayed, which prompts you to change the password:

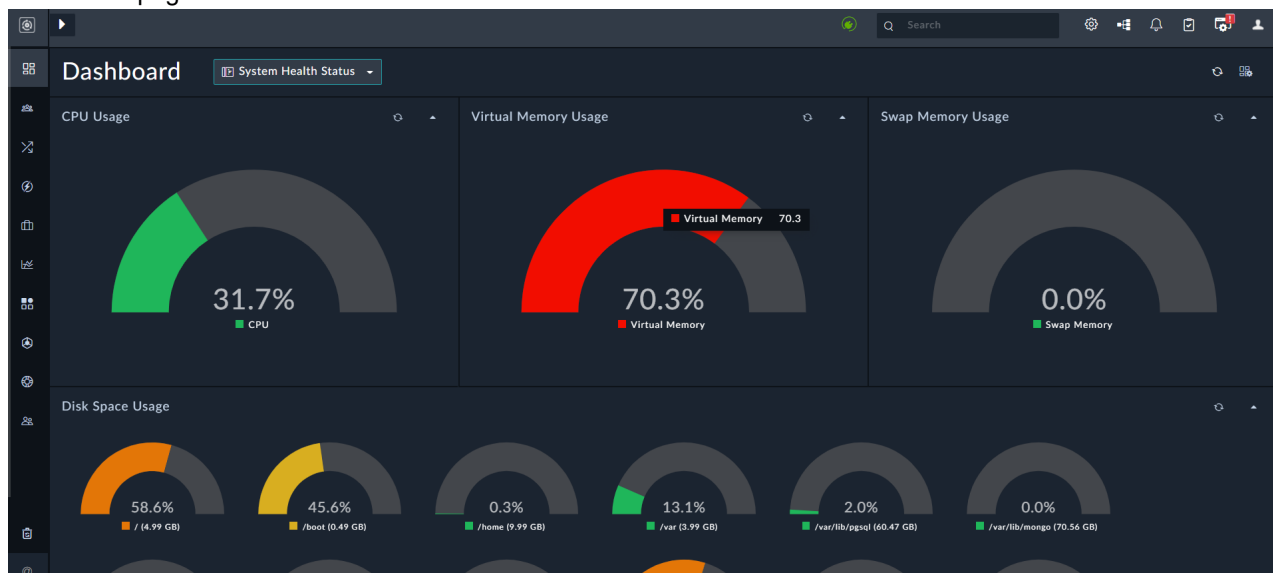


Ensure that you note down your csadmin password since if you forget your initial csadmin password, then you have to request FortiSOAR to reset this password. Also, when you are changing your csadmin password, you must ensure that you also update the email ID that is specified for csadmin, which by default is set to `soc@fortinet.com` (which is not a valid email ID). You can change the email ID by clicking the **User Profile** icon (  ) to open the **User Profile** page and change the email address in the **Email** field.

Once you set a valid email ID in the user profile, then you would be able to reset your password, whenever required, by clicking the **Forgot Password** link on the login page.

**Important:** It is also recommended that all new users should change their password when they first log on to FortiSOAR, irrespective of the complexity of the password assigned to the users.

After you have changed the default password, FortiSOAR logs you into the application and by default displays the Dashboard page:



Now you can begin configuring FortiSOAR for your network environment.

## Configuring SMTP for FortiSOAR

The SMTP connector comes pre-configured with FortiSOAR and it is required to receive any system or email notifications, including requests for resetting passwords. The SMTP connector is part of a number of pre-installed connectors or built-ins that are included with FortiSOAR. By default, the SMTP connector is configured to use FortiSOAR appliance as an SMTP relay server. You must point it to a production SMTP server in your organization. For more information on configuring the SMTP connector, see the "[FortiSOAR Built-in connectors](#)" article.



When you configure the SMTP connector, ensure that you select the **Mark As Default Configuration** option for the configuration that will be used for sending system notifications.

---

It is highly recommended that you review the [Additional configuration settings for FortiSOAR](#) chapter to understand the configurations that you should make in your FortiSOAR system before you begin to use FortiSOAR.

## Creating your first user and record



The following steps provide a high-level view of how to get started with FortiSOAR. These steps are explained in detail in "Administrators Guide."

---

1. Successfully log into FortiSOAR.
2. Click the **Settings** (⚙️) icon that is present in the upper right-hand corner near the **User Profile** icon. This displays the `System` page.  
Use the `Security Management` section to configure the following: Team Hierarchy, Teams, Roles, Users, Authentication, and Password Vault.
3. Add a new team in FortiSOAR.  
You can also use the default teams that are present in FortiSOAR.
4. Add a new role in FortiSOAR.  
You can also use default roles that are present in FortiSOAR.  
You provide user permissions on a module based on roles that you have assigned to that user.  
For example, if you want to provide a user with complete access to the Incident module, you must create a role that has `Create`, `Read`, `Update`, and `Delete` permissions on the Incident module and name it Incident Administrator.  
You must then assign that role to a user.
5. Add a new user and assign an appropriate role to the user.  
For example, create a user John A and assign John A the Incident Administrator role.
6. Create your first record.  
Log on to FortiSOAR as user John A, who has access to the `Incident` module. Click the **Add** button in the top bar of the `Incidents` module to open the `Create New Alert` form. Fill in the required details the `Create New Incident` form and click **Save** to create an incident.

## Additional configuration settings for FortiSOAR

You can optionally perform the following additional configurations for FortiSOAR based on your requirements.

If you want to externalize your FortiSOAR databases, which are PostgreSQL and ElasticSearch, see the "Administration Guide." The *Externalization of your FortiSOAR PostgreSQL database* chapter covers the steps for externalizing your PostgreSQL databases, and the *ElasticSearch Configuration* chapter covers the steps for externalizing your ElasticSearch database.

If you face any issues while deploying or upgrading FortiSOAR, see the [Troubleshooting FortiSOAR](#) chapter. If you face deployment or upgrade failures due to insufficient space, or if you face issues while using FortiSOAR that might be caused due to insufficient space, like you are unable to log into FortiSOAR or FortiSOAR services stop working, then see the [Issues occurring in FortiSOAR due to insufficient space](#) section in the [Troubleshooting FortiSOAR](#) chapter.

## Changing the hostname

The FortiSOAR Configuration Wizard is available only on the first `ssh` login. If at a later stage, you require to change the hostname of your FortiSOAR VM, then you can use the FortiSOAR Admin CLI (`csadm`). For more information on `csadm`, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."

To change the hostname, ensure that the hostname is resolvable and then do the following:

1. SSH to your FortiSOAR VM and login as a `root` user.
2. To change your hostname, type the following command:

```
# csadm hostname --set [<hostname>]
```

This command changes your current hostname to the new hostname that you have specified, sets up the message broker, regenerates certificates, and restarts FortiSOAR services.



It is recommended that you set the hostname of your FortiSOAR VM, at the time of deployment only and **not after** the FortiSOAR instance is in active use. If any errors occur when you are running the hostname change command, see the [Troubleshooting FortiSOAR](#) chapter.

---

**Note:** After the hostname has been reset, when users execute playbooks with an external manual input link, it is observed that the link that is generated in the email contains the original FQDN (hostname) rather than the one that has been updated. Therefore, users who are required to provide the input, have to manually update the FQDN (hostname) in the manual input link present in the email.

## Regenerating self-signed certificates

The default self-signed certificates shipped with FortiSOAR are valid for one year from the inception of your FortiSOAR instance. It is recommended to regenerate these certificates before the end of one year by running the following command as a *root* user (using 'sudo su' and using the *csadmin* password) using a SSH session:

```
csadm certs --generate `hostname`
```

Once this command is run successfully, you require to restart all services using the following command:

```
csadm services --restart
```

## Updating the SSL certificates

Use the following procedure to update Nginx certificates within the FortiSOAR Virtual Appliance when the FortiSOAR certificates expire. You can also use the following procedures to replace FortiSOAR self-signed certificates with your own signed certificates.

**Note:** Your SSL certificate file must be in the *.crt* and *.key* format. FortiSOAR does not support certificate formats such as *cer*, *p7b*, etc.

If your certificate is in another format such as, a CER certificate from Windows CA, then you need to create the *.crt* certificate from a *.cer* certificate, using the following command:

```
# openssl x509 -inform DER -in ssl_certificate.cer -out ssl_certificate.crt
```

There are two methods that you can use to update your SSL certificates:

- Using the FortiSOAR Admin CLI (*csadm*). For more information on *csadm*, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."
- Manually: You can use this method in case you face some issues with *csadm*.

### Method 1: Using *csadm*

1. SSH to your FortiSOAR VM and login as a *root* user.
2. To deploy your certificate, type the following command:  

```
# csadm certs --deploy
```

You must then specify the following at the prompt:

  - The complete path of the private key file of your ssl certificate.
  - The complete path to the crt file of your ssl certificate.

### Method 2: Manually

1. SSH to your FortiSOAR VM and login as a *root* user.
2. Copy your certificates to */etc/nginx/ssl/*.  
**Note:** When you deploy a custom certificate, you must ensure that the SAN name in the certificate should match the hostname (with or without a wildcard). If it is an IP address, it should be of type *IPAddress* in SAN name field.
3. Edit the *cyops-api.conf* file that is located in the */etc/nginx/conf.d* directory to update the *ssl\_certificate* and *ssl\_certificate\_key* as follows:  

```
ssl_certificate /etc/nginx/ssl/yourCert.crt;  
ssl_certificate_key /etc/nginx/ssl/yourCert.key;
```

For selinux permissions, run the following command:

```
# restorecon -v -R /etc/nginx/ssl
```
4. Edit the */etc/cyops/config.yml* file to update *crudhub\_host* to the DNS name specified in SSL Certificate.

5. Restart the nginx service using the following commands:  

```
# systemctl restart nginx
```
6. Clear your browser cache and re-login to FortiSOAR after updating the SSL Certificate.

## Adding self-signed CA certificates in CentOS as trusted certificates

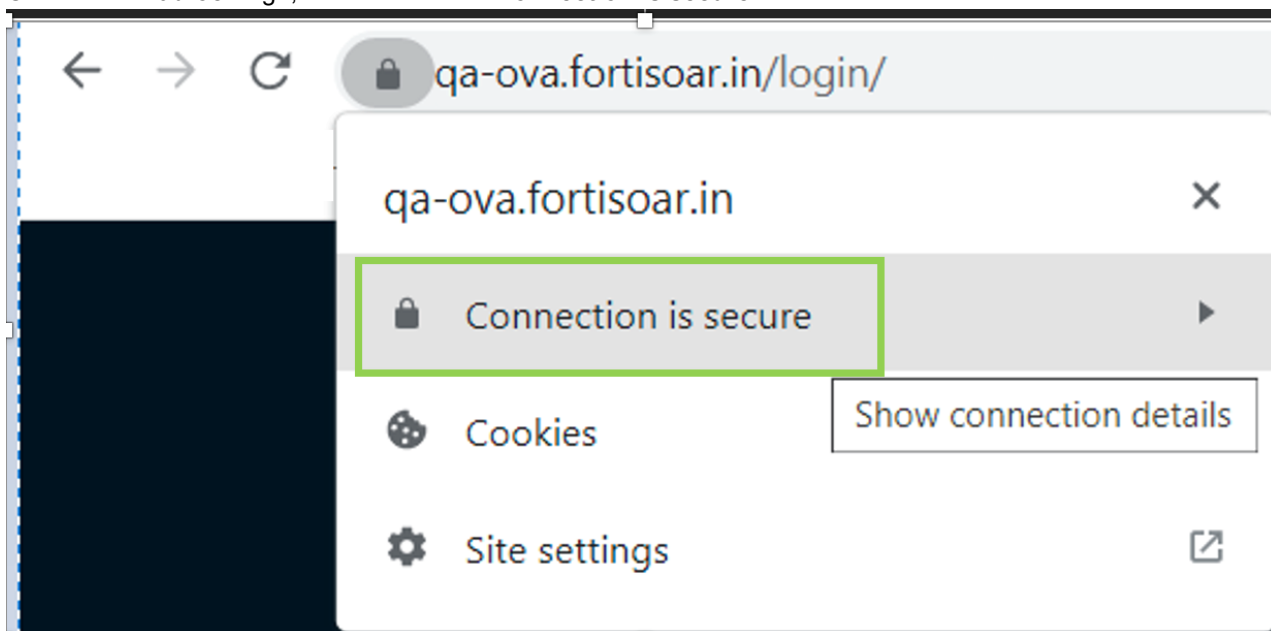
You might want to add self-signed CA certificates in OS as a trusted certificate in cases where you are using an offline repository with a self-signed certificate or you have agents that use self-signed certificates to communicate with your FortiSOAR instance.

A CA certificate is self-signed, so it is not trusted by default in any OS. Due to this tools like OpenSSL clients, curl, wget, etc raise issues. Sometimes, you can use tool flags to bypass certificate checks, for example, using `-k` in curl to bypass the certificate check

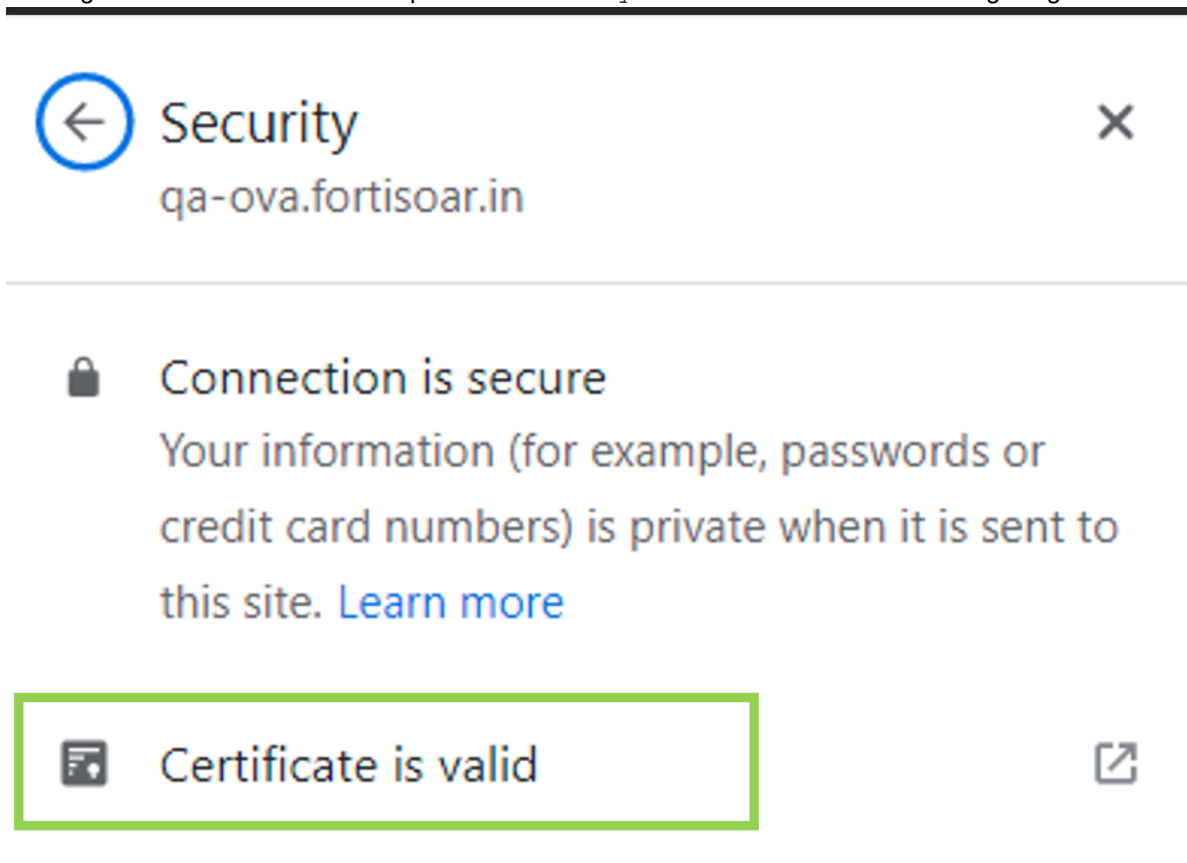
To solve this issue in CentOS, you can add the self-signed CA cert in the OS as a trusted certificate, by exporting the self-signed CA certificate (including all intermediate CA certs), then importing them into the Centos CA store using the process defined in <https://access.redhat.com/solutions/6339061>. The process is detailed as follows:

### Exporting the CA certificate using a browser

1. Open the offline repo URL in your browser.
2. Click on the **Padlock** sign, and then click on **Connection is secure**.



3. Clicking on **Connection is secure** opens the *Security* section as shown in the following image:



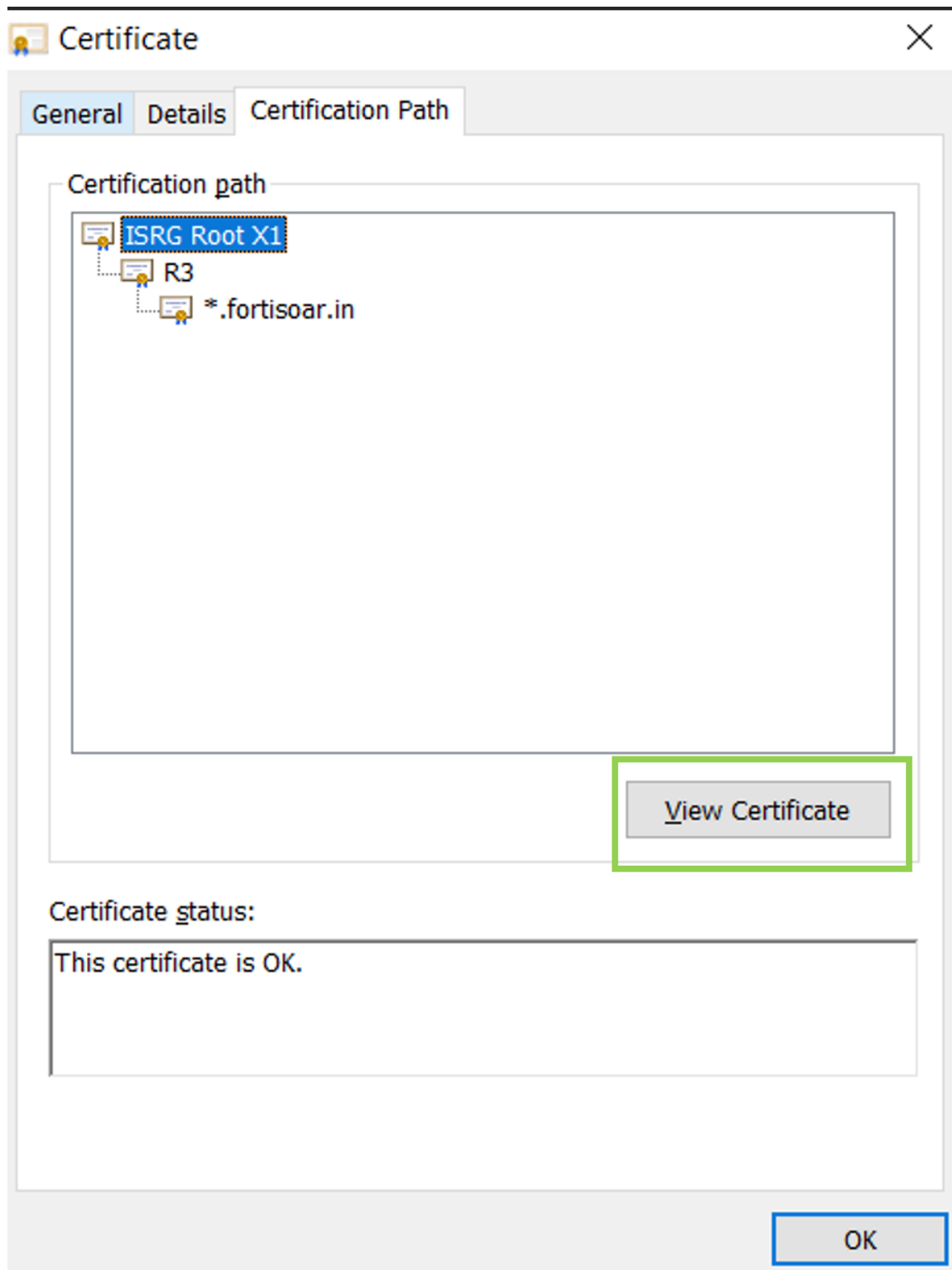
Click **Certificate is Valid** in the *Security* section.

4. Clicking on **Certificate is Valid** opens the `Certificate Detail` dialog as shown in the following image:



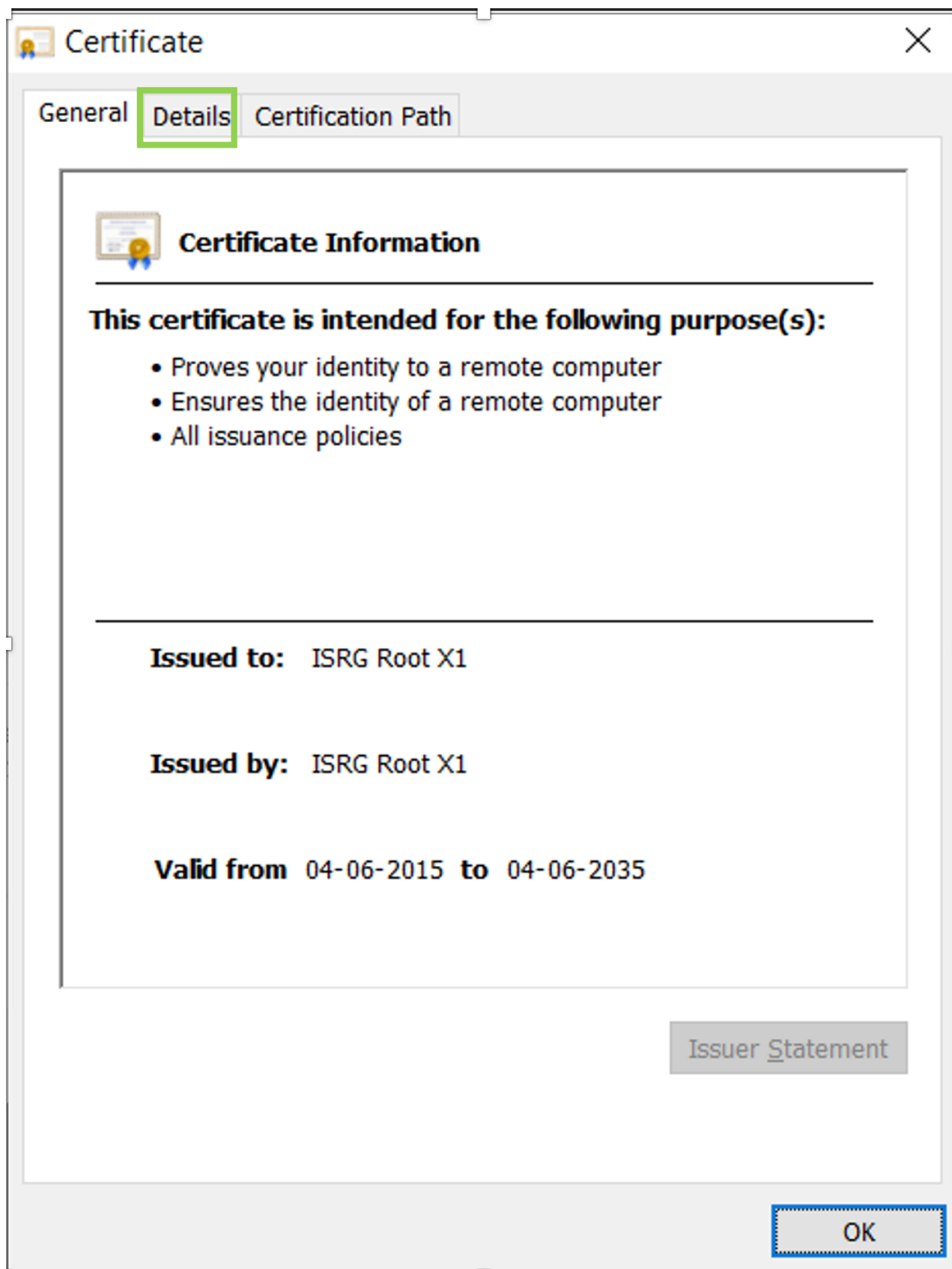
Click the **Certification Path** tab.

5. The **Certification Path** tab lists the complete CA chain as shown in the following image:

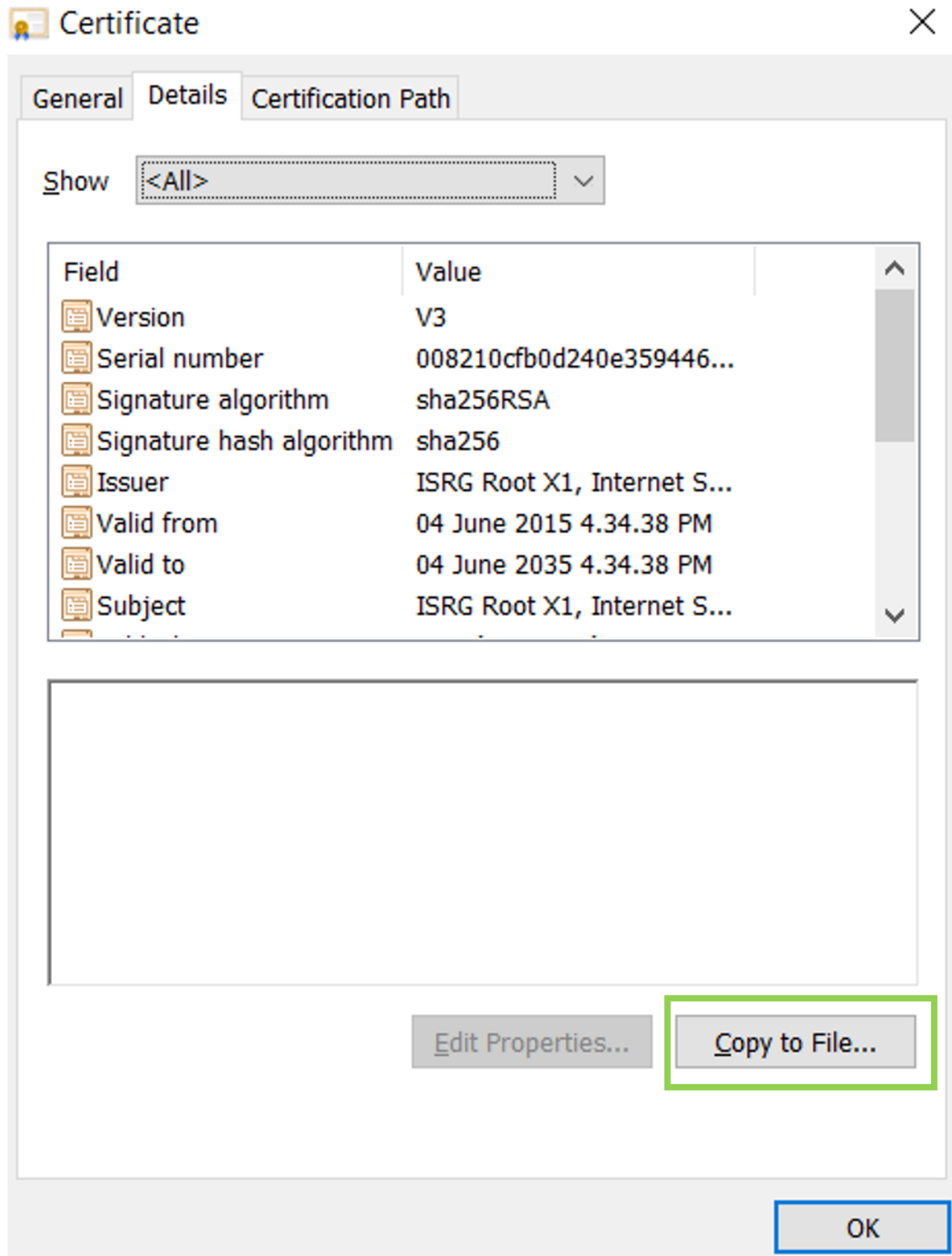


Select one of the CA certificates and click **View Certificate**.

6. On the `Certificate Detail` dialog, click the **Details** tab and click **OK**.




7. Click the **Copy to File** button to open the 'Certificate Export Wizard' that you can use to copy the certificate file.



8. On the **Welcome** screen of the 'Certificate Export Wizard', click **Next**.



←  Certificate Export Wizard

## Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.


To continue, click Next.

Next

Cancel

9. On the **Export File Format** screen, select **Base-64 encoded** as the file format to export, and click **Next**.



←  Certificate Export Wizard

### Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:


- ☐ DER encoded binary X.509 (.CER)
- ☒ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - ☐ Include all certificates in the certification path if possible
- ☐ Personal Information Exchange - PKCS #12 (.PFX)
  - ☐ Include all certificates in the certification path if possible
  - ☐ Delete the private key if the export is successful
  - ☐ Export all extended properties
  - ☐ Enable certificate privacy
- ☐ Microsoft Serialized Certificate Store (.SST)

Next

Cancel

10. On the **File to Export** screen, click **Browse** to specify the location to export the CA certificate as a file and click **Next**.



←  Certificate Export Wizard

### File to Export

Specify the name of the file you want to export

File name:

Browse...

Next

Cancel

11. On the **Completing the Certificate Export Wizard** screen, click **Finish**, to complete exporting the CA certificate.



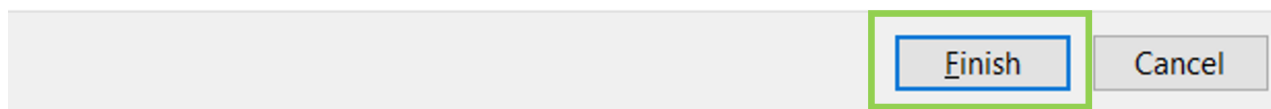
← Certificate Export Wizard

## Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\... \Downloads\x3-c
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)



Use the same procedure to export all your CA certs in the certificate chain.

## Adding the self-signed CA cert in the OS

You require to copy the CA certificate files that were exported to the destination CentOS system(s).

1. Create a certificate file `abc.crt` using for example your organization's name, `abc`, in the following location:  
`/etc/pki/ca-trust/source/anchors/ abc.crt`
2. Copy the contents from CA certificate files that were exported to `abc.crt`.
3. Execute the following command:  
`update-ca-trust enable ; update-ca-trust extract`

## Verifying that the self-signed CA certificates are added as trusted certificates in CentOS

Run the following commands to verify if the self-signed CA certificates are added as trusted CA in CentOS:

- `curl -v https://<offline-repo-server>`
- `wget https://<offline-repo-server>/7.0.0/upgrade-cyops-7.0.0.sh`

If both the above commands should work without any certificate warnings or errors it means that the self-signed CA certificates are added as trusted CA in CentOS.

## Setting up monitoring for your FortiSOAR system

It is recommended that you set up the following as part of your initial deployment and configuration process to monitor various important parts of your FortiSOAR system such as disk space, audit logs, execution logs, etc.

### Setting up system monitoring

From version 6.4.3 onwards, you should set up system monitoring for FortiSOAR, both in case of a single node system and High Availability (HA) clusters on the [System Configuration](#) page. To know more about the setting up thresholds and enabling notifications to effectively monitor various FortiSOAR system resources such as CPU, Disk Space and Memory utilization, and the statuses of various FortiSOAR services, see the *System Configuration* chapter in the "Administration Guide."

For versions prior to 6.4.3, you should set up thresholds, schedules, and notifications for the System Monitoring playbook that is included by default with FortiSOAR to effectively monitor various FortiSOAR system resources. To know more about configuring thresholds, schedules, and notifications, see the [System Monitoring: Setting up thresholds, schedules, and notifications](#) article present in the Fortinet Knowledge Base.

### Setting up purging for audit and playbook logs

FortiSOAR persists each workflow step inputs, outputs and error details for providing granular details of each action run, which is very useful for subsequent analysis and debugging. However, the Playbook Execution History data is significantly large and generates large volumes of data, which might not be useful after some point of time. Therefore, it is recommended that the retention period for the playbook logs should not be more than a few weeks and it is very important that you schedule purging for these logs at regular intervals.

FortiSOAR also audits every login, logout, record create, update, delete of records and other important activity on the system. These logs also might be useful for only a few years.

One must, therefore, configure a purge schedule for both the playbook and audit logs as per the organization's retention policy. This would help keeping the database and disk usage for these logs constant over time.

You can schedule purging, on a global level, for both audit logs and executed playbook logs. Scheduling purging of audit and executed playbook logs ensures that the logs are periodically cleared. For the procedure for enabling and scheduling purging, see the *System Configuration* chapter in the "Administration Guide."

For additional information about monitoring your FortiSOAR system, see the *Monitoring FortiSOAR* chapter in the "Administration Guide."

## Configuring High Availability or Disaster Recovery options

You can configure FortiSOAR with either an externalized PostgreSQL database or an internal PostgreSQL database. For both cases you can configure Active-Active or Active-Passive high availability clusters. For more information, see the *High Availability support in FortiSOAR* chapter in the "Administration Guide."

FortiSOAR provides backup scripts that are scheduled to run at pre-defined intervals and take full database backup on a shared or backed up drive. For more information on backing up and restoring FortiSOAR, see the *Backing up and Restoring FortiSOAR* chapter in the "Administration Guide."

## Starting and stopping FortiSOAR Services

You will need to stop and start the FortiSOAR Services in the following cases:

- Update/Upgrade your SSL certificates
- Post-update, if playbooks are not working as expected
- Post-reboot, if the FortiSOAR Platform is not working as expected

To stop and start all the FortiSOAR services, use the FortiSOAR Admin CLI (`csadm`). For more information on `csadm`, see the FortiSOAR *Admin CLI* chapter in the "Administration Guide." You can run the `csadm` command on any FortiSOAR machine using any terminal. Any user who has `root` or `sudo` permissions can run the `csadm` command.

To view the status of all FortiSOAR services, type: `# csadm services --status`

To restart FortiSOAR services, type: `# csadm services --restart`

To start FortiSOAR services, type: `# csadm services --start`

To stop FortiSOAR services, type: `# csadm services --stop`

## Changing the FortiSOAR default database passwords

After you complete the FortiSOAR deployment procedure, you can change the default database passwords using the FortiSOAR Admin CLI (`csadm`) as a `root` user:

```
# csadm db --change-passwd
```

The script will prompt you for the new passwords for the Postgres DB, and you must appropriately enter the password that you want to set for the Postgres DB.

After running this script and changing the passwords, this script makes FortiSOAR use the new passwords and stores the passwords in an encrypted format. For more information on `csadm`, see the FortiSOAR *Admin CLI* chapter in the "Administration Guide."

## Setting up a proxy server to service all requests from FortiSOAR

Your FortiSOAR instance would need access to the following endpoints on the public internet:

- For upgrading FortiSOAR, installing connectors, and accessing the widget library: <https://repo.fortisoar.fortinet.com/>
- For installing python dependencies for connectors: <https://pypi.python.org>  
**Note:** There is a parallel python repository also on [repo.fortisoar.fortinet.com](https://repo.fortisoar.fortinet.com) that can be used with some configuration if your organization does not approve pypi.
- For synchronization of FortiSOAR license details: <https://globalupdate.fortinet.net>
- For accessing any SaaS or API endpoint that you have configured, for example VirusTotal, and to which you require to be connected.

You must ensure that these endpoints are open from the organizations proxy. You can configure your proxy for the first time when you run the FortiSOAR Configuration Wizard. If you subsequently require to change the proxy, then you can use the `csadm cli` commands or use the UI as specified in the following procedure.

You can use the `# csadm network set-https-proxy` command to set the proxy for both your system and the web services. For more information on `csadm`, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."

Use the **Environment Variables** tab on the `System Configuration` page to configure proxy settings for FortiSOAR and to define any other environment variables.

The screenshot shows the FortiSOAR web interface. The left sidebar contains a navigation menu with items like System, System Configuration, Audit Log, License Manager, Notifications, Data Archival, Agent Configurations, Secure Message Exchange, Agents, Security Management, Team Hierarchy, Teams, and Roles. The main content area is titled 'System Configuration' and has several tabs: Application Configuration, Log Forwarding, Environment Variables (selected), Branding, and System Fixtures. A yellow warning box at the top states: 'Note that the system services will be restarted for the Environment variable changes to take effect. Ensure that there are no running workflows before saving the setting changes.' Below this, the 'Proxy Settings' section is visible. It has two main sections: 'HTTP' and 'HTTPS'. The 'HTTP' section includes a 'Proxy URL' field with 'http://example.com', a 'Port' field, a 'Username' field with 'Enter Username', and a 'Set Password' button. Below these is a note: 'Password fields are write-only. If you do not change this field, your password will not be overwritten.' The 'HTTPS' section has a checkbox labeled 'Use Same As Above'. At the bottom of the 'HTTP' section is a green 'Save' button.



External web pages that you open (for example, from a link included in the description field of an alert) or view (for example, using the iFrame Widget) in FortiSOAR goes through the configured proxy server if you have configured the proxy in the web browser's settings. If the proxy is not configured in the web browser's settings, then the external web pages are opened directly without using the configured proxy server.

## Configuring Proxy Settings and environment variables

Use the following procedure to add proxy details and environment variables for FortiSOAR:

1. Log on to FortiSOAR as an administrator.
2. Click **Setting** to open the `System Configuration` page (**Application Configuration** tab).
3. Click the **Environment Variables** tab.
4. To set up an HTTP proxy to serve all HTTP requests from FortiSOAR, enter the following details in the `Proxy Settings` section on the `Environment Variables` page:
  - a. In the **Proxy URL** field, enter the HTTP proxy server IP and in the **Port** field, optionally enter the HTTP proxy server port.  
**Note:** If you do not specify `HTTP` or `HTTPS` in the **Proxy URL** field, then by default `HTTPS` is set.
  - b. In the **Username** field, enter the username used to access the HTTP proxy server (if not applicable leave this field blank).
  - c. Click **Set Password** to enter the password used to access the HTTP proxy server (if not applicable leave this field blank).
  - d. Verify that the **Enabled** check box is selected to apply the proxy settings that you have specified. If you clear the **Enabled** check box, then the proxy settings that you have specified are saved but not applied.  
By default, the **Enabled** check box is selected.
5. To set up an HTTPS proxy server to serve all https requests from FortiSOAR, enter the following details in the `HTTPS` section on the `Environment Variables` page:
  - a. If you want to use the same proxy server that you have set up for HTTP requests for HTTPS requests as well, then select the **Use Same As Above** checkbox. Or set up the HTTPS proxy server as follows:
  - b. In the **Proxy URL** field, enter the https proxy server IP and in the **Port** field, optionally enter the HTTPS proxy server port.
  - c. In the **Username** field, enter the username used to access the HTTPS proxy server (if not applicable leave this field blank).
  - d. Click **Set Password** to enter the password used to access the HTTPS proxy server (if not applicable leave this field blank).
  - e. Verify that the **Enabled** check box is selected to apply the proxy settings that you have specified. If you clear the **Enabled** check box, then the proxy settings that you have specified is saved but not applied.  
By default, the **Enabled** check box is selected.
6. (Optional) In the **No Proxy List** text box, enter a comma-separated list of addresses that do not require to be routed through a proxy server.  
For example, enter `http://example.com` in the **No Proxy List** text box.  
`localhost` and `127.0.0.1` are added by default to the no proxy list by the system.
7. (Optional) In the `Other Environment Variables` section, you can add environmental variables and setup proxies for other protocols, such as FTP (other than HTTP or HTTPS) in a key-value pair. Click the **+Add New** link and the **Key** and **Value** text boxes will be displayed. Enter the protocol for which you want to set up the proxy in the **Key** text box and its value in the **Value** box.  
For example, enter `FTP` in the **Key** field and `1.1.1.1` in the **Value** field.
8. Click **Save** to save your proxy server settings or the environment variables you have added.

## Backing up the data encryption keys

Encryption keys are used to encrypt data in FortiSOAR. When you install FortiSOAR for the first-time default encryption keys are added, which are unique per instance; therefore, you do not need to change the encryption keys.

**Important:** It is highly recommended that you back up the encryption keys (`.Defuse.key`) from the `/opt/cyops/config/cyops-api` file. The `.Defuse.key` is a dot file, therefore you need to use `ls -la /opt/cyops/configs/cyops-api/` to list/view the file and store the data encryption keys securely in a Password Manager or Vault.



Once you encrypt your production data in FortiSOAR using the encryption keys, you should not change those keys again; since if your encryption keys are changed, this might result in the loss of previously encrypted production data. If you do require to change the encryption keys, then contact FortiSOAR Support.

---

## Configuring a reverse proxy (Apache proxy server)

If you have set up a reverse proxy, an Apache proxy server, in your environment, then configure this reverse proxy server so that the live sync functionality works, as follows:

**Important:** This procedure applies only to an Apache proxy server. You can enable any other reverse proxy using a similar pattern to support the web socket functionality.

Update the proxy configuration file on your proxy server as follows:

```
<VirtualHost *:80>

#ServerName
SSLProxyEngine on

SSLProxyCheckPeerCN on
SSLProxyCheckPeerName on

/** Section required for enabling Websockets **/
RewriteEngine On
RewriteCond %{HTTP:Upgrade} =websocket [NC]
RewriteRule /(.*) wss://<FortiSOAR-URL>/$1 [P,L]
/** End Section **/

ProxyPass / https://<FortiSOAR-URL>/
ProxyPassReverse / https://<FortiSOAR-URL>/

RequestHeader set Host "<FortiSOAR-URL>"
RequestHeader set Origin "https://<FortiSOAR-URL>"
</VirtualHost>
```

# Troubleshooting FortiSOAR Issues

## Troubleshooting issues occurring in FortiSOAR due to insufficient space

You can face deployment or upgrade failures due to insufficient space. If you have limited partition size for `/dev/mapper/vgapp-csapps`, then FortiSOAR upgrade might fail. Therefore, before you upgrade your FortiSOAR system, you must ensure that you increase the partition size to a minimum of 4 GB for `/dev/mapper/vgapp-csapps` to prevent potential loss of backups.

You might also experience any of the following symptoms when the disk space of the database on which FortiSOAR is running gets full:

- Users are unable to log into FortiSOAR.
- All FortiSOAR services might stop working, as they cannot write to their respective log files. For example, the PostgreSQL service fails to start when the PostgreSQL database disk is full.

Insufficient space in FortiSOAR can be caused due to a number of reasons, some of them are as follows:

- Increase in the number of log files in `/var/log/` and `/var/log/cyops`
- `/home` drive is full
- Increase in the data in the database
- PostgreSQL database disk is full



You can fix this issue using the `csadm system disk expand-lv` command to extend a logical volume to occupy space that is available in its own volume group or if a new disk is attached, then a single partition is created and the logical volume is expanded to occupy that partition based on the size (GB) you have specified. For information on this command, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."

You can also use the following methods to fix this issue: :

- Extend the disk space by adding a new disk and then extending the logical volume in the new disk.
- Extend the logical volume by using the free space that is already available in the volume group.
- Extend the logical volume on the existing disk without adding a new disk, if sufficient unallocated space is available on the existing disk.
- Procedure to be followed when the Postgres service has failed which could be due to the PostgreSQL database disk is full.

**Note:** Perform the following procedures as a `root` user using the `sudo su` command.

### Resolution 1

Perform the following steps to extend your disk space by adding a new disk and then extending the logical volume (LVM) in the new disk.



When you add a new disk, ensure that the disk size is less than 2TB. If you have a disk whose size is greater than 2TB size, you need to create multiple PVs with 2TB size and expand the Volume Groups accordingly. This is because FortiSOAR has the MBR disk type whose maximum hard drive size is 2TB.

1. Stop all FortiSOAR services using the following command:

```
# csadm services --stop
```

2. Add the new disk drive with the required size on the instance.

3. Run the following command to check the size of the newly added and unpartitioned disk.

```
# lsblk
```

This command displays the size of newly added and unpartitioned disk. In this example, `sde` is the newly added disk:

```
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 8G 0 disk
'-sda1 8:1 0 8G 0 part /
sdb 8:16 0 100G 0 disk
'-sdb1 8:17 0 100G 0 part
sdc 8:32 0 300G 0 disk
'-sdc1 8:33 0 300G 0 part
'-vg_repo-lvol0 253:0 0 500G 0 lvm /repos
sdd 8:48 0 200G 0 disk
'-vg_repo-lvol0 253:0 0 500G 0 lvm /repos
sde 8:64 0 200G 0 disk #This is the new attached partition
sr0 11:0 1 1024M 0 rom
```

**Note:** In case the disk is not reflected in the VM, you can run the following command:

```
## echo "- - -" > /sys/class/scsi_host/<host#>/scan
```

(Replace `host#` with the correct host number)

Then run the `# lsblk` command again to verify the newly added disk.

If even after running the above command the newly added disk is NOT visible under `lsblk`, then reboot the appliance using `reboot` command.

4. Run the following command to create the physical volume by specifying the name for the newly added disk:

```
# pvcreate /dev/<disk_name>
```

5. Run the following command to check the name of the volume group:

```
# vgs
```

The column **VG** corresponds to the volume group as seen in the following sample output:

```
VG #PV #LV #SN Attr VSize VFree
<volume_group_name> 1 13 0 wz--n- <243.65g 8.00g
```

6. Run the following command with the volume group name (from VG column in step 5) and `disk_name` as specified in step 4, to extend the volume group size:

```
# vgextend <lvm_group_name> /dev/<disk_name>
```

7. Run the following command to check the size of the extended volume group:

```
# vgs
```

The column **VFree** corresponds to the volume group size (20.00g) as seen in the following sample output:

```
VG #PV #LV #SN Attr VSize VFree
<volume_group_name> 1 13 0 wz--n- <243.65g 20.00g
```

8. Run the following command to extend the logical volume by the size you specify:

```
# lvextend -L +<disk_size>G <LVM_name>
```

The following example shows that the logical volume is being extended by 18GB:

```
lvextend -L +18G /dev/mapper/<LVM_name>
```

**Note:** You must extend the disk size to less than or equal to the total size of the volume group.

9. Run the following command to resize the file system for the disk that has been extended in step 8:

```
# xfs_growfs /dev/mapper/<LVM_name>
```

10. Run the following command to check if the volume size is extended:

```
# df -h /dev/mapper/<LVM_name>
```

11. Start all FortiSOAR services using the following command:

```
# csadm services --start
```

## Resolution 2

Perform the following steps to extend the logical volume by using the free space that is already available in the volume group:

1. Stop all FortiSOAR services using the following command:  

```
# csadm services --stop
```
2. Run the following command to check the free size available in volume group:  

```
# vgs
```

The column **VFree** corresponds to the volume group size (20.00g) as seen in the following sample output:

```
VG #PV #LV #SN Attr VSize VFree
<volume_group_name> 1 13 0 wz--n- <243.65g 20.00g
```
3. Run the following command to extend the logical volume by the size you specify:  

```
# lvextend -L +<disk_size>G <LVM_name>
```

The following example shows that the logical volume is being extended by 18GB:

```
# lvextend -L +18G /dev/mapper/<LVM_name>
```

**Note:** You must extend the disk size to less than or equal to the total size of the volume group.
4. Run the following command to resize the file system for the disk that has been extended in step 3:  

```
# xfs_growfs /dev/mapper/<LVM_name>
```
5. Run the following command to check if the volume size is extended:  

```
# df -h /dev/mapper/<LVM_name>
```
6. Start all FortiSOAR services using the following command:  

```
# csadm services --start
```

## Resolution 3

Perform the following steps to extend the logical volume on the existing disk without adding a new disk, if sufficient unallocated space is available on the existing disk. Before proceeding further, it is recommended that you find out whether sufficient unallocated space is available on existing disk using the following command:

```
# parted /dev/<disk_name> print free
```

For example, running the `# parted /dev/sdb print free` command will display the following:

```
Model: VMware Virtual disk (scsi)
Disk /dev/sdb: 215GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number  Start    End      Size     Type     File system  Flags
32.3kB  1049kB   1016kB   Free Space
1       1049kB   161GB    161GB    primary
161GB   215GB    53.7GB   Free Space
```

The “Free Space” in above the output refers to unallocated space. If the mentioned size is sufficient, then perform the following steps:

1. Stop all FortiSOAR services using the following command:  

```
# csadm services --stop
```
2. Create a partition on the existing disk using the following command:  

```
# fdisk /dev/<disk_name>
```
3. Enter `n` to create a new partition.
4. Enter `p` to choose the newly created partition as the primary partition.
5. Select the Partition number. The operating system will calculate this on its own, you just require to press `Enter`.
6. Select defaults for the `First Cylinder/Sector` and `Last Cylinder/Sector` values.

7. Enter `w` to write the changes to the partition table.
8. Run the following command to rewrite the filesystem:  
`# partprobe /dev/<disk_name>`
9. After the VM restarts, stop all FortiSOAR services using the following command:  
`# csadm services --stop`
10. Run the following command to see the new partition:  
`# fdisk -l /dev/<disk_name>`  
 This command displays the properties of the newly attached partition. For this example, `/dev/sda3` is the newly added partition.
11. Create a physical volume in the new partition using the following command:  
`# pvcreate`  
 For example, `# pvcreate /dev/sda3`
12. Extend the volume group using the following command:  
`# vgextend`  
 For example, `# vgextend <volume_group_name> /dev/sda3`
13. Extend the logical volume by the size you specify using the following command:  
`# lvextend -L<size>G <LVM_name>`  
 For example, to extend the logical volume by 20 G use the following command:  
`# lvextend -L20G /dev/mapper/cyops-relations`
14. Increase the file system size using the following command:  
`# xfs_growfs`  
 For example, `# xfs_growfs /dev/mapper/cyops-relations`
15. Start all FortiSOAR services using the following command:  
`# csadm services --start`

#### Resolution 4

Perform the following steps when you notice that your Postgres service has failed which could be due to the PostgreSQL database disk is full.

1. Run the following command and check the disk space in `/var/lib/pgsql/`:  
`# df -h /var/lib/pgsql/`  
 If there is no space or less than 1 GB space left in `/var/lib/pgsql/`, then the `psql` service will not start due to the space issue.
2. `# cd /var/lib/pgsql/`  
`# ls -lrth`  
 You will observe that there is a file named `resv_space` that is taking up 1GB of space.
3. Stop all the services using the following command:  
`csadm services --stop`
4. Move the `resv_space` file from `/var/lib/pgsql/` to `/home/csadmin` using the following command:  
`# mv /var/lib/pgsql/resv_space /home/csadmin`
5. Check the disk space in `/var/lib/pgsql/` again:  
`# df -h /var/lib/pgsql/`  
 You will observe that 1GB of space has been freed.
6. Start all the services again using the following command:  
`csadm services --start`
7. If this is a development or staging instance and you cannot extend the disk space, then the disk space can also be freed up by purging workflow logs. For information on purging workflow logs, see the *System Configuration* chapter in the "Administration Guide."
8. Move the `resv_space` file from `/home/csadmin` back to `/var/lib/pgsql/`:  
`# mv /home/csadmin/resv_space /var/lib/pgsql/`

## Increasing the disk space for record storage in case of AWS AMI deployment

If you are deploying a fresh instance of FortiSOAR in AWS with AMI, and you require larger disk space for record storage, do the following:

1. Increase the size Elastic and PostgreSQL disks, for example `/dev/sdg` (Elastic) and `/dev/sdf` (postgresql).
2. Provision your FortiSOAR instance and complete running the FortiSOAR VM Configuration Wizard.
3. Start an SSH session as a `root` user and check the allocated disk space using the `df -h` command.
4. If the newly increased disk space that is allocated is sufficient, then no changes are required, else you can use the `csadm system` command to increase the partition size and allocate unused space. For more information on the `csadm` command, see the FortiSOAR Admin CLI chapter in the "Administration Guide."

## Troubleshooting Deployment Issues

### The FortiSOAR Virtual Appliance deployment on ESX is failing

**Resolution:**

1. Verify that FortiSOAR Virtual Appliance file that you have downloaded is not corrupted by running a `# md5sum` command for the FortiSOAR Virtual Appliance.
2. Check that the ESX server has fulfilled all prerequisites specified for the VM. Refer to the *Planning* section for details.
3. If both points 1 and 2 are ok, contact VMWare support.

### Cannot access the FortiSOAR portal

**Resolution:**

1. Check the ESX network to which FortiSOAR VM is connected.
2. Check if the IP address is assigned to your FortiSOAR VM, in the case of DHCP or static IP addresses. Refer to the *Editing the VM configuration* section for more information on Setting a static IP and Determining your DHCP IP address.

### Cannot login to the FortiSOAR platform

**Resolution:**

1. Check if you are using the correct credentials that have been provided to you by FortiSOAR Customer Support.
2. ssh to the VM where you have deployed FortiSOAR to check the status of `cyops-auth` service. The `cyops-auth` service must be running.
3. If both points 1 and 2 are ok, and the `cyops-auth` service is running, contact FortiSOAR support.

### Getting a 502 error when you click on the Reports tab

**Resolution:**

1. ssh to the VM where you have installed FortiSOAR.
2. Log in using the ssh credentials.
3. Run the `$ sudo su` command.  
Enter your FortiSOAR password.
4. Run the `$ sudo systemctl restart tomcat` command.
5. Run the `$ sudo systemctl restart nginx` command.

If the issue yet does not get resolved, contact FortiSOAR support.

## Troubleshooting Upgrade Issues

For the procedure on how to upgrade to FortiSOAR 7.2.2, see the *Upgrading a FortiSOAR enterprise instance to 7.2.2* section in the “Upgrade Guide.”

### Post license renewal you cannot log into FortiSOAR

If you have requested for a license from FortiSOAR with lesser number of users than your existing users, you cannot log onto FortiSOAR post upgrade.

For example, when you had requested a license from FortiSOAR, you had requested for a license for 10 users; however, you have 15 users existing in your system, you will not be able to log onto FortiSOAR post-upgrade. So, it is very important for you to provide the correct number of users while requesting for a license from FortiSOAR.

**Resolution:**

Contact FortiSOAR Support to generate a new license for you with the correct number of users.

### Failure to upgrade FortiSOAR

In case you face a failure while trying to upgrade FortiSOAR, then perform the following steps:

**Resolution:**

1. To gather logs and send them to FortiSOAR Support, do the following:
  - a. ssh to machine as a *root* user and type the following command:  
`# csadm log --collect`
  - b. Specify the path where you want to collect the logs. By default, the logs are collected in the `/tmp/` folder. A file named `fortisoar-logs.tar.gz.gpg` gets generated in the path you have specified. Send this file to FortiSOAR Support.
2. Revert the snapshot of your system to the latest working state. You must take a snapshot of your system before you attempt to upgrade FortiSOAR on your system.  
Follow the steps mentioned in the documentation of your platform for taking a snapshot and reverting to the current snapshot.

## Post-upgrade your playbooks fail to execute, and the playbooks are also not listed in the executed playbooks log

If you have not cleaned the workflow history prior to upgrading your FortiSOAR version, and if you have a large number of records in the workflow history (> 50000), then the overall upgrade time would increase, and this issue might occur. For the method to clean the workflow execution run history, see the "Setting up auto-cleanup of workflow execution history" topic in the *Debugging and Optimizing Playbooks* chapter in the "Playbooks Guide."

### Resolution

Perform the following steps:

1. Check the install logs to see if errors such as the following are present:  

```
psycpg2.InternalError: missing chunk number 0 for toast value 1502832 in pg_toast_17046
```
2. Connect to the postgres db and run the following command:  

```
# REINDEX table pg_toast.pg_toast_XXXXX;
```

 (where XXXXX is the number from the error message present in step 1).
3. Run the following commands:  

```
# cd /opt/cyops-workflow/sealab
$ sudo -u nginx /opt/cyops-workflow/.env/bin/python3 manage.py migrate
```

**Note:** If `manage.py` fails again for `pg_toast` value (error mentioned in step 1), then you must execute steps 2 and 3 again with the new `pg_toast` value mentioned in the error, till the `manage.py` executes successfully.

## Login and logout events are not audited after you have upgraded your FortiSOAR version

After you have upgraded FortiSOAR on your system, you observe the following error in the `auditlog` log file located at `/var/log/cyops/cyops-gateway/auditlog.log`:

`ERROR c.c.a.service.RecordLogService.processRecordLogs - 500 Internal Server Error`, and you also do not see any Login and Logout events in **Audit Logs** on FortiSOAR UI, then perform the steps mentioned in the resolution.

### Resolution

To resolve this issue and include login and login events in audit logs, run the following commands on your FortiSOAR VM as a root user:

```
yes | cp /opt/cyops-workflow/sealab/.envdir/APPLIANCE_PUBLIC_KEY /etc/cyops/APPLIANCE_PUBLIC_KEY
yes | cp /opt/cyops-workflow/sealab/.envdir/APPLIANCE_PRIVATE_KEY /etc/cyops/APPLIANCE_PRIVATE_KEY
chmod -R 644 /etc/cyops/APPLIANCE_*_KEY
chown tomcat:tomcat /etc/cyops/APPLIANCE_*_KEY
systemctl restart tomcat
```

## Issues occurring when you have restored data on a FortiSOAR 6.0+ system with data backed up from a system prior to 6.0.0

If you have backed up a FortiSOAR system whose version is prior to 6.0.0 and restored this system on a fresh installation of FortiSOAR 6.0.0 or later, then you might face issues in creating records etc. since the system will not be able to find your record ID sequence.

### Resolution

To keep your record ID sequence and avoid issues on the FortiSOAR 6.0+ instance, you must run the following commands as a `root` user to keep your record ID sequence:

1. In the `/opt/cyops-api/config/parameters_prod.yaml` file set the `id_per_module` parameter to **false**.
2. `cd /opt/cyops-apisudo -u nginx php bin/console cache:clear --env=prod`



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 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.