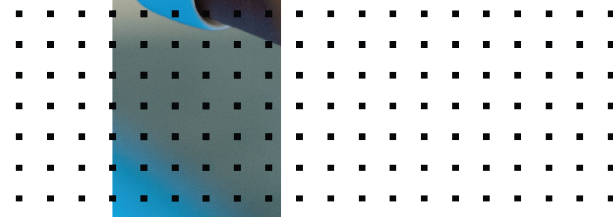
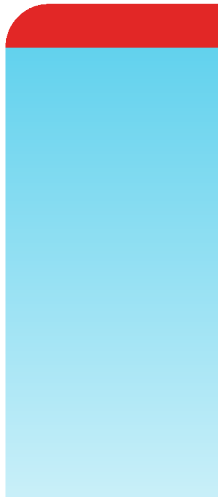


Deployment Guide

FortiSOAR 7.0.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

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



June, 2021

FortiSOAR 7.0.0 Deployment Guide

00-400-000000-20210113

TABLE OF CONTENTS

Change Log	5
Introduction	6
Purpose	6
Prerequisites	6
Browser Compatibility	6
Deploying FortiSOAR	7
Planning	8
Recommended Resource Requirements	8
Credentials	9
Requirements	9
Port Requirements	9
Importing the FortiSOAR Virtual Appliance	10
Deploying the FortiSOAR Virtual Appliance	10
Deploying the FortiSOAR Virtual Appliance using vSphere or vCenter	10
Deploying the FortiSOAR Virtual Appliance using AWS	11
Deploying FortiSOAR using KVM	11
Installing FortiSOAR 7.0.0 using the FortiSOAR installer	15
Prerequisites	16
Procedure	16
Installing the secure message exchange	18
FortiSOAR Configuration Wizard	18
Interactive VM configuration	18
Non-interactive VM configuration	20
Pointing the ntpd service to a valid ntp server	21
Editing the VM configuration	21
Setting a static IP	21
Determining your DHCP IP address	24
Deploying FSR Agents	24
Architecture	25
Recommended Resource Requirements for Virtual Machines (VM)	25
Prerequisites for installing a FSR agent	25
Process of setting up a FSR agent	26
Adding a FSR agent	28
Installing a FSR agent	30
Deboarding FSR Agents	31
Moving a FSR agent to a new secure message exchange	31
Licensing FortiSOAR	33
FortiSOAR licensing process	34
FortiSOAR licensing using FortiManager	35
Retrieving the FortiSOAR Device UUID	37
Deploying the FortiSOAR license	38
Deploying the FortiSOAR license using the FortiSOAR UI	38
Deploying the FortiSOAR license using the FortiSOAR Admin CLI	39
Activating the FortiCare Trial license for FortiSOAR	39

License Manager Page	40
Updating your license using the FortiSOAR UI	43
Troubleshooting licensing issues	43
Troubleshooting issues while deploying the FortiSOAR license in a proxy environment	44
Configuring FortiSOAR	45
Logging on to FortiSOAR for the first time	45
Configuring SMTP for FortiSOAR	46
Creating your first user and record	46
Additional configuration settings for FortiSOAR	48
Changing the hostname	48
Updating the SSL certificates	48
Setting up monitoring for your FortiSOAR system	49
Setting up system monitoring	49
Setting up purging for audit and playbook logs	50
Configuring High Availability or Disaster Recovery options	50
Starting and stopping FortiSOAR Services	50
Changing the FortiSOAR default database passwords	51
Setting up a proxy server to service all requests from FortiSOAR	51
Configuring Proxy Settings and environment variables	52
Backing up the data encryption keys	53
Configuring a reverse proxy (Apache proxy server)	53
Troubleshooting FortiSOAR Issues	55
Issues occurring in FortiSOAR due to insufficient space	55
Troubleshooting Deployment Issues	58
The FortiSOAR Virtual Appliance deployment on ESX is failing	58
Cannot access the FortiSOAR portal	59
Cannot login to the FortiSOAR platform	59
Getting a 502 error when you click on the Reports tab	59
Troubleshooting Upgrade Issues	59
Post license renewal you cannot log into FortiSOAR	60
Failure to upgrade FortiSOAR	60
Post-upgrade your playbooks fail to execute, and the playbooks are also not listed in the executed playbooks log	60
Login and logout events are not audited after you have upgraded your FortiSOAR version	61
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	61

Change Log

Date	Change Description
2021-04-23	Initial release of 7.0.0
2021-06-03	Added a note to the 'Deploying the license using the Admin CLI' section in the Licensing FortiSOAR chapter.
2021-08-09	Updated FortiSOAR licensing process section with respect to Device UUID information in the Licensing FortiSOAR chapter.

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

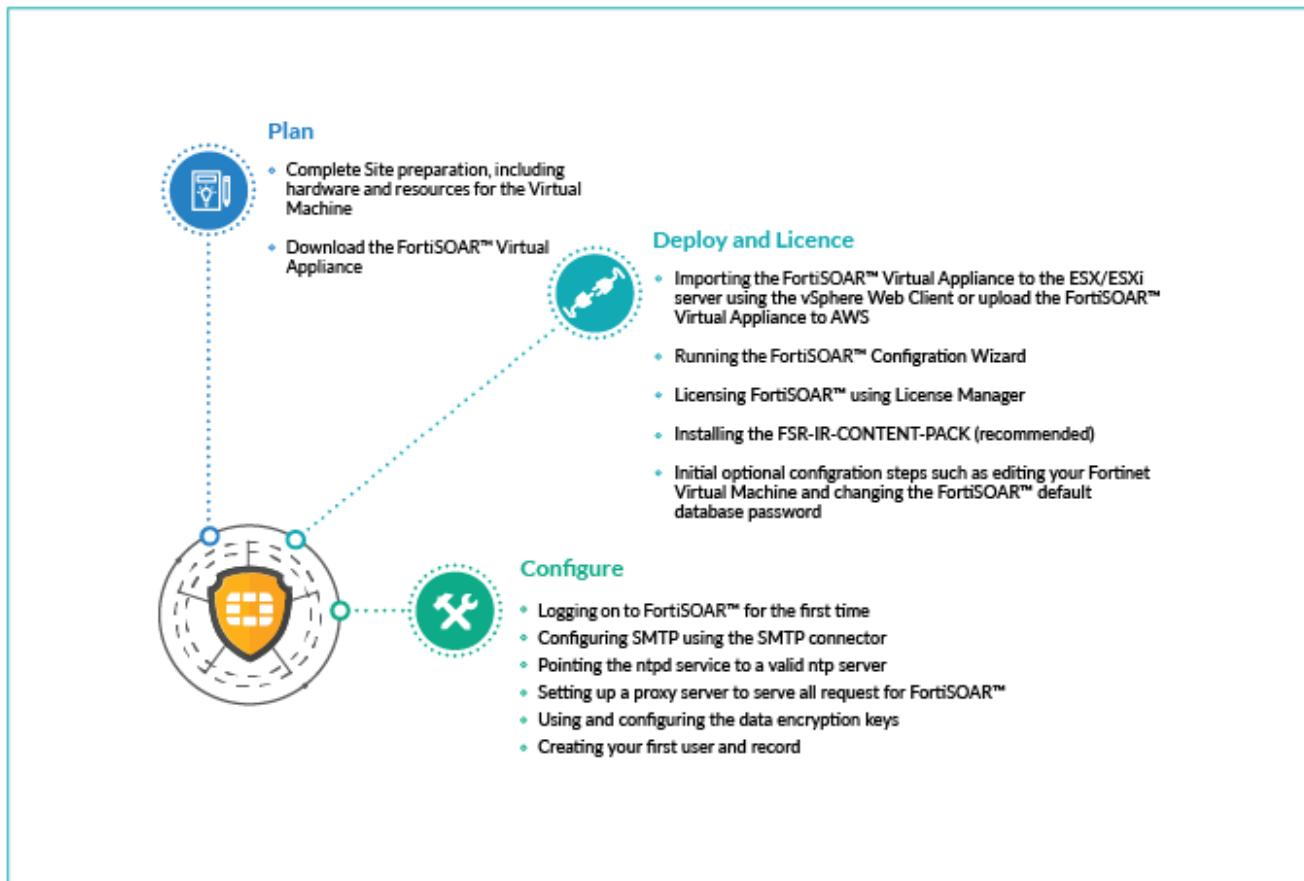
FortiSOAR 7.0.0 User Interface has been tested on the following browsers:

- Chrome version 89.0.4389.114
- Firefox version 87.0
- Internet Explorer Edge version 89.0.774.68

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 7.0.0 using the FortiSOAR installer (.bin file). For more information, see [Installing FortiSOAR 7.0.0 using the FortiSOAR installer](#).

Planning

Recommended Resource Requirements

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.

Supported Hypervisors

- AWS AMI
- VMware ESXi versions 5.5, 6.0, and 6.5
- Redhat KVM

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 7.0.0 onwards, on first FortiSOAR login, password change is mandated for the 'csadmin' users.

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://update.cybersponse.com>

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.

Deploying the FortiSOAR Virtual Appliance

Before you begin the deployment process, ensure that your VM is configured as per the specifications outlined in the *Planning* section.

Deploying the FortiSOAR Virtual Appliance using vSphere or vCenter

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):

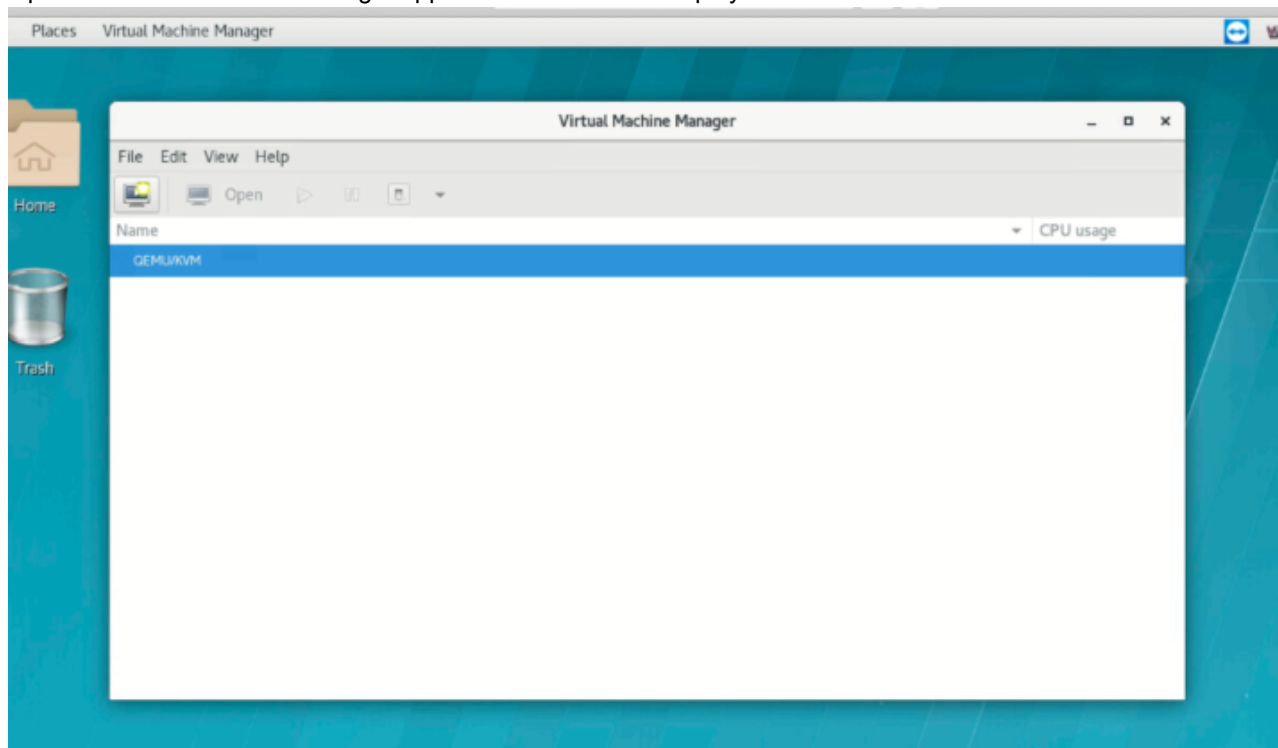
1. Log into your AWS account and upload the FortiSOAR Virtual Appliance to Amazon Web Services (AWS).
2. From the Amazon EC2 console dashboard, choose **Launch Instance**, to launch the FortiSOAR instance.
3. On the **Choose an Amazon Machine Image (AMI)** page, choose the AMI and start configuring the instance.

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.

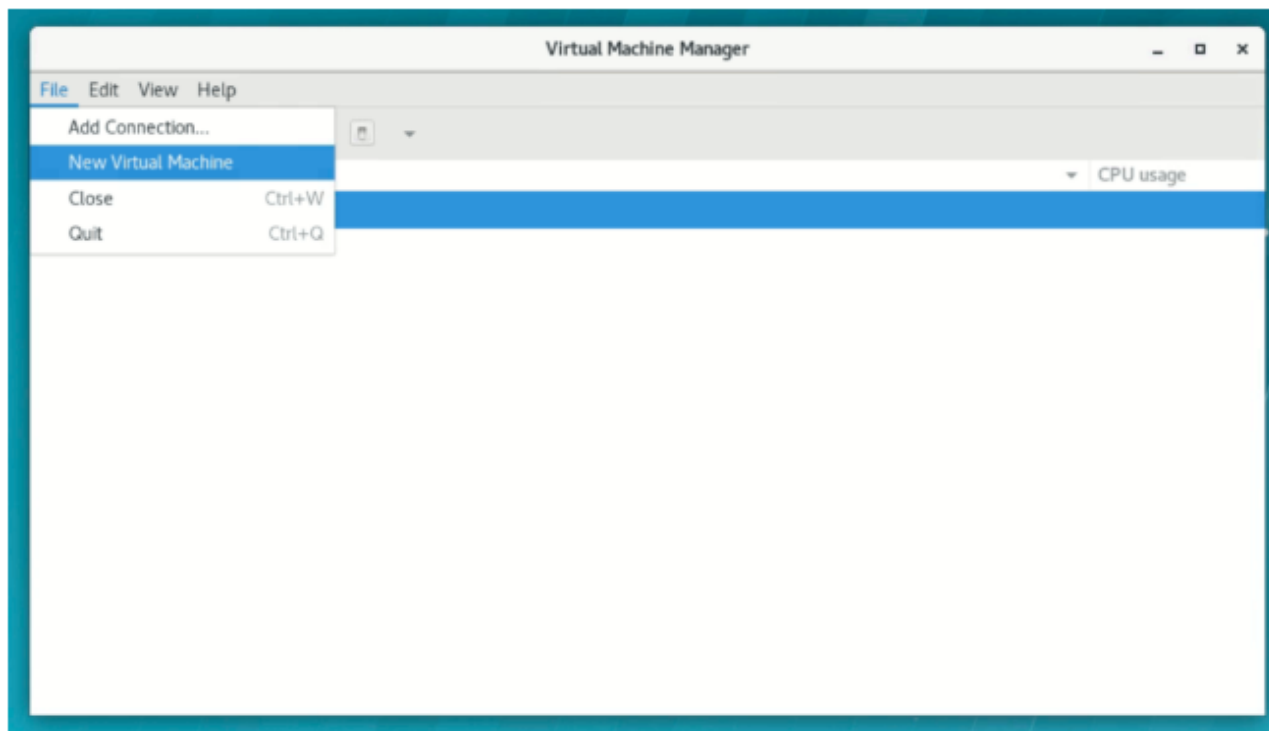
Deploying FortiSOAR using KVM

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

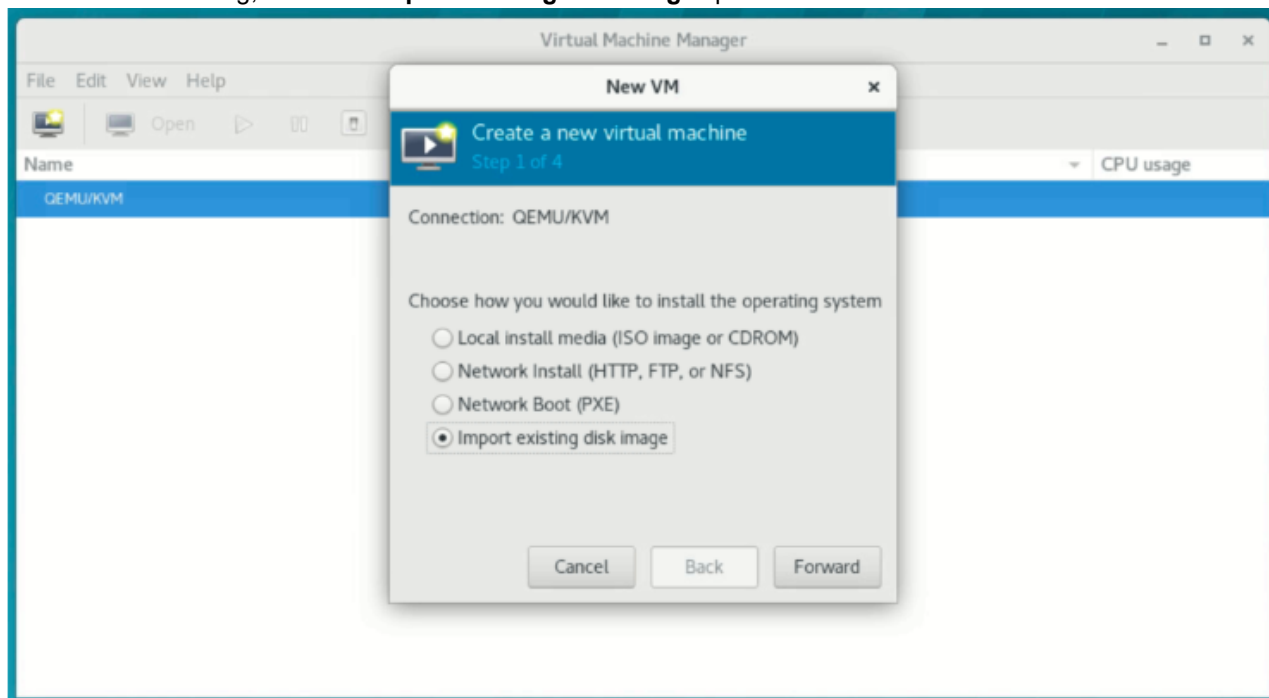
1. Download the KVM-Supported QCOW2 image from support.fortinet.com.
2. Copy the FortiSOAR QCOW2 image to the VM Image Datastore.
3. Open the Virtual Machine Manager application for KVM VM deployment.



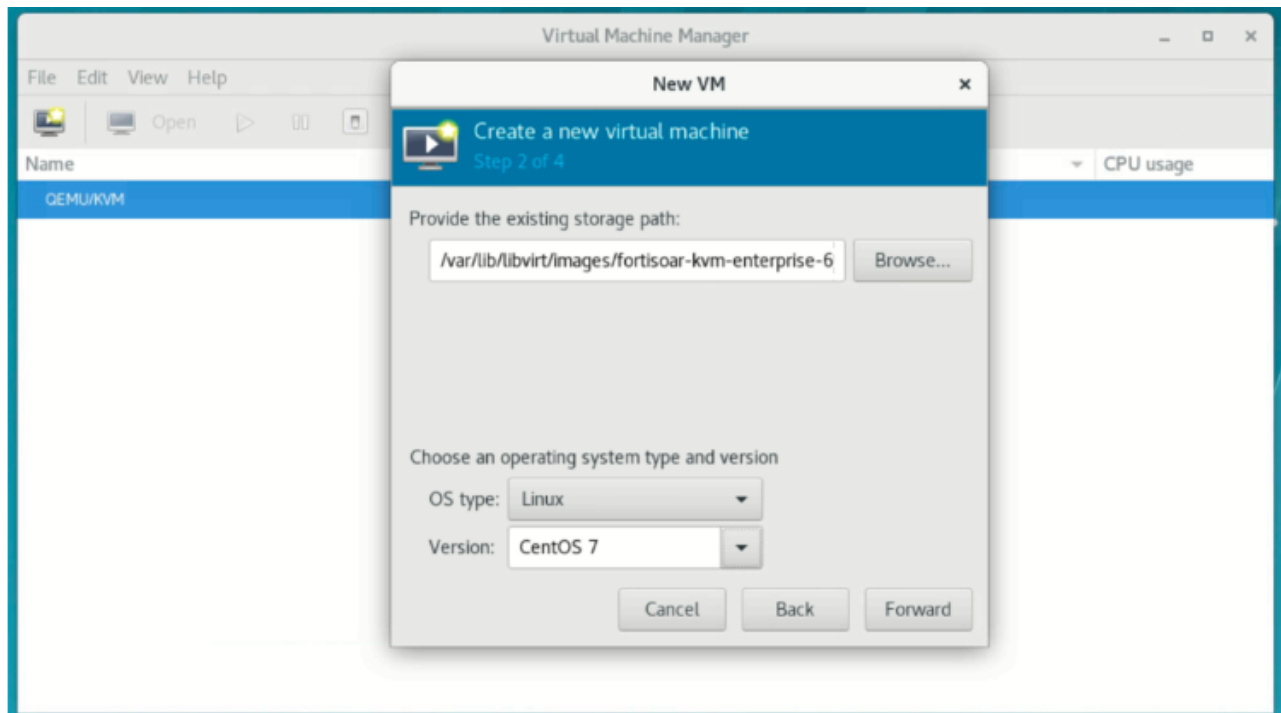
4. Click **File > New Virtual Machine**.



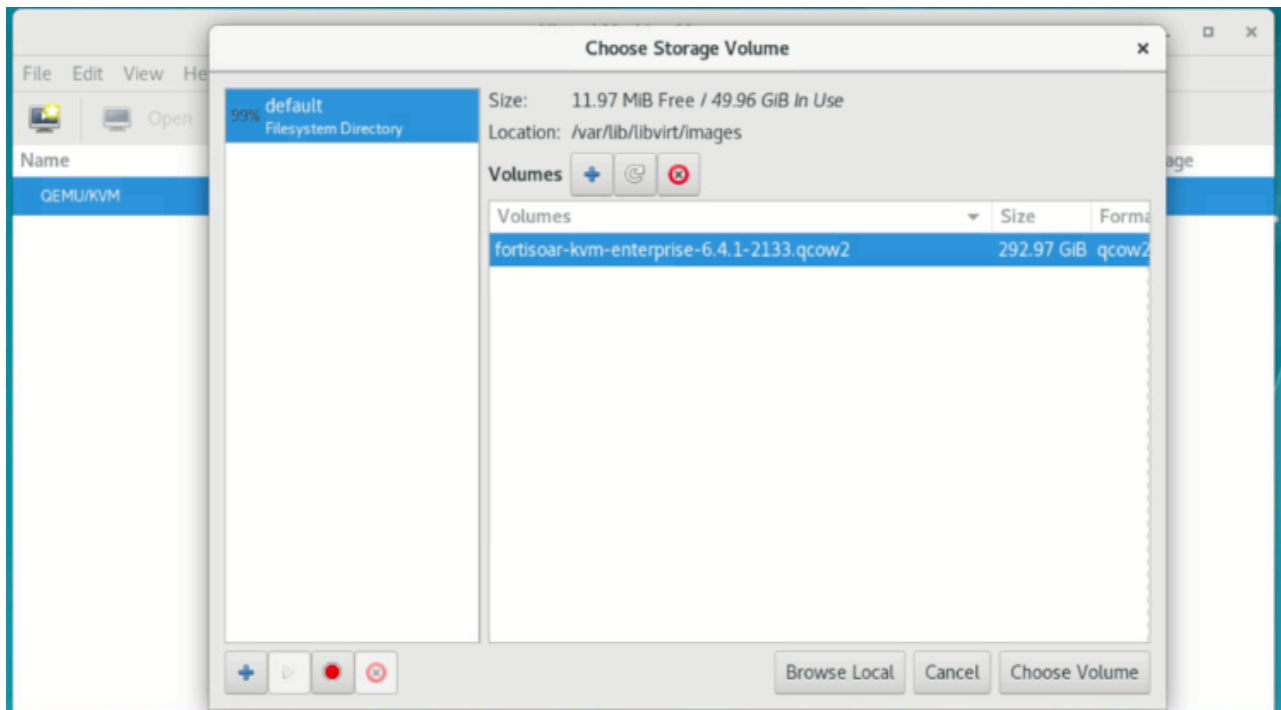
5. On the New VM dialog, select the **Import existing disk image** option and click **Forward**.



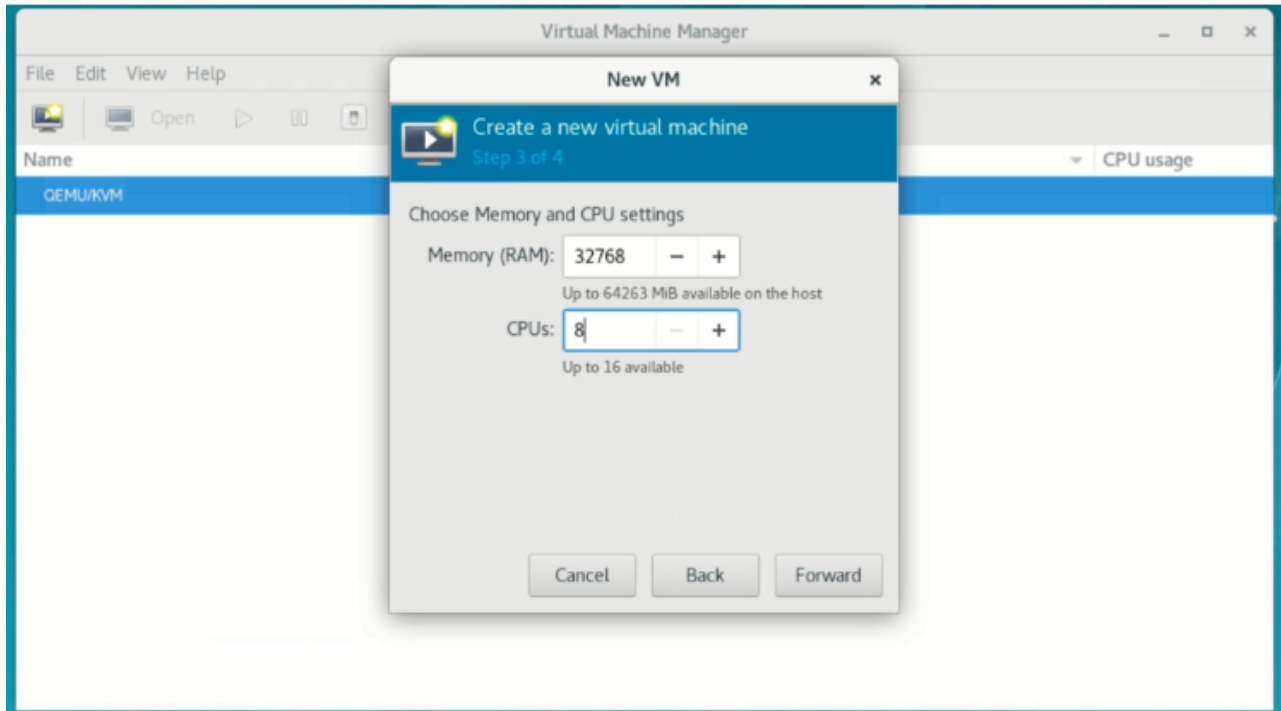
6. Click **Browse** and select the FortiSOAR image from the Image Datastore, select the **OS type** as **Linux** and **Version** as **CentOS 7**, and click **Forward**.



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

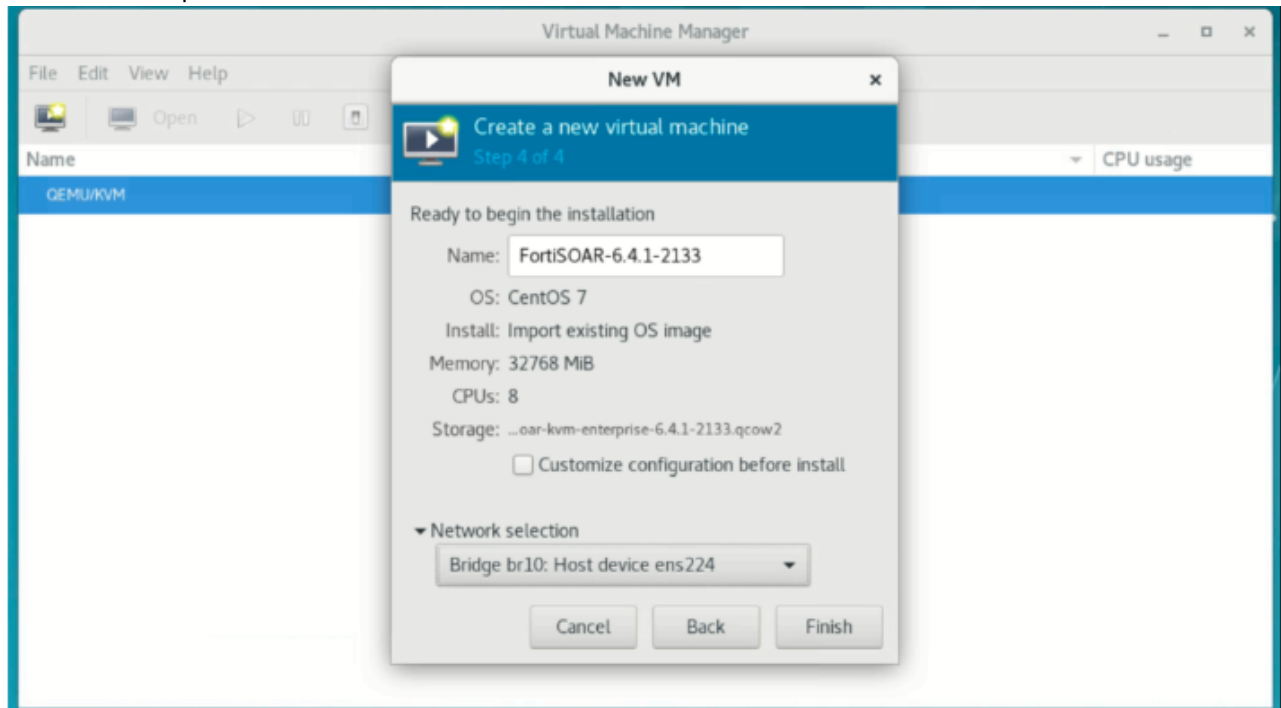


7. Enter 32768 (i.e. 32768 MB=32 GB) in the **Memory (RAM)** field and 8 in the **CPUs** field and click **Forward**.

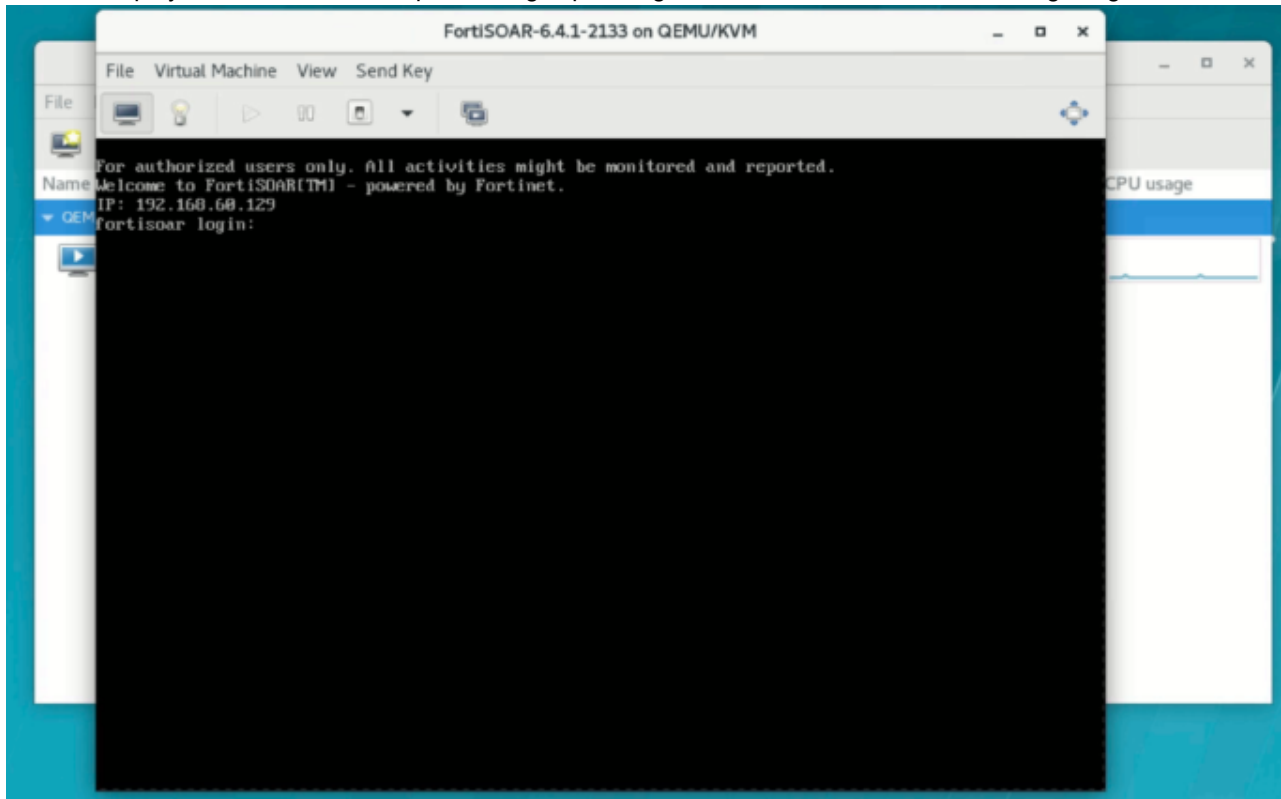


8. Enter the name that you want to specify for the new virtual machine in the **Name** field, select the correct network adapter for this new virtual machine from the **Network Selection** field, and click **Finish** to complete the deployment.

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 7.0.0 using the FortiSOAR installer

This section describes the steps that you require to follow to install FortiSOAR 7.0.0 on a plain CentOS system that has minimal skew selected while installing CentOS.

Prerequisites

Before you begin this procedure, ensure that you can access update.cybersponse.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=update.cybersponse.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://update.cybersponse.com/prod/connectors/deps/simple/`
`proxy='http://username:password@10.1.1.0:8080'`

Procedure

The following procedure describes the steps that you require to run for installing FortiSOAR 7.0.0 Enterprise Edition and Secure Message Exchange:

1. Provision a CentOS 7 (minimal) VM [recommended version 7.7.1908 (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 7.0.0:
`# wget https://update.cybersponse.com/7.0.0/install-fortisoar-7.0.0.bin`
5. To install FortiSOAR 7.0.0 run the following command as a root user:
`# sh install-fortisoar-7.0.0.bin`
 OR
`chmod +x install-fortisoar-7.0.0.bin`
`./install-fortisoar-7.0.0.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](https://globalupdate.fortinet.net) 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 credentials:
Username: `csadmin`
Password: `changeme`
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`

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 7.7.1908 (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 7.0.0 secure message exchange:

```
wget https://update.cybersponse.com/7.0.0/install-fortisoar-7.0.0.bin
```

5. To install FortiSOAR 7.0.0 secure message exchange run the following command as a root user:

```
# sh install-fortisoar-7.0.0.bin
```

OR

```
chmod +x install-fortisoar-7.0.0.bin
```

```
./install-fortisoar-7.0.0.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.

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: (Optional) You can change the hostname for your FortiSOAR VM. 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. **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]`
3. **Update network configuration:** This is an automatic process.
4. **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.
5. **Generate certificates:** This is an automatic process; you do not require to provide any inputs.
6. **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.
7. **Reset database passwords:** This is an automatic process to reset database password to a new password unique to your instance.
8. **Restart services:** This is an automatic process to reset all FortiSOAR services.
9. **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.
10. **Install python libraries:** This is an automatic process to install some python libraries required by FortiSOAR.

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.

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. The configuration in this case is done by using the default inputs from the configuration file that is shipped along with the FortiSOAR appliance. Non-interactive VM configuration is useful when users are expecting a ready-to-use appliance.

The default configuration files are:

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

You can customize the non-interactive VM configuration by providing additional custom configuration files. Values provided in the custom configuration files overrides the ones mentioned in the default 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 to 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` are applicable to only the 'Enterprise' edition
- The `static_ip`, `gateway`, `netmask`, `dns1`, and `dns2` keys are considered only in 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 are not applicable 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.

Once your system is appropriately deployed, it is recommended that you install the Content Pack (FSR-IR-CONTENT-PACK). The Content Pack enables users to experience the power of FortiSOAR incident response, both automated and manual, without having to configure FortiSOAR to ingest any data. With out-of-box (OOB) demo records and their corresponding playbooks that demonstrate various use cases along with best practices to combat various types of incidents. From version 7.0.0 onwards, you can install the content before deploying your FortiSOAR license. For more information on the Content Pack, see the [Content Pack](#) article present in the Fortinet Knowledge Base.

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.

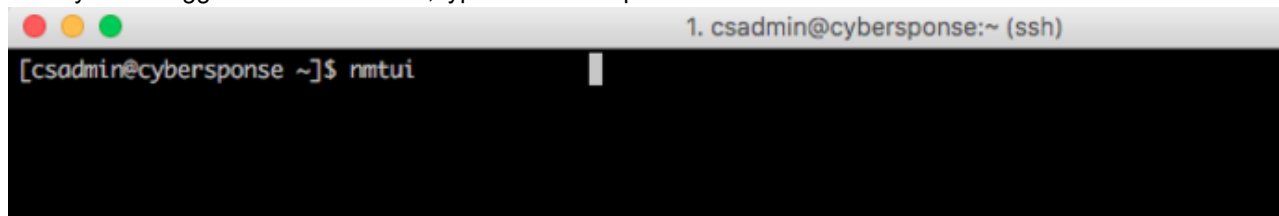
Editing the VM configuration

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

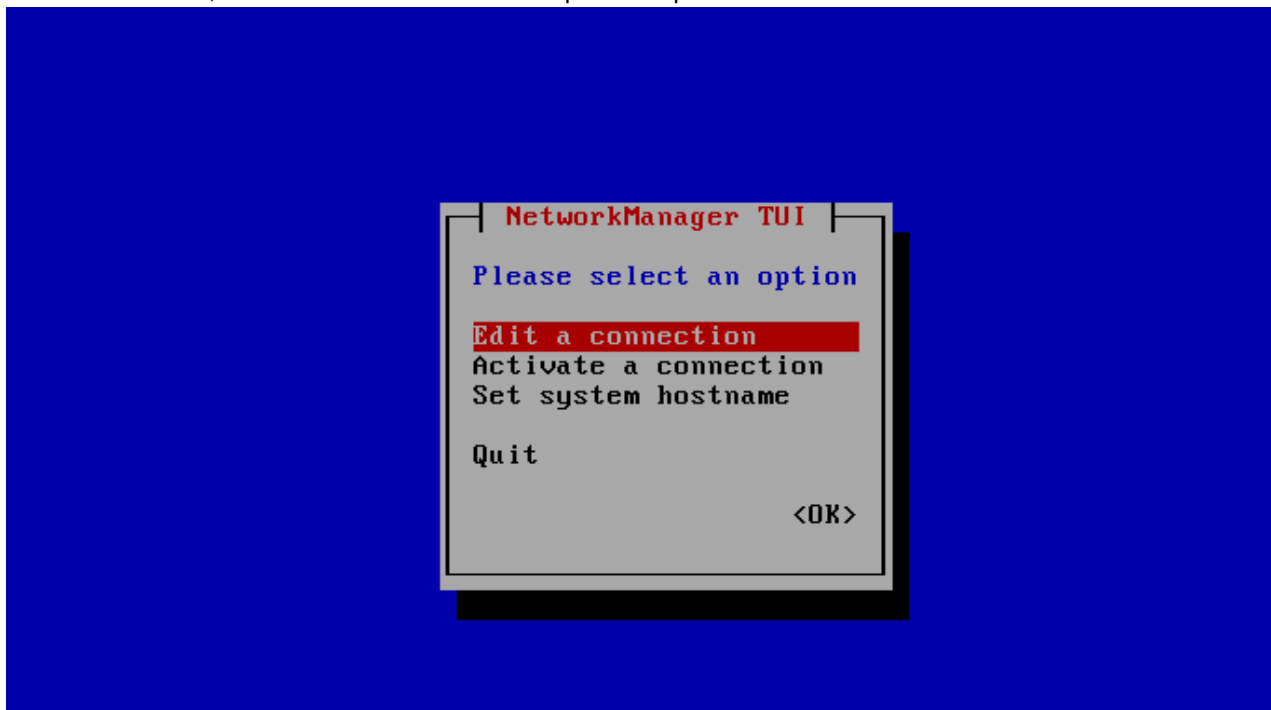
1. Setting a static IP
2. Determining your DHCP IP Address

Setting a static IP

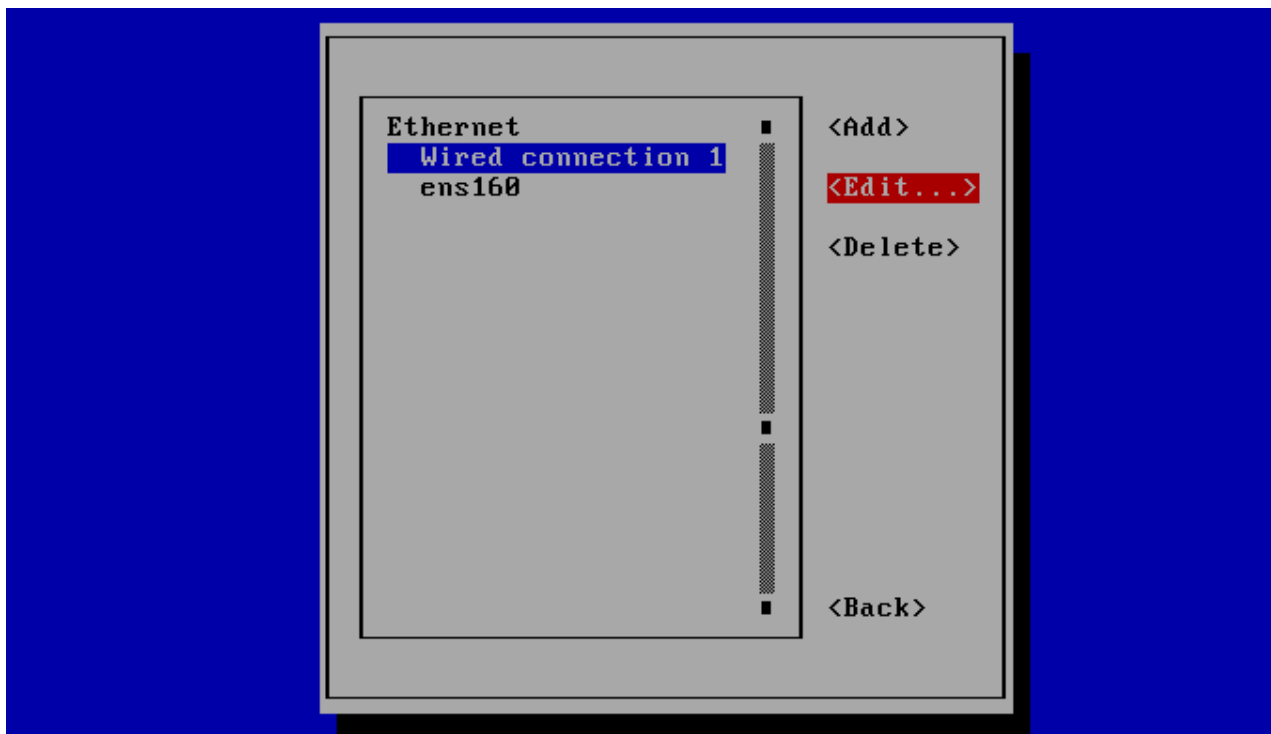
1. On the ESX console for your FortiSOAR VM, login to the VM as the `csadmin` user.
2. Type `sudo -i` in the terminal and press `Enter` to become a root user.
3. Once you are logged in to the terminal, type `nmtui` and press `Enter`.



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' window. At the top, the title bar says 'Edit Connection'. Below it, the 'Profile name' is 'Wired connection 1' and the 'Device' is '00:0C:29:EE:75:35 (ens160)'. There are two expandable sections: '= ETHERNET' with a '<Show>' button, and '= IPv4 CONFIGURATION <Manual>' with a '<Hide>' button. The IPv4 section is expanded, showing fields for 'Addresses' (192.168.1.10/32), 'Gateway' (192.168.1.1), 'DNS servers' (192.168.1.1), and 'Search domains' (cs.local). Each field has a '<Remove>' button and a '<Add...>' button. Below these fields is a 'Routing' section with the text '(No custom routes) <Edit...>' and four checkboxes: 'Never use this network for default route', 'Ignore automatically obtained routes', 'Ignore automatically obtained DNS parameters', and '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.

The screenshot shows the 'Edit Connection' window. The title bar says 'Edit Connection'. Below it, the 'Gateway' is '192.168.1.1', 'DNS servers' is '192.168.1.1', and 'Search domains' is 'cs.local'. Each field has a '<Remove>' button and a '<Add...>' button. Below these fields is a 'Routing' section with the text '(No custom routes) <Edit...>' and three checkboxes: 'Never use this network for default route', 'Ignore automatically obtained routes', and 'Require IPv4 addressing for this connection'. Below the routing section is an expanded section '= IPv6 CONFIGURATION <Automatic>' with a '<Show>' button. This section contains two checkboxes: '[X] Automatically connect' and '[X] Available to all users'. At the bottom right, there are '<Cancel>' and '<OK>' buttons.

10. Select <OK> and press Enter.

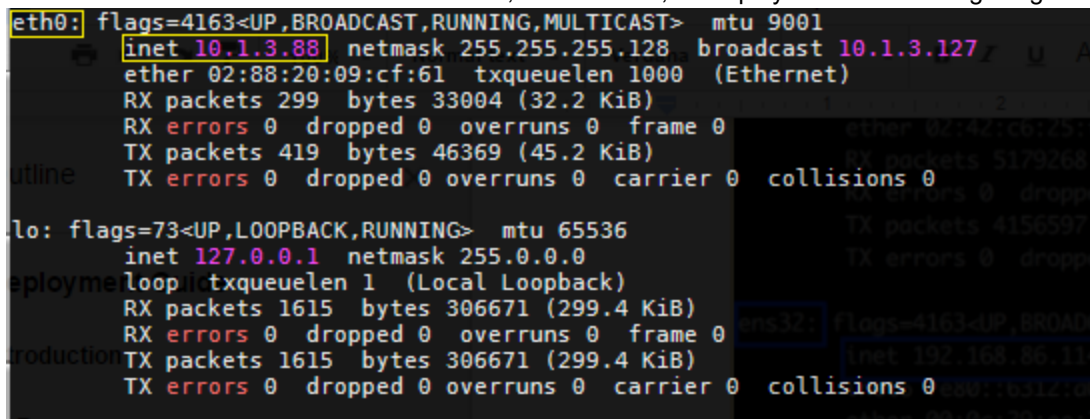
11. Select <Back> and press Enter.
12. Select <OK> and press Enter.
13. Restart the network service using the `systemctl restart network` command.

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:



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.1.3.88 netmask 255.255.255.128 broadcast 10.1.3.127
    ether 02:88:20:09:cf:61 txqueuelen 1000 (Ethernet)
    RX packets 299 bytes 33004 (32.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 419 bytes 46369 (45.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loopback txqueuelen 1 (Local Loopback)
    RX packets 1615 bytes 306671 (299.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1615 bytes 306671 (299.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



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".

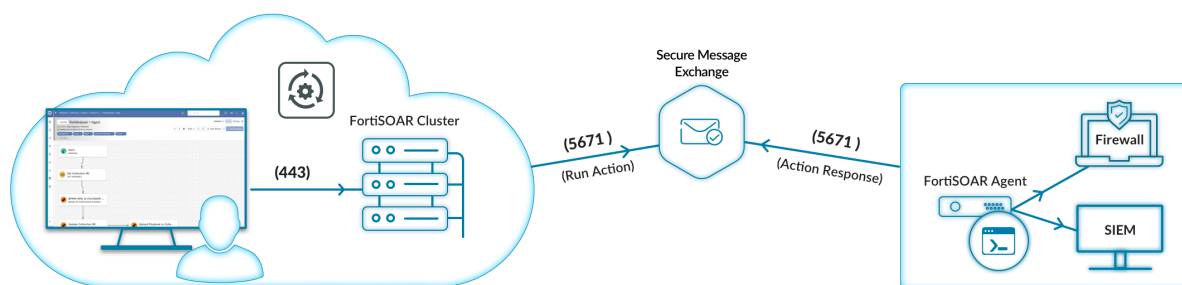
Automated ingestion, enrichment, or triage actions using a SOAR platform require network connectivity to various endpoints on which you want to run connector actions. These devices or endpoints, can at times, be in a different network segment than the one where the FortiSOAR node is deployed. To connect 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.

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 update.cybersponse.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.

The screenshot displays the 'Secure Message Exchanges' configuration page in FortiSOAR. The left sidebar contains the navigation menu with 'Secure Message Exchange' selected. The main content area shows a table with 2 items. The table has columns for Name, Address, API Port, TCP Port, User Name, Certificate, Configuration Status, and Actions. The first item is 'Dev Router' with Address 'secure.router.dev', API Port '15671', TCP Port '5671', User Name 'admin', and Certificate '-----BEGIN CERTIFI...'. The second item is 'Localhost router' with Address 'localhost', API Port '15671', TCP Port '5671', User Name 'admin', and Certificate '-----BEGIN CERTIFI...'. Both items are in 'Configured' status. The Actions column shows 'Refresh' and 'Delete' icons for each item.

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 **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.
- d. 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.
- e. In the **User Name** field, enter the username you will use to login to your secure message exchange as an administrator.
By default, it is set as `admin`.
- f. In the **Password** field, enter the password you will use to login to your secure message exchange as an administrator.
- g. In the **Certificate** field, copy-paste the certificate text of the Certificate Authority (CA) that has signed the secure message exchange certificate in the `pem` format. 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.
- h. To save the configuration for the secure message exchange on the FortiSOAR node, click **Create**.



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. (Optional) In the **Description** field, enter the description of the FSR agent.
 - c. 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.
 - d. 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

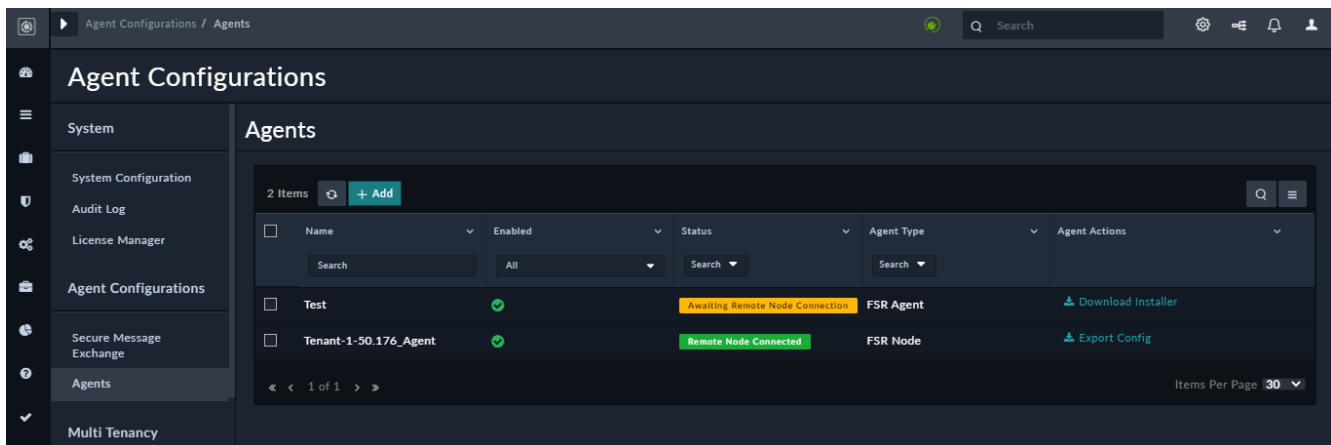
associated as owners of the agent. Teams help in governing RBAC for the FSR agent. While running connector actions using FSR agents, users will only see FSR agents that are associated with their teams.

- e. 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.

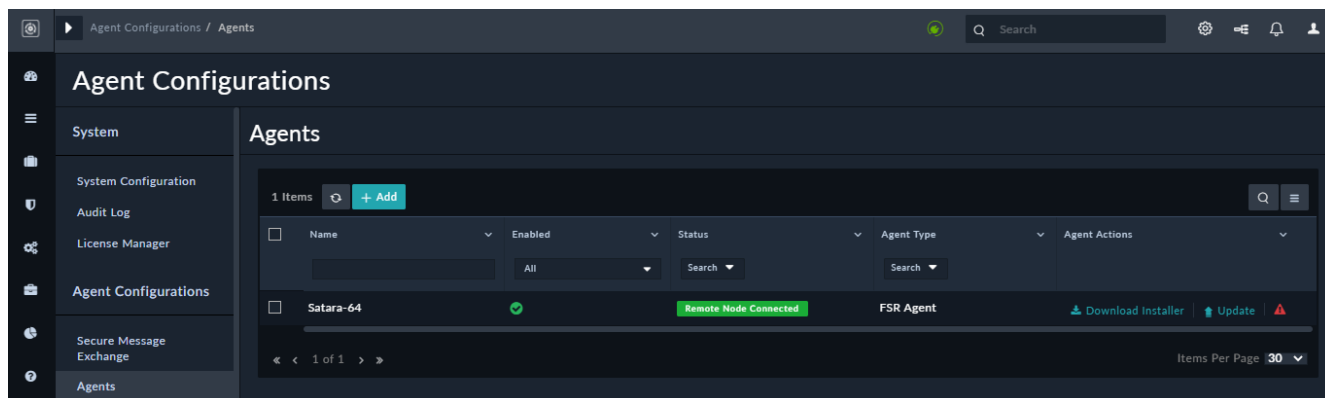
If the connection between the FortiSOAR node and secure message exchange is established, then the `Status` column displays "Awaiting Remote Node Connection" along a **Download Installer** link. Now, you are required to download the FSR agent installer and install the FSR agent as described in the following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

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.

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.



Support to use FortiManager (FMG) as an intermediary in case of a closed or air-gapped environment for FortiSOAR licensing has been validated on 'FortiSOAR Version 6.4.4 - Build 3164' and 'FMG Version 6.4.4 GA-Build 2253'.

In case of an air-gapped environment, do the following:

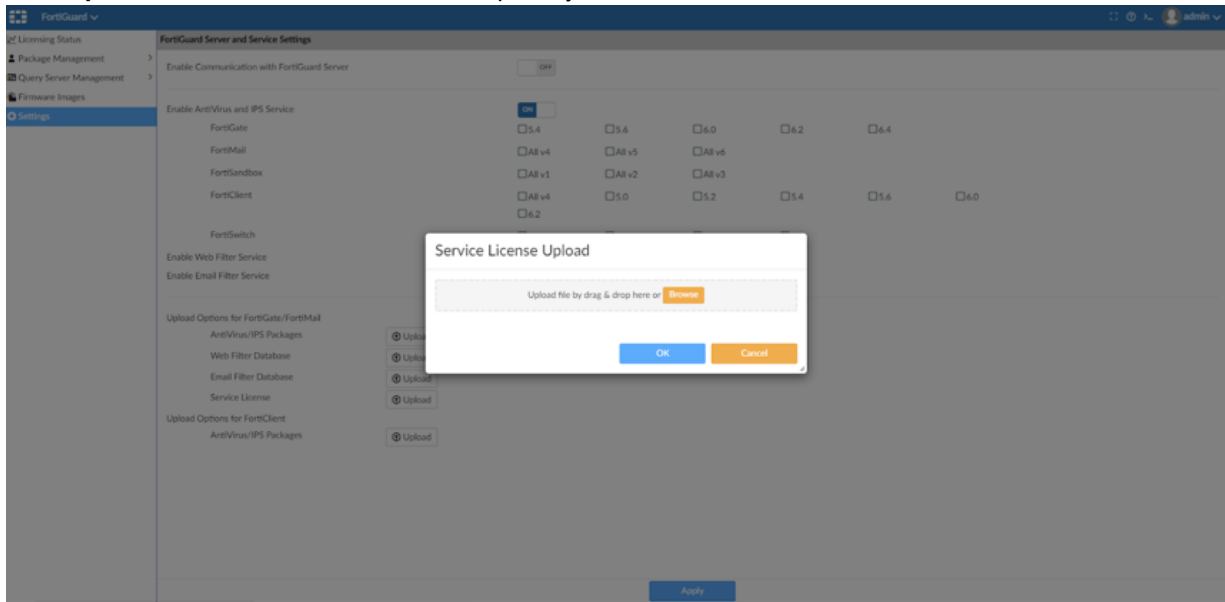
1. You must have an account in FortiManager (FMG).
2. Contact FortiSOAR Customer Support to obtain an entitlement file, which contains all the contract details.
3. Log onto FMG and navigate to FortiGuard.
4. On the left-menu, click **Settings**, and apply the following settings:
 - a. "Toggle OFF" the **Enable Communication with FortiGuard Server** setting.

The screenshot shows the FortiGuard Server and Service Settings page. The 'Enable Communication with FortiGuard Server' toggle is set to OFF. Below this, the 'Enable AntiVirus and IPS Service' toggle is set to ON. The page lists various services and their configurations:

- FortiGate:** 5.4, 5.6, 6.0, 6.2, 6.4
- FortiMail:** All v4, All v5, All v6
- FortiSandbox:** All v1, All v2, All v3
- FortiClient:** All v4, 5.0, 5.2, 5.4, 5.6, 6.0
- FortiSwitch:** 5.4, 5.6, 6.0, 6.2
- Enable Web Filter Service:** OFF
- Enable Email Filter Service:** OFF
- Upload Options for FortiGate/FortiMail:** Packages and Database (Upload), Service License (Upload)
- Upload Options for FortiClient:** AntiVirus/IPS Packages (Upload)

An 'Apply' button is located at the bottom right of the settings area. A Windows activation notice is visible in the bottom right corner of the interface.

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



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

5. Ensure that FMG is reachable or resolvable from your FortiSOAR instance.
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](#).

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



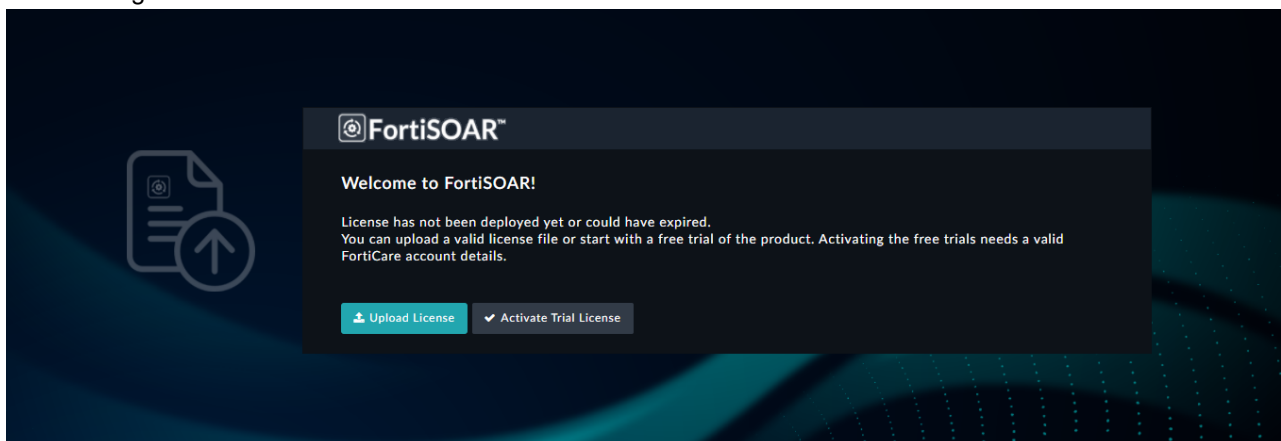
Before you start deploying your FortiSOAR license, you must ensure that you can connect to <https://globalupdate.fortinet.net>, else the license deployment will fail. Connectivity to this address is required for fetching the license entitlements and product functioning post-upgrade.

Deploying the FortiSOAR license using the FortiSOAR UI

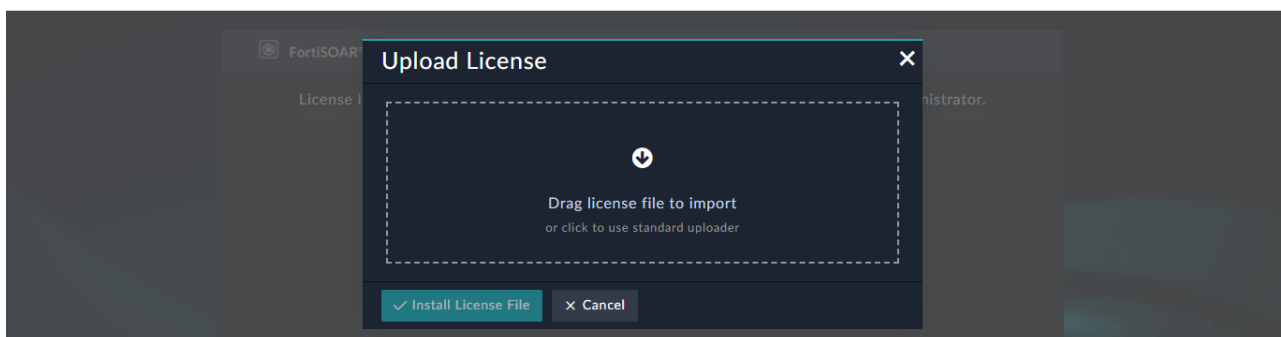
From version 7.0.0 onwards, you can deploy your FortiSOAR license from the FortiSOAR UI itself, without the need to SSH to your FortiSOAR machine. This is extremely useful if the administration does not have ssh access to the FortiSOAR machine.

To deploy the initial FortiSOAR license or to upload a new license, if your FortiSOAR license has expired, using the FortiSOAR UI, do the following:

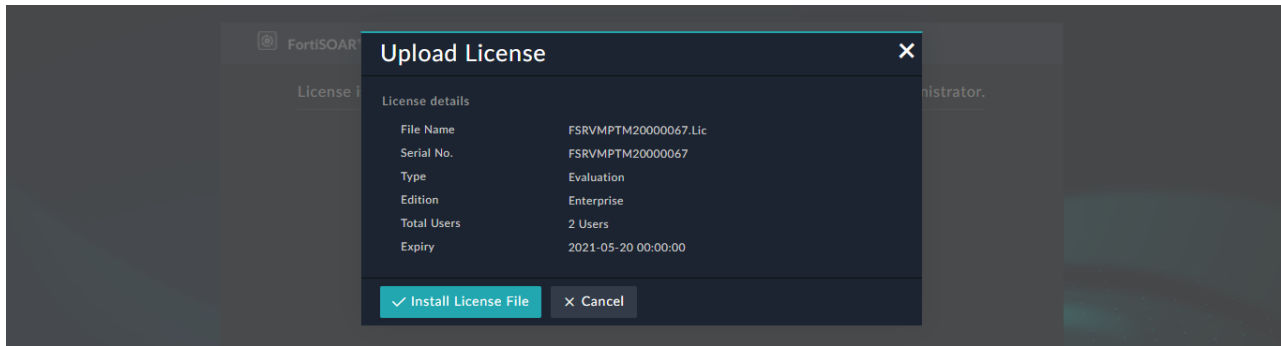
1. In the browser type `https://<YourFortisoarHostname>/login` to open your FortiSOAR UI. This will display the following screen:



2. Click **Upload License** to display the "Upload License" dialog:



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

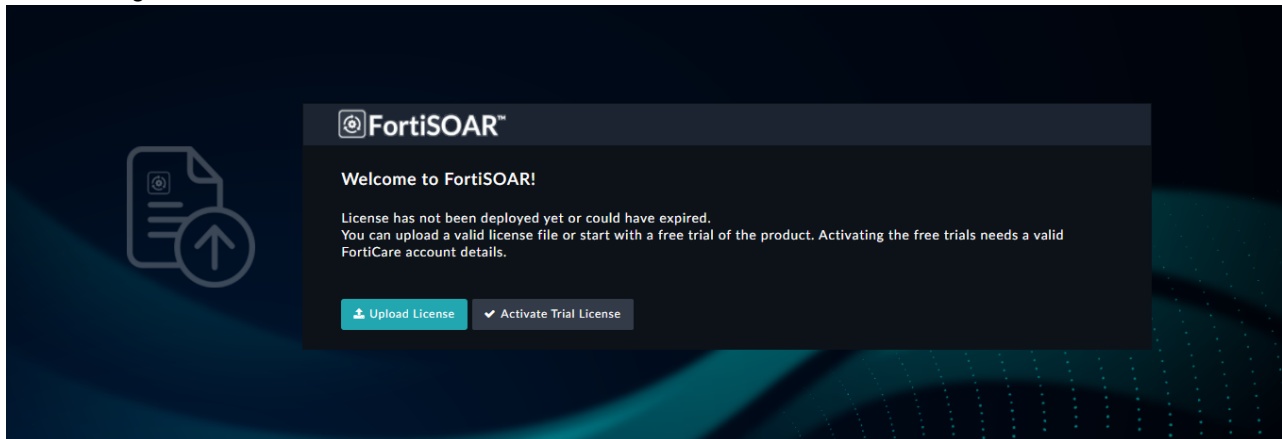
From version 7.0.0 onwards, you get a free trial license for an unlimited time for FortiSOAR per FortiCare account, i.e., if you have a FortiCare account, you can get FortiSOAR for free and for an unlimited time, but in a limited context. This license is an "Enterprise" type license and is restricted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



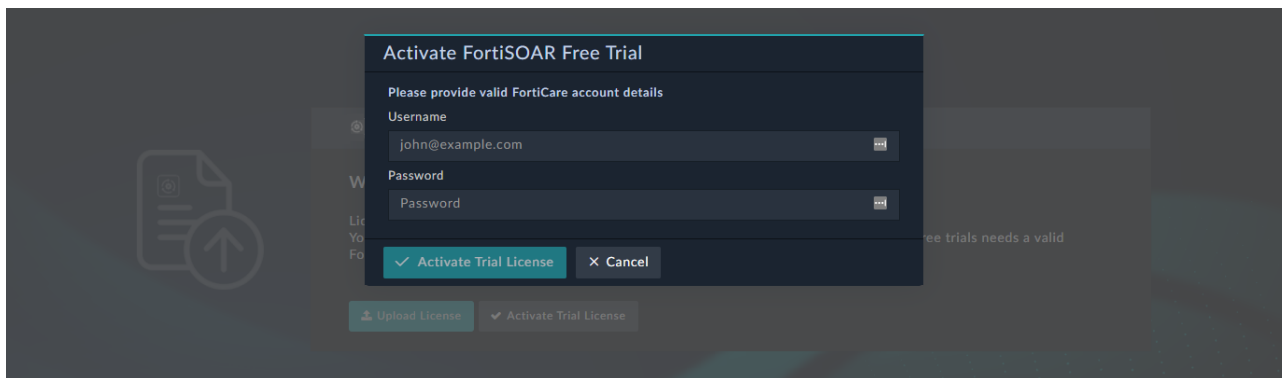
Important steps such as "Create Records", "Update Records", "Find Records", "Connection Actions", etc., are counted towards the maximum action count limit of 200. However, steps used for data manipulation such as "Wait", "Approval", "Loops", "Reference a Playbook", etc. are not counted towards the action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

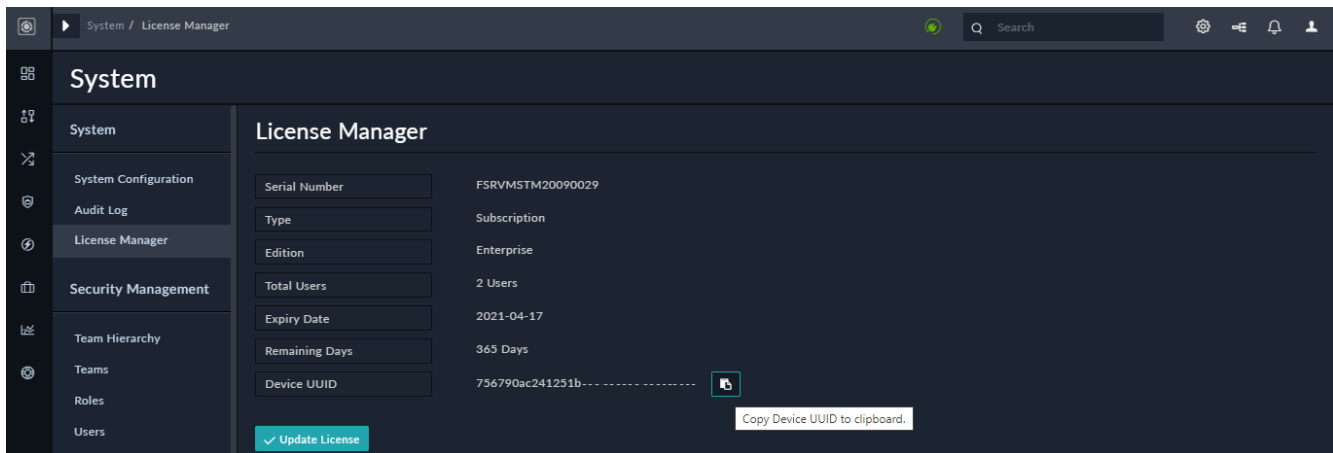


If the email address and password provided are correct, then your FortiCare trial license for FortiSOAR is activated.

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

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

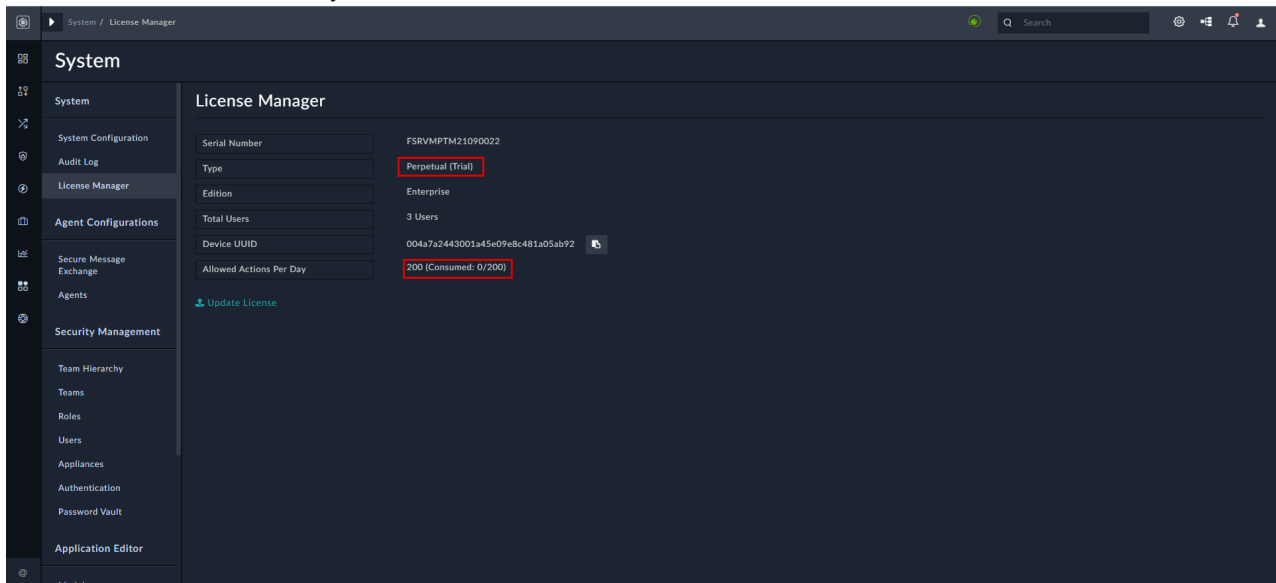


The `License Manager` page displays the serial number, type and edition of the license issued, the total number of users FortiSOAR is licensed for, the date when the FortiSOAR license will expire, the number of days till the expiry of the FortiSOAR license, and your Device UUID. You can click the **Copy Device UUID** button to copy your Device UUID.

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.

Total Users displays the number of active users that can use FortiSOAR. You cannot create more active users, in your FortiSOAR environment, than the value specified in this field. For example, if the Total Users field is set to 50, you cannot create a 51st active user in FortiSOAR.

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.

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:

The screenshot shows the FortiSOAR web interface. On the left is a sidebar menu with options like System Configuration, Audit Log, License Manager (selected), Agent Configurations, Secure Message Exchange, Agents, Security Management, Team Hierarchy, Teams, Roles, Users, Appliances, and Authentication. The main content area is titled 'License Manager' and contains two sections: 'System' and 'Nodes'.

The 'System' section displays the following license details:

Field	Value
Type	Evaluation
Edition	Enterprise
Total Users	7 Users
Expiry Date	2021-11-10
Remaining Days	358 Days

The 'Nodes' section contains a table listing the nodes in the HA cluster:

Node Name	Status	Role	License Details
node3.fortisoar.net	Active	Secondary	Serial Number: FSRVMPTM20000417 Total Users: 2 Expiry Date: 2021-11-10 Device UUID: 2db59a5d1c3cd352f4242069e598730d Update License
node1.fortisoar.net	Active	Secondary	Serial Number: FSRVMPTM20000415 Total Users: 2 Expiry Date: 2021-11-10 Device UUID: 3d7396b960720f330b65ceb291bd88e1 Update License
node2.fortisoar.net	Active	Primary	Serial Number: FSRVMPTM20000416 Total Users: 7 Expiry Date: 2021-11-10 Device UUID: 1c7b4990e6618fde3fb74a646c8ebd05 Update License

As shown in the above image, the primary node is Node 2 and that node is licensed with 7 users, therefore the total user 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."

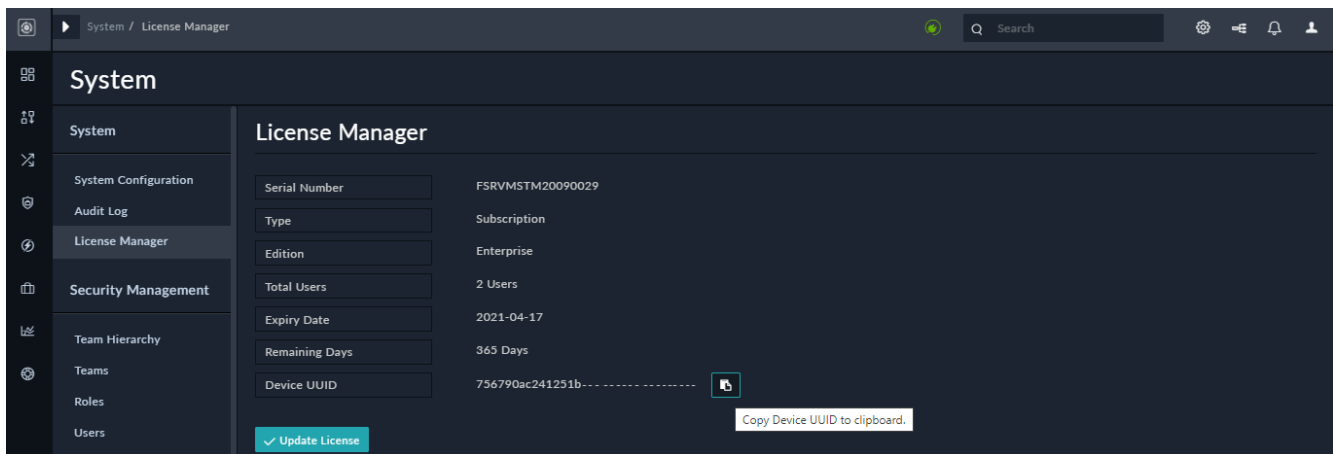
You can update the license for each node by clicking **Update License** and uploading the license for that node as described in the following section.



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.

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.license
=====
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 /opt/cyops-auth/bin/fdnclient.jar <serial_no> 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.

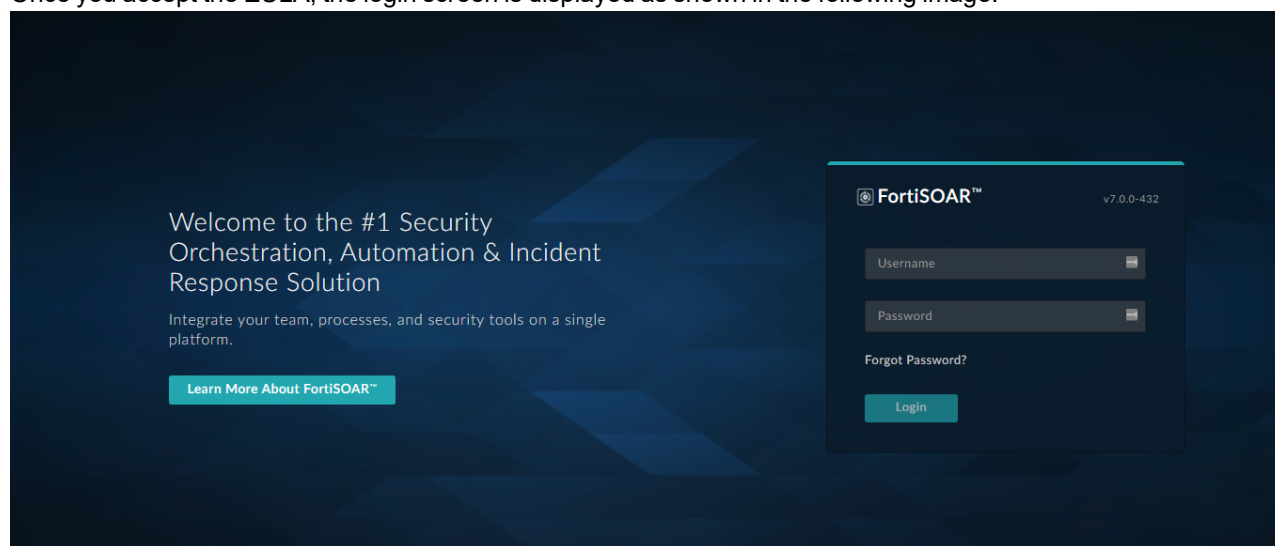
Logging on to FortiSOAR for the first time

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

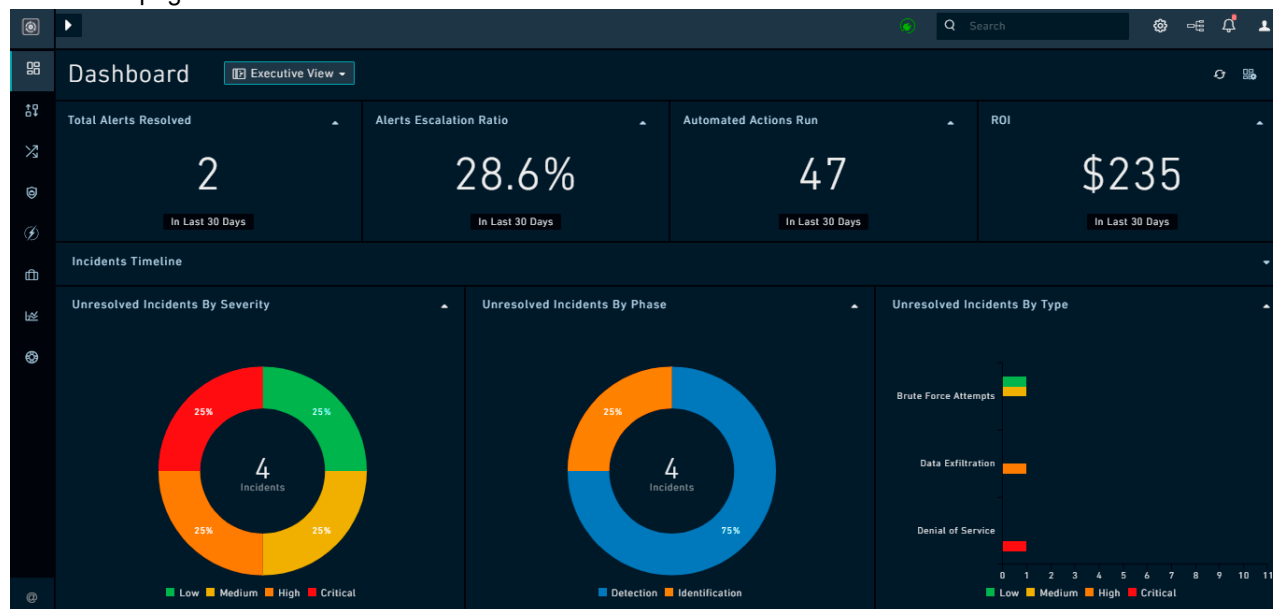
The UI password of the 'csadmin' user for AWS is set to the "instance_id" of your instance. To know the instance ID of your FortiSOAR AWS instance, you can SSH and run the `cloud-init query instance_id` command.

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. 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

You must configure the SMTP connector 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 "Beginners Tutorial to FortiSOAR for Administrators."

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.

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.

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://update.cybersponse.com>
- For installing python dependencies for connectors: <https://pypi.python.org>
Note: There is a parallel python repository also on update.cybersponse.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.



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.

1. 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>
```

2. On the FortiSOAR server perform the following steps:

- a. Update the `crud_hub` host with the `<FortiSOAR-URL>` in the `/etc/cyops/config.yml` file as shown in the following example:
 update `crudhub_host` to `https://<FortiSOAR-url>`
 Example: `crudhub_host: https://demo.fortinet.com`
Important: The `<FortiSOAR-URL>` must match with the SSL certificate Alternate DNS name.
- b. Restart all the FortiSOAR services by using `csadm` and running the following command as a *root* user:

```
# csadm services --restart
```

 After all the FortiSOAR services have been successfully restarted, you should be able to load all the modules using the reverse proxy server.

Troubleshooting FortiSOAR Issues

This section covers issues that you might face while deploying FortiSOAR, upgrading FortiSOAR, or while using FortiSOAR.

For the procedure on how to upgrade to FortiSOAR 7.0.0, see the *Upgrading a FortiSOAR enterprise instance to 7.0.0* section in the “Upgrade Guide.”

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 following methods:

- 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:

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 -L+20G /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. Move the `resv_space` file from `/var/lib/pgsql/` to `/home/csadmin` using the following command:
`# mv /var/lib/pgsql/resv_space /home/csadmin`
4. Check the disk space in `/var/lib/pgsql/` again:
`# df -h /var/lib/pgsql/`
 You will observe that 1GB of space has been freed.
5. Now you can extend or add space to `/var/lib/pgsql/` using the resolution 1, 2, or 3 mentioned above. You could also truncate workflow logs by running direct database commands with the help of FortiSOAR Support.
 If you have no disk space, then you add a new disk and perform steps mentioned in *Resolution 1*.
 If you have disk space in the volume group, then you can extend the logical group by performing steps mentioned in *Resolution 2*.
 If you have sufficient unallocated space available on an existing disk, then you can extend the logical group by performing steps mentioned in *Resolution 3*.
6. Move the `resv_space` file from `/home/csadmin` back to `/var/lib/pgsql/`:
`# mv /home/csadmin/resv_space /var/lib/pgsql/`

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 7.0.0, see the *Upgrading a FortiSOAR enterprise instance to 7.0.0* 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:


```
psycopg2.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/c
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/app/config/parameters_prod.yml` file set the `id_per_module` parameter to **false**.
2. `cd /opt/cyops-apisudo -u nginx php app/console cache:clear --env=prod`



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.