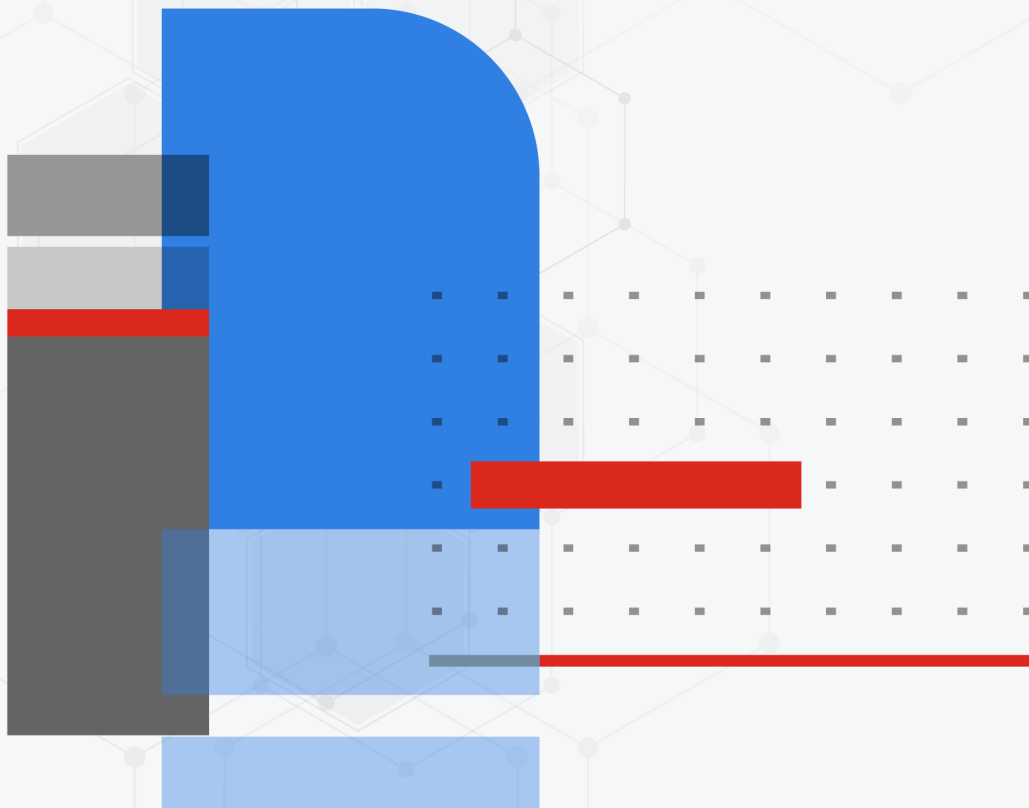




Upgrade Guide

FortiSOAR 7.4.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING 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



October, 2023

FortiSOAR 7.4.2 Upgrade Guide

00-400-000000-20210416

TABLE OF CONTENTS

Change Log	4
Introduction	5
Preparing to Upgrade FortiSOAR	6
Upgrading a FortiSOAR Enterprise Instance	7
Upgrading a FortiSOAR High Availability Cluster	9
Upgrading an Active-Active HA Cluster	9
Upgrading an Active-Passive HA Cluster	9
Upgrading a FortiSOAR Distributed Multi-Tenancy Configuration	11
Upgrading a FortiSOAR master node	11
Upgrading a FortiSOAR Tenant node	11
Upgrading a FortiSOAR Secure Message Exchange	12
Upgrading a FortiSOAR Secure Message Exchange Cluster	13
Troubleshooting upgrade issues for MSSP setups	13
Replication from tenant to master stops once you upgrade an MSSP with an HA setup	13
Upgrading FortiSOAR using the Offline Repository	14
Upgrading your FortiSOAR Docker image and upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster	15
Upgrading your FortiSOAR Docker image	15
Reverting the upgrade on your FortiSOAR Docker image	16
Upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster	17
Post-Upgrade Tasks	18
Change in the default behavior of the On Create, On Update, and On Delete playbooks for MSSP configurations	18
Restart the cyops-integrations-agent service on the tenant nodes for multi-tenant configurations	18
Update the config.ini file to prevent the Jinja Editor from traversing paths	19

Change Log

Date	Change Description
2023-10-14	Updated the Upgrading FortiSOAR using the Offline Repository chapter as an issue is resolved.
2023-10-11	Updated the Upgrading FortiSOAR using the Offline Repository chapter.
2023-10-04	Initial release of 7.4.2

Introduction

This guide covers upgrading a FortiSOAR™ enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration.



The FortiSOAR UI displays a notification when a new release (always the latest) is available. The notification also contains a link to that version's release notes so that you can get details about the latest available release. This keeps FortiSOAR users informed about the latest releases and then users can make informed decisions about upgrading to the latest available FortiSOAR version.

This document describes how to upgrade FortiSOAR to 7.4.2. This guide is intended to supplement the FortiSOAR Release Notes, and it includes the following sections:

- [Preparing to Upgrade FortiSOAR](#)
 - [Upgrading a FortiSOAR Enterprise Instance](#)
 - [Upgrading a FortiSOAR High Availability Cluster](#)
 - [Upgrading a FortiSOAR Distributed Multi-Tenancy Configuration](#)
 - [Upgrading FortiSOAR using the Offline Repository](#)
 - [Upgrading your FortiSOAR Docker image and upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster](#)
-



You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant instance to version 7.4.2 from version 7.4.0 or 7.4.1 only. Also, once you have upgraded your instance, you must log out from the FortiSOAR UI and log back into FortiSOAR.

Also, note that the upgrade procedure temporarily takes the FortiSOAR application offline while the upgrade operations are taking place. We recommend that you send a prior notification to all users of a scheduled upgrade as users are unable to log in to the FortiSOAR Platform during the upgrade.

Before you upgrade your FortiSOAR instance, it is highly recommended that you review the *Special Notices* chapter in the "Release Notes", so that you are aware of operational and breaking changes made in version 7.4.2.

For information on upgrading FortiSOAR using the offline repository and upgrading your FortiSOAR Docker image, see the "Deployment Guide."

To solve common issues that occur during the upgrade process, see the *Troubleshooting FortiSOAR* chapter in the "Deployment Guide."

Preparing to Upgrade FortiSOAR

We recommend performing the following tasks to prepare for a successful FortiSOAR upgrade:

To prepare for upgrading FortiSOAR (summary):

- Ensure that all data ingestion playbooks and schedules are stopped and wait for all existing active playbooks to complete before starting the upgrade process.
- Take a VM snapshot of your current system. Only after you have taken a VM snapshot of your system should you attempt to upgrade FortiSOAR. In case of any failures, these VM snapshots will allow you to revert to the latest working state. Follow the steps mentioned in the documentation of your platform for taking a snapshot and reverting to the current snapshot.
- Take a backup of your FortiSOAR Built-in connectors' (SSH, IMAP, Database, Utilities, etc.) configuration, since the configuration of your FortiSOAR Built-in connectors might be reset, if there are changes to the configuration parameters across versions.
- Execute the `tmux` command to ensure that your `ssh` session does not timeout. 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.
- Ensure that repo.fortisoar.fortinet.com is reachable from your VM. If you are connecting using a proxy, then ensure that proxy details set are correct using the `csadm network list-proxy` command and also ensure that `repo.fortisoar.fortinet.com` is allowed in your proxy. For more information on `csadm` CLI, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."
- Ensure that you have reviewed the *Special Notices* chapter in the "Release Notes", so that you are aware of operational and breaking changes made in version 7.4.2.

Upgrading a FortiSOAR Enterprise Instance

To upgrade your system to FortiSOAR from 7.4.0 or 7.4.1 to 7.4.2, perform the following steps:

1. Users who have `root` access must run the upgrade installer.
2. ssh to the VM that you want to upgrade.
3. Check that you are connected to a `tmux` session. A `tmux` session is needed for situations where network connectivity is less than favorable. You can check your `tmux` session using the following command:

```
# tmux ls
```

This command returns an output such as the following example:

```
0: 1 windows (created Thu Nov 24 09:37:47 2022) [170x47]
```

Log back into the SSH console and run the following command to reattach the `tmux` session:

```
tmux attach-session -t 0
```

4. Run the following command to download the upgrade installer:

```
# wget https://repo.fortisoar.fortinet.com/7.4.2/upgrade-fortisoar-7.4.2.bin
```

Note: If your instance can connect to "repo.fortisoar.fortinet.com" only by using a proxy, then ensure that the proxy is set in the `/etc/wgetrc` file. For example,

```
use_proxy=yes
```

```
http_proxy=<proxy_server_ip:port>
```

```
https_proxy=<proxy_server_ip:port>
```

You can also set the proxy while running the FortiSOAR Configuration Wizard or by using the `csadm network` command.

5. Run the upgrade installer using the following command:

```
# sh upgrade-fortisoar-7.4.2.bin
```

OR

```
# chmod +x upgrade-fortisoar-7.4.2.bin
```

```
# ./upgrade-fortisoar-7.4.2.bin
```

Notes: The FortiSOAR upgrade installer checks for the following:

- The space available in `/tmp` or `/var/temp` (if exist in `/etc/fstab`), which must be at least 500MB. If the space available in `/tmp` or `/var/temp` is less than 500MB, then the upgrade installer exits after displaying an appropriate error message. If you want to skip this space validation check, you can use the `--skip-tmp-validation` option while running the upgrade script:

```
# ./upgrade-fortisoar-7.4.2.bin --skip-tmp-validation
```
- The disk space available in `/boot`, and if the `/boot` has insufficient space, then the upgrade installer exits after displaying an appropriate error message. Use standard methods to remove old kernels and free up space in `/boot`.
- The disk space available in `/var/lib/pgsql` to ensure that you have sufficient disk space for `pgsql`. If you do not have sufficient disk space for `pgsql`, in this case also the upgrade installer exits. In these cases, you must increase the partition size for `/var/lib/pgsql`. For the procedure to increase the partition size, see the 'Issues occurring in FortiSOAR due to insufficient space' section in the *Deployment Troubleshooting* chapter in the "Deployment Guide" for more information.

Once you complete cleaning up `/boot` and/or increasing disk space and space in `/tmp` (as per the messages provided by the upgrade installer) and you have sufficient space for upgrading FortiSOAR, you must re-run the upgrade installer to continue the process of upgrading FortiSOAR.

Important: To upgrade a high availability cluster in FortiSOAR, you require to upgrade each node individually, one after the other. For more information, see the [Upgrading a FortiSOAR High Availability Cluster](#) section. For information on how to upgrade a FortiSOAR distributed multi-tenant configuration to 7.4.2, see the [Upgrading a FortiSOAR Distributed Multi-Tenancy Configuration](#) section.

Note: When you upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-

tenant configuration, the FortiSOAR appliance hostkey also gets changed.

6. Once your FortiSOAR instance is upgraded, you must log out from the FortiSOAR UI and log back into FortiSOAR.

After upgrading FortiSOAR to release 7.4.2 from a release prior to 7.4.2, review the tasks mentioned in the [Post-Upgrade Tasks](#) chapter.



Email notifications that you had set up for your FortiSOAR system or HA cluster for resource consumption after an update to release 7.4.2 or later will not include the system's swap utilization parameter. This change has been done because, even though Elasticsearch performance remained unaffected, the bulk of FortiSOAR upgrades issued notifications concerning swap consumption.

Upgrading a FortiSOAR High Availability Cluster

This section describes the procedure to upgrade a FortiSOAR High Availability (HA) cluster. This section considers that the HA setup has a Reverse Proxy or Load Balancer such as "HAProxy" configured.



Refer to the [Preparing to Upgrade FortiSOAR](#) section and ensure that all the prerequisites mentioned in that section are met. The upgrade installer will handle all FortiSOAR services management.

Upgrading an Active-Active HA Cluster

For the purpose of the following procedure, *Node1* is considered as the Active Primary node, *Node2* is considered as the Active Secondary node. Both the nodes are fronted by a Reverse Proxy or Load Balancer such as "HAProxy".



Approximately 30 minutes of downtime is required for the upgrade.

To upgrade your active-active HA cluster to FortiSOAR 7.4.2, perform the following steps:

1. Configure the Reverse Proxy to pass requests only to *Node1*.
This ensures that FortiSOAR requests are passed only to *Node1*, and *Node2* can be upgraded.
2. Use the `#csadm ha` command as a root user and run the `suspend-cluster` command on *Node2*.
This makes *Node2* a standalone system.
3. Upgrade *Node2* using `upgrade-fortisoar-x.x.x.bin`.
Once the upgrade of *Node2* is completed successfully, you can now upgrade *Node1*.
Important: Upgrade of *Node1* will incur downtime.
4. Once both the nodes are upgraded then run the `resume-cluster` command from *Node2*.
5. Configure the Reverse Proxy again to handle requests from both *Node1* and *Node2*.

Upgrading an Active-Passive HA Cluster

For the purpose of the following procedure, *Node1* is considered as the Active Primary node, *Node2* is considered as the Passive Secondary node. Both the nodes are fronted by a Reverse Proxy or Load Balancer such as "HAProxy".



Approximately 30 minutes of downtime is required for the upgrade.

To upgrade your active-passive HA cluster to FortiSOAR 7.4.2, perform the following steps:

1. Reverse Proxy is configured to have *Node2* as backup system. Therefore, you require to comment out that part from Reverse Proxy configuration.
2. Use the `#csadm ha` command as a `root` user and run the `suspend-cluster` command on *Node2*. This makes *Node2* a standalone system.
3. Upgrade *Node2* using `upgrade-fortisoar-x.x.x.bin`.
Once the upgrade of *Node2* is completed successfully, you can now upgrade *Node1*.
Important: Upgrade of *Node1* will incur downtime.
4. Once both the nodes are upgraded then run the `resume-cluster` command from *Node2*.
5. Configure the Reverse Proxy again to set *Node2* as the backup server.

Upgrading a FortiSOAR Distributed Multi-Tenancy Configuration

This section describes the procedure to upgrade a FortiSOAR distributed multi-tenant configuration for managed security services providers (MSSPs) or Distributed SOC configuration.

You must first upgrade the master node of your FortiSOAR distributed multi-tenant configuration and only then upgrade the tenant nodes of your FortiSOAR multi-tenancy setup.



In case of a distributed deployment, both the master and the tenant nodes must be upgraded. A version mismatch will not work if either of them upgrades to 7.4.2.

In release 7.4.2, the default behavior of the On Create, On Update, and On Delete playbooks is changed to run only on the instance where the record is created. If you want to retain the previous behavior for these playbooks, see the [Post-Upgrade Tasks](#) chapter.

Upgrading a FortiSOAR master node

Before you upgrade your FortiSOAR master node, ensure the following:

- All playbooks have completed their execution on the master.
- The tenant node(s) are deactivated from the master node before upgrading the master node, and tenant nodes have disabled communication to the master node from the "Master Configuration" page.

If the master node of your multi-tenant configuration is part of an HA setup, i.e., MSSP +HA, then follow the steps mentioned in the [Upgrading a FortiSOAR High Availability Cluster](#) chapter.

If the master node of your multi-tenant configuration is not part of an HA setup, then follow the steps mentioned in the [Upgrading a FortiSOAR Enterprise Instance](#) chapter.

Upgrading a FortiSOAR Tenant node

Before you upgrade your FortiSOAR tenant node, ensure the following:

- Data replication from the tenant node to the master node is stopped. You can stop data replication by logging on to the tenant node and clicking **Settings** to open the `System` page, then in the `Multi Tenancy` section, click the **Master Configuration** menu item and then in the `Communication With Master Node` section, toggle the **Enabled** button to **NO**.

Once you have completed the upgrade process, i.e., upgrading both your master and tenant nodes from a release prior to 7.4.2 to release 7.4.2 or later, you must restart the `cyops-integrations-agent` service on tenant nodes using the following command:

```
systemctl restart cyops-integrations-agent
```

You must restart the `cyops-integrations-agent` service at tenant nodes before you download the agent's or

tenant's logs, from the master node's console..

- All playbooks have completed their execution on the tenant.
- All schedule playbooks that fetch data from data sources to the tenant are stopped.
- Any application that pushes data from data sources to the tenant is stopped.

If the tenant node of your multi-tenant configuration is part of an HA setup, i.e., MSSP +HA, then follow the steps mentioned in the [Upgrading a FortiSOAR High Availability Cluster](#) section.

If the tenant node of your multi-tenant configuration is not part of an HA setup, then follow the steps mentioned in the [Upgrading a FortiSOAR Enterprise Instance](#) section.



After the tenant node has been successfully upgraded, you must toggle the **Allow Module Management** setting to **NO** and then back to **YES**. This is needed only if you were already using the 'Allow Module Management' feature and is required to synchronize the tenant module metadata with the master instance. You can ignore this step, if your 'Allow Module Management' setting was already disabled before the upgrade.

Upgrading a FortiSOAR 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. For information on agents see the *Segmented Network support in FortiSOAR* chapter in the "Administration Guide," and for more information on secure message exchange and tenants, see the "Multi-Tenancy support in FortiSOAR Guide".

1. Ensure that you stop data replication between the master and the tenant nodes. You can stop data replication by logging on to the tenant node and clicking **Settings** to open the *System* page, then in the *Multi Tenancy* section, click the **Master Configuration** menu item and then in the *Communication With Master Node* section, toggle the **Enabled** button to **NO**.
2. Upgrade the SSH to the secure message exchange VM that you want to upgrade.
3. Check that you are connected to a `tmux` session. A `tmux` session is needed for situations where network connectivity is less than favorable. You can check your `tmux` session using the following command:

```
# tmux ls
```

This command returns an output such as the following example:

```
0: 1 windows (created Thu Nov 24 09:37:47 2022) [170x47]
```

Log back into the SSH console and run the following command to reattach the `tmux` session:

```
tmux attach-session -t 0
```

4. Run the following command to download the upgrade installer:

```
# wget https://repo.fortisoar.fortinet.com/7.4.2/upgrade-fortisoar-7.4.2.bin
```
5. Run the upgrade installer using the following command:

```
# sh upgrade-fortisoar-7.4.2.bin
```

OR

```
# chmod +x upgrade-fortisoar-7.4.2.bin
```

```
# ./upgrade-fortisoar-7.4.2.bin
```

Notes: The FortiSOAR upgrade installer checks for the following:

- The space available in `/tmp` or `/var/temp` (if exist in `/etc/fstab`), which must be at least 2GB. If the space available in `/tmp` or `/var/temp` is less than 2GB, then the upgrade installer exits after displaying an appropriate error message. If you want to skip this space validation check, you can use the `--skip-tmp-validation` option while running the upgrade script:

```
# ./upgrade-fortisoar-7.4.2.bin --skip-tmp-validation
```

- The disk space available in `/boot`, and if the `/boot` has insufficient space, then the upgrade installer exits after displaying an appropriate error message. Use standard methods to remove old kernels and free up space in `/boot`.

Once you complete cleaning up `/boot` and/or increasing disk space and space in `/tmp` (as per the messages provided by the upgrade installer) and you have sufficient space for upgrading FortiSOAR, you must re-run the upgrade installer to continue the process of upgrading FortiSOAR.

6. Once you have successfully upgraded the secure message exchange, start the data replication between the master and the tenant nodes again by toggling the **Data Replication** button to **ON**, and then verify the replication.

Upgrading a FortiSOAR Secure Message Exchange Cluster

RabbitMQ supports clustering, that in conjunction with Queue Mirroring can be used for an Active-Active configuration as explained in the [Clustering Guide](#) and in the [Highly Available \(Mirrored\) Queues](#) article, which includes steps on how to set up the clusters and monitor queues. The clustered instances should be fronted by a TCP Load Balancer such as HAProxy, and clients should connect to the cluster using the address of the proxy. For more information, see the *Multi-tenancy support in FortiSOAR* guide.



For the purpose of the following procedure, we are considering a two-node MQ mirrored queue clusters that are both added to the Reverse Proxy.

1. Configure the Reverse Proxy to pass requests only to *Node1*, which is the primary node of the MQ cluster. Therefore, now all requests will be handled by *Node1* and *Node2* will be available for maintenance.
2. Log on to the *Node2* terminal session as a `root` user, and upgrade *Node2* by following the steps mentioned in the [Upgrading a FortiSOAR Secure Message Exchange](#) section.
3. Configure the Reverse Proxy to route requests through *Node2*. Therefore, now all requests will be handled by *Node2* and *Node1* will be available for maintenance.
4. Login to *Node1*, and upgrade *Node1* as per the procedure mentioned in **step 2**.
5. Reconfigure the Reverse Proxy to load balance both *Node1* and *Node2*.

Troubleshooting upgrade issues for MSSP setups

Replication from tenant to master stops once you upgrade an MSSP with an HA setup

If you have upgraded an MSSP+HA setup, then post-upgrade the replication from tenant nodes to the master node stopped.

Resolution

To resolve this issue, once you have upgraded your MSSP setup and created the HA cluster, you must restart all services on the primary master node and the primary tenant node using the following command:

```
csadm services --restart
```

Upgrading FortiSOAR using the Offline Repository

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

```
[root@localhost ~]# tmux
```
2. If you are using your private repository to install or upgrade FortiSOAR, then use the following command to export the "custom_yum_url" variable before running the fresh install or upgrade script:

```
export custom_yum_url=<"custom_yum_url_name">
```
3. Download the upgrade installer for FortiSOAR7.4.2 using the following command:

```
[root@localhost ~]# wget https://<offline_repo>/7.4.2/upgrade-fortisoar-7.4.2.bin
```
4. To upgrade to FortiSOAR7.4.2, run the following command as a *root* user:

```
[root@localhost ~]# sh upgrade-fortisoar-7.4.2.bin
```

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

```
[root@localhost ~]# sh upgrade-fortisoar-7.4.2.bin --ignore-ssl-check
```

Upgrading your FortiSOAR Docker image and upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster

Upgrading your FortiSOAR Docker image

1. Download the FortiSOAR docker image from <https://support.fortinet.com>; details are in the Downloading the FortiSOAR Docker image section of the "Deployment Guide".
2. Load the downloaded Docker image using the following command:
`docker load -i <image-path>`
3. Download the FortiSOAR Docker installer from
`https://repo.fortisoar.fortinet.com/7.4.2/install-fortisoar-docker-<release_version>.bin`
For example, `https://repo.fortisoar.fortinet.com/7.4.2/install-fortisoar-docker-7.4.2.bin`
4. Update the `fortisoar.env` file with the ID of the Docker Image that is loaded in step 2. For more information, see Understanding the `fortisoar.env` file topic in the *Deploying FortiSOAR on a Docker Platform* chapter in the "Deployment Guide."
Important: Ensure that the value of the `PROJECT_NAME` field in the `fortisoar.env` file must be the same as the value in the earlier version of the Docker image.
5. Before you begin the upgrade, it is recommended to take a backup of your FortiSOAR Docker as listed in the following commands.
Note: The following commands uses `fortisoar_fortisoar_1` as the Docker name. You must replace this sample name with your own Docker name, which you can find using the `docker ps` command.
 - a. `docker exec -ti fortisoar_fortisoar_1 bash -c 'export LANG=en_US.UTF-8;csadm db --backup /home/csadmin'`
Note: This command stores the backup file at `/home/csadmin/DR_BACKUP_<release_version>-*_*.tgz` (for example, `/home/csadmin/DR_BACKUP_7.4.2-*_*.tgz`) inside your FortiSOAR Docker.
 - b. Copy the backup file from your FortiSOAR Docker on the Docker host using the following command:
`docker cp fortisoar_fortisoar_1:/home/csadmin/DR_BACKUP_<release_version>-*_*.tgz /data`
For example, `docker cp fortisoar_fortisoar_1:/home/csadmin/DR_BACKUP_7.4.2-*_*.tgz /data`
Note: The FortiSOAR Docker backup file is stored in the `/data` directory on your Docker host.
6. Stop your FortiSOAR Docker using the following command:
`docker stop fortisoar_fortisoar_1`
7. Remove your FortiSOAR Docker using the following command:
`docker rm fortisoar_fortisoar_1`
8. Run the FortiSOAR Docker using the updated `fortisoar.env` file that contains the ID of the new Docker Image using the following command:
`./install-fortisoar-docker-<release_version>.bin --env-file fortisoar.env`
For example, `./install-fortisoar-docker-7.4.2.bin --env-file fortisoar.env`

Reverting the upgrade on your FortiSOAR Docker image

In case the FortiSOAR Docker image upgrade fails, and you want to revert to the previous release, then you need to restore the backup of the previous version that was taken in the `/data` directory on your Docker host. Following are the steps for restoring the backup.

Note: The following commands use `fortisoar_fortisoar_1` as the Docker name. You must replace this sample name with your own Docker name, which you can find using the `docker ps` command.

1. Stop the running FortiSOAR Docker using the following command:
`docker stop fortisoar_fortisoar_1`
2. Remove the FortiSOAR Docker using the following command:
`docker rm fortisoar_fortisoar_1`
3. Remove the FortiSOAR Docker volumes using the following command:
`docker volume rm $(docker volume ls --filter name=fortisoar_fortisoar_* -q)`
4. Update the `fortisoar.env` file with the ID of the previous Docker Image.
5. Run the previous version FortiSOAR Docker using the updated `fortisoar.env` file that contains the ID of the previous Docker Image using the following command:
`./install-fortisoar-docker-<release_version>.bin --env-file fortisoar.env`
For example, `./install-fortisoar-docker-7.4.2.bin --env-file fortisoar.env`
6. Wait until you see EULA page on the UI at `https://<docker-host-hostname>:<PORT_UI>/`
7. Copy the FortiSOAR Docker backup file from the `/data` directory on your Docker host using the following command:
`docker cp /data/DR_BACKUP_<release_version>-*_*_.tgz fortisoar_fortisoar_1:/home/csadmin/`
`docker cp /data/DR_BACKUP_7.4.2-*_*_.tgz fortisoar_fortisoar_1:/home/csadmin/`
8. Restore the Docker image using the following command:
`docker exec -it fortisoar_fortisoar_1 bash -c "export LANG=en_US.UTF-8;csadm db --restore /home/csadmin/DR_BACKUP_<release_version>-*_*_.tgz"`
For example, `docker exec -it fortisoar_fortisoar_1 bash -c "export LANG=en_US.UTF-8;csadm db --restore /home/csadmin/DR_BACKUP_7.4.2-*_*_.tgz"`

Upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster

1. Download the FortiSOAR docker image from <https://support.fortinet.com>; details are in the Downloading the FortiSOAR Docker image section of the "Deployment Guide".
2. Upload the downloaded FortiSOAR Docker image to your AWS Elastic container registry or any other Docker repository that is accessible from within your Kubernetes cluster. For example:

```
# docker push <account-id>.dkr.ecr.<region>.amazonaws.com/fortisoar/fortisoar:7.4.2
```
3. Before you begin the upgrade process, it is recommended to take a backup of your FortiSOAR pod as listed in the following commands.
The following commands uses `fsr-0` as the pod name. You must replace this sample name with your own pod name that you can find using the `#kubectl get pods -o=name -n fsr` command.

```
#kubectl exec -ti -n fsr -c fsr fsr-0 -- bash -c "csadm db --backup  
/\home/\csadmin/\ "
```

Note: This command stores the backup file in the `/home/csadmin/DR_BACKUP_<release_version>-*_*.tgz` folder inside your FortiSOAR pod. For example, `/home/csadmin/DR_BACKUP_7.3.2-*_*.tgz` inside your FortiSOAR pod.

Copy the backup file from your FortiSOAR pod on the EKS cluster node to your machine using the following command:

```
#kubectl cp fsr-0:/home/csadmin/DR_BACKUP_<release_version>-*_*.tgz -c fsr -n fsr  
DR_BACKUP_<release_version>.tgz
```
4. Stop the running FortiSOAR pod using the following command:

```
#kubectl delete statefulset <statefulset_name> -n <fortisoar_namespace>
```
5. Update the path of the new FortiSOAR image in the `fortisoar-statefulset.yaml` file.
6. Run the following command to deploy a new statefulset with the latest docker image:

```
#kubectl apply -f fortisoar-statefulset.yaml
```

Post-Upgrade Tasks

Change in the default behavior of the On Create, On Update, and On Delete playbooks for MSSP configurations

Prior to version 7.4.2, for modules that had multi-tenancy enabled and configured for data replication, the On Create, On Update, and On Delete playbooks executed on both the instances where the record is created as well as on the instance where the record is replicated. From release 7.4.2 onwards, the default behavior of the On Create, On Update, and On Delete playbooks is to run only on the instance where the record is created.

If you want to retain the previous behavior for these playbooks, i.e., run the On Create, On Update, and On Delete playbooks on both the source and the replicated instance of the record, then do the following:

1. Open the `parameters_prod.yaml` file:

```
vi /opt/cyops-api/config/parameters_prod.yaml
```
2. Change the value of the `execute_workflow_on_replicate_node` parameter to `true`. By default, this parameter is set to `false`.
3. Run the following command:

```
systemctl restart php-fpm && sudo -u nginx php /opt/cyops-api/bin/console  
cache:clear && systemctl restart php-fpm
```



These steps change the default behavior of playbooks to run on both the source and replicated instances of the record instead of only the source instance. However, you can update this behavior to run either on the instance where the record is created or where it is replicated by opening the playbook that contains the On Create, On Update, or On Delete step and selecting the appropriate option. *The behavior selected on the UI takes preference over the default behavior.* For information on updating the behavior from the UI, see the 'Distributed Tenancy Support' chapter in the *Multi-tenancy Support in FortiSOAR* guide.

Restart the cyops-integrations-agent service on the tenant nodes for multi-tenant configurations

Considering that data communication between the tenant node to the master node is stopped prior to an [upgrade of a FortiSOAR distributed multi-tenancy configuration](#), post-upgrade of both your master and tenant nodes from a release prior to 7.4.2 to release 7.4.2 or later, you must restart the `cyops-integrations-agent` service on the tenant nodes using the following command:

```
systemctl restart cyops-integrations-agent
```

You must restart the `cyops-integrations-agent` service at tenant nodes before you download the agent's or tenant's logs, from the master node's console.

Update the config.ini file to prevent the Jinja Editor from traversing paths

FortiSOAR playbooks create or edit operations allow path traversal, giving authorized attackers access to sensitive system files. Perform the following actions after the upgrade to make sure that this does not happen:

1. SSH to your FortiSOAR VM and login as a *root* user.
2. Edit the `config.ini` file:
`vi /opt/cyops-workflow/sealab/sealab/config.ini`
3. Add the following parameter in the `[application]` section of the `config.ini` file:
`DISALLOWED_JINJA_FILTERS = ['readfile']`
4. Restart the 'uwsgi' service using the following command:
`systemctl restart uwsgi`



www.fortinet.com

Copyright© 2023 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.