

Upgrade Guide

FortiSOAR 7.3.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August, 2024

FortiSOAR 7.3.3 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
Post-Upgrade Tasks	15
Modify the 'Notify On Pending External Manual Input' Delivery Rule	15
Disable the 'Notify On Pending Manual Input' Delivery Rule	15

Change Log

Date	Change Description
2024-08-12	Initial release of 7.3.3

Introduction

This guide covers upgrading a FortiSOAR™ enterprise instance, High Availability (HA) cluster, distributed multi-tenant configuration, and upgrading FortiSOAR using an offline repository.



Upgrading the FortiSOAR Docker image to the 7.3.3 release is not supported.

From version 7.0.0 onwards, 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 guide describes how to upgrade FortiSOAR to 7.3.3 and is intended to supplement the FortiSOAR Release Notes. This guide includes the following chapters:

- [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](#)
-



You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant instance to version 7.3.3 from version 7.3.1 or 7.3.2 only. FortiSOAR release 7.3.3 is available only as an upgrade. Fresh installation is not supported for FortiSOAR release 7.3.3.

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. Also, once you have upgraded your instance, you must log out from the FortiSOAR UI and log back into FortiSOAR.

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 7.3.3.

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.
- Run the `tmux` command to ensure that the upgrade is not affected if your ssh session times out.
- 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 7.3.3.

Upgrading a FortiSOAR Enterprise Instance



FortiSOAR release 7.3.3 is available only as an upgrade. Fresh installation is not supported for FortiSOAR release 7.3.3. Upgrade from v7.3.0 onwards fails if your instance is behind proxy servers or you are upgrading using offline repositories that do not have access to <https://mirrors.rockylinux.org>, and therefore the upgrade script is unable to connect to <https://mirrors.rockylinux.org> to upgrade the rocky linux repo files. To resolve this issue, see the steps mentioned in the [Upgrading FortiSOAR using the Offline Repository](#) chapter.

To upgrade your system to FortiSOAR from 7.3.1 or 7.3.2 to 7.3.3, 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/7.3.3/upgrade-fortisoar-7.3.3.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-7.3.3.bin
```

OR

```
# chmod +x upgrade-fortisoar-7.3.3.bin
# ./upgrade-fortisoar-7.3.3.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-7.3.3.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 7.3.3, 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.

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 7.3.3, 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 7.3.3, 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 7.3.3.

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**.
- 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/7.3.3/upgrade-fortisoar-7.3.3.bin`
5. Run the upgrade installer using the following command:
`sh upgrade-fortisoar-7.3.3.bin`
OR
`chmod +x upgrade-fortisoar-7.3.3.bin`
`./upgrade-fortisoar-7.3.3.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-7.3.3.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.

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

IMPORTANT: Upgrade from FortiSOAR v7.3.0 onwards fails if your FortiSOAR instance is behind proxy servers or you are upgrading FortiSOAR using offline repositories that do not have access to <https://mirrors.rockylinux.org>, and therefore the upgrade script is unable to connect to <https://mirrors.rockylinux.org> to upgrade the rocky linux repo files. To resolve this issue, run `setup-environment.bin` as follows:

1. 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 `setup-environment.bin` script:
`export custom_yum_url=<"custom_yum_url_name">`
 For example, `export custom_yum_url="offline-repo.fortisoar.in"`
Note: You do not need to run this step for FortiSOAR instances behind proxy servers, etc.
2. Download the script `setup-environment.bin` from
<https://repo.fortisoar.fortinet.com/fortisoar/scripts/setup-environment.bin>
3. Copy the script to your FortiSOAR instance.
4. Login as a 'root' user.
5. Run `setup-environment.bin` with its mandatory 'version' parameter that specifies the version of FortiSOAR to which the user wants to upgrade. For example:
`sh setup-environment.bin -v 7.3.3`
 OR
`sh setup-environment.bin --version 7.3.3`

Now, you can upgrade your FortiSOAR instance as follows:

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 FortiSOAR 7.3.3 using the following command:
`[root@localhost ~]# wget https://<offline_repo>/7.3.3/upgrade-fortisoar-7.3.3.bin`
4. To upgrade to FortiSOAR 7.3.3, run the following command as a *root* user:
`[root@localhost ~]# sh upgrade-fortisoar-7.3.3.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-7.3.3.bin --ignore-ssl-check`

Post-Upgrade Tasks

Modify the 'Notify On Pending External Manual Input' Delivery Rule

From FortiSOAR 7.3.0 onwards, you can choose to run unauthenticated manual inputs in segmented networks using FSR agents. To achieve this, the 'Notify On Pending External Manual Input' delivery rule has been updated in the case of fresh installations of FortiSOAR 7.3.0. However, if you have upgraded your FortiSOAR instance to release 7.3.0 or later from a release prior to 7.3.0, you must modify the 'Notify On Pending External Manual Input' rule to allow the running of manual inputs on FSR agents. For the steps on how to achieve this, see the [Modifying the 'Notify On Pending External Manual Input' delivery rule post-upgrade to release 7.3.0 or later](#) topic in the *System Configuration* chapter of the "Administration Guide."

Disable the 'Notify On Pending Manual Input' Delivery Rule

Post-upgrade to release 7.3.0 or later from a release prior to 7.3.0, you can disable the `Notify On Pending Manual Input` rule, if you want to disable the manual input notification from the 'Notifications Panel'; else you will receive the manual input notification in both the 'Notifications Panel' and the 'Pending Tasks'. In the case of a fresh installation of FortiSOAR 7.3.0 (or later), notifications for manual input are visible on only the **Manual Input** tab in the 'Pending Tasks' panel. For the steps on how to achieve this, see the [Disabling a Delivery Rule](#) topic in the *System Configuration* chapter of the "Administration Guide."



www.fortinet.com

Copyright© 2024 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 Chief Legal Officer, 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.