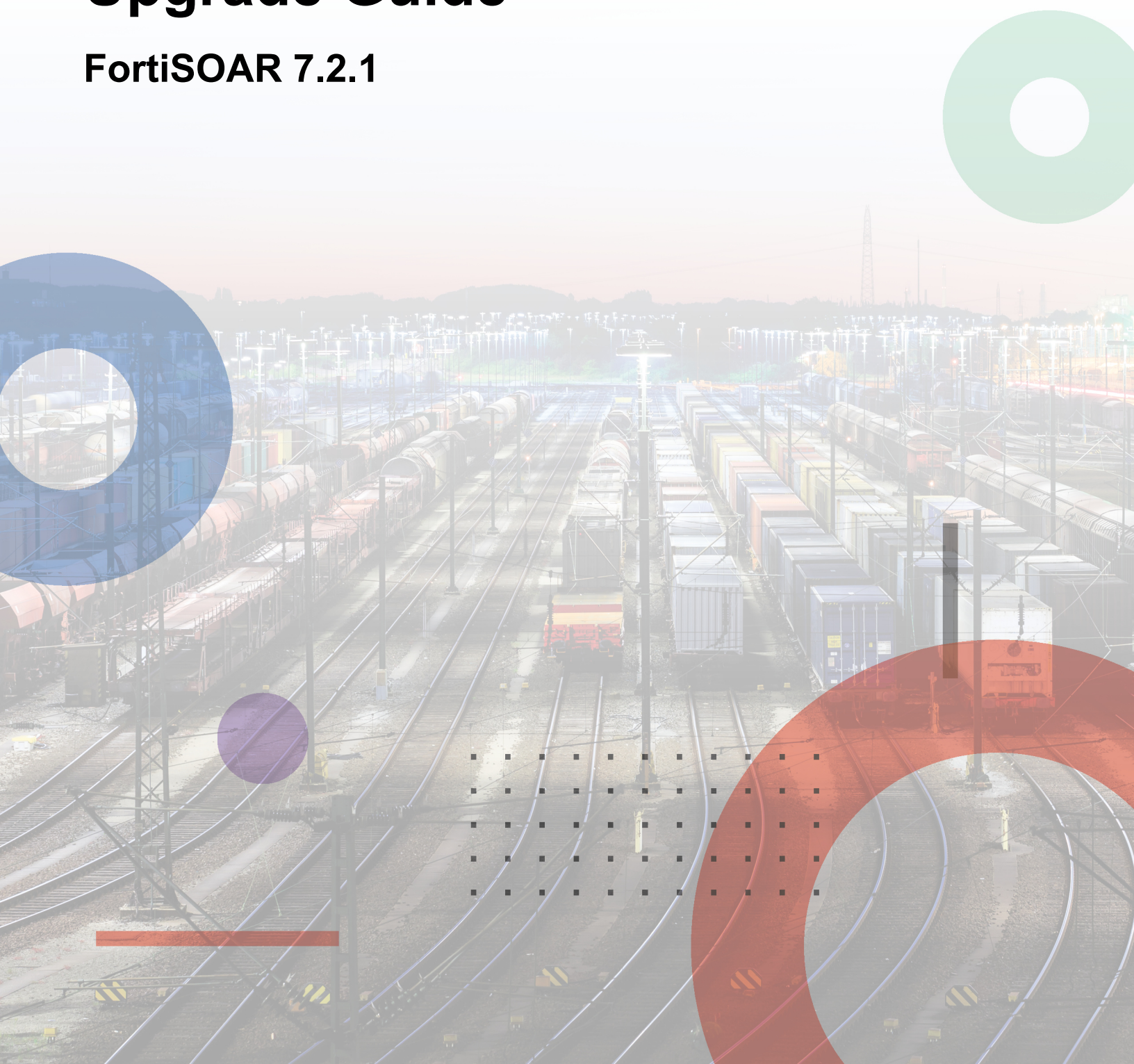
Upgrade Guide

FortiSOAR 7.2.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

July, 2022
FortiSOAR 7.2.1 Upgrade Guide
00-400-000000-20210416

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-07-04	Added the 'Enable appropriate default 'Notification' rules for incident and alert updations' topic in the Post-Upgrade Tasks chapter.
2022-06-30	Initial release of 7.2.1

Introduction

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

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 document describes how to upgrade FortiSOAR to 7.2.1. 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

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant instance to version 7.2.1 from versions 7.0.0, 7.0.1, 7.0.2, or 7.2.0 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 7.2.1.

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):

- 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.
- Ensure that the playbook appliance has '`Create`' and '`Read`' permissions on the `Widgets` module. Playbook appliance is used to install the widgets required by the war room, and if the permissions to the Widgets are not assigned; the required war room widgets will fail to install.
- 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.
- Ensure that the `ssh` session does not timeout by entering into the `screen` mode. 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."
  Note: In release 7.2.0 update.cybersponse.com has been renamed to https://repo.fortisoar.fortinet.com/. Both these repositories will be available for a while to allow users who are on a release prior to FortiSOAR release 7.2.0 to access connectors and widgets. However, in time, only https://repo.fortisoar.fortinet.com/ will be available.
- 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 7.2.1.

Upgrading a FortiSOAR Enterprise Instance

To upgrade your system to FortiSOAR from 7.0.0, 7.0.1, 7.0.2, 7.2.0 to 7.2.1, 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 `screen` session. A `screen` session is needed for situations where network connectivity is less than favorable. You can check your screen session using the following command:
   ```
   # screen -ls
   ```
   This command returns an output such as the following example:
   ```
   There is a screen on:
   12081.upgrade(Detached)
   ```
   Log back into the SSH console and run the following command to reattach the screen session:
   ```
   screen -r 12081.upgrade
   ```
   OR
   ```
   screen -r upgrade
   ```
4. Run the following command to download the upgrade installer:
   ```
   # wget https://repo.fortisoar.fortinet.com/7.2.1/upgrade-fortisoar-7.2.1.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-7.2.1.bin
   ```
   OR
   ```
   # chmod +x upgrade-fortisoar-7.2.1.bin
   # ./upgrade-fortisoar-7.2.1.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-7.2.1.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. Steps for cleaning up `/boot` are present in the Clean up /boot article present in the Fortinet Knowledge Base.
   - 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 7.2.1, 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.
Note: The SOAR Framework solution pack is marked 'Installed' by default after you have upgraded to release 7.2.1 or later from a release prior to 7.2.1. This is done to enable users with upgraded systems to install other solution packs.

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 7.2.1, 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*.
   Important: For releases prior to release 7.2.0 you need to run the `leave-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*.
   Important: For releases prior to release 7.2.0 you need to run the `join-cluster` command on *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 7.2.1, 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*.
   Important: For releases prior to release 7.2.0 you need to run the `leave-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*.
   Important: For releases prior to release 7.2.0 you need to run the `join-cluster` command on *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 7.2.1.

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.

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 section.

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 section.

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. SSH to the secure message exchange VM that you want to upgrade.
3. Check that you are connected to a `screen` session. A `screen` session is needed for situations where network connectivity is less than favorable. You can check your screen session using the following command:
   ```
   # screen -ls
   ```
   This command returns an output such as the following example:
   ```
   There is a screen on:
   12081.upgrade(Detached)
   ```
   Log back into the SSH console and run the following command to reattach the screen session:
   ```
   screen -r 12081.upgrade
   ```
   OR
   ```
   screen -r upgrade
   ```
4. Run the following command to download the upgrade installer:
   ```
   # wget https://repo.fortisoar.fortinet.com/7.2.1/upgrade-fortisoar-7.2.1.bin
   ```
5. Run the upgrade installer using the following command:
   ```
   # sh upgrade-fortisoar-7.2.1.bin
   ```
   OR
   ```
   # chmod +x upgrade-fortisoar-7.2.1.bin
   # ./upgrade-fortisoar-7.2.1.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 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-7.2.1.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. Steps for cleaning up `/boot` are present in the Clean up /boot article present in the Fortinet Knowledge Base.
   - 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*.

Post-Upgrade Tasks

Enable appropriate default 'Notification' rules for incident and alert updations

During the upgrade process of your FortiSOAR system to 7.2.1 from a system that was upgrade to 7.2.0 and has the SOAR Framework solution pack installed, the following two default 'Notification' rules are disabled and renamed:

- 'Incident - Notify Updation' will be renamed as 'Default - Incident - Notify Updation'
- 'Alert - Notify Updation' will be renamed as 'Default - Alert - Notify Updation'

Therefore, once your system is upgraded successfully to release 7.2.1, you will have the following rules:

- 'Incident - Notify Updation' - Enabled state
- 'Default - Incident - Notify Updation' - Disabled state
- 'Alert - Notify Updation' - Enabled state
- 'Default - Alert - Notify Updation' - Disabled state

You have to enable or disable appropriate notification rules as per your requirement.

SOAR Framework solution pack is not marked installed as default after you upgrade to release 7.2.1

The SOAR Framework solution pack is marked 'Installed' by default after you have upgraded to release 7.2.1 or later from a release prior to 7.2.0 (for example 7.0.2). This is done to enable users with upgraded systems to install other solution packs. However, if you do not see SOAR Framework solution pack marked as installed on your upgraded FortiSOAR system, it might be because you have deleted the 'default appliance' on your FortiSOAR system. Do the following to mark the SOAR Framework solution pack as 'Installed' on your upgraded FortiSOAR system:

1. Assign appropriate 'Content Hub' and 'Solution Pack' permissions (roles) to the "`new/custom`" appliance.
2. Run the following command to synchronize the solution packs:
   ```
   sudo -u nginx php /opt/cyops-api/bin/console fortisoar:contenthub:sync -fs
   ```
3. Run the following command to mark the SOAR Framework solution pack as installed:
   ```
   sudo -u nginx php /opt/cyops-api/bin/console app:sp:update --
   solutionPackName='sOARFramework' --markInstalled
   ```

The Update link on your FSR Agent is not visible after you have upgraded your FortiSOAR system to 7.2.1

After you have upgraded to release 7.2.1 or later from a release prior to 7.2.1 and you see that the **Update** link is not available on your FSR Agent node, or your FSR Agent displays the **Awaiting Remote Node Connection** status, this

means that agent connectivity is lost. To regain agent connectivity, restart the `cyops-integrations-agent` service on the FSR Agent.

Assign appropriate permissions for Content Hub

Once you have upgraded to release 7.2.0 or later from a release prior to 7.2.0, appropriate permissions must be assigned to users who require to work with Content Hub, i.e., solution packs, widgets, and connectors. For users who need to work with all the components assign the 'FSR Content Hub' role; however, users who need to work only with an individual component such as widgets or connectors, appropriate permissions should be assigned for 'Content Hub' and individually for 'Widgets' or 'Connectors'.

Assign appropriate permissions to the Playbook Appliance

Once you have upgraded to release 7.2.0 or later from a release prior to 7.2.0, if you observe that connectors that were installed prior to the upgrade are missing from the Content Hub, due to some issues or if you do not have a default 'Playbook Appliance', do the following:

- Assign appropriate permissions on the `Solution Pack` module to the 'Playbook Appliance'. FortiSOAR synchronizes Content Hub content at the thirtieth minute of every hour (for example, 1:30, 2:30); therefore, after you have given the permissions, in around thirty minutes, you should be able to see the connectors that were installed prior to the upgrade in both the **Discover** as well as **Manage** tabs on Content Hub.
- If you want to see the missing connectors instantaneously in Content Hub, then run the following command:
  `/opt/cyops/scripts/api_caller.py --endpoint "https://localhost/api/3/solutionpack/sync" --method GET`

Perform a manual synchronization for Content Hub data if your FortiSOAR instance does not have a default playbook appliance

If your FortiSOAR does not have a default Playbook Appliance or if the Playbook Appliance is renamed before you upgrade to release 7.2.0, then post upgrade you must update roles with appropriate Content Hub permissions for the used Appliance. Once you have updated the roles, you have to perform a manual synchronization to get Content Hub data using an API call:
`/opt/cyops/scripts/api_caller.py --endpoint "https://localhost/api/3/solutionpack/sync" --method GET`

After this, FortiSOAR automatically synchronizes Content Hub data using the scheduled API call.

Retrain your Machine Learning Model

Once you have upgraded to release 7.2.0 or later from a release prior to 7.2.0, you might observe that errors are being displayed for field suggestions and record similarity. In such cases, you must retrain your Machine Learning model.

Deactivation of notification system playbooks and customization of notification rules

If you have upgraded to release 7.2.0 or later from a release prior to 7.2.0, then users will receive two emails for a single notification. This is because the upgraded FortiSOAR system would have both the new notification rules and the system playbooks that triggered notifications prior to 7.2.0. To resolve this issue, the earlier system playbooks that used to send the notifications emails must be deactivated and the notification rules must be customized to suit your requirements. For details on Notification Framework, see the *System Configuration* chapter in the "Administration Guide."

Following is a list of system playbooks that can be deactivated:

- In the Approval/Manual Task Playbooks collection, you can deactivate the following playbooks:
  - Approval > Notify Owners
  - Approval > Notify Updated Owners
  - In the System Notification and Escalation Playbooks collection, you can deactivate the following playbooks:
  - Alert > Notify Creation (Email)
  - Alert > Notify Creation (System)
  - Alert > Notify Updation(System)
  - Incident > Notify Creation (Email)
  - Incident > Notify Creation (System)
  - Incident > Notify Updation
  - Task > Notify Creation (Email)
  - Task > Notify Creation (System)
  - Task > Notify Updation

Tasks to be performed if you have enabled Multihoming

If you have enabled 'Multihoming' on FortiSOAR, and you are upgrading FortiSOAR 7.0.2 MP2 to FortiSOAR 7.2.0, then you have to redo the configurations that are required for multihoming in the `/opt/cyops-rabbitmq/configs/ssl/openssl.cnf` file:

Add the service and management interface DNS names in `alt_names` section in the **`/opt/cyops-rabbitmq/configs/ssl/openssl.cnf`** file.
For example,
The original `alt_names` section in the `openssl.cnf` file:

```
[alt_names]
DNS.1 = fortisoar.myorgdomain
```

After adding the service and management interface DNS names:

```
[alt_names]
DNS.1 = fortisoar-management.myorgdomain
DNS.2 = fortisoar.myorgdomain
```

Note: If you use signed certificates, ensure that the certificate resolves both the service and management interface names.

For more information on setting up multihoming on FortiSOAR, see the *High Availability* chapter in the "Administration Guide."

Updates needed to the Task Management Widget

Once you have upgraded to release 7.2.0 from release 7.0.0, you will observe that the task management widget does not work as expected in War Rooms (or any other modules where it is configured).

Resolution

1. Use the **Export Wizard** to export the Tasks, War Rooms, and any other module that is configured with task management from your upgraded 7.2.0 instance.
2. Use the **Import Manager** to import these modules back into your upgraded 7.2.0 instance.

www.fortinet.com