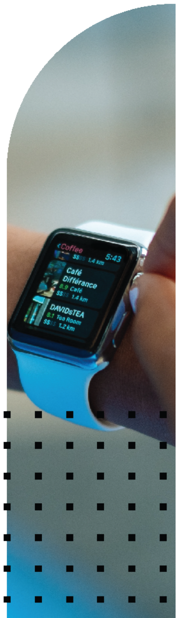
Maintenance Packs

FortiSOAR 7.0.2



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May, 2022
FortiSOAR 7.0.2 Maintenance Packs
00-400-000000-20210111

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-05-23	Updated the contents in the 'Maintenance Pack 2' section of the FortiSOAR Maintenance Packs chapter
2022-05-06	Third Maintenance Pack for 7.0.2
2022-03-17	Second Maintenance Pack for 7.0.2
2021-12-23	First Maintenance Pack for 7.0.2

FortiSOAR Maintenance Packs

FortiSOAR Maintenance Packs are used to deploy cumulative fixes for a particular released version. This document talks about maintenance packs that will apply to FortiSOAR release 7.0.2.

Maintenance Pack 3

Enhancements made and Issues Fixed

- Fixed the Spring4Shell and CVE-2022-22965 vulnerabilities by upgrading the Spring Boot Framework to 2.5.12.
- Fixed the failure of Ansible installation, which is installed by default during FortiSOAR VM configuration.
  Note: It is recommended to run the MP3 installation on new deployments to fix the root certificate and Ansible installation issues.
- Fixed issues faced while configuring data ingestion, if the data ingestion playbooks take more than 60 seconds of time to complete their execution.
- Fixed the issue of takeover failing in case of a break in network connectivity between the primary and secondary nodes in an HA cluster.
- Fixed the issue of workflow notifications that are generated on a HA node not being sent to other nodes in the HA cluster.
- Fixed the issue with manual input playbooks that are triggered using an 'Action' button such as the Escalate playbook that used to continue to wait for the playbook execution results, resulting in the manual input spinning icon continuing to spin even if the manual input is deleted or canceled. Now, the manual input playbook does not wait for any playbook execution results and FortiSOAR displays a toaster message such as, "`<PB_name> executed successfully on <no_of_records_selected> record.`"

Steps to install FortiSOAR Maintenance Pack 3

1. Ensure that you have taken a VM snapshot of your current FortiSOAR system. Only after you have taken a VM snapshot of your system should apply the Maintenance Pack.
   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.
2. Ensure that update.cybersponse.com is reachable from your VM.
   Note: If your instance can connect to update.cybersponse.com using only a proxy, then ensure that you set the proxy in the `/etc/wgetrc`, `/etc/profile`, and `yum.conf` files. This is required to download the maintenance pack file.
   For example:
   ```
   use_proxy=yes
   http_proxy=<proxy_server_ip:port>
   https_proxy=<proxy_server_ip:port>
   ```
3. SSH to your FortiSOAR 7.0.2 VM and log in as a *root* user.
4. Download the installer for 7.0.2 maintenance pack 3 using the following command:
   ```
   # wget https://update.cybersponse.com/7.0.2/maintenance-packs/install-fortisoar-maintenance-pack-7.0.2-mp3.bin
   ```
5. To install Maintenance Pack 3 for FortiSOAR 7.0.2, run the following command as a *`root`* user:
   ```
    # sh install-fortisoar-maintenance-pack-7.0.2-mp3.bin
   ```
   OR
   ```
   chmod +x install-fortisoar-maintenance-pack-7.0.2-mp3.bin
   ./install-fortisoar-maintenance-pack-7.0.2-mp3.bin
   ```

Maintenance Pack 2

Enhancements made and Issues Fixed

- Fixed the performance issues faced with 'Manual Inputs' by making all the manual input playbooks as 'Public' playbooks, i.e., the visibility of manual inputs playbooks is always set to 'Public', and therefore all users with appropriate permissions will be able to view the manual input in the **Pending Decisions** list on the top-right corner in FortiSOAR.
  Note: If you have a requirement of creating a 'Private' manual input playbook, contact FortiSOAR Customer Support.
- Enhanced the *High Availability* chapter in the "Administration Guide" by adding instructions for extending support for two NICs on a FortiSOAR appliance for controlled traffic routing.
- Added the `Failed Authentication Settings` section on the **Authentication Configuration** > **Account Configuration** page to provide users with the following options:
  - In the **Maximum Failed Login Attempts** field, you can specify the number of times that users can enter an incorrect password while logging into FortiSOAR before their account gets locked. By default, this is set to 5 (times).
  - In the **Account Unlock Time**, you can specify the duration, in minutes, after which the user accounts get automatically unlocked, in cases where user accounts were locked due to exceeding the number of failed login attempts. By default, this is set to 30 (minutes).
- Provided administrators with the ability to set up custom password policies, which enforces additional restrictions (apart from the default rules) on the passwords that users can create. For more information, see the `Enabling custom password policies for users configured with Basic Authentication` topic in the *Security Management* chapter of the "Administration Guide."

- Added entries in the 'Audit Log' for locking users' accounts in the event of multiple failed login attempts.
- Fixed the issue of playbooks not getting triggered even after the trigger conditions were met.
- Fixed issues with user preference settings, including the following:
    - Saving of user preferences.
    - Saving of user-created filters as 'User' filters and not as 'System' filters.
    - Displaying of user-level filters only to the users.
- Fixed the issue with users being unable to add or edit log forwarding details.

Steps to install FortiSOAR Maintenance Pack 2

1. Ensure that you have taken a VM snapshot of your current FortiSOAR system. Only after you have taken a VM snapshot of your system should apply the Maintenance Pack.
   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.
2. Ensure that update.cybersponse.com is reachable from your VM.
   Note: If your instance can connect to update.cybersponse.com using only a proxy, then ensure that you set the proxy in the `/etc/wgetrc`, `/etc/profile`, and `yum.conf` files. This is required to download the maintenance pack file.
   For example:
   ```
   use_proxy=yes
   http_proxy=<proxy_server_ip:port>
   https_proxy=<proxy_server_ip:port>
   ```
3. SSH to your FortiSOAR 7.0.2 VM and log in as a *root* user.
4. Download the installer for 7.0.2 maintenance pack 2 using the following command:
   ```
   # wget https://update.cybersponse.com/7.0.2/maintenance-packs/install-fortisoar-maintenance-pack-7.0.2-mp2.bin
   ```
5. To install Maintenance Pack 2 for FortiSOAR 7.0.2, run the following command as a *`root`* user:
   ```
    # sh install-fortisoar-maintenance-pack-7.0.2-mp2.bin
   ```
   OR
   ```
   chmod +x install-fortisoar-maintenance-pack-7.0.2-mp2.bin
   ./install-fortisoar-maintenance-pack-7.0.2-mp2.bin
   ```

Maintenance Pack 1

Issues Fixed

- Fixed the issue of new appliance users not getting created using the FortiSOAR UI.
- Fixed the issue of a reference playbook that contains a `do_until` condition, running in a loop until it reaches the maximum retries limit. This was because the condition evaluation in `do_until` always used to return `false` causing the playbook to run in a loop.
- Fixed the issue of API queries not working for text and string fields if the values specified in these fields had any upper-case content.
- Fixed the issue in the case of a high availability cluster of publishing taking longer and errors being present in the `ha.log` for all non-primary nodes.

- Fixed the issue disk usage going over the 75% threshold and increasing `/opt` space due to crud-hub intermediate files not getting cleared. Now, an option has been added to physically delete token cache and file metadata cache after a day.
- Enhanced the Export and Import Wizards by adding an option using which users can select the items from the navigation structure they want to export, and also selectively choose the items from the navigation structure they want to import. Before this, you could export and import only the complete navigation structure.
- Fixed the issue in scheduling in case of reports whose input field is of type 'lookup'.
- Fixed an issue that occurred in MSSP systems that caused an Upsert request to fail when the record is internally updated if the value of the tenant sending the request is set to 'null'. Now, the request will not fail and the existing value of the tenant field is retained.

Steps to install FortiSOAR Maintenance Pack 1

1. Ensure that you have taken a VM snapshot of your current FortiSOAR system. Only after you have taken a VM snapshot of your system should apply the Maintenance Pack.
   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.
2. Ensure that update.cybersponse.com is reachable from your VM.
   Note: If your instance can connect to update.cybersponse.com using only a proxy, then ensure that you set the proxy in the `/etc/wgetrc`, `/etc/profile`, and `yum.conf` files. This is required to download the maintenance pack file.
   For example:
   ```
   use_proxy=yes
   http_proxy=<proxy_server_ip:port>
   https_proxy=<proxy_server_ip:port>
   ```
3. SSH to your FortiSOAR 7.0.2 VM and log in as a *root* user.
4. Download the installer for 7.0.2 maintenance pack 1 using the following command:
   ```
    # wget https://update.cybersponse.com/7.0.2/maintenance-packs/install-fortisoar-maintenance-pack-7.0.2-mp1.bin
   ```
5. To install Maintenance Pack 1 for FortiSOAR 7.0.2, run the following command as a *`root`* user:
   ```
     # sh install-fortisoar-maintenance-pack-7.0.2-mp1.bin
   ```
   OR
   ```
   chmod +x install-fortisoar-maintenance-pack-7.0.2-mp1.bin
   ./install-fortisoar-maintenance-pack-7.0.2-mp1.bin
   ```

www.fortinet.com