FORTINET

Release Notes

FortiSOAR 7.2.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

April, 2022
FortiSOAR 7.2.0 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log **4**
FortiSOAR 7.2.0 Release **5**
New features and enhancements **6**
Special Notices **10**
Removed Rules Engine 10
Removal of the approvalHost global variable 10
System user for integrations runtime should have minimal privileges on the file system 10
Renamed the update.cybersponse.com repository 11
Deprecated Queue Management 11
Blocked importing of OS-related packages (os, sys, subprocess) using the Code Snippet connector 11
Introduction of the SOAR Framework Solution Pack 11
Post-upgrade to 7.2.0 users should be assigned appropriate permissions for Content Hub 12
Post-upgrade to 7.2.0 user cannot see the earlier record assignment notifications 12
Upgrade Information **13**
Product Integration and Support **14**
Web Browsers & Recommended Resolution 14
Virtualization 14
Resolved Issues **15**

Change Log

Date	Change Description
2022-05-18	Added the 'Post-upgrade to 7.2.0 users should be assigned appropriate permissions for Content Hub' topic and updated the 'Introduction of the SOAR Framework Solution Pack' topic in the Special Notices chapter.
2022-04-21	Initial release of 7.2.0

FortiSOAR 7.2.0 Release

Yet another poppy blooms! We are ecstatic to share the latest version of Fortinet Security Orchestration, Automation, and Response Platform (**FortiSOAR™**) 7.2.0 with you. The release was nothing short of an eventful journey for us, where we tasked ourselves to ornate the release with not few, but many significant solutions together and that required us to unlearn and relearn many things about product research, execution, and testing.

A powerful Haiku by Katsushika Hokusai sums up the journey very well -

I write, erase, rewrite
Erase again, and then
A poppy blooms.

For a detailed list of all the new features and enhancements, see the New features and enhancements chapter.

New features and enhancements

FortiSOAR Content Hub

- Content Hub is FortiSOAR's all-new, central, curated repository of rich content that meets your need to find suitable solutions. It hosts Solution Packs, Use Cases, Integrations, Playbooks, Widgets, Dashboards, Reports, and much more of such helpful content – all packed in a searchable, filter-friendly interface.
- Available both as a public-facing page on: https://fortisoar.contenthub.fortinet.com/ where you can discover and learn more about the latest content available and embedded within the product, where you can discover, install and create your own content. So, see you at the Hub!
- The SOAR Framework Solution Pack is the foundational solution Pack that creates the framework, including modules, dashboard, roles, widgets, etc., required for effective day-to-day operations of any SOC. The Incident Response modules have been removed from the FortiSOAR platform and moved to the SOAR Framework SP, making it essential for users to install the SOAR Framework SP to optimally use and experience FortiSOAR's incident response.
  Note: *In release 7.2.0 the SOAR Framework Solution Pack is installed by default on your FortiSOAR system.*

Threat Intelligence Management (TIM) Solution

- Built upon the Threat Intelligence Life Cycle, FortiSOAR's well-researched TIM Solution allows for comprehensive threat feed management and a framework to create, consume and share, contextual, actionable threat intelligence.
- Offers native integration with FortiGuard for reputation lookup and daily feed ingestion.
- Noteworthy highlights of the solution include the ability to create and share feed datasets (using TAXII server) and generate threat intelligence reports. It also includes the ability to create goal-based workspaces for collecting, analyzing, and sharing actionable threat intelligence and feed management capabilities using source confidence, TLP, expiry, etc., parameters.
- Released in the 'Preview' mode to gather your important feedback. It is available as an add-on solution pack in the content hub.

Machine Learning Powered Phishing Classifier

- Addressing the need to triage Phishing alerts more efficiently, the Phishing Classifier feature provides a Machine Learning-based classifier that helps to identify Phishing emails with a confidence score.
- To get you going faster, FortiSOAR gets installed with a pre-trained dataset, and yet it allows you to provide your own organization's contextual dataset.

Queue and Shift Management

- Intelligent, automated assignment solution based on queues and shift spreads. Multiple assignment models offer better ways to assign records.
- Shift Management allows the creation of Shift Rosters with Shift leads and team members.
- Ability to manage shift handover processes for smooth shift transitions.
  Note: *The Queue and Shift Management feature replaces the Queue Management feature that was present in the earlier releases of FortiSOAR. Automated record assignments were not supported in Queue Management.*

Notification Framework

- Notification framework makes its debut as a centralized framework for diverse notifications, such as email notifications, UI notifications from various services (such as alerts/incidents/tasks assignments), Comments @mentions, workflow failures, etc.
- Allows for the ability to use integrations in creating custom notification channels and using the new rule engine to create notification rules.

FortiSOAR integration with FortiMonitor

- FortiSOAR is integrated with FortiMonitor to enable monitoring including CPU, RAM, Disk monitoring, network card bandwidth, Nginx, PostgreSQL monitoring, etc., of your FortiSOAR instances using FortiMonitor.
- FortiMonitor can also monitor nodes of an HA cluster, and tenancy data replication lag in an MSSP environment.

Data Archival

- Never miss your compliance of preserving important data, while keeping your application nimble and high-performant. This release introduces a well-defined process for archiving data to store of your choice. Data archival enables you to retain data for longer by preserving it in your data lake. You can archive data into an external database instance, or into a SIEM/log management product using Syslog forwarding.
- Every record is archived with a signature so that any tampering can be easily identified.

Recycle Bin

- 'Recycle Bin' is made available for soft deletion of workflow and module records, making it possible to restore these in case of accidental deletions.

Manual Input Step Enhancements

- This much-used step in playbook workflows gets significant enhancements like the ability to create global manual inputs that are independent of records, the ability to display manual inputs on a different suitable record other than the source, RBAC enhancements, improvements to show more information in its playbook execution logs, usability enhancements, integration in notification framework and other important updates.

Support For RADIUS Server Authentication

- Users can be authenticated for FortiSOAR using RADIUS authentication. Users whose authentication type is set to RADIUS can log in to FortiSOAR using their RADIUS credentials.

Important HA Enhancements

- Ability to install custom connectors on a High Availability (HA) cluster using the UI.
- Ability to use replication slots to set up replication for your HA cluster. Using replication slots to set up HA clusters, adds support for differential synchronization between the primary node and the secondary nodes when the secondary nodes get out of sync with the primary node.

- Other enhancements include:
  - Addition of the `clone-db` option to the HA command in the admin CLI.
  - Updates in the "Administration Guide" for multihoming containing instructions for extending support for two NICs on a FortiSOAR appliance for controlled traffic routing.

Case Management Enhancements

- A new 'Date' field type is added to support the requirement of fields that need only the date to be displayed without the time component.
- Additionally, DateTime fields, such as 'Created On', 'Modified On', etc. are now stored with milliseconds precision (earlier it was seconds), allowing greater accuracy in sequencing events.
- Added a lighter version of the data grid widget, for better performance and usability.
- The information shown in the row-expansion section can now be edited inline for meeting a wider range of use case requirements.
- MIME type validations for file uploads, allowing administrators to restrict potentially malicious files of types such as .exe, .bat, etc. to be uploaded into FortiSOAR.
- Ability to change the listing page title if you want to name it something other than the plural name of the module.
- Usability enhancements to relationship widget to include or exclude relationships.

Playbook Framework Enhancements

- A new '*Ingest Bulk Feed*' playbook step is added to enable you to insert and update large volumes of records, primarily used while ingesting from Threat Intel Feeds, or others such as Vulnerabilities and Assets.
- Significant optimizations in the runtime of the workflows for better Memory and CPU consumption thereby improving playbook execution times as well as OS resource consumption during playbook execution.
- Important enhancements are made to the Data ingestion experience including the ability to trigger the ingestion instantly (ad-hoc), utilize previously saved ingestion logs for data mapping, and the ability to attach a custom data ingestion playbook collection for meeting advanced use cases.
- Added support for YAQL as an additional query filter language (in addition to JINJA). YAQL (Yet Another Query Language) is an embeddable and extensible query language, which allows users to perform complex queries against arbitrary objects and makes data filtering and manipulation much easier while developing playbooks. More details about YAQL are available here.
- RBAC-controlled ability to view all “System” playbook collections on the playbook listing section.

Export and Import Wizards Enhancements

- Multiple enhancements have been made to the Export and Import Wizards including the ability to selectively export and import fields in a module and items in the navigation structure. Support is also added for inclusion or exclusion of correlations of export of correlations data along with module's record data and for displaying total records imported on the 'Review Import' page of the Import Wizard.

Connector Enhancements

- Ability to install custom connectors on an FSR Agent from the FortiSOAR node using the UI.
- Ability to install connector dependencies from the FortiSOAR UI.

Support to configure account lockout settings

- Administrators now have the option to configure the number of times users can enter incorrect passwords while logging into FortiSOAR before their account gets locked. By default, this is set to 5 (times). Administrators can also 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).

Onboarding Guide

- The Onboarding or Setup guide helps first-time or recurrent administrators of to optimally set up based on best practices.

Built-in Connector and Widget Enhancements

- Multiple built-in connectors like Utilities, Report Engine, FortiSOAR ML Engine, SMTP, and Code Snippet have been updated.
  For more information on FortiSOAR Built-in connectors, see the "FortiSOAR™ Built-in connectors" article.
- A new 'Phishing Classifier' connector has been introduced as a system connector.
- New widgets such as Manage Datasets, Card Tiles, and Feed Configuration Settings, are now available on the Content Hub.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR version 7.2.0.

Removed Rules Engine

- The Rules Engine is removed in the 7.2.0 release. The Rules Engine was already marked as 'Deprecated' from release 7.0.1 onwards, and now will no longer be available.
- The rules engine is removed since you can achieve its functionality and more, by using FortiSOAR's powerful conditional playbook triggers. For example, the conditional triggers in playbooks enable users to execute steps on a combination of conditions, which was very complicated using the rules engine.

Before you upgrade your system to FortiSOAR release 7.2.0, ensure that you have moved existing rules to FortiSOAR's powerful conditional playbook triggers, else the rules information will be lost.

Removal of the `approvalHost` global variable

Playbooks that contain a reference to the `approvalHost` global variable fail with the '`approvalHost variable undefined`' error since the `approvalHost` global variable is removed from release 7.2.0 onwards. To resolve this error, replace the `approvalHost` global variable in the playbook with the `Server_fqhn` global variable.

System user for integrations runtime should have minimal privileges on the file system

From FortiSOAR release 7.2.0 onwards, integrations are run using the `fsr-integrations` user instead of the `nginx` user. Therefore, code snippets that try to write on a file system that is outside `/opt/cyops-integrations` or `/tmp` might be impacted and you also need to ensure appropriate permissions have been given to the `fsr-integrations` user.

Writing on file systems using code snippets outside `/tmp` is highly discouraged.

Renamed the update.cybersponse.com repository

The FortiSOAR repository update.cybersponse.com has been renamed to https://repo.fortisoar.fortinet.com/ in release 7.2.0. 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.

Deprecated Queue Management

Queue Management has been deprecated from this release. If you have set up queue management the same will not be affected when you upgrade to release 7.2.0. However, it is highly recommended that you migrate your queues (manually) to the newly introduced 'Queue and Shift Management' feature in place of queue management. This feature handles automated record assignments, which were not supported in Queue Management. For more information, see the *Queue and Shift Management* chapter in the "User Guide."

Blocked importing of OS-related packages (os, sys, subprocess) using the Code Snippet connector

By default, users cannot import and run OS-related packages (os, sys, subprocess) using the Code Snippet connector. This has been done to prevent users from running arbitrary Python codes that could result in system code execution.

If users require to import and run OS-related packages using the Code Snippet connector, then they require to customize the `/opt/cyops-integrations/integrations/configs/config.ini` file by adding the `allow_os_packages = true` statement in the `config.ini` file.

Introduction of the SOAR Framework Solution Pack

Release 7.2.0 introduces the SOAR Framework Solution Pack (SP) which is the **Foundational** Solution Pack that creates the framework, including modules, dashboard, roles, widgets, etc., required for effective day-to-day operations of any SOC. The Incident Response modules have been removed from the FortiSOAR platform and moved to the SOAR Framework SP. Therefore, from release 7.2.0 the Incident Response modules, i.e., Alerts, Incidents, Indicators, and War Rooms are not part of the FortiSOAR platform, making it essential for users to install the SOAR Framework SP to optimally use and experience FortiSOAR's incident response. For detailed information about the SOAR Framework SP, see the SOAR Framework SP documentation.

Fresh installations of FortiSOAR release 7.2.0 will by default, have the SOAR Framework Solution Pack installed.

Post-upgrade to 7.2.0 users should be assigned appropriate permissions for Content Hub

Once you upgrade 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'.

Post-upgrade to 7.2.0 user cannot see the earlier record assignment notifications

Once you upgrade to 7.2.0, record assignment notifications such as task assignment notifications from earlier releases are not visible in FortiSOAR's new notifications framework.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 7.2.0 from versions 7.0.0, 7.0.1, or 7.0.2 only. Also, once you have upgraded your configuration, you must log out from the FortiSOAR UI and log back into FortiSOAR.

When you upgrade FortiSOAR, all current users are treated as 'Named' users and associated restrictions are applied.

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 into the FortiSOAR Platform during the upgrade.

For details about upgrading FortiSOAR, see the *FortiSOAR Upgrade Guide*.

Product Integration and Support

Web Browsers & Recommended Resolution

FortiSOAR 7.2.0 User Interface has been tested on the following browsers:

- Google Chrome version 100.0.4896.75
- Mozilla Firefox version 99.0
- Microsoft Edge version 99.0.1150.55
- The recommended minimum screen resolution for the FortiSOAR GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI might not get properly displayed.

Virtualization

This section lists FortiSOAR version 7.2.0 product integration and support for virtualization:

- AWS Cloud
- Fortinet-FortiCloud
- VMware ESXi versions 5.5, 6.0, and 6.5
- Redhat KVM

For any other virtualization or cloud hosting environment, you can install CentOS 7.x and then install FortiSOAR using CLI. For more information, see the "Deployment Guide."

Resolved Issues

Following is a list of some of the important defects addressed in **FortiSOAR release 7.2.0**. This release also includes important security fixes.

- **Bug #0679817**: Fixed the issue of import failing in the case of playbook collections if playbooks in the collection contained a remote reference step.
- **Bug #0730539**: Fixed the issue in the handling of default value attributes so that the default value gets honored even if records are updated using APIs, such as updating the attribute using a playbook, such as the 'Escalate' playbook. Earlier, the default value attribute defined in the MMD got applied only when records were created using the FortiSOAR UI.
- **Bug #0703540**: Fixed the issue with generated reports to improve their readability. Earlier, generated reports that had long paragraphs would have their word-wrapped, which caused issues with readability. Now, the generated reports have end-of-the-line words formatted as hyphenated words, or the words are moved to the next line.
- **Bug #0744893**: Fixed the following issues in the grid view of a playbook:
  - Inability to horizontally scroll the playbooks grid if more columns are added to the grid.
  - Visibility of the 'Last Modified On' option in the grid. The 'Last Modified On' option is for system use and it being visible on the grid used to create confusion. Now, only the 'Modified On' option is visible in the grid.
- **Bug #0746678**: Fixed the issue with the default sort that is specified in the model metadata for query API.
- **Bug #0747880**: Fixed the issue of export silently failing in the case of referenced playbooks that contain references to themselves or looped references.
- **Bug #0758480**: Fixed the issue of the 'Configure Report Inputs' field in reports not getting sorted in alphabetical order.
- **Bug #0763209**: 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.
- **Bug #0766486**: Fixed the issue in report scheduling where scheduling would not work if the input type is specified as 'lookup' for the report.
- **Bug #0769338**: Fixed the issue with the 'Comments' widget, both on the collaboration panel and the main record detail view, wherein some records that contain HTML in a rich text field, users cannot see the text that they are typing in the text field; however, the text is visible in the 'preview' mode on the widget.
- **Bug #0770460**: Fixed the inconsistency in the naming convention for many-to-many fields when self-linking for the reverse module by the API.
- **Bug #0770515**: Fixed the 'log4j' security vulnerability and removed the dependencies on affected packages.
- **Bug #0770706**: Fixed an issue with relative date filters that caused a custom filter using the 'created on' field to not work in the 'Find Records' playbook step.
- **Bug #0775432**: Fixed the issue of failed cluster commands accumulating for passive nodes in an HA cluster environment.
- **Bug #0777960**: Fixed the issue of FortiSOAR not displaying maintenance pack or security patch information on the UI/CLI, leading to the inability of administrators to confirm whether a maintenance pack or security patch is installed on the FortiSOAR system. Now, you can see these details on the UI wherever FortiSOAR's version information is displayed, including the version dialog, login page, etc.
- **Bug #0782224**: Fixed the issue breaking of a `do_until` loop in the case of a reference playbook that contains a manual input. Now, until user input is provided, the reference playbook will continue retrying and keep sending the manual input.
- **Bug #0782839**: Removed the requirement of assigning `Create` or `Modify` permissions on the `Application` module to save user preferences, which fixed the following issues:

  - Saving user preferences.
  - Saving user-created filters as 'User' filters and not as 'System' filters.
  - Displaying of user-level filters only to the users.
- **Bug #0784317**: Fixed an issue with SSO users being unable to log into FortiSOAR in an AWS instance, where the user_id was set as the email of the users.
- **Bug #0789581**: Fixed the issue of administrators being unable to implement custom password policies. Now, administrators can set up custom password policies, which enforce additional restrictions (apart from the default rules) on the passwords that users can create.
- **Bug #0796003**: Fixed the issue with the 'Is In List' and 'Is Not In List' conditions when added to the 'On Create' trigger playbooks that caused a failure to trigger the 'On Create' playbooks even after fulfillment of the 'Is In List' and 'Is Not In List' conditions.
- **Bug #0797162**: Fixed the Spring4Shell and CVE-2022-22963 vulnerabilities.

www.fortinet.com