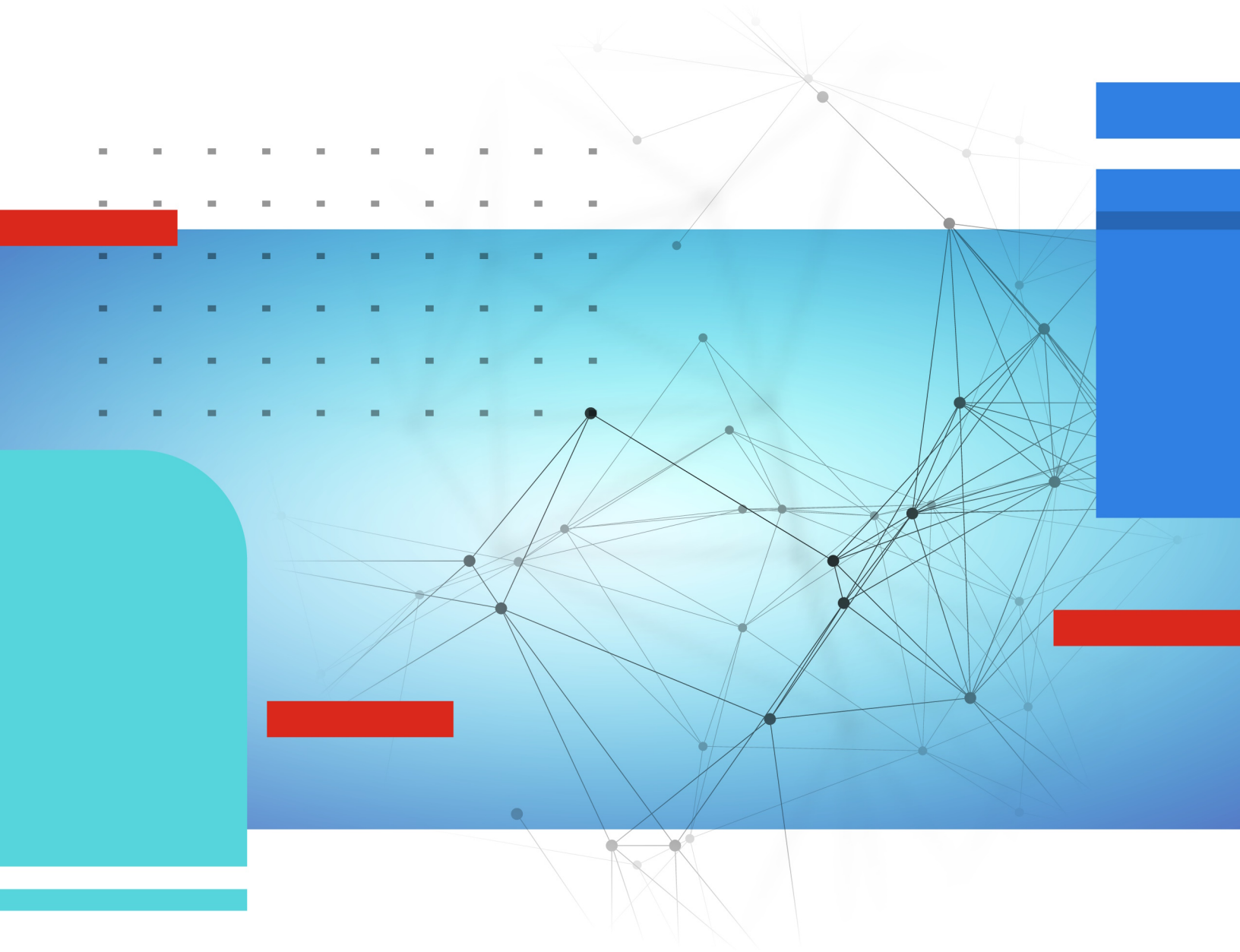
Release Notes

FortiSOAR 7.5.0



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

March, 2024
FortiSOAR 7.5.0 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-03-26	Initial release of 7.5.0

FortiSOAR 7.5.0 Release

Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) release 7.5.0 offers notable enhancements in terms of performance, usability, and stability. An operating system upgrade to RHEL/Rocky Linux 9.3 is one of the main changes, along with support for internationalization (i18n), API-based authentication, enhanced generative AI (FortiAI) for AI-based alert insights, increased upgrade reliability, and CICD-related improvements. The release also includes support for essential widget customizations, such as non-modal widgets, which have a fully functional background when a widget is open. Additionally, the release includes performance enhancements and multiple security fixes to address vulnerabilities in FortiSOAR.

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

New Features and Enhancements

Support added for Internationalization on the FortiSOAR platform

- Release 7.5.0 brings 'Internationalization' capability to the FortiSOAR platform, allowing FortiSOAR to adapt to the language, cultural, and other requirements of a particular locale.

API key based authentication support

- Release 7.5.0 adds support of using API keys for authentication, i.e., for managing automation scenarios and using FortiSOAR APIs. Automation can now utilize an API key or HMAC authentication. API key authentication is also beneficial in outbound Threat Intelligence Management feed distributions, particularly for clients such as firewalls that only support basic authentication.

Upgrade of the Operating System used for FortiSOAR

- In release 7.5.0, the operating system (OS) used for FortiSOAR is upgraded to Rocky Linux/RHEL 9.3 from Rocky Linux/RHEL 8.8/8.7 to ensure that FortiSOAR is running on a stable and secure OS. Rocky Linux/RHEL 9.3 offers several improvements over Rocky Linux/RHEL 8.8/8.7, including enhanced security, improved kernel and updated packages; details can be found in the Release Notes For Rocky Linux 9.3 and Upgrading from RHEL 8 to RHEL 9 articles. For details, see the *Deployment* and *Upgrade* guides.

Upgrade Framework

- Release 7.5.0 introduces an "Upgrade Framework" to enhance the flexibility, usability, and efficiency of the FortiSOAR upgrade process. This framework improves the upgrade experience by offering users the ability to customize the pre- or post-upgrade phases.

Support for Pre and Post Processing Rules for records being ingested into FortiSOAR

- FortiSOAR includes a rule-based pre-processing feature that is activated before incoming records are stored in the database, providing the flexibility to make decisions such as dropping records based on predefined criteria. Additionally, the implementation of a post-processing rule improves record management by linking similar records based on specified similarity criteria. This post-processing rule enables intelligent linking of records, reduces reliance on resource-intensive playbooks and optimizes system performance. In summary, these rule-based pre- and post-processing features enhance the control and efficiency of the SOAR platform.

API Enhancements

- Added validation for picklist values and their attributes configured in the module when passed using an API.

Support for GPT disk partitioning

- To support disk sizes larger than 2 TB, FortiSOAR OVAs starting with the 7.5.0 release come pre-configured with a GPT-based disk layout. Previously, FortiSOAR OVAs were shipped with an MBR-based disk layout, which limited disk management to a size of 2TB. If you already have a FortiSOAR instance and need a partition larger than 2 TB, we recommend creating a new FortiSOAR VM on release 7.5.0 or later and utilizing the Export and Import wizards to migrate your data from the old instance to the new one. This is required as FortiSOAR does not support a combination of MBR and GPT partitions.

Widget customizations

- Added support for the following widget customizations:
  - Non-modal, to allow the widget to be accessed across the FortiSOAR application. Alternatively, you can specify the pages in FortiSOAR where the widget will appear as a `drawer`.
  - Interactive background, enabling users to perform tasks in the current context.
  - Assign a name to the widget.
  - Draggable.

Performance Improvements

- Release 7.5.0 includes several performance improvements, such as limiting the number of many-to-many relation records fetched when sending response. This helps improve performance and prevent out-of-memory exceptions.

Documentations Updates

- Added the "Widget Development" guide that contains step-to-step information on developing widgets, right from creating a repository to submitting the widget on the FortiSOAR Content Hub.
- Added the Widget Development guide aimed at helping new or experienced administrators configure the system optimally using best practices. It intends to familiarize you with the application and start exploring some of the core capabilities offered by FortiSOAR.

Built-in connectors, connectors, solution packs, and widget enhancements

- Updated multiple built-in connectors such as the Utilities connector, Report Engine connector, and Utilities connector etc. For more information on FortiSOAR Built-in connectors, see the "FortiSOAR™ Built-in connectors" article.
- Added multiple connectors such as SecurityTrails, Keeper Secret Manager, Splunk (and its associated application) and Cymulate ASM. Updated multiple connectors such as Palo Alto Enterprise DLP, Tenable Security Center, Fortinet FortiGuard Threat Intelligence, and Qualys.
- Added multiple solution packs such as ConnectWise ScreenConnect Attack, Outbreak Response Lazarus Rat Attack, and Androxgh0st Malware Attack. Updated multiple solution packs such as FortiManager ZTP Flow, OT Vulnerability Management, and SOAR Framework Solution Pack.
- Added multiple widgets such as AI Assistant, SOC Overview Sankey, and Outbreak Framework Configuration. Updated multiple widgets such as Fields of Interest widget and Record Distribution widget.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR release 7.5.0.

Upgraded the Operating System supported for FortiSOAR

In release 7.5.0, the operating system (OS) used for FortiSOAR is upgraded from Rocky Linux/RHEL 8.8/8.7 to Rocky Linux/RHEL 9.3 to ensure that FortiSOAR is running on a stable and secure OS. Rocky Linux/RHEL 9.3 delivers a number of enhancements over Rocky Linux/RHEL 8.8/8.7, including increased security, an improved kernel, and updated packages. For detailed procedures, see the *Deployment Guide*.

Change in the default notifications purging behavior

Starting from release 7.5.0, FortiSOAR, by default, runs a system schedule, every day at midnight (00:00 hrs) to purge all system notifications, both read and unread, that are older than 14 days. Previously, FortiSOAR only purged only 'read' system notifications that were older than 30 days. Therefore, if you are upgrading to FortiSOAR release 7.5.0 and have a large number of notifications, the deletion process might take some time.

Change in the default behavior fetching records with many to many relationships

Prior to release 7.5.0, fetching records with many-to-many relationships, such as Alerts and Indicators often led to out of memory exceptions, especially during memory-intensive processes such as indicator extraction, where it was possible for indicators being linked to thousands of alerts. In release 7.5.0, the default limit for fetching records with many-to-many relationship has been set to 100. This change is intended to enhance performance and prevent out-of-memory exceptions during response serialization.

Change in the behavior of picklist value validation when data is submitted using an API

Release 7.5.0 onwards, the picklist values and their attributes configured in the module are validated when passed using an API. For example, when creating an alert record and specifying its status, the value of the status passed must be one of the options from the 'AlertStatus' picklist. If a value from any other picklist is passed, the API call will fail. In releases prior to 7.5.0, this validation was not in place, allowing API calls to pass. Therefore, from release 7.5.0 onwards, the

playbook execution will fail for playbooks created with any attribute that is mapped to a picklist value not part of the configured picklist name.

Picklist values and their attributes configured in the module are not validated for the 'bulk feed' step of records when passed using an API.

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. You can change the default behavior using the playbook designer, for more information, see the 'Distributed Tenancy Support' chapter in the *Multi-tenancy Support in FortiSOAR* guide.

Post-upgrade to release 7.4.2 or later, the system's swap use parameter is not included in the email notifications set up to track your system's resource utilization

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.

The Pending Tasks icon does not display the count of legacy approvals

The number of historical (legacy) approvals, i.e., those that were in place before your FortiSOAR instance was upgraded, are not displayed in the **Pending Tasks** icon. However, the historical approval count is considered after you click the **Pending Tasks** icon.

Removed the source-control subcommand from the FortiSOAR Admin CLI

The source-control subcommand has been removed from the FortiSOAR Admin CLI (csadm) because the FortiSOAR Continuous Delivery solution pack performs the same purpose more effectively. The Continuous Delivery solution pack enables you to release higher-quality code and automate your content development operations while creating, testing, and deploying content through Source Control in a continuous and iterative manner. For more information, see the FortiSOAR Content Hub.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 7.5.0 from version 7.4.0, 7.4.1, 7.4.2, or 7.4.3 only. In release 7.5.0, the operating system (OS) used for FortiSOAR is upgraded is upgraded from Rocky Linux/RHEL 8.8/8.7 to Rocky Linux/RHEL 9.3 to ensure that FortiSOAR is running on a stable and secure OS. Rocky Linux/RHEL 9.3 delivers a number of enhancements over Rocky Linux/RHEL 8.8/8.7, including increased security, an improved kernel, and updated packages. More information can be found in the Release Notes for Rocky Linux 9.3 and Upgrading from RHEL 8 to RHEL 9 articles. For detailed procedures, see the *Upgrade Guide*.

Once you have upgraded your configuration, 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 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 7.5.0 User Interface has been tested on the following browsers:

- Google Chrome version 122.0.6261.113
- Mozilla Firefox version 123.0
- Microsoft Edge version 122.0.2365.80
- Safari version 17.3 (19617.2.4.11.8)
- 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 7.5.0 product integration and support for virtualization:

- AWS Cloud
- Fortinet-FortiCloud
- VMware ESXi versions 5.5, 6.0, 6.5, 7.0, and 8.0
- Redhat KVM
  NOTE: The KVM OVA is not certified on FortiSOAR release 7.5.0.

For any other virtualization or cloud hosting environment, you can install Rocky Linux or RHEL 9.3, and then install FortiSOAR using CLI. For more information, see the "Deployment Guide."

Resolved Issues

The following important issues have been fixed in **FortiSOAR release 7.5.0**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

FortiSOAR UI Fixes

Bug ID	Description
0870699	Fixed an issue where a working session would abruptly close and the FortiSOAR application would log out when opened in multiple tabs on the same browser.
0968722	Fixed the issue where adding self-module relations, such as many-to-many or lookup links for the same module, did not display the relationship in the relationship tab even though the relationship was created.
0998623	To export a module's records, such as Alert records from the modules grid view, you can select options such as 'Export All Columns As CSV', 'Export Visible Columns As PDF', etc. Previously, the date/time fields in the exported CSV or PDF file were displayed in the UNIX Epoch format, which was not human-readable. Now, the date/time fields in the exported CSV or PDF file are displayed according to the datetime format selected on the FortiSOAR UI.
0973790	Fixed an issue with threshold values not being set or validated in the 'System Health Thresholds' section on `System Configuration` page in FortiSOAR. Previously, users could input excessively high values like 999999999 in percentage fields such as Memory Utilization (%) or the Workflow Queue field, and the configuration would still be saved. To address this, threshold values and validations have been implemented for the system health monitoring properties.

Playbook Fixes

Bug ID	Description
0933597	Fixed the issue with comment linking in the "Step Utilities > Message" step. The comment in this step was not linked to the provided record IRI; instead, it was linked to the record on which the playbook executed.
0963506	Fixed an issue that caused a playbook to fail when a user specified an incorrect Jinja expression for an FSR agent configuration in the playbook's connector step. Now, if an incorrect agent is selected dynamically based on the configuration name in the playbook connector step, the connector step will be executed using the connector’s default configuration on the system instead of the agent.

0996235	Fixed the issue where users without a last name were unable to provide input for a playbook containing a manual input step. Now, users can now provide manual inputs regardless of whether they have a last name.
1009285	Fixed the issue that caused the 'Bulk Ingest' step to fail when the module contained a field of type 'checkbox'.

Other Fixes

Bug ID	Description
0873027	In your FortiSOAR high-availability (HA) cluster, you might have experienced a delay in loading the manual input popup on a record. This performance issue has been resolved, and now the manual input popup is displayed almost immediately.
0952643	In your FortiSOAR HA cluster, you might encounter websocket issues such as the Data Ingestion Wizard continuously displaying "fetching in progress" even after the 'fetch' playbook has failed or succeeded, if the nodes of your HA cluster are in different timezones. This issue has been resolved and the Data Ingestion Wizard fetches data, even if the nodes of your HA cluster are in different timezones.
0975974	Fixed the inconsistency displaying the median value on dashboards and grids. Now, the same data will be shown in both the dashboards and the grids. For example, if you are using the Time to X widget in the dashboard with the median operation and specify the time range filter as last the 15 days on 16 January 2024 09:00 hours, then it will filter records from 1st January 2024 00:00 hours to 16th January 2024 09:00 hours.
0985051	Fixed an issue with schedules where setting a schedule to `*/<some value>` always defaulted to UTC instead of the specified timezone.
0985949	Fixed an issue that caused performance problems by allowing services like the workflow service to keep the PostgreSQL connection idle. To avoid idle connections, these services are now periodically restarted.
0987103	Fixed the issue with searching and filtering teams when the number of teams exceeds 30.
0997906	Fixed the issue with Queue Management, where the 'Round Robin' method was not working as intended and was not distributing the load evenly.
1005105	Fixed the issue where the `csadm package content-hub sync --force` command was failing because the request was timing out.

Known Issues and Workarounds

Issue 0931649: For the RichText HTML editor error messages for any unavailable resources are not displayed. For example, if you have a playbook with the "Create Record" step on the "Alert" module and you insert an image URL that is inaccessible to your instance into an HTML-type field such as "Description," RichText HTML editor does not display any errors. Earlier an error such as "`Cannot convert blob:.....Resource might not exist or is inaccessible`." used to be displayed.
This issue will be addressed in upcoming releases of FortiSOAR.

Issue 0950880: Avoid using the correlations 'Append' option in the 'Create Record' step of Data Ingestion Playbooks, as this is not currently supported. Instead, if you have a special use case for linking relationships while creating records, utilize the 'Overwrite' option to add correlations in the 'Create Record' step.
This issue will be addressed in upcoming releases of FortiSOAR.

www.fortinet.com