

Release Notes

FortiSOAR 7.6.0



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



August, 2024

FortiSOAR 7.6.0 Release Notes

00-400-000000-20210112

TABLE OF CONTENTS

Change Log	4
FortiSOAR 7.6.0 Release	5
New Features and Enhancements	6
Special Notices	9
Changes to FortiSOAR Licensing	9
Changes to the manual upgrade process for FSR Agent	9
Upgrade Information	10
Product Integration and Support	11
Web Browsers & Recommended Resolution	11
Virtualization	11
Resolved Issues	12
FortiSOAR UI Fixes	12
Playbook Fixes	12
Other Fixes	13
Known Issues and Workarounds	15

Change Log

Date	Change Description
2024-08-13	Updated information about the Trial License in the Special Notices chapter.
2024-08-01	Initial release of 7.6.0

FortiSOAR 7.6.0 Release

Welcome to the new release of FortiSOAR™ 7.6.0. This update introduces enhancements to elevate your security orchestration, automation, and response capabilities. Whether you're a small team or a large enterprise, our new licensing options cater to your needs. Experience improved High Availability with cost-effective options for on-premise deployments and streamlined resilience for cloud environments. Enjoy an enhanced product trial experience, a more intuitive code editor, and a variety of new solution packs and connectors. Additionally, benefit from advancements in FortiAI for more effective analyst investigations and explore improved SOAR Framework and Outbreak Management solutions. Discover how FortiSOAR 7.6.0 can transform your security management.

In line with Mark Twain's wisdom, "**The secret to getting ahead is getting started,**" we introduce the FortiSOAR Starter Edition in this release—your perfect entry point into advanced security orchestration. So, you could also say - "**The secret to SOARING ahead is getting started with FortiSOAR!**"

The release also includes performance enhancements and security updates 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

In this release, we have introduced a variety of new features and enhancements designed to maximize your efficiency and enhance your overall experience with FortiSOAR™ 7.6.0.

Licensing Updates

- **Starter Edition:** Ideal for small to medium-sized enterprises or teams within larger organizations, this affordable entry point offers advanced security orchestration capabilities with support for up to 10,000 actions per day. It is also suitable for developers or as a staging instance for FortiSOAR.
- **Cost-Effective On-Premise HA Option:** Deploy the new on-premise High Availability (HA) edition as a secondary node in a clustered setup for both 'Perpetua' and 'Subscription' licenses. This ensures seamless failover and enhanced reliability without breaking the bank.
- **Enhanced Trial License:** Experience FortiSOAR to its fullest with increased action limits from 200 to 1000 actions per day. Select either the 'Enterprise' or 'Multi-Tenant' trial license based on your deployment requirements. For details, see the [Licensing FortiSOAR](#) chapter in the "Deployment Guide."

Upgrade Process Enhancements

- **Streamlined Upgrade Process:** The upgrade framework validates the feasibility of the upgrade before proceeding with the actual process. It also separates post-upgrade tasks, such as database migrations, to facilitate smoother upgrades and simplify failure handling. Furthermore, it enhances the upgrade experience by allowing users to customize the pre- or post-upgrade phases. Additionally, the ability to pre-download upgrade packages helps reduce application downtime and ensures a faster and more reliable upgrade experience. For details, see the ["Upgrade Guide."](#)

Code Editor Enhancements

- **IntelliSense Integration:** Boost your coding efficiency with IntelliSense in the code editing features of FortiSOAR. Benefit from intelligent code completion, syntax error highlighting, and a more intuitive and responsive interface. For details, see the [Building your own connector](#) chapter in the "Connectors Guide," and the [Widgets Library](#) chapter in the "User Guide."

FortiSOAR User Interface Enhancements

- **Enhanced Jinja Editor:** Improved editor UI with ability to view the test JSON data in a better way and including playbook step execution data for easier debugging. This makes Jinja editing and testing much easier and simpler. For details, see the [Dynamic Values](#) chapter in the "Playbooks Guide."
- **Improved System Configuration:** Easily locate settings with an organized layout on the "Application Configuration" tab and a new "General" tab for added convenience.
- **Enhanced 'Choose Widget' Dialog:** Experience a more organized layout with categorized widgets, icons, titles, descriptions, and a search box for easier widget selection.
- **Grid Widget Light Mode:** Enable the 'Light Mode' globally for better performance and usability.
- **'Executed Playbooks Log' filter enhancement:** Included an option for filtering playbooks based on their execution mode, INFO, DEBUG, or, ANY.

- **Improved Manual Trigger Step:** The "Configure Visibility Condition" option in a manual trigger has been enhanced to enable the triggering of playbooks based on a record's UUID. Multiple UUIDs can be included in a list or CSV format.
- **Improvements in the Connector UI:** A new field called "Contributor" has been added to the connector's configuration page to show the names of contributors. This feature is particularly helpful for community contributions. Additionally, an option to display extra information about parameters as a subtitle has been included on the Fetch Data screen of the Data Ingestion Wizard.
- **Other UI Enhancements:** Improved user experience by alphabetically sorting event types in the `Purge Audit Log` dialog, making it easier for users to find a specific event type. Additionally, a '**Refresh**' button has been added to the **Shift Management** tab on the `Queue & Shift Management` page.

Administrative Enhancements

- **Record Ownership Customization:** In multi-tenant environments, restrict record ownership to tenant teams for better control.
- **Improved ROI Calculations & Analytical Widgets:** Customize the ROI widget with your preferred currency and make the 'Time Range' and 'Percentage Change' fields optional in performance widgets.
- **Disk Space Optimization:** Reclaim unused disk space using advanced PostgreSQL utilities to address database bloat and improve performance.
For details, see the `Setting up auto-cleanup of workflow execution history` topic in the [Debugging and Optimizing Playbooks](#) chapter of the "Playbooks Guide."
- **Export and Import Wizards Enhancements:** Directly export and import 'Export Templates' using these wizards. Additionally, the Export Wizard enables filtering records by their UUID, making it easier to export specific records. For details, see the [Application Editor](#) chapter in the "Administration Guide."
- **Playbook Updates:** Global variables will no longer be automatically replaced when importing a playbook collection.
- **Segmented Network Support Improvements:** A new option called '**Update Config**' has been added to the 'Agent Actions' column in the FSR Agent grid. This option allows updating the configuration on the Agent machine with the latest settings.
For details see the "[Administration Guide](#)."

Setup Guide Updates

- **Setup Guide as a widget:** From release 7.6.0 onwards, the Setup Guide has been transformed into a standalone widget. This change was made to allow for a more focused approach to the Setup Guide and the flexibility to release updates as needed. For details, see the [Setup Guide Widget documentation](#).
- **Improved Exclusion List Management:** Easily exclude specific extracted indicators from enrichment by adding them to an exclusion list. For details, see the [SOAR Framework Solution Pack documentation](#).

Solution Packs, Connectors, and Widget Enhancements

A wealth of new content and enhancements have been added. Here are some examples:

- **Notable New and Updated Solution Packs:**
Added important Solution Packs such as Platform Utilities, which includes the Key Store module for improved data management across various solution packs, ensuring smooth integration and efficient storage of structured data, and the SLA Management Solution Pack offers precise SLA calculation and comprehensive automation for efficient management across industries. Multiple Outbreak Response solution packs have also been introduced to conduct hunts that identify and investigate potential Indicators of Compromise (IOCs) associated with vulnerabilities within operational environments of FortiSIEM, FortiAnalyzer, QRadar, and Splunk.
Furthermore, several key solution packs are updated, including the SOAR Framework Solution Pack, which

includes significant changes such as the migration of the Key Store module and playbook reorganization across solution packs, and the SOC Utilities Solution Pack has also been enhanced to optimize efficiency with streamlined utilities for seamless integration, improving security operations and workflow efficiency.

- **New and Updated Connectors:** Multiple integrations (Fortinet Fabric and third-party) have been released and updated – few notable ones being Fortinet FortiEDR, Fortinet FortiGate, Utilities, Database, Exchange, Slack, GitHub, IBM IAM, RSS Feed, Cisco Meraki MX L3 Firewall, SAP Enterprise Threat Detection Cloud, and NetScaler ADC.
- **New and Updated Widgets:** Added multiple widgets such as Submit Content Form, Playbook Buttons, and Playbook Execution Wizard. Updated multiple widgets such as Picklist as Phases, AI Assistant, and JSON to Grid. For details, see the [FortiSOAR Content Hub](#).
- **Updated FortiSOAR Rapid Development Kit:** A new version of the Rapid Development Kit has been released, featuring debugging functionality and improved user experience. For details see the [FortiSOAR Rapid Development Kit](#) documentation.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR release 7.6.0.

Changes to FortiSOAR Licensing

In release 7.6.0, two new license editions have been added and the trial license has been updated:

- **HA Edition:** This edition enables an instance to operate as a High Availability (HA) node in a clustered setup. If not included as a cluster node, it can function as a standalone instance supporting 2 users and 1000 actions per day. The HA edition is available for both 'Perpetual' and 'Subscription' licenses and can be used in all environments supporting HA configurations. The 'HA' license should be applied to the node designated as the 'Secondary' node of the cluster, not the 'Primary' node. Additionally, all existing licenses installed on secondary nodes can be converted to the HA license, except for the Dedicated Tenant (Single User Locked), and vice versa.
NOTE: HA License can only be used in conjunction with the FortiSOAR base license. Other licenses, such as TIM or additional users, do not need to be duplicated, and therefore are not applicable to the HA edition.
- **Starter Edition:** Priced lower than the full "Enterprise" edition, this edition offers small to medium-sized enterprises or teams within larger organizations an affordable way to access advanced security orchestration capabilities. It also allows the use of FortiSOAR as a development or staging instance without requiring a full FortiSOAR edition. The Starter edition supports up to 2 users and 10,000 actions per day by default and does not include multi-tenancy support.
- **Trial License Changes:** Starting from release 7.6.0, the trial license for FortiSOAR restricts usage to 2 users and 1000 actions per day. Previously, the trial license was limited to 3 users and 200 actions per day under the "Enterprise" type. Users now have the option to select either the "Enterprise" or "Multi-Tenant" edition for this license.

Key Points for Existing Users:

- Users who have activated their trial license previously will retain their current action count of 200. If after upgrading you do not see the new action count of 1000, you should contact Fortinet Support to clear your existing trial license from your FortiSOAR system and then reactivate the trial license to get the updated action count of 1000.
- Users with an active trial license will remain on the "Enterprise" edition. To switch to the "Multi-Tenant (Manager)" edition, contact Fortinet Support to decommission their current trial and re-register for a new trial license with the "Multi-Tenant (Manager)" edition.

For more information, see the [Licensing FortiSOAR](#) chapter in the "Deployment Guide."

Changes to the manual upgrade process for FSR Agent

In release 7.6.0, the **Perform Manual Upgrade** button has been removed from the 'Agent Upgrade' dialog. Users can now directly click the **Download Agent Installer** link in the Agent Upgrade dialog to manually upgrade their FSR agent if the automatic upgrade fails for any reason.

For details, see the [Segmented Network Support](#) chapter in the "Administration Guide."

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to release 7.6.0 from release 7.5.0. 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 7.6.0 User Interface has been tested on the following browsers:

- Google Chrome version 126.0.6478.127
- Mozilla Firefox version 128.0.2
- Microsoft Edge version 126.0.2592.113
- Safari version 17.5 (19618.2.12.11.6)
- 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 7.6.0 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 7.6.0.



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 7.6.0**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

FortiSOAR UI Fixes

Bug ID	Description
0951771	Fixed the issue where the visibility condition did not work when applied to a multiselect picklist field that was populated.
0955945	Fixed an issue with the Date/Time format for a filter applied on 'Global Search'. The filter's Date/Time format did not match the format set on the FortiSOAR UI.
0961995	Fixed the issue where the 'Set as Default' filter was not being retained or applied to grids in the 'Correlations' sub-tabs of the 'View' panel.
1022900	Fixed the issue where the username was not being populated when using the @ sign in the collaboration panel.

Playbook Fixes

Bug ID	Description
0984457	Fixed an issue where a playbook's trigger step did not respect multiple selections made for a dynamic list field type provided in an input prompt.
1000576	Fixed the issue where web components such as a drop-down on an external manual input form, appeared with a white background, making it challenging to read. From now on, all components on the external manual input form will now adhere to the default 'Space' theme.
1010821	Fixed the issue of UI-triggered playbooks that required record inputs. UI-triggered playbooks are playbooks where users have added a button to trigger a Manual Trigger or Reference Playbook on pages such as the Dashboard, View Panel, Listing, etc. for specific operations.
1015887	Fixed the issue with the Jinja expression not rendering correctly in the 'Simplified' view when a dictionary key contained a space.

Other Fixes

Bug ID	Description
0882723	Fixed the issue where the default value of a field was not being respected in the 'Add' view of a record for a user who does not have access to the field. Now, the default value of that field is applied in the 'Add' view of a record for such users.
0950816	Fixed an issue where changes made to the owners of queues were not being saved while editing queues.
0950880	Fixed the issue where the Data Ingestion Wizard was unable to proceed past the 'Fetch Data' step when the 'Append' option was chosen to include correlations in the 'Create Record' step of Data Ingestion Playbooks.
0957360	Fixed the issue where records were not being cloned when there was an integer field in the display name of a module.
0966289	Fixed the performance metrics widget's Median calculation handling. The time range field value is not considered in the payload if the filter criteria contains any date-time type field.
0973850	Fixed the issue of multiple roles not being considered for field-level permissions. Now, aggregated field-level permissions are being taken into account.
0993829	Fixed the issue where users needed the 'Security Update' permission to mark a comment as important, granting access to unintended security options. Now, users only require the 'Update' permission on the Comment module to mark a comment as important.
1008243	Fixed the browser storage issue related to large metadata and its copies. Release 7.6.0 included optimized browser storage usage for efficient management of model metadata.
1008615	Fixed the issue where FortiSOAR Configuration VM would fail when the proxy username and password contained special characters such as '@', '.', '\$', etc. Support has now been added to allow the inclusion of special characters in the proxy username and password.
1010299	Fixed the issue where listeners started during the testing or editing of connectors were not stopped unless the test configuration or connector was deleted, leading to performance issues due to memory consumption. Now, when a new test configuration is added while editing a connector in FortiSOAR, the listeners started by previous test configurations will be stopped. Furthermore, once the connector is published and configured, all previous listeners started by the test configurations will be stopped.
1040066	Increased the license verification grace period for FortiSOAR to improve handling during an FDN outage.
1014915	Fixed the error with the 'Round Robin' queue, which was incorrectly assigning alerts to the same member instead of assigning alerts to each member of the queue sequentially when alerts were created more than ten minutes apart.

1014917	Fixed the issue where FSR Agent's appliance keys were not getting propagated to other nodes of a cluster when the Agent was created after cluster formation.
1024559	Fixed the issue that prevented FortiSOAR from connecting to the local server if a user skipped the 'Set Hostname' step in the FortiSOAR Configuration VM, resulting in missing entries in the <code>/etc/hosts</code> file. Now, the default hostname entry will be automatically added to the <code>/etc/hosts</code> file if the user skips changing the hostname in the FortiSOAR Configuration VM.
1039585	Fixed the issue of schedules were not being saved when its frequency was set for multiple days in a week.
1047562	Fixed the issue of missing audit logs entries for records such as a manual inputs with its IRI set to null, relationship processing failing in case of linked records such as comments that were not associated with a specific module, etc.
1050554	Fixed the issue encountered by non-admin users when navigating to a dashboard or report that requires user input and then moving to a module page (such as alerts or incidents). Previously, opening and closing the detail view of a record would result in a blank page with a message saying "Please provide required inputs to load the report." Now, opening and closing the detail view of a record correctly displays the listing page of the module.
1050823	Added a check to display lag replication statistics during the suspend-cluster operation.
1053596	Fixed the issue of Threat Intelligence Management (TIM) Feeds not getting purged as the scheduled playbook "Purge Expired Threat Intel feed" was failing due to an out-of-memory error.

Known Issues and Workarounds

There are no significant known issues in this release of FortiSOAR.



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.