

Release Notes

FortiSOAR 7.5.2



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



July, 2025

FortiSOAR 7.5.2 Release Notes

00-400-000000-20210112

TABLE OF CONTENTS

Change Log	4
FortiSOAR 7.5.2 Release	5
New Features and Enhancements	6
Special Notices	7
FortiSOAR release 7.5.2 is an upgrade-only release	7
Upgrade Information	8
Product Integration and Support	9
Web Browsers & Recommended Resolution	9
Virtualization	9
Resolved Issues	10
Graphical User Interface	10
System and Security	10
Known Issues and Workarounds	11

Change Log

Date	Change Description
2025-07-22	Initial release of 7.5.2

FortiSOAR 7.5.2 Release

Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) release 7.5.2 contains some important usability and security fixes to ensure vulnerabilities are fixed in FortiSOAR. It is highly recommended to upgrade FortiSOAR 7.5.0 or 7.5.1 instances to the 7.5.2 release.

New Features and Enhancements

FortiSOAR release 7.5.2 includes important usability and security fixes but does not introduce new features or significant enhancements. We recommend that users currently on release 7.5.0 or 7.5.1 upgrade to release 7.5.2 or later to benefit from these fixes.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR release 7.5.2.

FortiSOAR release 7.5.2 is an upgrade-only release

You can only upgrade to FortiSOAR release 7.5.2 from only FortiSOAR release 7.5.0 or 7.5.1. Fresh installation is not supported for this release. It is highly recommended to upgrade existing FortiSOAR 7.5.0 or 7.5.1 instances to the 7.5.2 release as it includes important usability and security fixes.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 7.5.2 from version 7.5.0 or 7.5.1 only. Also, 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 7.5.2 User Interface has been tested on the following browsers:

- Google Chrome version 138.0.7204.101
- Mozilla Firefox version 140.0.4
- Microsoft Edge version 138.0.3351.83
- Safari version 18.5 (20621.2.5.11.8)
- 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 7.5.2 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.



For any other virtualization or cloud hosting environment such as GCP, Azure, OCI, or, OCI DRCC, you can install Rocky Linux 9.3/9.4/9.5 or RHEL 9.3/9.4/9.5 and then install FortiSOAR using the FortiSOAR CLI installer. Note that release 7.5.2 has been tested with RHEL 9.5 and Rocky Linux 9.5. For more information, see the "[Deployment Guide](#)."

Resolved Issues

FortiSOAR release 7.5.2 release addresses critical security and usability issues. For inquiries about specific bugs, please reach out to Customer Service & Support.

Graphical User Interface

Bug ID	Description
1121559	Fixed the issue where filters in the 'Timeseries' chart stopped working after upgrading FortiSOAR, causing the chart to display all available data instead of the filtered data.

System and Security

Bug ID	Description
1081488	Fixed the issue that required users to have Create, Update, and Delete permissions on the 'Security' module and Read permission on the 'Playbook' module to export alert records as CSV files. CSV files can now be downloaded without these permissions. However, CSV downloads will not be available in the Export Wizard History page, as accessing this page requires Read permission on the 'Security' module.
1098659	Audit log entries larger than 64MB were not being processed. To resolve this, users must add the <code>max_inbound_message_body_size</code> parameter to the <code>gateway.properties</code> file. By default, this parameter value is set to 64MB. To process audit logs larger than 64MB, increase the value of <code>max_inbound_message_body_size</code> as needed. Detailed steps are provided in the topic " Audit Logs not processed when file size exceeds 64MB " in the FortiSOAR Administration Guide.

Known Issues and Workarounds

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



www.fortinet.com

Copyright © 2025 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.