

Release Notes

FortiSOAR 7.3.2



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



February, 2023

FortiSOAR 7.3.2 Release Notes

00-400-000000-20210112

TABLE OF CONTENTS

Change Log	4
FortiSOAR 7.3.2 Release	5
New Features and Enhancements	6
Special Notices	7
FortiSOAR release 7.3.2 is an upgrade-only release	7
Upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster is not supported	7
Upgrade Information	8
Product Integration and Support	9
Web Browsers & Recommended Resolution	9
Virtualization	9
Resolved Issues	10
Security Fixes	10
Other Fixes	10
Known Issues and Workarounds	11

Change Log

Date	Change Description
2023-03-28	Updated the Upgrade Information chapter.
2023-02-22	Initial release of 7.3.2

FortiSOAR 7.3.2 Release

Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) release 7.3.2 contains some important usability and security fixes. It is highly recommended to upgrade FortiSOAR 7.3.0 and 7.3.1 instances to the 7.3.2 release.

New Features and Enhancements

Release 7.3.2 does not have any new features or enhancements and is aimed at fixing some important security and usability issues.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR release 7.3.2.

FortiSOAR release 7.3.2 is an upgrade-only release

You can only upgrade to FortiSOAR release 7.3.2 from FortiSOAR releases 7.3.0 or 7.3.1. Fresh installation is not supported for this release. It is highly recommended to upgrade FortiSOAR 7.3.0 and 7.3.1 instances to the 7.3.2 release as it contains some important usability and security fixes.

Upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster is not supported

There is no support for upgrading your FortiSOAR Docker on an Amazon Elastic Kubernetes Cluster to release 7.3.2.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, distributed multi-tenant configuration, or using an offline repository to version 7.3.2 from version 7.3.0 or 7.3.1 only. It is highly recommended to upgrade FortiSOAR 7.3.0 and 7.3.1 instances to the 7.3.2 release as it contains some important usability and security fixes. Also, once you have upgraded your configuration, you must log out from the FortiSOAR UI and log back into FortiSOAR.



Upgrading the FortiSOAR Docker image to the 7.3.2 release is not supported.

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 7.3.2 User Interface has been tested on the following browsers:

- Google Chrome version 108.0.5359.125
- Mozilla Firefox version 108.0.1 (64-bit)
- Microsoft Edge version 108.0.1462.54 (Official build) (64-bit)
- Safari version 15.5 (17613.2.7.1.8)
- 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 7.3.2 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 Rocky Linux 8.6 or RHEL 8.6, 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 7.3.2**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

Security Fixes

Bug ID	Description
0882107, 0883505	Fixes for possible privilege escalations.
0885301	Fixed issues with renewing the Threat Intelligence Management license.

Other Fixes

Bug ID	Description
0880816	Groups (blocks) in playbooks were not getting deleted even when a playbook was permanently deleted, i.e., removed from the recycle bin.
0882106	Uniqueness constraint validation was being honored while importing modules in Solution Packs that could cause the import to fail. Now, the uniqueness constraint validation in the case of modules in Solution Packs is skipped. For example, if an existing 'Alert' module has uniqueness constraint defined on 'Source' and 'SourceID' fields and you import a solution pack with uniqueness constraint defined on 'SourceID' and 'Name' fields for the 'Alert' module, then the uniqueness constraints validation for the Solution Pack is skipped.
0883520	The Elasticsearch service was not starting post-upgrade to 7.3.1. The Elasticsearch service is now accessible following the upgrade to 7.3.2 because this issue has been fixed.

Known Issues and Workarounds

Release 7.3.2 does not have any known issues.



www.fortinet.com

Copyright© 2023 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 General Counsel, 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.