



FortiSOAR - Release Notes

Version 6.4.4

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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

January, 2021

FortiSOAR 6.4.4 Release Notes

00-400-000000-20210112

TABLE OF CONTENTS

Change Log	4
FortiSOAR 6.4.4 Release	5
New features or enhancements	6
Upgrade Information	7
Product integration and support	8
Web browsers	8
Virtualization	8
Resolved issues	9
Known Issues and Workarounds	10

Change Log

Date	Change Description
12-14-2020	Initial release of 6.4.4
12-18-2020	Updated the New features or enhancements section to add support for using FortiManager (FMG) for FortiSOAR licensing.
01-11-2021	Updated the Known Issues and workarounds section and added information about Maintenance Packs.

FortiSOAR 6.4.4 Release

The Fortinet Security Orchestration, Automation, and Response Platform (**FortiSOAR™**) 6.4.4 release adds support to configure allowing or disallowing the master from managing and executing connector actions on the tenant node. Apart from this, enhancements have also been made in the areas of FSR agent, reporting, cluster licensing, and SSO configuration.



The recommended minimum screen resolution for the FortiSOAR GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

New features or enhancements

Feature	Details
Added support for using FortiManager (FMG) for FortiSOAR licensing	<p>Added support to use FortiManager (FMG) as an intermediary in case of a closed or air gapped environment, so that FMG can provides license validation and FortiGuard Distribution Network (FDN) updates to FortiSOAR with limited or no internet connectivity.</p> <p>Note: This feature has been validated on 'FortiSOAR Version 6.4.4 - Build 3164' and 'FMG Version 6.4.4 GA-Build 2253'.</p>
Configurable Remote Connector Management	<p>Added the Allow Connector Management button in the <code>Master Configurations</code> page on the tenant node, for allowing or disallowing the master from managing and executing connector actions, including actions executed using remotely executable playbooks ("Reference Remote Playbooks") on the tenant node.</p>
Automatic FSR Agent Upgrade Support	<p>Added support for automatically upgrading a FortiSOAR (FSR) agent. You can now automatically upgrade a FSR agent without having to SSH to the agent's VM and run the agent installer. Minimum version of FSRNode and FSR Agent to have the automatic upgrade support is 6.4.3.</p>
Enhanced reporting to support page breaks	<p>Added support for adding page breaks in reports. You can choose to print a row automatically on a new page if a page break occurs within a row of a report.</p>
Added support for entering your own (external) certificates for SAML (SSO Configuration)	<p>Provided the ability to enter or edit private and public keys of a service provider on the SSO configuration page in FSR. This is useful in cases where you want to enter your own certificate information.</p>
Updated built-in connectors	<p>The following built-in connectors have been updated in the 6.4.4 release:</p> <ul style="list-style-type: none"> • IMAP connector updated to version 3.5.5 • Report Engine connector updated to version 1.2.0 <p>For more information on FortiSOAR Built-in connectors, see the "FortiSOAR™ Built-in connectors" article.</p>
Cluster Licensing Changes	<p>Removed the need of buying additional users for clustered nodes</p>

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 6.4.4 from version 6.4.3 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 login to the FortiSOAR Platform during the upgrade.



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

Product integration and support

Web browsers

FortiSOAR 6.4.4 User Interface has been tested on the following browsers:

- Chrome version 86.0.4240.198
- Firefox version 82.0.3
- Internet Explorer version 11.1198.18362.0

Virtualization

This section lists FortiSOAR version 6.4.4 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- VMware ESXi versions 5.5, 6.0, and 6.5
- Linux KVM Redhat 7.1

Resolved issues

Following is a list of some of the important defects addressed in **FortiSOAR release 6.4.4**:

- **Bug #0662917**: Fixed the issue of the collaboration panel displaying images that are lesser than 500 KB in low resolution thumbnail mode. Now, the collaboration panel provides a preview option even for images that are lesser than 500 KB.
- **Bug #0665875**: Fixed the issue of being unable to configure the Syslog server with the RELP protocol when TLS is enabled.
- **Bug #0667672**: Fixed the issue of reports getting exported in UTC timezone even if a different timezone is selected. Now, reports get exported as per the selected timezone.
- **Bug #0671098**: Fixed the issue of memory consumption in case of connector actions while running large ingestions and other workflows that load several records into the memory since the 'env' was passed on to each action and it also used to get the 'env' triggered from the workflow (worker 'env'). Now, the connectors are passed only the required 'env' fields and not the complete environment information.
- **Bug #0673915**: Fixed the issue of being unable to externalize the PostgreSQL database when the external database is running on a non-default port. Now, you can externalize the PostgreSQL database when the external database is configured on the default or on any other port.
- **Bug #0676523**: Fixed the issue of the "Is null" filter not working on lookup fields in the 'Grid' widget.

Known Issues and Workarounds

- **Issue #48414:** You must ensure that the relations that you are adding while configuring co-relationships between modules are correct. FortiSOAR does not prevent the creation of incorrect relationships between modules. Therefore, you must ensure that you add correct bidirectional relationships for both the modules for which you want to define the relationship. For example, if you define a Many to One relationship on the Alerts module for the Events Module, then in the Events module you must define a "One to Many" relationship for the Alerts module.
- **Issue #56957:** If you select both the Row Expandable and Enable Horizontal Scrolling in the grid view template and if in the grid view of the module you expand a record, then, in this case, the UI of the records following the expanded row might get scattered.
This issue will be resolved in future releases of FortiSOAR.
- **Issue #58653:** When you stop a schedule the value, i.e., the DateTime of the Last Run At field becomes blank. This issue will be resolved in future releases of FortiSOAR.
- **Issue #61040:** The `csadm db --externalize` command fails with a "Failed to drop database <name of database>" error in case the FortiSOAR database is present on an external PostgreSQL server.
This issue occurs if there is a stale connection present to the FortiSOAR database on the external PostgreSQL server. To resolve this issue and release all stale connections, restart the Postgres service using the following command:

```
systemctl start postgresql-<postgresql version>
```


For example, `systemctl start postgresql-12`
- **Issue #79682:** Custom expressions that you have added to Dynamic Values throw errors when you try to use those expressions.
To resolve this issue, restart the `celeryd` service using the following command:

```
# systemctl restart celeryd
```
- **Issue #0665610:** In an MSSP setup, after you perform leave cluster for a secondary/active node and then again join back that secondary/active node to the HA cluster, the alias for new playbooks, i.e., playbooks marked as "Remote Executable" do not get displayed in the **Remote Tenant Manager > Manage Playbook Mappings** page on the master node.
To resolve this issue, restart the `cyops-postman` service on both the primary and the secondary nodes using the following command:

```
# systemctl restart cyops-postman
```
- **Issue #0665614:** In a High Availability (HA) setup, after you perform leave cluster for a secondary/active node and then again join back that secondary/active node to the HA cluster, you cannot install connectors on the agent.
To resolve this issue, restart the `cyops-integrations-agent` and `cyops-postman` services on the primary node.
- **Issue #0678796:** If the version of your Report Engine connector is prior to 1.0.2, the "Export Report" system playbook (Settings > System Fixtures > Report Management Playbooks) did not have the timezone parameter, so if after upgrading the Report Engine to the latest version (1.2.0), even then the report does not get exported based on the selected timezone.
To resolve this issue, and export the report based on the selected timezone, do the following:
 - a. Navigate to **Settings > System Fixtures > Report Management Playbooks**.
 - b. Open the **Export Report** Playbook.
 - c. Open the **Generate Report from Report ID** step from which copy the values of the **Report ID** and **Report Params** fields.
 - d. Delete the **Generate Report from Report ID** step.
 - e. Add a "Connector" step and select the **Report Engine v1.2.0** connector.

- f. Select the **Generate Report From Report ID** action.
- g. Paste the values of the Report ID and Report Params fields that you had copied in step 3.
- h. Save the playbook and export the report as PDF.

Now, the report gets exported based on the selected timezone.

- **Issue #0684636:** FortiSOAR license deployment sometimes fails when FortiManager (FMG) acts as an intermediary between the FortiSOAR instance and the FortiGuard Distribution Network (FDN) server. This issue occurred due to an occasional delay in syncing entitlements to the FMG server. To resolve this issue, you need to install FortiSOAR Maintenance Pack 1. For more information on Maintenance Packs, see the [FortiSOAR Documentation Library](#).
- **Issue #0685174:** File operations such as creating a file that you want to reuse in a subsequent playbook step are not working as expected on a tenant or regional SOC systems that have enabled its remote connector management. To resolve this issue, you need to install FortiSOAR Maintenance Pack 1. For more information on Maintenance Packs, see the [FortiSOAR Documentation Library](#).
- **Issue #0686254:** DNS resolution issue with the Amazon Web Service (AWS) 6.4.4AMI for Enterprise and Secure Message Exchange. Due to an error with the network service, nameservers were not correctly applied to the FortiSOAR VM and its initial bootstrapping wizard failed to complete. To resolve this issue, you need to install FortiSOAR Maintenance Pack 1. For more information on Maintenance Packs, see the [FortiSOAR Documentation Library](#).
- **Issue #0686557:** Intermittent issue that caused the failure of playbooks and direct connector actions. To resolve this issue, you need to manually restart the `uwsgi` and `cyops-integrations-agent` services. You can also resolve this issue by installing FortiSOAR Maintenance Pack 1. For more information on Maintenance Packs, see the [FortiSOAR Documentation Library](#).



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.