



RELEASE NOTES

RELEASE 6.4.3

SEPTEMBER 2020

Copyright

EXCEPT WHERE EXPRESSLY STATED OTHERWISE, NO USE SHOULD BE MADE OF MATERIALS ON THIS SITE, THE DOCUMENTATION, SOFTWARE, HOSTED SERVICE, OR HARDWARE PROVIDED BY FORTINET. ALL CONTENT ON THIS SITE, THE DOCUMENTATION, HOSTED SERVICE, AND THE PRODUCT PROVIDED BY FORTINET INCLUDING THE SELECTION, ARRANGEMENT AND DESIGN OF THE CONTENT IS OWNED EITHER BY FORTINET OR ITS LICENSORS AND IS PROTECTED BY COPYRIGHT AND OTHER INTELLECTUAL PROPERTY LAWS INCLUDING THE SUI GENERIS RIGHTS RELATING TO THE PROTECTION OF INTELLECTUAL PROPERTY. YOU MAY NOT MODIFY, COPY, REPRODUCE, REPUBLISH, UPLOAD, POST, TRANSMIT OR DISTRIBUTE IN ANY WAY, ANY CONTENT, IN WHOLE OR IN PART, INCLUDING ANY CODE AND SOFTWARE UNLESS EXPRESSLY AUTHORIZED IN WRITING BY FORTINET. UNAUTHORIZED REPRODUCTION, TRANSMISSION, DISSEMINATION, STORAGE, AND OR USE WITHOUT THE EXPRESS WRITTEN CONSENT OF FORTINET CAN BE A CRIMINAL, AS WELL AS A CIVIL OFFENSE UNDER THE APPLICABLE LAW.

© 2008-2020, Fortinet, Inc. All Rights Reserved.

Trademark

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Fortinet are the registered or unregistered Marks of Fortinet, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Fortinet or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Fortinet or the applicable third party. Fortinet is a registered trademark of Fortinet Inc.

Table of Contents

| | |
|--|---|
| Release Notes v6.4.3..... | 4 |
| New Features and Enhancements..... | 4 |
| Defects Addressed..... | 7 |
| Known Issues and Workarounds..... | 8 |
| Technical support contact information..... | 8 |



Release Notes v6.4.3

The Fortinet Security Orchestration, Automation, and Response Platform (**FortiSOAR™**) 6.4.3 makes it easier for you to manage and automate security incidents using FortiSOAR™. This release revamps the configuration manager and introduces a wizard-based export and import of FortiSOAR™ configuration information, dashboards, application settings, etc., which enhances the user experience and provides benefits of the improved architecture. It also adds support for the forwarding of FortiSOAR™ logs to your central log management server. Apart from this, enhancements have also been made in the areas of FortiSOAR™ Agent, Widget Library, system monitoring, and reporting.

New Features and Enhancements

| Feature | Details |
|---|---|
| CI/CD support for moving configurations enhancements | Enhanced CI/CD support for moving configurations across UAT and production FortiSOAR™ environments: <ul style="list-style-type: none">• Wizard-based export and import of configurations that includes many granular options to control the data you want to export or import.• APIs that accomplish the same so that the process can be automated and scheduled. |
| System Monitoring enhancements | Enhanced System Monitoring as follows: <ul style="list-style-type: none">• Extended monitoring to include new statistics such as CPU load average, pending workflows in queue, replication status, processes consuming highest CPU and memory, etc.• Provided a uniform monitoring interface for both a single node and a cluster.• Simplified the interface used for configuring monitoring thresholds for disk, CPU, memory usage, replication lag, etc.• Added new APIs for fetching system statistics with a JSON response. You can easily integrate these with external monitoring tools. |
| Log Forwarding to Syslog Server | Added support for forwarding of FortiSOAR™ application logs and audit logs, to your central log management server that supports a Rsyslog client. You can use both the FortiSOAR™ UI and the <code>csadm</code> CLI to forward FortiSOAR™ logs to your log management server. |
| Playbook Prioritization | Added support for changing the prioritization of playbook execution based on the importance of that playbook, thereby enabling the higher priority playbooks to be executed first even |

| | |
|--|---|
| | <p>if there are some normal priority playbooks already queued for execution. As an example, a Managed Security Services Provider might want to assign certain ingestion playbooks with a higher priority than enrichment playbooks, or over other ingestion playbooks that are less critical in terms of an SLA impact to their end customer.</p> |
| Widget Library enhancements | <p>Enhanced the "Widget Library" to include a very rich user interface for development of custom widgets including,</p> <ul style="list-style-type: none"> • HTML and JavaScript editor with code validations • "Previewing" widgets before publishing • "Downloading" and "Cloning" widgets. |
| FortiSOAR™ Agent enhancements | <p>Enhanced the FortiSOAR™ Agent as follows:</p> <ul style="list-style-type: none"> • Added support for listener-based connector configuration on the agent. Listener-based connectors, for example the "Exchange" connector, listen for live events on a server, and then these events are notified to FortiSOAR™ by triggering a playbook. • Added support for running file-based operations on the agent, enabling you to perform connector actions that require file resources from FortiSOAR™. For example, creating a "Communication" record in FortiSOAR™ with emails pulled from the exchange connector using an agent. • Added support for running the data ingestion wizard on agent configurations. |
| HTML WYSIWYG editor for Rich Text | <p>Added a "HTML WYSIWYG" editor in addition to the Markdown editor giving users the option to use their preferred editor. You can select the editor to be used in the Richtext Content widget and in Rich Text fields such as, Description in record detail views, or in case of comments and messages. An "HTML WYSIWYG" editor is extremely easy to use and format the content such as using text color, aligning the text, etc. In case of emails, HTML is better than markdown for both formatting the contents of an email and also for rendering the content in browsers.</p> |
| Audit Log enhancements | <p>Enhanced the FortiSOAR™ audit logs to include auditing of SVT changes, rule and schedule actions, team and role modifications, etc., providing you with comprehensive records of all activities across FortiSOAR™. The audit log has also been enhanced to include changes made in the team hierarchy.</p> |
| Reporting enhancements | <p>Enhanced FortiSOAR™ reporting by making the following improvements in widgets:</p> <ul style="list-style-type: none"> • Improved the Simple Grid widget by displaying the complete text instead of "..." for fields that could contain |

| | |
|--|---|
| | <p>longer content such as "Description". This enhancement ensures that reports do not contain truncated field content and instead contain the complete content for all fields.</p> <ul style="list-style-type: none"> Improved all types of Chart widget by providing you with the choice to either always display the chart or to display the chart only if there is at least one record present in the selected module. Improved the Donut widget by providing you with the choice of displaying the actual counts of records instead of the percentages. |
| Ability to delete associations with parent | Added the Delete Associations With Parent option for Many to One relation type fields in the Module Editor. Selecting the Delete Associations With Parent checkbox cascades the deletion of a parent record to all the associated records for this type of fields. This is useful for example, in case of cascade delete of comments associated with a deleted alert, etc. |
| Ability to attach files to Comments | Enhanced the layout for the "Comments" Widget making it easier to add, style, search, and filter comments. Also, now you can attach a maximum of five files to a single comment |
| Jinja expressions additions | Added a new jinja expression named "IRI to UUID", which is used to convert valid FortiSOAR™ IRIs to UUID. This can be used in the "Find Records" step to find a record in a module within FortiSOAR™. |
| Ability to add ownership for queues | Added an Owners option, in the create and update queues dialogs enabling you to add ownership for queues. |
| Ability to exclude all the "Executed Playbook Logs" from the backup | Added the optional <code>--exclude_workflow</code> option to the <code># csadm db --backup</code> subcommand which allows you to exclude all the "Executed Playbook Logs" from the backup. Executed playbook logs are primarily meant for debugging so they are not a very critical component to be backed up. However, they constitute a major part of the database size, so excluding them from the backup reduces time and space needed for the backup. |
| FortiSOAR Secure Message Exchange Configuration Wizard enhancements | Enhanced the FortiSOAR Secure Message Exchange Configuration Wizard by consolidating certain pages of the wizard. For example, earlier there were two separate pages displayed for entering the API port and the TCP port; now you can enter the port information in a single page. |
| Versions of the built-in connectors | <ul style="list-style-type: none"> Utilities connector version 3.0.4 Database connector version 2.1.1 IMAP connector version 3.5.4 SMTP connector version 2.4.0 SOAP connector version 2.3.0 |

| | |
|--|--|
| | <ul style="list-style-type: none">• SSH connector version 2.1.1• Report Engine connector version 1.1.0• Code Snippet connector version 1.2.4• BPMN version 1.0.2• System Monitoring version 1.3.0 <p>For more information on FortiSOAR™ Built-in connectors, see the "FortiSOAR™ Built-in connectors" article.</p> |
|--|--|

Defects Addressed

Following is a list of some of the important defects addressed in **FortiSOAR™ release 6.4.3**:

- **Bug #0639434**: Jinja picklist filter now supports picklist items with underscores.
- **Bug #0641441**: Enabled setting of an IPv6 proxy using the FortiSOAR Configuration Wizard.
- **Bug #0641443**: Provided an option in the Configuration Wizard to configuring the proxy without specifying a username and password.
- **Bug #0644625**: Improved readability of content within images added to comments. Earlier, this issue occurred in case of large images getting resized in the **Comments** section. Now, a large image does not get resized in the **Comments** section; however, when you click that attached image name it gets enlarged, or if the image is added as an inline image, click the image name to download the image as per its original size, making it possible to read the contents of the images within comments.
- **Bug #0644743**: Scrolling using key page up and down now works in the detailed view of a record.
- **Bug #0645027**: Fixed the issue of maximum length validation for an integer field.
- **Bug #0646854**: Existing module templates will now not be overwritten now due to empty API response. Templates will now be generated only if the templates do not exist.
- **Bug #0649475**: Widgets can now be installed in systems where port 80 is disabled in the firewall.
- **Bug #0650224**: Audit log purge will now not fail with an "Out-of-Memory" error for a huge number of records, i.e., the total audit log data was more than 4GB.
- **Bug #0653090**: Relative date time ranges now consider the "current unit of time" while applying filters. The time range definition has been changed to include the current unit of time.
- **Bug #0654434**: "Scheduled Purge" functionality will now purge audit logs and the scheduled purge is now working correctly and purging audit logs as per the set schedule.
- **Bug #0655477**: "Data Ingestion Wizard" will now not fail to load playbooks with the error **Playbooks tags not available for #create #ingest**, if the playbook contain

correct tags such as `#create` and `#ingest`. This issue used to occur if the playbooks in the sample playbook collection was greater than 30.

- **Bug #0657479:** Lookup fields will now display the complete list of users, even when the number of users is greater than 30.
- **Bug #0658454:** Replaced the expired default SSO certificates.

Known Issues and Workarounds

For a list of known issues and workarounds, see the *Known Issues and Workarounds* guide.

Technical support contact information

Contact the FortiSOAR™ support team for any technical issues or customer service requests using the Fortinet Customer Service & Support web portal at <https://support.fortinet.com/>.