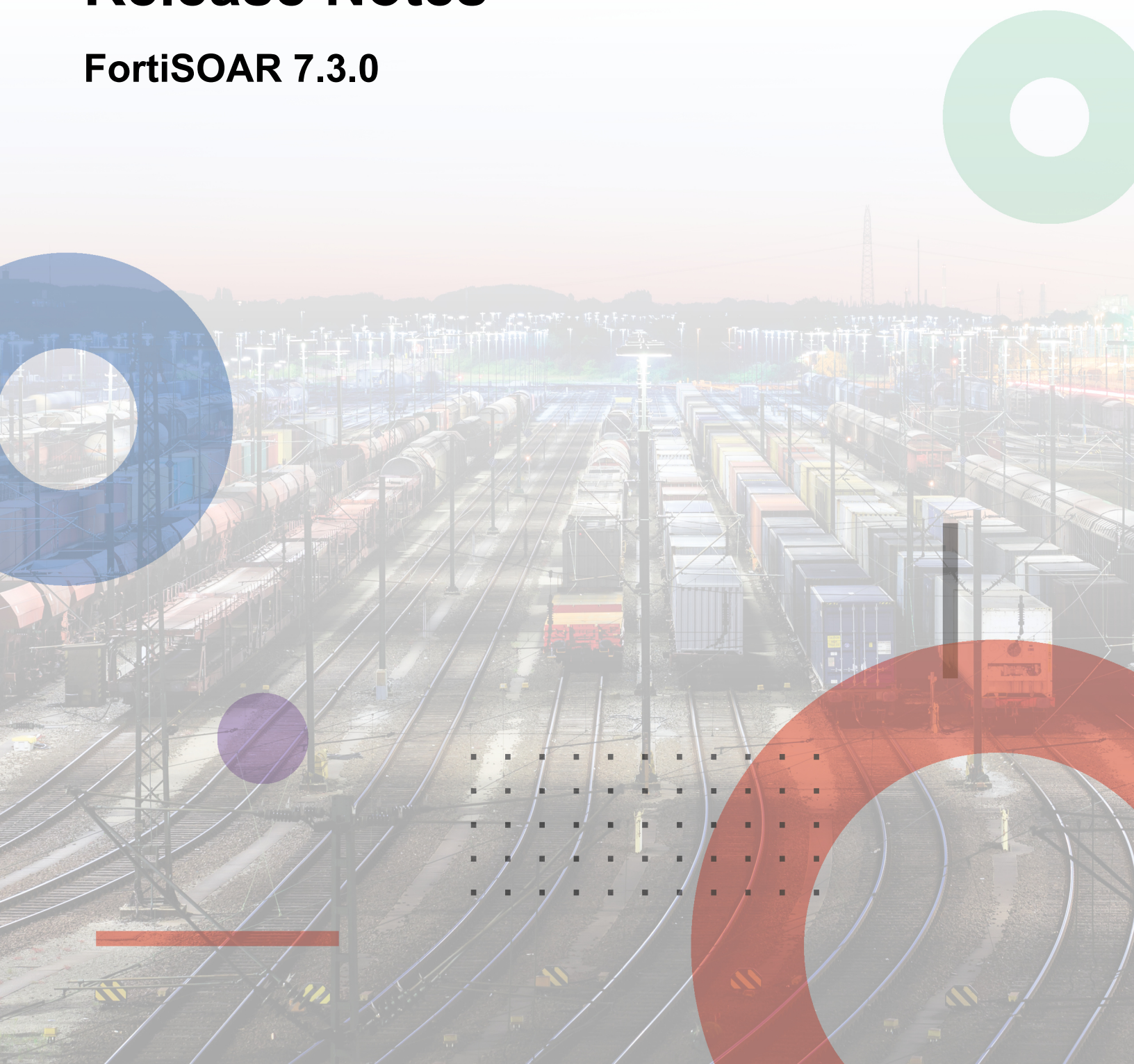
FORTINET

Release Notes

FortiSOAR 7.3.0



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

November, 2022
FortiSOAR 7.3.0 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-11-04	Initial release of 7.3.0

FortiSOAR 7.3.0 Release

The Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) release 7.3.0 introduces several crucial updates to ensure the optimal working of FortiSOAR, such as upgrading the FortiSOAR OS platform from CentOS to Rocky Linux or RHEL, adding support for deploying FortiSOAR on Docker platforms, the ability to run unauthenticated manual inputs in segmented networks using FSR agents, etc. It also optimizes various processes in FortiSOAR, such as the backup and restore process, as well as enhancing FortiSOAR's usability. This release also adds multiple security fixes to ensure vulnerabilities are fixed in FortiSOAR.

For a detailed list of all the new features and enhancements, see the New Features and Enhancements chapter.

New Features and Enhancements

Upgraded the FortiSOAR OS platform from CentOS to Rocky Linux or RHEL

- FortiSOAR release 7.3.0 has upgraded its OS platform to Rocky Linux release 8.6 or RHEL 8.6) systems and support for the CentOS operating system has been discontinued. CentOS is going to be EOL in 2024, so now the FortiSOAR appliance is embedded with a newer, stable OS. For more information, see the "Upgrading FortiSOAR" chapter in the *FortiSOAR Upgrade Guide*.

Added support for deploying FortiSOAR on Docker platforms

- FortiSOAR release 7.3.0 adds support for deploying FortiSOAR on Docker platforms such as VMware ESX or AWS. This allows you to easily provision FortiSOAR into your microservice's architecture and use it as cloud-native and DevOps-enabled.

Ability to run unauthenticated manual inputs in segmented networks using FSR agents

- FortiSOAR in release 7.3.0 can temporarily host the manual input form on a page on the FSR agent's network, and then send an email containing the link to the input form page to users that are external to your FortiSOAR network. Prior to FortiSOAR release 7.3.0, when inputs were required from users outside FortiSOAR, an email containing a link to provide inputs was sent to the user. The URL link created for the manual input was from the originating instance, i.e., the instance where the playbook is running. Due to this, organizations were required to add their FortiSOAR instance for external IP's to their 'allowlist' of their firewall or proxy servers, which could have some implications for organization policies. To overcome these issues, FortiSOAR release 7.3.0 introduces the ability to run unauthenticated manual inputs in segmented networks using FSR agents.

Introduction of a FortiSOAR Licensing option that enables unrestricted FortiGuard threat feeds and premium Threat Intelligence Management features

- FortiSOAR release 7.3.0 introduces a new licensing option that allows for unrestricted ingestion of FortiGuard threat feeds and premium Threat Intelligence Management (TIM) features. To get this new SKU, you need to contact Fortinet Support. For more information, see the *Licensing FortiSOAR* chapter in the "Deployment Guide."

Optimized the FortiSOAR Backup and Restore processes

- Release 7.3.0 optimizes the FortiSOAR backup and restore process, enhancing its performance and making it more time-efficient and effective. The backup process now includes backups for files such as JWT keys, and the Elasticsearch database.

Improvements made to the 'Add Block' functionality for playbooks

- In the playbook designer, while deleting a block in a playbook, FortiSOAR provides you with a choice of whether you want to only delete the block and not the playbook steps that are part of that block *OR* delete the block and the playbook steps that are part of that block. Earlier, you could only delete the block and not the playbook steps that were part of that block.

- Enhanced the 'Block' options in the 'Executed Playbook Log' to display metrics such as the total execution time for each block, and you can also view the time taken by individual steps within a block in its 'Step Output'. This helps in determining the ROI of automation with a granular lens.

Improvements in FortiSOAR UI usability

- An 'Advanced Filter' option has been provided on the module's listing page that enables you to apply conditional filters to the grid columns in a list view. You can achieve complex sorting and filtering of records as well as set a default view per user using the advanced filter.
- An option to render tabs on the record's view panel based on visibility conditions has been enhanced to support relational fields.

Improvements in working with playbooks

- Enhanced the 'Fetch Records' playbook step to include an option that allows users to specify the maximum number of correlated records to be fetched. Specifying the maximum number of correlated records to be fetched can help in avoiding the playbook timeout issue.
- Improved the UX for selection of playbooks in the 'Reference a Playbook', 'Reference Remote playbook' steps, and also in the 'Edit Schedule' dialog.
- Added support for using the 'Email Template Field' as a 'Custom' input field type in the 'Manual Trigger' and 'Manual Input' steps only. The ability to include an email template makes it easier for SOC teams to respond to routine operations. For example, sending emails to users when they have forgotten their password. In this case, SOC teams can create a template response to be sent to users and include the same as a field in the user prompt.
- Enhanced the Jinja Editor to allow users to filter playbook executions based playbook status and on a specific record ID, allowing for the retrieval of playbook logs based on the specific record and making debugging more effective.

Added the ability to view the data of the 'Line' and 'Timeseries' charts in a tabular format

In FortiSOAR release 7.3.0, the 'Line' and 'Timeseries' charts have been enhanced to provide you with a choice of viewing the 'Line' and 'Timeseries' data both as a line graph and in the tabular format. Having the data represented in the tabular format helps you to view the varied information in one go without having to hover on the line or timeseries chart.

Support for Content Hub synchronization

- You can use the FortiSOAR Admin CLI to synchronize Content Hub with your FortiSOAR system.

Enhancements made for monitoring FortiSOAR

- If you have an HA environment, then Nginx certificates and self-signed PostgreSQL certificates are now also monitored and notifications can be sent to specified users when any of the certificates is nearing expiry. Earlier, only the expiry of RabbitMQ certificates was monitored.
- Added support for adding multiple email addresses for monitoring your FortiSOAR system. The 'System & Cluster Health Monitoring' configuration available on the `System Configuration` page, is enhanced to allow you to add a comma-separated list of email addresses, so that multiple users can receive email notifications of any FortiSOAR

service failure, or of any monitored threshold exceeding the set threshold, etc. Prior to this release, you could only add a single email address.

Added the count of playbooks to the existing playbook collections that are being imported using the Import Wizard

When you are importing an existing playbook collection using the import wizard, FortiSOAR now displays the count of playbooks both within the collection that is being imported and the collection that exists on your system, making it easier for users to know whether the correct playbook collection is being imported.

Script-based installation improvements

- Added an option to skip the installation of the SOAR Framework Solution Pack (SFSP), which is *Not Recommended*. However, you might want to skip the SFSP installation in cases such as wanting a fresh installation of FortiSOAR without the SFSP content. By default, SFSP is installed with every fresh installation of FortiSOAR, since it is required for the functioning of FortiSOAR.
  Note: It is recommended that you install SFSP on your FortiSOAR instance, using **Content Hub** on the FortiSOAR UI, before you begin working with FortiSOAR.

Built-in Connector and Widget Enhancements

- Updated multiple built-in connectors such as the Database connector, FortiSOAR ML Engine connector, Utilities connector, etc. For more information on FortiSOAR Built-in connectors, see the "FortiSOAR™ Built-in connectors" article.
- Updated multiple widgets such as Feed Configuration Settings have been updated. The Feed Configuration Settings widget has been updated to provide the API endpoint information that supports export of threat feeds in the JSON format or the CSV format. You can use the exported threat feeds for consumption in other use cases.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR version 7.3.0.

There are steps that need to be performed after you have upgraded your FortiSOAR instance to release 7.3.0 or later from a release prior to 7.3.0. For details on the post-upgrade steps, see the *Post-Upgrade tasks* chapter in the *FortiSOAR Upgrade Guide*.

The FSR Agent cannot be directly upgraded

You cannot directly upgrade the FSR Agent to release 7.3.0, as FortiSOAR release 7.3.0 upgraded its OS platform to Rocky Linux release 8.6 or RHEL 8.6 systems. The agent installer is only supported for Linux kernel versions 4.18.0-372.13.1 and higher. To upgrade the FSR Agent, you must deploy a new VM with RHEL or Rocky Linux as the base operating system, and then download the FSR agent installer to install the agent.

Playbooks fail if any of their steps attempt to connect to a database directly, without a valid password

In release 7.3.0, access to PostgreSQL without a password has been restricted. This causes a failure in the case of any playbook step that uses the 'Database' connector to access a database directly, without a valid password. Therefore, we recommend that you create a read-only database user for such operations.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 7.3.0 from version 7.2.1 or 7.2.2 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 7.3.0 User Interface has been tested on the following browsers:

- Google Chrome version 105.0.5195.127
- Mozilla Firefox version 105.0.3 (64-bit)
- Microsoft Edge version 106.0.1370.42 (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 7.3.0 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 is a list of some of the important defects addressed in **FortiSOAR release 7.3.0**. This release also includes important security fixes.

- **Bug #0762733**: Fixed the issue of connectors containing old code, after publishing a new version of the connector with the "**Delete all existing versions**" option selected.
- **Bug #0776615**: Fixed the issue that allowed users to skip adding 'Closure Notes', which is require to close an alert or incident by just adding a newline character or a space, a tab in the 'Closure Notes' popup.
- **Bug #0799227**: Fixed the issue of Jinja `.timestamp` expression getting automatically changed to `int_timestamp`.
- **Bug #0799815**: Fixed the issue of links to module records, such as incident records, not working in the case of dashboards, i.e., when users used to click record links in dashboards, the browser would just spin and the linked record would not be loaded. Now, when users click record links in dashboards, the linked record gets displayed.
- **Bug #0804108**: Fixed the issue with 'Code Snippet' not working as by default, the YAQL python package was not getting installed. Users required to install the YAQL python package to get the 'Code Snippet' to work. Now, the YAQL python package is installed by default, like other packages such as json, etc.
- **Bug #0811600**: Fixed the issue to allow meta characters such as % in search keywords while sanitizing user input to prevent various exploits to ensure that users can find strings with such characters. Earlier meta characters such as % were not being recognized in search queries.
- **Bug #0827229**: Fixed the issue of the **Create** page in Content Hub not being refreshed when an add-on (connector, widget, or solution pack) is published. Now, a **Refresh** button has been added to the Create page beside the **Search** box that refreshes the page on publish. Also, when you delete an add-on from the **Create** page, a progress spinner is added to the add-on card to indicate the progress of the delete operation.
- **Bug #0828565**: Fixed the issue that caused styles from email body to break record comments, in cases where data was coming from external data sources such as data or email ingestion.
- **Bug #0835016**: Fixed the issue that the "do until" loop in the playbook steps did not have a Jinja option for "Retries" and "Delay (seconds)" fields.
- **Bug #0840159**: Fixed the issue of free text search not working for an email type field at the grid level.

Known Issues and Workarounds

- **Issue 0797219**: Fields with large integer values get round-off causing issues while working with connectors.
  To resolve this issue, represent large integers using the 'String' type, i.e., instead of passing integers directly such as, 123456, pass integers in a single quote such as, '123456'.
  For more information on this issue and its resolution, see the '`Handling rounding of large integer values`' topic in the *Introduction to connectors* chapter of the "Connectors Guide."
- **Issue 0842527**: The FortiSOAR VM Configuration Wizard UI breaks on the MacOS terminal. However, this is just a UI issue, and it does not hamper the VM Configuration Wizard operations.
  We have reported this issue to the Rocky Linux community.
- **Issue 0855048**: The status of the FSR Agent might display "Awaiting Remote Node Connection" after you have restored your FortiSOAR instance to 7.3.0.
  To resolve this issue, on your FortiSOAR node, restart the `cyops-integrations-agent` service and then the `cyops-postman` service. You also require to restart the `cyops-integrations-agent` service on FSR agent.

www.fortinet.com