Release Notes

FortiSOAR 7.6.3

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

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-14	Added the SSO users are not getting redirected to FortiSOAR login page topic to the Special Notices chapter.
2025-08-06	Initial release of 7.6.3

FortiSOAR 7.6.3 Release

Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) release 7.6.3 contains some important usability and security fixes to ensure vulnerabilities are fixed in FortiSOAR. It is highly recommended to upgrade FortiSOAR 7.5.* or 7.6.* instances to the 7.6.3 release.

New Features and Enhancements

FortiSOAR release 7.6.3 includes important usability and security fixes but does not introduce new features or significant enhancements. We recommend that users currently on releases 7.5.0 and 7.5.1 or 7.6.0, 7.6.1, or 7.6.2 upgrade to release 7.6.3 or later to benefit from these fixes.

Special Notices

This section highlights key operational changes in FortiSOAR release 7.6.3 for administrators to consider.

SSO users are not getting redirected to FortiSOAR login page

SSO users cannot access the FortiSOAR login page because the Content-Security-Policy (CSP) for the redirect URL is currently set to "self" in the Nginx configuration.

After completing the Identity Provider (IdP) and Service Provider (SP) configuration in FortiSOAR and your IdP, update the Content-Security-Policy (CSP) header in FortiSOAR to include your SSO domain. This step is necessary to enable proper functioning of the SSO login interface. For detailed instructions, see the Configuring Content-Security-Policy for SSO Integration topic in the "Administration Guide."

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to release 7.6.3 from releases 7.6.2, 7.6.1, 7.6.0, 7.5.2, 7.5.1, or 7.5.0. For detailed procedures, see the *Upgrade Guide*.

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 7.6.3 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 7.6.3 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

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 7.6.3 has been tested with RHEL 9.5 and Rocky Linux 9.5. For more information, see the "Deployment Guide."

Resolved Issues

The following important issues have been fixed in **FortiSOAR release 7.6.3**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

Graphical User Interface

Bug ID	Description
0864218	Fixed an issue where filters from dashboard widgets, such as 'Record Distribution' or 'Card Count', were not applied when navigating from the dashboard to module listings such as, 'Alerts'. For example, clicking a 'Record Distribution' widget with 'Severity' set to 'Critical' did not apply the `severity = critical` filter on the Alerts listing page. Filters are now correctly applied when users navigate from dashboard widgets to module listings.
1163172	Fixed an issue where column-specific filters were reset after viewing a record and returning to the Dashboard, which contain multiple Grid widgets from various data sources. Filters now remain applied when users open and close a record's detail view.
1175154	Fixed an issue that occurred after upgrading FortiSOAR to release 7.6.2, where the filter panel in the global grid view automatically expanded when users clicked into a record and then returned to the module listing. With this fix, the filter panel now opens by default only when navigating to the listing page from a widget (for example, by clicking a section within a chart). When returning to the module listing from a record, the filter panel remains collapsed, as expected.

Playbooks

Bug ID	Description
1079928	Fixed an issue where playbooks failed due to invalid Unicode characters. A generic sanitization method now removes these invalid characters by replacing them with the text 'CYOPS_NULL', allowing playbooks to trigger and execute successfully.

System & 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.
1175219	Fixed an issue with 'Queue and Shift Management' where creating shifts with a "Starting on" date from a different month than the current one incorrectly created the shifts in the current month. For example, creating a shift for July 3–7 by selecting July 3 as the "Starting on" date while in June resulted in shifts being created from June 3–7. This issue has now been resolved, and shifts are now correctly created based on the selected date.

CLI & API

Bug ID	Description
1180597	Fixed a pagination issue that prevented the TAXII client from retrieving the next page of data when fetching TAXII feeds from FortiSOAR. The API response has been updated to add support for the `'next'` and `'limit'` parameters, which fetches the next page of data from TAXII feeds.

Known Issues and Workarounds

- **1132542**: After upgrading a FortiSOAR deployment configured with Multi-Tenancy (MSSP) and High Availability (HA) in an Active-Active cluster, the WebSocket connection on the secondary node remains disconnected.
  Workaround:
  Restart the `cyops-tomcat` service on the secondary node:
  `#systemctl restart cyops-tomcat`
  This restores the WebSocket connection on the secondary node and ensures that all nodes are properly connected.
- **1175148**: After clearing the default filters, the default sorting functionality for the Grid widget is broken in FortiSOAR 7.6.2.
  This issue will be resolved in the next FortiSOAR release.
- **1177294**: After upgrading to FortiSOAR 7.6.2, users occasionally get logged out of active sessions.
  This issue will be addressed in the next FortiSOAR release.
- **1182042**: The Timeseries widget does not display months or fields with no data, instead of showing a value of 0. For example, if a month has no records, it is omitted from the timeseries chart. Similarly, if there are no records for a specific field (e.g., no records with 'Critical' severity), the corresponding column is not displayed in the table.
  This issue will be addressed in the next FortiSOAR release.
- **1183076**:When updating a field using Advanced Edit (Jinja2) with the 'Append' option as the update method, the field is overwritten instead of being appended. The 'Append' option does not take effect, and the 'Overwrite' method is applied instead.
  This issue will be addressed in the next FortiSOAR release.
- **1185741**: When custom roles are created and assigned to an existing user, they may override that user's existing roles and permissions for certain modules.
  This issue will be addressed in the next FortiSOAR release.

FÜRTINET

www.fortinet.com