Release Notes

FortiSOAR 7.5.3

March, 2026
FortiSOAR 7.5.3 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-03-18	Initial release of 7.5.3

FortiSOAR 7.5.3 Release

Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) release 7.5.3 includes usability, administrative, and security fixes that address known issues and vulnerabilities. We strongly recommend users to upgrade from versions 7.5.0, 7.5.1, or 7.5.2 to ensure system stability and security.

Release 7.5.3 is an ***upgrade-only*** release and does not support new installations.

New Features and Enhancements

FortiSOAR release 7.5.3 focuses on usability, administrative, and security fixes. It does not introduce new features or significant enhancements. Users running releases 7.5.0, 7.5.1, or 7.5.2 are strongly encouraged to upgrade to release 7.5.3 to benefit from these fixes.

FortiSOAR Administrative Enhancements

- **iFrame Configuration Settings**: Release 7.5.3 (for 7.5.x series and 7.6.5 for 7.6.x and later series) introduces iFrame configuration options that allow you to control how external content is embedded within the application. Sandbox restrictions are enabled by default for enhanced security, and you can specify which domains are allowed to load inside iFrames.
  For details, see the *iFrame Settings* topic in the System Configuration chapter of the "Administration Guide."

Security Enhancements

- **New:Unique Encryption key for Data Protection**: Release 7.5.3 now automatically generates a unique encryption key, per instance, during the Configuration Wizard process. This change significantly strengthens data protection by securing stored credentials, database entries, and inter-service communication with 256-bit encryption – all while maintaining full backward compatibility. All passwords saved after deployment are encrypted using this new key.
  For more information, see the Deploying FortiSOAR chapter in the "Deployment Guide."
- **New: Advanced Development Features Tab in System Configuration**: Added a new **Advanced Development Features** tab in the `System Configuration` page! This tab empowers administrators to review security risks and usage guidelines for creating or updating custom connectors and widgets. With this update, administrators now need to provide explicit consent–based on their organization's requirements–before users can create new connectors, widgets, or update existing ones.
  For details, see the *Advanced Development Features* topic in the System Configuration chapter of the "Administration Guide."
- **Enhanced iFrame Widget Security**: The iFrame widget now runs in a **sandboxed environment by default**, fully restricting the loading of external content. This update enhances the security by preventing Stored Cross-Site Scripting (XSS) attacks.
  For details on the iFrame widget, see the Dashboards, Templates, and Widgets chapter in the "User Guide."
- **Enhanced Security Validation for Connector Configuration Updates**: Beginning with release 7.5.3 (for the 7.5.x series) and 7.6.5 (for the 7.6.x series), any change to connector configuration fields, such as Server URL, Hostname, Address, Server IP, etc., requires users to re-enter all password-type fields before the configuration can be saved or applied. This update strengthens security by ensuring that when a server or endpoint detail is modified, the associated credentials are explicitly validated, reducing the risk of misconfiguration or unintended access.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR release 7.5.3.

FortiSOAR Release 7.5.3 is an Upgrade-Only Release

You can only upgrade to FortiSOAR release 7.5.3 from only FortiSOAR release 7.5.0, 7.5.1, or 7.5.2. Fresh installation is not supported for this release. It is highly recommended to upgrade existing FortiSOAR 7.5.0, 7.5.1, or 7.5.2 instances to the 7.5.3 release as it includes important usability and security fixes.

Administrator Consent required for to create or edit custom connectors and widgets in FortiSOAR 7.5.3 or later [for 7.5.x series] or 7.6.4 or later [for 7.6.x and later series])

FortiSOAR allows users to create and update custom connectors and widgets, providing flexibility for automated solutions across various use cases. However, this also introduces the risk of malicious or unauthorized code. To mitigate this risk, starting with FortiSOAR 7.5.3 (for 7.5.x series) and 7.6.4 (for 7.6.x and later series), a new **Advanced Development Features** tab has been added. Administrators must review the associated risks and usage guidelines on this tab, and provide explicit consent before users can create or update custom connectors and widgets. To provide consent the administrator must be assigned the `Security Update` permission.

Usage Impact

Upgrade to 7.5.3 or later [for 7.5.x series] or 7.6.4 or later [for 7.6.x and later series]):

In upgraded environments where **administrator consent has not yet been provided**:

- Existing custom connectors and widgets will remain available in their current state.
- However, the existing connectors and widgets will **not** be editable—users cannot modify them or upload new versions (i.e., the **Edit** and **Add Versions** options will be disabled).

For details, see the *Advanced Development Features* topic in the System Configuration chapter of the "Administration Guide."

Changes to the iFrame Widget

- **Updated behavior**: Release 7.5.3 updates the behavior of the iFrame widget to enhance security and prevent stored cross-site scripting (XSS) attacks. By default, the widget now operates in a **sandboxed** environment, which restricts the loading of external content within the embedded `<iframe>` element. In previous versions, the iFrame widget displayed embedded content from both internal and external sources without sandbox restrictions.
  This new security behavior is configurable. If your use case requires loading external content, you can disable the 'sandbox' feature. Instructions for modifying this setting are provided in the *iFrame* topic the Dashboards, Templates, and Widgets chapter in the "User Guide."
- **Enhanced Security for iFrame Content**: After upgrading to release 7.5.3 or later (for 7.5.x series or 7.6.5 (for 7.6.x and later series), iFrame content may no longer display. Instead, the following message appears: `This domain is not added in the 'Allowed Domains list' and cannot be accessed. Please contact your administrator for further assistance.`
  This behavior occurs because release 7.5.3 (for 7.5.x series) and 7.6.5 (for 7.6.x series) introduce enhanced iFrame security controls that affect how external content is embedded in the application. Sandbox restrictions are enabled by default, and all domains are blocked unless explicitly added to the 'Allowed Domains' list. To enable iFrame content from specific external domains, update the 'iFrame Settings'. For details on how to change these settings, see the *iFrame Settings* topic in the System Configuration chapter of the "Administration Guide."
- **Change in Sandbox Restriction Settings**: In release 7.5.2, users could remove sandbox restrictions for external content embedded in iFrames by setting the `sandbox` parameter to '`false`' in the `config.json` file (`/opt/cyops-ui/vendor/config.json`):

  ```
  "iframe":{
            "sandbox": false
      }
  ```

  After upgrading to release 7.5.3, this setting is automatically set to '`true`'. As a result, sandbox restrictions are always enabled for external iFrame content.
  From release 7.5.3 onward, the sandbox can be enabled or disabled using the **Enable Sandbox** option in *iFrame Settings* on the **Application Configuration** tab of the `System Configuration` page. For details on how to change this setting, see the *iFrame Settings* topic in the System Configuration chapter of the "Administration Guide."

Enhanced Security Validation for Connector Configuration Updates

Starting with release 7.5.3 (for the 7.5.x series) and 7.6.5 (for the 7.6.x series), changing any connector configuration fields (e.g., Server URL, Hostname, Address, or Server IP) now requires users to re-enter all password-type fields before saving or applying the configuration. This change strengthens security by ensuring that updated host or endpoint details are always paired with reconfirmed credentials, reducing the risk of misconfiguration or unintended access.

User Impact: Prior to this update, password re-entry was not required after updating the connector configuration fields. Users will now encounter an additional validation step, specifically a prompt to re-enter password-type fields before completing the update.

Note: This requirement does not apply to fields that are dynamically populated from the vault.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 7.5.3 from versions 7.5.0, 7.5.1, and 7.5.2. 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 7.5.3 User Interface has been tested on the following browsers:

- Google Chrome version 143.0.7499.193
- Mozilla Firefox version 147.0.1 (aarch64)
- Microsoft Edge version 144.0.3719.92
- Safari version 26.1 (20622.2.11.119.1)
- 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 7.5.3 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
  NOTE: The KVM OVA is not certified on FortiSOAR.

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

Resolved Issues

Release 7.5.3 addresses critical security and usability issues. For information about specific issues contact Customer Service & Support.

Playbooks

Bug ID	Description
1215034	Fixed an issue where a playbook stopped and skipped all remaining steps when a 'Reference Playbook' step finished with an error. This occurred when a child playbook failed with the `Ignore Error` option enabled, causing the parent playbook to finish with an error and skip subsequent pending steps. With this fix, parent playbooks continue executing remaining steps even if a referenced playbook finishes with an error.

System and Security

Bug ID	Description
1196805	Improved security for LDAP and RADIUS configurations by requiring users to re-enter passwords before saving changes to server settings.

Known Issues and Workarounds

There are no significant known issues in this release of FortiSOAR.

www.fortinet.com