Release Notes

FortiSOAR 7.6.5

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

December, 2025
FortiSOAR 7.6.5 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-01-19	Enhanced the documentation related to disabling root shell access for `csadmin` users in the New Features and Enhancements, Special Notices, and Upgrade Information chapters.
2026-01-08	Added issue '1222226' to the Resolved Issues chapter
2026-01-06	Added issue '1220684' to the Known Issues and Workarounds chapter and also updated the 'Upgrade Notes' in the Upgrade Information chapter.
2025-12-17	Initial release of 7.6.5

FortiSOAR 7.6.5 Release

The 7.6.5 release introduces a range of security, performance, and usability enhancements designed to strengthen your environment and streamline daily operations:

- **Playbook** and **FortiSOAR UI enhancements** designed to boost usability, security, and overall editing experience. Highlights include an upgraded Markdown editor, configurable iFrame settings, secure password input via user prompts, and improvements to the Jinja editor.
- **Per-deployment unique encryption keys** for improved data security.
- **Refined security controls for 'csadmin' sudo access**, restricted to required commands.
- **Expanded enhancements across key solution packs**—SOAR Framework—to improve functionality and performance.

For a complete list of updates, see the New Features and Enhancements chapter.

New Features and Enhancements

This release introduces features and improvements that enhance usability, increase performance, and elevate your FortiSOAR™ experience.

FortiSOAR User Interface Enhancements

Improved Markdown Editor

- Fields whose type was set to "Rich Text (Markdown Editor)" were previously slow to render, which negatively impacted UI performance. This release introduces several improvements to deliver a faster and smoother editing experience:
  - **Faster Loading with Markdown as View-Only Mode**: The Markdown editor now loads in a view-only mode, reducing load times and preventing UI lag.
  - **Optional Lazy Loading for Better Stability**: Markdown Editor fields now support lazy loading, reducing CPU usage and helping prevent “Page Unresponsive” issues. Lazy loading is disabled by default to preserve existing behavior, but can be enabled as needed.
    - **Form View**: Markdown fields now initially render as plain textareas. The full editor loads only when the user clicks the field, improving responsiveness.
    - **Detail View**: Fields display in read-only mode by default. If the field is editable, the user clicks once to open the textarea and clicks again to open the editor.
  - **Optimized Content Display with Configurable Word Limit**: Markdown fields now display up to 50 words by default when in 'View' mode for faster page loads. Users can click **View More** to reveal the full content. Both the word-limit feature and the maximum word count are fully configurable.

  For more information, see the Working with Detail Views topic in the *Customize Modules and Data Views* chapter of the "User Guide."

iFrame Configuration Settings

- Release 7.6.5 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 require to specify which domains are allowed to load inside iFrames (by default, all domains are blocked). For details, see the *iFrame Settings* topic in the Application Configuration section of the "Administration Guide."

Bulk Activation and Deactivation of Schedules

- You can now activate or deactivate schedules in bulk. Previously, users had to disable and re-enable each schedule individually, which was time-consuming and inefficient when managing a large number of schedules, for example during upgrades or maintenance. This new capability streamlines the process by allowing you to pause or restart multiple schedules with just a few clicks. For details, see the Schedules chapter in the "User Guide."

Copy Uploaded Files Directly to Collaboration Comments

- You can copy files uploaded through the File Upload widget directly into the Comments tab of the Collaboration pane. When pasted, the file is automatically added as an attachment, with no need to reupload it through the form editor or create a new file. For details, see the File Upload topic in the *Build and Customize Dashboards, Templates, and Widgets* chapter of the "User Guide."

Enhanced Relationship Widgets

- The **Relationships** and **Relationships Single Line Card** widgets have been enhanced with a **Filter Criteria** section. This allows you to define filtering rules for related module records, which are applied automatically when the grid loads for more focused data display. For details, see the Working with Template Widgets chapter of the "User Guide."

Playbook Enhancements

Secure Password Input via User Prompt

- Starting with release 7.6.5, users can securely provide passwords to FortiSOAR via a manual input prompt. This allows users without connector-page access to enter credentials that can be used in automation workflows, such as playbooks that create or update connector configurations. For details, see the Playbook Triggers chapter in the "Playbooks Guide."

Improved Default View for Global Executed Playbook Logs

- To improve the user experience when viewing executed playbook logs, the global Executed Playbook Log view (accessed from the upper-right corner of the screen) now defaults to displaying logs from the past 7 days. This setting is configurable: users can disable the limit to view all playbook executions or adjust the number of days shown. This enhancement reduces the number of clicks required to access older execution logs and provides a more streamlined viewing experience. For details, see the Viewing Executed Playbook Logs topic in the Playbook Execution and Debugging chapter and the Optimizing and Troubleshooting

chapter of the "Playbooks Guide."

Improved Jinja Editor

- The Jinja Editor now slides in from the right, improving screen-space usage and providing more room to view and edit input and output expressions for a better overall experience. Additionally, step results are now handled correctly in the Jinja Editor and are presented in dictionary format, allowing step-level Jinja expressions to be evaluated without modification. For details, see the Jinja Editor topic in the *Dynamic Values* chapter of the "Playbooks Guide."

Enhanced User Prompt

- Starting with release 7.6.5, the 'Build Input Prompt' includes a new option: **+Add Required Condition**. This enhancement lets you define when a field should be mandatory during step execution, giving you more precise control over your workflows. Requirement types have also been streamlined—Manual Inputs now support Required, Not Required, Required by Condition, and Required by Mapping, while Manual Triggers support Required, Not Required, and Required by Condition.
  Previously, fields could only be marked as required or not. With this added flexibility, the system can better account for functional differences between steps and apply required-field rules only when they are relevant. For details, see the Playbook Triggers chapter in the "Playbooks Guide."

System and Security Updates

Unique Encryption key for Data Protection

- FortiSOAR 7.6.5 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."

Restricted 'csadmin sudo' for User Access Control

- FortiSOAR 7.6.5 has limited the `csadmin` user's `sudo` privileges to only the commands required to work with FortiSOAR, rather than granting full '`root`' access. This enhancement aligns with the *principle of least privilege*, significantly reducing exposure to sensitive system files and strengthening overall platform security. Therefore, commands such as `yum`, `systemctl`, `csadm`, etc., must be prefixed with `sudo`, for example, `sudo csadm --help`.
  To open or edit a file, prefix the command with '`sudo`' and specify the file's full path (`sudo vi <full path of file>`).
  For example, `sudo vi /opt/cyops-auth/utilities/das.ini`.

Note: For security reasons, '`root`' access is provided via the system console and is not available over SSH. Since FortiSOAR 7.6.3, users running `sudo` commands as the '`csadmin`' user have been prompted for a password on all systems except AWS. Together, these improvements ensure tighter access control and a more secure operating environment.

Solution Packs, Connectors, and Widget Enhancements

FortiSOAR 7.6.5 introduces significant enhancements across solution packs, connectors, and widgets—expanding automation capabilities, improving integration reliability, and boosting platform performance for SecOps teams.

- **Enhanced Solution Packs**:
  - ***SOAR Framework Solution Pack (SFSP) v3.4.0***: Delivers a broader and more flexible automation experience, including improved MSSP playbook execution, expanded indicator and file-content extraction, and noticeable SVT performance gains. Additional playbook updates, new localized strings, and targeted bug fixes further refine usability and reliability.
  - ***FortiAI v4.0.1***: Ensures user prompts work correctly when modules lack correlated fields or key mappings in the Key Store, with the recommendation engine enabled.
  - ***OTbase Inventory v1.0.0***: Adds support for managing vulnerabilities discovered in OTbase Inventory devices.
  - ***Outbreak Response – React2Shell Remote Code Execution v1.0.0***: Introduces response capabilities for the React2Shell RCE threat.
  - ***Outbreak Response – UNC1549 Critical Infrastructure Espionage Attack v1.0.0*** – Adds response workflows for the UNC1549 espionage campaign.
    Note: All widgets in the respective solution packs have been updated.
- **Enhanced Connectors**: Impactful updates have been introduced across System, Fabric, and third-party connectors - few notable ones being:
  - *System /Default Connectors*:
    - ***SysLog v1.3.0***: Fixes truncation of long messages.
    - ***FSR Agent Communications Bridge v1.2.0***: Adds support for password-type fields in external manual playbook inputs and includes general improvements.
  - *Fabric Connectors*:
    Enhanced Fortinet Fabric connectors include:
    - ***Fortinet FortiDLP v1.1.0***: Adds support to retrieve lists and details of agents, users, labels, and more.
    - ***Fortinet FortiProxy v1.0.1***: Updates API authentication to use bearer tokens.
    - ***Fortinet FortiSIEM v5.4.3***: Fixes issues with data ingestion and actions not executing as expected.
    - ***Fortinet FortiRecon EASM v1.2.0***: Adds new actions, including updating IPs, assets, and issues.
  - *Third-Party Connectors*:
    - ***ServiceNow v3.5.0***: Supports creating and editing business rules using API Key Authentication, enabling stronger and more modern integration security.
    - ***Exchange v4.7.0***: Adds attachment and inline-image support for *Send Reply*, along with other improvements.
    - ***SendGrid v1.1.0, GSuite for Gmail v3.1.0, and Microsoft Graph Mail v1.4.0***: Adds support for email templates.

- ***HashiCorp Vault v2.0.0***: Enhances access to secrets across an entire secret engine, including nested directories.
- ***Google Threat Intelligence v1.0.0***: New connector that provides visibility into threat actors, attacks, and IOCs.
- ***CrowdStrike Falcon v3.1.0*** – Adds Spotlight actions such as *Search Vulnerabilities, Get Host List by Vulnerability*, and *Get CVE List by Vulnerability*.
- ***OKTA v1.1.0***: Adds an action to revoke all active user sessions.
- ***Jira v2.0.0***: Updated to support the JIRA API v3.
- ***Microsoft Entra ID v2.2.1***: Renamed from Azure Active Directory; associated actions and playbooks updated.
- ***Atlassian Confluence Cloud v1.0.0***: New connector enabling collaboration and knowledge-management workflows.
- ***AWS Commands v1.1.0***: Adds an action to revoke active sessions associated with a role.
- ***Cyware CTIX v2.0.0***: Introduces 20+ new actions, including *Create Intel via Open API*, *Get Threat Data*, and *Bulk Add Relation*.
- ***Darktrace v1.4.0***: Adds support to retrieve enumerated types and corresponding string values.
- ***Ansible Tower v2.0.0*** and ***VMRAY v1.1.0***: Introduces new actions that expand automation and malware-analysis workflows.
- ***Mimecast S2 v3.0.0***: Upgraded to the latest Mimecast API v2.0 for improved compatibility and functionality.
- ***Alloy ITSM v1.0.0****: A new connector that streamlines and automates ticket-based operations.*
- ***Rapid7 Threat Command Cloud v1.1.0***: New connector for monitoring external threats across the web, deep web, and dark web.
- ***SentinelOne v3.5.3***: Added SSL verification to Create BlockList Item to prevent failures.
- ***TEHTRIS EDR v1.0.0***: New connector providing real-time endpoint detection and response.
- ***URLhaus v1.1.0***: New connector for collecting, tracking, and sharing malware URLs.
- ***Elastic Kibana v1.0.0***: New connector to search, visualize, and manage Elasticsearch data.
- ***Elastic Security v1.0.0***: New connector offering unified SIEM, endpoint, and cloud security.

- **Enhanced Widgets**:
  - ***Language Pack v2.1.0***: Adds more translatable strings, improving localization coverage and accuracy.
  - ***Widget Picklist as Phases v1.1.0***: Updated the widget to correctly hide or disable picklist options based on the module's Fields Editor setting.

For details, see the FortiSOAR Content Hub.

Special Notices

This section highlights key operational changes in FortiSOAR release 7.6.5 for administrators to consider.

Root Shell Access Disabled for csadmin

Starting with release 7.6.5, the csadmin user's sudo privileges are restricted to only the commands required to work with FortiSOAR, instead of providing full 'root' access. This enhancement aligns with the principle of least privilege and reduces exposure to sensitive system files. Therefore, commands such as `yum`, `systemctl`, `csadm`, etc, must be prefixed with `sudo`, for example, `sudo csadm --help`.

To open or edit a file, prefix the command with '`sudo`' and specify the file's full path (`sudo vi <full path of file>`).
For example, `sudo vi /opt/cyops-auth/utilities/das.ini`

For security reasons, '`root`' access is provided via the system console and is not available over SSH.

Enhanced Security Validation for Connector Configuration Updates

Starting with release 7.6.5, 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 release, 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.

Enhanced Security for iFrame Content

After upgrading to release 7.6.5 or later, 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 7.6.5 introduces 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 Application Configuration section of the "Administration Guide."

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to release 7.6.5 with the following guidance.

The FortiSOAR UI displays a notification when a new General Availability (GA) release is available. The notification includes a direct link to the release notes for more details.

Before You Upgrade

The upgrade process will temporarily take your FortiSOAR application offline. During this time, users will not be able to access or log in to the platform.

To ensure a smooth upgrade:

- **Notify users**: Inform all users in advance about the planned maintenance window and expected downtime.
- **Stop active processes**: Confirm that no critical playbooks, automations, or integrations are running before starting the upgrade.
- **Back up your system**: Perform backup of the FortiSOAR database and configuration to prevent data loss in case of unexpected issues.
- **Confirm prerequisites**: Verify that your environment meets all system requirements (OS version, disk space, dependencies, etc.).

Downgrading to previous firmware versions

Downgrading to previous firmware versions **is not supported**.

Upgrade Path

The following table provides version compatibility between FortiSOAR components and the supported upgrade paths:

Enterprise or MSSP Master Node	Supported Upgrade	Compatible Tenant Node	Compatible Agent	Compatible SME
7.6.5 (c)	7.6.4-7.6.0 7.5.2 -7.5.0	7.6.4 -7.6.0 7.5.2 -7.5.0 **Note**: When upgrading to FortiSOAR 7.6.5 without upgrading the FortiSOARAgents, users must also upgrade the Utilities Connector on the FortiSOAR Agent to ensure proper functionality.		
7.6.4 (c)	7.6.3-7.6.0 7.5.2-7.5.0	7.6.4 -7.6.0 7.5.2 -7.5.0 **Note**:Upgrade-only releases, such as 7.6.3 and 7.5.2, do not support upgrading external SMEs to these versions.		
7.6.3 (5) (c) (*upgrade-only release*)	7.6.2-7.5.0	7.6.3 -7.6.0, 7.5.2-7.5.0		7.6.2 -7.6.0, 7.5.1-7.5.0
7.6.2 (b) (c)	7.6.1-7.5.0	7.6.2-7.6.0		
7.6.1	7.6.0-7.5.0	7.6.1, 7.6.0		
7.6.0	7.5.2-7.5.0	7.6.0, 7.5.0		
7.5.2 (5) (*upgrade-only release*)	7.5.0, 7.5.1	7.5.2-7.5.0		7.5.1, 7.5.0
7.5.1 (*upgrade-only release*)	7.5.0	7.5.1, 7.5.0, 7.4.5 -7.4.0		
7.5.0	7.4.5- 7.4.0	7.5.0, 7.4.5-7.4.0		
7.4.5 (4) (*upgrade-only release*)	7.4.4, 7.4.3	7.4.5-7.4.0		
7.4.4 (4) (*upgrade-only release*)	7.4.3-7.4.0	7.4.4-7.4.0		
7.4.3 (a) (4) (*upgrade-only release*)	7.4.2-7.4.0	7.4.3-7.4.0		
7.4.2 (4)	7.4.1, 7.4.0	7.4.2-7.4.0		
7.4.1 (3)	7.4.0	7.4.1, 7.4.0, 7.3.2		
7.4.0	7.3.3-7.3.0	7.4.0, 7.3.2		
7.3.3 (2) (*upgrade-only release*)	7.3.2, 7.3.1	7.3.3-7.3.1		
7.3.2 (2)	7.3.1, 7.3.0	7.3.2-7.3.0		

(*upgrade-only release*)		
7.3.1 (1)	7.3.0	7.3.1, 7.3.0
7.3.0 (*for upgrade and migration support*)	7.2.2, 7.2.1	7.3.0

Upgrade Notes:

- *Upgrade-only* releases contain critical usability and security enhancements. We advise users to upgrade their FortiSOAR setups to the latest releases corresponding to their installed FortiSOAR versions.
- (**c**) Upgrading from release 7.6.1 to a later release (for example, 7.6.4, 7.6.5 and later) causes the Utilities Connector '*Create an attachment from file*' action to fail. A workaround for this issue is described in the Known Issues and Workarounds chapter.
  Additionally, after upgrading from release 7.6.1, the TAXII server configuration is automatically disabled. If the TAXII server is required, manually re-enable it. For more information, see the Threat Intel Management Solution Pack documentation.
- (**b**) If you are upgrading your FortiSOAR HA cluster from releases 7.6.0, 7.5.2, 7.5.1, or 7.5.0 to release 7.6.1 or later, follow the steps in the Upgrading to releases prior to 7.6.1 topic. If you are upgrading your FortiSOAR HA cluster from release 7.6.1 or later to release 7.6.2 or any subsequent release such as releases, 7.6.3, 7.6.4, 7.6.5, you can use the 'rolling upgrades' process. Steps for rolling upgrade are mentioned in the Upgrading to releases post 7.6.1 topic.
  The 'rolling upgrade' process, which minimizes downtime for high availability (HA) clusters, ***is not supported*** for Docker images.
- (**a**) Release 7.4.3 addresses a critical issue of connectors not working after backup and restore due to missing 'Python' dependencies, which affects fresh installations of FortiSOAR 7.4.2. Therefore, it is highly recommended to upgrade fresh installations of 7.4.2 instances to 7.4.3.

Compatibility Notes:

(**1**) No incompatibility issues were observed in MSSP use cases; however, the 'Manual Input' step operates differently in systems that have a lower-version tenant node and a higher-version master node since, FortiSOAR release 7.3.1 has an enhanced UI and upgraded functionality.

(**2**) No incompatibility issues were observed in MSSP use cases; however, in FortiSOAR release 7.3.1, the 'Complete' playbook environment can be passed to child playbooks, which was not possible in earlier versions, leading to some differences in systems that have a lower-version tenant node and a higher-version master node.

(**3**) Pushing approval playbooks from FortiSOAR release 7.4.1 master node to a lower-version tenant node is not supported. In such cases, the playbook is not visible on the tenant node, and neither will FortiSOAR display any error.

(**4**) No incompatibility issues were observed between versions 7.4.2 , 7.4.3, and 7.4.4 of the FortiSOAR enterprise/MSSP-master and FSR agent, Secure Message Exchange (SME), or MSSP-tenants.
However, it is important to consider the following when using versions 7.4.2, 7.4.3, or 7.4.4 of the FortiSOAR enterprise/MSSP-master with 7.4.0 or 7.4.1 versions of FSR agent or MSSP-tenants:
In the case of MSSP environments, it is recommended that you upgrade both the master and tenant nodes to release 7.4.4 or 7.4.3. If your master and tenant nodes are both not upgraded to release 7.4.4 or 7.4.3, take note of the following:

- Ensure that you synchronize records along with their relationships when you use the 'Sync Records' feature, if your master node is on release 7.4.2 or later, and your tenant nodes are on releases earlier than 7.4.2, such as 7.4.1 or 7.4.0.

- To download 'FSR Agent/Tenant node' logs, both the master and agent/tenant must be on release 7.4.2 or later. If the master node is on release 7.4.2 or later, and the agent is on a release earlier than 7.4.2, the log download is unsuccessful and returns an error such as "`For agents, log collection is accessible on version 7.4.2 and beyond`" .
- Replication from a tenant node that is on release 7.4.1 or 7.4.0 to a master node that is on release 7.4.2 or later will not fail if related records are not present on the master node. However, in the same case, replication from the master node to tenant nodes will fail if related records are not present on the tenant node.
- The update record request fails when the record is unavailable at the replicated end when a tenant node is on release 7.4.1 or 7.4.0 and the master node is on release 7.4.2 or later.

(**5**) Releases 7.5.2 and 7.6.3 are upgrade-only releases and upgrading an external FortiSOAR SME to both these releases are not supported.

Upgrade Procedure

During the upgrade, you are prompted to reset the `root` password and confirm it. If the two entries match, the password is updated successfully. If they do not match, the prompt is displayed again. If you cancel the prompt by entering n, the upgrade continues without resetting the root password. You are allowed up up to three attempts to enter matching passwords. If all attempts are exhausted, the upgrade task is marked as failed.
Carefully review and respond to all upgrade prompts. If the `root` password reset step is missed, the password must be reset later from the VM console. Refer to the Red Hat or Rocky Linux documentation for instructions on resetting the root password.
Note: After login, the 'csadm' user is assigned limited sudo privileges. For security reasons, '`root`' access is provided via the system console and is not available over SSH.
For detailed procedures on upgrading FortiSOAR, see the "Upgrade Guide"

After the Upgrade

Once the upgrade is complete, perform these checks to ensure system stability and optimal performance:

- **Clear browser cache**: Clear your cache and log out before signing back in to avoid any UI or functionality issues.
- **Verify key functions**: Review key system areas such as playbook audit logs, user access, and automation services.
- **Validate integrations**: Confirm that all connectors, integrations, and scheduled jobs are working properly.
- **Monitor performance**: Observe system health metrics and logs for any irregular behavior in the hours following the upgrade.

Product Integration and Support

Web Browsers & Recommended Resolution

FortiSOAR 7.6.5 User Interface has been tested on the following browsers:

- Google Chrome version 142.0.7444.162
- Mozilla Firefox version 145.0.1
- Microsoft Edge version 142.0.3595.90
- 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 7.6.5 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 9.3/9.4/9.5/9.6 or RHEL 9.3/9.4/9.5/9.6 and then install FortiSOAR using the FortiSOAR CLI installer. Note that release 7.6.5 has been tested with RHEL 9.6 and Rocky Linux 9.6. For more information, see the "Deployment Guide."

Resolved Issues

The following important issues have been fixed in **FortiSOAR release 7.6.5**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

Graphical User Interface

Bug ID	Description
1095054	Fixed an issue where applying advanced filters caused earlier column-level filters to be retained on grids. When an advanced filter was combined with column-level filters (for example, `status = open`), results displayed correctly, but after selecting **Clear All**, refreshing the grid, and reapplying advanced filters, the previous column-level filters persisted.
1212939	Fixed an issue where mouse scrolling did not work correctly when users scrolled to the extreme left or right of a grid. FortiSOAR would navigate to the previously visited pages (back or forward) instead of remaining on the current page, which prevented proper scrolling.
1222226	Fixed an issue where tags added to comments in the Collaboration Panel were not visible after reopening the record.
1231024	Fixed an issue where dashboards using the Summary widget displayed zero records when upgrading from versions earlier than 7.6.4 (e.g., 7.6.1) to release 7.6.4.

Playbooks & Connectors

Bug ID	Description
1054897	Fixed an issue where playbooks would enter the "Incipient" state when there were a large number of playbooks and historical logs.
1199787	Fixed an issue with reference playbooks containing a 'Manual Input' step. Previously, if the reference playbook failed at any step, the parent playbook was marked as failed, even if the "Ignore Error" option was enabled for the referenced step in the parent playbook. Now, if the reference playbook fails, the parent playbook will continue and be marked as 'Finished with Error.'

1148809	Fixed an issue where playbooks could remain in the *Awaiting* state when a *Wait* step was configured for less than 60 seconds. The task now stays with the current worker instead of being re-queued, preventing playbooks from getting stuck in the *Awaiting* state.
1203480	Fixed an issue with hierarchical picklists in playbooks (defined using JSON). Previously, when a parent category was selected and a child option was chosen, changing the parent category did not refresh the child picklist. As a result, the previously selected child options remained visible instead of updating to reflect the new parent category selection.
1206575	Fixed an issue where a scheduled playbook for storage space reclamation failed if the activity was already in progress when the playbook was triggered again. Now, in this scenario, the playbook correctly returns an “In Progress” status instead of failing.

System & Security

Bug ID	Description
1220039	During a rolling upgrade, the takeover operation failed when a node attempted to rejoin the cluster because one or more files under `/var/lib/pgsql/16/data/` were not owned by `postgres:postgres`. Since the PostgreSQL data directory did not meet the required ownership constraints, the cluster join process was aborted. This issue is resolved by adding an ownership-validation check that ensures all files in the directory have the correct ownership before the node attempts to rejoin the cluster.

Known Issues and Workarounds

- **1126843**: When a filter is applied on the listing page and a record is opened in a new tab, users may encounter a '`414 Request-URI Too Large`' error if the URL generated with the filters exceeds the default length limits.
  Workaround:
  To resolve this issue, increase the buffer size for client headers in your **Nginx** configuration file.
  Update the `large_client_header_buffers` setting from `4 8k;` to `4 50k;` in the `/etc/nginx/nginx.conf` file. After making the change, restart the '`nginx`' service as the '`root`' user to apply the changes by running the following command:
  `# systemctl restart nginx`
  If you are using HAProxy as a load balancer, follow these steps:
  a. SSH to your HAProxy VM and log in as *root* user.
  b. Edit `/etc/haproxy/haproxy.cfg` file.
  c. In the '`global`' section, add the following parameter:
  `tune.bufsize 32768`
  d. Restart HAProxy to apply the changes by running the following command:
  `# systemctl restart nginx`
- **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.
- **1220684**: Upgrading from release 7.6.1 to a later release (for example, 7.6.4, 7.6.5) causes the Utilities Connector '*Create an attachment from file action*' to fail with the following error:
  `CS-INTEGRATION-5: Error occurred while executing the connector action. ERROR :: 400 Client Error: Bad Request for url: https://localhost/api/3/files :: {'type': 'TypeError', 'message': \"Internal Server Error. Check log 'prod.log' for more details\"} :: Url: https://localhost/api/3/files Call for URL: https://localhost:9595/integration/execute/ failed with status code 400 \n`
  The issue occurs because the **Restricted File MIME Types** setting under **Settings** > **Application Configuration** has no values configured. As a result, file uploads fail.
  Workaround:
  After upgrading from release 7.6.1:
  a. Navigate to **Settings** > **Application Configuration**.
  b. Update **Restricted File MIME Types** to include the default values:
  `image/svg`
  `image/svg+xml`
  c. If any custom MIME types were configured before upgrading from release 7.6.1, re-add those values as well.
  d. Save the updated settings.
  For details, see the Enabling MIME type validations for file uploads topic in the "Administration Guide."
  NOTE: After upgrading from release 7.6.1, the TAXII server configuration is also automatically disabled.

If the TAXII server is required, manually re-enable it. For more information, see the Threat Intel Management Solution Pack documentation.

www.fortinet.com