Release Notes

FortiSOAR 7.6.4

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

October, 2025
FortiSOAR 7.6.4 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-11-11	Added the Additions to the Reserved Keywords List topic in the Special Notices chapter and updated the Upgrade Information chapter to reflect support for upgrading from versions 7.5.0–7.5.2 to 7.6.4.
2025-10-14	Initial release of 7.6.4

FortiSOAR 7.6.4 Release

Introducing the 7.6.4 release — packed with enhancements across security, performance, internationalization, and usability. This release delivers the following key features and improvements:

- **Enhanced Threat Intelligence Capabilities in FortiSOAR** : FortiSOAR continues to strengthen its native Threat Intelligence Management (TIM) capabilities by introducing new, purpose-built modules such as `Threat Actors`, along with a restructured user interface and simplified navigation. These enhancements deliver a more intuitive and efficient experience for security teams, enabling deeper threat context, faster investigations, and improved operational efficiency.
- **Improved Browser Performance**: Faster browser speed and better memory efficiency for a more seamless user experience.
- **Docker Support for FortiSOAR Agents**: Added support to deploy FortiSOAR Agents on Dockers, providing more flexible and scalable deployment options.
- **Vault Configuration Support in FortiSOAR Agents**: Strengthened credential management and security with Vault configuration support within FortiSOAR Agents. This enhancement enables secure, seamless integration between FortiSOAR Cloud and on-premises Agents configured with Vaults—allowing users to centrally manage sensitive credentials while ensuring compliance with internal security policies.
- **Extended Internationalization**, now including **French** and **Traditional Chinese** language support.
- **Refined User Interface**: Improved usability, visual consistency, and overall user interface design for a better experience.
- **Optimized Core Components**: Enhanced functionality across playbooks, connectors, solution packs, widgets, and core security services.
- **Expanded enhancements across key solution packs**—SOAR Framework, Threat Intel Management, Outbreak Management, and CICD—to improve functionality and performance.

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

New Features and Enhancements

This release brings exciting new features and enhancements to improve usability, boost performance, fortify data security, and enhance your FortiSOAR™ experience.

Threat Intelligence Capabilities integrated into FortiSOAR

- FortiSOAR now integrates advanced Threat Intelligence capabilities, powered by FortiGuard intelligence, Outbreak Alerts, and automated response workflows. These enhancements help security teams detect, respond to, and mitigate advanced threats faster—improving visibility and strengthening the security posture of your digital environment.
  To enable threat intelligence and outbreak management features, install and configure the Threat Intel Management and Outbreak Response Management Solution Packs.
  Key Highlights:
  - **Outbreak Management**:
    Receive real-time Outbreak Alerts from FortiGuard Labs, enabling your team to monitor, contain, and resolve widespread cyberattacks efficiently.
  - **Threat Intelligence Management**:
    Collect, analyze, and centralize threat intelligence from multiple sources. Enrich the data with context to better understand attacker tactics, techniques, and motivations. You can also **correlate Common Vulnerabilities and Exposures (CVEs) with active threat reports and actors** to identify which vulnerabilities are actively being targeted—prioritizing your patching efforts for maximum impact.
    The **Threat Intelligence Management** menu in FortiSOAR's left navigation contains the following items:
    - **Dashboard**:
      The **TIM Overview and ROI** dashboard offers insights into feed ingestion effectiveness, the connection between observables and indicators, and the relevance of threat feeds.
    - **Threat Intel Search**:
      Search FortiGuard's vast threat intelligence database to uncover detailed information on Indicators of Compromise (IOCs), including malware, threat actors, CVEs, and threat relationships.
    - **Intelligence**:
      - Provides a centralized location to manage threat feeds, actors, and reports. It contains the following tabs:
        - **Threat Reports**: Displays threat intelligence reports ingested from FortiGuard, FortiRecon ACI, and other sources.
        - **Threat Feeds**: Allows you to set up feed connectors such as FortiGuard, Anomali Limo, Cisco Talos, etc.
          Note: By default, Fortinet FortiGuard Threat Intelligence is added as a threat source.
        - **Threat Actors**: The `Threat Actors` (TA) page gets data from FortiGuard and gives analysts detailed information about attackers, their motives, and methods (TTPs).
        - **WorkSpaces**: The WorkSpaces page lets you create workspaces based on Priority Intelligence Requests (PIRs) to support focused workflows.

- **Feed Configurations**: The `Feed Configurations` page manages feed settings, lets you set up a TAXII Server to share threat intelligence externally, and create rules to automate feed ingestion.

- **MITRE ATT&CK**:
  The installation of the TIM Solution Pack configures the MITRE ATT&CK connector and schedules its data ingestion by default, allowing use of the globally accessible MITRE ATT&CK® Framework.
- **Hunts**:
  A centralized module to store and manage threat hunting activities.

For details, see the Threat Intel Management and Outbreak Response Management Solution Packs and the Threat Intelligence Capabilities chapter in the "User Guide."

Enhanced Browser Performance & Memory Efficiency

- FortiSOAR 7.6.4, FortiSOAR includes several improvements designed to reduce memory usage and boost browser performance, especially for memory-intensive tasks.
  Key Enhancements:
  - **Faster, More Responsive UI**:
    - **Optimized User Interface**: Refined codebase to minimize memory footprint and deliver faster performance.
    - **Smart Field Loading**: Lazy loading has been implemented for UI fields, so required fields load immediately at the top of the screen, allowing you to focus on essential data right away. Additional fields load dynamically as you scroll, ensuring a fast and seamless experience.
    - **Improved Data Ingestion Wizard (Field Mapping screen)**:
      - **Lazy Loading Support**: As with the UI, required fields appear first, allowing you to start quickly. Other fields load progressively as you scroll, maintaining efficiency and responsiveness.
      - **Enhanced Rich Text Fields**: Rich text fields now display as plain text inputs by default, improving initial loading times. You can toggle to the rich text view whenever needed, ensuring flexibility without sacrificing performance.
    - **Form View Update**: If a form structure is not defined for the records in a module, only fields marked as *required* or *required by condition* will be loaded in the Form View Template, i.e., in the **Add Record** form in the *List* view and the **Edit Record** form in the *Detail* view. This improves performance by avoiding the loading of all fields.
    - **Internationalization**: Improved management of translation keys by implementing one-time binding for UI translations in HTML files, reducing overhead and improving load performance.
    - **Widget Updates**:
      - **Playbook Buttons Widget**: More efficient rendering.
      - **Tabs Widget**: Only the active tab loads content, significantly reducing the initial load time and enhancing overall responsiveness.
      - **Uncategorized Fields Widget**: Lazy loading has been implemented to enhance performance. Fields now load dynamically as you scroll, providing a faster and more responsive experience.

  For details, see the 'Best Practices' topics in the *Working with Modules - Alerts & Incidents* chapter of the "User Guide."

Support for FortiSOAR Agent on Docker

- Starting with release 7.6.4, FortiSOAR Agents can now be deployed in Docker environments. This allows organizations that prefer containerization over traditional virtual machines to easily install and manage Agents within existing Docker environments and automate containerized operations.
  For details on deploying Agents on Docker instances, see the Deploying an FSR Agent on a Docker Platform chapter in the "Deployment Guide."

Support for Configuring Vaults on FortiSOAR Agents

- Release 7.6.4 introduces support for installing and configuring vault connectors on FortiSOAR (FSR) Agents, enabling those agents to access their associated vault and perform actions such as retrieving credentials for use in remote or isolated sites. This enhancement enables secure, seamless integration between FortiSOAR Cloud and on-premises Agents configured with Vaults—allowing users to centrally manage sensitive credentials while ensuring compliance with internal security policies.
  Key highlights are as follows:
  - **Agent Vault Access**: FSR Agents can retrieve credentials from their associated vaults, enabling operations in remote or isolated sites.
  - **Secure Access Model**: Each tenant or agent is limited to accessing only its own vault, ensuring secure and segregated access.
  - **Central Node Support**: FSR Agents can be deployed on a central node, such as the master node in an MSSP setup. The master node can access vaults configured on any associated agent or tenant and use the credentials for executing actions.

  

  If the FortiSOAR and Agent systems are on different networks, network latency may affect playbook execution time when the playbook needs to access a vault configuration on the agent node.

  For details, see the Configuring the Password Vault Manager in the *Security Management* chapter of the "Administration Guide."

Extended Internationalization Support with French and Traditional Chinese

- FortiSOAR now supports French and Traditional Chinese, expanding its internationalization capabilities. This update enhances the platform's accessibility and usability for global teams by enabling native language support and alignment with local preferences.
  For details on internationalization settings in FortiSOAR, see the Setting a language other than English for your FortiSOAR system topic in the *System Configuration* chapter of the "Administration Guide."

FortiSOAR User Interface Enhancements

- **Chart Enhancements**:
  - **Enhanced Line and TimeSeries Charts**:
    - Support continuous monthly series rendering, displaying all months even when some have no data. This ensures all months are displayed, improving trend visibility over time
    - Added a **Quarterly** option to the **X-Axis Date Range** drop-down. Users can now view data by quarter based on the selected X-Axis date field (e.g., Created On, Modified On). Quarters are displayed in a *year-quarter* format (e.g., 2024-Q3, 2025-Q1) in charts and/or tables. Daily and Monthly options remain available.
  - **Enhanced Pie, Bar, Timeseries, and Line Charts**:
    Improved to offer greater flexibility in data visualization. Users can now choose to display data as a chart, a table, or both. For example, an aggregation table can be viewed independently of the chart, enabling more focused analysis when needed.

  For details on charts, see the Charts and Metrics topic in the *Dashboards, Templates, and Widgets* chapter of the "User Guide."

Security Enhancements

- **New: Advanced Development Features Tab in System Configuration**: introduced 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."

Playbook Enhancements

- **Jinja Editor Enhancement**: In Release 7.6.4, the **Choose A Recent Playbook Execution** drop-down (**Tools** > **Jinja Editor** in Playbook Designer) now shows execution times in "`MM/dd/yyyy hh:mm a`" format (e.g., 09/21/2025 07:08 PM) instead of relative times like "2 hours 23 minutes ago." This change provides precise timestamps, improving debugging—especially when multiple executions occur close together.
  For details, see the 'Jinja Editor' topic in the *Dynamic Values* chapter of the "Playbooks Guide."

Solution Packs, Connectors, and Widget Enhancements

FortiSOAR 7.6.4 introduces key enhancements across solution packs, connectors, and widgets—designed to expand automation and integration for SecOps teams:

- **Notable Enhanced Solution Packs**:
  - *Threat Intel Management v2.1.0*: Now integrates with **MITRE ATT&CK** as a submenu, offering easy access to threat intelligence. A new **Threat Actor Info** page enhances investigations, while the **Threat Intel Search** feature enables customizable widget-based indicator searches, supporting faster, more accurate incident response.
  - *Continuous Delivery Solution Pack v3.1.0*: The Continuous Delivery pack simplifies lifecycle management of FortiSOAR content, enabling efficient change control across development, staging, and production. Key enhancements:
    - Improved CR tracking with new `CR Status` visibility
    - Better environment synchronization and automated export/import workflows.
    - Pull request monitoring and pre-approval content review.
    - Simplified reviewer selection via dropdown.
    - Unified Source Control Settings card for managing playbooks, modules, and connectors.
    - Enhanced import wizards for smoother deployments.

    This release boosts operational consistency by improving transparency, auditability, and control over SOC content deployment.
  - *SOAR Framework Solution Pack (SFSP) v3.2.1*: Improves user experience with new language support (Traditional Chinese and French). A `KeyStore` module update resolves post-installation issues by populating the new **JSON Value** field by default, enhancing installation reliability.
  - *Outbreak Response Framework v2.2.1*: This update (for FSR v7.6.1 and later) enhances outbreak response with smarter automation and richer threat context. Key features include:
    - Streamlined solution pack installation.
    - New **Summary** tab for critical alert details.
    - Improved dashboards with reorganized, clearer data.
    - Real-time automation actions for CVEs, IOCs, and outbreak alerts.
    - Renamed playbooks and restructured schedules for better manageability.
    - Expanded field mapping for Threat Actors and Reports, providing deeper context for SOC analysts.

    Additionally, a series of **Outbreak Response solution packs** have been introduced to provide countermeasures for newly detected security outbreaks. These packs include custom detection rules to mitigate risks from various attack types, enhancing proactive threat detection. Recent additions—such as **Citrix Bleed 2**, **Microsoft SharePoint Zero-day**, and **Earth Lamia APT**—demonstrate coverage of high-impact vulnerabilities and advanced persistent threats. When **outbreak auto-deployment** is enabled, these packs are **automatically deployed**, providing SOC teams with timely, prebuilt defenses without manual effort.
    These enhancements support faster, more efficient responses using up-to-date intelligence from FortiGuard Labs.
  - *FortiAI v4.0.1*: Includes bug fixes and performance improvements. User prompts now work as expected when key mappings are missing in the `KeyStore` (with **Recommendation Engine** enabled). Module performance is optimized for better responsiveness during operations.

  NOTE: All widgets in the respective solution packs have been updated.
- **Enhanced Connectors**: Multiple integrations (System, Fortinet Fabric and third-party) have updated – few notable ones being:
  - *System Connectors*:
    - **Utilities Connector v3.7.0**:
      - Adds a new `FSR: Evaluate Email Template Expressions` action, which evaluates Jinja2 expressions from the subject and content fields within email templates.

        - Enhances `Utils: Make REST API Call` with an **Upload File** parameter.
        - Fixes attachment extraction issues from `.eml`/`.msg` files with invalid byte sequences.
          For details, see the Utilities Connector v3.7.0 document.
      - **Code Snippet Connector v2.1.4**:
        - Defaults to '**Safe Mode**'.
        - Includes security-related fixes making working with this connector more secure.
          For details, see the Code Snippet Connector v2.1.4 document.
  - *Fabric Connectors*:
    Enhanced Fortinet Fabric connectors include:
    - **FortiSIEM**: Resolves API rate limit issues in Get Events For Incident (FSRv7.4.0+).
    - **FortiEDR**: Adds operations for collector search and management.
    - **FortiGuard Outbreak**: Adds a new action to retrieve threat actor details.
    - **FortiRecon ACI**: Supports new reporting and IOC actions, removes deprecated ones to streamline ingestion. These updates collectively enhance threat visibility and response across the Fortinet security ecosystem.
  - *Third-Party Connectors*:
    Key Updates include:
    - **Zscaler**: Now supports *OAuth 2.0* for improved security and easier setup.
    - **Microsoft Graph API**: Adds new parameters and actions for enhanced alert management (supports API versions V1 and V2).
    - **AWS EC2**: Resolves health check issues with an updated *boto3* library for better stability.

For details, see the FortiSOAR Content Hub.

Special Notices

This section highlights key operational changes in FortiSOAR release 7.6.4 for administrators to consider.

Administrator Consent required for Custom Connectors and Widgets in FortiSOAR 7.6.4 and later

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, FortiSOAR 7.6.4 introduces a new **Advanced Development Features** tab. 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:

Fresh Installation (FortiSOAR 7.6.4 or later):

Until administrator consent is granted:

- In **Content Hub**:
  - Users will **not** see the **Upload Connector** or **Upload Widget** options under the **Manage** tab.
  - Users will be unable to edit connectors or widgets, i.e., the **Edit** option will not appear when users click on the connector or widget cards.
  - Users will **not** see the **New Connector** or **New Widget** options under the **Create** tab, i.e., users will be unable to create new connectors or widgets.
- In **Export and Import Wizards**:
  - Users will **not** be able to export or import custom Connectors or Widgets.

Upgrade to FortiSOAR 7.6.4 or later:

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

- Existing custom connectors and widgets will remain available in their current state.
- However, they 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."

Change in iFrame Widget Behavior

Starting with release 7.6.4, the behavior of the iFrame widget has changed 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 directly displayed embedded content from both internal and external sources.

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 Widget topic in the "User Guide".

Change in Field Loading Behavior for Form View Template

Starting with release 7.6.4, the field loading behavior in form view has changed ***if a form structure is not defined (i.e., the form view template is not configured) for the records in a module*** (i.e., widgets are not added or configured as required—see the Dashboards, Templates, and Widgets chapter in the "Administration Guide"):

- **Before release 7.6.4**: All fields in the module were automatically included in the form by default, which could result in performance issues. For details on adding fields to a module, see the Module Editor topic in the "Administration Guide".
- **Starting with release 7.6.4**: Only fields that are *required* or *required by condition* are loaded in the Form View Templates, i.e., in the **Add Record** form in the *List* view and the **Edit Record** form in the *Detail* view. This improves performance by avoiding the loading of all fields.

Additions to the Reserved Keywords List

The keywords `task_id` and `wf_id` have been added to the list of reserved keywords. These are variables that **cannot be used in playbooks**.
Playbooks that currently use variables with these names will fail silently when attempting to create or reference them.

To resolve this issue, update the variable names in any affected playbooks.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to release 7.6.4 from releases 7.6.0 to 7.6.3 and 7.5.0 to 7.5.2. 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 "Upgrade Guide".

Product Integration and Support

Web Browsers & Recommended Resolution

FortiSOAR 7.6.4 User Interface has been tested on the following browsers:

- Google Chrome version 140.0.7339.134
- Mozilla Firefox version 143.0.1 (20250918214338)
- Microsoft Edge version 140.0.3485.81
- Safari version 18.6 (20621.3.11.11.3)
- 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 7.6.4 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 7.6.4 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 7.6.4**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

Graphical User Interface

Bug ID	Description
0947048	Fixed an issue where the **Select a Field** drop-down list did not display a scroll bar when using `Create Advanced Grid Filter` in module grids (e.g., Alerts).
1150477	Fixed an issue where record sorting was displayed incorrectly in module grids (e.g., Incidents) after applying filters and then removing them from the GUI using "Clear All" or "Clear Filter Criteria".
1157483	Fixed an issue where the data table was not reset (i.e., not *hidden*) when switching from a chart that supports data tables (e.g., Bar or Pie chart) to one that does not support them (e.g., Donut chart).
1173226	Fixed an issue that prevented adding visibility conditions to picklists in custom modules.
1175148	Fixed an issue where using the "Clear All" button to remove default filters broke the default sorting on the grid.
1177294	Fixed an issue where users were unexpectedly logged out of active sessions in FortiSOAR after upgrading to release 7.6.2.
1182042	Fixed the issue with the Timeseries widget not displaying months or fields with no data, instead of showing a value of 0. Now, the Line and TimeSeries charts support rendering as a continuous monthly series—even when some months have no data.
1190127	Fixed an issue where the 'View Password' (eye) icon on the FortiSOAR login page did not toggle the password visibility when a browser-based password manager extension (e.g., LastPass or NordPass) was enabled.

Playbooks & Connectors

Bug ID	Description
0970165	Fixed an issue where the vertical scrollbar in the Playbook Designer did not respond to mouse input and only worked with the keyboard.
0986751	Fixed an issue where playbooks configured as 'Private' did not retain their privacy setting or the `owners` attribute when exported.
0990406	Fixed an issue where multiple versions of the same connector (e.g., 4.2.0 and 4.2.3 of the Exchange connector) were occasionally displayed in the FortiSOAR UI after an upgrade.
1059984	Fixed an issue where playbook imports failed with the error message "`Some of the Playbooks already exist.`" even when the playbook was not present. This issue occurred when a playbook step, part of a playbook group, was exported and imported into another system, but the playbook containing the group did not exist. Now, during import, if a playbook step contains a group IRI that does not exist in the current playbook, the IRI is set to null, and the import proceeds successfully.
1078777	Fixed an issue where errors were shown instead of the connection status when using the '**Test Configuration**' button with invalid configurations while creating or editing a custom connector.
1142314	Fixed the health check failure on the Master node for connectors configured on Agent or Tenant. This issue occurred when traffic was initiated from the Master node, and both the Master and Tenant nodes used proxies.
1155786	Fixed an issue where the Manual Input form became unresponsive — text could not be selected, no cursor appeared, scrolling was disabled, and text was hidden. The form would only become responsive again after toggling to full screen and back. The issue was caused by the Markdown editor and has now been resolved.
1191496	Fixed an issue where opening the 'Executed Playbook Log' from a record detail page or the Playbook Designer page incorrectly applied a filter to the 'Historical Playbook Logs'. Now, when accessed from these pages, no filters are applied to either 'Historical Playbook Logs' or 'Recent Playbook Logs'. However, the global 'Executed Playbook Log' applies filters to both log types to display logs beginning 24 hours prior to the current time.
1129173	Fixed an issue where playbooks remained indefinitely in the "awaiting" state when the FSR Agent failed to respond. A scheduled task has been added to the `celerybeatd` service, which initializes at service startup and runs hourly. This task identifies playbooks stuck in the "awaiting" state that have exceeded the `CELERYD_TASK_TIME_LIMIT` and terminates them.

1191119	Fixed an issue where the Field Mapping screen became unresponsive when updating a module (e.g., Alert > Incident) in the Data Ingestion Wizard. The fix adds lazy loading for fields and initially displays rich text fields as text inputs, which users can toggle to rich text view.

System & Security

Bug ID	Description
1068738	Fixed an issue where users were incorrectly redirected to the FortiSOAR login screen when SSO was initiated from the Service Provider (e.g., Okta). This occurred when users did not log out properly—such as closing the browser directly—leaving an expired token in the browser. On the next login attempt, FortiSOAR used the expired token instead of the new one, causing the login screen to appear. FortiSOAR now correctly uses the new token, enabling seamless login without displaying the login screen.
1127495	Fixed an issue where users were unable to log into the FortiSOAR UI after the administration disabled 2FA configuration or the 2FA mandate at the global level. Users used to encounter the error: `"Your account is locked due to failure to comply with the 2FA mandate."` Now, when 2FA is disabled at the global level, users can log into the FortiSOAR UI without encountering the 2FA mandate error.
1183076	Fixed an issue where, when updating a field using *Advanced Edit* (Jinja2) with the **Append** option selected as the update method, the field was incorrectly overwritten instead of appended.
1185741	Fixed an issue where assigning a custom role to an existing user incorrectly overrode the user's existing roles and permissions for certain modules.

CLI & API

Bug ID	Description
1200233	Fixed an issue where the `csadm ha show-health --all-nodes` command and `/api/auth/cluster/health/` API returned a `"TypeError: 'builtin_function_or_method' object is not subscriptable error"` The command and API now correctly return the expected health details.

1141317	Fixed an issue where authentication with the HMAC token failed due to an unnecessary port number being appended when copying the API route in the Custom API Endpoint playbook trigger.

Known Issues and Workarounds

- **1126843**: When applying a filter on the "**Assigned to**" field in the 'Alerts' listing page and opening a record in a new tab, users may encounter a "`414 Request-URI Too Large`" error.
  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:

1. SSH to your HAProxy VM and log in as *root* user.
2. Edit `/etc/haproxy/haproxy.cfg` file.
3. In the '`global`' section, add the following parameter:
   `tune.bufsize 32768`
4. 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.

www.fortinet.com