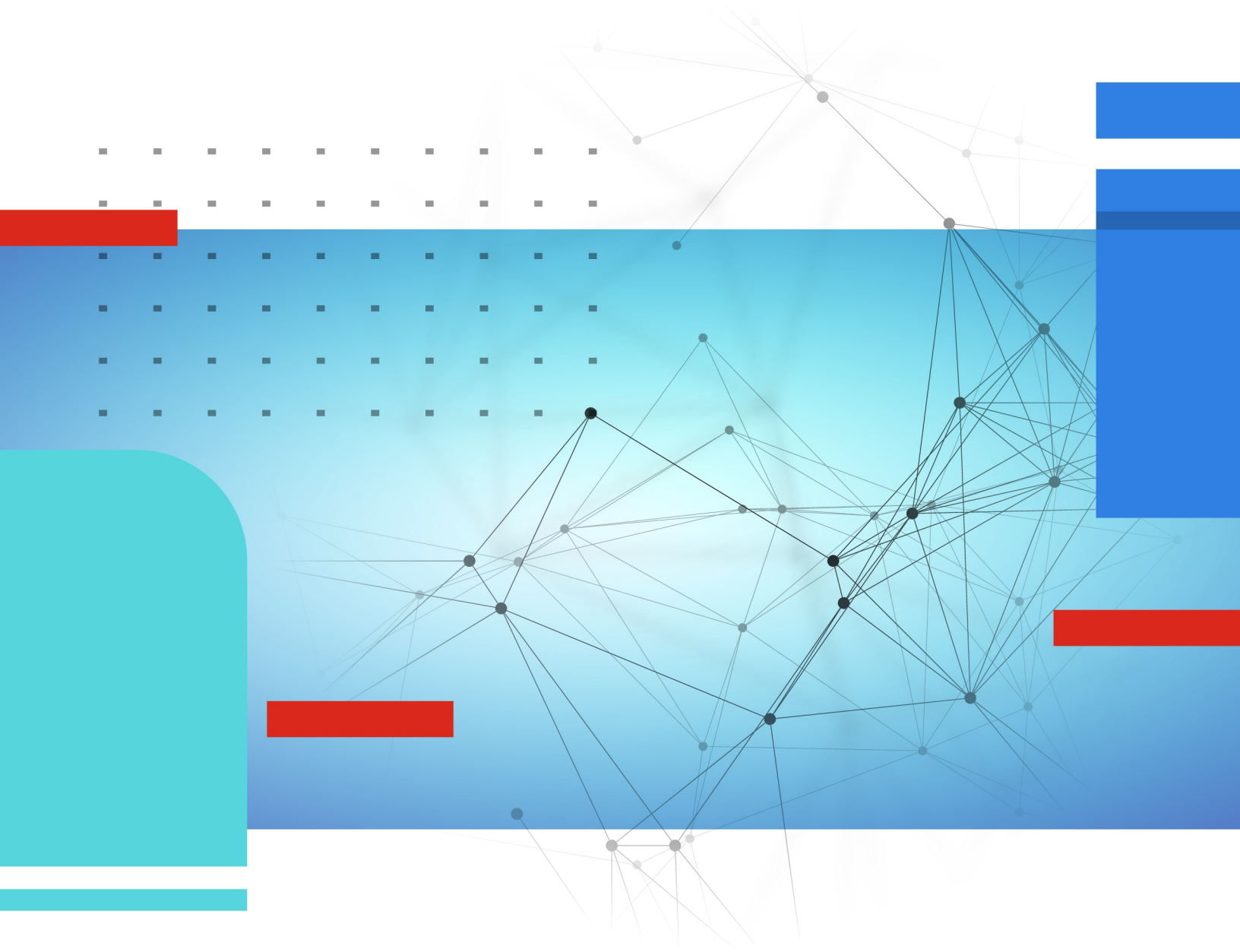
Release Notes

FortiSOAR 7.6.1



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, 2024
FortiSOAR 7.6.1 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-04-23	Minor update in the 'Virtualization' topic of the Product Integration and Support chapter.
2025-03-19	Updated the Special Notices chapter to include impact on upgrading to release 7.6.1 on the TAXII Server and MIME Type settings.
2024-12-09	Initial release of 7.6.1

FortiSOAR 7.6.1 Release

Welcome to FortiSOAR™ 7.6.1 release! This version introduces exciting new features and enhancements aimed at improving the user experience, performance, and security. Key highlights include usage-based licensing via FortiFlex, offering greater flexibility and scalability, and rolling upgrade support for high availability clusters, which minimizes downtime during updates. Data security is strengthened with the encryption of FortiSOAR data at rest.
Admin improvements include retaining customized playbook updates that were imported through a Solution Pack during solution pack upgrades, and optimized playbook log storage. The playbook designer now lets you view referenced playbooks, making it easier to identify parent playbooks. Executed playbook logs are now categorized as 'Recent' and 'Historical'; additionally, a new HA Node filter has been added to simplify searching for playbook executions on specific HA nodes. UI updates feature customizable page sizes for grids, enhanced widget configuration for automatic expansion in list views, and more!

Additionally, enjoy a variety of new solution packs, widgets, and connectors, and benefit from advancements in FortiAI, including support to give voice commands, to enhance analyst investigations and improve accessibility. The release also improves the SOAR Framework and Outbreak Management solutions, strengthening your security operations.

The release also includes performance enhancements and security updates to address vulnerabilities in FortiSOAR. For a detailed list 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 performance, strengthen data security, and elevate your FortiSOAR™ experience.

Usage-based licensing for FortiSOAR via FortiFlex

- Starting with release 7.6.1, FortiSOAR integrates with FortiFlex, offering usage-based licensing. FortiFlex provides a straightforward, points-based approach that empowers organizations to optimize their cybersecurity services and spending, providing flexibility in deployment and scaling.
- Using the FortiFlex portal you can easily manage and scale your entitlements, license seats, and expirations, as well as monitor your FortiPoint usage for effective cost tracking.
  For details, see the *Licensing FortiSOAR* chapter in the "Deployment Guide."

Rolling Upgrade Support for High Availability clusters

- FortiSOAR now supports rolling upgrades for high availability (HA) clusters, reducing downtime from approximately 30 minutes to just 2 minutes. This optimization ensures minimal disruption during upgrades.
  For details, see the *Upgrading a FortiSOAR High Availability Cluster* chapter in the "Upgrade Guide."

Strengthened Data Security: Data-at-Rest encryption for FortiSOAR

- FortiSOAR introduces a powerful new feature that elevates your data security: encrypting FortiSOAR's data at rest. Data at rest encryption is vital for safeguarding sensitive information against unauthorized access. FortiSOAR achieves this using 'Disk Encryption', which is a robust solution that helps to ensure data remains secure on Linux systems, even in the event of physical theft or breaches. This on-demand feature puts you in control of your data security.
  For details, see the *Encrypting FortiSOAR's Data At Rest* chapter in the "Deployment Guide."

Administrative Enhancements

- **Retention of customized playbooks that were imported through a solution pack during Solution Packs upgrades**: In release 7.6.1, any custom changes you make to your playbooks that are imported through a solution pack will be preserved during solution pack upgrades, saving you time and effort. Previously, if you edited playbooks that were part of a solution pack, it was recommended to clone them first to prevent losing your customizations during upgrades. With this update, you no longer need to take this extra step—your custom playbooks are preserved, simplifying your upgrade process.
  For details, see the *Introduction to Playbooks* chapter in the "Playbook Guide" and the *Solution Packs* chapter in the "User Guide."
- **Playbook log movement to optimize workflow logs storage**: This enhancement moves playbook logs to historical storage after playbooks are completed. This helps reduce the size of the active storage, improving performance, and making playbooks more efficient.
  For details, see the *Debugging and Optimizing Playbooks* chapter in the "Playbook Guide" and the *System Configuration* chapter in the "Administration Guide."
- **Navigation Structure Optimization**: The navigation structure options when exporting and creating solution packs have been enhanced. Previously, you could only append navigation items. You can now choose to replace or

merge all the navigation items or apply these options to selected individual items. This enhancement offers you greater flexibility in customizing your navigation experience.
For details, see the *Export and Import Wizards* topic in the Application Editor chapter of the "Administration Guide."

Playbook Designer and Executed Playbook Logs Dialog Enhancements

- **Option to view playbooks referencing the current playbook**: In release 7.6.1, we've added a new option at the top of the playbook designer canvas. This option allows you to quickly view a list of playbooks that are referencing the current playbook, making it easier to identify the parent playbooks.
  For details, see the *Introduction to Playbooks* chapter in the "Playbook Guide."
- **Executed Playbook Logs enhancements**: In release 7.6.1, we've improved the Executed Playbook Log dialog with the following updates:
  - **Bifurcated Log Display**: Playbook logs present in the active storage are displayed in the '**Recent Playbooks Logs**' list, while logs in the historical storage are shown in the '**Historical Playbook Logs**' list.
  - **New HA Node Filter**: A new filter has been added to the Executed Playbook Logs dialog for high availability (HA) clusters. You can now filter logs by node name, making it easier to find playbook executions on specific HA nodes.
    For details, see the *Debugging and Optimizing Playbooks* chapter in the "Playbook Guide."

FortiSOAR User Interface Enhancements

- **Enhanced Widget Configuration**: Widgets can now be set to always expand in the list view of modules, allowing for quicker access to important information.
  For details, see the *Dashboards, Templates, and Widgets* chapter in the "User Guide."
- **Customizable Page Sizes for Grids**: Grids now support customizable record display options on the list view of modules, both at the module and user levels. Users can select their preferred default number of records per page from the following options: 5, 10, 30, 50, 100, or 250. This enhancement replaces the previous default of 30 records, offering greater flexibility and a more personalized viewing experience.
  For details, see the *Dashboards, Templates, and Widgets* chapter in the "User Guide."
- **Pagination Support for Executed Playbook Logs**: Pagination support has been added to the Executed Playbook Logs dialog. You can now effortlessly navigate through your executed playbook logs, making it easier to find what you need.
  For details, see the *Debugging and Optimizing Playbooks* chapter in the "Playbook Guide."
- **Enhanced License Manager page**: Added a refresh button next to the **Allowed Actions Per Day** field. This field displays both the total action count and the remaining number of FortiSOAR actions users can perform each day. With the addition of the refresh button users can quickly update the count without reloading the 'License Manager' page.
  For details, see the *Licensing FortiSOAR* chapter in the "Deployment Guide."

Solution Packs, Connectors, and Widget Enhancements

Several new enhancements are introduced across solution packs, connectors, and widgets. Here are some key updates:

- **Notable New and Updated Solution Packs**:
  - *Multiple Outbreak Alert Response Solution Packs* are added to conduct hunts that help identify and investigate potential Indicators of Compromise (IOCs) related to vulnerabilities across operational environments such as FortiSIEM and FortiAnalyzer.

- *Outbreak Response Framework* (ORF) has been revamped with several key enhancements including a dynamic outbreak response dashboard that provides a comprehensive overview. Automation capabilities have been improved with the addition of new schedules, streamlining outbreak response tasks. An enhanced configuration wizard simplifies the process of configuring ORF for various integrations from the configuration wizard page. Additionally, the framework now includes a pluggable threat hunting framework that integrates with FortiSIEM and FortiAnalyzer, enabling more effective outbreak alert detection. For details, see the Outbreak Response Framework document.
- *SOAR Framework Solution Pack (SFSP)* includes a single keystore record that simplifies the management of all types of Indicators of Compromise (IOCs). It also comes with optimized pre-installed connectors that accelerate deployment, among other updates. Some key enhancements include:
  - *Streamlined Indicator Extraction*: A user-friendly, wizard-like interface simplifies the process of:
    - defining indicators to be excluded from extraction, both in small groups and in bulk
    - mapping alert and incident fields to be extracted as indicators
    - creating custom indicator types
    - adding comments to excluded file indicators and creating file indicators from email attachments
  - *Enhanced Record Security*: The role 'Full App Permission' no longer grants the ability to delete 'Key Store' records, preventing accidental removal and adding an extra layer of fail-safe protection.
  - *Setup Guide*: The **Streamline** section of the Setup Guide has been updated to prioritize indicator extraction as the first setup step, offering a smoother and more efficient setup experience.

  These updates make SFSP faster, more efficient, and highly configurable, so you can work smarter and with greater confidence. For details, see the SFSP document.
- *FortiAI*, is now more powerful, allowing users to easily create prompts using their own voice. Additionally, you can search any FortiSOAR record simply by providing a prompt, with the flexibility to make searches as complex as needed. These enhancements drastically reduce the time SOC analysts spend querying data or writing complex prompts, empowering them to investigate and complete tasks more efficiently, while also improving accessibility. For details, see the FortiAI document.
- *Lacework FortiCNAPP*, now integrates with Microsoft Teams to streamline operations. It also introduces secure authentication for webhooks in incident response, along with other improvements that further enhance incident response capabilities. For details, see the Lacework FortiCNAPP Composite Alert Incident Response document.

◦ **New and Updated Connectors**: Multiple integrations (Fortinet Fabric and third-party) have been released, along with updates to existing connectors – few notable ones being:

- *New integrations* include: AWS WAF, Bitbucket, Coralogix, IBM Randori, ManageEngine Log360, Proofpoint TRAP, SonicWall Firewall. Additionally, new threat feed integrations such as alphaMountain Feed, CINS Army Feed, and ViriBack C2 Tracker Feed have also been added.
- *Enhanced Fortinet Fabric* integrations include: Fortinet FortiSASE, Lacework FortiCNAPP, Fortinet FortiManager, Fortinet FortiAnalyzer, Fortinet FortiWeb Cloud.
- *Enhanced Third-Party* integrations include: Exchange, Qualys, Palo Alto Firewall, Palo Alto Cortex XDR, OpenAI, Microsoft Teams, Microsoft WinRM, Microsoft 365 Defender, Joe Sandbox Cloud.

For details, see the FortiSOAR Content Hub.

◦ **New and Updated Widgets**: Key widgets have been enhanced for better usability and functionality:

- *Playbook Buttons* widget adds playbooks as separate buttons in the record's detailed view, allowing them to be executed directly from the record's view panel. For details, see the Playbook Buttons document.

Special Notices

This section highlights key operational changes in FortiSOAR release 7.6.1 that administrators need to know.

Upgrade to FortiSOAR 7.6.1 causes the TAXII Server to be disabled and MIME Type fields to be reset

The impact of upgrading to FortiSOAR 7.6.1 on the TAXII Server and MIME Type settings are as follows:

- **TAXII Server Disabled**: The TAXII server configuration will be automatically disabled. You must manually re-enable the TAXII server. For details, see the Threat Intel Management Solution Pack documentation.
- **MIME Type Settings Reset**: Any custom MIME type validations for file uploads, added based on your organization's policies in the **Restricted File MIME Types** field, will be reset to their default values. You will need to manually re-add these MIME types to the **Restricted File MIME Types** field. For details, see the Enabling MIME type validations for file uploads topic in the "Administration Guide."

NOTE: These issues will be addressed in FortiSOAR 7.6.2.

FortiSOAR MEA discontinued for FortiAnalyzer and FortiManager

Starting with release 7.6.1, the FortiSOAR Management Extension Application (MEA) is discontinued for FortiAnalyzer and FortiManager.

Change in Playbook Execution Logs API behavior

In release 7.6.1, the Playbook Execution Logs API is divided into 'recent' and 'historical' execution logs. To retrieve consolidated records i.e., both the recent and historical playbook execution logs use the `/api/wf/api/workflows` API. To retrieve historical playbook execution logs, use the `/api/wf/api/historical-workflows/` API. Previously, the single API (`/api/wf/api/workflows/`) was used.

Added a maximum allowable wait time for playbooks that include a wait, manual input, or approval step

For playbook optimization, playbooks that remain in the 'awaiting' state for more than 7 days will be automatically terminated. As a result, the maximum allowable wait time for a playbook is now 7 days. Previously, there was no maximum wait time.

Change in the behavior of purging executed playbook logs

Starting with release 7.6.1, the purge function excludes 'Recent' playbook logs and playbooks executed on the same day when purging 'Historical' logs.

Playbook execution logs movement to historical storage

Once you have upgraded your FortiSOAR system to 7.6.1, existing playbook execution logs are moved to historical storage to optimize workflow logs storage. This background process could take some time depending on the size of existing playbook execution logs; however, this will not affect FortiSOAR's functionality.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to release 7.6.1 from release 7.6.0. 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 7.6.1 User Interface has been tested on the following browsers:

- Google Chrome version 131.0.6778.86
- Mozilla Firefox version 133.0
- Microsoft Edge version 131.0.2903.70
- Safari version 18.1 (20619.2.8.11.10)
- 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 7.6.1 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 7.6.1 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 7.6.1**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

FortiSOAR UI Fixes

Bug ID	Description
0835378	Resolved an issue where applying or removing advanced filters automatically set the page size to 30. Users can now apply or remove advanced filters without affecting the page size.
0864218	Fixed the issue with nested filters not being retained in the grid. Previously, when a filter was applied from the bar chart in a module like 'Incidents' and additional filters were selected from the List view pane, the extra grid filter conditions were cleared after closing the detail view of an incident. Now, when returning to the records list after viewing a record's detail view, all previously selected grid filter conditions will be retained.

Playbook Fixes

Bug ID	Description
1079928	Fixed the issue where playbooks with invalid Unicode characters were failing. A generic sanitize method has been implemented to remove these invalid characters. Additionally, any arguments evaluated during failures are now saved after sanitization. Do note that in this case, the playbook will still fail, as it remains in an exception state; however, a clear error message will now be displayed.
1081480	Fixed the issue that required users to have '`Security Update`' permission to rerun playbooks. Now, users only need '`Playbook Read`' and '`Playbook Execute`' permissions to rerun playbooks.

Other Fixes

Bug ID	Description
1009821	Fixed the issue of log forwarding settings from the primary node not being reflected on the secondary node(s) in High Availability clusters.

1060002	Fixed the issue with aggregation operations, such as median, displaying incorrect results for 'Ownable' modules with multiple teams.
1066053	Fixed the SAML Sign-On (SSO) issue that caused FortiSOAR to remain logged in on the IdP side after FortiSOAR logout.
1074507	Fixed the issue of memory consumption reaching 100% after the 7.6.0 upgrade. In release 7.6.1, memory consumption no longer reaches 100% post-upgrade.

Known Issues and Workarounds

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

www.fortinet.com