Release Notes

FortiSOAR 7.4.1

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

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 CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-06-23	Initial release of 7.4.1

FortiSOAR 7.4.1 Release

Fortinet Security Orchestration, Automation, and Response Platform (FortiSOAR™) release 7.4.1 comes with improved usability, including enhancing the user experience for building playbooks, including revamping the Approval step, adding an option to exclude a certain set of workflows, etc. Additionally, added support in the FortiSOAR Licensing option for the FortiSOAR "Perpetual" license type to include support for FortiSOAR Threat Intel Management Subscription Service, added support for Leave Management to the Queue and Shift Management feature, added support for conditional visibility for widgets on the View Panel, and various enhancements in the FortiSOAR UI. This release also adds multiple security fixes to ensure vulnerabilities are fixed in FortiSOAR.

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

New Features and Enhancements

Added support for Leave Management to the Queue and Shift Management feature

You can use the Leave Management feature in Queue and Shift Management, to prevent assignment of records to users who are on leave or paid time off (PTO). Using Leave Management, users who are on leave are excluded, and records are not assigned to them for the duration of their leave.

Revamped the Approval Step

○ Updated the 'Approval' step to honor RBAC, customizations, etc. Also, the response from the approval step now includes the approval status.

Added support for conditional visibility for widgets on the View Panel

○ Provided a setting for conditional visibility of widgets that appear on the detail view of the record, i.e., the View Panel. You can choose to restrict the visibility of widgets based on the conditions you have specified. In such cases, widgets are displayed only if the visibility condition is satisfied; otherwise, they are hidden.

Added support for creating custom functions and function references using connectors

○ Support is added for creating custom functions and function references using connectors. You can add custom functions or function references to your custom connector, edit an existing connector to add custom functions, or expose an action of a connector as a function. The following benefits to users are brought about by this improvement:
  - Export/Import of custom functions using the Export and Import Wizards.
  - Jinja2/Ansible/YAQL or simple python function references can be easily added to the Functions tab in Dynamic Values, making them usable in playbooks and the Jinja Editor.

Introduction of a FortiSOAR Licensing option for the FortiSOAR "Perpetual" license type that includes support for the FortiSOAR Threat Intel Management Subscription Service

○ Added a new licensing option for the FortiSOAR "Perpetual" license type that supports the subscription service for FortiSOAR Threat Intel Management Service, including FortiGuard Premium Threat Feeds. This service allows you to use the Threat Intel Management service to its fullest extent, and includes unrestricted consumption of FortiGuard feeds.

Enhanced Global Search

○ Added a **Query Based Search** option to Global Search that enables users to efficiently search across FortiSOAR by utilizing wildcards or operators such as 'NOT', 'AND', 'OR', fuzzy queries, etc.

○ Added support for UUID searches in Global Search. Using global search, which enables searching for playbooks, records, etc. using their UUIDs, users are now able to use playbook failure notifications to quickly search for failed playbooks and related records.

Administrative Enhancements

○ Enhanced the `--status` argument of the `csadm` command to include information about how long the services have been active. Knowing the last active time of a service can assist with troubleshooting when a service is restarting repeatedly due to an issue.

○ Added the `--validate` argument to the `csadm system disk expand-lv` command, with either the `--disk` or `--use-vg` argument. This argument validates the inputs passed for the `csadm system disk expand-lv` command and provides a summary of changes that will be made after running this command. This enables users get details of the available space on the partition, the new expanded size of the disks, etc. Users will also be aware of any issues that could prevent them from expanding the partition. Therefore, it is advisable to use the `--validate` argument before executing the `csadm system disk expand-lv` command.

○ Improved are made to the **System Fixtures** tab in System Configuration to include links to dedicated pages for self agent and self tenant. This makes it simpler to update details of the self tenant and agent such as remapping teams linked to the self tenant or tenants linked to the self agent.

Playbook Enhancements

○ Provided an option to exclude a certain set of workflows, such as 'Pause SLA', from appearing as suggestions in the 'Suggested Playbooks' list.

○ Introduced the 'Step Utilities' option in the Input/Output tab in Dynamic Values that enables you to use the values of list items if the step contains a loop. This option makes it easier to use the values of the items that are part of a list in the playbook step.

○ Added query params (`api_params`) in Input > Parameters in Dynamic Values displayed for steps of the Custom API Endpoint trigger playbook so that you can get some input from outside FortiSOAR and then further process that data in the next steps of the playbook.

○ Provided users with the option to provide customized messages that are displayed on the FortiSOAR UI when an approval playbook or a manual input playbook is resumed.

○ Provided users with the option to either customize the message that is displayed when a manual trigger playbook is triggered or to disable the system message from appearing. In playbooks when a manual input form is displayed right away after the playbook is triggered, you might not want to see this message because it is superfluous and can detract from the user experience.

○ Enhanced the Dynamic List option in User Prompt to allow users to select multiple options from the input prompt.

○ Added the 'Message' step utility to the 'Set Variable' and 'Decision' steps, enabling users to add custom messages to these steps. For example, adding a message with the outcome of the decision step, such as "`Blocked the IP <IP address> based on the reputation retrieved from FortiGuard`".

○ Added error details to the 'Terminated' playbooks that explain why they were terminated. When playbooks are terminated for reasons, such as exceeding the permissible time limits set for playbook execution, this information is helpful for troubleshooting playbook failures.

Connector Enhancements

○ Added a `Dependent Solution Packs` section that contains a list of solution packs that are dependent on the connector for them to work correctly in the **Summary** tab in the connector configuration popup. Users can use this information to install specific solution packs that use the connector.

- Provided a choice to users to configure connectors on a remote FSR Agent or on the current FortiSOAR node (Self) while creating or updating a notification channel.
- Removed the confusion caused by the display of two tiles of the same connector that were being edited on the **Discover** tab of the Content Hub. For example, if you were editing VirusTotal v1.0.0, the **Discover** tab displayed both "VirusTotal v1.0.0" and "VirusTotal_v1.0.0_dev." The **Discover** tab now just displays "VirusTotal v1.0.0," as copies of the connector that is being edited are no longer displayed on this tab.

Improvements in FortiSOAR UI

- Improved the presentation of tags with long names in reference blocks, comments, and single line item widgets so that the text of these tags does not break, and the entire tag is displayed on a new line.
- Provided an option in the Purge Audit Logs dialog that allows users to deselect all the event type options; by default, all the options are selected. This is useful for users who want to purge just a few event types.
- Added Field Suggestions, Similar Records, and Playbook Suggestions are now independent tabs in the Recommendations pane, which increases the visibility of the content in each of these pages. There have also been performance enhancements made to the Recommendations pane.
- Added an option to the Reference a Playbook step to open a referenced playbook in a new window. By allowing users the option to view the contents of the referenced playbook in a new window while viewing the referencing playbook's whole flow on the same canvas in the playbook designer, improves the user experience when creating playbooks.
- Provided an option to pin a playbook to the 'Relationships' widget. This is useful for frequently used playbooks that users want to display directly on the Relationships grid rather than having to choose them from the 'Execute' drop-down list.
- Added pagination support for the 'Simple Grid' widget to enable easy navigation through records.
- Differentiated the display of tags and categories in the "Filtered By" section on the Content Hub page when users apply the same filter for both 'Category' and 'Tags'.
- Added support for disabling links in Rich Text (HTML) or Rich Text (Markdown) fields. You can disable links in fields such as 'Email Body,' as you might want to prevent users from clicking on links in phishing emails, etc.
- Enhanced the `Prerequisites` section in the Solution Pack **Summary** tab to display **Update Available** for dependent solution packs that have a lower-level version installed on your FortiSOAR system than what is required for the solution pack that you want to install.

Added a failure message and failure icon on the FortiSOAR Configuration Wizard for provisioning failures

- If the FortiSOAR Configuration Wizard fails when provisioning your instance, then the "The FortiSOAR system provisioning has failed" message and a failure icon for that component are both displayed on the configuration wizard. The functionality associated with the failed services is affected but you have the option to fix the provisioning issues after configuring your FortiSOAR instance and continue with setting up your FortiSOAR instance by clicking the **Proceed Anyway** button.

Allowed for the direct editing of connectors and widgets that are part of the FortiSOAR repository

- The FortiSOAR repository's connectors and widgets can now be modified directly without having to be cloned. Previously, editing connectors and widgets that were a part of the FortiSOAR repository required users to first clone them, which was incompatible with editing other types of content in Content Hub and complicated troubleshooting.

Enhanced the 'cyops-search' service performance

○ Added sub processes for the 'Data', 'Status', 'System', and 'Search' queues to improve the 'cyops-search' service. Sub processes enable the parallel execution of operations such as indexing, searching, etc., which improves performance and user experience.

Built-in Connector and Widget Enhancements

○ Updated multiple built-in connectors such as the FSR Agent Communication Bridge Connector, Utilities Connector, etc. For more information on FortiSOAR Built-in connectors, see the "FortiSOAR™ Built-in connectors" article.
○ Added multiple widgets such as Funnel Chart widget, C3 Charts widget, Time Series Charts, etc.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR release 7.4.1.

Approval step does not support 'Email' as a mode of approval

In release 7.4.1, the Approval step has been revamped to honor RBAC, customizations, etc. However, from release 7.4.1 onwards, you can use only system notification as a mode of approval and cannot use **Email**.
In the case of systems upgraded to release 7.4.1, your existing Approvals steps will appear as were present in releases prior to 7.4.1 and if **Email** as a mode of approval (apart from the default, which is system notification) had been setup, then that would work. However, when you add new playbooks with the Approval step, those cannot have **Email** as a mode of approval.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 7.4.1 from version 7.4.0 only. 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 7.4.1 User Interface has been tested on the following browsers:

- Google Chrome version 113.0.5672.127
- Mozilla Firefox version 113.0.2 (64-bit)
- Microsoft Edge version 113.0.1774.57 (Official build) (64-bit)
- Safari version 15.5 (17613.2.7.1.8)
- The recommended minimum screen resolution for the FortiSOAR GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI might not get properly displayed.

Virtualization

This section lists FortiSOAR version 7.4.1 product integration and support for virtualization:

- AWS Cloud
- Fortinet-FortiCloud
- VMware ESXi versions 5.5, 6.0, and 6.5
- Redhat KVM

> For any other virtualization or cloud hosting environment, you can install Rocky Linux 8.7 or RHEL 8.7, and then install FortiSOAR using CLI. For more information, see the "Deployment Guide."

Resolved Issues

The following important issues have been fixed in **FortiSOAR release 7.4.1**. This release also includes important security fixes. To inquire about a particular bug, please contact Customer Service & Support.

FortiSOAR UI Fixes

Bug ID	Description
0834659	For Updated, Created, or Deleted conditions in Rules used in, for instance, the Wait step, Queue Management, or Notifications, module listing presented module names in the plural format. This displayed a condition such as 'When a(n) Alerts is Created', which is not a correct sentence. Now, the module names are listed in the singular format, so that the condition appears correctly as 'When a(n) Alert is Created'.
0843723	Fixed the issue with auto refresh not working when widgets, connectors, or solution packs were deleted from the **Create** tab on the "Content Hub" page.
0871309	Fixed the issue of users being unable to terminate playbooks that were in the 'Incipient' state from the FortiSOAR UI.
0875546	An update made to the profile picture of a user was not getting reflected on the 'User Tile' widget. This issue has been fixed and now the updated profile picture of the user gets displayed on the 'User Tile' widget.
0888574	Fixed the issue with the 'Escalate' button on the alert details page appeared to be loading indefinitely if the alert details page was closed immediately after clicking the 'Escalate' button. Now, the status of the 'Escalate' button in the alert details page is updated after refreshing the page.
0907312	In the Content Hub, users were unable to create content with a name that was the same as any existing content. For instance, if your FortiSOAR instance had the 'Fortinet FortiSIEM' connector, you would be unable to create a Solution Pack with that name. Now, as both the name and type are verified for uniqueness in the Content Hub, you can generate content with the same name. However, it is recommended that unique names be given to content created in the Content Hub.
0908850	Fixed the issue with 'Last Calendar Month' parameter not being retained while editing widgets.
0917002	Users were unable to remove filters that had been added to a module's grid view, such as the 'Type' and 'Status' column filters for the Alerts module. Now that this issue has been fixed, filters can removed, and the results get updated in the grid view.

Playbook Fixes

Bug ID	Description
0737157	The complete dictionary of picklist fields such as status, category, etc. in playbook steps such as create record, update record, etc. were getting saved. Saving the complete dictionary of picklists is unnecessary; only the IRI of picklists is required. Therefore, now only the IRI of the picklist fields is saved, which helps reduce that amount of data in the playbook log.
0892267	Fixed an issue where, playbooks with multiple manual inputs, the last manual input would trigger all the steps rather than just those specific to that manual input.
0899284	Fixed the issue that the reference playbook step was unable to retrieve the last run result.
0905854	Child reference playbooks were not being exported along with their parent playbook collection when they were present in a playbook collection other than the parent playbook collection. This issue has been resolved and now, child reference playbooks are exported along with their parent playbook collection, even if they are present in a playbook collection other than the parent playbook collection.
0910205	In a conditional field of a decision step in a playbook, the UI automatically adds the opening and closing parenthesis while saving the playbook. Now, if the condition is generated using some functions from the 'Dynamic Variables' window, then parenthesis get added twice, which causes the playbook to fail. To resolve this issue and prevent parenthesis from being automatically re-added, parenthesis are deleted from the condition field of the decision step.
0915789	An issue that caused extra iterations for three-level nested child playbooks with 'Wait' steps or steps set to run on 'Agent' nested at the third level has been fixed.
0920299	The issue with playbooks displaying IRI values in picklist fields, which made it difficult for users to understand the value of the assigned picklist item, has been fixed. Playbooks now display the item values of picklist fields.

Connector Fixes

Bug ID	Description
0856982	Users were not prompted to save their changes before publishing a new connector using the Connector Wizard, which could result in the loss of changes. The 'Publish Connector' button is now disabled if changes are not saved, requiring users to save their changes before publishing the connector.

Other Fixes

Bug ID	Description
0871307	Fixed an issue with schedulers not terminating playbook instances that were stuck in the 'Incipient' state. Now, playbooks stuck in the 'Active' or 'Incipient' state are terminated automatically when their permissible execution time limit is exceeded.
0877140	The error code of the failure was not previously recorded in the failed record logs. Now, the failed record logs include the failure code and the cause of the failure, which simplifies debugging.
0879780	To embed an image inside the widget html, the entire path, including the widget version, required to be specified. To resolve this issue, the `widgetBasePath` variable has been added, which may be used to reference version agnostic paths for assets such as images in the widget html. **Note**: This is supported from FortiSOAR release 7.4.1 onwards.
0886300	Fixed the problem with the Global Audit page loading slowly when there was a lot of audit data.
0891773	While setting up a proxy server using the `csadm network set-https-proxy` command, the 'https' protocol is used even if the protocol is set as 'http', which causes errors during upgrades and when downloading packages like cryptography, uwsgi, pycryptodome, pyOpenSSL, etc. To fix this issue, the `--protocol` argument has been concealed in the of the `csadm network set-https-proxy` command's help and suggestions, and 'http' is used as the default protocol to communicate with the proxy server.
0892715	The 'module_permissions' table was never cleaned up, so even when an existing role was re-imported, new permissions were added to that role without cleaning up the old permissions. Now, the new permissions for an existing role that is re-imported now replace prior permissions.
0909745	The starting and stopping of schedules were not logged in the audit log. As this is required, the start and stop activities for schedules are now logged in audit logs.
0911517	Users were presented with an incomplete prompt "Have you taken the snapshot of your virtual machine (Yes/No)", when they first ran the upgrade script. As a result, this prompt has been updated to be more thorough: "The upgrade process makes important changes to the kernel and application layer. You need to take a snapshot of your virtual machine in order to restore it to its pre-upgrade condition in the event of any failures. Before starting the upgrade, please ensure that you have taken a VM snapshot. (Yes/No)."
0922475	Fixed the issue of users getting an internal server error when removing an existing client certificate from the detail view of a FSR Agent record.

Known Issues and Workarounds

Issue 0856205: Users cannot login to the FortiSOAR Web UI if the password of the `'cyberpgsql'` users of your externalized FortiSOAR PostgreSQL database contains any of the following characters: `' ^ $`.
Run the following command on the external database to update the password for the "`cyberpgsql`" user in order to resolve this problem:
`psql -c "alter user cyberpgsql with password 'new_password'"`
Also, this issue will be fixed in upcoming releases of FortiSOAR.

FortiNET

www.fortinet.com