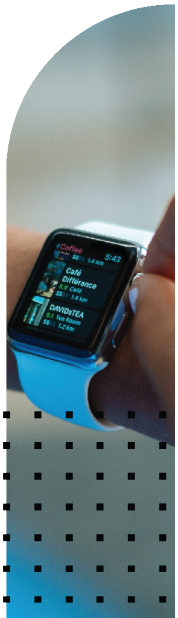
Release Notes

FortiSOAR 7.0.0



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

NSE 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

April, 2021
FortiSOAR 7.0.0 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-04-23	Initial release of 7.0.0
2021-09-06	Updated the "Arrow Library Update" section in the Special Notices chapter.

FortiSOAR 7.0.0 Release

The Fortinet Security Orchestration, Automation, and Response Platform (**FortiSOAR™**) 7.0.0 release introduces many new features and product enhancements, that aim to empower smart, quick, and informed threat investigations like never before. Main release highlights are an all-new collaborative crisis management hub, the 'Incident War Room', the FortiSOAR mobile application for facilitating quick and important actions on the move, and the 'Connector Builder Wizard' that allows to edit existing and build new connectors in the UI. There are notable enhancements as in the ML-powered Recommendation Engine, Action level RBAC, FortiSOAR Management extensions in FortiManager and FortiAnalyzer, FortiSOAR Trial License, and provisioning manual inputs from non-FortiSOAR users using links in emails. There have also been very significant architectural and UX changes that add wings to performance, security and usability of the product.

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

The recommended minimum screen resolution for the FortiSOAR GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

New features and enhancements

Feature	Details
Introduced the FortiSOAR Mobile Application	The FortiSOAR mobile application is an extension to the FortiSOAR's Web interface, which facilitates important and urgent actions such as immediate approvals, notifications, critical actions on the go, and viewing and reassigning records. **Note**: The FortiSOAR mobile application is part of the FortiExplorer application.
Introduced War Rooms	War rooms enable SOC teams to get into a collaborative space to mitigate a critical cyber threat scenario or campaign. FortiSOAR makes it easy for analysts to quickly provision a War Room and ensures that the task force is well-equipped to handle and coordinate all aspects of critical situations. FortiSOAR enables stakeholders to analyze and collaborate to quickly mitigate the threat.
Added ML-based clustering recommendation strategy to the 'Recommendation Engine'	The Recommendation engine adds the Machine-learning (ML) based clustering strategy as one of its recommendation strategies. The ML-based clustering strategy trains the ML engine using the data existing on your FortiSOAR instance to recommend similar records and predict and assign field values in records.
Introduced the "Connector Wizard"	You can create your own connector or edit an existing connector as per your requirements, using the "Connector Wizard" present in the FortiSOAR UI.
Added support for activating the FortiCare trial license for FortiSOAR	You get a free trial license for an unlimited time for FortiSOAR per FortiCare account, i.e., if you have a FortiCare account, you can get FortiSOAR for free and for an unlimited time, but in a limited context. This license is an "Enterprise" type license and is restricted to 3 users using FortiSOAR for a maximum of 200 actions a day.
Added SSO Auto Redirect Support	Prior to version 7.0.0, users required to click the **Use Single Sign On (SSO)** link to get redirected to the SSO login page or login using SSO active session. However, there are some organizations that have policies, which require direct redirection to the SSO login page, if SSO is configured. Therefore, in version 7.0.0 an **Auto Redirect** checkbox is added to the SSO Configuration page in FortiSOAR. Selecting the **Auto Redirect** checkbox, redirect users directly to the SSO login page or automatically logs the user into FortiSOAR in case the SSO session is active.
Added support for deploying the FortiSOAR license from the FortiSOAR UI	You can now choose to deploy your FortiSOAR license, in case of the initial deployment, or in case your FortiSOAR license has expired, from the FortiSOAR UI itself, without the need to SSH to your FortiSOAR machine. This is extremely useful if the administration does not have SSH access to the FortiSOAR machine.

Added support or Role-based Access Control for connector actions	Administrators can now permit only certain teams or users, based on roles, to perform certain connector actions. For example, the administrator might want to allow a "Block IP" action to be performed by only certain teams or users in the organization. The ownership of connector configurations can also be defined, by marking the connector configuration as 'Private'; thereby, controlling who can view and execute that particular connector configuration.
Added support for log collection using FortiSOAR UI	The FortiSOAR version dialog now displays a **Download Logs** link using which you can collect logs directly from UI. Prior to version 7.0.0, log collection was only possible using CLI commands. There could be some SOC environments where SSH access to systems are very restricted and required to go through various approvals. Therefore, in such cases, collecting logs for troubleshooting or for upgrade or installation operations would become a tedious task. To ease the process of log collection, you can directly collect logs from the FortiSOAR dialog and share them with support team for further troubleshooting.
Enabled FortiSOAR users to request decisions and inputs from non-FortiSOAR users via emails	FortiSOAR users can now request for decisions or inputs from non-FortiSOAR via emails. FortiSOAR users can use the decision-based or input-based prompts in the 'Manual Input' step in playbooks and specify the email addresses of the non-FortiSOAR users from whom they want to get decisions or inputs.
Mandated password change for the 'csadmin' users on first FortiSOAR login	The 'csadmin' user is now mandated to change their FortiSOAR *default password* during their first login. This enhances the security of your csadmin account and prevents unauthorized parties from accessing the administration account for FortiSOAR.
Enhancements made in the Collaboration Panel / Comments Widget	Following enhancements have been made in the Collaboration Panel / Comments Widget: • Introduced Message Threads or Nested Replies to help in keeping track of conversations and making it easier to respond to a specific thread. • Added support for adding mentions or tagging users in comments by typing `@`, and then selecting the users from the displayed list. • Added the ability to mark a comment as important. • Added the ability to filter comments based on tags, mentions, and the importance flag. • Option to open and expand the collaboration panel by default, on the first load of the selected module's record. Subsequent expansion/collapse is determined by the last state of the panel, maintained by each user. • Option for enabling and disabling the recommendation tab.
Added support for Undo and Redo buttons and shortcuts in the playbook designer	The toolbar in the playbook designer has been updated to include **Undo**/**Redo** buttons so that you can reverse changes made in a playbook or restore undone changes made in a playbook. This feature is very useful while building a playbook when there is a lot of trial and back and forth to be done.
Added support to bulk insert, upsert, or update records in batches	A '**Batch Size**' option has been added to the 'Bulk' execution type to support batching of large number of records, by default, in the Create/Update record steps. By default, the batch size is set to 100 records. This has made it easier to bulk insert, upsert, or update records, without the need of manually batching the record list manually and running the Create/Update record steps in a reference playbook step.

Added support for purging of executed playbook logs based on criteria other than day or date	Purge functionality for the executed playbook logs has been enhanced to support purging based on some complex query condition that involves multiple parameters and not just the date or days criteria. For example, clearing logs of ingestion playbooks that have completed their execution. Being able to clear logs based on these criteria is useful since ingestion playbooks are generally scheduled and they can occupy a major chunk of playbook history in the database. Therefore, this feature provides you with an option to build desired queries for purging executed playbook logs and scheduling purging of logs based on defined query.
Enhanced the Configuration Import and Export Wizards	Configuration Import and Export Wizards have been enhanced to support the import and export of templates, installed connectors, connector configurations, widgets, teams, and users.
Support for replicating files between the master and tenant nodes	File replication between the master and tenant nodes has been added. Therefore, records containing the "file" type fields or records with correlations that map to modules containing "file" type fields also get replicated. For example, now you can replicate 'Alert' records that contain 'Attachments' correlations. Now, you can also add attachments (files) to comments and those comments along with the associated files get replicated between the respective master and the tenant nodes.
Support for adding visibility conditions in Manual Triggers and Manual Inputs	You can now add visibility conditions to the fields that are displayed in the user input form, i.e., fields in the user form would be visible based on the conditions you specify. You can define visibility conditions in user prompts both when you trigger the playbook using the *Manual Trigger* option and also during the execution of the playbook using the *Manual Input* step (Input-based user prompt).
Added support for importing and exporting FortiSOAR configurations between systems using the CLI	You can now use the CLI, i.e., the '`csadm source-control`' command to import and export FortiSOAR configurations, such as, MMD and SVT updates along with playbooks and other required configuration changes between systems. This is required for Continuous Integration or Continuous delivery (CICD), which is a pipeline that automates of your software delivery process. The pipeline builds code, runs tests (CI), and safely deploys a new version of the application (CD).
Replaced Redis with RabbitMQ for communication within a cluster	As part of the technology stack simplification and performance improvement, FortiSOAR has replaced redis with rabbitmq for communication and message queuing within a cluster.
Introduced display of upgrade notifications on the FortiSOAR UI	From version 7.0.0 onwards, the FortiSOAR UI will display a notification when a new release (always the latest) is available. The notification also contains a link to that version's release notes so that you can get details about the latest available release. This keeps users informed about the latest releases and then users can make informed decisions about upgrading to the latest available version.
Enhancements made to Widgets	• The 'Relationships Single Line Card' widget has been enhanced to make it more intuitive and represent relationships in a user-friendly way. You can now link new records from the rendered widget, and also display more fields using this widget with greater control over the layout of the fields. • The 'Tabs' widget has been enhanced to enable you to add a description or sub title to the tabs that are marked as "primary". • A new widget named 'Featured Relationship' is added to the Primary Detail widget.

	This widget displays a single related record, which is usually utilized to show any active war room or other investigation. • Enhanced the "Row" structure widget to include a left-hand or right-hand side "Collapsible Sidebar". Using Collapsible Sidebars, you can expand or collapse the available sidebar space and optimize the available space.
Enhanced System Monitoring	System monitoring has been enhanced to include information about the processes that are consuming the most memory information in the email that is sent in the case of high CPU consumption. Earlier, the email would just say that the CPU consumption is high and has reached or breached the set threshold levels.
Enhanced Audit and System Logs	Enhanced the audit and system logs to include fields such as deviceid (devid), virtual domain name (vd), severity level of the event (level), etc. that provide information about your FortiSOAR system.
Added support for backup and restore of external SME data	Added support to backup and restore the data of your external Secure Message Exchange (SME) system using the `csadm db --backup [<backup_dir_path>]` and `csadm db --restore [<backup_file_path>` commands.
Added a new license type for FortiSOAR	A new license type named **Perpetual (Trial)** has been introduced for FortiSOAR, which will be displayed on both the FortiSOAR UI and on the CLI when you use the `csadm license --show-details` command. This type of license provides you with a free unlimited time license for FortiSOAR, but in a limited context, i.e., with restrictions on the number of users and actions that can be performed in FortiSOAR in a day. By default, this license is an "Enterprise" type license and is restricted to 3 users using FortiSOAR for a maximum of 200 actions a day.
Added new Widgets to the Widget Library	The following built-in widgets have been added in the 7.0.0 release: • **Task Management**: Use this widget to manage tasks and gain visibility into the current task board. • **Record Summary**: Use this widget to showcase the highlights or summary of a particular record. This widget houses multiple utility widgets within it that allow for customized uses. • **Access Control**: Use this widget to change or update the teams or users that have access to records.
Updated built-in connectors	The following built-in connectors have been updated in the 7.0.0 release: • Utilities connector updated to version 3.1.0 • IMAP connector updated to version 3.5.6 • SMTP connector updated to version 2.4.1 For more information on FortiSOAR Built-in connectors, see the "FortiSOAR™ Built-in connectors" article.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR version 7.0.0.

Secret Store Support Discontinued

FortiSOAR 7.0.0 has discontinued support for 'Secret Store'. The Secret Store was deprecated from version 5.0.0 onwards, but it was yet available from the FortiSOAR UI in the 6.x.x series. However, from 7.0.0 onwards you will not be able to use Secret Store and neither will it be available from the FortiSOAR UI.

Arrow Library Update

FortiSOAR 7.0.0 workflow engine has updated the arrow library due to which the `timestamp` attribute has been changed to `int_timestamp` for `DateTime` jinja expressions. For example, to get the current timestamp, use `{{arrow.utcnow().int_timestamp}}`.

For more information see, https://arrow.readthedocs.io/en/latest/releases.html#id4.

New playbooks must use the `int_timestamp` for any DateTime jinja expressions.

The workflow engine does a best effort handling of auto converting `.timestamp` to `.int_timestamp` before running playbooks on FortiSOAR version 7.0.0 and later, so not all playbooks will fail. However, some jinja expressions used might not match the regular expression causing such playbooks to fail; therefore, therefore you need to know which playbooks are impacted due to this change, so that you can update those playbook steps either before or after you upgrade your FortiSOAR instance. To know which playbooks have been playbooks have been impacted by this change in your FortiSOAR system, so that you can review and update those playbooks, see the Technical Note: How to know which playbooks are impacted due the Arrow Library update in FortiSOAR 7.0.0 which has changed the timestamp attribute article.

API Framework upgrade

FortiSOAR 7.0.0 has revamped its API layer for improved performance, security and adherence to latest api specifications. Due to this upgrade, you will observe the following behavior changes when you make API calls in FortiSOAR:

- The 'Pagination' response has changed as follows:
  - Sample old pagination spec keys that have been deprecated:
    `hydra:firstPage: "/api/query/alerts?%24limit=30"`

```
hydra:itemsPerPage: 30
hydra:lastPage: "/api/query/alerts?%24limit=30"
```

- New `hydra:view` key has pagination information, if the response has multiple pages:

```
"hydra:totalItems": 39,
    "hydra:view": {
     "@id": "/api/query/alerts?%24limit=30&%24page=1",
     "@type": "hydra:PartialCollectionView",
     "hydra:first": "/api/query/alerts?%24limit=30&%24page=1",
     "hydra:last": "/api/query/alerts?%24limit=30&%24page=2",
     "hydra:next": "/api/query/alerts?%24limit=30&%24page=2"
    }
```

- The '`Type`' agnostic API, i.e. `/api/3`, now displays 'failure' and 'success' per item. Earlier, a single flush was performed, i.e., used to display either complete failure or complete success.
- The '`Retry`' API for retrying failed configuration for agent and router has now been changed to simple '`PUT`' requests with change values of the configuration status.
- The support for getting the count of related records by passing the `$relationshipCount` flag (`api/3/<module>/uuid/<associateModule>?Countonly=true`) on only queries has been removed. Now, to get relationships count, FortiSOAR has provided alternate route of aggregation support on `/api/query/module`, which is much faster. Similar update has been made for getting the count of workflows from the workflow collection.
- The bulk API response has been changed to 'success' or 'failure', compared to earlier releases where multistage single, failed, and bad requests were passed.

Integrations API call changes

The Integrations API call has been changed in version 7.0.0 to support only `POST` calls; earlier `GET` calls were also supported. Therefore, if you have any existing playbooks that uses the GET calls, then that playbook will fail. To resolve this issue, you have to manually change the method from `GET` to `POST` in your playbooks.

Change in the behavior of linking relationships

The behavior of linking records relationships has changed in version 7.0.0 for some performance enhancements. Now, the maximum number of records that can be linked to a record, for example, indicators linked to an alert has been **capped at 99 for a single request**.

Requirement to install SCP if you want to move files from or to FortiSOAR systems

If you want to move any file from and to a FortiSOAR system, then you must install SCP (`yum install openssh-clients -y`) or any SCP client. This is required since the `openssh-clients` package has been removed from FortiSOAR for security compliance.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to version 7.0.0 from versions 6.4.3 or 6.4.4 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 login to the FortiSOAR Platform during the upgrade.

For details about upgrading FortiSOAR, see the *FortiSOAR Upgrade Guide*.

Product integration and support

Web browsers

FortiSOAR 7.0.0 User Interface has been tested on the following browsers:

- Chrome version 89.0.4389.114
- Firefox version 87.0
- Internet Explorer Edge version 89.0.774.68

Virtualization

This section lists FortiSOAR version 7.0.0 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- VMware ESXi versions 5.5, 6.0, and 6.5
- Linux KVM Redhat 7.1

Resolved issues

Following is a list of some of the important defects addressed in **FortiSOAR release 7.0.0**:

- **Bug #0629191**: When you would create dashboards where its inputs were configured of type 'lookup', then the generated dashboard would print the IRI value instead of the real value. For example, the IRI of the user instead of the name of the user. Now, the generated dashboards prints the actual value.
- **Bug #0691158**: `/var/log/messages` is fixed to collect rotating logs. Earlier, `/var/log/messages` was not collecting rotating logs. which hampered the working of the `csadm log --collect` command.
- **Bug #0692771**: Fixed the issue with that reports generated using the Report Engine were unable to render eastern and fast east languages such as Korean, in the PDF format.
- **Bug #0693146**: Added a FortiSOAR device serial number for outgoing syslog message, enabling the SIEM to write a parser for easily identifying the FortiSOAR logs.
- **Bug #0693265**: Fixed an issue with visibility in the team hierarchy that caused the parent team to view the records of only some of its children teams. Now, the parent team can view all its child records.
- **Bug #0694300**: Details of which processes are consuming swap space was not included in HA monitoring. Now, CPU and RAM consuming processes, swap space consuming processes, and also details of which processes are consuming swap space was not included in HA monitoring and these details are sent in the HA notification email.
- **Bug #0694553**: The `createDate` field was not indexed causing searches to slow down the system. Now, the `createDate` field has been indexed, which should improve the performance of searches.
- **Bug #0694964**: Fixed the issue that tomcat logs were not collected using the `csadm log --collect` command. Now, the `csadm log --collect` command collects tomcat logs from the `/opt/cyops-tomcat/logs/` path.
- **Bug #0695784**: Fixed the issue of not finding any records when a global search is performed in the Korean language, especially if the search string contained a space.
- **Bug #0698302**: Fixed the issue of uncontrolled resource consumption for rich text fields. Now, a minimum (0) and maximum (10485761) character limit has been applied to rich text fields, which should fix this issue.
- **Bug #0700993**: Fixed the issue in the connector configuration that caused the complete password not to be sent, if the password started with a number followed by #. In this case, the connector used to consider # as a comment and it would not send the complete password, leading to multiple login failure attempts and locking of the user account.
- **Bug #0701352**: Fixed the issue that caused FortiSOAR to keep crashing infinitely, if a message containing invalid JSON was received.
- **Bug #0702512**: Made changes to the framework and changed the behavior of linking records relationships so that if there is a record that is linked to thousands of other records, an update to such records does not cause constant high CPU usage. Now, the maximum number of records that can be linked to a record, for example, indicators linked to an alert has been **capped at 99 for a single request**.

Known Issues and Workarounds

- **Issue #0678796**: If the version of your Report Engine connector is prior to 1.0.2, the "Export Report" system playbook (Settings > System Fixtures > Report Management Playbooks) did not have the timezone parameter, so if after upgrading the Report Engine to the latest version (1.2.0), even then the report does not get exported based on the selected timezone.
  To resolve this issue, and export the report based on the selected timezone, do the following:
  a. Navigate to **Settings** > **System Fixtures** > **Report Management Playbooks**.
  b. Open the **Export Report** Playbook.
  c. Open the **Generate Report from Report ID** step from which copy the values of the **Report ID** and **Report Params** fields.
  d. Delete the **Generate Report from Report ID** step.
  e. Add a "Connector" step and select the **Report Engine v1.2.0** connector.
  f. Select the **Generate Report From Report ID** action.
  g. Paste the values of the Report ID and Report Params fields that you had copied in step 3.
  h. Save the playbook and export the report as PDF.
  Now, the report gets exported based on the selected timezone.
- **Issue #0679697**: The `csadm db --externalize` command fails with a "Failed to drop database `<name of database>`" error in case the FortiSOAR database is present on an external PostgreSQL server.
  This issue occurs if there is a stale connection present to the FortiSOAR database on the external PostgreSQL server. To resolve this issue and release all stale connections, restart the Postgres service using the following command:
  `systemctl start postgresql-<postgresql version>`
  For example, `systemctl start postgresql-12`
- **Issue #0679759**: When you stop a schedule the value, i.e., the DateTime of the Last Run At field becomes blank.
  This issue will be resolved in future releases of FortiSOAR.
- **Issue #0679776**: If you select both the Row Expandable and Enable Horizontal Scrolling in the grid view template and if in the grid view of the module you expand a record, then, in this case, the UI of the records following the expanded row might get scattered.
  This issue will be resolved in future releases of FortiSOAR.
- **Issue #0679841**: You must ensure that the relations that you are adding while configuring co-relationships between modules are correct. FortiSOAR does not prevent the creation of incorrect relationships between modules. Therefore, you must ensure that you add correct bidirectional relationships for both the modules for which you want to define the relationship. For example, if you define a Many to One relationship on the Alerts module for the Events Module, then in the Events module you must define a "One to Many" relationship for the Alerts module.

www.fortinet.com