



# ADMINISTRATION GUIDE

RELEASE 6.4.4

DECEMBER 2020

## Copyright

EXCEPT WHERE EXPRESSLY STATED OTHERWISE, NO USE SHOULD BE MADE OF MATERIALS ON THIS SITE, THE DOCUMENTATION, SOFTWARE, HOSTED SERVICE, OR HARDWARE PROVIDED BY FORTINET. ALL CONTENT ON THIS SITE, THE DOCUMENTATION, HOSTED SERVICE, AND THE PRODUCT PROVIDED BY FORTINET INCLUDING THE SELECTION, ARRANGEMENT AND DESIGN OF THE CONTENT IS OWNED EITHER BY FORTINET OR ITS LICENSORS AND IS PROTECTED BY COPYRIGHT AND OTHER INTELLECTUAL PROPERTY LAWS INCLUDING THE SUI GENERIS RIGHTS RELATING TO THE PROTECTION OF INTELLECTUAL PROPERTY. YOU MAY NOT MODIFY, COPY, REPRODUCE, REPUBLISH, UPLOAD, POST, TRANSMIT OR DISTRIBUTE IN ANY WAY, ANY CONTENT, IN WHOLE OR IN PART, INCLUDING ANY CODE AND SOFTWARE UNLESS EXPRESSLY AUTHORIZED IN WRITING BY FORTINET. UNAUTHORIZED REPRODUCTION, TRANSMISSION, DISSEMINATION, STORAGE, AND OR USE WITHOUT THE EXPRESS WRITTEN CONSENT OF FORTINET CAN BE A CRIMINAL, AS WELL AS A CIVIL OFFENSE UNDER THE APPLICABLE LAW.

© 2008-2020, Fortinet, Inc. All Rights Reserved.

## Trademark

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Fortinet are the registered or unregistered Marks of Fortinet, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Fortinet or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Fortinet or the applicable third party. Fortinet is a registered trademark of Fortinet Inc.

# Table of Contents

Introduction .....	12
Common Tasks.....	12
Tasks and Permissions .....	12
System Configuration.....	14
Application Configuration.....	15
Configuring Notifications .....	15
Configuring System and Cluster Health Monitoring .....	16
Configuring Comments.....	18
Scheduling purging of audit logs and executed playbook logs .....	19
Configuring Playbook Recovery .....	21
Configuring the default timezone for exporting reports .....	21
Configuring Themes .....	22
Configuring Default Country Code .....	22
Configuring Navigation Preferences .....	22
Log Forwarding .....	22
Persisting the FortiSOAR™ logs .....	24
Environment Variables .....	25
Branding.....	26
System Fixtures.....	29
Audit Log.....	32
Viewing Audit Log.....	34
Viewing User-Specific Audit Logs .....	37

Viewing Audit Log in the detailed view of a record .....	38
Purging Audit Logs.....	41
License Manager.....	45
Segmented Network support in FortiSOAR™ .....	47
Overview.....	47
Architecture.....	48
Recommended Resource Requirements for Virtual Machines (VM) .....	48
Recommended specifications for Secure Message Exchange .....	48
Recommended specifications for agents .....	48
Prerequisites for installing an agent.....	48
Process of setting up a FortiSOAR agent .....	49
Minimal permissions required .....	50
Enabling the secure message exchange.....	50
Adding a Secure Message Exchange .....	50
Adding an agent .....	52
Installing an agent .....	55
Upgrading an agent.....	55
FortiSOAR™ Agent CLI .....	58
Deboarding Agents.....	58
Moving an agent to a new secure message exchange.....	59
Invoke connector actions using agents in segmented networks .....	59
Installing a connector on an agent.....	59
Configuring connectors .....	61
Running remote actions .....	62



Troubleshooting.....	67
Files to be used for troubleshooting.....	67
Deactivated agent does not come back to the connected state even after activating the agent.....	67
Agents configuration page displays a "Agent <Agent UUID> does not exist" error when you click the Export Config link.....	67
Security Management.....	68
Important Concepts.....	68
Authentication versus Authorization .....	68
Users and Appliances .....	69
Teams and Roles.....	69
Security Management Menus .....	70
Team Hierarchy .....	70
Teams .....	70
Roles .....	70
Users.....	70
Appliances .....	71
Authentication.....	71
Password Vault.....	71
Configuring Team Hierarchy.....	71
Relationships .....	72
Using the Editor.....	73
Configuring Teams.....	77
Editing Teams .....	77

Configuring Roles .....	79
Default Roles .....	80
Modules in the Role Editor .....	83
Adding Roles .....	84
Assigning Roles to Users and Appliances .....	84
Configuring User and Appliance Profiles .....	85
Adding Users .....	85
User Profiles .....	86
Appliances .....	90
Configuring Authentication .....	94
Configuring Accounts .....	94
Configuring LDAP / AD .....	96
Configuring SSO .....	98
Configuring the Password Vault Manager .....	99
Configuring the Secrets Store (Deprecated) .....	103
Adding a secret .....	105
Delete Users .....	107
SAML Configuration .....	109
Introduction .....	109
Benefits of SAML .....	110
SAML Principles .....	110
Prerequisites to configuring SAML .....	111
Configuring SAML in FortiSOAR™ .....	111
Configuring SAML in FortiAuthenticator .....	116

Configuring SAML in OneLogin .....	119
Configuring SAML in Auth0 .....	123
Configuring SAML in Okta .....	125
Configuring SAML in Google.....	133
Configuring SAML in ADFS.....	137
Support for mapping roles and teams of SSO users in FortiSOAR™ .....	145
Troubleshooting SAML issues.....	150
Unable to login to FortiSOAR™ when ADFS SAML is configured .....	150
Application Editor .....	152
Module Editor .....	152
Modifying an existing module.....	154
Adding a related module to the related records for a module.....	168
Creating a New Module .....	171
Saving your changes .....	172
Viewing your changes .....	172
Publishing modules .....	173
Picklist Editor .....	173
Creating or modifying a picklist.....	174
Navigation Editor .....	176
Modifying the Navigation bar .....	177
Correlation Settings .....	179
Configuration Export and Import .....	182
Permissions required.....	182
Configuration Export Wizard.....	183

Configuration Import Wizard .....	189
SLA Management .....	198
Overview .....	198
Permissions required for managing SLAs .....	198
Creating SLA Templates .....	198
Viewing SLAs .....	200
FortiSOAR™ Admin CLI .....	202
Overview .....	202
Prerequisites .....	202
FortiSOAR™ Admin CLI - Usage .....	202
CLI commands used for forwarding syslogs .....	207
High Availability support in FortiSOAR™ .....	209
Overview .....	209
High Availability Types supported with FortiSOAR™ .....	209
High Availability with an internal PostgreSQL database .....	210
High Availability with an externalized PostgreSQL database .....	212
Cluster Licensing .....	213
Viewing and updating the license of an HA cluster .....	214
Prerequisites to configuring High Availability .....	214
Process for configuring High Availability .....	215
Steps to configure FortiSOAR™ HA cluster with an internal PostgreSQL database .....	215
Steps to configure FortiSOAR™ HA cluster with an external PostgreSQL database .....	216
Takeover .....	216
Usage of the csadm ha command .....	217

Overview of nodes in a FortiSOAR™ HA cluster .....	219
Checking replication between nodes in an active-passive configuration .....	220
Upgrading an HA cluster .....	220
Load Balancer .....	220
Setting up HAProxy as a TCP load balancer fronting the two clustered nodes .....	220
Behavior that might be observed while publishing modules when you are accessing HA clusters using a load balancer .....	221
Tunables.....	221
Best Practices.....	222
Monitoring health of HA clusters .....	223
Understanding HA Cluster Health Notifications .....	223
Troubleshooting issues based on the notifications .....	226
Sample scale test that were done in the lab to understand the behavior of 'csadm ha get- replication-stat' .....	228
Troubleshooting.....	236
Failure to create an HA cluster.....	236
Unable to add a node to an HA cluster using join-cluster, and the node gets stuck at a service restart.....	237
Fixing the HA cluster when the Primary node of that cluster is halted and then resumed	237
Unable to join a node to an HA cluster when a proxy is enabled.....	238
Changes made in nodes in an active-active cluster fronted with a load balancer take some time to reflect.....	238
Post Takeover the nodes in an HA cluster do not point to the new active primary node ..	239
Elasticsearch Configuration .....	240
Introduction .....	240

Externalization and Authentication of Elasticsearch .....	240
Migration of Elasticsearch data .....	241
Troubleshooting.....	241
FortiSOAR™ Search Errors .....	241
Externalization of your FortiSOAR™ PostgreSQL database .....	243
Prerequisites .....	243
Externalizing FortiSOAR™ databases .....	244
Setting up an externalized database on the cloud .....	245
Troubleshooting DB Externalization issues .....	246
Unable to log onto FortiSOAR™ if the IP of the externalized PostgreSQL database changes .....	246
Backing up and Restoring FortiSOAR™ .....	247
Prerequisites .....	247
Backup Process .....	247
Data that is backed up during the backup process .....	247
Prerequisites to running the backup process .....	248
Performing a backup .....	248
Restore process .....	249
Restoring data .....	249
Backup and Restore process for FortiSOAR™ High Availability systems .....	250
About FortiSOAR™ .....	251
Monitoring FortiSOAR™ .....	253
Overview .....	253
Benefits of monitoring .....	253

Setting up monitoring.....	254
Monitoring uptime of FortiSOAR™ .....	254
Monitoring FortiSOAR™ services.....	254
Monitoring databases .....	255
Monitoring Disk Space Utilization .....	255
Monitoring CPU and Memory Utilization .....	256
Monitoring connectors .....	256
Monitoring workflows .....	256
Debugging, Troubleshooting, and optimizing FortiSOAR™ .....	258
Overview .....	258
List of logs used for troubleshooting FortiSOAR™ .....	258
List of key FortiSOAR™ services and processes .....	262
Additional settings for record similarity and field predictions.....	263
Troubleshooting Tips .....	264
Your Workflow data size has increased .....	264
Change the default value of some of the user profile parameters .....	264
Error displayed while performing a search operation in FortiSOAR™ .....	266
Reindexing FortiSOAR™ modules for search.....	267
FortiSOAR™ crashing with "out of memory" errors.....	267
Changing Postgres worker memory .....	267
Issues while accessing FortiSOAR™ UI while using Chrome on MacOS Catalina .....	268


## Introduction

Use the administration guide to understand how to customize and administer FortiSOAR™, including system, security and user management, and configuring templates.

## Common Tasks

Some of the common task that an administrator can perform are:

- License management
- System configuration
- Security management
- User management
- Appliance management
- Password Vault management
- Playbook configuration
- Application management

You can perform administration tasks using the **Settings** () icon in the upper right-hand corner near the **User Profile** icon.

## Tasks and Permissions

To manage different modules, appropriate rights must be assigned to users. In FortiSOAR™, modules are applied to roles, for example, the **Security** module is applied to the **Security Administrator** role. Role permissions are based on the Create, Read, Update, and Delete model (CRUD). Each module within FortiSOAR™ has explicit CRUD permissions that you can modify and save within a single Role.

For example, to perform all tasks for system configuration, you must be assigned a role that has **CRUD** permissions on the **Application** module, or to be able to add and manage users, you must be assigned a role that at the minimum has **Create** and **Update** permissions on the **People** module.

By default, FortiSOAR™ has at least one role in place after installation, the **Security Administrator**.

### Task

System configuration: Customizing FortiSOAR™ and configure several default options used throughout the system, including setting up

### Permissions required on the module

Create, Read, Update, and Delete (CRUD) permissions on **Application** module. Default Role - Application Administrator.



authentication mechanisms and configuring dashboards and templates.

Security management: Managing teams and roles.

User management: Adding and removing users and editing their permissions.

Appliances management: Configuring data models, including picklist values and system navigation.

Password Vault management: Integrating with third-party external vaults to manage sensitive data.

Playbook management: Configuring playbook collections and playbooks

CRUD permissions on **Security** module. Default Role - Security Administrator. The security administrator role also has CRUD permissions on the **Secure Message Exchange** and **Tenants** modules, so that this role can configure multi-tenant systems.

CRUD permissions on **People** module.

CRUD permissions on **Appliances** module.

CRUD permissions on **Connectors** module and Read permission on **Application** module.

CRUD permissions on **Playbook** module. Default Role - Playbook Administrator.

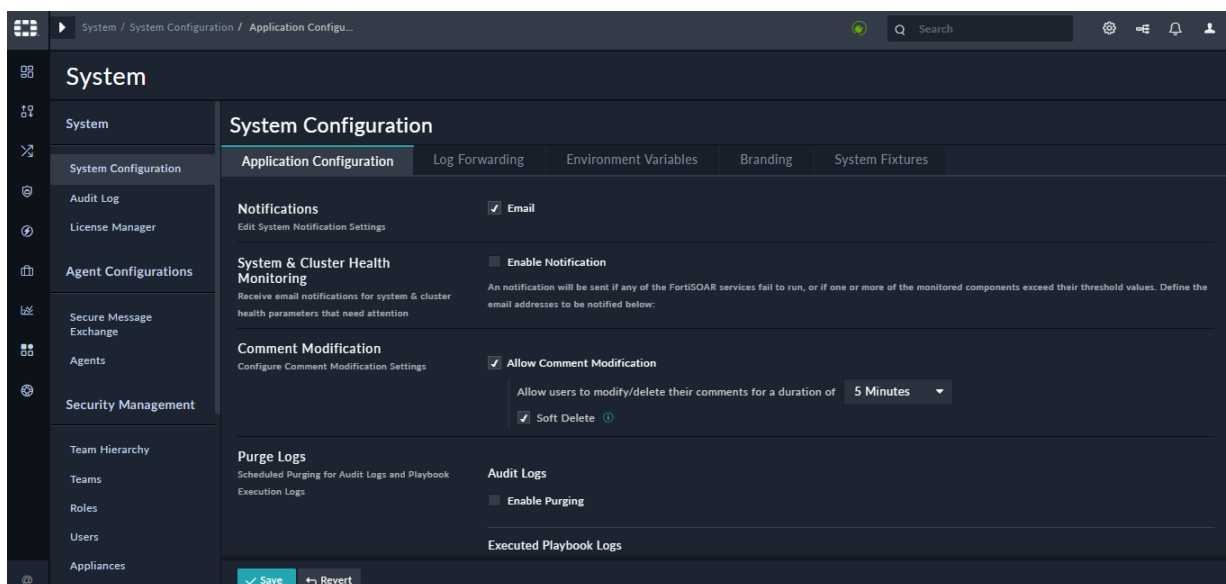
## System Configuration

You can customize FortiSOAR™ and configure several default options used throughout the system, including the way FortiSOAR™ gets displayed to the users and the way notifications are sent to the users. To configure the system, you must be assigned CRUD permissions to the **Application** module. The Application module is assigned by default to the **Application Administrator** role. For information about roles, refer to the *Default Roles* section in the “Security Management” chapter.

Click the **Settings** (⚙️) icon to open the **System** (System Configuration) page. Use the **Application Configuration** tab on the System Configuration page to edit several default options found throughout the system, especially in the user profile. These include the following:

- Default notifications mechanism
- Default notifications for system and HA cluster health monitoring
- Default Comment Modification
- Default Playbook Recovery options
- Default timezone for exporting reports
- Default theme
- Schedule purging of audit logs and executed playbook logs
- Default country code
- Default navigation bar style

For more information on user profile configuration, refer to the *User Profiles* section in the “Security Management” chapter.



**Figure 1.** System Configuration Menu - Application Configuration tab

**Tip:** You can modify all the default values on a per-user basis on any user's Profile page.

To enable sending system notifications, including requests for resetting passwords, and also for sending emails outside FortiSOAR™ you must configure the SMTP connector. For more information on FortiSOAR™ Built-in connectors, including the SMTP connector, see the "[FortiSOAR™ Built-in connectors](#)" article.

Click **Settings > Audit Log** to open the Audit Log page. Use the Audit Log page to view a chronological record of all actions across FortiSOAR™. For more information, see [Audit Log](#).

Click **Settings > License Manager** to open the License Manager page. Use the License Manager page to update your license and view the details of your FortiSOAR™ license. For more information, see [License Manager](#).

Use the **Environment Variables** tab on the System Configuration page to add proxies to serve HTTP, HTTPS, or other protocol requests from FortiSOAR™ or define environment variables. For the procedure for configuring proxy settings and defining environment variables is included in the *Configuring Proxy Settings and environment variables* topic in the *Additional configuration settings for FortiSOAR™* chapter of the "Deployment Guide."

Use the **Branding** tab on the System Configuration page to customize FortiSOAR™ branding based on your license type. For more information, see [Branding](#).

Use the **System Fixtures** tab on the System Configuration page to view the links to various playbook collections and templates, which are included by default with FortiSOAR™. For more information, see [System Fixtures](#).

## Application Configuration

On the Application Configuration page, you can configure settings that will apply across FortiSOAR™. You can edit the settings and then click **Save** to apply the changes or click **Revert** to revert your changes.

### Configuring Notifications

Currently, FortiSOAR™ supports only email as a notification mechanism.

FortiSOAR™ sends notifications to users for updates to tasks or activities. Non-admin users can change their notification setting by editing their user profile to either enable or disable email notifications. Changes made by a non-admin user to the notification settings are applicable only to those users who have not changed their default user profile settings.

**Important:** You must configure your SMTP connector before you can configure notifications and to complete the process of adding new users. If you do not configure the SMTP connector, users are created. However, the password reset notification link cannot be sent to the users. For more information on FortiSOAR™ Built-in connectors, including the SMTP connector, see the "[FortiSOAR™ Built-in connectors](#)" article.

In the future, in-app notifications and SMS notifications will enable additional notification mechanisms.

**Note:** SMS messages and other notification means can be integrated using Playbooks. Some mechanisms, such as Everbridge, are already built with some defaults in place.

## Configuring System and Cluster Health Monitoring

From version 6.4.3 onwards, you can set up system monitoring for FortiSOAR™, both in case of a single node system and High Availability (HA) clusters. To receive email notifications of any FortiSOAR™ service failure, or of any monitored thresholds exceeding the set threshold, etc., click the **Enable Notification** checkbox in the **System & Cluster Health Monitoring** section.

**Figure 2.** Application Configuration Page - System & Cluster Health Monitoring section for a single node

Once you click the **Enable Notification** checkbox, from the **Service** drop-down list, select the service to be used for notifications. You can choose between **SMTP** or **Exchange**. In the Email field, specify the email address that will be notified in case of any service failures, threshold breaches, etc.

In the **Monitoring Interval (Minutes)** field specify the interval in minutes at which you want to monitor the system and perform the health check of the HA cluster. By default, the system is monitored every 5 minutes.

In the **System Health Thresholds** section, you can set the thresholds, in percentages, for Memory Utilization (80% default), CPU Utilization (80% default), Disk Utilization (80% default), and Swap Memory Utilization (50% default). If the thresholds set are reached or crossed for any of the monitored parameters, an email notification is sent to the specified email addresses.

If you have an HA environment, then in addition to the above settings, you can also monitor and get notified in case of heartbeat failures and high replication lags between nodes of your HA cluster. You can specify values for these parameter in the **Cluster Health** section:

**Figure 3.** *Application Configuration Page - System & Cluster Health Monitoring section for an HA cluster*

In the **Missed Heartbeat Count** field, specify the count of missed heartbeats after which notifications of failure will be sent to the email addresses you have specified.

**Note:** You cannot specify a value lesser than 3 in the Missed Heartbeat Count field.

In the **Replication Lag** field, specify the threshold, in percentage, for the replication lag between nodes. By default, this is set to **60%**. This 60% is relative of the total max lag of 5 GB (wal\_segment\_count, 320 in postgresql.conf). If the replication lag threshold is reached or crossed, then an email notification is sent to the specified email addresses.

Some examples of how Monitoring Interval (Minutes) and Missed Heartbeat Count values help you in monitoring heartbeats between nodes in an HA cluster:

## Case 1

If you have set the Monitoring Interval to 5 minutes and the Missed Heartbeat Count to 3, this means that when the heartbeat is missed (the `cyops-ha` service is down) for the last  $\geq 15$  minutes (monitoring interval \* missed heartbeat count), the heartbeat missed notification will be sent to the email address that you have specified in the **Email** field.

The cluster health check is performed based on the monitoring interval specified. For example, if you specify 3 minutes in the **Monitoring Interval (Minutes)** field, then the HA cluster health check will be run every 3 minutes.

Notifications get sent based on the multiplication of the values that you have set in the monitoring interval and missed heartbeat count. For example, if you have set monitoring interval to 3 and missed heartbeat count to 4, and if the heartbeat is missed for the last  $\geq 12$  minutes, then heartbeat missed notifications will be sent to the email address that you have specified in the **Email** field.

## Case 2

If you have no heartbeats missed for the last  $\geq 15$  minutes, considering monitoring interval set to 5 minutes and missed heartbeat count set to 3; however, there is a service down or a service connectivity failure found in the health check, then a notification for service down or service connectivity failure will be sent to the email address that you have specified in the **Email** field.

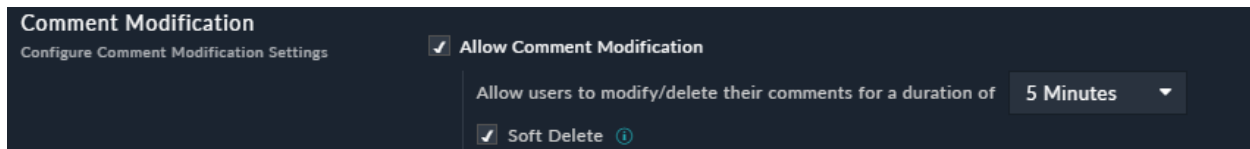
For more information on HA, see the *High Availability support in FortiSOAR™* chapter.

## Configuring Comments

A user who has **Security Update** permissions can edit comments of any FortiSOAR™ user, and a user who has **Security Delete** permissions can delete comments of any FortiSOAR™ user. There is no time limit for the Security user to update or delete comments.

Users can edit and delete their own comments in the "Collaboration" window or in the Comments widget, if you (the administrator) has enabled the settings for comment modification and if the user has appropriate CRUD permissions on the **Comments** module.

To allow users to edit and delete their own comments, click the **Settings** icon, which opens the **System Configuration** page. On the **Application Configuration** tab, in the **Comment Modification** section, select the **Allow Comment Modification** checkbox.



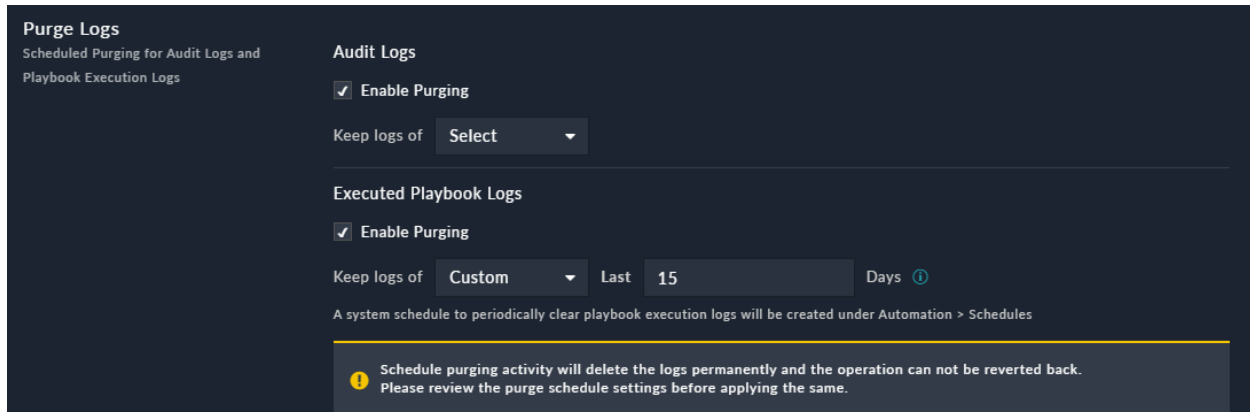
**Figure 4.** *Comments Modification section*

You can also specify the time until when the user can edit or delete their comments in the **Allow users to modify /delete their comments for a duration of** field. For example, if you select 1 minute from this field, then users can edit and delete their comments until 1 minute after which they have added the comment. By default, the **Allow users to modify/delete their comments for a duration of** field is set to 5 minutes. Users cannot edit or delete their comments after the time specified in the **Allow users to modify/delete their comments for a duration of** field.

From version 6.4.1 onwards, you can specify the behavior of the comment "delete" action, i.e., when a user deletes a comment, you can choose to permanently delete the comment or flag the comment for deletion, i.e., **Soft Delete**. If you choose to keep the **Soft Delete** checkbox checked (default), then the comments will be soft deleted, i.e., on the UI you will see **--Comment Deleted--** instead of the comment. In case you have cleared the **Soft Delete** checkbox, you will not see anything on the UI since the comment has been permanently deleted.

## Scheduling purging of audit logs and executed playbook logs

You can schedule purging, on a global level, for both audit logs and executed playbook logs. Click the **Settings** icon, which opens the System Configuration page. In the **Purge Logs** section, you can define the schedule for purging both Audit Logs and Executed Playbook Logs. By default, audit logs and not purged and executed playbooks logs are purged.



**Figure 1.** *Purge Logs Section*

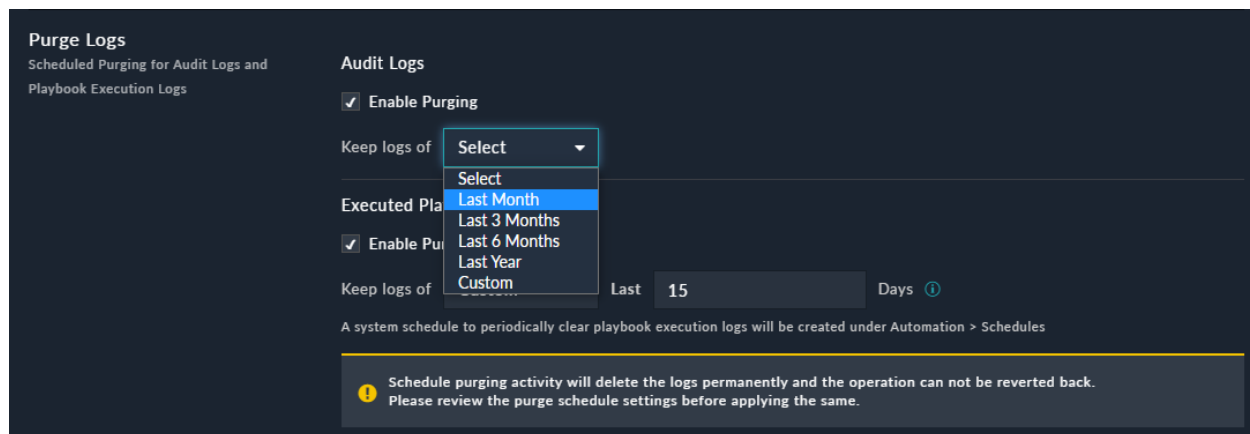
**Warning:** The schedule purging activity deletes logs permanently, and you cannot revert this operation.

## Scheduling purging of audit logs

To purge **Audit Logs**, you must be assigned a role that has a minimum of **Read** permission on the **Security** module, **Read** permission on the **Application** module, and **Delete** permissions on the **Audit Log** module.

To enable purging of Audit logs, you require to select the **Enable Purging** checkbox that appears in the **Audit Logs** section.

Once you select the **Enable Purging** checkbox, you require to define the schedule for purging of audit logs. To specify the time for which you want to retain the logs, you must select the appropriate option from the **Keep logs of** drop-down list. You can choose from the following options: **Last month**, **Last 3 months**, **Last 6 months**, **Last year**, or **Custom** as shown in the following image:



**Figure 2.** *Purge Logs - Specifying time to retain audit logs*

If you choose **Custom**, then you must specify the *number of days* for which you want to retain the logs.

**Note:** For purging purposes, 1 month is considered as 30 days and 1 year is considered as 365 days.

Schedule purging clears all logs that belong to a timeframe earlier than what you have specified.

For example, if you want to retain audit logs for a month, then select **Last month** from the **Keep logs of** drop-down list. Once you save this setting all audit logs that are older than 1 month (30 days) will be cleared, and this will be an ongoing process, as the audit log records will all be time-stamped and the ones older than 30 days will be purged.

**Note:** By default, the purge schedule job runs every midnight (UTC time) and clears all logs that have exceeded the time duration that you have specified. If you want to run the purging activity at a different time of the day or for a different duration, you can do so by editing the schedule of purging on the **Schedules** (**Automation** > **Schedules**) page once you enable purging of the logs.

## Scheduling purging of executed playbook logs

To purge **Executed Playbook Logs**, you must be assigned a role that has a minimum of **Read** permission on the **Security** module and **Delete** permissions on the **Playbooks** module.

From version 6.4.3 onwards, the Executed Playbook Logs are purged by default, and therefore the **Enable Purging** checkbox is already selected in the Executed Playbook Logs section. By default, any executed playbook logs that are older than 15 days are purged. You can change time for which you want to retain the playbook execution logs by selecting the appropriate option from the **Keep logs of** drop-down list, as is the case with audit logs.



A system schedule, named "Purge Executed Playbook Logs" is also already created and active on the **Schedules** page. This schedule runs every midnight (UTC time) and clears all logs that have exceeded the time duration that is specified. If you want to run the purging activity at a different time of the day or for a different duration, you can do so by editing this schedule.

## Configuring Playbook Recovery

Use the autosave feature in playbooks to recover playbook drafts in cases where you accidentally close your browser or face any issues while working on a playbook.

In the **Playbook Recovery** section, you can define the following:

- If you do not want FortiSOAR™ to save playbook drafts, clear the **Enable Playbook Recovery** option. By default, this option is checked.
- In the **Save Drafts Every** field, enter the time, in seconds, after which FortiSOAR™ will save playbook drafts. By default, FortiSOAR™ saves playbook drafts **15** seconds after the last change.  
The minimum time that you can set for saving playbook drafts is **5** seconds after the last change.

## Configuring the default timezone for exporting reports

You can define a timezone that will be used by default for exporting reports. This timezone will be applied by default to all reports that you export from the Reports page. To apply the default timezone, click the **Enable Timezone Selection** option in the **Report Export** section. Then from the **Timezone** drop-down list, search for and select the timezone in which you want to export the report. For example, if you want to search for the timezone of Los Angeles, you can type **los** in the search box below the Timezone field to find the correct timezone, as shown in the following image:

**Figure 3.** Selecting the default Timezone for exporting reports

## Configuring Themes

You can configure the FortiSOAR™ theme that will apply to all the users in the system.

Non-admin users can change the theme by editing their user profile. Changes made by a non-admin user to the theme are applicable only to those users who have not changed their default user profile settings.

There are currently three theme options, **Dark**, **Light**, and **Space**, with **Space** being the default. On the **Application Configuration** page, select the theme that you want to apply across FortiSOAR™. Click **Preview Theme** to view how the theme would look and click **Save** to apply the theme.

To revert the theme to the default, click **Revert Theme**.

## Configuring Default Country Code

You can configure country code format for contact numbers that will apply to all users in the system. In the **Phone Number** section, select the **Default Country** and thereby the default country code that you want to apply across FortiSOAR™ and click **Save** to apply the code.

## Configuring Navigation Preferences

You can configure the behavior of the left navigation bar across FortiSOAR™. You can choose whether you want the left navigation bar to collapse to just display icons of the modules or expand to display both icons and titles of modules. In the **Navigation Preferences** section, click **Collapse Navigation** to collapse the left navigation bar and click **Save** to apply the behavior of the left navigation bar across the system.

## Log Forwarding

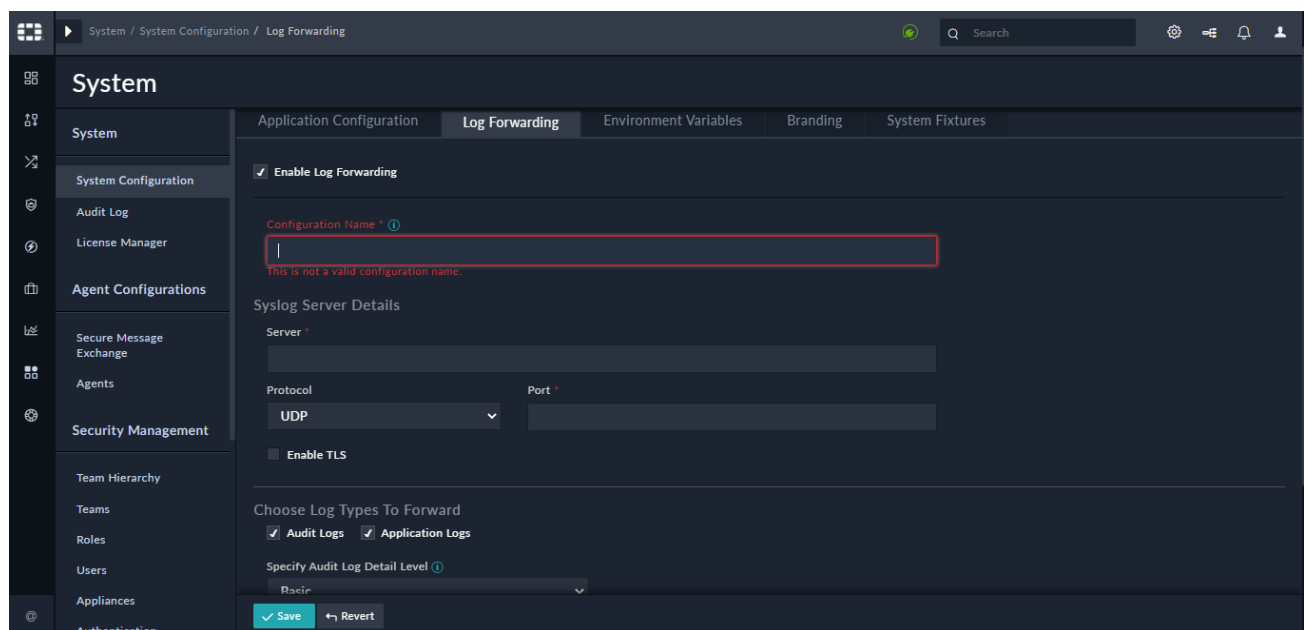
Many organizations use an external log management server to manage logs and maintain all logs at a single place, making analysis efficient. From version 6.4.3 onwards, FortiSOAR™ application logs and audit logs can be forwarded to your central log management server that supports a Rsyslog client, using both the FortiSOAR™ UI and the **csadm** CLI. You can also select the category of the logs you want to forward to the external log management server. For information about configuring syslog forwarding using the CLI, see the *FortiSOAR™ Admin CLI* chapter.

**Important:** If you have a FortiSOAR™ HA setup, then note that Syslog settings are not replicated to the passive node. If you want to forward logs from the passive node, you must enable it manually using the **csadm log forward** command.

You could also send FortiSOAR™ logs to a SIEM, since all SIEMs support syslog ingestion, which would achieve the following:

- Improve High Availability (HA) troubleshooting since now you can use consolidated logs instead of having to go individual nodes to debug HA issues.
  - Ability to forward FortiSOAR™ logs to your SIEM, if you have a policy of setting up log forwarding to SIEM for all your production devices.
- Once the logs are in the a SIEM, you can further configure rules for raising alerts for specific failure, making system monitoring more effective.

Click **Settings > System Configuration** and then click the **Log Forwarding** tab to open the Log Forwarding page. Use the Log Forwarding page to setup, modify, and enable or disable your syslog forwarding of FortiSOAR™ logs to your central syslog server. To enable syslog forwarding, click the **Enable Log Forwarding** check box.



**Figure 4.** System Configuration Menu – Log Forwarding page

Once you select the **Enable Log Forwarding**, you require to fill in the details of the syslog server to which you want to forward the FortiSOAR™ logs, the type of logs to forward, etc.

**Note:** You can configure only a single syslog server.

1. In the **Configuration Name** field, add the name of the configuration in which you want to store the log forwarding configuration details.  
**Note:** The name that you specify must not have any special characters, underscores, or spaces.
2. In the **Syslog Server Details** section, enter the following details:
  - a. In the **Server** field enter the DNS name or IP address of the syslog server to which you want to forward the FortiSOAR™ logs.

- b. From the **Protocol** drop-down list, select the protocol that you want to use to communicate with the syslog server. You can choose between **UDP**, **TCP**, or **REL**.
  - c. In the **Port** field enter the port number that you want to use to communicate with the syslog server.
  - d. (Optional) To securely communicate with the syslog server, click **Enable TLS**. Once you click **Enable TLS**, in the **Certificate** field, you must enter your CA certificate.  
If you have a client certificate for your FortiSOAR™ client, then in the **Client Certificate** and **Client Key** fields, you must enter the client certificate and the client key.
3. In the **Choose Log Types To Forward** section, choose the types of FortiSOAR™ logs you want to forward to the syslog server.  
**Application Logs** include OS logs, and this checkbox is selected by default. To also forward FortiSOAR™ audit logs, click the **Audit Logs** checkbox. Once you select audit logs, you can define the following:
  - a. From the **Specify Audit Log Detail Level** drop-down list, select the amount of data, **Basic** or **Detailed** that you want to forward to the syslog server. Basic (default and recommended) sends high-level details of the event per audit log, whereas Detailed sends detailed information about the event per audit log.
  - b. In the **Configure Audit Log Forward Rules** section, define the rules to forward audit logs:  
From the **Record Type** drop-down list, select the record types such as, Alerts, Incidents, etc. whose audit logs you want to forward to the syslog server.  
From the **User** drop-down list, select the users such as, CS Admin etc., whose audit logs you want to forward to the syslog server.  
From the **Operation** drop-down list, select the operations such as Create, UpdateConfig, Delete, etc., whose audit logs you want to forward to the syslog server.  
From the **Playbooks** drop-down list, select the operations such as Generate Incident Summary Report, Playbook Execution History Cleanup, etc., whose audit logs you want to forward to the syslog server.  
To add more rules, click the **Define More Rules** link.  
**Important:** If you do not define rules, then all the audit logs will be forwarded.
4. Once you have completed configuring syslog forwarding, click **Save**.  
FortiSOAR™ performs validations such as, whether the syslog server is reachable on the specified port etc. before adding the syslog server.  
Once the syslog server is added, you can update or remove the configuration as per your requirements.

## Persisting the FortiSOAR™ logs

If your external log management server goes down, then the FortiSOAR™ logs generated during that time period will not be sent by FortiSOAR™ to your syslog server. If you want to

persist the logs for the time frame when external log management server is down and send those logs when server comes back online, you need to do the following:

In the `/etc/rsyslog.d/00-rsyslog-fortisoar-settings.conf` file, add the following contents after the `####` add the server details after this `####` line:

`####` add the server details after this `####`

```
$ActionQueueType LinkedList
$WorkDirectory /home/csadmin/.offline-rsyslogs/
#
# for the workdir mentioned above, make sure you run
# chown -R -t syslogd_var_lib_t /home/csadmin/.offline-rsyslogs/
#
$ActionQueueMaxDiskSpace 1gb # 1gb space limit (You can change this value)
$ActionQueueFileName fortisoar-offline-rsyslog
$ActionResumeRetryCount -1
$ActionQueueSaveOnShutdown on
```

Next, run the following commands:

```
mkdir -p /home/csadmin/.offline-rsyslogs/
chcon -R -t syslogd_var_lib_t /home/csadmin/.offline-rsyslogs/
systemctl restart rsyslog
```

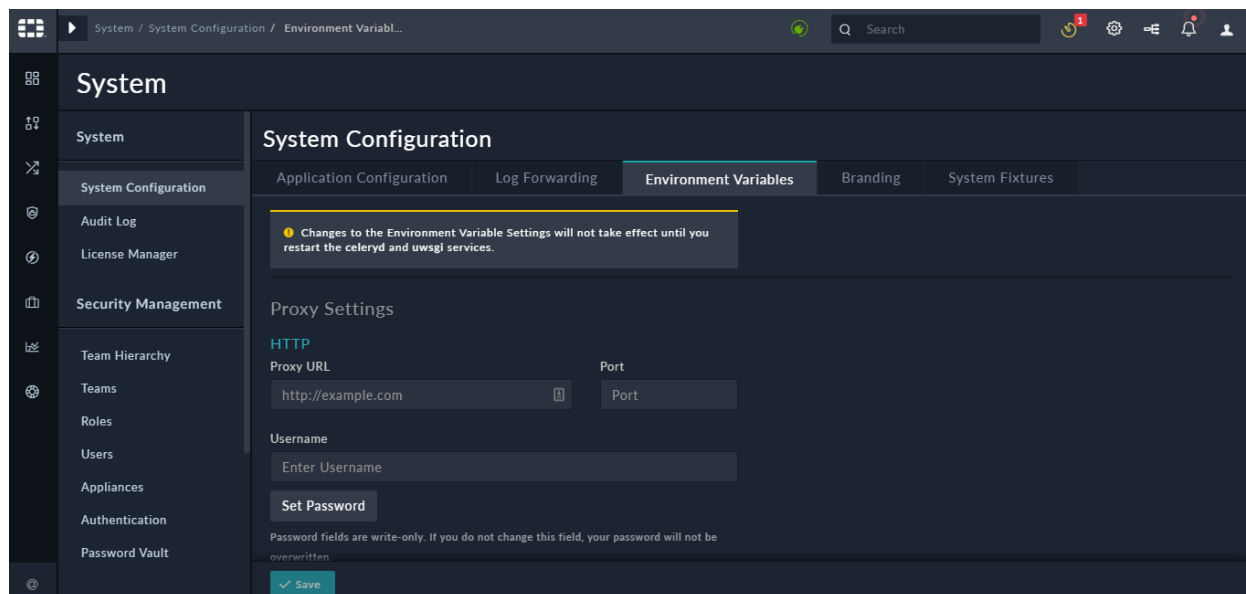
## Environment Variables

You can use the **Environment Variables** tab on the `System Configuration` page to configure proxy settings for FortiSOAR™ and to define any other environment variables.

**Important:** When you configure proxies using the FortiSOAR™ UI, the Environment Variables tab, the proxies get applied at the application level but not at the OS level. To configure proxies at the OS level, you need to make that entry in the `/etc/environment` file.

The procedure of how to configure proxy settings and define environment variables is included in the `Configuring Proxy Settings and environment variables` section in the *Additional configuration settings for FortiSOAR™* chapter of the “Deployment Guide”.

**Important:** Whenever you change the proxy server settings or the environment variables you must restart the **celeryd** and **uwsgi** services for the changes to take effect. Use the `# systemctl restart celeryd` and `# systemctl restart uwsgi` commands to restart the celeryd and uwsgi services.



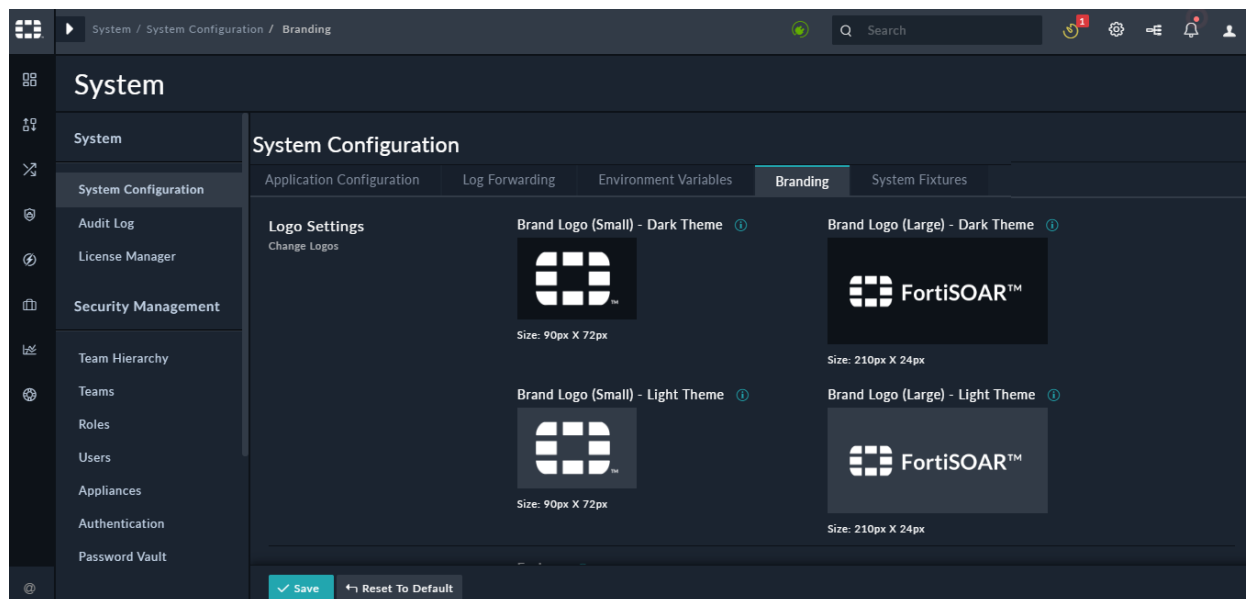
**Figure 5.** *System Configuration Menu - Environment Variables tab*

**Note:** External web pages that you open (for example, from a link included in the description field of an alert) or view (for example, using the iFrame Widget) in FortiSOAR™ goes through the configured proxy server if you have configured the proxy in the web browser's settings. If the proxy is not configured in the web browser's settings, then the external web pages are opened directly without using the configured proxy server.

## Branding

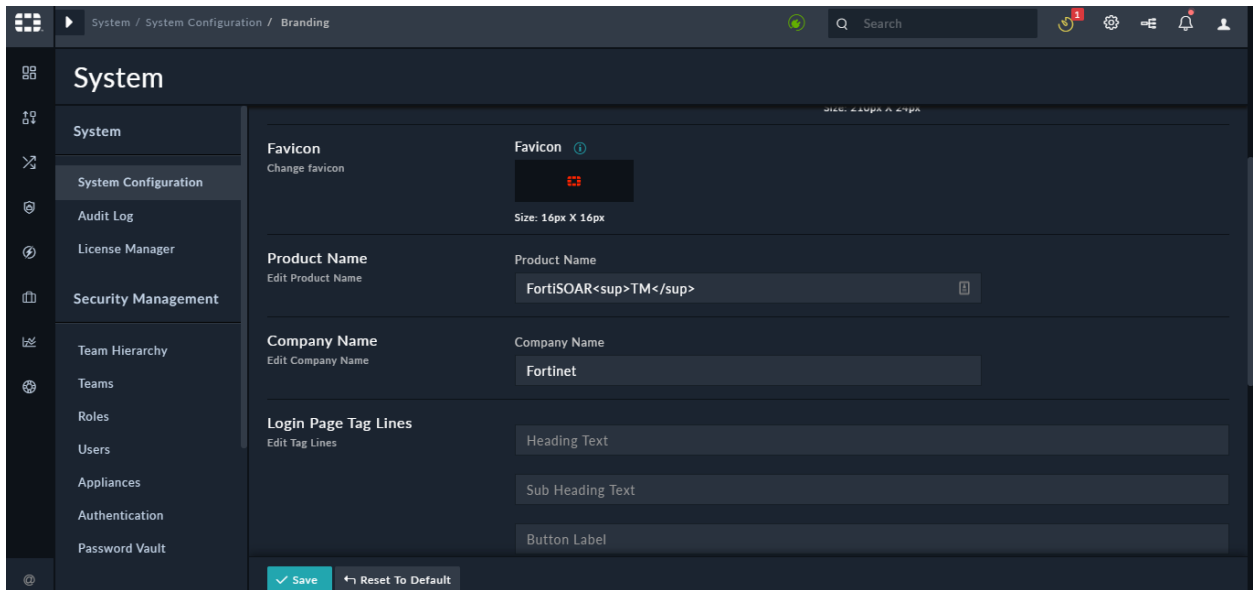
You can customize branding of FortiSOAR™ as per your requirement. From version 6.4.0 onwards, branding is not bound based on licensing, i.e., all customers can customize FortiSOAR™ branding as per their requirements.

To customize your branding in FortiSOAR™, you must have a role which has a minimum of **Application Update** permission and then can do any or all of the following branding changes:

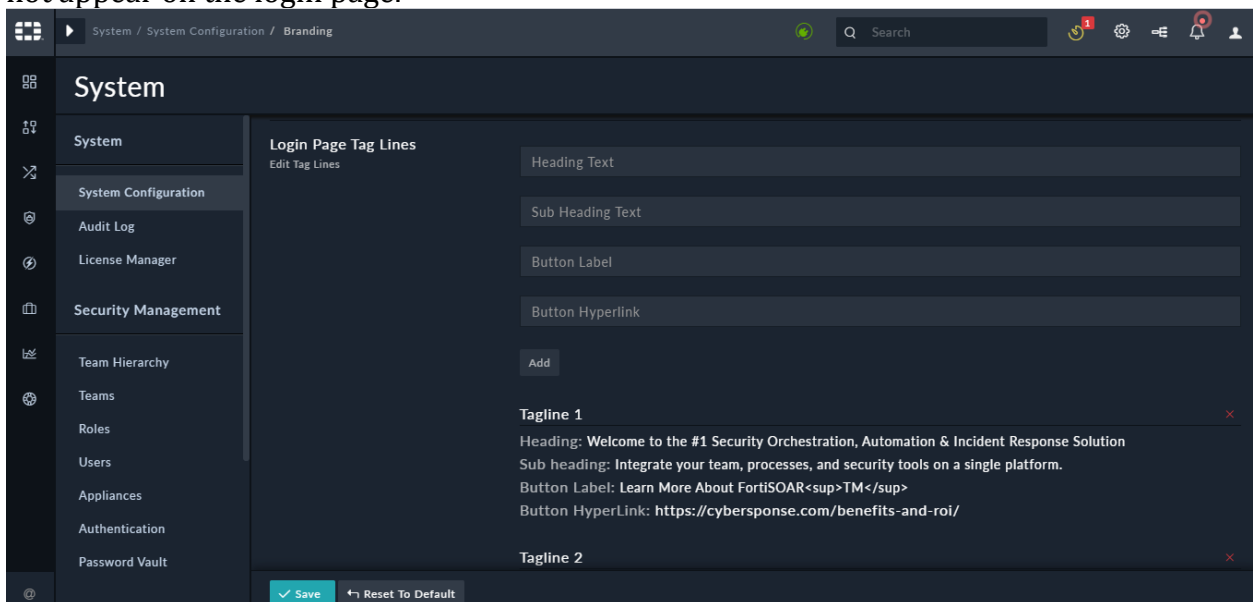


**Figure 6.** System Configuration Menu - Branding tab

- Changing Logos:** You can update the FortiSOAR™ logo to reflect your logo in the FortiSOAR™ UI. However, note that the maximum size for a logo is 1 MB.  
 Update your logo in the **Logo Settings** section:  
 Brand Logo (Small) - Dark Theme and Brand Logo (Large) - Dark Theme: Click the FortiSOAR™ logos and browse to the logos that you want to display in FortiSOAR™ Dark or Steel theme in two sizes: Small (90px X 72px) and Large (210px X 24px).  
 Brand Logo (Small) - Light Theme and Brand Logo (Large) - Light Theme: Click the FortiSOAR™ logos and browse to the logos that you want to display in FortiSOAR™ Light theme in two sizes: Small (90px X 72px) and Large (210px X 24px).  
**Note:** You can hover on the information icon to view where these logos will appear in FortiSOAR™.
- Changing the Favicon:** To change the favicon that is displayed in FortiSOAR™, click the FortiSOAR™ favicon and browse to the icon that you want to display as a favicon.  
**Note:** You can hover on the information icon to view where this favicon will appear in FortiSOAR™.



- **Editing the Product Name:** To change the name of the product displayed in the FortiSOAR™ UI, in the Product Name field, enter the name of the product that you want to display in the UI.
- **Editing the Company Name:** To change the name of the company displayed in the FortiSOAR™ UI, in the Company Name field, enter the name of the company that you want to display in the UI.
- **Editing the Login Tagline:** To change the customized messages or taglines that appears to all users on their login screen, you can deselect the default tagline(s) by clicking the red cross that appears beside the tag line. The tagline that you deselect will not appear on the login page.



You can then add your own tag line in the Login Page Tag Lines section as follows:  
In the **Heading Text** field: Enter the heading for your tagline.



In the **Sub Heading Text** field: Enter the sub-heading for your tagline.

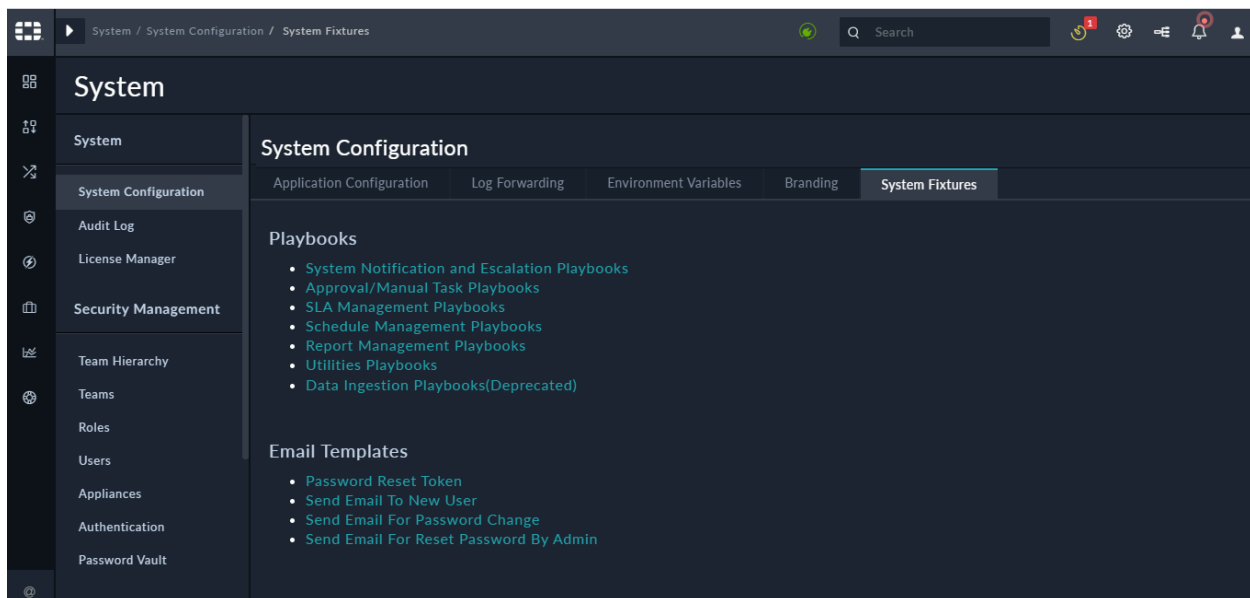
In the **Button Label** and **Button Hyperlink** fields: If you want to add a button on your login page, which on clicking by the user, navigates the user to another web page, then enter the label of the button and the URL of the other web page in the Button Label and Button Hyperlink fields respectively.

Once you complete adding your tag line, click **Add**.

To save your branding updates, click **Save**, to reset the branding to its default, click **Reset to Default**.

## System Fixtures

The FortiSOAR™ UI includes links in the **System Configuration** page to the various playbook collections and templates, which are included by default when you install your FortiSOAR™ instance. Click the **System Fixtures** tab on the System Configuration page to view the links to the system playbook collections and templates. Administrators can click these links to easily access all the system fixtures to understand their workings and make changes in them if required. In the previous versions, administrators required to know the complete URL for these fixtures to access them and make required changes.



**Figure 7.** *System Fixtures tab*

The following fixtures are included:

### Playbooks:

- System Playbook collection (System Notification and Escalation Playbooks collection): Includes a collection of system-level playbooks that are used to automate tasks, such as the **Escalate** playbook which is used to escalate an alert to an incident based on specific inputs from the user and linking the alert(s) to the newly created incident.

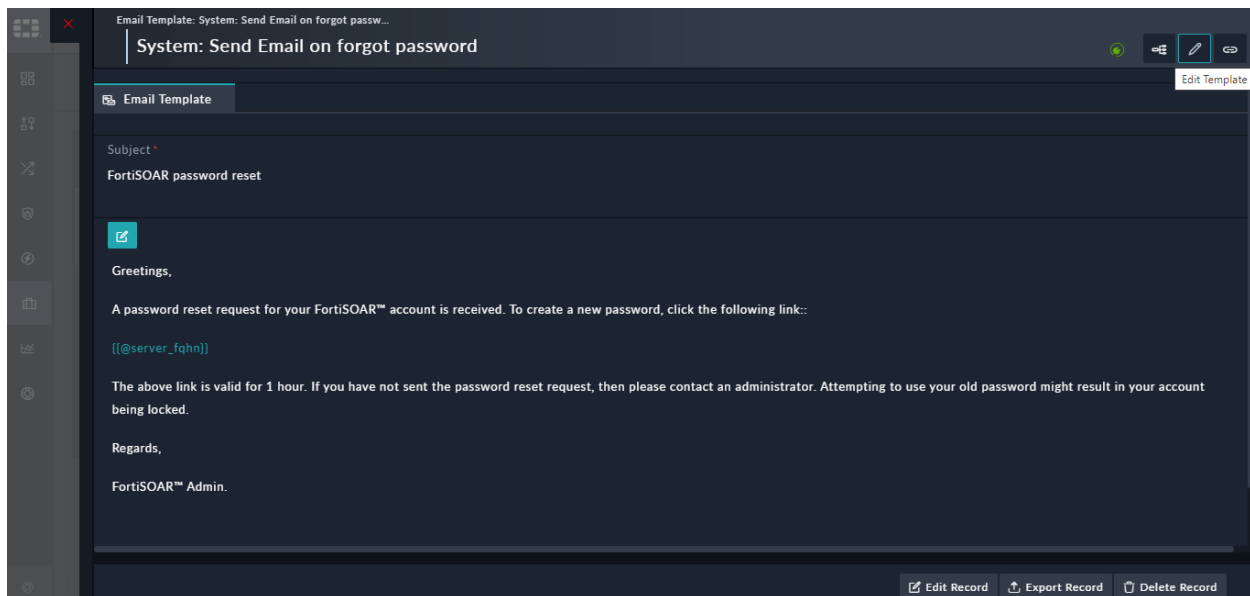
- **Approval/Manual Task Playbooks collection:** Includes a collection of system-level playbooks that are used to automate approvals and manual task, such as the playbook that will be triggered when an approval action is requested from a playbook.
- **SLA Management Playbooks collection:** Includes a collection of system-level playbooks that are used to auto-populate date fields in the following cases: when the status of incident or alert records have been changed to **Resolved** or **Closed** or when incident or alert records are assigned to a user.
- **Schedule Management Playbooks collection:** Includes a collection of system-level playbooks that are used for the scheduler module and used for various scheduler actions such as scheduling playbook execution history cleanup, audit log cleanup, etc.
- **Report Management Playbooks collection:** Includes a collection of system-level playbooks that are used to manage generation of FortiSOAR™ Reports.
- **Utilities Playbook collection:** Includes a collection of system-level playbooks that are used by system utilities.
- **Data Ingestion Playbooks collection:** Includes a collection of data ingestion playbooks for all the connectors that are enabled for data ingestion. This has been deprecated.

For more information on system-level playbooks, see the *Playbooks Overview* chapter in the “Playbooks Guide.”

## Email Templates

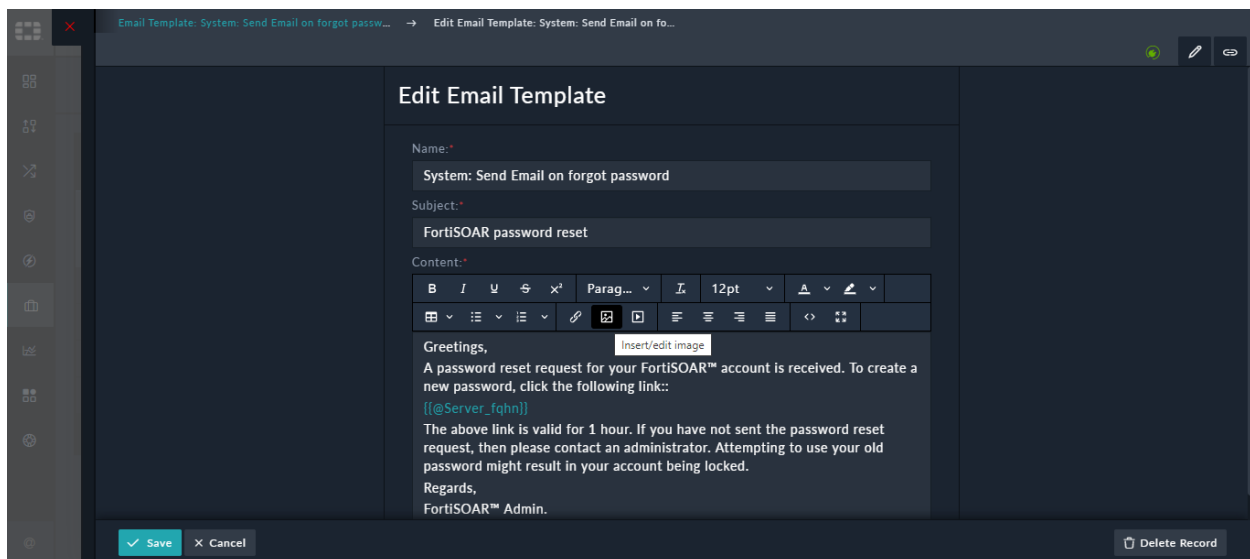
- **Password Reset Token:** Includes an email template that is sent to FortiSOAR™ users’ who forget their password and click on the **Forgot Password** link, so that they can reset their password. This email contains a link that the user can use to create their new password.
- **Send Email To New User:** Includes an email template that is sent to a new FortiSOAR™ users’ and it contains a link that the new user can use to create their own new password.
- **Send Email For Password Change:** Includes an email template that is sent when a user requests for a change in their FortiSOAR™ password.
- **Send Email For Reset Password By Admin:** Includes an email template that is sent to FortiSOAR™ users’ whose password has been reset by an administrator.

To modify the content of the email templates, click the email template whose content you want to change, for example, click **Password Reset Token** to open the email template. Click the **Edit Record** button to edit the contents of the template. You can also click the **Edit Template** icon to edit the structure of the email or click **Actions** to perform actions on the record.



**Figure 8.** Opening the Password Reset Token Email Template

To change the content of the email, click the **Edit** icon, or click the **Edit Record** to open the email template in a "form" format in which you can change the contents of the email as per your requirement, and then click **Save** to save your changes.



**Figure 9.** Editing the Email Template in the Form Format

In case you have deleted the email templates, and you require to update or modify the default email templates, then you require to edit the `mailtemplate.yml` file located at `/opt/cyops/configs/cyops-api/`.

## Audit Log

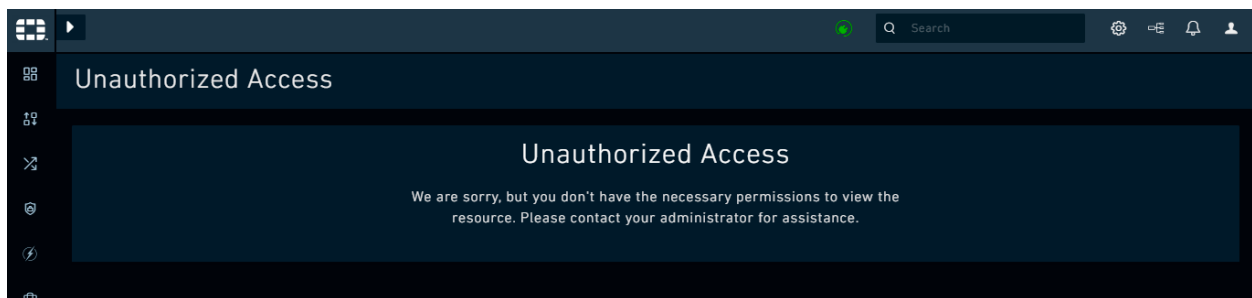
You can view the historical record of activities across FortiSOAR™ using the Audit Log, the User-Specific Audit Logs, and the graphical representation of the Audit Log in the detail view of a record.

### Audit Log Permissions

- To view your own audit logs, you must have a role with a minimum of **Read** permission on the **Audit Log Activities** module. To view audit logs of all users, you must have a role with a minimum of **Read** permission on the **Security** and **Audit Log Activities** modules.
- To delete your own audit logs, you must have a role with a minimum of **Delete** permission on the **Audit Log Activities** module. To delete audit logs of all users, you must have a role with a minimum of **Delete** permission on the **Security** and **Audit Log Activities** modules.

**Note:** The **Delete** permission on the **Audit Log Activities** module will be removed for both **csadmin** and **playbook appliances** roles, and also this will not be enabled (checked) by default for the **Full App Permissions** role. Therefore, if you want any user or role to have the right to delete audit logs, you must explicitly assign the **Delete** permission on the **Audit Log Activities** module to that particular user or role.

If you cannot access the Audit Log, you must ask your administrator for access. FortiSOAR™ displays an error, as shown in the following image, if you do not have access to Audit Logs:



**Figure 10.** *Audit Log - No access error message*

You can view historical record of activities across FortiSOAR™ using the following options:

- **Audit Log:** Audit Log displays a chronological list of all the actions across all the modules of FortiSOAR™. Click **Settings > Audit Log** to open the **Audit Log** page.
- **User-Specific Audit Logs:** User-Specific Audit Logs displays a chronological list of all the actions across all the modules of FortiSOAR™ for a particular user.
- **Viewing Audit Log in the detailed view of a record:** You can view a graphical presentation, or grid view, of all the actions performed on that particular record. The audit log is displayed in a graphical format using the **Timeline** widget.

Audit Logs include data such as, recording the name of the user who had deleted the record, linking and delinking events, picklist events, and model metadata events (including

changes made in model metadata during the staging phrase). Free text search, additional filtering criteria, the ability to quickly add auditing for a new service and lazy loading has also been implemented in audit logs.

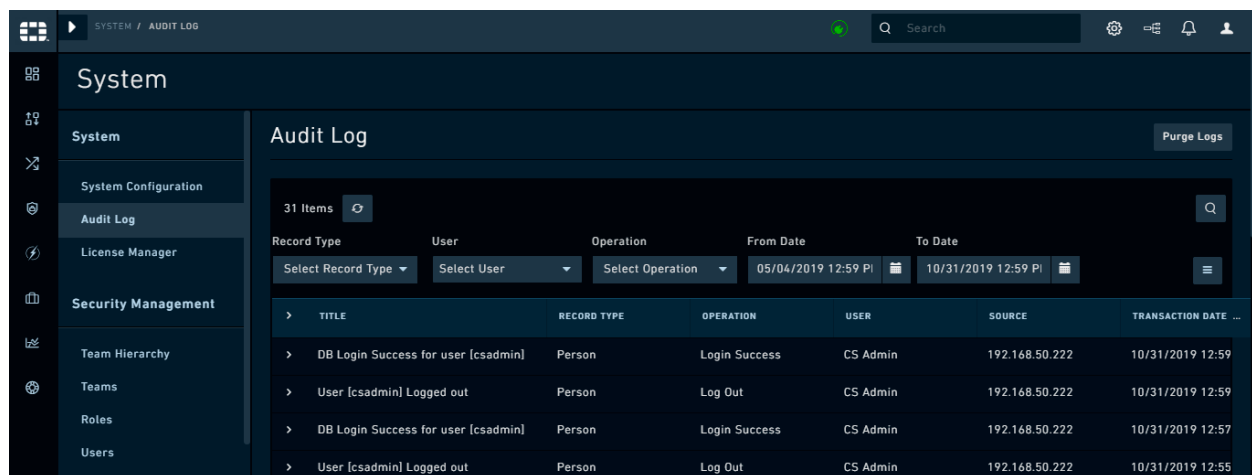
Audit logs also contain operations related to playbooks such as trigger, update, terminate, resume, create and delete playbook versions, etc. From version 6.4.1 onwards, the operations such as `Snapshot Created` and `Snapshot Deleted` operations are renamed to `Version Created` and `Version Deleted` since snapshots have been renamed to versions. However, for older audit logs in cases of an upgrade, you will see the old audit log entries with the older names such as `Snapshot Created` and `Snapshot Deleted`.

The data included in the audit log also contain the following types of entries:

- Users' login success or failures and logout events. The login event includes all three supported login types, which are DB Login, LDAP Login, and SSO Login.
- Users' login with an invalid username.
- Locked users's attempts to log on to FortiSOAR™.
- Inactive users's attempts to log on to FortiSOAR™.

**Important:** If you have a field, in a module, whose `Singular Description` attribute value contains a `.` or `$` then the Audit Logs replace the `.` or `$` with an `_`. For example, if you have a field `SourceID` whose singular description you have specified as `Source.ID`, then in this field will appear as `Source_ID` in Audit Logs.

You can purge Audit Logs using the **Purge Logs** button on the top-right of the `Audit Log` page. You will see the **Purge Logs** button only if you have **Delete** permissions on the `Audit Log Activities` module.

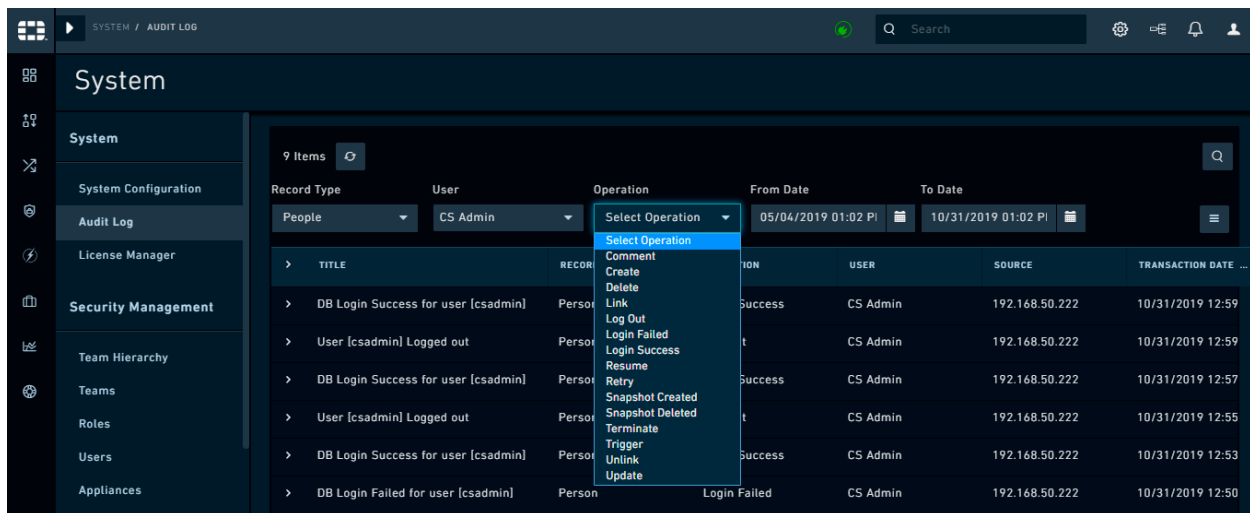


**Figure 11.** *Audit Logs - Purge Logs*

You can also use the Audit Log Purge API to purge audit logs on an automated as well as an on-demand basis. For more information, see the *API Methods* section in the “API Guide.”

## Viewing Audit Log

Use the Audit Log to view a chronological list of all the actions across all the modules of FortiSOAR™. To view the Audit Log page, you must have access to the Audit Log Activities module. Click **Settings** > **Audit Log** to open the Audit Log page. The audit log also displays users' login success or failures and logout events. The login event includes all three supported login types, which are DB Login, LDAP Login, and SSO Login.



**Figure 12.** Audit Log

You can filter the audit logs to display the audit logs for a particular record type by selecting the record type (module) from the **Record Type** drop-down list. You can also filter audit logs on users, operations, and data range, apart from modules.

To filter audit logs on for a particular user, select the user from the **Select User** drop-down list.

To filter audit logs on for a particular operation, select the operation from the **Select Operation** drop-down list. You can choose from the operations such as, Comment, Create, Delete, Link, Login Failed, Snapshot Created, Trigger, Unlink, Update, etc.

You can also filter audit logs for a particular date range by selecting the **From Date** and **To Date** using the calendar icon.

You can also search for audit logs using free text search. Click the **Search** icon and enter a search criterion in the **Search Logs** field to search the audit logs.

The Audit Log displays the following historical information for each record:

- **Title:** Title of the record on which the action was performed.  
**Note:** In case of Approval playbooks the playbook audit log displays the Approval Description field, which represents the name of the approval record, in the Title field. In this case, the Title field will be displayed in the format Approval [Approval]

Description] Operation Performed. For example, Approval [Approval Test] Created.

- **Record Type:** Type (module) of the record on which the action was performed.
- **Operation:** Operation that was performed.
- **User:** User who performed the operation
- **Source:** Source IP address where the operation that was performed.
- **Transaction date:** Date and time that the record was updated in the format DD/MM/YYYY HH:MM.

To view the details of an audit log entry, click the expand icon (>) in the audit entry row. Details in the audit log entry are present in the JSON format, and include the old data and updated (new) data for a record, in case of an update operation, and all attributes and their details, such as ID and type, for a record, in case of a create operation. You can copy the data using the **Copy to Clipboard** button.

The screenshot displays the 'Audit Log' interface. At the top, there's a 'Purge Logs' button. Below it, a summary bar shows '3 Items' and a refresh icon. A filter bar includes 'Record Type' (set to 'Alerts'), 'User' (set to 'CS Admin'), 'Operation' (set to 'Select Operation'), 'From Date' (05/04/2019 01:06 PM), and 'To Date' (10/31/2019 01:06 PM). A search icon and a 'More Options' icon (three horizontal lines) are on the right. Below the filter bar is a table with columns: TITLE, RECORD TYPE, OPERATION, USER, SOURCE, and TRANSACTION DATE. The first row is expanded, showing details for 'Attribute(s) [Status] Updated in Alert ...'. A 'Copy to Clipboard' button is visible. Below the table, a JSON viewer shows the details of the expanded row, including 'newData : Open'.

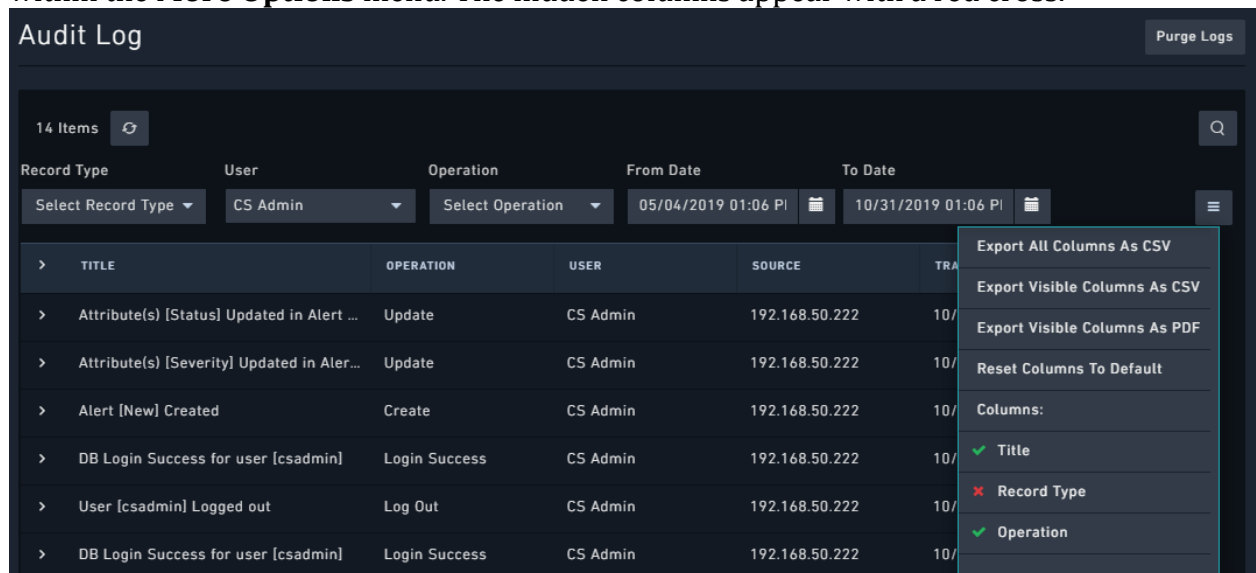
**Figure 13.** *Audit Log: Log Details*

You can perform the following operations on the Audit Log page, by clicking the **More Options** icon (≡) to the right of the table header:

- **Export All Columns As CSV:** Use this option to export all the columns of the audit log to a .csv file.
- **Export Visible Columns As CSV:** Use this option to export visible columns of the audit log to a .csv file.

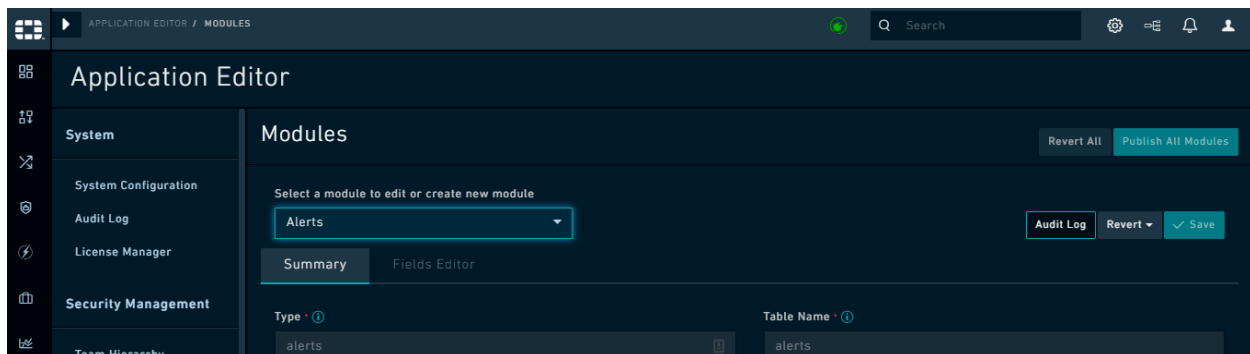
**Note:** You can hide columns by deselecting a column from the list of columns present

within the **More Options** menu. The hidden columns appear with a red cross.



- **Export Visible Columns As PDF:** Use this option to export visible columns of the audit log to a .pdf file.
- **Reset Columns To Default:** Use this option to reset the audit log fields to the default fields specified for the audit log.

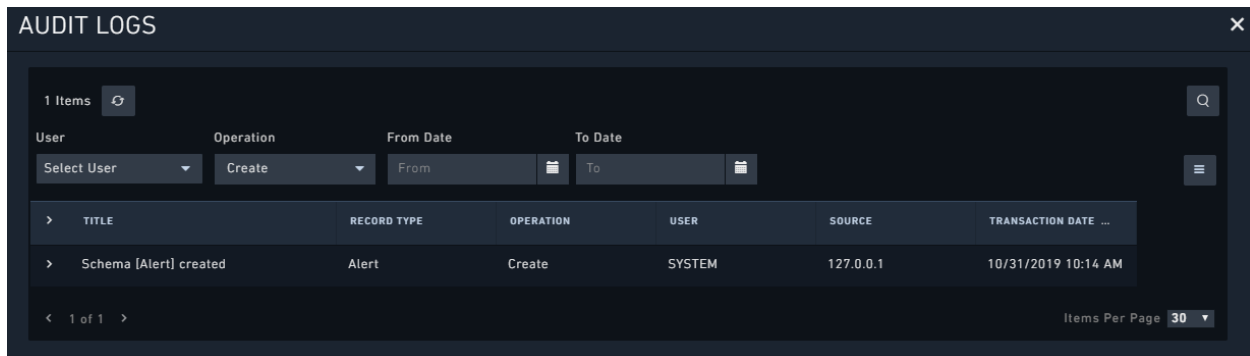
You can view logs specific to a particular module, by clicking **Settings > Modules** (in the Application Editor section) and from the **Select a module to edit or create new module** drop-down list, select the module whose audit log you want to view, and then click the **Audit Logs** button.



**Figure 14.** Audit Log for a particular module

You view the same details and perform the same actions as mentioned earlier on the Audit Logs Dialog. You can filter the audit logs for modules on users, operations, and date range. For example, you can filter logs which have an **Create** operation performed on a particular record type (module), as shown in the following image:





**Figure 15.** *Audit Logs: Alert Module Audit log*

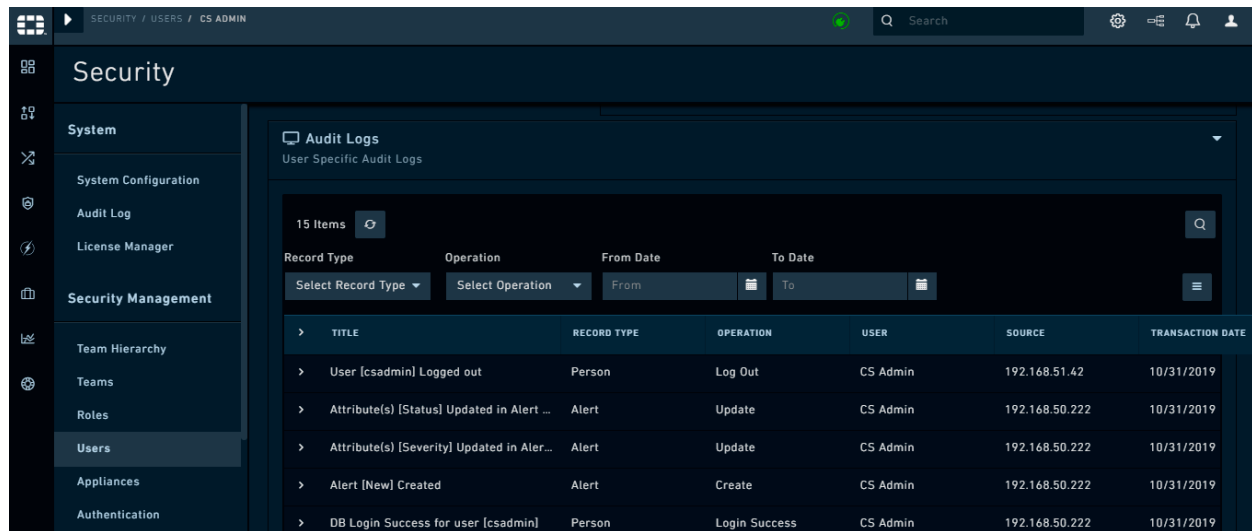
Similarly, you can also view logs specific to a particular picklist, go to **Settings > Picklists** (in the **Application Editor** section). From the **Select a picklist or edit or create a new picklist** drop-down list select the picklist whose audit log you want to view and click the **Audit Logs** button. You view the same details and perform the same actions as mentioned earlier on the **Audit Logs** Dialog. You can filter the audit logs for picklists on users, operations, and date range.

From version 6.4.3 onwards, audit logs have been further enhanced so that you can get comprehensive records of all activities across FortiSOAR™. Audit logs now include the auditing of the following actions:

- Schedule actions - Create, update and delete, start, and stop
- Rules actions - Create, update, delete, activate, and deactivate
- Dashboard/Report actions - Create, update, and delete
- Navigation actions - All
- Authentication actions - All
- License Update actions - All
- SVT Update actions - All
- Role - Modification (Create and Delete already gets audited)
- Team - Modification (including team hierarchy updates), User Link/Unlink (Create and Delete already gets audited)

## Viewing User-Specific Audit Logs

Use the User-Specific Audit Logs to view the chronological list of all the actions across all the modules of FortiSOAR™ for a particular user. Users can view their own audit logs by clicking the **User Profile** icon and selecting the **Edit Profile** option and clicking the **Audit Logs** panel. Administrators who have a minimum of **Read** access on the **Audit Log Activities** module along with access to the **People** module, which allows them to access a user's profile, can view **User Specific Audit Logs**. The user-specific audit log also displays user's login success or failures and logout events. The login event includes all three supported login types, which are DB Login, LDAP Login, and SSO Login.



**Figure 16.** *User-Specific Audit Logs*

Use the same filtering and searching techniques mentioned in the [Viewing Audit Log](#) section. You can filter the user-specific audit logs on record types (modules) and date range.

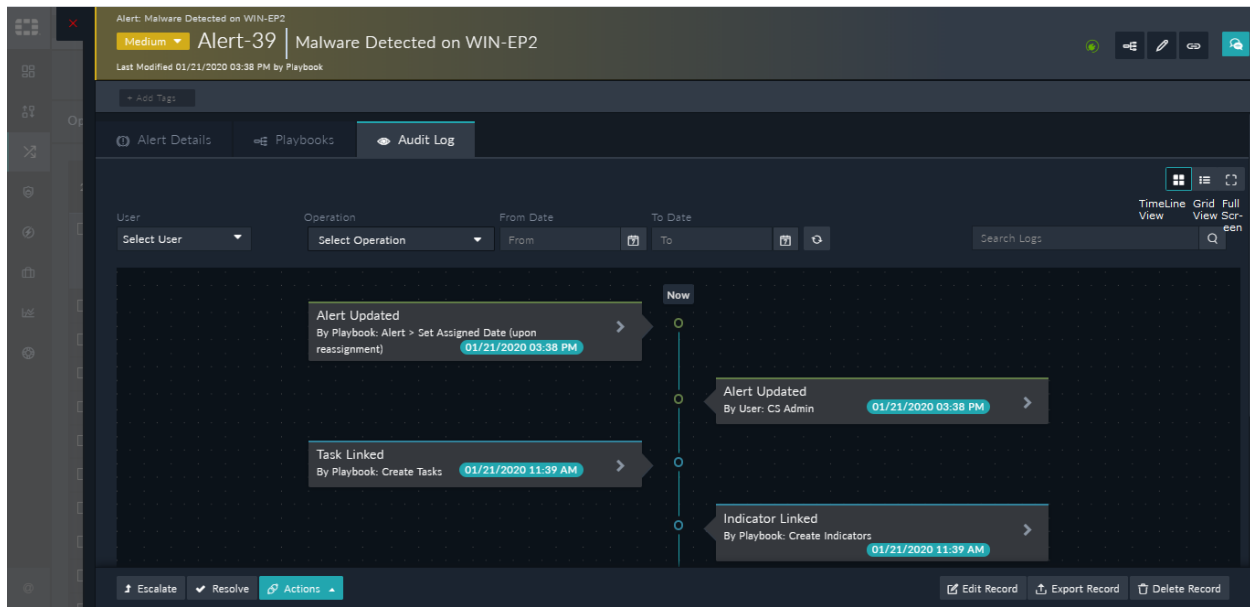
The user-specific audit logs display the same information as the audit log, and you can also perform the same actions here as you can perform in case of audit logs. For more information, see the [Viewing Audit Log](#) section.

## Viewing Audit Log in the detailed view of a record

Use the **Audit Log** tab, which is present in the detail view of a record, to view the graphical presentation of all the actions performed on that particular record. The **Audit Log** tab uses the **Timeline** widget to display the graphical representation of the details of the record. You cannot edit the **Timeline** widget. For more information about widgets, see the *Using Template Widgets* topic in the “User Guide.”

You can toggle the view in the **Audit Log** tab to view the details in both the grid view and the timeline (graphical) view. Use the same filtering and searching techniques mentioned in the [Viewing Audit Log](#) section. You can filter the user-specific audit logs on record types and date range.

Click a record within a module to open the detail view of a record and then click the **Audit Log** tab to view the graphical representation, or grid view of the details of the record, as shown in the following image:

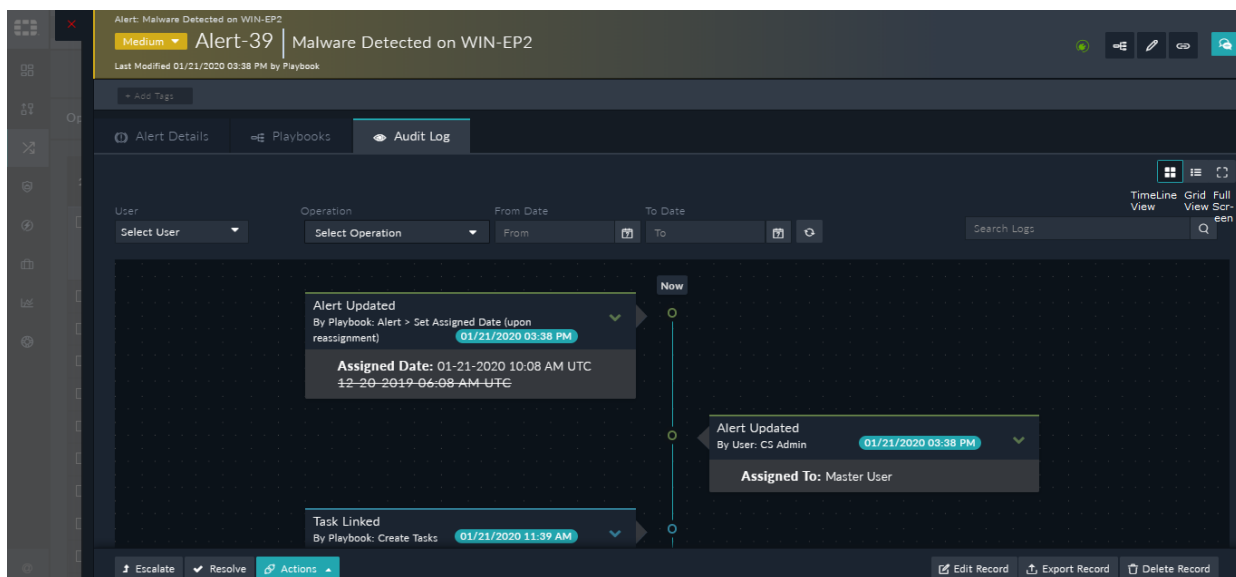


**Figure 17.** *Timeline Widget output on the Detail View page*

A timeline item mentions the action performed on the record, such as **Created**, **Updated**, **Commented**, **Attached**, or **Linked**, the name of the person who has made the update, and the date and time that the update was made.

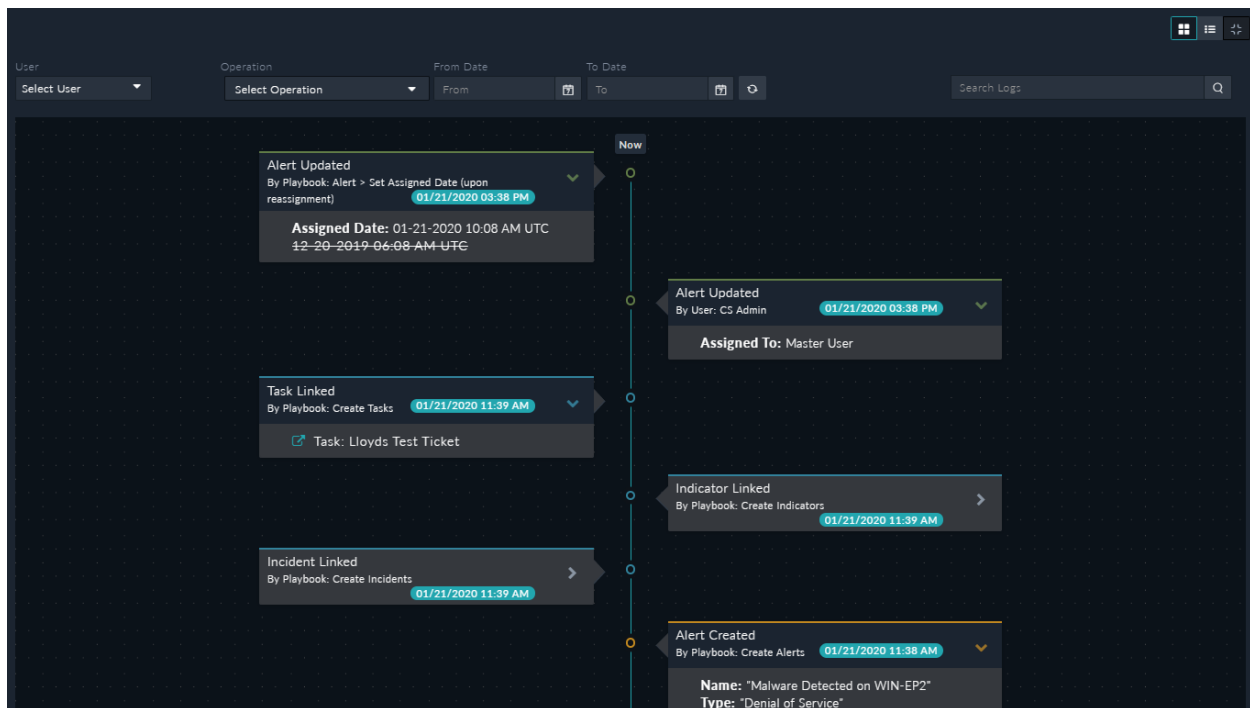
**Note:** In the timeline, you might see some records created by **Playbook**. This signifies that the record was created by a workflow entity, such as a Playbook or a Rule.

When you update any detail in a record, then you can click the refresh button in the timeline to view the updates in timeline immediately. To view the complete details of the updates made at a particular timeline item, click the arrow (>) present to the right of the item. The following image displays the details shown for a specific timeline item:



**Figure 18.** *Detailed timeline item*

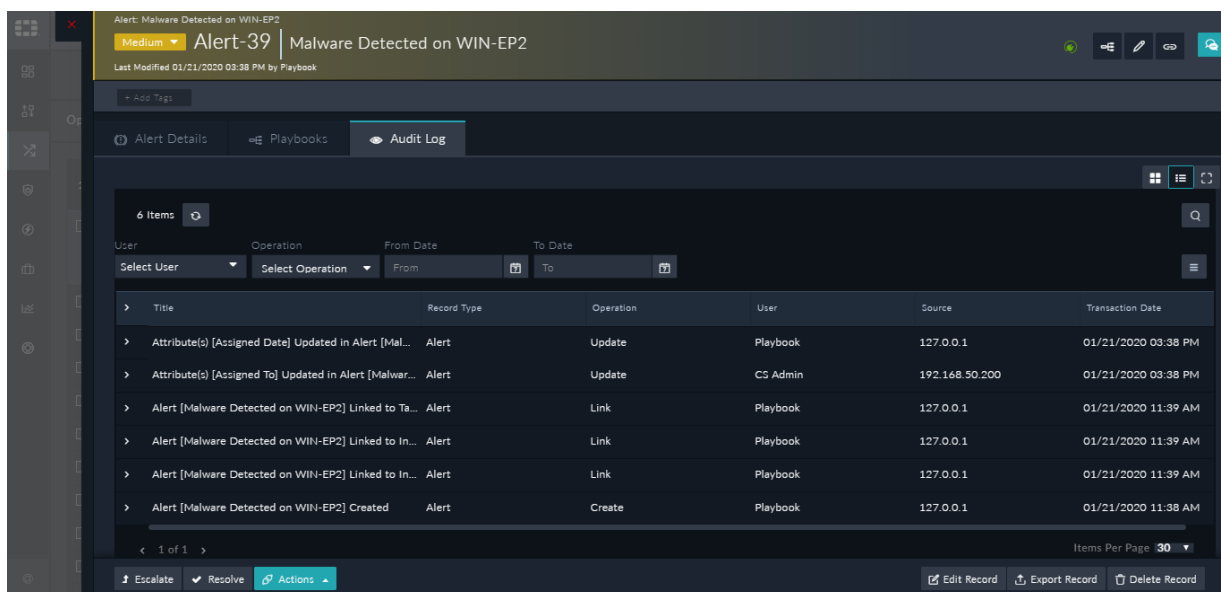
You can toggle between the expanded and collapsed view of the audit log tab, using the **Full-screen Mode** icon. To move to a full screen view of the audit log, click the **Full-screen Mode** icon, which opens the audit log in the full screen as shown in the following image:



**Figure 19.** *Audit log in full screen*

To exit the full screen, press **ESC**.

You can toggle between the timeline view and grid view in the Audit Log tab. The grid view in the detailed view of a record appears as shown in the following image:



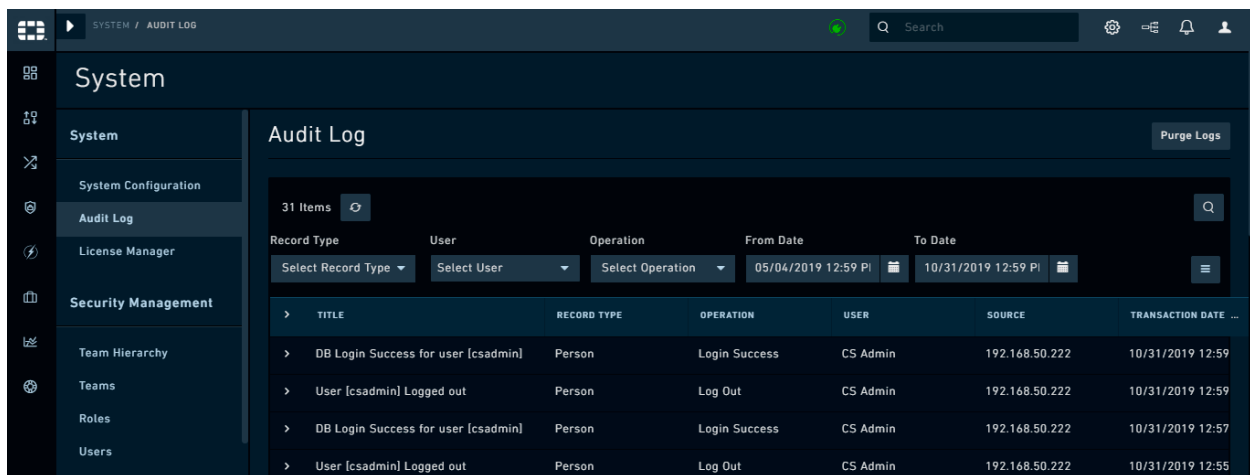
**Figure 20.** *Grid Widget output on the Detail View page*

The grid view also displays the same information as the audit log, and you can also perform the same operations here as you can perform in case of audit logs. For more information, see the [Viewing Audit Log](#) section.

## Purging Audit Logs

You can purge Audit Logs using the **Purge Logs** button on the top-right of the **Audit Log** page. Purging audit logs allows you to permanently delete old audit logs that you do not require and frees up space on your FortiSOAR™ instance. You can also schedule purging, on a global level, for both audit logs and executed playbook logs. For information on scheduling Audit Logs and Executed Playbook Logs, see [Scheduling purging of audit logs and executed playbook logs](#).

To purge Audit Logs, you must be assigned a role that has a minimum of Read permission on the **Security** module and Delete permissions on the **Audit Log Activities** module.



**Figure 21.** *Audit Logs - Purge Logs*

To purge Audit Logs, click the **Purge Logs** button on the **Audit Log** page, which displays the **Purge Audit Logs** dialog:

PURGE AUDIT LOGS

×

Provide the date and time until which the audit logs are to be purged. Logs before the specified time frame will be permanently deleted.

Purge all logs before,

PURGE LOGS OF SPECIFIC EVENT TYPE

Various event types are recorded within audit logs. You can select the event types for which you want to purge the logs. By default, logs for all event types are purged.

☒ Create

☒ Update

☒ Delete

☒ Link

☒ Unlink

☒ Comment

☒ Trigger

☒ Login Failed

☒ Login Success

☒ Log Out

☒ Resume

☒ Retry

☒ Terminate

☒ Snapshot Created

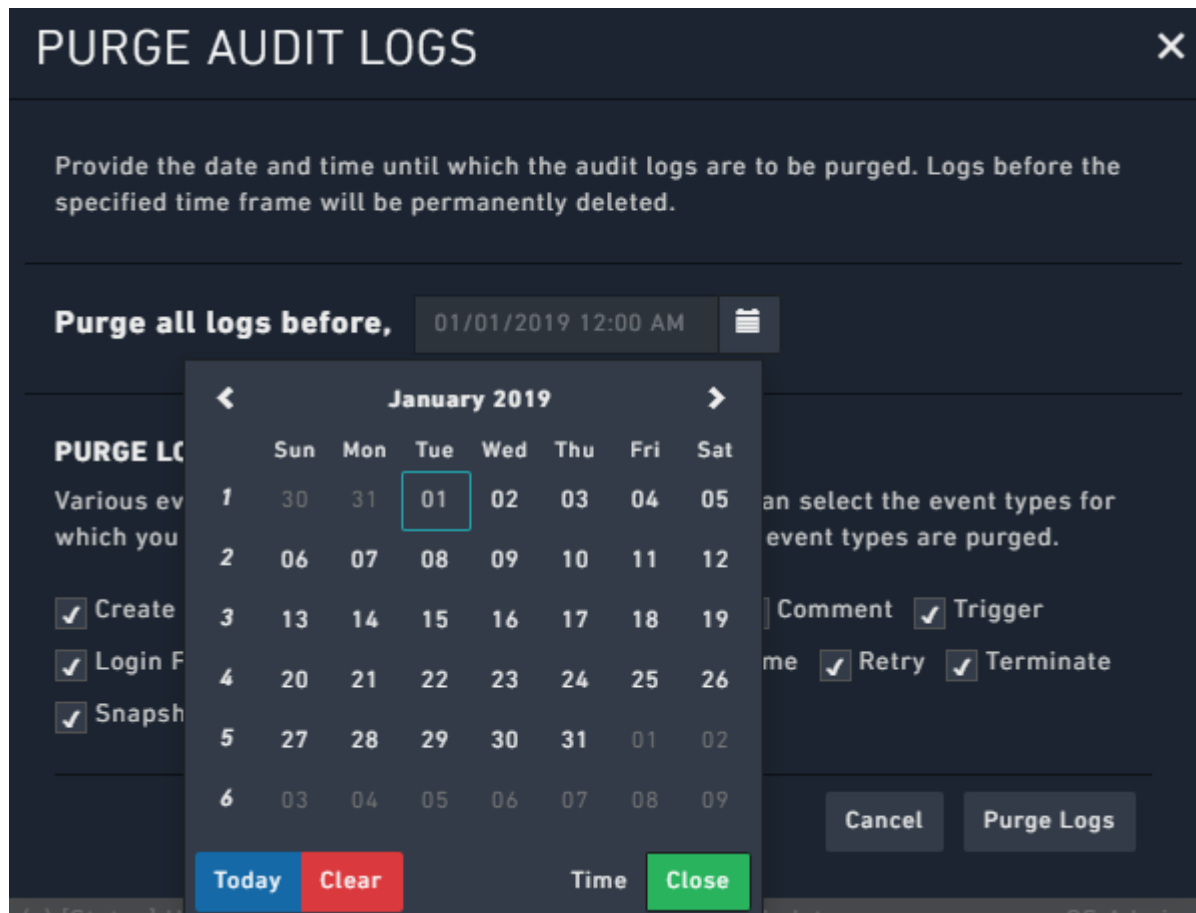
☒ Snapshot Deleted

Cancel

Purge Logs

**Figure 22.** *Purge Logs Dialog - Date and Time Selection*

In the **Purge all logs before,** field, select the time frame (using the calendar widget) before which you want to clear all the audit logs. For example, if you want to clear all audit logs before January 1st, 2019, 12:00 AM, then select this date and time using the calendar widget.



**Figure 23.** *Purge Logs Dialog - Date and Time Selection*

By default, logs of all events are purged. However, you can control the event types that will be chosen for purging. For example, if you do not want to purge events of type “Login Failure” and “Trigger”, then you must clear the **Login Failure** and **Trigger** checkboxes, as shown in the following image:

PURGE AUDIT LOGS

×

Provide the date and time until which the audit logs are to be purged. Logs before the specified time frame will be permanently deleted.

Purge all logs before,

01/01/2019 12:00 AM

PURGE LOGS OF SPECIFIC EVENT TYPE

Various event types are recorded within audit logs. You can select the event types for which you want to purge the logs. By default, logs for all event types are purged.

☒ Create

☒ Update

☒ Delete

☒ Link

☒ Unlink

☒ Comment

☐ Trigger

☐ Login Failed

☒ Login Success

☒ Log Out

☒ Resume

☒ Retry

☒ Terminate

☒ Snapshot Created

☒ Snapshot Deleted

Cancel

Purge Logs

**Figure 24.** *Purge Logs Dialog - Choosing Events to Purge*

To purge the logs, click the **Purge Logs** button, which displays a warning as shown in the following image:



PURGE AUDIT LOGS

×

Provide the date and time until which the audit logs are to be purged. Logs before the specified time frame will be permanently deleted.

Purge all logs before,

01/01/2019 12:00 AM

PURGE LOGS OF SPECIFIC EVENT TYPE

Various event types are recorded within audit logs. You can select the event types for which you want to purge the logs. By default, logs for all event types are purged.

☒ Create

☒ Update

☒ Delete

☒ Link

☒ Unlink

☒ Comment

☐ Trigger

☐ Login Failed

☒ Login Success

☒ Log Out

☒ Resume


☒ Retry

☒ Terminate

☒ Snapshot Created

☒ Snapshot Deleted

Warning:



This operation deletes the audit logs permanently. Hence, ensure that you only purge those logs that are no longer required.

Cancel

I Have Read The Warning - Purge Logs

**Figure 25.** *Purge Audit Log Dialog Warning*

Click the **I Have Read the warning - Purge Logs** to continue the purging process.

## License Manager

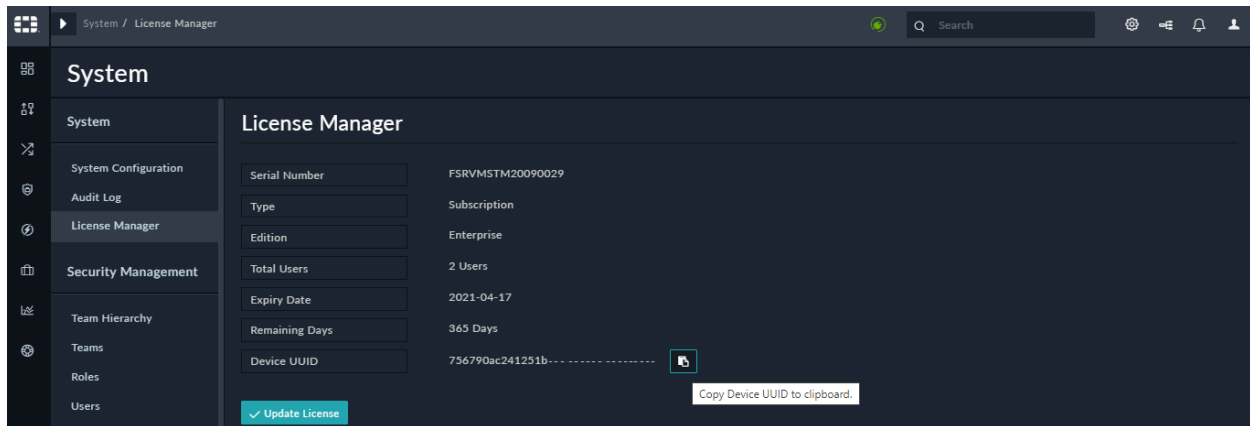
FortiSOAR™ enforces licensing using the License Manager. The License Manager restricts the usage of FortiSOAR™ by specifying the following:

- The maximum number of active users in FortiSOAR™ at any point in time.
- The type and edition of the license.
- The expiry date of the license.

For details of the FortiSOAR™ licensing process, including deploying your FortiSOAR™ license for the first time, see the *Licensing FortiSOAR™* chapter in the “Deployment Guide.”

You can use the **License Manager** page to view your license details and to update your license. FortiSOAR™ displays a message about the expiration of your license 15 days prior to the date your license is going to expire. If your license type is **Evaluation** or **Perpetual**, then you must update your license within 15 days, if you want to keep using FortiSOAR™. To update your license, click **Update License** and either drag-and-drop your updated license or click and browse to the location where your license file is located, then select the file and click **Open**. If your license type is **Subscription**, you must renew your subscription. For more information, see the *Licensing FortiSOAR™* chapter in the "Deployment Guide."

Click **Settings > License Manager** to open the **License Manager** page as shown in the following image:



**Figure 26.** *License Manager*

For details about the various parameters on the **License Manager** page, see the *Licensing FortiSOAR™* chapter in the "Deployment Guide."

# Segmented Network support in FortiSOAR™

## Overview

FortiSOAR™ supports segmented networks, which facilitates investigation in a multi-segmented network by allowing secure remote execution of connector actions and playbooks. If your requirement is to be able to remotely run connector actions and playbooks, then you can use the "FSR Agent".

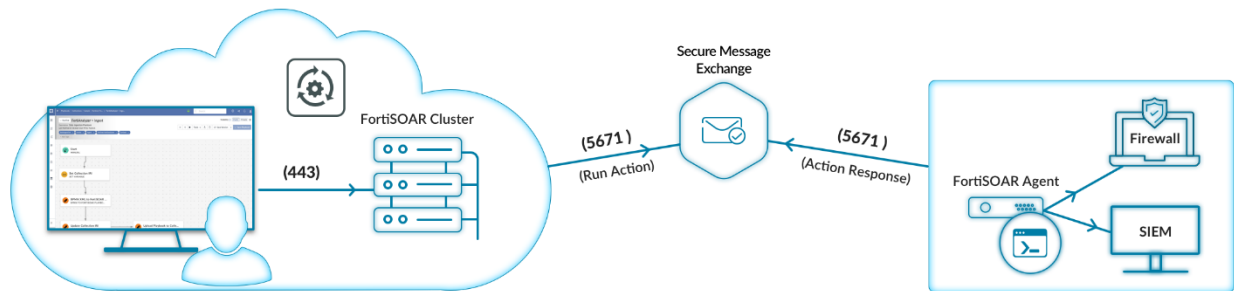
Automated ingestion, enrichment, or triage actions using a SOAR platform require network connectivity to various endpoints on which you want to run actions. These devices or endpoints, can at times, be in a different network segment than the one where the FortiSOAR™ appliance is deployed. To connect to such endpoints in segmented networks, FortiSOAR™ provides a lightweight component, called the "FortiSOAR Agent". An Agent can be deployed in a network segment and configured to receive and execute actions from a FortiSOAR™ node using its secure message exchange. The agent only needs an outbound network connectivity to the secure message exchange server on its TCP port. It does not need a VPN setup or an inbound network connectivity.

A FortiSOAR™ on-premise agent is small, lightweight, consumes minimal system resources and it is very easy to deploy and maintain. An agent can represent a standalone agent that can be deployed at a specific endpoint, or an agent can represent a dedicated tenant.

In cases such as a multi-segmented network where deploying a dedicated FortiSOAR™ node per segment is not feasible or required you can use the lightweight agent. You can install multiple agents on your FortiSOAR™ enterprise node using which you can run remote actions on various segments of your network.

**Note:** You do not require any additional licensing for the FortiSOAR™ secure message exchange.

### Agents for Segmented Network Support



**Figure 27.** *Architecture of Segmented Network Support*

## Recommended Resource Requirements for Virtual Machines (VM)

### Recommended specifications for Secure Message Exchange

- 8 available vCPUs
- 16 GB available RAM
- 100 GB available disk space: Recommended to have high-performance storage, preferably SSDs.
- 1 vNIC

### Recommended specifications for agents

- 4 GB available RAM
- CentOS Linux release 7.8.2003 (Kernel - 3.10.0-1127.el7.x86\_64) or Red Hat Enterprise Linux Server release 7.7 (Maipo) (Kernel - .10.0-1062.el7)

## Prerequisites for installing an agent

- Ensure that the VM on which you want to install the agent matches the recommended specifications, see [Recommended specifications for agents](#).
- Ensure that [update.cybersponse.com](https://update.cybersponse.com) is reachable or resolvable from the VM on which you want to install the agent.

- Ensure that the secure message exchange that you have specified when you have added the agent is reachable or resolvable from the VM.
  - Ensure that the following packages are installed on the instance where you are going to install the agent:
    - **Python36-devel:** The agent runtime needs "python36-devel". During agent installation, the installer looks for an existing installation, and in the case it is not installed, tries to install it using `yum install`. If this package is not found, the agent installation will fail.
    - **GCC:** Some connectors have a dependency on GCC. Therefore, the agent installer looks for an existing installation, and try to install it using `yum install`. If this package is not found, the agent installation will display a "warning" and will not fail the installation. You can install GCC later on an agent using the `yum install gcc` command, if you want to use a connector that is dependent on GCC.

You can either keep these packages pre-installed on the agent's system, or along with the default repos ensure that the following repos are enabled, so that they get installed during agent binary installation:

For CentOS: `CentOS-Base.repo`

For RHEL: `rhel-7-server-optional-rpm` and `rhel-server-rhsc1-7-rpms` for RHEL
- Note:** If the connector has dependency on any other package or application to work then that package or application will require to be separately installed on the agent. For example, the nmap connector requires the nmap application to be installed, therefore you would require to install this application separately on the agent.

## Process of setting up a FortiSOAR agent

1. Add a secure message exchange.

A Secure Message server is used for communication with FortiSOAR™ Agents or dedicated tenant nodes. You can add both externally deployed secure message exchange or the Default (Embedded) secure message exchange.

If you want to use the local i.e., Default (Embedded) secure message exchange to connect to external agents and run remote actions on various segments of your network or in case of a dedicated tenant, then you must enable the secure message exchange as described in the [Enabling the secure message exchange](#) section. If your secure message exchange is external to your FortiSOAR™ instance, then add the secure message exchange as described in the [Adding a Secure Message Exchange](#) section.
2. Add agents to your FortiSOAR™ instance. See the [Adding an agent](#) section.
3. Install agents. See the [Installing an agent](#) section.

## Minimal permissions required

To configure and install agents:

- **Create**, **Read**, and **Update** permissions on Agents.
- **Read** permissions on Application and Secure Message Exchange.

To use agents to run connector actions:

- **Execute** permissions on Connectors.
- **Read** permissions on Application and Agents.

**Note:** A role named "FortiSOAR SNS" is created on upgrade with the permissions listed above. Upgraded users can assign this role to the admin users to start configuring and using agents for various actions. The "FortiSOAR SNS" role must be added to the **Agent** and **Playbook** appliance roles.

## Enabling the secure message exchange

A secure message exchange establishes a secure channel using which you can relay information to your agent or tenant nodes. A Default (Embedded) secure message exchange configuration is available on every FortiSOAR™ that can be enabled as explained in this section.

To use the Default (Embedded) to connect to external agents, you must enable the secure message exchange using the `csadm secure-message-exchange enable` command. For more information on `csadm`, see the *FortiSOAR™ Admin CLI* chapter in the "Administration Guide."

**Note:** For a production setup, it is recommended that you add and configure a separate secure message exchange for handling scale and high availability.

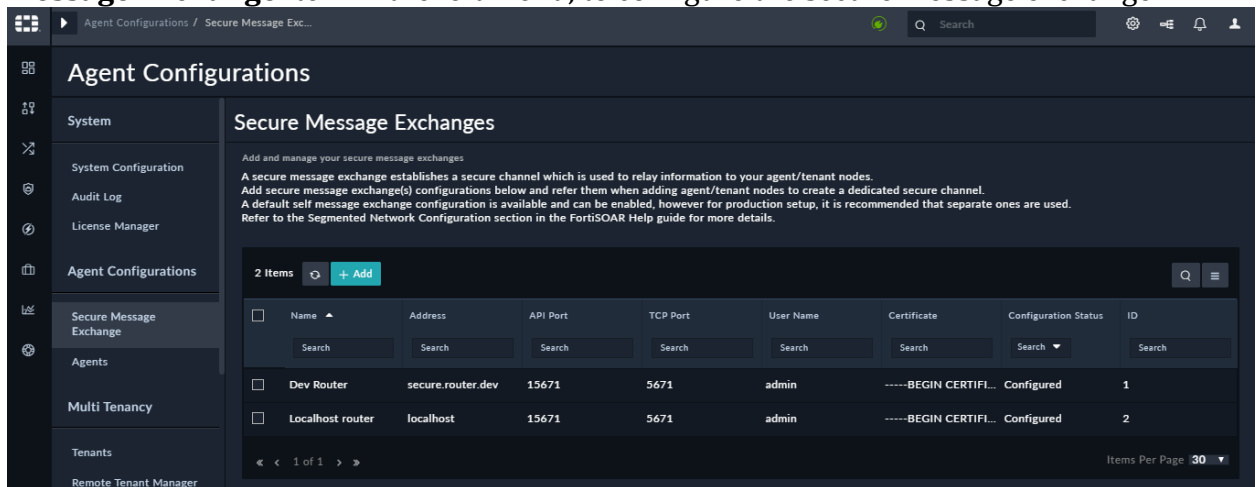
## Adding a Secure Message Exchange

For the procedure on deploying a secure message exchange, see the "Deployment Guide."

Adding a secure message exchange to the base FortiSOAR™ node and then adding the reference of this secure message exchange in the tenant or agent node(s) creates a dedicated secure channel of communication. You can have more than one secure message exchange in the configuration. You can distribute tenants across secure message exchanges based on the geographical locations, scale, or compliance policies of the respective customers.

To add a secure message exchange, do the following:

1. Log on to FortiSOAR™ as an administrator.  
**Note:** Administrator role must have **Create**, **Update**, and **Delete** permissions on Secure Message Exchange.
2. Click the **Settings** (⚙️) icon to open the **System** page.
3. On the **System** page, you will see the **Agent Configurations** section. Click the **Secure Message Exchange** item in the left menu, to configure the secure message exchange.



4. Click **Add** on the **Secure Message Exchanges** page.  
**Important:** To add a secure message exchange and configure tenants, you must have a role that has a minimum of **Create** and **Read** permissions on the **Secure Message Exchange** and **Tenants** modules. To update the details of the secure message exchange you additionally require **Update** permissions on the **Secure Message Exchange** and **Tenants** modules.

To edit the configuration of an existing secure message exchange, click the secure message exchange row whose configuration you want to update. This displays the **Edit Secure Message Exchange** dialog. Update the configuration parameters, as required, in the dialog and click **Update**.

5. In the **Add New Secure Message Exchange** dialog, configure the following parameters:
  - a. In the **Name** field, enter the name of the secure message exchange that you have configured to act as a secure channel of data replication between the FortiSOAR™ node and tenant or agent nodes.
  - b. In the **Address** field, enter the FQHN (Fully Qualified Host Name) of the secure message exchange.  
**Important:** Ensure that the FQHN matches the Certificate Name (CN) or the Subject Alternative Name (SAN) provided in the SSL certificate used to configure the secure message exchange.
  - c. In the **API Port** field, enter the RabbitMQ Management port number that you had specified while configuring the secure message exchange, and ensure that the FortiSOAR™ node has outbound connectivity to the secure message exchange at this port.  
By default, it is set as **15671**.

- d. In the **TCP Port** field, enter the TCP port number that you had specified while configuring the secure message exchange, and ensure that the FortiSOAR™ node has outbound connectivity to the secure message exchange at this port. By default, it is set as **5671**.
- e. In the **User Name** field, enter the username you will use to login to your secure message exchange as an administrator. By default, it is set as **admin**.
- f. In the **Password** field, enter the password you will use to login to your secure message exchange as an administrator.
- g. In the **Certificate** field, copy-paste the certificate text of the Certificate Authority (CA) that has signed the secure message exchange certificate in the pem format. If it is a chain, then the complete chain must be provided. By default, the CA certificate for the FortiSOAR™ self-signed certificate is present at the following location:  
`/opt/cyops/configs/rabbitmq/ssl/cyopsca/cacert.pem`.  
**Important:** If in the future, your secure message exchange certificate expires, and you need to deploy a new certificate, then the new certificate must be copied back to the master node as well as the tenant's router entry.
- h. To save the configuration for the secure message exchange on the FortiSOAR™ node, click **Create**.

**Note:** After you have updated your secure message exchange configuration, the updated configurations might take some time to get reflected.

## Adding an agent

To add an agent, do the following:

1. Log on to your base FortiSOAR™ node as an administrator and click the **Settings** icon to open the **System** page.
2. To add agents, in the **Agent Configurations** section, click **Agents** in the left menu and on the **Tenants** page, click **Add**.  
To edit the configuration of an existing agent, click the agent whose configuration you want to update, which opens the agent record in the detail view. Update the configuration parameters as required.  
If you no longer require an existing agent you can deactivate or deboard an agent. To deactivate an agent, clear the **Enabled** checkbox in the tenant record.  
Deboarding an agent is an irreversible operation which also deletes all data related to that agent from the FortiSOAR™ node. For more information, see [Deboarding Agents](#).
3. On the **Agent** page, click **Add** to open the **Add New Agent** dialog and configure the following parameters for the agent:
  - a. In the **Name** field, enter the name of the agent.
  - b. (Optional) In the **Description** field, enter the description of the agent.

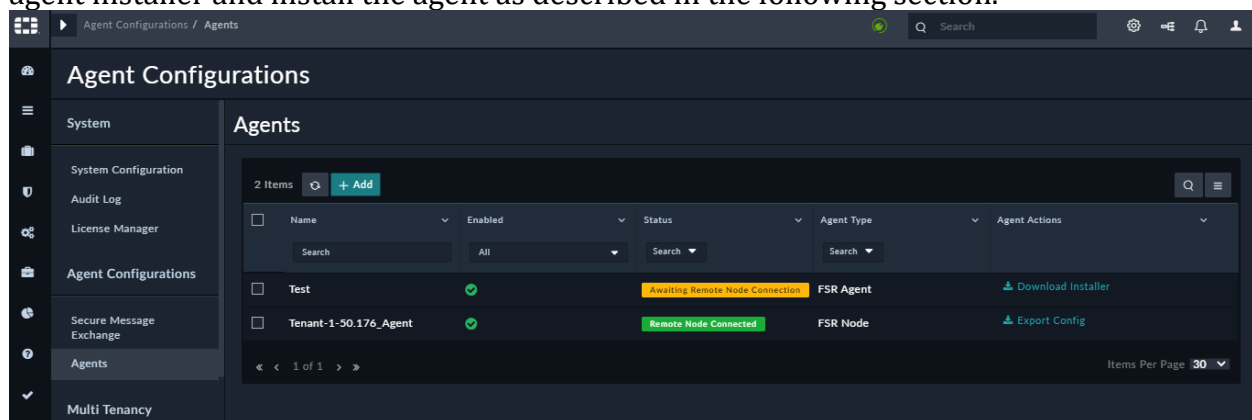


- c. From the **Secure Message Exchange** drop-down list, choose the secure message exchange that you have configured as the secure channel using which you can relay information to your agent.
- d. From the **Owners** drop-down list, select the teams that you want to add as owners of the agent and click **Link Team**.  
If you do not select any team, then the teams that the user who adds the agent belongs to will be associated as owners of the agent. Teams help in governing RBAC for the agent. While running connector actions using agents, users will only see agents that are associated with their teams.
- e. To complete adding the agent, click **Create**.

Once you have completed adding the agent, you will see the status for the agent. Following is the list of statuses that can be displayed:

- **Configuration In Progress:** Process of configuring the agent has begun.
- **Awaiting Remote Node Connection:** Connection between the FortiSOAR™ node and secure message exchange is established and awaiting the connection to the agent.
- **Remote Note Connected:** Agent has been connected to the FortiSOAR™ node using secure message exchange.
- **Configuration Failed:** Agent failed to be added on the secure message exchange.
- **Message Exchange Unreachable:** Secure message exchange is unreachable.
- **Remote Node Unreachable:** Agent is unreachable from the FortiSOAR™ node.

If the connection between Connection between the FortiSOAR™ node and secure message exchange is established, then the **Status** column displays "Awaiting Remote Node Connection" along a **Download Installer** link. Now, you are required to download the agent installer and install the agent as described in the following section.

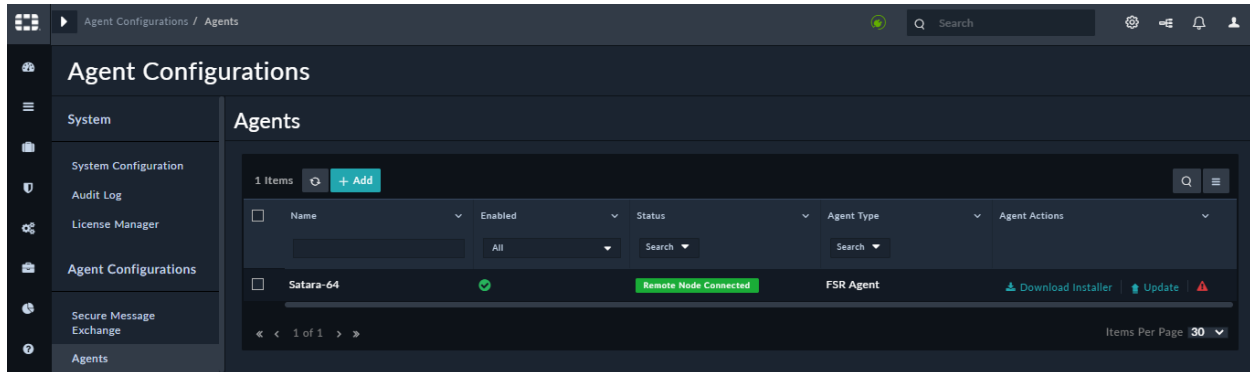


**Figure 28.** Added the agent - Download installer link

In the **Agent Actions** column, you will see either the Export Config link or the Download Installer link. The **Download Installer** link represents a “FSR Agent” and you can use this link to install the agent at a specified endpoint. The **Export Config** link represents a “FSR Node”, i.e., in this case the agent represents a dedicated tenant and you can use this link to export the configuration of the dedicated tenant.

If the Status column displays statuses like "Message Exchange Unreachable" or "Remote Node Unreachable", the Agent Actions column will also display a **Retry** link that allows you to again perform the operation.

From FortiSOAR™ version 6.4.4 onwards, you might also see a **Warning** symbol in the Agents Action column as shown in the following image:



**Figure 29.** Agents Action column - Warning symbol

The **Warning** symbol indicates that the master cannot remotely execute or manage connector actions on the agent. Prior to version 6.4.4., the FortiSOAR™ UI did not provide any indication of remote connector management, and if remote connector management was disabled at the agent, then the master was not notified. Due to this if the master triggers any remote request then that would get ignored by the tenant since the remote operation had been disallowed. Therefore, in version 6.4.4, the **Warning** icon is introduced to indicate when remote connector management is disabled.

To enable or disable remote connector management on the agent, you must have a minimum of Upgrade permission on the Agent module, and to disallow the master from remotely executing connector actions on an agent, ensure that the agent's version must be 6.4.4 and later.

Then, ssh to the agent's VM and edit the `/opt/cyops-integrations/integrations/configs/config.ini` file and set the value of the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter:

- To enable remote connector management, set the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter to `true`.
- To disable remote connector management, set the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter to `false`.

Once you have completed editing the config.ini file and setting the value of the `ENABLE_REMOTE_CONNECTOR_OPERATION` parameter, restart the `cyops-integrations-agent` service. Restarting the `cyops-integrations-agent` service notifies these changes to the master node.

## Installing an agent

Before you install an agent, ensure that you meet all the prerequisites to installing an agent. For more information, see [Prerequisites for installing an agent](#).

To install an agent, do the following:

1. Click the **Download installer** link on the **Agents** page.
2. On the **Prepare and Download Agent Installer** dialog, from the **Include Specified Connectors to install on Agent** drop-down list, choose which connectors you want to include while installing the agent. You can choose from the following options: Do not install connectors by default, Custom, All connectors installed on Master, or Include pre-existing connectors on agent.

Agents use connectors to remotely run actions on a remote network. If you select **Do not install connectors by default**, then connectors are not installed on the agent, except for the "Utilities" connector that is installed, by default, on the agent.

If you select **Custom**, then from the **Select Connectors** drop-down list you have to select the connectors that you want to install on the agent. Note that only connectors that are installed on FortiSOAR™ (master) node can be installed on the agent. If you select **All connectors installed on Master**, then all the connectors that are installed on FortiSOAR™ are installed on the agent.

If you had an agent system on which you had configured some connectors that you required to re-provision, if for example, there were some issues with the agent's system, then you can download the agent installer again, and select the **Include pre-existing connectors on agent** option. Selecting the **Include pre-existing connectors on agent** bundles up the connectors and their configurations of those connectors that were previously installed and configured on the agent.

3. Click **Download Installer**.

Once you click **Download Installer**, the installer file named as `<agent-name>-install.bin` is downloaded on your VM. Copy-paste this installer to the agent VM and install the agent.

The installer installs the following for the agent:

- PostgreSQL database.
- cyops-integrations-agent

After the installation is complete, you should check the status of the `cyops-integrations-agent` service. Also, note that the password for PostgreSQL is the Agent ID.

## Upgrading an agent

You can upgrade an agent from FortiSOAR™ version 6.4.1 onwards.

**Important:** If you have upgraded your base FortiSOAR™ node, then updating your agent to the version of your base FortiSOAR™ node is highly recommended to ensure compatibility with the base product version and to benefit from the latest enhancements. Also, note that

you cannot upgrade your agent node to the latest FortiSOAR™ until you have upgraded your base FortiSOAR™ node.

Before you upgrade an agent ensure the following:

- Ensure that [update.cybersponse.com](https://update.cybersponse.com) is reachable or resolvable from the VM on which you want to install the agent.
- Ensure that the agent status is "Remote Node Connected".

You can upgrade an agent using the following two methods:

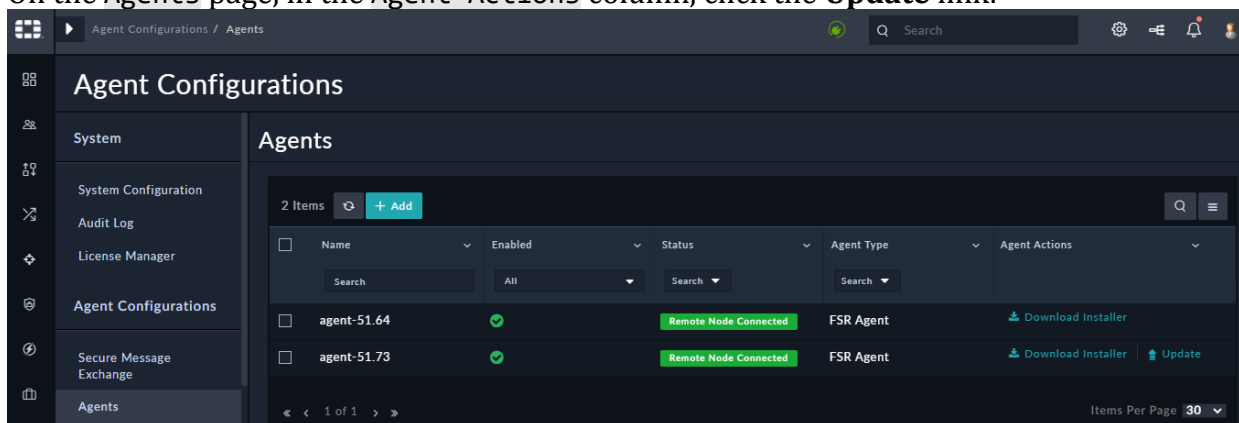
- Automatic Upgrade - Minimum applicable FSR Agent and FSR Node version for automatic upgrade is 6.4.3.
- Manual Upgrade - Minimum applicable FSR Agent version for manual upgrade is 6.4.1.

## Performing an Automatic Upgrade

You can perform an automatic upgrade for a FSR Agent that is on version 6.4.3 (or later).

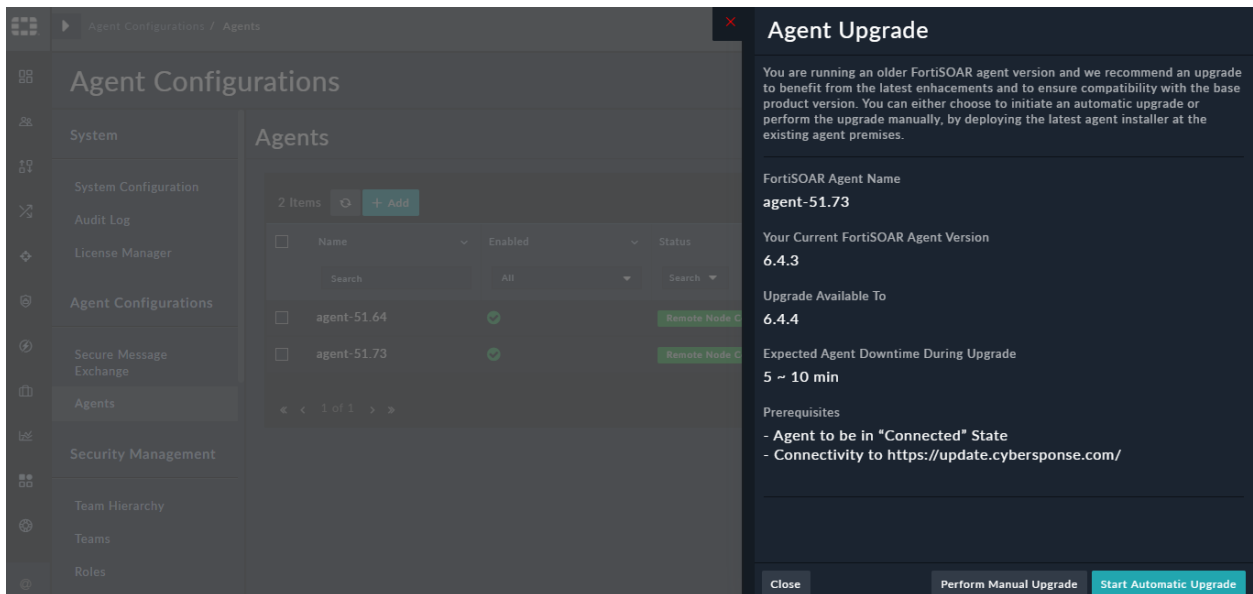
To perform an automatic upgrade, do the following:

1. Log on to your base FortiSOAR™ node as an administrator and click the **Settings** icon to open the **System** page.
2. In the **Agent Configurations** section, click **Agents** in the left menu.
3. On the **Agents** page, in the **Agent Actions** column, click the **Update** link:



Clicking the **Update** link opens the **Agent Upgrade** dialog.

4. The **Agent Upgrade** dialog contains the current version information of your FSR Agent and the version it to which it will be upgraded, as well as other information such as prerequisites to the upgrade and expected downtime:



Click **Start Automatic Upgrade** to display a confirmation dialog, and once you click **Confirm**, the FSR Agent begins to get automatically upgraded. You can see messages related to the upgrade on the same screen and once the FSR Agent is successfully upgraded to the same version as your base FortiSOAR™ node, you will no longer see the **Update** link in the **Agent Actions** column.

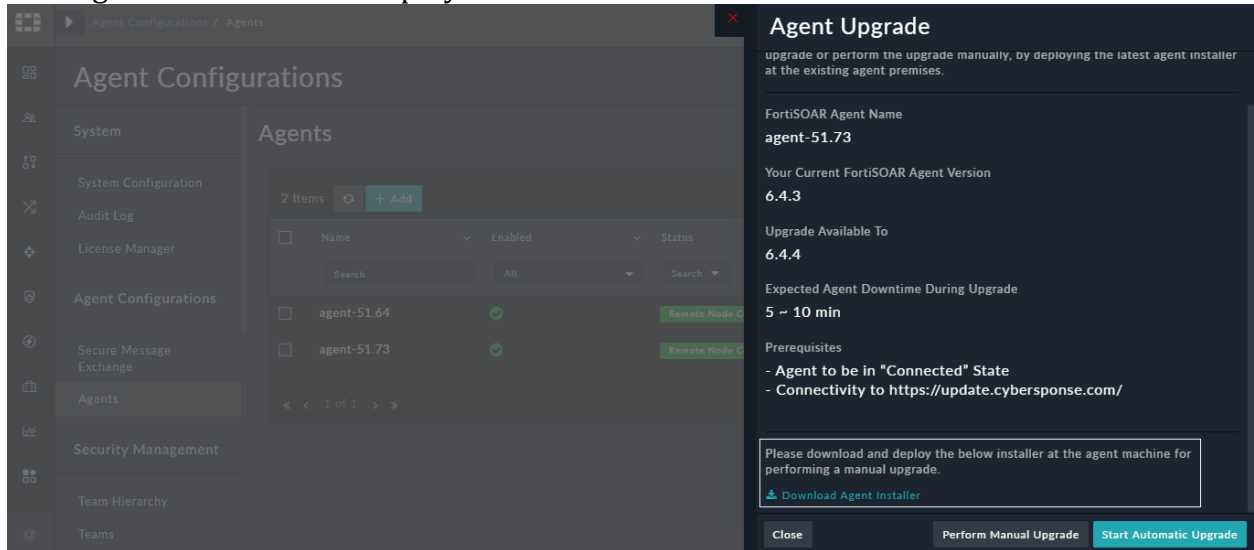
## Performing a Manual Upgrade

You can perform a manual upgrade for a FSR Agent that is on version 6.4.1 (or later). Therefore, if you have a FSR Agent that is on version 6.4.1 and you want to upgrade that FSR Agent to version 6.4.4, then you have upgrade that FSR Agent manually to version 6.4.3, and then you can perform an automatic FSR Agent upgrade from 6.4.3 to 6.4.4 or later.

To perform a manual upgrade, do the following:

1. Log on to your base FortiSOAR™ node as an administrator and click the **Settings** icon to open the **System** page.
2. In the **Agent Configurations** section, click **Agents** in the left menu.
3. On the **Agents** page, in the **Agent Actions** column, click the **Update** link. Clicking the **Update** link opens the **Agent Upgrade** dialog.

- On the **Agent Upgrade** dialog, click **Perform Manual Upgrade**, which in turn displays a message to download and deploy the installer:



- Click **Download Agent Installer** to download the upgrade file named as <agent-name>-install.bin to your VM.
- Copy and paste the <agent-name>-install.bin to your agent's VM (FSR Agent Node).
- SSH to the agent's VM as a **root** user and run the following command:  

```
# sh install.bin or # ./install.bin
```

 Now, your agent is upgraded to the same version as your base FortiSOAR™ node, and the **Update** link is no longer displayed in the **Agent Actions** column.

## FortiSOAR™ Agent CLI

Use the FortiSOAR™ Agent CLI (**csagent**) to perform various administrative functions on the agent such as, importing a connector, starting or stopping services, listing connectors, checking the health of the agent, etc. For more details on the options available with **csagent**, use the help command: **csagent --help**.

## Deboarding Agents

To deboard existing agents, you require to have **Read** and **Delete** permissions on the **Agents** module. Deboarding agents not only deletes the agent, but also removes the list of connectors installed and all the configurations of the connectors that have been installed on the specific agent from the FortiSOAR™ node. Once you delete an agent, you cannot retrieve any information related to that agent, therefore you must be careful while performing this operation.

To deboard an agent, log on to FortiSOAR™ as an administrator and click the **Settings** icon to open the **System** page. Click **Agents** in the left menu and on the **Agents** page, click **Delete**. FortiSOAR™ will display a warning dialog, click **Confirm** on the warning dialog to deboard the agent.

**Important:** Once you deboard a tenant, all the agents linked to that tenant are also deleted.

## Moving an agent to a new secure message exchange

If you have added a new secure message in your environment, and you want to move your agent to the new secure message exchange, do the following on the FortiSOAR™ system:

1. Add the new secure message on your FortiSOAR™ system. For more information, see the [Adding a Secure Message Exchange](#) section.
2. Log on to your FortiSOAR™ node, master node in case of a multi-tenant configuration, as an administrator and click the **Settings** icon to open the **System** page.
3. In the **Agent Configurations** section, click **Agents** in the left menu.
4. Click to open the agent record that you want to move to the new secure message exchange.
5. In the agent record, from the **Secure Message Exchange** drop-down list, select the secure message exchange on which you want to move the agent.
6. Restart the `cyops-postman`, `uwsgi`, and `cyops-integrations-agent` services on the master node, using the following command:  
`systemctl restart cyops-postman uwsgi cyops-integrations-agent`  
After you have completed updating the router information and restarting the services, you must download the agent installer again and reinstall the agent on the agent VM.

## Invoke connector actions using agents in segmented networks

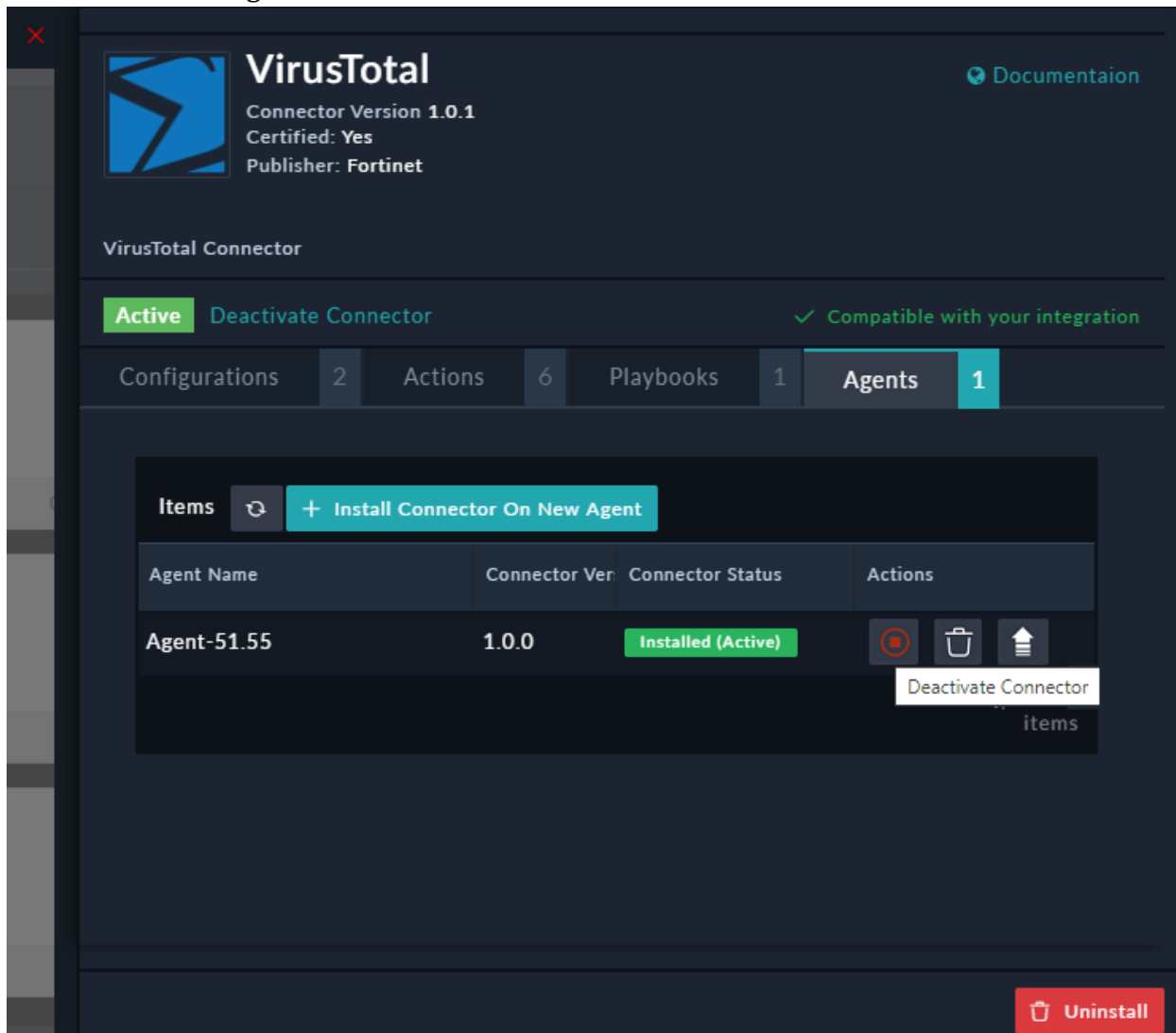
Once you have installed the agent, you can install and configure connectors on the agent and then run remote actions on the agent using connectors.

### Installing a connector on an agent

Connectors that are installed on the FortiSOAR™ instance can be installed on agents. When you are [installing an agent](#) can you choose to install some pre-defined connectors.

1. Log on to FortiSOAR™.
2. On the left navigation pane, click **Automation > Connectors > Installed**.  
**Important:** Only connectors that are installed on the FortiSOAR™ instance can be installed on agents
3. Click the connector that you want to install on the agent, which opens the **Connector Configuration** popup.
4. On the **Connector Configuration** popup click the **Agent** tab.  
To install the connector on a new agent, click **Install Connector on New Agent**, and from the **Agents** dialog, which contains a list of installed agents, select the agent on which you want to install the connector and click **Install**.  
**Note:** The Agents dialog lists only those agents whose Status is "Remote Node Connected."

The **Agent** tab displays the names of the agents on which the connector is installed, the version of the connector installed, and the connector status. You can also use this tab to install that connector on a new agent, and activate, deactivate, delete, or upgrade the connector on the agent:



**Figure 30.** *Connector Configuration - Agent tab*

To install the connector on a new agent, click **Install Connector on New Agent**, and from the Agents dialog that contains a list of installed agents select the agent on which you want to install the connector.

You can activate, deactivate, or uninstall the connector for a particular agent by clicking the **Activate Connector**, **Deactivate Connector**, or **Uninstall Connector** buttons respectively. If the version of the connector on the FortiSOAR™ instance and on the agent is the same, then the **Upgrade Connector** button will not be visible in the agent row. However, the version of the connector on the FortiSOAR™ instance is higher than the version of the connector installed on the agent, then you can upgrade the connector by clicking the **Upgrade Connector** button.



**Note:** Activating, deactivating, uninstalling or upgrading the connector for an agent only activates, deactivates, uninstalls, or upgrades that connector for that particular agent and not for any other agent or the FortiSOAR™ instance.

## Installing a custom connector on an agent

If you want to use a custom connector on the agent, you require do the following:

1. Import the custom connector on your FortiSOAR™ (base) node.
2. Create an agent installer (see [Adding an agent](#)) but do not select the custom connector.
3. Run the agent installer on the agent (see [Installing an agent](#)) and confirm that the agent is successfully installed.
4. Copy the custom connector's .tgz file to the agent's system.
5. Run the following commands to install and configure the custom connector:
  - a. `csagent --option import`  
For example, `csagent --option import --name sns_con --version 1.0.0 --bundle <path_to_tgz>`
  - b. `csagent --option configure`  
For example, `csagent --option configure --name <conn_name> --version <conn_version>`  
To set the default configuration for the connector, use the `csagent --option configure --default` command.

## Configuring connectors

You can configure connectors for the current FortiSOAR™ node, the agent, or both. You can configure the connector on the current node (Self) or on a remote Agent node (Agent) by clicking the **Self**, which is the default, or **Agent** buttons besides **Target**. You can configure multiple configurations for a connector on both the current node and the agent node.

**Important:** Configuration details, such as passwords, credentials, or other sensitive data can be stored by your administrator using "Password Vault" or "Secrets" (deprecated). However, you will not be able to use these stored credentials to configure a connector on an agent since vaults and secrets do not work on agents.

To configure connector, on the **Connectors** page, click the connector that you want to configure to open the **Connector Configuration** popup in which you can add connector configurations. To configure and execute connector actions on the "Self" node, click **Self**, which is the default, if you are configuring the connector for the first time or if you want to add a new configuration, then click **Add new configuration** from the **Select Configuration** drop-down list and then add the name of the configuration and specify the configuration parameters. If you want to update an existing configuration, then select the configuration from the **Select Configuration** drop-down list and update the configuration parameters. If there is only one configuration, then that configuration will be selected automatically.

To configure and execute connector actions on the "Agent" node, click **Agent**, and from the **Select Agent** drop-down list select the agent on which you want to run the connector actions. If there is only one agent installed, then that agent will be selected automatically.

**Note:** The Select Agent drop-down lists only those agents whose Status is "Remote Node Connected."

If you are configuring the connector for the first time or if you want to add a new configuration, then click **Add new configuration** from the **Select Configuration** drop-down list and then add the name of the configuration and specify the configuration parameters. If you want to update an existing configuration, then select the configuration from the **Select Configuration** drop-down list and update the configuration parameters. If there is only one configuration, then that configuration will be selected automatically. For more information on configuring connectors, see the *Introduction to connectors chapter* in the "Connectors" Guide.

## Running remote actions

Once you have completed configuring the connectors, you can run remote actions on the agent either directly on the agent, or by using playbooks, or by running connector actions on records.

In case of playbooks, you can add the connector as a step and then choose whether to execute that step on the current FortiSOAR™ node or remotely on the agent node by clicking the **Self** or **Agent** buttons besides Target. By default, **Self** is selected, which means that the action will run on the current FortiSOAR™ node, then you must select the configuration using which you want to run the action since the FortiSOAR™ node can have multiple configurations.

From version 6.4.3 onwards, Listener-based connector configuration on the agent is also supported. Listener-based connectors listen for live events on a server, and then these events are notified to FortiSOAR™ by triggering a playbook. For example, the Exchange connector, which has enabled its listener-based configuration starts a live listener for the specified email account. Therefore, if any new emails are received in the configured account or folder, the connector fetches that emails and triggers playbooks, such as the ingestion playbook, which is specified in the configuration.

**Important:** For Listener-based connectors to work and trigger playbooks such as triggering the data ingestion playbook, the agent appliance must have "Execute" permissions on 'Playbooks'.

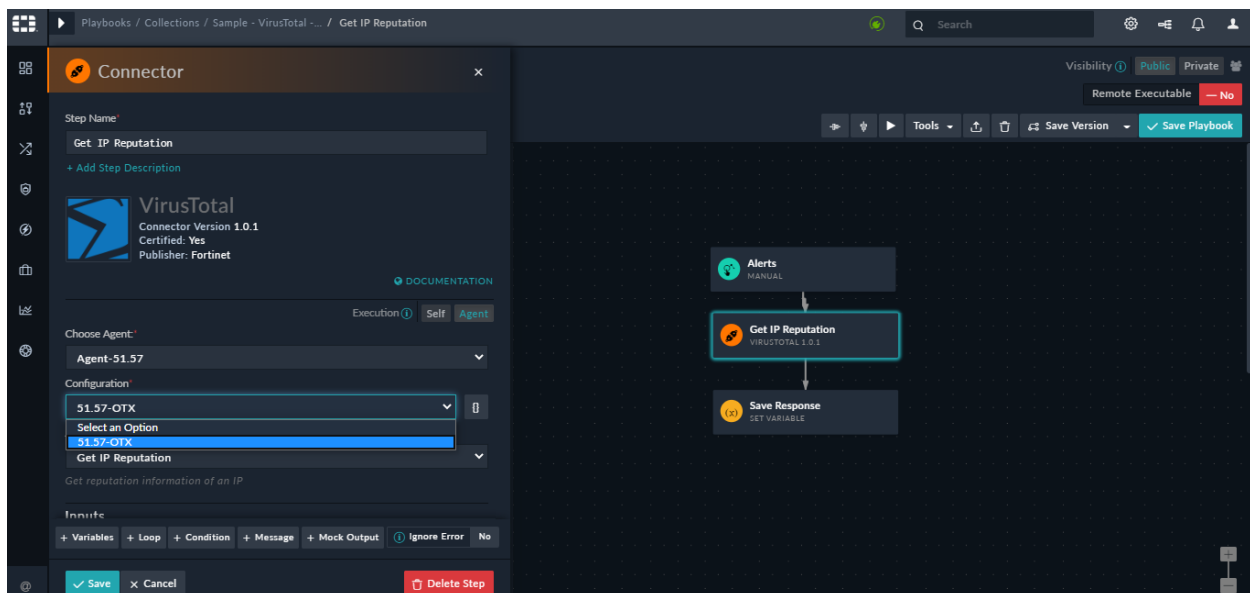
From version 6.4.3 onwards, file-based operations are supported on the agent, enabling you to perform connector actions that require file resources from FortiSOAR™. For example, the "Get Unread Emails" action of the Exchange connector, has an option where you can choose to upload an attachment received in an email to FortiSOAR™. You can perform the following operations:

- Upload a file to FortiSOAR™

- Download a file from FortiSOAR™.
- Support of any generic API request for GET, PUT, POST, and DELETE methods  
**Note:** To perform the operations, roles having appropriate permissions to the required modules must be assigned to the agent. For example, to download an attachment, the agent would require a minimum of 'Read' permission on the "Attachment" module.

However, note that any file that is downloaded on the agent using the download file action of the Utilities connector will not be available to any of the next steps in the playbook. For example, if you create a playbook add then add the Utilities connector operation "File: Download File From URL" step for an FSR Agent configuration, add the download URL, and save the step. Next, you add the "File: Create Attachment From File" step in which provide the file reference from "Download" step and save and run the playbook. The playbook will fail with an error such as "Connector step is failing with error 'Invalid input :: Given filename/filepath /tmp/f68ab00fb7da4dfd9db4bb95abb1471e doesn't exists' ". This is expected behavior since when a file download operation is performed on an FSR agent, the operation cleans the file when the response is returned to the base FortiSOAR™ node. Therefore, if any following step expects the downloaded file to be present at the agent will cause that step to fail.

You can click **Agent** and then from the **Choose Agent** drop-down list, you can select the agent on which you want to run the action and you must also select the configuration using which you want to run the action since agents can have multiple configurations. If you want the agent configuration to be resolved dynamically, you can click **{}** in the **Configuration** field and then specify the connector configuration by either typing the connector configuration name or ID or specifying a Jinja variable that contains the connector configuration name or ID.



**Figure 31.** Playbook Designer - Adding execution options for the Connector step

In case of a multi-tenant configuration on the master node, if you click **Agent**, then you can also select the **Pick From Record's Ownership** option in the **Choose Agent** drop-down list, which would then read the record of the tenant and accordingly select the agent to be run the action.

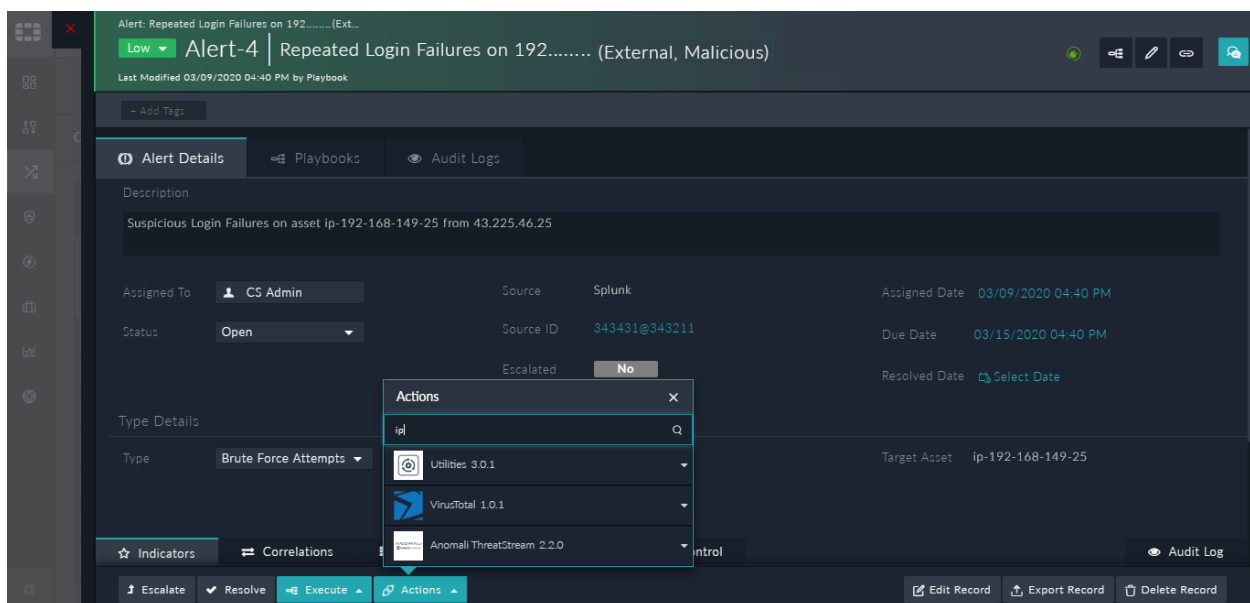
If you have only one configuration for the connector or have specified a default configuration, then that configuration automatically gets selected.

**Note:** The **Configuration** drop-down lists only those agents whose Status is "Remote Node Connected."

Next, you can select the action that you want to run, for example "Get IP Reputation", and provide the necessary input parameters for this action and save this step. Then you can continue to build the playbook as per your requirements.

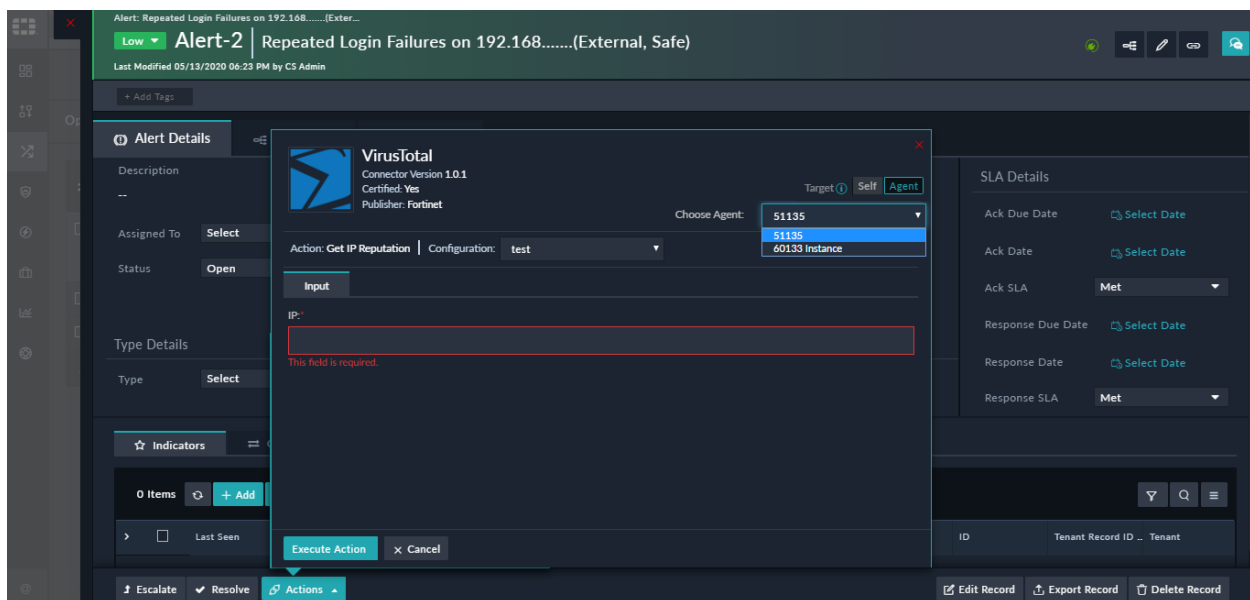
Once you have developed the playbook, which should execute on a remote agent, and you execute the same, you will observe in the Executed Playbook Log, that the playbook goes into the "Awaiting" state when it reaches the Connector step. This happens because this step is being executed on the remote agent and then the playbook is consuming the result received back from the remote agent for further processing.

Similarly, you can run connector actions on records remotely for agents. To run connector actions on records, open the detail view of a record, for example, the detail view of an alert record and click the **Actions** button. The Actions list will display the active and configured connectors. Search for actions that you want to perform using the **Search Action** box. For example, if you want to search for a reputation of an IP address, then you can type **IP** in the **Search Action** box, and the connectors that have any action related to an IP address will be displayed:



**Figure 32.** Searching for actions

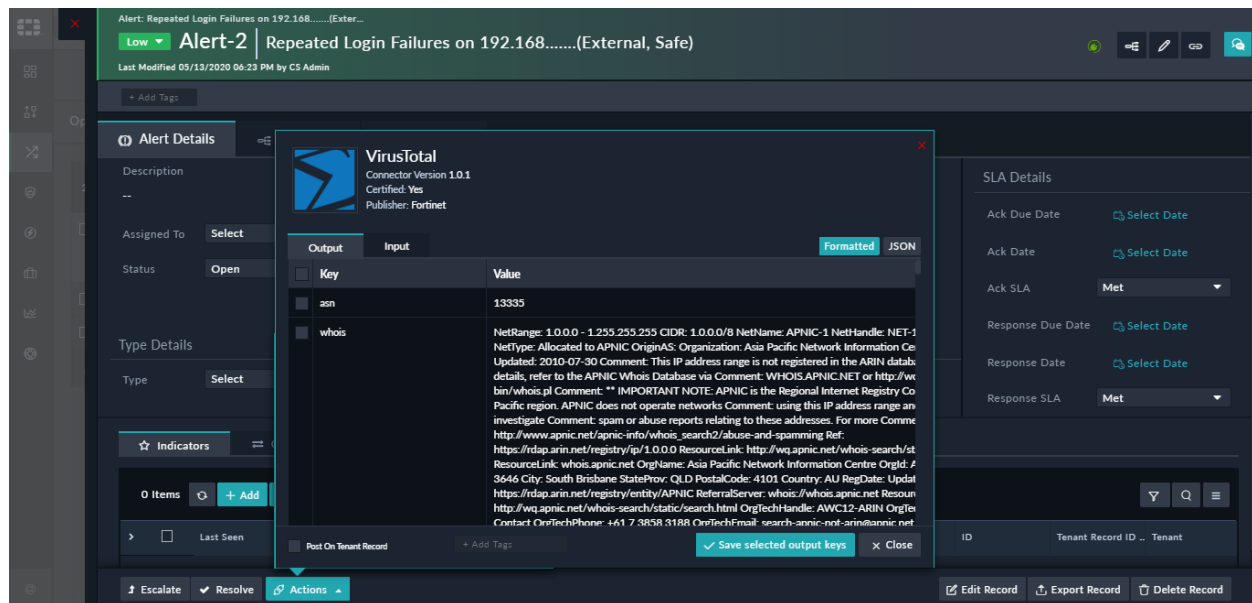
As shown in the above image, VirusTotal, Anomali Threatstream, and the Utilities connector have "IP" in their actions. Click the down arrow to view the actions associated with IP for each connector. For example, if you click VirusTotal, you will see the "Get IP Reputation" action, which for example we want to perform on the remote agent. Select the **Get IP Reputation** action, which displays the VirusTotal dialog. From version 6.4.1 onwards, you are required to specify whether you want to run the action on the current FortiSOAR™ node or remotely on the agent node by clicking the **Self** or **Agent** buttons besides Target. By default, **Self** is selected, which means that the action will run on the current FortiSOAR™ node, then you must select the configuration using which you want to run the action since the FortiSOAR™ node can have multiple configurations. If you click **Agent**, then you can select the agent on which you want to run the action and you must also select the configuration using which you want to run the action since agents can have multiple configurations.



**Figure 33.** Specifying the execution mode for the action - Agent Mode

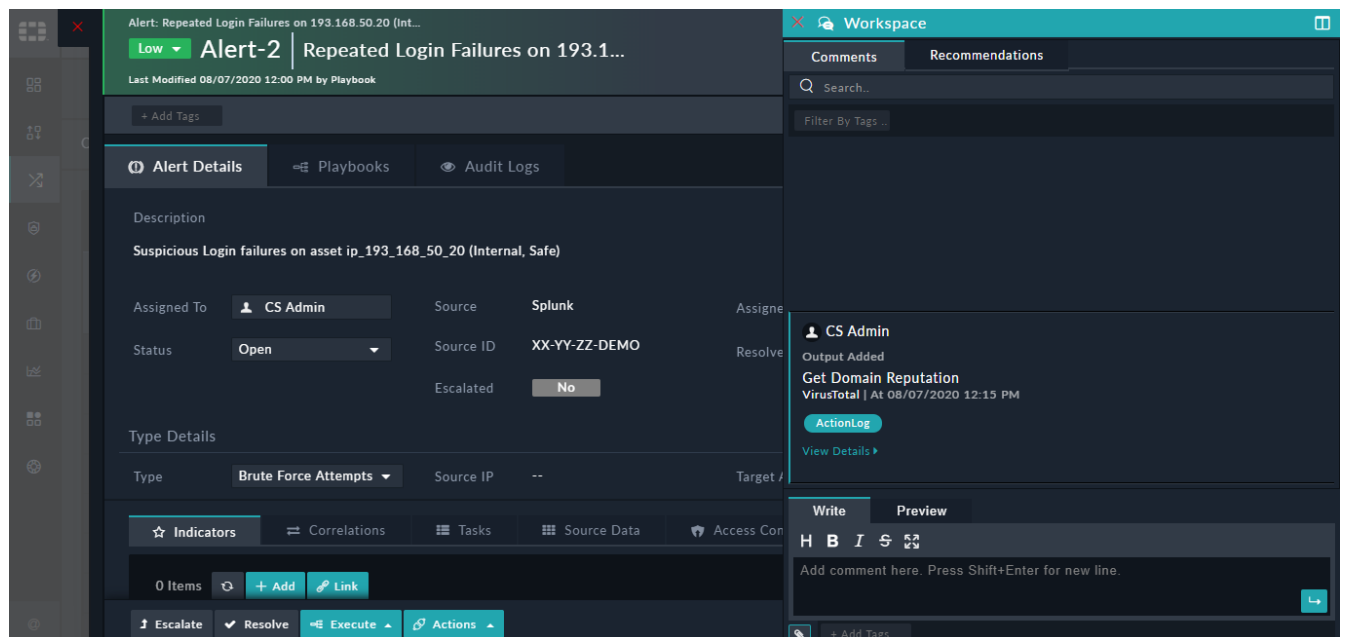
For our example, select **Agent**, then in the Input tab either enter an IP address or use the value of a record field and click **Execute Action**. The action will then be executed on the remote agent, and you will be able to see the output of the action in the **Output** tab.

**Note:** RBAC is applicable for Agents, i.e., if you do not have appropriate permissions for Agents, then agents will not be visible for running connector action on records.



**Figure 34.** Output tab containing results of the action executed on the remote agent

Once you run the connector action, the output the action is displayed in the collaboration panel as shown in the following image:



**Figure 35.** Executed action output in collaboration panel

From version 6.4.3 onwards, if you run the connector action on the agent, then collaboration panel also displays the name of the agent after the connector name. For example, "VirusTotal on <agent name> | At 08/07/2020 12:15 PM".

For more information on 'Running connector actions on a record', see the *Working with Modules - Alerts & Incidents* chapter in the "User Guide."

## Troubleshooting

### Files to be used for troubleshooting

Use the "connectors.log" to troubleshoot FortiSOAR™ connectors. This log is located at: `/var/log/cyops/cyops-integrations/connectors.log`.

Use the "config.ini" file to update the connector settings, such as changing the logging level of connectors. This file is located at: `/opt/cyops-integrations/integrations/configs/config.ini`. Once you complete updating the "config.ini" file, you must restart the `cyops-integrations-agent` service.

Use the "agent\_config.yml" file on the agent instance for details such as the FortiSOAR™ node to which the agent requires to be connected, the secure message exchange to be used, etc. This file is located at: `/opt/cyops-integrations/integrations/configs/agent_config.yml`.

### Deactivated agent does not come back to the connected state even after activating the agent

Activating a deactivated agent does not change its connection state from "Remote Node Unreachable" to "Remote Node Connected" if the live connection mechanism does not correctly reflect the status.

#### Resolution

Restart the `cyops-integrations-agent` service on the agent.

### Agents configuration page displays a "Agent <Agent UUID> does not exist" error when you click the Export Config link

This issue occurs if you have removed the default admin team, i.e., "SOC Team" and have not assigned the new admin team to the agent and playbook appliance.

#### Resolution

Recommended not to remove the default "SOC Team". However, if you have removed the SOC Team, then you must create a new admin team and assign that team to the agent and playbook appliance. To assign the new admin team to the agent and playbook appliance, click **Settings > Appliances** to open the Appliances page, and then click the **Agent** row to edit the agent appliance page. On the Edit Appliance page, in the Team and Role section, in the Teams table, select the new admin team to assign the same to the agent appliance. Perform the same steps for the playbook appliance.



## Security Management

FortiSOAR™ gives you the power to assign levels of accessibility to users with Role-Based Access Control (RBAC) combined with Team membership. You can grant access to specific modules in FortiSOAR™ to users based on their Role Permissions. Users exercise their permissions in conjunction with their Team membership(s). Appliances are governed by the same authorization model.

The security model within FortiSOAR™ achieves the following four essential security goals:

- Grants users the level of access necessary based on your desired organization structure and policies.
- Supports sharing of data for collaboration while still respecting your team boundaries.
- Supports data partitioning and prevents users from accessing data that is not explicitly meant for them.
- Restricts external applications and scripts (appliances) from using the API beyond the requirements for accomplishing the desired RESTful actions.

The following sections describe several vital concepts you must keep in mind while working with the FortiSOAR™ security model. In-depth discussion and examples might be found in the individual Knowledge Base sections.

## Important Concepts

### Authentication versus Authorization

The FortiSOAR™ security model consciously treats authentication and authorization separately.

- Authentication defines your ability to log in and access FortiSOAR™. FortiSOAR™ enforces authentication based on a set of credentials.
- Authorization governs users' ability to work with data within FortiSOAR™ *after* authentication is complete. You control authorization by assigning teams and roles to users.

This is an important distinction since when you are setting up user accounts, you must always define both the authentication and desired authorization for a user. Otherwise, once a user logs onto FortiSOAR™, the user might be presented with a blank screen due to lack of authorization.



## Users and Appliances

Users represent a discrete individual human who is accessing the system. Users are differentiated from Appliances in that they receive a time-expiring token upon login that determines their ability to authenticate in the system. The Authentication Engine issues the token after users have successfully entered their credentials and potentially a 2-factor authentication. By default, tokens are set to have a lifespan of 30 minutes before being regenerated.

The default 2-Factor authentication consists of a username and password for the primary authentication, and a unique code sent using an SMS or Voice message for the secondary authentication. The secondary authentication method is not mandatory but highly recommended. You can configure the authentication methods on a per-user basis. Use the **System Configuration** menu to configure the system defaults for the secondary authentication.

**Tip:** The 2-Factor Authentication can be different for each user, but you can set it at a default preference level across the system. You can also allow a non-admin user to update their own 2-Factor Authentication mechanism. However, this is not recommended.

Appliances represent non-human users. Appliances use Hash Message Authentication Code (HMAC) to authenticate messages sent to the API. HMAC construction information is based on a public / private key pair. Refer to the “API Guide” for instructions for generating the HMAC signature.

**Note:** For HMAC authentication the timestamp must be in UTC format.

## Teams and Roles

Teams and Roles are closely aligned with a data table design. Teams own specific records, which are rows in a table. Roles govern permissions on the columns within that table around Create, Read, Update, and Delete (CRUD) activities.

Teams define ownership of discrete records within the database. A record can have more than one Team owner. Users can belong to multiple teams allowing them to access all records, which are owned by their assigned teams.

Roles define users’ ability to act upon data within a CRUD permission set on any module in the system.

**Note:** You must be assigned a role that has CRUD permissions on the Security module to be able to add, edit and delete teams and roles.

## Security Management Menus

The Security Management Administration menu is split into the following areas:

### Team Hierarchy

Use the **Team Hierarchy** menu to edit the relationships between teams defined within the system. You can also add and delete teams using the Team Hierarchy page.

### Teams

Use the **Teams** menu to add new teams and edit user membership in bulk within each Team. You can also define membership within teams on an individual basis, using the individual user or appliance profile.

### Roles

Use the **Roles** menu to create and define roles within the system. You assign roles based on CRUD permissions defined across all modules. You can assign roles in the User or Appliance profiles only. Currently, you cannot bulk assign roles.

FortiSOAR™ implements RBAC for playbooks; for example, for uses to run playbooks, administrators require to assign roles that have **Execute** permission on the **Playbooks** module to such users.

**Note:** Users who do not have Execute permissions will not be shown the **Execute** buttons for the module records, for example alert records. Execute actions include actions such as **Escalate**, **Resolve**, or any actions that appear in the **Execute** drop-down list.

### Users

Use the **Users** menu to create and manage existing users. Each user has a profile with contact information including email and phone numbers plus additional reference information. You can assign teams and roles to users and control a user's state from the user's profile. User states are **Active**, **Unlocked**, **Inactive**, and **Locked**.

**Note:** You must be assigned a role that has Create, Read, and Update (CRU) permissions on the People module to be able to add users and edit their user profiles. You cannot delete a user using the FortiSOAR™ UI, though you can make a user "Inactive" to stop that user from using the system. However, you can delete users using a script, for more information, see the [Delete Users](#) script.

## Appliances

Use the **Appliances** menu to create and manage Appliances, which use the HMAC authentication model. Appliances are also governed by the same authorization model as users, which means that you must add the appliances to a team, and they must be assigned a role to perform any actions within the system.

## Authentication

Use the **Authentication** menu to configure various authentication settings in FortiSOAR™, including setting session and idle timeouts and settings options for user accounts. You can also setup and manage the LDAP / AD integration and Single Sign-On (SSO) integration within your environment. When you use an external server to perform authentication, you must have an administrative username and password to perform searches to import users. FortiSOAR™ supports the FreeIPA LDAP authentication.

FortiSOAR™ supports the following methods of authentication: Database users, LDAP users, and SSO.

**Note:** Even if you configure SSO, you can still provision database and LDAP users.

## Password Vault

Use the **Password Vault** menu to manage integrations with external vaults such as "Thycotic Secret Server" and "CyberArk" that are used by organizations to securely store their sensitive data and credentials. You can also use the **Password** field in the connector configuration instead to securely store and manage sensitive data, such as keys, API Keys, tokens, or credentials.

## Configuring Team Hierarchy

Teams represent groups of "owners." If you are a member of a Team that owns a record, then you can apply any Role permissions you have on that record.

There is no direct connection between your Team and Role. If your Team or Teams own a record, you can do whatever you are permitted to do by your Role or Roles. If you are on multiple Teams, you have the permissions provided by your Roles across all those Teams.

Teams only provide ownership of records. Team Relationships extend ownership from one Team's members to another Team's members. Team Relationships are almost a form of "sudo" to borrow from Linux concepts, where you are effectively acting as if you were a member of another Team though you might not be explicitly on the roster of that Team.

*Team Relationships do not govern any user permissions. A user's Role or Roles determines their permissions. If you have extended ownership of a record AND sufficient privileges for that record module, then you can exercise those permissions on the extended ownership record.*

If your Team has the appropriate relationship, you can work with a record owned by another Team as if you were on that Team, even though your Team may not be identified as an owner.

*All user actions in the system are audited, so there is no way for a user to work on a record from another team through a relationship that is not known and recorded.*

## Relationships

Teams govern record ownership within the FortiSOAR™ Security Model. Team Hierarchy reflects how team ownership relates between discrete teams.

Use the Team Hierarchy editor to define team relationships in accordance with each team's relationships with other teams in the system. The possible team relationships are shown in the following table:

Relationship Type	Description
Parent	Parent Teams are virtual owners of the records of the Child Team. A Parent team can act on those records as if they were a member of the Child Team.
Sibling	Sibling Teams can act on each other's records as if they were each members of the same team.
Child	Child Teams are the opposite of Parent Teams. Members of the Parent Teams can act on the records owned by the Child Team, but members of the Child Team cannot act records owned by the Parent teams.

A simple organization chart cannot capture the relationships in this definition. The real structure looks more like a mind map. This was a conscious design decision to support more advanced Team relationship use cases, such as allowing for internal investigations among existing users without alerting the user and providing Legal personas with their own permissions during Incidents.

Records created by 'nth' level of team hierarchy will be visible to parent teams. For example, records created by grandchildren teams will be visible to the grandparent teams.

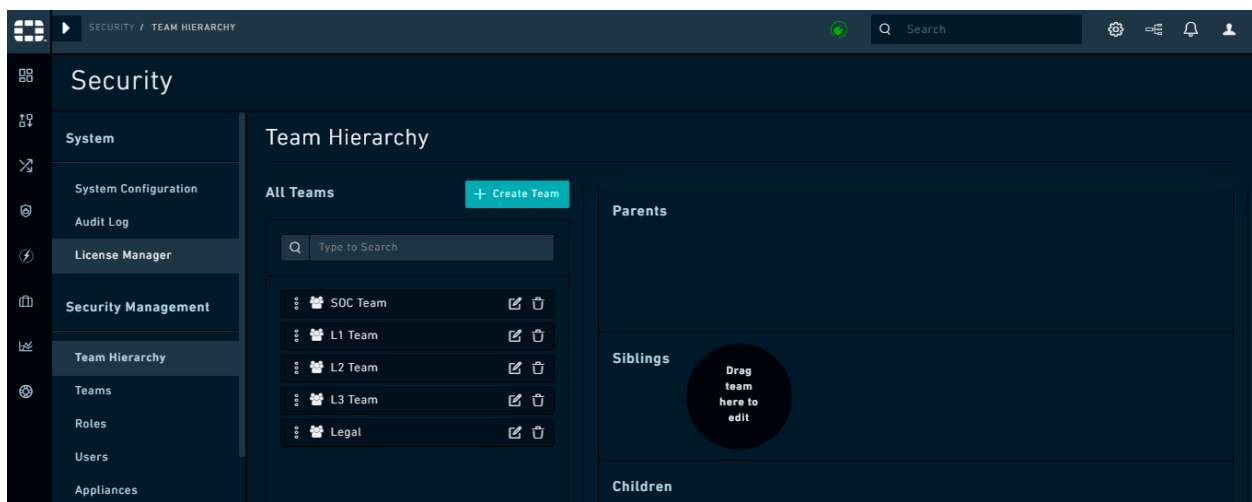
There is **no inheritance** in relationships among Teams or implications from one Team's relationship to another. That means if two teams are Children of a Parent, this does not

mean that the Children are Siblings to each other. If you want them to be Siblings, then you must explicitly define them as Siblings.

## Using the Editor

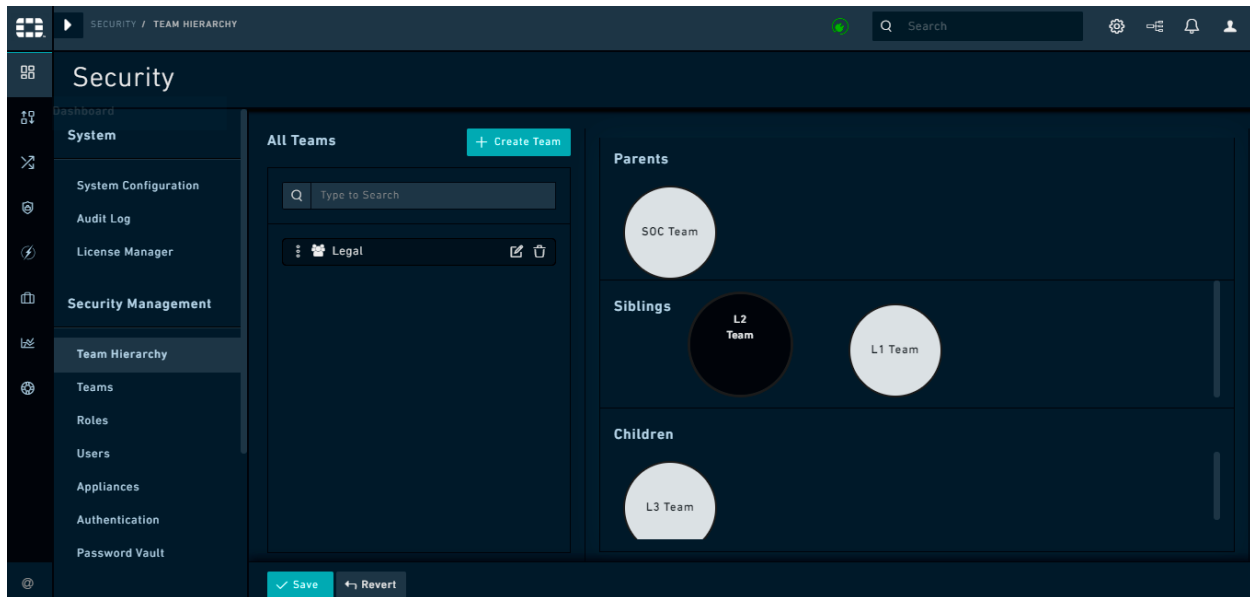
The Team Hierarchy Editor is built to centralize around one team at a time and to define how that Team relates to all other teams in the system. The Central Team is referred to as the “Team in Focus” for this document. Click **Settings > Team Hierarchy** to open Team Hierarchy Editor.

The Team Hierarchy Editor has the All Teams menu and three swim lanes used to define the three relationship types, which are Parent, Sibling, and Child.



**Figure 36.** *Team Hierarchy Editor*

To edit the relationships of any team, you must first bring that team in focus. To bring a team in focus, you must drag and drop that team to the **Drag team here to edit** area or double click that Team’s title in the **All Teams** menu.



**Figure 37.** Team Hierarchy Editor-Team in focus

Once you have put a Team ‘in focus’ on the Hierarchy Editor, the relationships that the team in focus has with all other teams is displayed in the respective swim lanes. For example, in the image above, the team in focus is the **L1 Team**. The L1 Team has SOC Team as the Parent team, L2 Team as its Sibling team and L3 Team as its Child team.

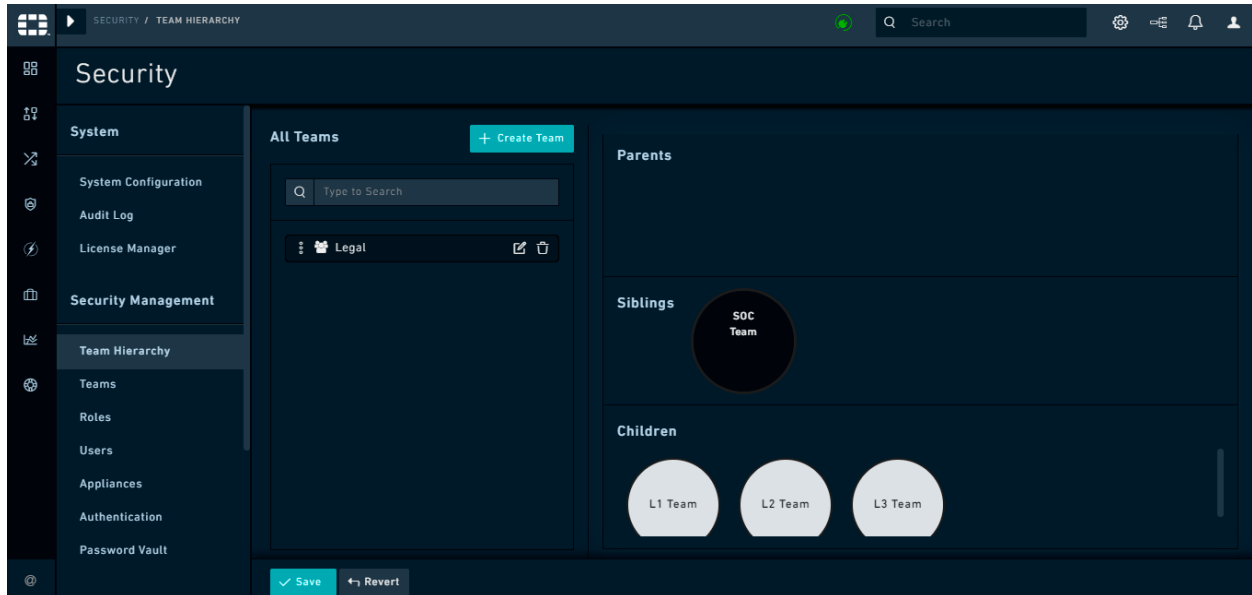
To edit the relationships, drag and drop Team bubbles or the Team titles in All Teams onto the appropriate swim lane. Changes are staged until you click **Save**. Once you click **Save**, changes immediately go into effect.

Following is an illustrative example of what is possible in this model:

## Example

The SOC Team is the Parent of L1, L2, and L3 so the members of the SOC team can act across all records of the L1, L2, and L3 teams as if they are a member of all teams.

*Note you can achieve the same result by adding managers to every team in the organization. However, managers would then never be able to own any records exclusively.*



**Figure 38. SOC Management Team**

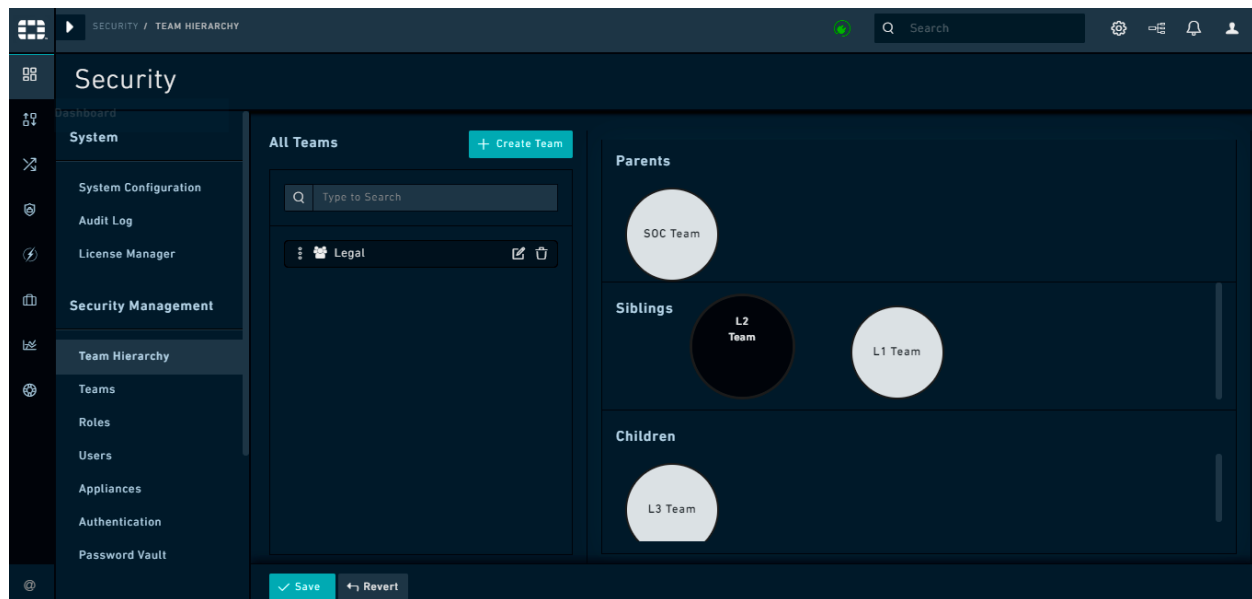
The Legal Team is unrelated to all other Teams in this case, which means that the SOC Team team is isolated from all the Legal Team’s records and vice versa. If the Legal Team were related to the SOC Managers team, you would have seen the relationship in one of the swim lanes.

*The Security Module governs the Role for editing all Teams and Team hierarchies. Anyone with Read access to the Security Module can see all the Teams and Roles within the system. We recommend you provide Security Module permissions with caution as anyone with the Role can see any relationship in the system and would be alerted if any investigation into their activities were initiated at the Team level.*

To summarize the relationships in this view, the SOC Managers:

1. Effectively own all records of L1, L2, and L3
2. Own none of Legal

Now let’s turn to a different team. If you were to focus L2 Team, you would find a slightly different case. We know that the SOC Team are a Parent Team, so we expect to see that relationship inverted. Beyond the relationship between SOC Team and the L2 Team, no other relationships are implied until you put L2 as the Team in Focus.



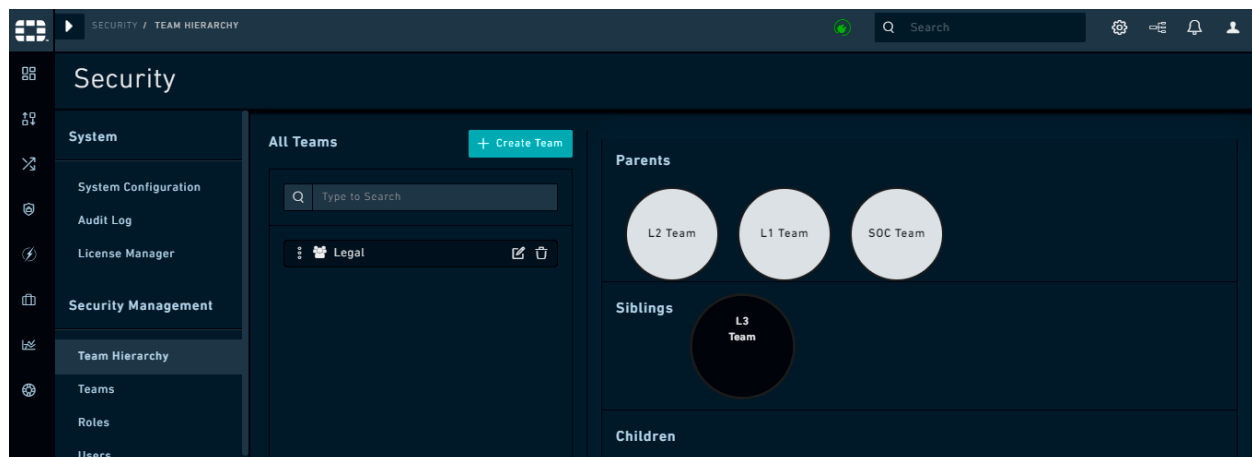
**Figure 39. L2 Team**

When L2 is the Team in Focus, you see that there is another set of relationships governing that Team. The L1 Team is a Sibling of L2, though **that is not** because the Teams are both Children of the SOC Managers. The Sibling relationship has been explicitly defined between L2 and L3. You also see that the L3 Team is a Child of L2.

To summarize the relationships in this view, the L2 Team can:

1. Effectively own all records of L1 and L3
2. Own none of SOC Managers records

The final piece of the example comes from placing L3 as Team in Focus. We know some things already about L3, namely that the SOC Team and L1 Teams are Parent Teams. But we do not know about L2.



**Figure 40. L1 Team**



When L3 is in focus, we see the expected relationships between the SOC Managers and L2 Teams, but we now see that L1 is also a Parent.

To summarize the relationships in this view, the L3 Team can:

1. Effectively own only their own records
2. Own none of SOC Managers, L2, or L1 records

## Configuring Teams

Use the **Teams** page to manage members of a team centrally. You can assign a user to multiple teams; in fact, you can assign a user to be a part of all the teams.

By default, FortiSOAR™ has at least one team in place after installation, the **SOC Team**. We recommend that you do not modify or delete the default teams and instead add new teams, as per your requirements.

There is no limit to how many Teams you can have in the system. Teams do not necessarily have to represent a specific team within your organization, but instead, Teams represent a group of users who own a set of records. In this way, you can think of Teams as row ownership within a table. The records are rows, and at least one and potentially more than one Team must own that row.

**Important:** Whenever you add a new team, you must update the Playbook (called **WFUSER** in previous versions) assignment. **Playbook** is the default appliance in FortiSOAR™ that gets included in a new team. Only a user with **CRUD** access to the **Appliances** module can update the **Playbook** assignment, to ensure that the appliance has the necessary role to perform data read or write to modules. If the **Playbook** does not have appropriate permissions, then Playbooks will fail.

## Editing Teams

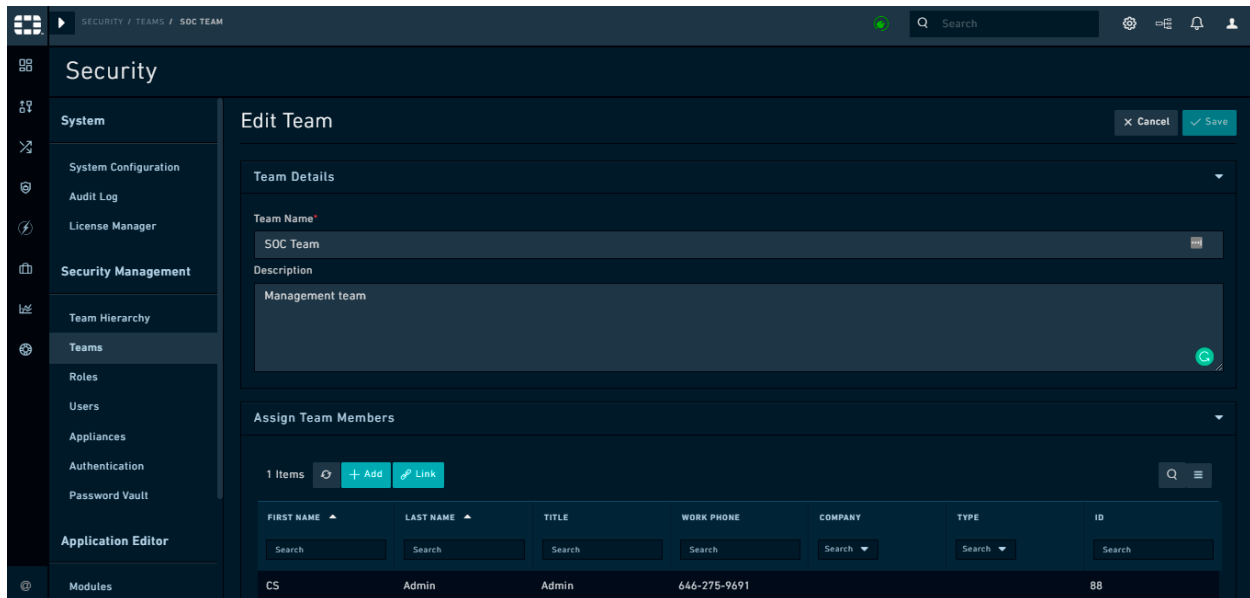
Click **Settings > Teams** to open the **Teams** page. Use the Team Editor to create new teams and to assign users in bulk to teams. You can quickly move users between teams by selecting users who are designated to be Team Members. You can use filtering and searching techniques to assign users to teams easily.

You can perform the following operations on the Teams page:

- Add a team
- Delete a team
- Clone a team
- Edit team details, including editing the name and description of the team and changing the assignment of users within a team

To Delete or Clone a team, on the **Teams** page, select the team you want to delete or clone, and click **Delete** or **Clone**.

To edit a team, on the **Teams** page, click the team you want to edit. On the **Edit Team** page, you can change the name and description of the team and edit members. Members of a team are “linked” using the **Link** button on the **Assign Team Members** grid.



**Figure 41.** Team membership page

To add a user and then immediately assign that user to a team click **Add**.

To add members to a team, click **Link**, which brings up the **Change Relationships** modal window. The Change Relationships window displays all the users within the system. Click the checkbox on the user row to add the user to the team. To remove members from a team, click the checkbox on the user row. Click **Save Relationship** to complete your actions and add or remove members from a team.

Team membership takes effect immediately upon saving across the system.

CHANGE RELATIONSHIPS

3 of 2 selected

<input checked="" type="checkbox"/>	FIRST NAME ...	LAST NAME ...	TITLE	WORK PHONE ...	COMPANY	TYPE	ID
<input checked="" type="checkbox"/>	New	User					321
<input checked="" type="checkbox"/>	CS	Admin	Admin	646-275-9691			88

1 of 1
Items Per Page 30

Cancel Save Relationship

**Figure 42.** Team membership editing

## Configuring Roles

The Roles menu allows you to define and modify all the roles within the application. Roles are not hardcoded in the system; therefore, Role editing is a sensitive permission and must be carefully governed by system users.

**Important:** Any user that requires to work with FortiSOAR™ and records within FortiSOAR™ must be assigned a Role with a minimum of Read permission on the Application, Audit Log Activities, and Security modules.

Use the Role Editor to add and edit RBAC permissions within FortiSOAR™. Role permissions are based on the Create, Read, Update, and Delete model (CRUD). Each module within FortiSOAR™ has explicit CRUD permissions that you can modify and save within a single Role. You can also explicitly assign permissions for each field within a module by clicking the **Set Field Permissions** link for that module.

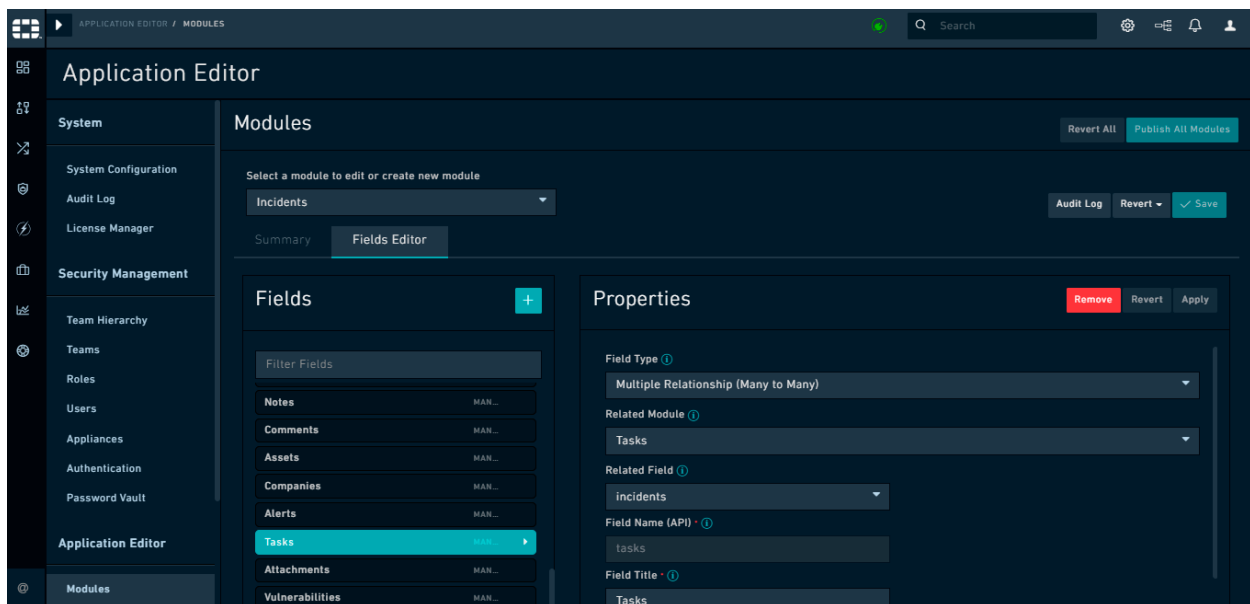
A user can have more than one role applied to their RBAC model. Each role granted to a user is additive to the users' overall RBAC permission set. Therefore, a users' RBAC permissions is an aggregation of all the CRUD permissions granted to them by each Role they are assigned.

**Example 1:** If you assign roles of Security Administrator and Application Administrator to User A, then User A will have CRUD permissions on both the Security and Application modules.

Note that the **Security Administrator** role also has CRUD permissions on the **Secure Message Exchange** and **Tenants** modules, so that this role can configure multi-tenant systems.

**Example 2:** If you had assigned the role of **Application Administrator** to User B, then User B gains all the CRUD permissions on the **Application** module and this user can configure your FortiSOAR™ system.

**Example 3:** If you want a user to work with Incident records, then you must assign that user with CRUD permissions on the **Incident** module, apart from that you must also assign the user a Role that has a minimum of **Read** access on all the related modules. To view the related modules, click **Settings > Modules**. Select the module whose records you want the user to work on, for example, **Incidents** from the **Select a module to edit or create new module** drop-down list. Click the **Fields Editor** tab to view all the fields and related modules, such as **Indicators** and **Tasks**, as shown in the following image. In this case, when you add a user to work in the **Incident** module, you must also assign the user a Role that has a minimum of **Read** access on the **Indicators** and **Tasks** modules.



**Figure 43.** *Fields Editor - Incident Module*

## Default Roles

By default, FortiSOAR™ has at least one role in place after installation, the **Security Administrator**. Apart from the **Security Administrator** role, FortiSOAR™ generally also has the following default roles defined:

- **Security Administrator** - administers Teams and Roles and is responsible for creating the appropriate team structure, building and assigning roles.
- **Application Administrator** - given full access to application-wide features, so that they can configure the system and customize FortiSOAR™ as required.

- **Full App Permissions** - generally, this role is defined as one that has full permissions across FortiSOAR™, i.e., a *root* user. You can define this role as per your requirements. Use this role carefully.
- **Playbook Administrator** - manages playbooks and connectors and also has permission to the **Security** module.
- **T1 Analyst** - triages alerts, filters false positives, and escalates potentially malicious alerts to incidents for review by T2 Analysts.
- **T2 Analyst** - investigates incidents and performs other remediation and containment tasks.
- **FortiSOAR Agent** - contains agent permissions, i.e., agent appliances are auto-assigned to this role.

All Roles are “soft” roles, meaning none of the default Roles are hard coded. You can add, modify, reassign permissions, and delete roles at will, but use this power with extreme caution.

**Tip:** We recommend that you do not modify or delete the default roles (and teams) and instead add new roles (and teams), as per your requirements.

## Security Administrator

The Security Administrator role starts by having full CRUD permissions across the **Security** module. This allows the Security Administrator to add and manage Roles and Teams within the application. The security administrator role also has CRUD permissions on the **Secure Message Exchange** and **Tenants** modules, so that this role can configure multi-tenant systems.

The Security Administrator should be assigned to someone who has been tasked with the responsibility for building and maintaining the role and team structure for your organization.

**Danger “Do not remove the Security Administrator Role”:** We recommend you never remove the Security Administrator role. If you remove the Security Administrator role, you must ensure that at least one other role with an assigned user has the Security module enabled if you always want to maintain access to edit teams and roles within the application. You can assign the Security Module to another role, or to another user, as required.

## Playbook Administrator

The Playbook Administrator has access to the Orchestration and Playbooks component. Only users who have explicitly been given a minimum of Read access to Playbooks can see this component on the left navigation bar. For users to have full privileges to manage playbooks, you must be given Read, Create, Update, Delete, and Execute permissions.

**Note:** System-level playbooks are also configured and should remain in place permanently. These are tagged as 'system, dev' and are now in a hidden Collection.

## Application Administrator

The Application Administrator is granted access to configure application settings, found in the **Application Editor** section on the **Settings** screen.

**Tip:** All users must have Read privileges to the Application module to be able to use the application interface. Non-human users, API users, can be restricted from entering into the application GUI by not giving them any access to the Application module.

## Full App Permissions User

Full App Permission user is a "root" user, who has full permissions across FortiSOAR™. However, data partitioning is still in effect depending on the Team to which the Full App Role user belongs. The result of data partitioning is that a user with the Full App Permissions role might not see all the data within the application unless they have made their Team a Parent of all other Teams in the Application.

## T1 Analyst

The T1 Analyst role is given access to the **Alerts** module and modules associated with alerts, such as **Comments**, **Attachments**, etc, and also **Schedules**. These users are responsible for alert Triaging, false positive filtering and escalating potentially malicious alerts to Incidents for review by T2 Analysts.

## T2 Analyst

The T2 Analyst role is given access to the **Incidents** module and modules associated with incidents, such as **Alerts**, **Indicators**, etc, and also **People**, **Schedules**, and **Reporting**. These users are responsible for investigating incidents and performing other remediation and containment tasks.

## FortiSOAR Agent

You can add this role directly to users so that they get access to agents. Agent appliances are auto-assigned to this role, and by default has access (CRU permissions) on **Files** and **Attachments**.

## Modules in the Role Editor

Modules are discrete areas or record sets within the application. Some modules represent discrete record tables while some represent areas of modification within the administrator's panel.

**Tip:** Not all modules present in the Roles menu are available in the interface. Some of the modules are administrative or for particular purposes, such as the Files module.

### Table Modules

Table modules are record sets that are editable within the FortiSOAR™ UI from a component level, i.e., these are all the modules that are listed in the Roles Editor, which is used to set module-specific permissions. Components, which include Incident Management, Vulnerability Management, Resources, etc., consist of a logical grouping of modules. For example, the Incident Management component contains modules such as Alerts, Incidents, Tasks, etc., and the Vulnerability Management component contains modules such as Vulnerabilities, Assets, and Scans. Each of these individual modules is accessible within the navigation menus.

**Important:** Users can access and modify modules if they are given appropriate CRUD permissions to those modules within FortiSOAR™. For example, if a user requires to modify alerts and incidents, that user must be assigned a role that at the minimum has Read and Update permissions on the Alerts and Incidents modules.

### Administration Modules

Administration modules refer to specific areas of administration within the application. These are generally accessible in the **Settings** menu, with discrete tabs for each of the menu options.

Some of the admin modules found in the system, in alphabetical order, are:

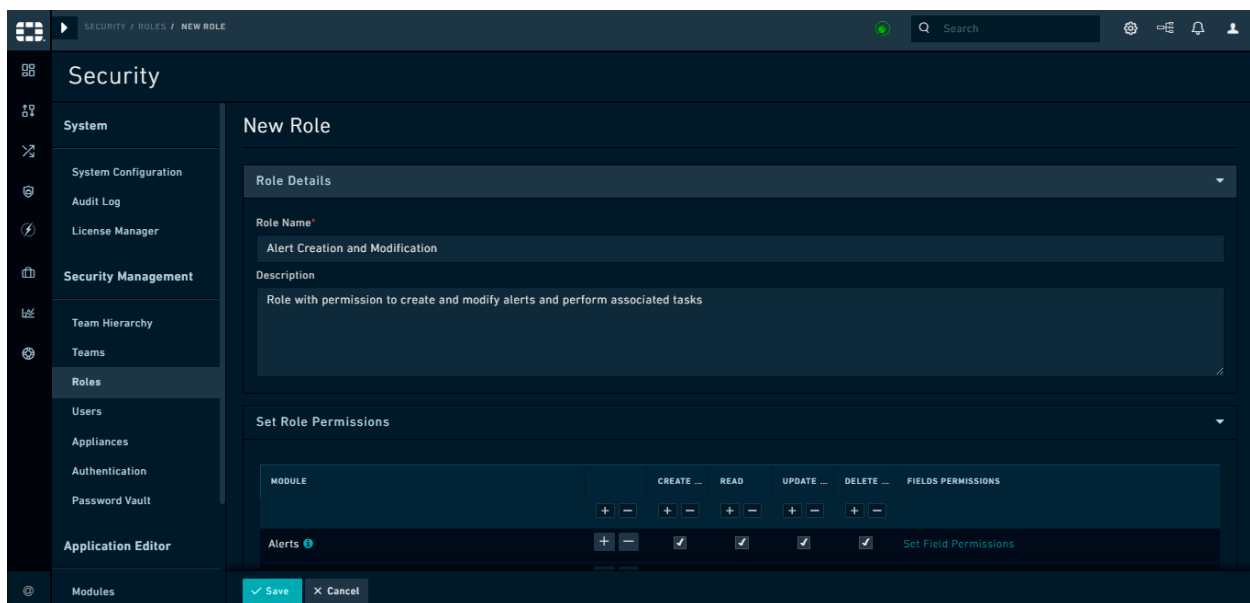
- **Appliances** - the ability to manage appliances from the **Appliances** item.
- **Application** - the ability to change system defaults used throughout the system from the **System Configuration** item.
- **People** - the ability to manage human users from the **Users** item.
- **Playbook** - the ability to access and manage the Orchestration and Playbooks component in the left navigation menu.
- **Password Vault** - the ability to integrate with external vaults such as "Thycotic Secret Server" and "CyberArk" to securely store their sensitive data and credentials.
- **Security** - the ability to manage teams and roles from the **Team Hierarchy**, **Teams**, and **Roles** item.

## Adding Roles

To add a new role, click **Settings > Roles** to open the **Roles** page. Click **Add** to open the **New Role** page enter the role name and description in the respective fields. In the **Set Role Permissions** grid, the **Module** column displays the name of the various modules to which you can assign permissions. Each of the **Create**, **Read**, **Update**, and **Delete** columns have checkboxes that allow you to assign specific permissions for each module. The **Playbook** module has an additional **Execute** permission that is required for users to execute actions and playbooks.

**Note:** Whenever you add a new role, then by default the **Read** permission for **Application** will be selected.

For example, if you require to create a user who needs to add and modify alerts and their associated tasks, you can create a new role as shown in the following image:



**Figure 44.** Role Editor Page with Alerts and Incidents modules selected

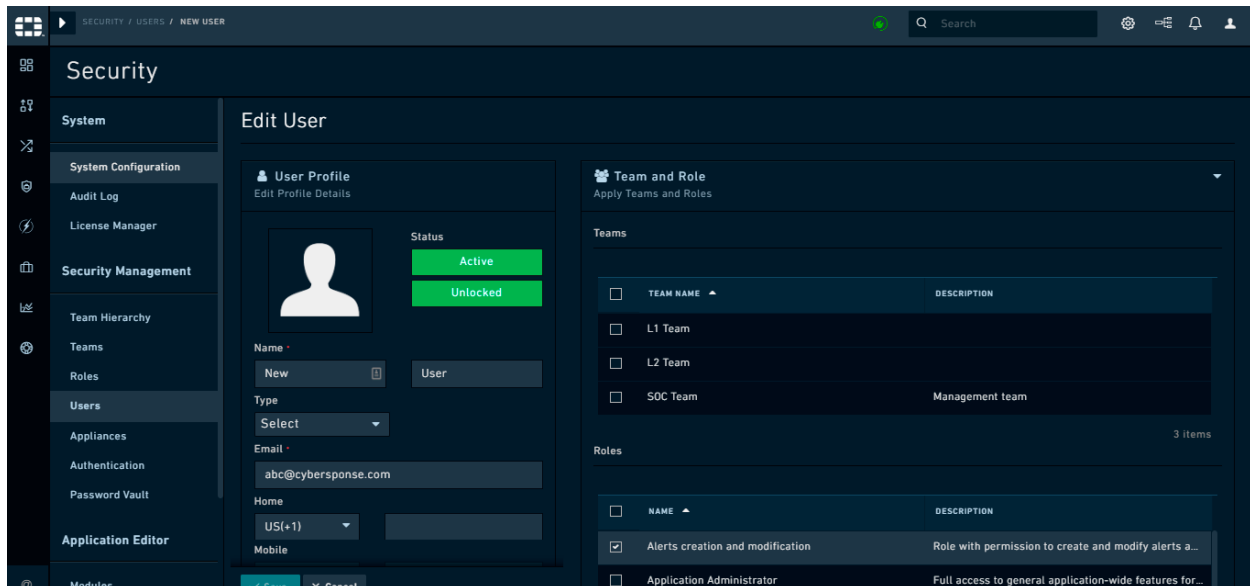
## Assigning Roles to Users and Appliances

You cannot assign roles in bulk to Users or Appliances. You must assign roles directly assigned to users at the time of creating or updating user or appliance profiles.

To assign a role to a user, click **Settings > Users** to open the **Users** page. The **Users** page displays a list of users (active and inactive) for the organization. On the **Users** page, click the username to whom you want to assign the role. On the **Edit User** page, select the role(s) from the **Roles** table in the **Team** and **Role** section that you want to assign to the user, and click **Save**. If there are more than five roles in the system, the **Roles** table becomes scrollable.



For example, you can assign the Alerts creation and modification role to New User as shown in the following image:



**Figure 45.** User Profile page with User A assigned the Alerts and Incidents role

Roles can be added or removed at any time from any profile. When permissions to a Role is changed, then enforcement begins immediately. However, as the UI is built upon login, some aspects of the UI for navigation might still be available until the UI is refreshed or logged out. For instance, if Playbook privileges are removed from your user, you will still be able to see the Playbooks navigation button in the UI, but when you navigate to it, you will be notified that you are not authorized to view that page (401 error).

## Configuring User and Appliance Profiles

### Adding Users

To add a new user, click **Settings > Users** to open the **Users** page. Click **Add Person** and enter the user details on the **New User** page and click **Save** to save the new user profile.


**Note** that the **Username** field is **mandatory** and **case sensitive** and it cannot be changed once it is set.

**Important:** All new users, including the csadmin user, must change their password when they first log on to FortiSOAR™, irrespective of the complexity of the password assigned to the users. Ensure that you note down your csadmin password since if you forget your initial csadmin password, then you have to request FortiSOAR™ to reset this password. Also, when you are changing your csadmin password, you must ensure that you also update the email ID that is specified for csadmin, which by default is set to soc@fortinet.com (which is not a valid email ID). You can change the email ID by clicking the **User Profile** icon (👤) to open the User Profile page and change the email address in the **Email** field.

Once you set a valid email ID in the user profile, then you would be able to reset your password, whenever required, by clicking the **Forgot Password** link on the login page.

Use the SMTP connector to configure SMTP, which is required to complete the process of adding new users. The SMTP connector is used to send email notifications. If you have not set up the SMTP connector, the user gets created. However, the password reset notification link cannot be sent to the users, and therefore the process remains incomplete. For more information on FortiSOAR™ Built-in connectors, including the SMTP connector, see the “[FortiSOAR™ Built-in connectors](#)” article present on the support site. You must log onto the support site to view this information.

## User Profiles

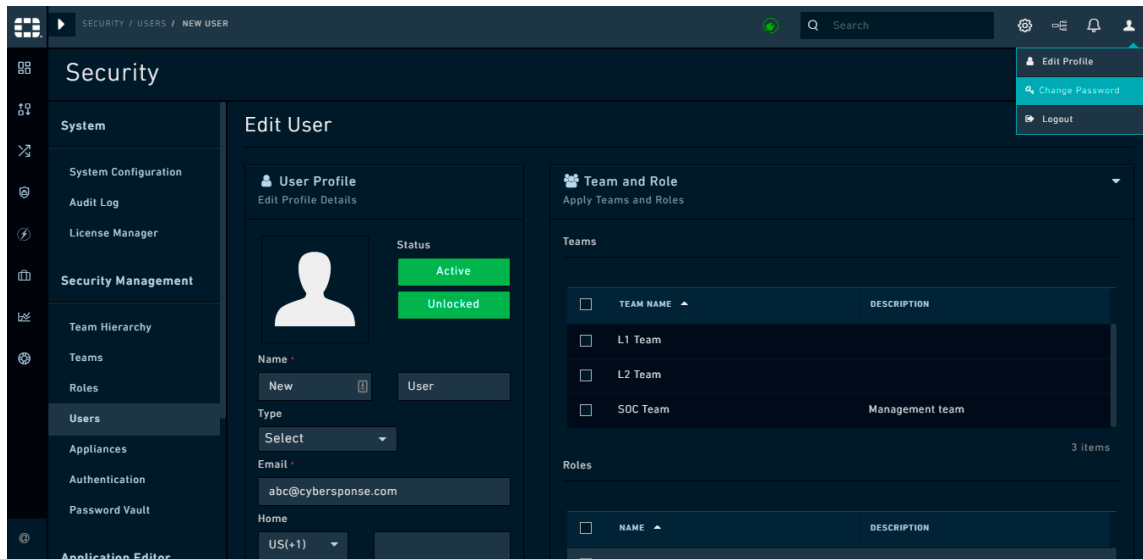
All users within the system have a profile. Each user has access to their own profile so that they can update specific information about them by clicking the **User Profile** icon (.

The user profile includes users' name, email, username, password, and phone numbers. Users can also view the team and roles they belong to as well as update their theme. Users can also view their own audit logs, which display a chronological list of all the actions that you have performed across all the modules of FortiSOAR™.

You must change your password when you log on to FortiSOAR™ for the first time. To change your password, click the **User Profile** icon and then select the **Change password** option. You can also change your password at any time using this option.

**Note:** The **Username** field is mandatory that cannot be edited once it is set.

To edit user profiles, you must be assigned a role that has a minimum of **Read**, **Create** and **Update** permission on the **People** module. Click **Settings > Users** to open the **Users** page and click the user whose profile you want to edit. This opens the **Edit User** page, where you can edit the user's profile, including the user's email ID, name, phone and fax numbers, users' teams, roles, 2-factor authentication settings, notification settings, and theme settings. You can also see their login history.



**Figure 46.** User Profile Page

A user is one whose **People** record is **Active**. If you have **Read** and **Update** permissions on both the **Security** and **People** modules, you can edit a user's Active or Inactive status on their profile page. If you change a user's status to Inactive, you stop that user from using the system upon expiration of their issued token.

Locked users are those who have exceeded the number of authentications tries allowed within a one-hour period. You can define the maximum number of attempts allowed before the user is locked. The User can only be unlocked by an administrator who has **CRUD** permissions on the **People** module and **Read** and **Update** permission on the **Security** module.

By default, users' can enter an incorrect password 5 times, while logging into FortiSOAR™, before their account gets locked for 30 minutes. A Security Administrator can change these default values, see the *Debugging, Troubleshooting, and optimizing FortiSOAR™* section for further details.

If a Security Administrator has enforced 2FA across all FortiSOAR™ users, then the **Work Phone** becomes a mandatory field and you must enter the work phone number for all FortiSOAR™ users. For more information see, [Configuring User Accounts](#).

**Note:** If you face issues with user preferences such as applying filters on the grid or column formatting within a grid, click the **More Options** icon (☰) and click on the **Reset Columns To Default** option.

## Teams and Roles

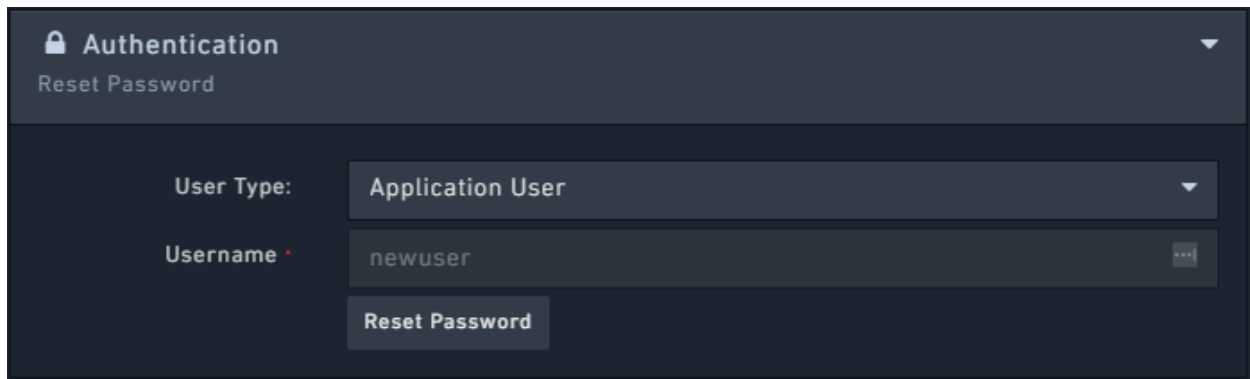
If you are editing your own profile and you have no access to the **People** module, then you can only view to which teams and roles you belong.

If you are assigned a role with **Read**, **Create**, and **Update** permissions on the **People** module then:

- You can assign roles to users by selecting the roles from the **Roles** table in the **Team** and **Role** section on the **Edit User** page. If there are more than five roles in the system, the **Roles** table becomes scrollable.
- You can assign teams to users by selecting the teams from the **Teams** table in the **Team** and **Role** section on the **Edit User** page. If there are more than five teams in the system, the **Teams** table becomes scrollable.

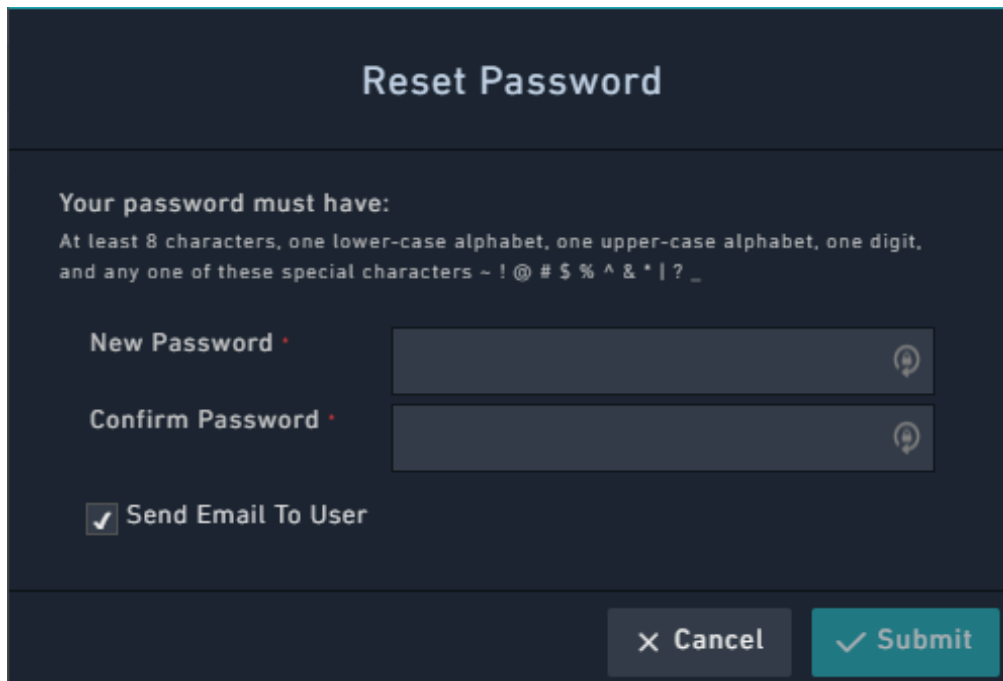
## Authentication

An administrator who is assigned a role with **Read**, **Create** and **Update** permissions on the **People** module and **Read** and **Update** permission on the **Security** module can reset passwords for users on the **User Profile** page. To reset passwords, open the profile page of the user whose password you want to reset and go to the **Authentication** section.



**Figure 47.** *User Profile Page: Authentication Section*

Click the **Reset Password** button to reset the password for a user. Clicking **Reset Password** displays the **Reset Password** dialog, in which you must enter the new password in the **New Password** field and re-enter the same password in the **Confirm Password** field.



**Reset Password**

Your password must have:  
At least 8 characters, one lower-case alphabet, one upper-case alphabet, one digit, and any one of these special characters ~ ! @ # \$ % ^ & \* | ? \_

New Password \*

Confirm Password \*

☒ Send Email To User

✕ Cancel ✓ Submit

**Figure 48.** *Reset Password Dialog*

Select the **Send Email to User** check box to send an email notification to the user whose password you have reset. The email notification tells the user that the administration has changed their password and the user must contact their administrator for the new password or reset their password using the Forgot Password option on the FortiSOAR™ login page. For more information on the Forgot Password option, see the *Regenerating your password* topic in the “User Guide.” Click **Submit** to reset the users’ password.

By default, users’ can click the **Reset Password** link 10 times before actually resetting their password, after which users’ will not get a new link to reset their password for 12 hours. A Security Administrator can change these default values, see the *Debugging, Troubleshooting, and optimizing FortiSOAR™* section for further details.

You can also configure whether the user is an Application User or Dashboard User. You can set different reauthentication times for an Application user and a Dashboard user.

## 2-Factor

The **2-Factor** authentication menu displays the current user preference for the 2-factor method. Currently, FortiSOAR™ supports only TeleSign for 2-Factor authentication. You require to have a TeleSign account to configure 2-Factor Authentication (2FA) to send the one-time password (OTP) code to the users’ mobile devices and log onto FortiSOAR™.

The options for 2FA are:

- No 2-Factor authentication. Security Administrators can enforce 2FA across all FortiSOAR™ users. Therefore, this option is displayed only if you have not enforced

2FA across all FortiSOAR™ users. For more information see, [Configuring User Accounts](#).

- 2FA Voice, which sends a voice message to the user's work phone.
- 2FA SMS, which sends a text message to the user's work phone.

**Note:** Once you enable 2FA in a user's profile, then the work phone field becomes mandatory.

## Notifications

Currently, notification preferences are limited to email. In the future, in-app notifications and SMS notifications will enable additional notification mechanisms.

## Theme Settings

You can update your FortiSOAR™ theme, if you have appropriate rights, using the **Theme Settings** menu on the **Edit User** page. There are currently three theme options, **Dark**, **Light**, and **Space**, with **Space** being the default. Click **Preview Theme** to see the Theme as it would look and save the profile to apply the theme. To go back to the original theme, after previewing the theme, click **Revert Theme**.

## History

The **History** menu contains the authentication history for the user and displays the ten most recent authentication attempts and their outcome.

## Audit Logs

The **User Specific Audit Logs** panel displays a chronological list of all the actions that a user has performed across all the modules of FortiSOAR™. Click the **Audit Logs** panel to view the list of actions. The audit log displays users' login success or failures and logout events. The login event includes all three supported login types, which are DB Login, LDAP Login, and SSO Login. Audit logs also contains user-specific terminate and resume playbook events.

## Appliances

Appliance users have a few essential differentiators versus Users (People). The most important one is that API access for appliances uses HMAC verification as opposed to issuing a token from the Authentication Engine. The Authentication Engine uses the HMAC signature to validate the Public and Private key pair, which is issued at the time of Appliance creation. Appliance users also do not have a login ID and do not add to your license count.

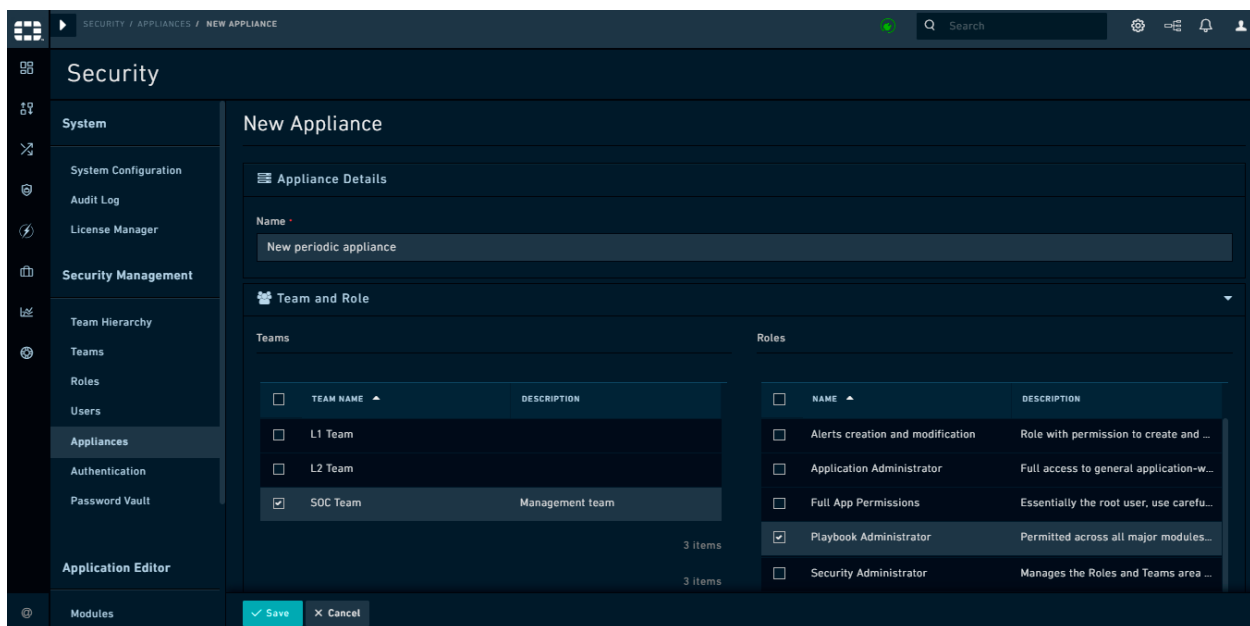
Appliance users are generally used for authenticating to FortiSOAR™ while calling Custom API Endpoint triggers. Mostly while configuring auto-forwarding of events and alerts from a SIEM to FortiSOAR™, you can use an appliance user, otherwise you might require to add a user password, in plain text, in the configuration files.

Like Users, you must assign appropriate roles to appliances and also add the appliances as a member of the teams who would be running playbooks, so that appliances can access or modify any data within the system. Team hierarchy and such is restrictions that apply to Users also apply to Appliance Users.

**Note:** We recommend that you scope the role and team of an Appliance to give it only the bare minimum level of privilege needed to do the job as a good security practice.

## Creating a New Appliance

Click **Settings > Appliances > Add** to create a new appliance. On the **New Appliance** page enter a name with which to identify that Appliance and select the Team(s) and Role(s) that apply to that Appliance.



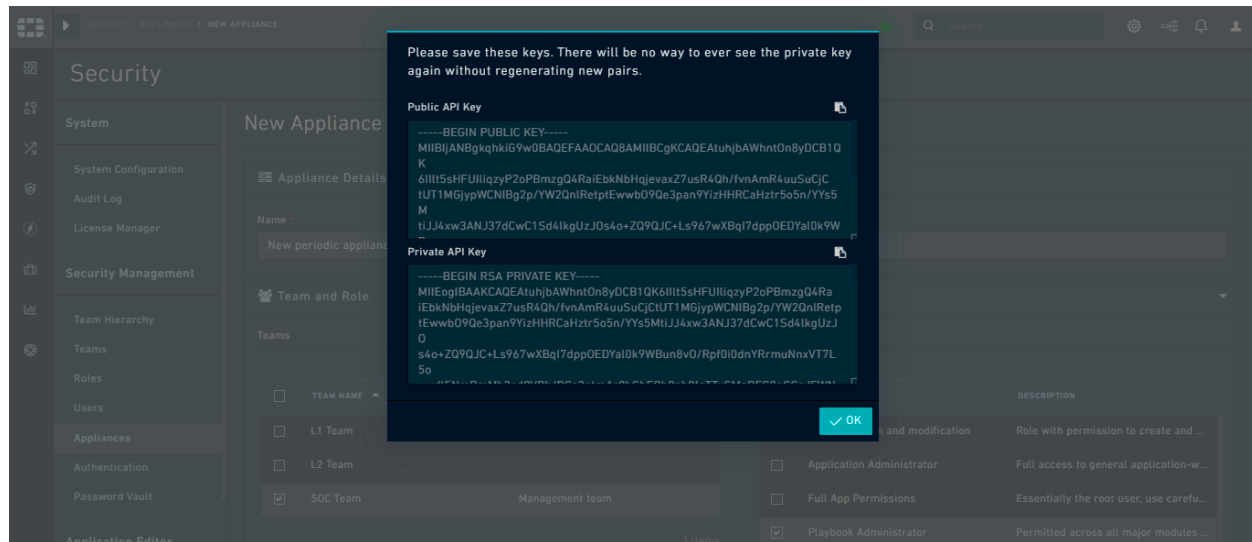
**Figure 49.** *Creating a New Appliance*

## Generating Appliance Keys

Once you save the new Appliance record, FortiSOAR™ displays a pair of Public / Private cryptographic keys in a modal window.

**Important:** When the Public / Private key pair are generated, the Private key is shown only once. You must ensure to copy this key and keep it somewhere safe for future reference. If you lose this key, it cannot be retrieved. You can always regenerate these keys when

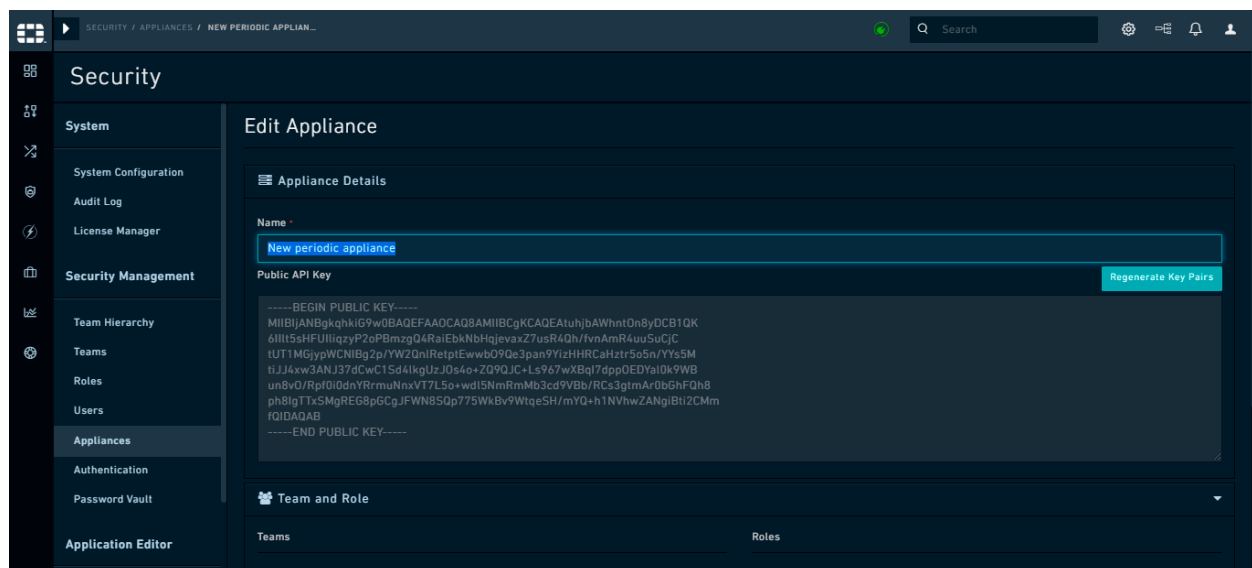
required, and a new Private Key gets displayed. However, you must then update the keys as the old keys will be invalidated.



**Figure 50. Cryptographic Keys**

## Appliance Profile

You can modify details of the Appliance user after the Appliance has been created. Click **Settings > Appliances** to open the **Appliances** page and click the appliance user whose profile you want to edit. On the **Edit Appliance** page, you can modify the name, teams, and roles for the appliance user. You can also use **Edit Appliance** page to access and copy the Public API Key for the appliance at any time.



**Figure 51. Appliance Profile**

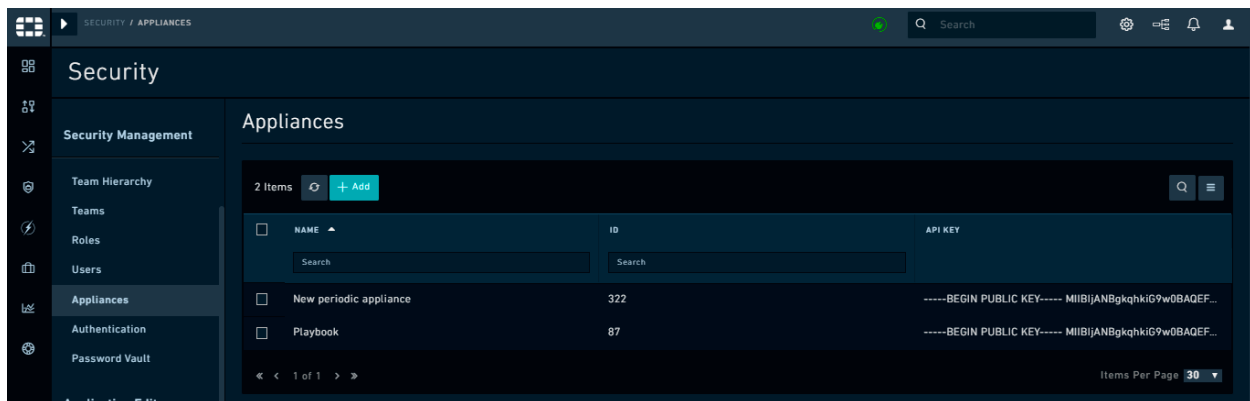


## Playbook Appliance

By default, an appliance user is created as **Playbook** who belongs to the **SOC Managers** team. This appliance is used by the FortiSOAR™ workflow service to authenticate to the API service when a workflow step is run that reads, creates, updates, or deletes records. Hence, it should have all necessary permissions on the modules that are accessed using playbooks. Also, as a consequence, when a record is inserted by a workflow such as a Playbook or a Rule that uses the appliance, then the inserted record is owned by the appliance user, which by default is **Playbook**.

For example, If a new incident record is inserted by a playbook or workflow, then the **Created By** field of this newly inserted record displays the name of appliance user who has executed the playbook, which by default is **Playbook**. The owner of this newly inserted record will be the team that is assigned to the appliance that has executed the playbook, which by default is **SOC Manager**. If multiple teams have been assigned to the appliance, then this newly inserted record would have all those teams as 'owners.' Example to explain this is, if you have created a different appliance named **QA**, which has been assigned **SOC Manager** and **Team A** as its teams. Now if a playbook that inserts an alert record is executed using the **QA** appliance, then the **Created By** field of this newly inserted alert record will display **QA** and its owners will be **SOC Manager** and **Team A**.

**Note:** We recommend that you scope the role and team of a Playbook Appliance to give it only the bare minimum level of privilege needed to do the job as a good security practice.



**Figure 52.** *Appliances Overview Screen*

You must however assign the new playbook appliance with a minimum of **Read** permission on the **Playbook** module so that the new appliance user can run playbooks without getting permission denied errors. You must also assign appropriate permissions on the other modules such as **Alerts**, based on the playbooks that you intend to run using the appliance.

### *Regenerating playbook appliance keys*

You can regenerate your playbook appliance keys using the process mentioned in the [Generating Appliance Keys](#) topic.

If you regenerate the key pair for the playbook appliance, replace the content of the `APPLIANCE_PUBLIC_KEY` and `APPLIANCE_PRIVATE_KEY` files at the following locations with the public and private keys that you have regenerated:

- `/opt/cyops-workflow/sealab/.envdir`
- `/opt/cyops-integrations/integrations/configs`

After you have replaced the playbook appliance keys, you must restart all the FortiSOAR™ services.

You must take care of the following:

- Ensure that there are no extra files or folders in the `sealab/.envdir` directory.
- Do Not change the `SEALAB_PUBLIC_KEYS` or the `SEALAB_PRIVATE_KEYS`.

## Troubleshooting

### *Getting an HMAC failure*

**Resolution:** If HMAC fails, ensure that the server time for the application server is synced with that of the FortiSOAR™ server. You can synchronize both servers to a common NTP server, for example, `time.apple.com`, to synchronize the time.

## Configuring Authentication

Click **Settings > Authentication** to configure various authentication settings in FortiSOAR™, including setting session and idle timeouts, settings options for user accounts, configuring LDAP / AD, and configuring SAML to enable users to use sign-on (SSO).

FortiSOAR™ supports the following methods of authentication: Database users, LDAP users, and SSO.

**Note:** Even if you configure SSO, you can still provision database and LDAP users.

To configure authentication settings, you must be assigned a role that at a minimum has **Read** and **Update** permissions on the `Security` module.

## Configuring Accounts

### Configuring Session and Idle timeouts

Click **Settings > Authentication** to open the `Account Configuration` tab. On the `Account Configuration` page, in the `Session & Idle Timeout` section, you can configure the following settings for session and idle timeouts:

Setting	Description
Idle Timeout	The number of minutes a user can be idle on FortiSOAR™ after which the Idle Warning dialog is displayed. The default value is 30 minutes.
Idle Timeout Grace Period	The number of seconds a user is given to view the Idle Warning dialog after which FortiSOAR™ logs the user out. The default value is 60 seconds.
Token Refresh	The number of minutes after which the session token is refreshed. The default value is 60 minutes.
Reauthenticate Dashboard User	The number of hours after which a dashboard user is forced to be reauthenticated. The default value is 24 hours.
Reauthenticate Application User	The number of hours after which an application user is forced to be reauthenticated. The default value is 24 hours.

### Notes:

In the case of a non-admin user the **Token Refresh**, **Reauthenticate Dashboard User**, and **Reauthenticate Application User** settings do not work. In the case of **Token Refresh**, the user gets logged off from the FortiSOAR™ UI once the session token refresh time is reached. In the case of **Reauthenticate Dashboard User** and **Reauthenticate Application User**, users are not forcefully logged off from the FortiSOAR™ UI, and they do not need to reauthenticate themselves.

## Configuring User Accounts

Click **Settings > Authentication** to open the **Account Configuration** page. On the **Account Configuration** page, you can configure the following option for user accounts:

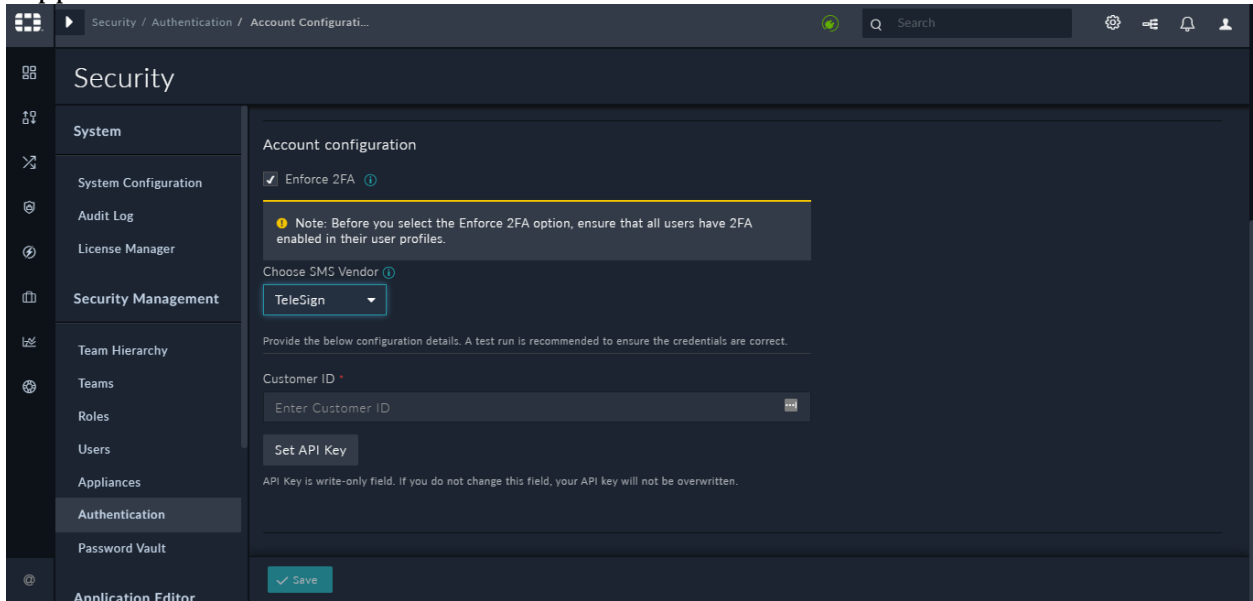
**Enforce 2FA:** Globally enforces 2FA across FortiSOAR™ users. Before you enforce 2FA across all FortiSOAR™ users, you must ensure that all users have enabled 2FA in their user profiles. For more information, see [2-Factor](#).

Currently, FortiSOAR™ supports only TeleSign for 2-Factor authentication. You require to have a TeleSign account to configure 2-Factor Authentication (2FA) to send the one-time password (OTP) code to the users' mobile devices and log onto FortiSOAR™.

To configure 2FA, do the following:

1. On the **Account Configuration** page, click the **Enforce 2FA** checkbox.  
In **Choose SMS Vendor**, **TeleSign** will be displayed, since currently only TeleSign is

supported for 2-Factor authentication in FortiSOAR™.

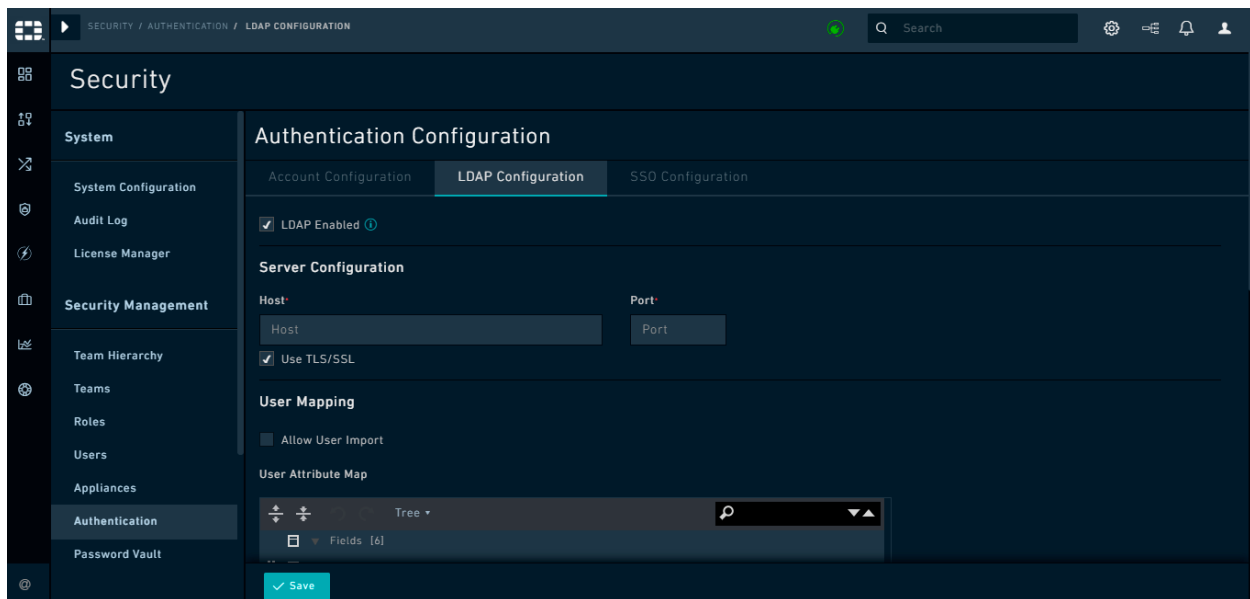


2. In the **Customer ID** field, enter the customer ID that has been provided to you for using TeleSign.
3. In the **Set API Key** field, enter the API Key that has been provided to you for using TeleSign.

## Configuring LDAP / AD

Use the **Authentication** menu to setup, modify, and turn on or off your LDAP / AD authentication provider. Click **Settings > Authentication** to open the **Account Configuration** page. Click the **LDAP Configuration** tab and click the **LDAP Enabled** checkbox, if you want to enable LDAP authentication for FortiSOAR™.

Enter the hostname and port of your LDAP / AD authentication server. Click **Use TLS/SSL** and then provide a user search the directory and import users. You can add users either by mapping users using the **User Attribute Map**, or search for users in the directory and then import users.

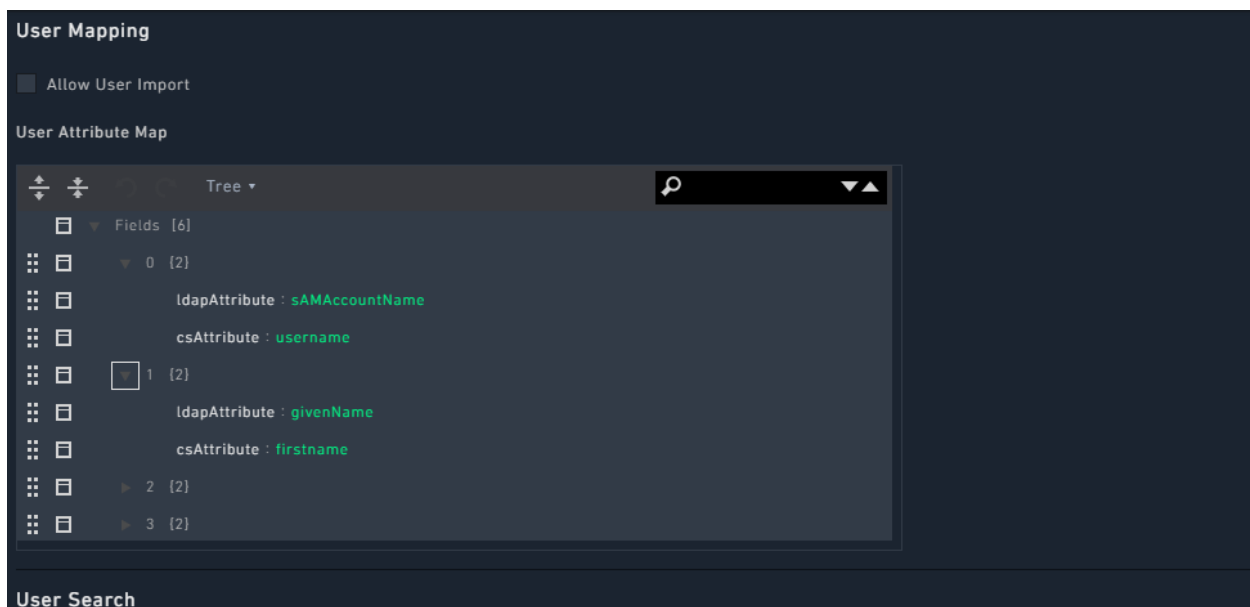


**Figure 53.** *Authentication Administration Menu*

## User Attribute Map

To map users, configure the **User Attribute Map**. FortiSOAR™ provides you a default user attribute map array that contains the most common combination of field mappings. You can modify the mappings based on your own LDAP container fields by editing the map.

In the **User Attribute Map**, under **Fields**, click the editable field name (right-side field name), to map it to your LDAP fields. The non-editable field name (left-side field name) is the FortiSOAR™ attribute.



**Figure 54.** *User Attribute Map*

## User Search

You must have valid administrative username and password to search the LDAP / AD resource for user information. You do not have to use admin credentials, but at a minimum, you must have user credentials to access and import all desired user containers.

**Figure 55.** *User Search*

**Search User:** Searches LDAP / AD for a user in the format `CN=UserName,CN=Users,DC=XXXX,DC=XXX`.

**Base DN:** Base DN for user search in the format `CN=Users,DC=XXX,DC=XXX`.

**Search Attribute (s):** Attribute for searching a user, for example, `sAMAccountName`. Check the **Recursive** checkbox for recursively searching for users.

**Search Criteria:** Criteria for searching a user, for example, `SOCMembers`.

Once you have added the credentials in the `User Search` section, click **Allow User Import** to configure your environment to look in the LDAP / AD resource for **all new users**.

**Tip:** If you want to add local users, you must clear the `Allow User Import` checkbox to revert your system to the local user import in the Users administration menu.

## Configuring SSO

Use the `Authentication` menu to setup, modify, and turn on or off your SSO configuration. Click **Settings > Authentication** to open the `Account Configuration` page. Click the **SSO Configuration** tab and click the **SAML Enabled** check box if you want to enable SAML for FortiSOAR™.

You must configure SAML in FortiSOAR™ to enable users to use single sign-on. See the *SAML Configuration* chapter for more information on how to setup SAML and user profiles for your organization.

## Configuring the Password Vault Manager

FortiSOAR™ integrates with external vaults such as “Thycotic Secret Server” and “CyberArk” that are used by organizations to securely store their sensitive data and credentials. Integration with external vaults also enables users to periodically change system credentials in their central vaults, and automatically having the configurations fetch those passwords using the vault.

**Note:** To configure the Password Vault, you must be assigned a role that has Read permissions on the Connector module, Read permissions on the Security module, and Update permission on the Application module. To install and configure the connector for using the vault, you must be assigned a role that has Create, Read, Update and Execute permissions on the Connector module and Read permission on the Application module.

FortiSOAR™ must have a connector created for a vault for you to be able to use an external vault in FortiSOAR™. FortiSOAR™ has integrated with Thycotic Secret Server, and therefore we have a Thycotic Secret Server and CyberArk connectors in the Connector Store.

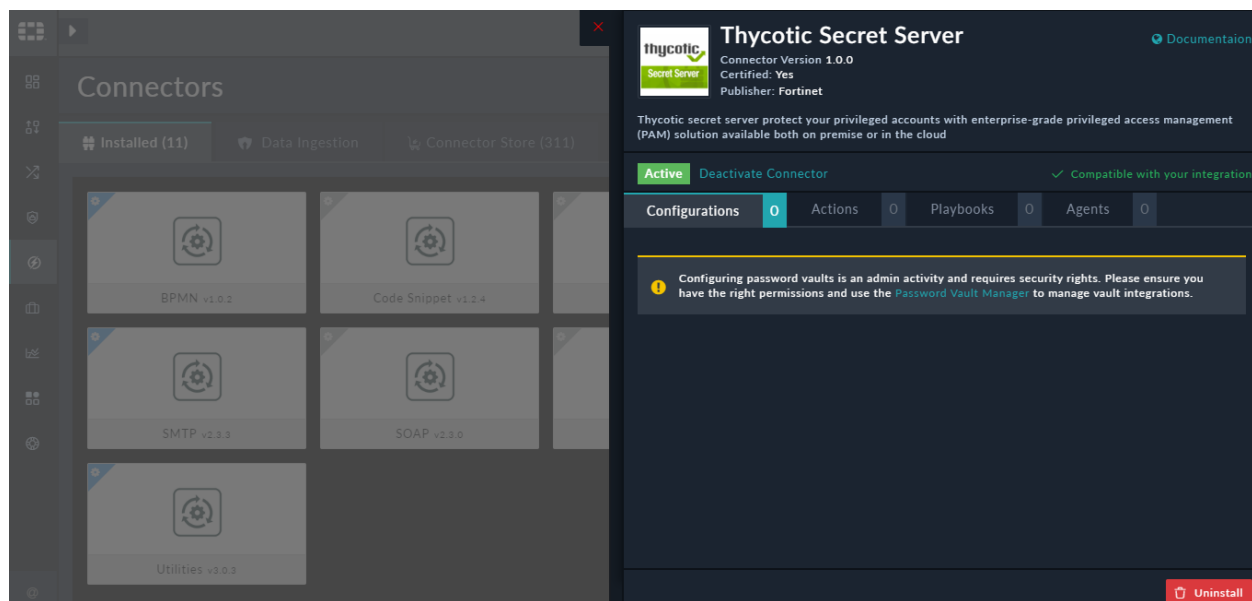
To use a vault in FortiSOAR™, you must first install the connector from the Connector Store. For more information on installing a connector, see the *Introduction to connectors* chapter in the “Connectors Guide.”

Once you have installed the connector, you must configure the connector.

**Note:** To install and configure the connector for using the vault, you must be assigned a role that has Create, Read, Update (CRU) permissions on the Connector module and Read and Update permissions on the Security module, Read and Update permission on the Application module.

This section describes configuring the “Thycotic Secret Server” connector. You can configure “CyberArk”, or any other vault connector that gets integrated with FortiSOAR™ in the future in the similar manner

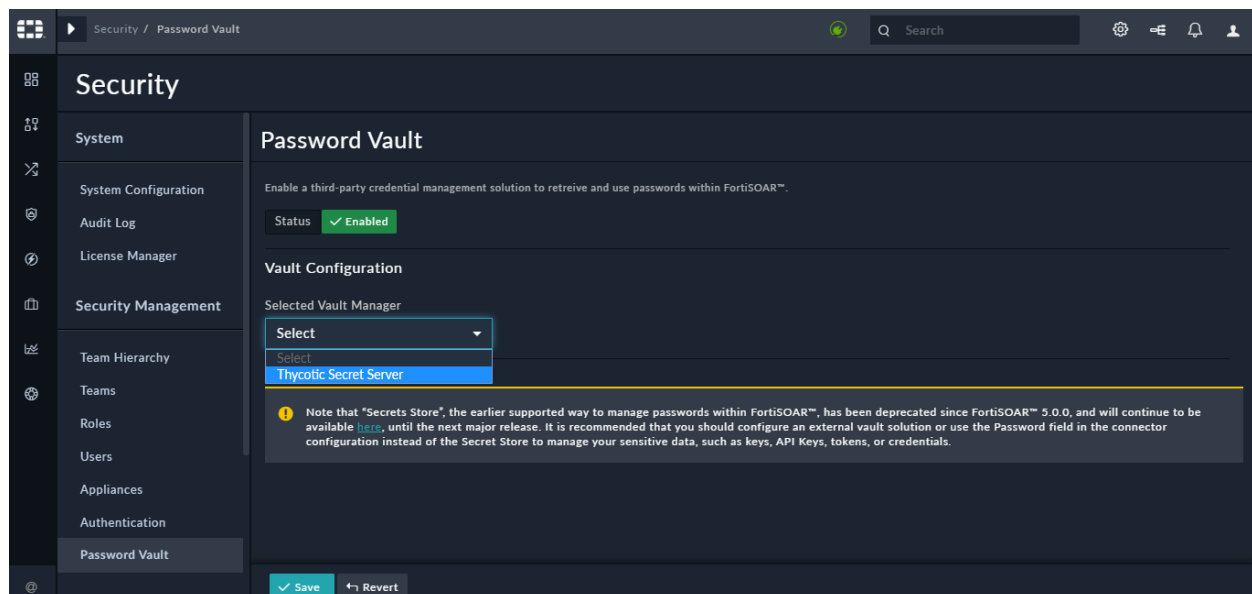
**Important:** You cannot configure a connector that is integrated with an external vault on the **Connector Configuration** dialog as is the case with other connectors. Once you installed the connector and if you have appropriate permissions, the following the **Connector Configuration** dialog is displayed:



**Figure 56.** Connector Configuration dialog in case of connectors that integrate with external vaults

You can open the Password Vault Manager by either clicking the **Password Vault Manager** link on the connector configuration dialog or by clicking **Settings > Password Vault**.

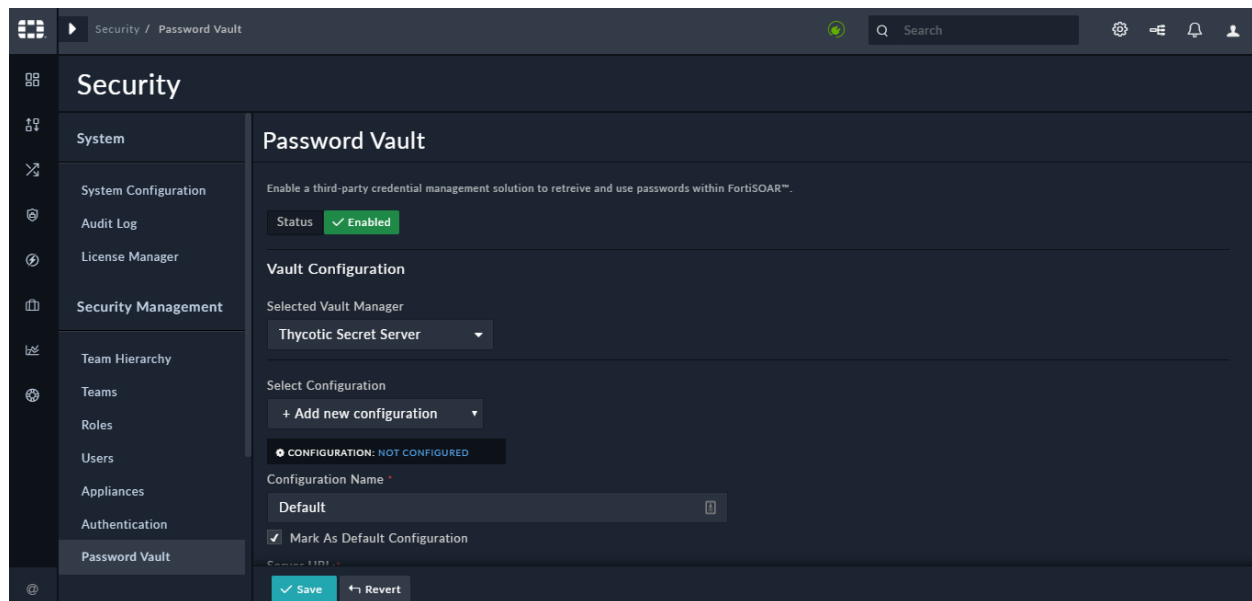
On the **Password Vault** page, click the **Disabled** button to enable integration with external vaults and configure the selected vault. From the **Selected Vault Manager** drop-down list select the vault that you want to use.



**Figure 57.** Password Vault Manager - Enabling the integration

In our example, select Thycotic Secret Server, configure the connector, and then click **Save**.

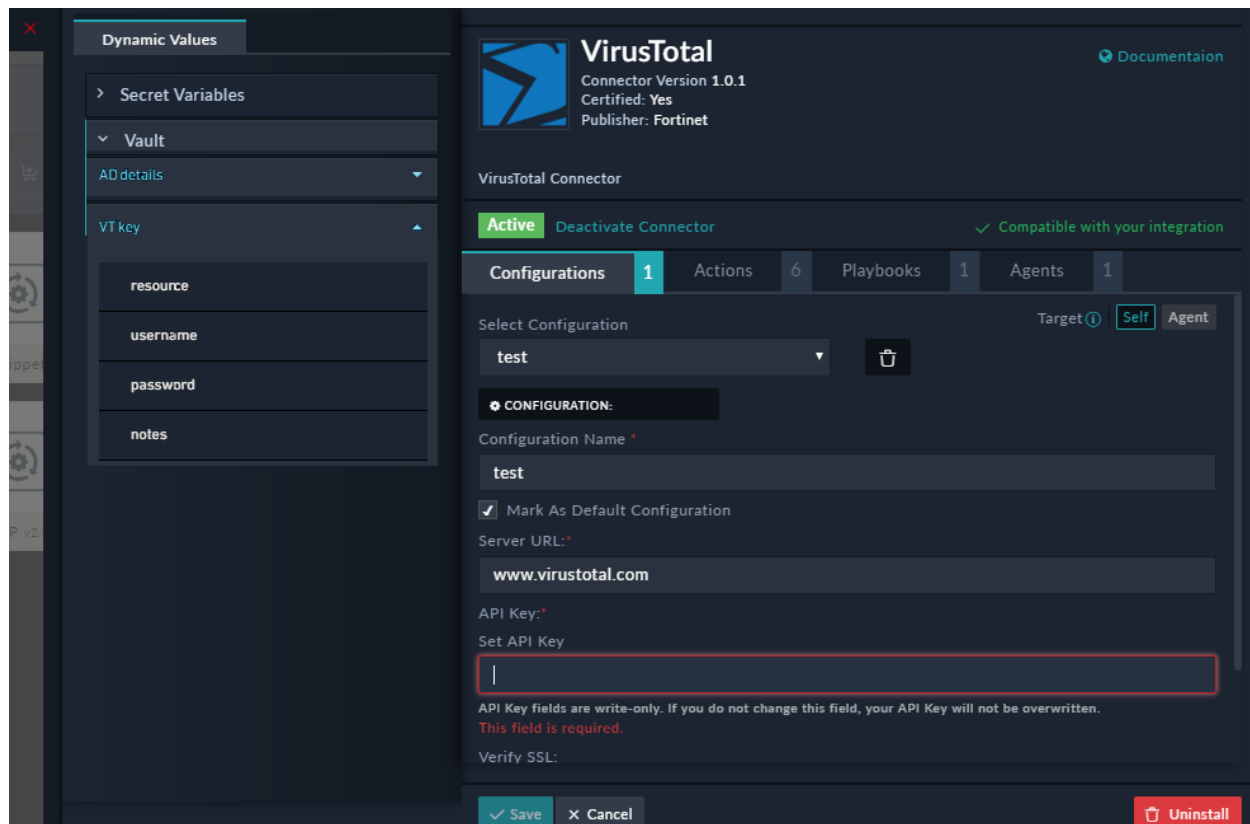




**Figure 58.** Password Vault - Configure the vault connector

**Note:** You can add multiple configurations for a vault; however, you must select a particular configuration for integration with FortiSOAR™. Similarly, you might have multiple vaults, but you can only have one vault integrate with FortiSOAR™.

Credentials (passwords, keys, tokens, etc) that you have stored in the vault are not visible to the users. However, once you have configured your vault, then users can use the credentials stored in the vault in connector configurations. For example, if you have a user who is creating a playbook that requires access to VirusTotal, a 3<sup>rd</sup> party integration, and you do not want to provide the VirusTotal API key to users, you can store the credentials in an external vault. Users can then select the vault credentials in the connector configuration steps by clicking the Password or Set API Key field, which then displays the **Dynamic Values** dialog from which you can select the required credentials, as shown in the following image:

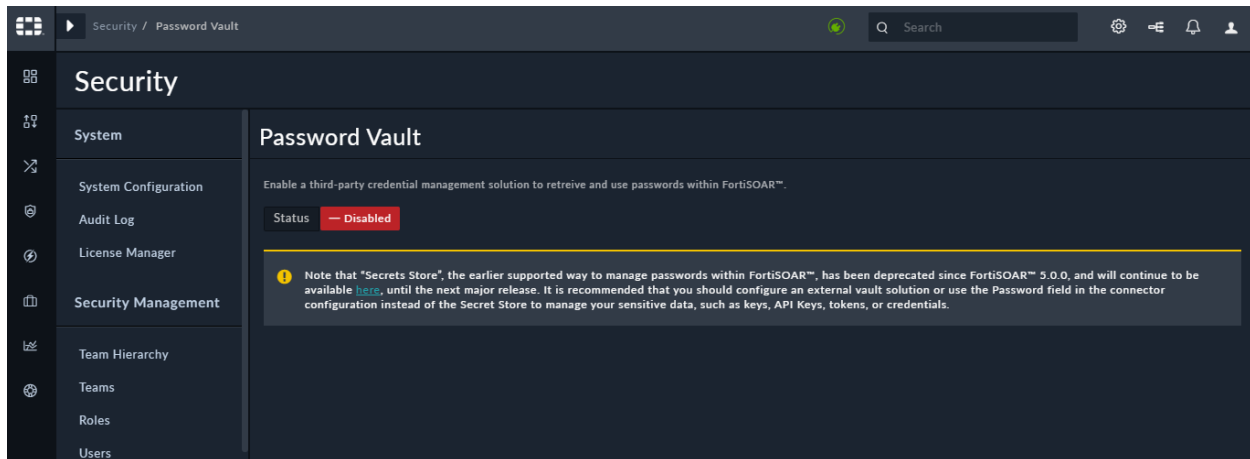


**Figure 59.** Connector Configuration - Vault Option

For more information on Dynamic Values, see the *Dynamic Values* chapter in the “Playbooks Guide.”

You can also continue to use the **Set Password** field in the connector configuration to securely store and manage sensitive data, such as keys, API Keys, tokens, or credentials.

If you have upgraded to FortiSOAR™ 6.0.0 or later, and if you had used the Secrets Store (which has been deprecated since version 5.0.0) to securely store and manage sensitive data, then the credentials that you had stored within the Secrets Store will yet be available as **Secret Variables** in the **Dynamic Values** dialog. You can open the Secrets Store by clicking **Settings > Password Vault** and on the Password Vault Manager click the link (**here**) available in the **Note**, as shown in the following image:



**Figure 60.** Password Vault - Link to Secrets Store

Clicking [here](#) opens the **Secrets Store** page. However, it is highly recommended to move your sensitive data to your external vault or use passwords to securely store and manage data since the **Secrets Store** will not be available from the next major release.

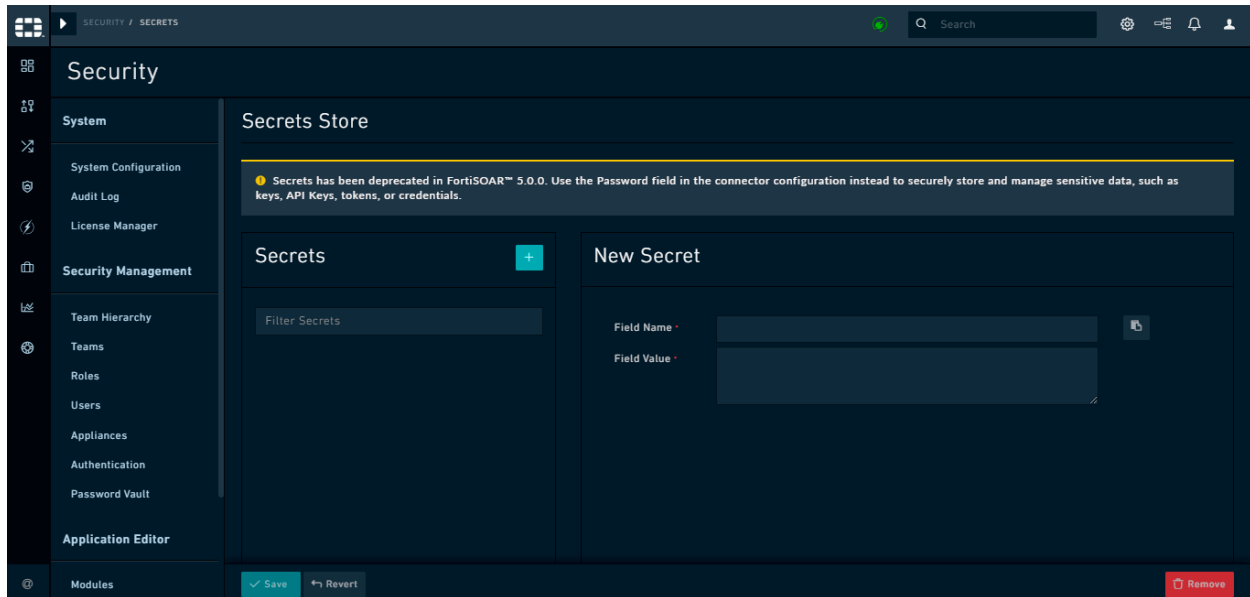
## Configuring the Secrets Store (Deprecated)

You can use the Secrets store to securely store and manage sensitive data, such as keys or credentials. You can also use the “secrets” API to perform all the operations, such as adding, editing, and deleting secrets.

**Important:** This feature has been deprecated in version 5.0.0 and will not be available in the next major release after version 6.0.0. Use the **Password** field in the connector configuration or use an external vault to securely store and manage sensitive data, such as keys, API Keys, tokens, or credentials.

To open the connector configuration, in the FortiSOAR™ left navigation, click **Automation** > **Connector**. Then select the connector whose data you want to store, which opens the connector configuration pane. In the connector configuration pane, click **Set Password** and type the secret that you want to save.

In FortiSOAR™ 6.0.0, open the **Secrets Store** page as explained in the earlier section:



**Figure 61.** *Deprecated Secrets Store page*

When you store data in the **Secrets** store, users cannot see that data. However, they can use this data when required. FortiSOAR™ stores the Secret store data in an encrypted format providing strong security for sensitive information.

**Important:** To add or update secrets, you must be assigned a role that has Read, Create, and Update permissions on the Secrets module, as well as, a minimum of Read permission on the Application module. To delete secrets, you must also be assigned the Delete permission on the Secrets module.

## Example

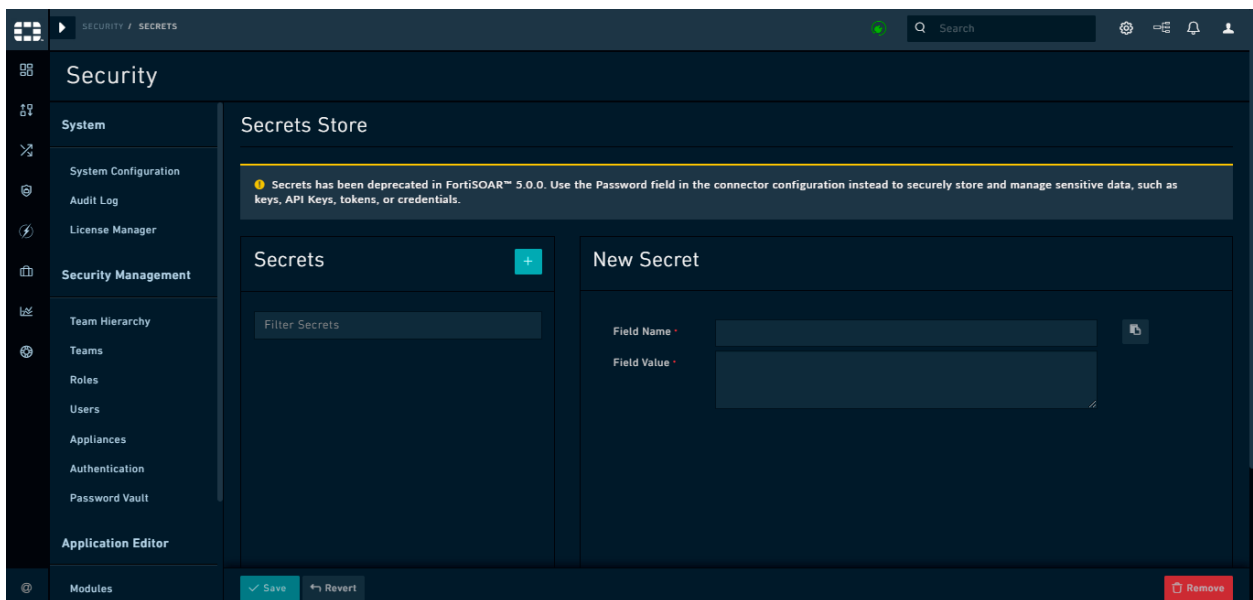
If you have a user who is creating a playbook that requires access to JIRA, a 3<sup>rd</sup> party integration, and you do not want to provide the JIRA credentials (username-password pair) to users, you can add a secret to store the credentials. FortiSOAR™ stores the secret fields' variable reference in a jinja format. You can provide this jinja format to users, who can add them to the playbooks where the JIRA credentials are required. The process of adding this secret is mentioned in the following section.

## Adding a secret

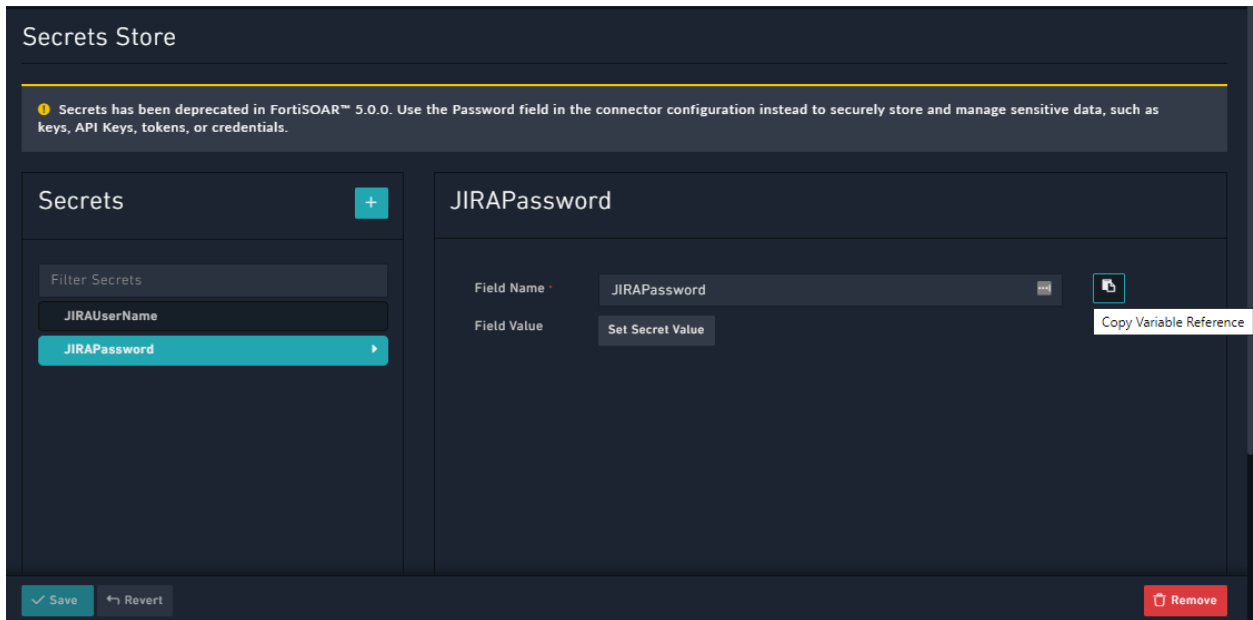
**Note:** The following procedure details the method of adding a secret in version 5.0.0 and later, though this is **not recommended**.

To add a new secret:

1. Open the **Secrets Store** page.

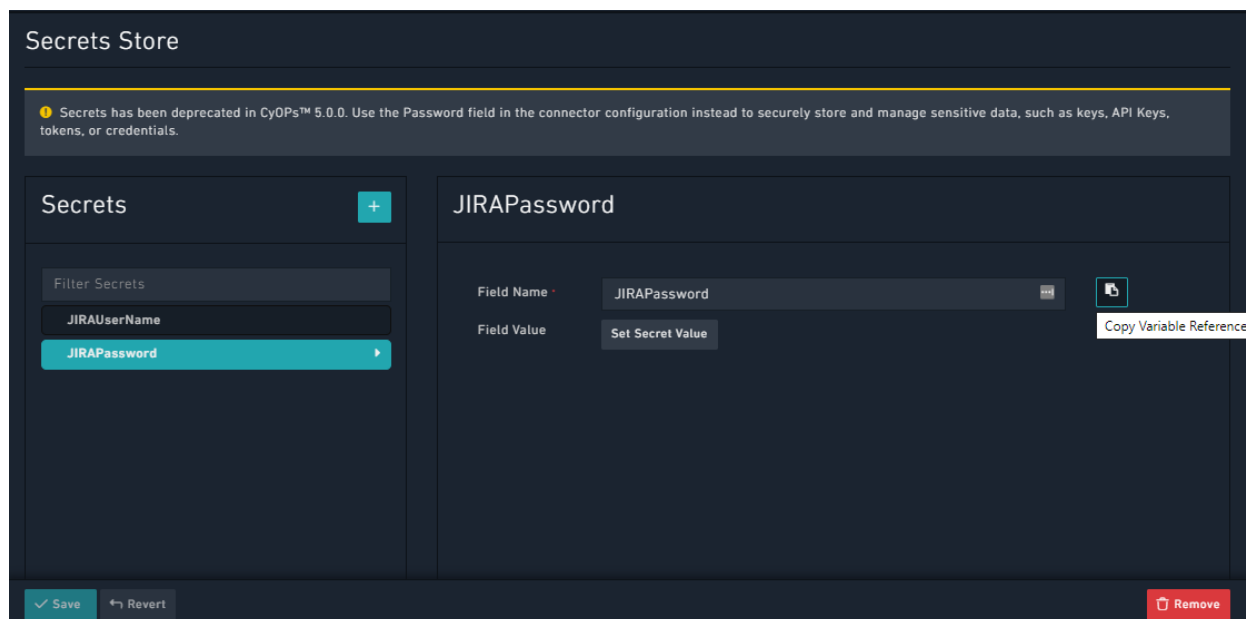


2. Click **Add (+)** and in the **New Secret** page, in the **Name** field, add the name of the secret.  
**Note:** Secret names must be unique within the system. The Name field can have upper-or-lower case alphabets or numbers. However, it must not contain spaces or special characters, except **\_** and **\$**.  
For example, adding JIRA credentials (username-password pair) to the secret store.
3. In the **Field Name** field, add the field name that you want to store as a secret and reference at a later stage.  
**Note:** The restrictions that apply to the Name field also apply to the Field Name field.  
For our example, add **JIRAUserName** in this field.
4. In the **Field Value** field, add the value of the field.  
For our example add the username used to access your JIRA instance.
5. Click **Save**.  
To revert the changes that you have made, click **Revert**.  
To delete the secret field click **Remove**. To delete secrets, you must also be assigned the **Delete** permission on the **Secrets** module.  
For our example, you can add another secret for the JIRA password, i.e., add **JIRAPassword** in the **Field Name** field, and in the **Field Value** field add the password used to access your JIRA instance and click **Save**.



**Note:** To edit a secret, in case of the **Field Name**, you can just edit its value and click **Save**. To change the value that you have set in the **Field Value** field, click **Set Secret Value** and add the new value. You will not be able to see the older value that you had set in the Field Value field, however you can update its value.

Once you save your **JIRAUsername** and **JIRAPassword** secrets, you can provide the Jinja template of these secrets to users to add to their playbooks that require JIRA credentials, so that the credentials are fetched from the secret store and used for referencing purpose. The Jinja value of these fields are `{{secret_store.JIRAUserName}}` and `{{secret_store.JIRAPassword}}` respectively. Click the **Copying a field's variable reference in jinja format** icon that is present beside the **Field Name** field to copy a field's variable reference in jinja format:



**Figure 62.** Secrets - Copy Variable Reference icon

You can use the Dynamic Values in the Playbook Designer to add Secrets that are in the jinja format to your playbook. For more information, see the *Dynamic Values* section in the “Playbooks Guide.”

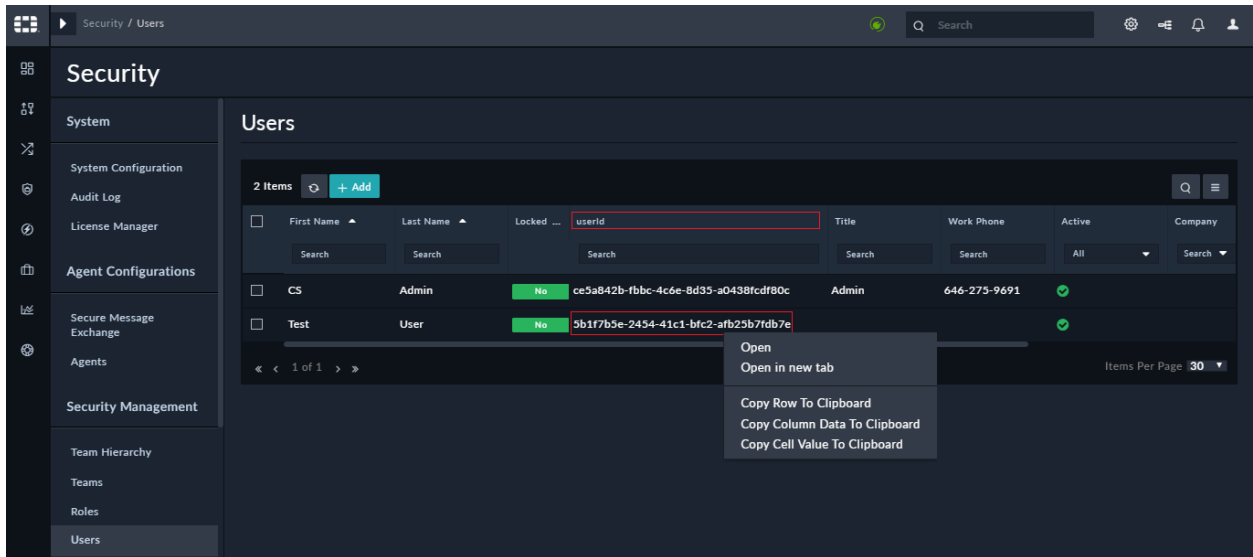
## Delete Users

Apart from the above functions that an administrator can perform on the FortiSOAR™ UI, administrators can also delete users using a script.

**Warning:** It is highly recommended that you use this script to delete or cleanup users during the initial stages of setting up your FortiSOAR™ system. If you delete users who have been using FortiSOAR™ for a while, then the records for which the deleted user was the only owner, will also be lost forever.

To delete users, perform the following steps:

1. Enter the `userID` of the user(s) that you want to delete in the `usersToDelete.txt` file, which is located at `/opt/cyops/configs/scripts/`.  
The ID of uses is displayed on the FortiSOAR™ UI as shown in the following image:



To copy the user ID, right-click the userID cell and from the context menu, select the **Copy Cell Value To Clipboard** option.

The `usersToDelete.txt` file is an empty text file in which you can enter the ID of users.

- SSH to your FortiSOAR™ VM and login as a `root` user.
  - Run the following command: `# /opt/cyops/configs/scripts/userDelete`
- Important:** The User Delete script deletes users in the local database and does not work for externalized databases.

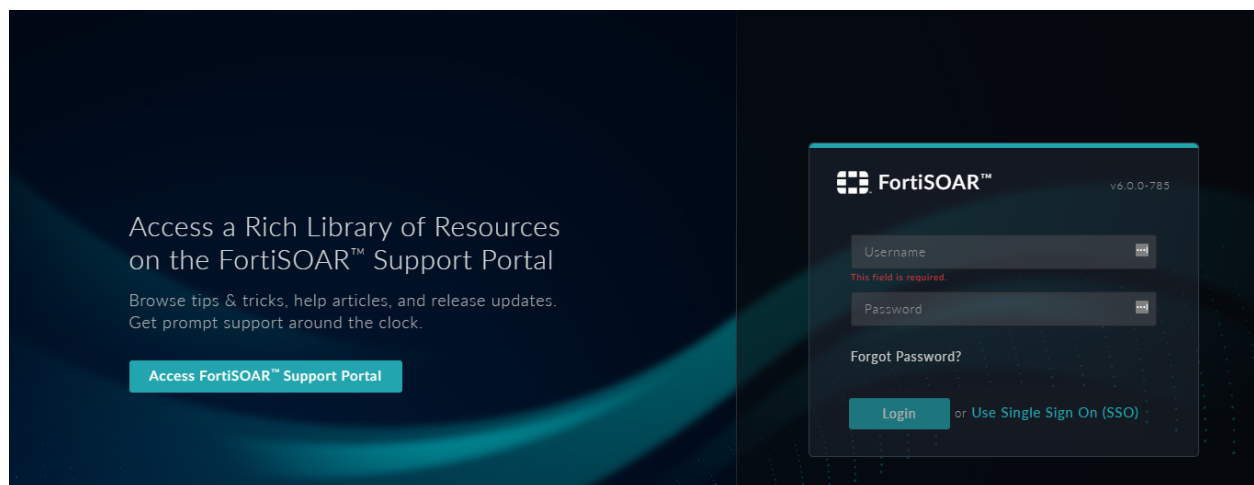


## SAML Configuration

### Introduction

Security Assertion Markup Language (SAML) is an XML-based, open standard data format for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider. The single most important requirement that SAML addresses are web browser single sign-on (SSO).

By using SAML, FortiSOAR™ does not require to store user credentials, and FortiSOAR™ is independent of the underlying authentication mechanism used by a user. Once you complete making all the SAML configurations on both the FortiSOAR™ and Identity Provider (IdP) side, then the FortiSOAR™ login page will display a **Use Single Sign On (SSO)** link. Users can then log on to FortiSOAR™ using the **Use Single Sign On (SSO)** link that is present on the FortiSOAR™ login page.



**Figure 63.** *FortiSOAR™ login page with Single Sign-On*

Once the user clicks the **Use Single Sign On (SSO)** link, the user is redirected to a third-party identity provider login page, where the user must enter their credentials and get themselves authenticated. Once a user successfully logs on to FortiSOAR™, the user profile automatically gets created. The User profile is created based on the configurations you have set while [Configuring SAML in FortiSOAR™](#). For example, when the user is created, the user is assigned the default team and role based on what the administrator configured during SAML configuration. Users can update their profile by editing their user profile.

You can map the role and team of SSO users in FortiSOAR™ based on their roles defined in the IdP. Thereby you can set different roles for different SSO users, i.e., you can set the role of an SSO user in FortiSOAR™ based on the role you have defined in your IdP. For more information, see [Support for mapping roles and teams of SSO users in FortiSOAR™](#).

## Benefits of SAML

**User experience:** SAML provides the ability for users to securely access multiple applications with a single set of credentials entered once. This is the foundation of the federation and single sign-on (SSO). Using SAML, users can seamlessly access multiple applications, allowing them to conduct business faster and more efficiently.

**Security:** SAML is used to provide a single point of authentication at a secure identity provider, meaning that user credentials never leave the firewall boundary, and then SAML is used to assert the identity to others. This means that applications do not need to store or synchronize identities, which in turn ensures that there are fewer places for identities to be breached or stolen.

**Standardization:** The SAML standardized format is designed to interoperate with any system independent of implementation. This enables a more open approach to architecture and identity federation without the interoperability issues associated with vendor-specific approaches.

## SAML Principles

### Roles

SAML defines three roles: Principal (generally a user), Identity Provider (IdP), and the Service Provider (SP).

#### *Principal*

The principal is generally a user that has an authentic security context with IdP and who requests a service from the SP.

#### *Identity Provider (IdP)*

IdP is usually a third-party entity outsourced to manage user identities, or in other terms, an IdP is a user management system. The IdP provides user details in the form of assertions. Before delivering the identity assertion to the SP, the IdP might request some information from the principal, such as a username and password, to authenticate the principal. SAML specifies the assertions between the three parties: in particular, the messages that assert identity that is passed from the IdP to the SP. In SAML, one identity provider can provide SAML assertions to many service providers. Similarly, one SP might rely on and trust assertions from many independent IdPs.

#### *Service Provider (SP)*

The SP maintains a security wrapper over the services. When a user request for a service, the request first goes to the SP, who then identifies whether a security context for the given user exists. If not, the SP requests and obtains an identity assertion from the IdP. Based on

this assertion, the service provider makes the access control decision and decides whether to perform some service for the connected principal.

## Attribute Mapping

Each IdP has its own way of naming attributes for a user profile. Therefore, to fetch the attribute details for a user from an IdP into the SP, the attributes from the IdP must be mapped to attributes at the SP. This mapping is taken care in a separate part at the SP. If the attribute mapping is not set correctly, the SP sets default values for mandatory attributes like First Name, Last Name, and Email.

## Prerequisites to configuring SAML

- Ensure that you are assigned a security administrator role that at a minimum has **Read**, **Create** and **Update** permissions on the **Security** module. You also require to have **Read** permissions for **Teams** and **Roles**.
- Ensure that you have enabled SAML in your FortiSOAR™ instance. To enable SAML, log on to FortiSOAR™, click **Settings**. In the **Security Management** section click **Authentication** to open the **Authentication Configuration** page. Click the **SSO Configuration** tab and click the **SAML Enabled** checkbox.

## Configuring SAML in FortiSOAR™

Configuring SAML is a two-way process. The SP configuration that is present in the FortiSOAR™ UI must be made at the IdP. Similarly, the IdP configuration must be added to the FortiSOAR™ UI.

This section covers configuring SAML with five IdPs, namely, OneLogin, Auth0, Okta, Google, Active Directory Federation Services (ADFS) which are the five IdPs that have been tested with FortiSOAR™. You can use a similar process to configure any other IdP that you use.

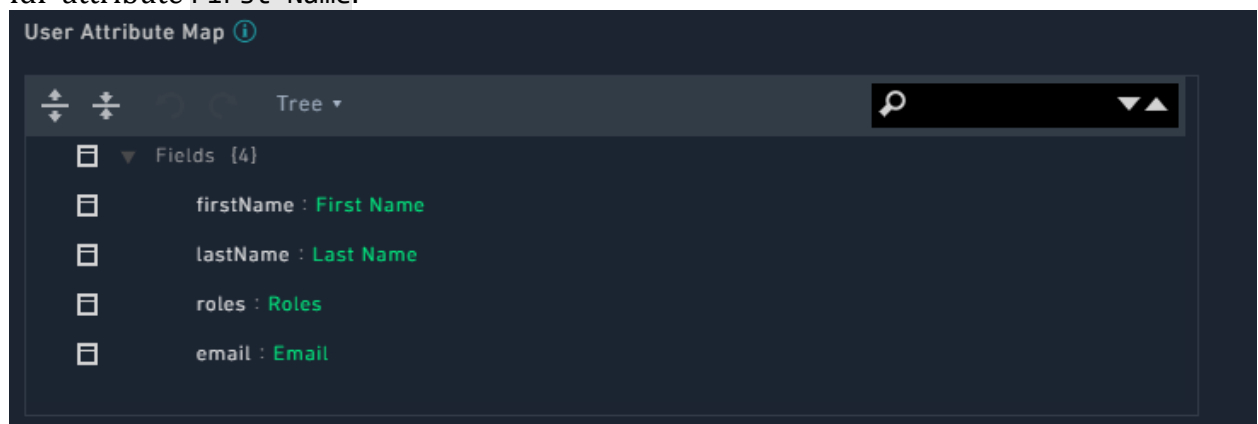
1. Log on to FortiSOAR™ as an administrator.
2. Click **Settings > Authentication > SSO Configuration**.
3. To enable SAML for FortiSOAR™, click the **SAML Enabled** check box.
4. In the **Identity Provider Configuration** section, enter the IdP details.  
Get the details for FortiAuthenticator (FAC) from the [Configuring SAML in FortiAuthenticator](#) section  
Get the details for OneLogin from the [Configuring SAML in OneLogin](#) section.  
Get the details for Auth0 from the [Configuring SAML in Auth0](#) section.  
Get the details for Okta from the [Configuring SAML in Okta](#) section.  
Get the details for Google from the [Configuring SAML in Google](#) section. You must have an administrator account for your G Suite account.  
For information on Configuring SAML in FortiSOAR™ for Active Directory Federation

Services (ADFS) from the [Configuring SAML in ADFS](#) section. For specific information about the values, you need to add for the SSO configuration, see [Configuring FortiSOAR™ for ADFS](#).

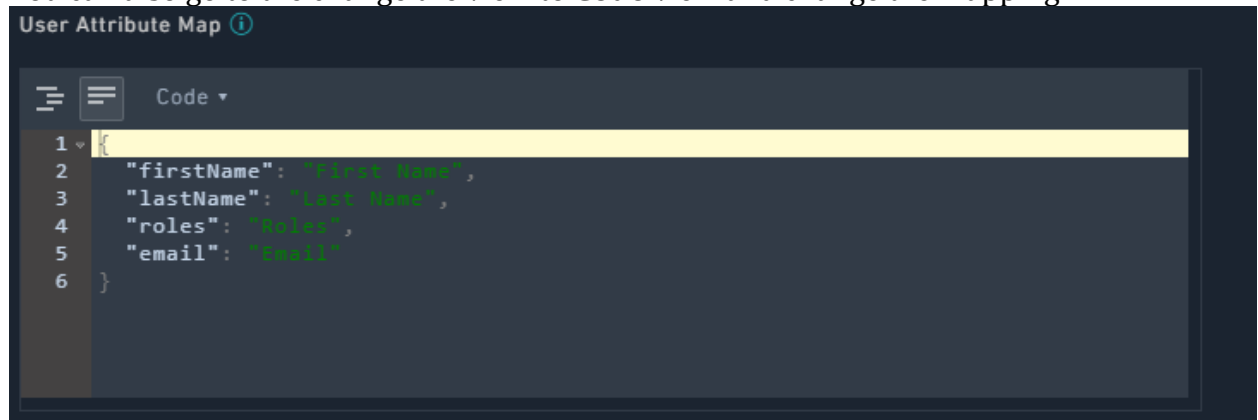
5. Map the user attributes received from the IdP with the corresponding attributes of FortiSOAR™.

Use the **User Attribute Map** to map the attributes received from the IdP with the corresponding attributes required by FortiSOAR™. FortiSOAR™ requires the firstname, lastname and email attributes to be mapped.

In the **User Attribute Map**, under **Fields**, in the **Tree** view, click the editable field name (right side field name), to map it to the attribute that will be received from the IdP. The non-editable field name (left-side field name) is the FortiSOAR™ attribute. For example, in the following image, you map the FortiSOAR™ attribute **firstname** to the IdP attribute **First Name**.



You can also go to the change the view to **Code** view and change the mapping:



6. To map roles that you have defined in your IdP (see [Support for mapping roles and teams of SSO users in FortiSOAR™](#)) to teams and roles in FortiSOAR™, do the following:
  - a. If you want to ensure that roles defined as part of SAML role mapping will be applied to SSO users in FortiSOAR™, then select the **Enforce SAML Role**

## Mappings checkbox.

**Team and Role Mapping**  
Map SAML Roles and Teams in FortiSOAR™

☒ **Enforce SAML Role Mappings** | Enforcing this setting will ensure that the roles defined as part of SAML role mapping will be applied. Any changes made in the user level roles in FortiSOAR™, will not be taken into account.

[+ Add Role Mapping](#)

**SAML Roles**  
Choose from existing SAML roles mappings to view its assigned roles and teams in FortiSOAR™

Default (Fallback Role) [Edit](#) [Delete](#)

**!** Roles and team configuration defined under "Default" would be used as fallback in cases when there is no role mapping defined in FortiSOAR™ or no mapping is present in FortiSOAR™ for a role in SAML.

**Assigned Roles**  
No Roles assigned.

**Assigned Teams**

- b. To map a role in the IdP to a FortiSOAR™-role and optionally a team in FortiSOAR™, in the **Team and Role Mapping** section, click **Add Role Mapping**.
- c. In the **Add New Role Mapping** dialog, do the following:
  - i. In the **SAML Role** field, add the name of the roles that you have defined in your IdP.  
**Note:** The name that you have specified in your IdP, and the name that you enter in this field must match exactly, including the matching the case of the name specified.
  - ii. From the **Roles** column, select the FortiSOAR™ role(s) that you want to assign to the role that you have specified in the SAML Role field.
  - iii. (Optional) From the **Teams** column, select the FortiSOAR™ teams(s) that you want to assign to the role that you have specified in the SAML Role field.

**ADD NEW ROLE MAPPING**

SAML Role ⓘ  
oneLoginSAMLRole

Roles		Teams	
<input type="checkbox"/>	NAME ▲	DESCRIPTION	
<input type="checkbox"/>	Application Administrator	Full access to general application...	
<input checked="" type="checkbox"/>	Full App Permissions	Essentially the root user, use caref...	
<input type="checkbox"/>	Playbook Administrator	Permitted across all major module...	
<input type="checkbox"/>	Security Administrator	Manages the Roles and Teams area...	
<input type="checkbox"/>	T1 Analyst	Responsible for Alert Triaging, fals...	
<input type="checkbox"/>	T2 Analyst	Responsible for Incident Investigati...	

<input checked="" type="checkbox"/>	TEAM NAME ▲	DESCRIPTION
<input checked="" type="checkbox"/>	SOC Team	Management team

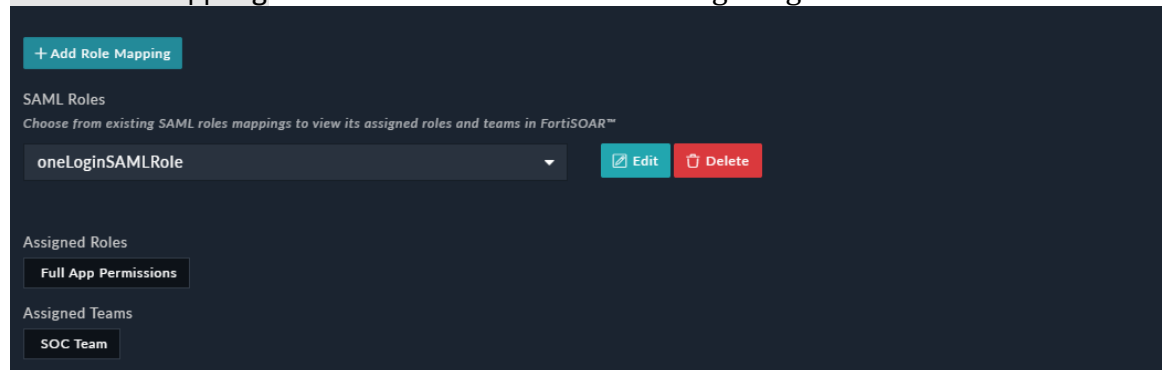
Cancel [Add Mapping](#)

Once you assign the default team and roles to users, all user profiles created contain this team and role assigned to them.

If you do not assign the default team and roles to users, and you have also not defined a **Default (Fall Back Role)**, details given in a further step in this procedure, then all user profiles are created without team or role information and will have only basic access. In this case, users will require to request the administrator for appropriate access and privileges.

iv. Click **Add Role Mapping**.

This adds the mapped role in the SAML Roles drop-down list in the **Team and Role Mapping** section as shown in the following image:



As shown in the above image, the **oneLoginSAMLRole**, i.e., the role defined in the IdP has been mapped to the **Application Administrator** role and the **SOC Team** in FortiSOAR™.

- d. To define a default role (and optionally teams) that will be assigned to the SSO user if you have not set up mapped roles of SSO users in FortiSOAR™, or if FortiSOAR™ receives a response from the IdP that does not contain any roles, or receives a response that does not map to any of the FortiSOAR™ roles, do the following:
  - i. From the **SAML Roles** drop-down list, select **Default (Fall Back Role)** and click **Edit**.
  - ii. In the **Update Role Mapping** dialog, from the **Roles** column select the role(s) that you want to assign to the default role. You can also optionally select the team(s) that you want to assign to the default role from the **Teams** column and click **Update Mapping**.
- e. (Optional) To delete or update an existing role do the following:
  - i. To update an existing role, select the role from the **SAML Roles** drop-down list and click **Edit** and in the **Update Role Mapping** dialog, you can update the name of the mapped SAML role, and the mapped FortiSOAR™ roles and teams.

Once you have completed modifying the existing role as per your requirement, click **Update Mapping**.

- ii. To delete an existing role, select the role from the **SAML Roles** drop-down list and click **Delete**.  
FortiSOAR™ displays a confirmation dialog, click **Confirm** to delete the role.
7. Add the information provided in the **Service Provider** section to **Configuration** section your IdP.  
This information is pre-configured. However, you can edit the fields, such as **Entity ID** (hostname) within this section. This is especially useful if you are using an alias to access FortiSOAR™. You can also edit the certificate information and the private and public keys of your service provider, which is useful in cases where you want to use your own certificates.

**Service Provider**  
Configuration

Entity ID ⓘ

ACS URL ⓘ

Logout Redirect URL ⓘ

Logout POST URL ⓘ

X509 Certificate ⓘ 

```
-----BEGIN CERTIFICATE-----
MIIFtTCCAS2gAwIBAgIJA0ihHr13izm8MA0GCSqGSIb3DQEBBQUAMEUxOzA7BgNV
BAYTAkFVMHRmEQYDVQIEwPb211LVN0YXR1MSEwHwYDVQQKEWhbnR1cm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNDEwMTEyNTA4WjcNMjAwNDA5MTEyNTA4WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECBKU29tZS1TdGF0ZTEhMB8GA1UEChMYSM50
ZXJuZXQvV2lkZ210cy8QdHkgTHRkMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEazB0AC+G/emNtH11J7Juo+3kVihpkfsMhXpyKB61n48n3FMeTkV9DESEJ
r40BUp6idntGk4gyLKLq1ApJiYs11Ups2vW211/aKNy5IUo+088bw05NUcvv4Spi
```

Public Key ⓘ

Service Provider Metadata ⓘ

For OneLogin, enter this information in the **Configure IdP** step. See the [Configuring SAML in OneLogin](#) section for more details.

For Auth0, enter this information in the **Configure IdP** step. See the [Configuring SAML in Auth0](#) section for more details.

For Okta, enter this information in the **Configure IdP** step. See the [Configuring SAML in Okta](#) section for more details.

8. (Optional) Configure advanced settings for SAML.  
Select the **Auth Request Signed** checkbox if your IdP requires FortiSOAR™ to send signed authentication requests.  
Select the **Logout Request Signed** checkbox if your IdP requires FortiSOAR™ to send signed logout requests.  
Select the **Messages Signed** checkbox if you want messages coming from your IdP to be signed.  
Select the **Assertion Encrypted** checkbox if you want assertions within the

SAMLResponse to be encrypted.

**Advanced Properties**  
SAML Advanced Settings

**Security Configuration**

☐ Auth Request Signed ⓘ ☐ Logout Request Signed ⓘ ☐ Messages Signed ⓘ ☐ Assertions Encrypted ⓘ

9. Click **Save** to complete the SAML configuration in FortiSOAR™.

## Configuring SAML in FortiAuthenticator

1. Log on to FortiAuthenticator (FAC) as an administrator.
2. Configure IdP. To configure general SAML IdP portal settings, navigate to **Authentication > SAML IdP > General**, and then select **Enable SAML Identity Provider portal**.

**Edit SAML Identity Provider Settings**

☒ Enable SAML Identity Provider portal

Device FQDN: fac.school.net

Server address:

Username input format:   
☒ username@realm   
☐ realm\username   
☐ realm/username

Realms: 

Default ⓘ	Realm	Allow local users to override remote users	Groups ⓘ	Delete
-----------	-------	--	----------	--------

Login session timeout:  minutes (5-1440)

IdP certificate:

3. In the **Edit SAML Identity Provider Settings** section, enter the following details:
  - **Device FQDN:** To configure this setting, you must enter a Device FQDN in the System Information widget in the Dashboard.
  - **Server address:** Enter the IP address, or FQDN, of the FAC device.
  - **Username input format:** Select one of the following three username input formats:
    - username@realm
    - realm\username
    - realm/username
  - **Realms:** Select **Add a realm** to add the default local realm with which the users will be associated. Use **Groups** and **Filters** to add specific user groups.
  - **Login session timeout:** Set the user's login session timeout limit between 5 - 1440 minutes (one day). The default is 480 minutes (eight hours).
  - **IDP certificate:** Select a certificate from the dropdown menu.
4. Configure a Service Provider. Navigate to **Authentication > SAML IdP > Service Providers**, and then click **Create New**.



Create New SAML Service Provider

SP name:

IDP prefix:

[Generate unique prefix]

IDP address:

Please configure SAML IDP server address first.

IDP entity id:

http://www.example.com/saml-idp/xxx/metadata/

IDP single sign-on URL:

https://www.example.com/saml-idp/xxx/login/

IDP single logout URL:

https://www.example.com/saml-idp/xxx/logout/

[Download IDP metadata]

[Import SP metadata]

SP entity ID:

SP ACS (login) URL:

[Alternative ACS URLs]

SP SLS (logout) URL:

☒ SAML request must be signed by SP

Certificate fingerprint:

[Import SP certificate]

Fingerprint algorithm:

Unknown

Authentication

Authentication method:

☐ Enforce two-factor authentication
 ☒ Apply two-factor authentication if available (authenticate any user)
 ☐ Password-only authentication (exclude users without a password)
 ☐ FortiToken-only authentication (exclude users without a FortiToken)

☒ Bypass FortiToken authentication when user is from a trusted subnet

[Configure subnets]

Debugging Options

☒ Do not return to service provider automatically after successful authentication, wait for user input.

☐ Disable this service provider

Assertion Attributes

Subject NameID:

Username

Format:

Unspecified

OK

Cancel

In the **Create New SAML Service Provider** section, enter the following information:

- **SP name:** Enter the name of the Service Provider (SP).
- **IDP prefix:** Enter a prefix for the IDP that will be appended to the end of the IDP URLs.  
Alternatively, you can select **Generate unique prefix** to generate a random 16 digit alphanumeric string.
- **IDP address:** To configure the IDP address (and IDP settings below), you must have already configured the server's address in **Authentication > SAML IdP > General**.
- **SP entity id:** Enter the entity ID of the SP. Retrieve the SP entity id, SP ACS URL, and SP SLS URL from FortiSOAR™ by navigating to **Settings > Authentication > SSO Configuration**. Then click the **Service Provider Configuration** section to get these details.  
Alternatively, you can download the metadata of the SP from FortiSOAR™ and import the same here.
- **SP ACS (login) URL:** Enter the Assertion Consumer Service (ACS) login URL of the SP.
- **SP SLS (logout) URL:** Enter the Single Logout Service (SLS) logout URL of the SP.

- **SAML Attributes:** Map the User attributes to SAML attributes. This is needed so that users created in FortiSOAR™ have the correct details.

SAML attributes must be configured as shown in the following image:

SAML Attribute	User Attribute	Actions
First Name	First name	
Last Name	Last name	
Email	Email	
Roles	FAC local group	

**Important:** You must not change the **SAML Attribute** names as these are the attribute names expected by FortiSOAR™. You can change the **User Attribute** names as per your requirement.

The remaining fields can be left unmodified, or can be modified as per your requirement.

You must download the IdP metadata.

5. In FortiSOAR™, navigate to **Settings > Authentication > SSO Configuration**, and then enter the following details in the Identity Provider Configuration section:

### Identity Provider Configuration

Entity ID \* ⓘ

`http://192.168.51.220/saml-idp/xl8dqhrsh4zbfcez/metadata/`

Single Sign On URL \* ⓘ

`https://192.168.51.220/saml-idp/xl8dqhrsh4zbfcez/login/`

Single Logout Request URL ⓘ

`https://192.168.51.220/saml-idp/xl8dqhrsh4zbfcez/logout/`

X509 Certificate\* ⓘ

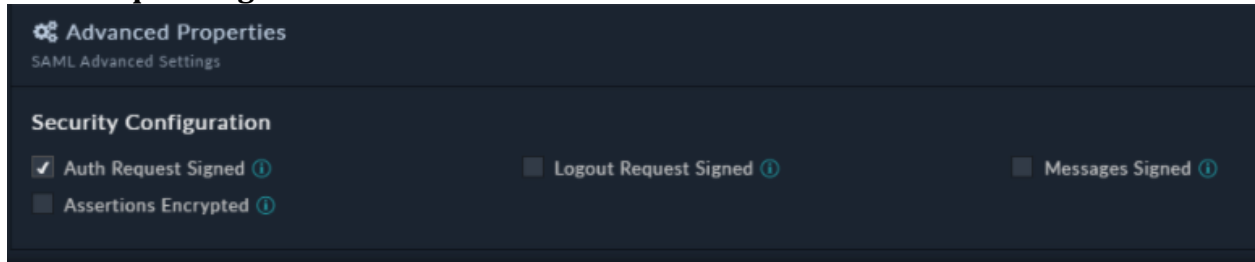
```

MIIGsDCCBjgAwIBAgIIzES25EQ1ReswDQYJKoZIhvcNAQELBQAwgZQxCzAJBgNVBAYTAIVTMRMwE
QYDVQQIDApDYWxpZm9ybmlhMRlwEAYDVQQHDAITdW5ueXZhbGUxETAPBgNVBAoMCEZvcnRpbm
V0MRswGQYDVQQLDBJGbzJ0aWF1dGhlnbnRyY2F0b3IxLDAqBgNVBAMMI0RIZmF1bHQtU2VydM
VYUNlcnRpZmljYXRILTAyM0E2RkM3MB4XDTEwMDkwnZmF1bHQtU2VydM1NFowgZQxCzAJBg
NVBAYTAIVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRlwEAYDVQQHDAITdW5ueXZhbGUxETAPBg
NVBAoMCEZvcnRpbmV0MRswGQYDVQQLDBJGbzJ0aWF1dGhlnbnRyY2F0b3IxLDAqBgNVBA
MMI0RIZmF1bHQtU2VydM1NFowgZQxCzAJBgNVBAYTAIVTMRMwEQYDVQQIDApDYWxpZm9ybmlh
MRlwEAYDVQQHDAITdW5ueXZhbGUxETAPBgNVBAoMCEZvcnRpbmV0MRswGQYDVQQLDBJGbzJ0a
WF1dGhlnbnRyY2F0b3IxLDAqBgNVBA

```

- **Entity ID:** Enter the **IDP entity id** from the **Create New SAML Service Provider** section mentioned in step 4.
- **Single Sign On URL:** Enter the **IDP single sign-on URL** from the **Create New SAML Service Provider** section mentioned in step 4.
- **Single Logout Request URL:** Enter the **IDP single logout URL** from the **Create New SAML Service Provider** section mentioned in step 4.
- **X509 Certificate:** Retrieve the signing certificate from IDP metadata that you have downloaded in step 4 and enter it in this field. The signing certificate is located under the `<md:KeyDescriptor use="signing">` key in the metadata xml file.

- **Advanced Properties:** In the **Security Configuration** section, ensure that the **Auth Request Signed** checkbox is enabled:



- For **Team and Role Mapping**, the Role name can be given as the 'User Group' name from FortiAuthenticator that is present in **Authentication > User Management > User Groups**. You can utilize an existing Group or create a new one as per your requirement. The login user should be from the same group as mentioned in 'Team and Role' mapping.
6. Click **Save** in FortiSOAR™ to save the changes to the IdP configuration.

## Configuring SAML in OneLogin

1. Log on to OneLogin as an administrator.
2. Create a new application in OneLogin. Navigate to **APPS > Company Apps > ADD APP**. In the Find Applications section, search for **saml** and select **SAML Test Connector (IDP w/attr w/sign response)**. Save the application.



3. Configure IdP. On the SAML Test Connector (IDP w/attr w/sign response), click the **Configuration** tab and enter your SP details as shown in the following image:

← SAML Test Connector (IdP w/ attr w/.. MORE ACTIONS SAVE

Info	Configuration	Parameters	Rules	SSO	Access	Users	Privileges
<b>Application Details</b>							
RelayState		<input type="text"/>					
Audience		<input type="text" value="https://dev.cyber/api/saml/metadata"/> <span>Entity ID</span>					
Recipient		<input type="text" value="https://dev.cyber/api/public/saml/lo"/> <span>ACS URL</span>					
ACS (Consumer) URL Validator*		<input type="text" value="https://dev.cyber/api/public/saml/lo"/> <span>ACS URL</span>					
*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest							
ACS (Consumer) URL*		<input type="text" value="https://dev.cyber/api/public/saml/lo"/> <span>ACS URL</span>					
*Required							
Single Logout URL		<input type="text" value="https://dev.cyber/logout"/> <span>Logout Redirect URL</span>					

4. Get SSO details. On the SAML Test Connector (IDP w/attr w/sign response), click the **SSO** tab and you will see the SSO details of OneLogin (IdP) as shown in the following

image:

The screenshot displays the 'SSO' configuration page in FortiSOAR. The page has a top navigation bar with tabs: Info, Configuration, Parameters, Rules, **SSO** (active), Access, Users, and Privileges. Below the navigation bar, the 'Enable SAML2.0' section is active. It includes the following settings:

- Sign on method:** SAML2.0
- X.509 Certificate:** Standard Strength Certificate (2048-bit) with a 'Change | View Details' link.
- SAML Signature Algorithm:** SHA-1 (selected from a dropdown menu).
- Issuer URL:** https://app.onelogin.com/saml/metadata/647489
- SAML 2.0 Endpoint (HTTP):** https://mailinator-dev.onelogin.com/trust/saml2/http-post/s
- SLO Endpoint (HTTP):** https://mailinator-dev.onelogin.com/trust/saml2/http-redire

5. Add the SSO details shown in step 4 in FortiSOAR™. To add the SSO details, log on to FortiSOAR™, click **Settings > Authentication > SSO Configuration**. In the **Identity Provider Configuration** section, enter the IdP details as shown in the following

image:

☒ SAML Enabled ⓘ

### Identity Provider Configuration

Entity ID ⓘ

`https://app.onelogin.com/saml/metadata/647489` ⓘ

Single Sign On URL ⓘ

`https://mailinator-dev-onelogin.com/trust/saml2/http-post/sso/647489`

Single Logout Request URL ⓘ

`https://mailinator-dev-onelogin.com/trust/saml2/http-redirect/slo/647489`

X509 Certificate ⓘ

```
-----BEGIN CERTIFICATE-----
MIIFtTCCA52gAwIBAgIJAOihHrI3izm8MA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb211LVN0YXRIMSEwHwCgKCAgEAzB0AC+G.....
-----END CERTIFICATE-----
```

6. Add the default user attribute mapping for OneLogin in FortiSOAR™ by updating the **User Attribute Map** as shown in the following image:

User Attribute Map ⓘ

Tree ▾

Fields {3}

- firstName : User.FirstName
- lastName : User.LastName
- email : User.email

**Note:** You can change the default user attribute mapping if required.

7. Click **Save** in FortiSOAR™ to save the changes to the IdP configuration and user attribute mapping.
8. Create a new user in OneLogin. Log on to OneLogin as an administrator and navigate to the **USERS** main menu and create a new user by clicking on **NEW USER** and entering relevant details. Once the user is created, open the user details, click the **Applications** tab and select the application created in step 2.

**Note:** While attaching the application to the user, the 'SAVE' button might be disabled. To enable the Save button, click any field and then press space or any key and then clear the space or character using backspace.

← test user

MORE ACTIONS
SAVE USER

User InfoAuthenticationApplicationsActivity

Roles

Default

Applications

1
SAML Test Connector
test@email.com
Admin-configured

(IdP w/attr) (Two)

Once the user is created, you must assign the user a password by clicking **MORE ACTIONS**.

## Configuring SAML in Auth0

1. Log on to Auth0 as an administrator.
2. Create a new application in Auth0. In the **Clients** section, create a new client by selecting **Regular Web Applications**.
3. Configure IdP (Auth0). In Auth0, go to the **Addon** tab of the application you have created in step 1 and select **SAML2 WEB APP**. On the **Settings** page that appears, in the **Application Callback URL** field enter the **ACS URL** from your SP configuration. In the **Settings** field, uncomment the logout portion and set the **callback** field to the value that is present in the **Logout POST URL** field that is present in the **Service Provider**





5. Add the SSO details shown in step 4 in FortiSOAR™. To add the SSO details, log on to FortiSOAR™, click **Settings > Authentication > SSO Configuration**. In the **Identity Provider Configuration** section, use the Identity Provider Metadata to fill in the **Entity ID**, **Single Sign On URL**, **X509 Certificate**, and **Single Logout Request URL** details.

Based on Identity Provider Metadata screenshot in step 4, you would fill in the SSO details in FortiSOAR™ as follows:

- In the **Entity ID** field enter the following value that you get from the Identity Provider Metadata:  
`urn:o1084360.auth0.com`
- In the **Single Sign On URL** field enter the following value that you get from the Identity Provider Metadata:  
`https://o1084360.auth0.com/samlp/o9Apfoanc8KS5VqQv0DphA1FLyWhtg`
- In the **Single Logout Request URL** field enter the following value that you get from the Identity Provider Metadata:  
`https://o1084360.auth0.com/samlp/o9Apfoanc8KS5VqQv0DphA1FLyWhtgZm/logout`
- In the **X509 Certificate** field enter the following value that you get from the Identity Provider Metadata:  
`zCCAeegAwIBAgIJZAzJWzHeGwUjMA0GCSqGSIb3DQEBwUAMB0xGzAZBgNVBAMTE8xMDg0MzYwLnF1dGgwLnNvbTAEFw0xNzA0MDEwNzYwMDAwFw0xMDEyMDkxNzYwMDAwGzAZBgNVBAMTE8xMDg0MzYwLnF1dGgwLnNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKH0ggZ4r3jq2iAgrFNZv0IoEJZVKA6mhmpfFiqs8vAlIubtEireTpSfS01SP/Yaw70DamSBZrb06VRCmt+LzsGwsXPJTZDwQORYraA3w4dSp5mnC7VLjyTrmMazRbcw6Egg6N6v+0E48z0Qtd/Fb5wTdiByKmxV8xNYIEhRdcTIRoTjYZ0oc1j26BX7x0e3wYBIZly0JzKRCkZjpeOFZMEC8cmMEJdDS3UEV/4nYsgLV4CB/Y9Wwf4kbyLE1pTAKWbsbdgbBk5aYRxxu1qNhu3ZuUT7AV/PEgXo8J1sFJiru370RVp08Sm14F/Ji2rZk85Loj3hG0+G6CFYkzKnMCaWEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUuRCNNTfA0fiQNeZdDE0nQUwza9Qw0gYDVR0PAQH/BAQDAgKEMA0GCSqGSIb3DQEBwUAA4IBAQB0G53tNSW9wByql+hHZ83268Cow3t8iTeWmkW9PLYZIL6AviKgN7Xa8vHos05/Kf0p5A1MoXKJ460kUIEhusDIufBGNC7i3c3UpZYgaLcIDrf5BXPjUYCQW+ogiQPCuadrZjeIngAmMsV/ChEucbYUD/mDwUqLc3RQ+0+cBhtfQ0eGSivAogm0bbkoB3xwL1hUn+XI3UEC3zLLTNj72FXadDt57Pp9p4acIOnm1kR/Ynq0B1MxUNLcM7a1nvSwgwSU6zu81PUZkhuFb8VnVA2QXh0zrKVENWhL8Bf2Dbn9W0kPychGxDrgnTCBF+VZTqdZf/n9a7E00AGbK7Nw`
- Click **Save** in FortiSOAR™ to save the changes to the IdP configuration and user attribute mapping.

## Configuring SAML in Okta

1. Log on to Okta as an administrator.  
If you don't have an Okta organization, you can create a free [Okta Developer Edition organization](#).
2. Create a new application in Okta and configure IdP in the application.
  - In Okta, click the blue **Admin** button.
  - On the **Applications** tab, click **Add Applications > Create New App**.

- On the **Create a New Application Integration** dialog, select **SAML 2.0** and click **Create**.

Create a New Application Integration

What type of application integration?

☐ Secure Web Authentication (SWA)  
Uses the Okta plugin to log users into the app. This integration works with most web-based apps

☒ SAML 2.0  
Uses the SAML protocol to log users into the app. The app must support SAML. This is a better integration when available

Create Cancel

### 3. Configure IdP.

- In the newly created application, on the **General Settings** dialog, in the **App name** field, enter the application name and click **Next**.

1 General Settings

App name: Example SAML Application

App logo (optional) ?

Upload Logo

App visibility

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile app

- On the **Configure SAML** dialog, in the **SAML Settings** section, in the **Single Sign On URL** field, enter or paste the **SP ACS URL** and in the **Audience URI** field,

enter or paste the **SP Entity ID**.

**GENERAL**

Single sign on URL ?  🔍

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

- Click **Show Advanced Settings**.
- Select the **Enable Single Logout** checkbox.  
In the **Single Logout URL** field, enter or paste the SP Logout POST URL.  
In the **SP Issuer** field, enter or paste the SP Entity ID.  
In the **Signature Certificate** field, browse to where you have downloaded the SP X509 certificate and click **Upload Certificate**.

Enable Single Logout ? ☒ Allow application to initiate Single Logout

Single Logout URL ?

SP Issuer ?

Signature Certificate ?  Browse..

Upload Certificate

- In the **ATTRIBUTE STATEMENTS (OPTIONAL)** section, set the mapping as shown in the following image:

**ATTRIBUTE STATEMENTS (OPTIONAL)** LEARN MORE

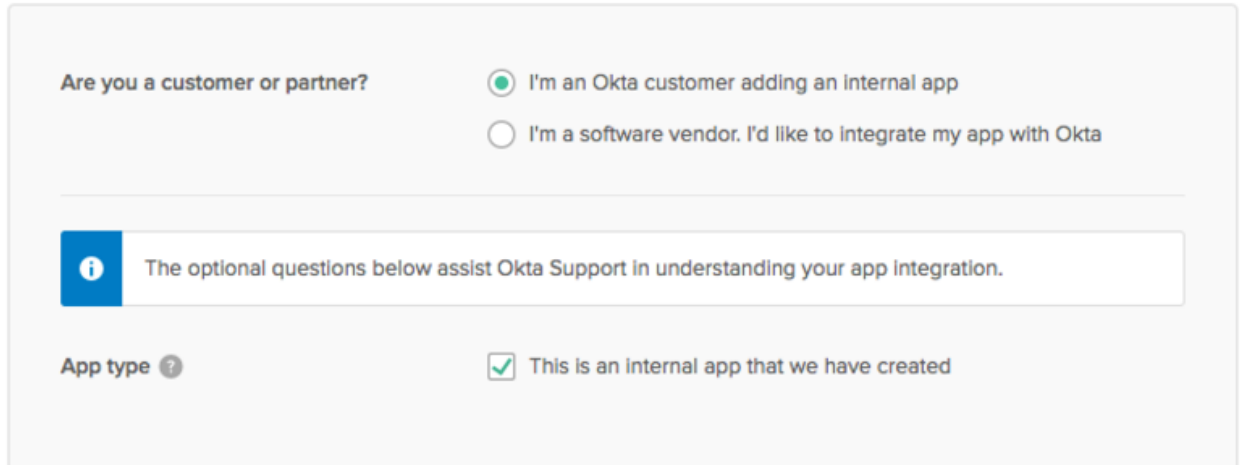
Name	Name format (optional)	Value
First Name	Unspecified ▼	user.firstName ▼ ×
Last Name	Unspecified ▼	user.lastName ▼ ×
Email	Unspecified ▼	user.email ▼ ×

**Note:** You must remember the attribute names specified in the above image. You will require to map these user attribute names while configuring the **User Attribute Map** on the **SSO Configuration** page in FortiSOAR™.

- Click **Next**.

- On the Help Okta Support understand how you configured this application dialog, select **I'm an Okta customer adding an internal app**, and **This is an internal app that we have created**.

**3** Help Okta Support understand how you configured this application



The screenshot shows a configuration dialog for Okta. At the top, it asks "Are you a customer or partner?" with two radio button options: "I'm an Okta customer adding an internal app" (which is selected) and "I'm a software vendor. I'd like to integrate my app with Okta". Below this is a horizontal line, followed by an information icon and the text "The optional questions below assist Okta Support in understanding your app integration." Underneath that is the "App type" label with a help icon, and a checked checkbox for "This is an internal app that we have created".

- Click **Finish**.  
The **Sign On** tab of your newly created SAML application gets displayed. Keep this page open in a separate tab or browser window as you will require the information present on this page to complete the **Identity Provider**

## Configuration section in FortiSOAR™.

General

Sign On

Import

People

Groups

### Settings

Edit

#### SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

☒ SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState



**SAML 2.0** is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#)



**Copy this link**

ports dynamic configuration.

#### APPLICATION USERNAME

The default username that is pre-filled when an application is assigned to a user.

Application username format

Okta username

4. Get SSO details. Click **View Setup Instructions** and information as shown in the following image:

- 1 Identity Provider Single Sign-On URL:  
`https://dev-696354.oktapreview.com/app/companydev696354_test_1/exkaf81i2vLW0tIlt0h7/sso/saml`
- 2 Identity Provider Single Logout URL:  
`https://dev-696354.oktapreview.com/app/companydev696354_test_1/exkaf81i2vLW0tIlt0h7/slo/saml`
- 3 Identity Provider Issuer:  
`http://www.okta.com/exkaf81i2vLW0tIlt0h7`
- 4 X.509 Certificate:  
-----BEGIN CERTIFICATE-----  
MIIDpDCCAoygAwIBAgIGAVsye0tzMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG  
A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU  
MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAhMcRldi02OTYzNTQxHDAaBgkqhkiG9w0BCQEW  
DW1uZm9Ab2t0YSSjY2b20wHhcNMjcwNDAzMjYxOTM3WmcNMjcwNDAzMjYxMDM2WjCBKjELMAkGA1UE  
BhMCVVMxEzARBgNVBAgMCkNhbmG1mb3JuaWExFjAUBgNVBAcMDVNhbGlBQcmFueY21zY28xDTALBgNV

5. Add the SSO details shown in step 4 in FortiSOAR™. To add the SSO details, log on to FortiSOAR™, click **Settings > Authentication > SSO Configuration**. In the **Identity Provider Configuration** section, enter the IdP details as shown in the following image:

### Identity Provider Configuration

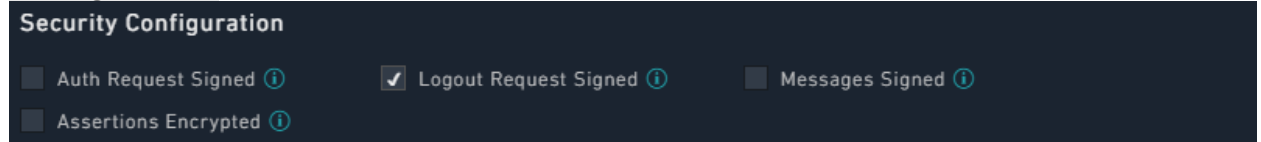
Entity ID \* ⓘ  
`https://okta.com/exka009e0q80e.....`

Single Sign On URL \* ⓘ  
`https://dev-696354.oktapreview.com/app/companydev696354_test_1/exka009e0q80e.....`

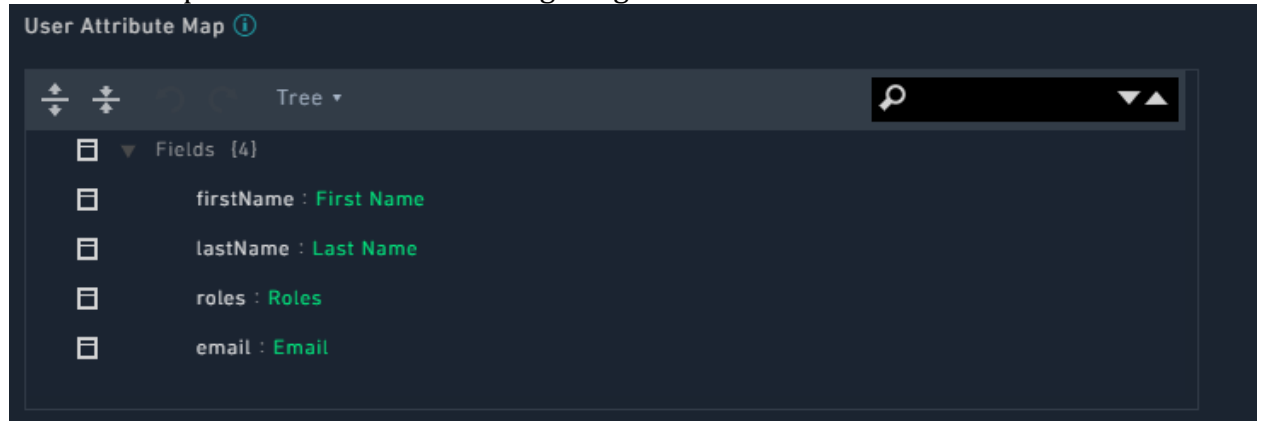
Single Logout Request URL ⓘ  
`https://dev-696354.oktapreview.com/app/companydev696354_test_1/exka009e0q80e.....`

X509 Certificate \* ⓘ  
-----BEGIN CERTIFICATE-----  
CgKCAgEAzB0AC+G/emNtH11J7Juo+3kVihpkfsMhxyKB61n48n3FMeTkV9DESEJ  
r4DBUpGidntGk4gy.....  
-----END CERTIFICATE-----

**Note:** The LogoutRequest message for Okta must be signed for Single Logout (SLO). Therefore, you must select the **Logout Request Signed** checkbox that is present in the Advanced Properties SAML Advanced Settings pane in the Security Configuration section.



6. Add the default user attribute mapping for Okta in FortiSOAR™ by updating the User Attribute Map as shown in the following image



**Note:** The IdP keys, the keys on the right side, are obtained from the ATTRIBUTE STATEMENTS (OPTIONAL) section in Okta, as specified in step 3. You can change the default user attribute mapping later if required.

7. Click **Save** to complete the SSO configuration in FortiSOAR™.
8. Create a new user in Okta. Log on to Okta as an administrator and navigate **Directory > People > Add Person** and enter all the user details.

**Okta** Dashboard Directory Applications Security Reports Settings

**People**

+ Add Person Reset Password

Search...

**FILTERS**

Everyone	2
Activated	2
Pending Activation	0
Password Reset	—
Deactivated	0
Suspended	0
Locked out	0

**Add Person**

First name: Test

Last name: User

Username: test@user.com

Primary email: test@user.com

Secondary email (optional):

Groups (optional): You haven't added any groups

☐ Send user activation email now ?

Save Save and Add Another Cancel

Once the user is created and activated successfully, you can assign this user to the SAML application that you have created. Click on a user to get the user details, and then assign the user to an application using the **Assign Applications** dialog as shown in the following image:

**Test User**  
p72013@mvrt.co  
Active

Applications Groups

**Assigned Applications**

Assign Applications

**Assign Applications**

Search

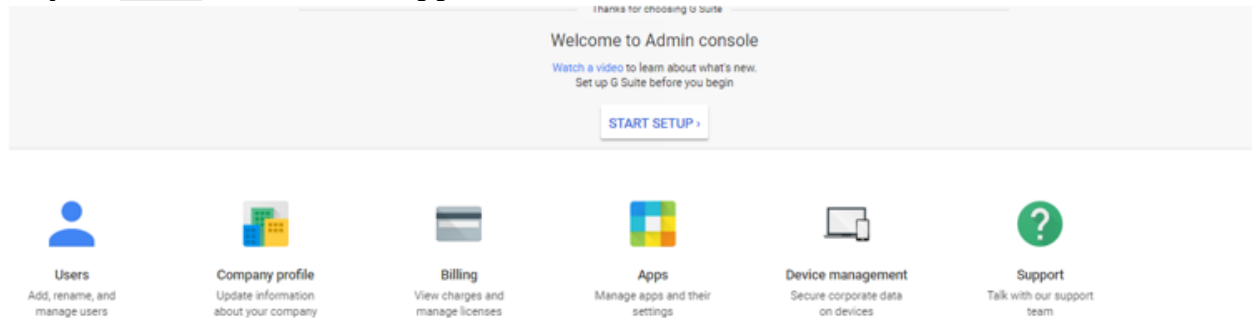
	Saml App One	Assign
	Test	Assign



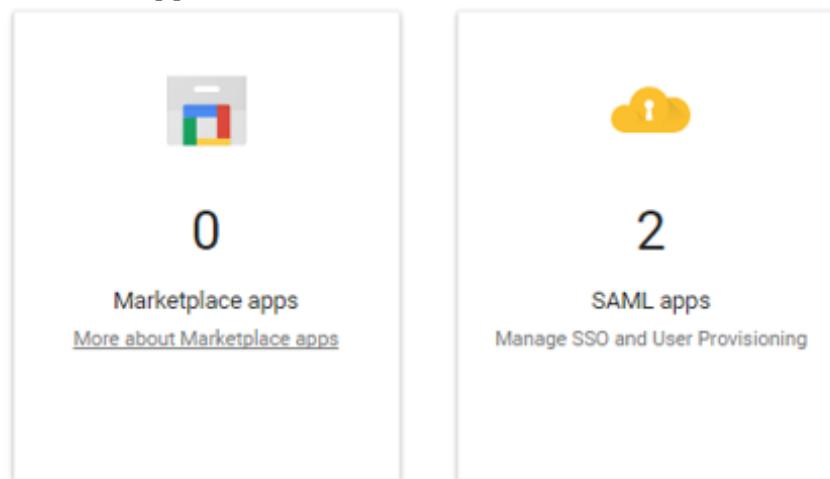
## Configuring SAML in Google

1. Ensure that you have Administrator access for your G Suite account and log on to G Suite using the admin account.
2. Configure IdP.

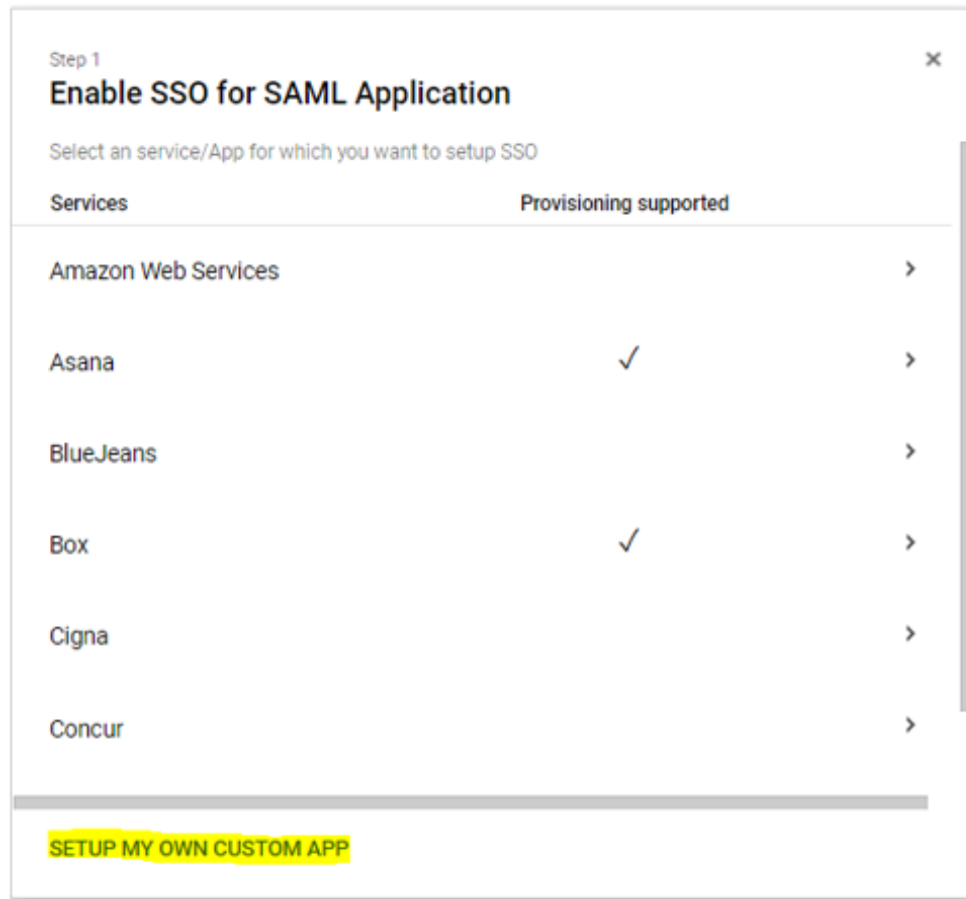
- On your **Admin** console, click **Apps**.



- Click **SAML apps**. On the **SAML** page, click **+** on the right bottom corner, to add a new SAML Application.

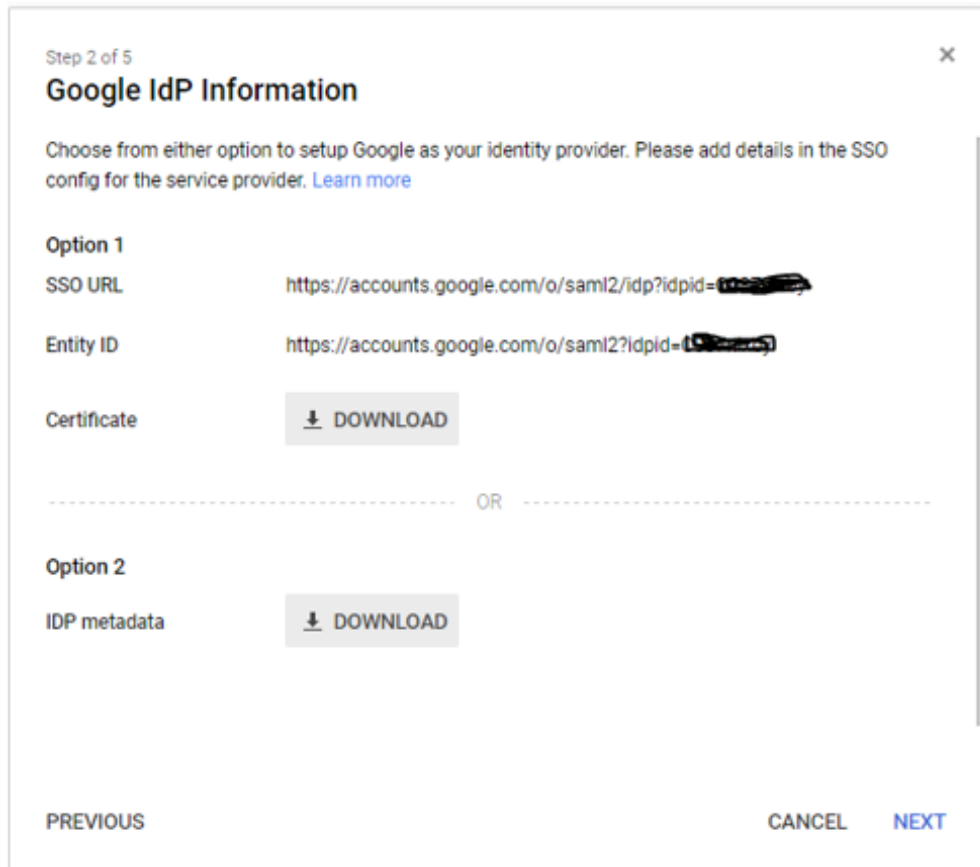


- On the **Enable SSO for SAML Application** page, click **SETUP MY OWN CUSTOM APP**.



- Click **Next** to display the Google IdP information. Save the Google IdP information and download the **Certificate**. You will require the IdP information for Google to configure SSO within

FortiSOAR™.



The screenshot shows a configuration window titled "Google IdP Information" with a close button (X) in the top right corner. The window indicates it is "Step 2 of 5". Below the title, there is a paragraph: "Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)".

Under "Option 1", the following fields are visible:

- SSO URL: `https://accounts.google.com/o/saml2/idp?idpid=` followed by a redacted value.
- Entity ID: `https://accounts.google.com/o/saml2?idpid=` followed by a redacted value.
- Certificate: A button with a download icon and the text "DOWNLOAD".

A dashed line with the word "OR" in the center separates Option 1 from Option 2.

Under "Option 2", the following field is visible:

- IDP metadata: A button with a download icon and the text "DOWNLOAD".



At the bottom of the window, there are three buttons: "PREVIOUS" on the left, "CANCEL" in the center, and "NEXT" on the right.

- Click **Next** and add basic information about the App, such as **Name** and **Description** and then click **Next**.
- On the **Service Provider Details** page, enter the **Entity ID** and **ACS URL** from the **Service Provider** section in FortiSOAR™. Log on to FortiSOAR™ and navigate to **Settings > Authentication > SSO Configuration**, go to the **Service**

**Provider** section to get the details. See [Configuring SAML in FortiSOAR™](#).

## ^ Service Provider Details

Please provide service provider details to configure SSO for CyOPs-QA-ENV1. The ACS url and Entity ID are mandatory.

Application Name	CyOPs- <span style="background-color: black; color: black;">[REDACTED]</span>	 app-id: cyops-qa-env1
Description	SSO Configuration for <span style="background-color: black; color: black;">[REDACTED]</span>	
ACS URL *	https:// <span style="background-color: black; color: black;">[REDACTED]</span> /api/public/saml/login	
Entity ID *	https:// <span style="background-color: black; color: black;">[REDACTED]</span> /api/saml/metadata 	
Start URL		
Signed Response	<input type="checkbox"/>	
Name ID	Basic Information ▼	Primary Email ▼
Name ID Format	EMAIL ▼	

- Click **Next** and add more attribute mapping as required.

## ^ Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

Email	Basic Information ▼	Primary Email ▼
FirstName	Basic Information ▼	First Name ▼
LastName	Basic Information ▼	Last Name ▼

ADD NEW MAPPING

- Save the app configuration and click **Exit**.
  - Set up user access for the Google SAML App, see [Set up your own custom SAML application](#).
3. Add the SSO details saved in step 2 in FortiSOAR™. To add the SSO details, log on to FortiSOAR™, click **Settings > Authentication > SSO Configuration**. In the **Identity Provider Configuration** section, enter the Google IdP details and certificate as shown in the following image:

**Identity Provider Configuration**

Entity ID \* ⓘ  
 https://accounts.google.com/o/saml2?idpid=0000000 ⓘ

Single Sign On URL \* ⓘ  
 https://accounts.google.com/o/saml2?idpid=0000000

Single Logout Request URL ⓘ  
 URL

X509 Certificate\* ⓘ  
 -----BEGIN CERTIFICATE-----  
 uIBanpU49Fa50IPdD/lwydJzVAorozBvc712u+OtEey+t6AB/9H7aPr8BgdK8sS9  
 iHYQnid63DkSXnjeoNmjG10pMzMURw23rQ.....  
 -----END CERTIFICATE-----

**Note:** Google SAML app does not provide a Logout URL. Therefore, users remain logged into their Google account even if they log off from FortiSOAR™.

In FortiSOAR™ the **Single Logout Request URL** field is optional and can be left blank.

4. Add the default user attribute mapping for Google in FortiSOAR™ by updating the **User Attribute Map**, based on what you have set in the attribute mapping in the Google SAML app, as shown in the following image:

**User Attribute Map** ⓘ

Tree ▾

Fields {4}

- firstName : First Name
- lastName : Last Name
- roles : Roles
- email : Email

5. Click **Save** in FortiSOAR™ to save the changes to the IdP configuration.

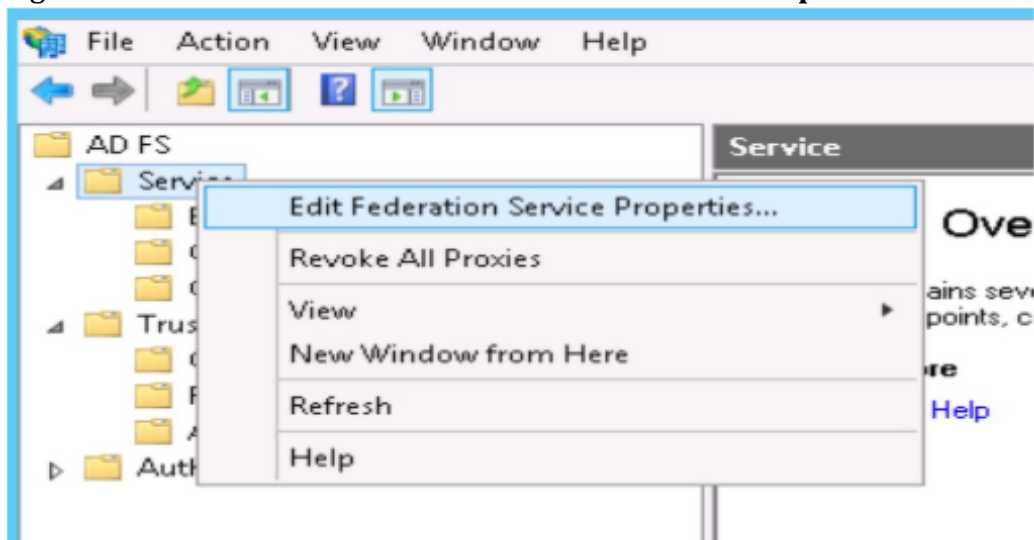
## Configuring SAML in ADFS

**Note:** If you change the hostname for your FortiSOAR™ system, you will require to delete the old ADFS configuration and re-configure ADFS.

## General ADFS Setup

This procedure uses ADFS 3.0 and uses `samlportal.example.com` as the ADFS website. The values you use in your setup will be based on your ADFS website address. See [ADFS integration with SAML 2.0](#) for more information.

1. Log on to the ADFS server and open the management console.
2. Right-click **Service** and click **Edit Federation Service Properties**.



3. On the Federation Service Properties dialog, in the General Settings tab, confirm that the DNS entries and certificate names are correct. Note the Federation Service Identifier, since you will use as the **Entity ID** in the Identity Provider

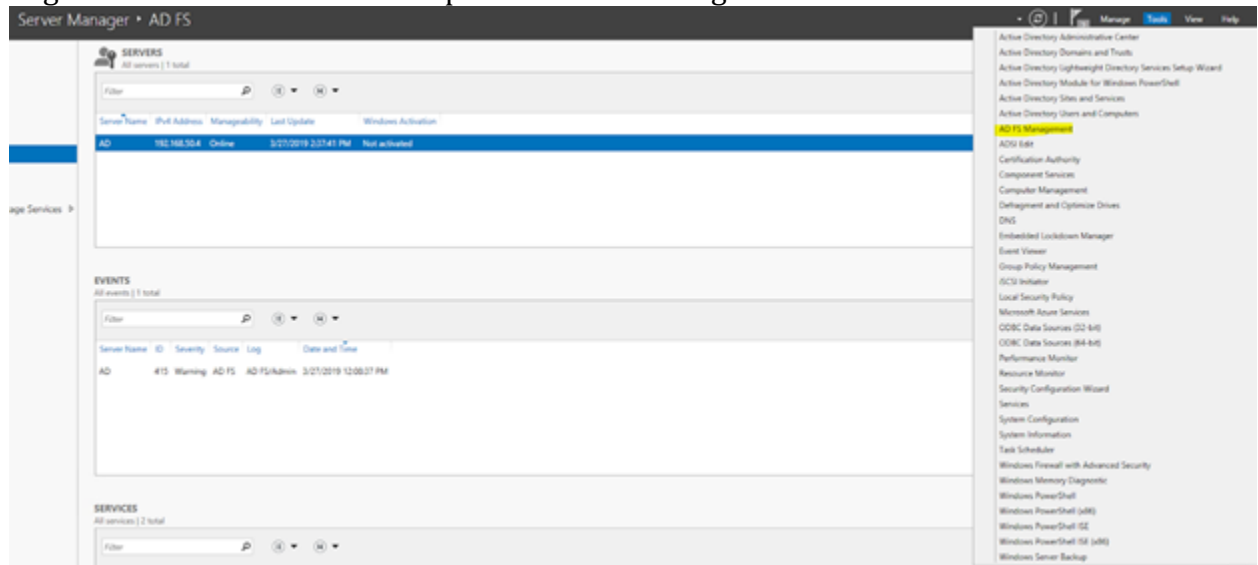
Configuration in the FortiSOAR™ UI.

4. In the **Services** panel, browse to **Certificates** and export the Token-Signing certificate using the following steps.
  - a. Right-click the certificate and select **View Certificate**.
  - b. Select the **Details** tab and click **Copy to File**, which opens the **Certificate Export** wizard.
  - c. On the Certificate Export Wizard, click **Next**.
  - d. Select **Base-64 encoded binary X.509 (.cer)**, and then click **Next**.
  - e. Select where you want to save the Token-Signing certificate and provide a name to the certificate, and then click **Next**.
  - f. Click **Finish**.
  - g. Copy the contents of the Token-Signing certificate and paste the contents in the **X509 Certificate** area in the **Identity Provider Configuration** in the FortiSOAR™ UI.

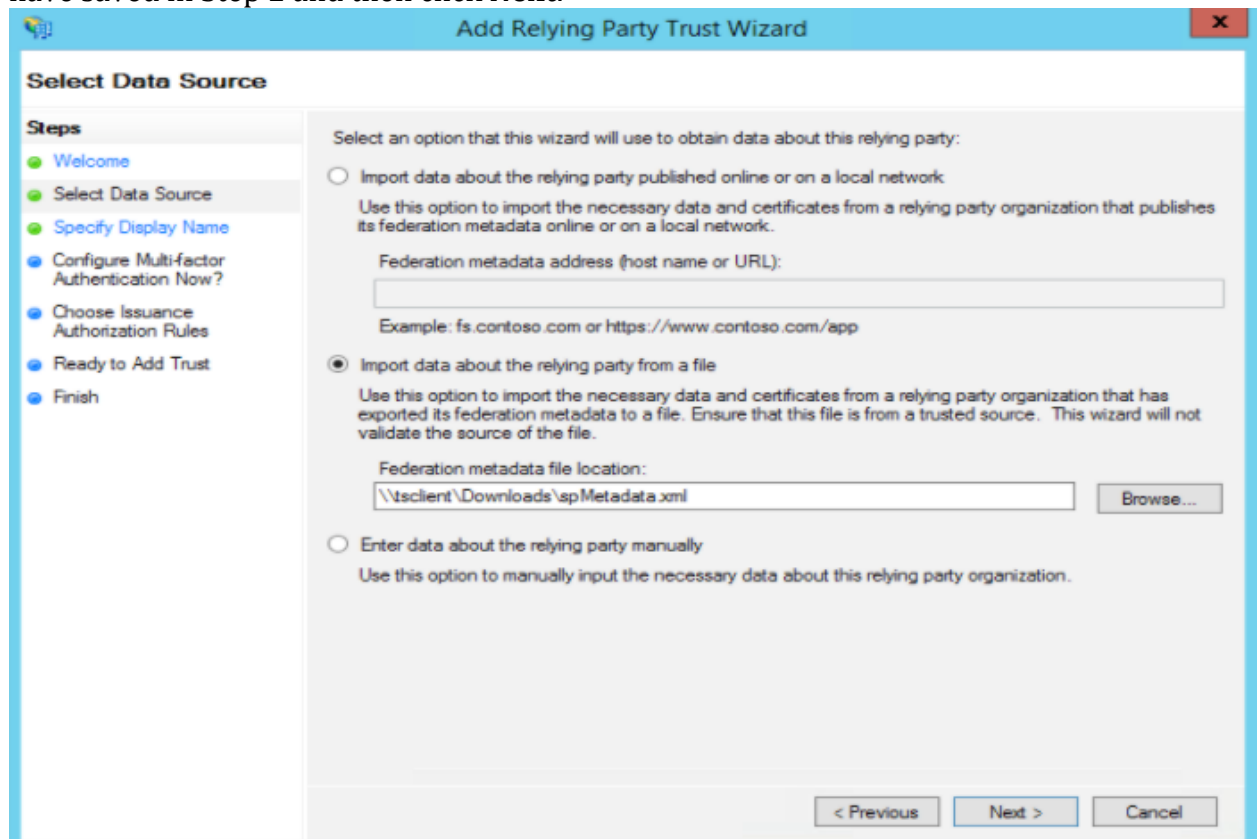
## Configuring ADFS Relying Party Trust

1. Log on to FortiSOAR™ as an administrator.

- Click **Settings > Authentication > SSO Configuration** and download the SAML metadata file by clicking **Download** in the **Service Provider Configuration** section.
- Log on to the ADFS server and open the ADFS management console.



- Expand **Trust Relationships** and right-click **Relying Party Trust** and select **Add**.
- On the **Add Relying Party Trust Wizard** click **Start**.
- In the **Select Data Source** panel, select the **Import data about the relying party from a file** option and click **Browse** to navigate to the SAML metadata file that you have saved in Step 2 and then click **Next**.





7. In the **Specify Display Name** panel set the display name and then click **Next**.
8. (Optional) In the **Configure Multi-factor Authentication Now?** panel configure MFA and then click **Next**.
9. In the **Choose Issuance Authorization Rules** panel, select the **Permit all users to access this relying party** option and then click **Next**.
10. In the **Ready to Add Trust** panel, click **Next**.
11. In the **Finish** panel, ensure that the **Open the Edit Claim Rules dialog** statement is selected and then click **Close**. This opens the **Edit Claim Rules Wizard** in which you can immediately add and configure rules as mentioned in the next section, or if you have closed **Edit Claims Rules** then use the steps mentioned in the next section to open **Edit Claim Rules** and add and configure rules.

## Configuring ADFS Relying Party Claim Rules

You must edit the claim rules to enable communication with FortiSOAR™ SAML

1. Log on to the ADFS server and open the management console.
2. Right-click the relying party trust (as configured in the previous section) and select **Edit Claim Rules**.
3. Click the **Issuance Transform Rules** tab and select **Add Rules**.
4. Select **Send LDAP Attribute as Claims** as the claim rule template to use and then click **Next**.
5. On the **Configure Claim Rule** dialog, in **Claim rule name**, enter a name to the claim rule. For example, name the claim rule as **Get LDAP Attributes**.
6. From the Attribute store drop-down list, select **Active Directory**.
7. In the Mapping of LDAP attributes to outgoing claim types section, map the following values:
  - a. Select **SAM-Account-Name** from the **LDAP Attribute** column and map that to **E-Mail Address** in the **Outgoing Claim Type** column.
  - b. Select **E-Mail-Addresses** from the **LDAP Attribute** column and map that to **Email** in the **Outgoing Claim Type** column.  
**Note:** You must manually type the values in the **Outgoing Claim Type** column.
  - c. Select **Surname** from the **LDAP Attribute** column and map that to **Last Name** in the **Outgoing Claim Type** column.  
**Note:** You must manually type the values in the **Outgoing Claim Type** column.
  - d. Select **Given-Name** from the **LDAP Attribute** column and map that to **First Name** in the **Outgoing Claim Type** column.  
**Note:** You must manually type the values in the **Outgoing Claim Type** column and the values that you specify in the **Outgoing Claim Type** column must match the what you enter in the right-side field in the **User Attribute Map** in the **Identity Provider Configuration** in the FortiSOAR™ UI.
  - e. Select **Token-Groups - Unqualified Names** from the **LDAP Attribute** column and map that to **Roles** in the **Outgoing Claim Type** column.

**Note:** You must manually type the values in the **Outgoing Claim Type** column.

Edit Rule - Get LDAP Attributes
✕

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	E-Mail Address
	E-Mail-Addresses	Email
	Surname	Last Name
	Given-Name	First Name
	Token-Groups - Unqualified Names	Roles

8. Click **Finish** and select **Add Rules**.
9. Select **Transform an Incoming Claim** as the claim rule template to use and then click **Next**.
10. On the Add Transform Claim Rule Wizard, in **Claim rule name**, enter a name to the claim rule. For example, name the claim rule as Email to Name ID.
11. From the **Incoming claim type** drop-down list, select **E-Mail Address**, from the **Outgoing claim type** drop-down list, select **Name ID** and select the **Pass through all**

**claim values** option and click **Finish** and then click **OK**.

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values  
☐ Replace an incoming claim value with a different outgoing claim value  
     Incoming claim value:   
     Outgoing claim value:    
☐ Replace incoming e-mail suffix claims with a new e-mail suffix  
     New e-mail suffix:   
     Example: fabrikam.com

< Previous    Finish    Cancel

## Configuring FortiSOAR™ for ADFS

1. Log on to FortiSOAR™ as an administrator.
2. Click **Settings > Authentication > SSO Configuration**.
3. To enable SAML for FortiSOAR™, click the **SAML Enabled** check box.
4. In the **Identity Provider Configuration** section, enter the IdP details.  
 Enter the **Entity ID** as the one that you had noted in Step 3 of the [General ADFS Setup](#) procedure. For example, `https://samlportal.example.com/adfs/services/trust`  
 Enter the **Single Sign On URL** as `<server_address>/adfs/ls`. For example, `https://samlportal.example.com/adfs/ls`  
 Enter the **Single Logout Request URL** as `<server_address>/adfs/ls?wa=wsignout1.0`. For example, `https://samlportal.example.com/adfs/ls?wa=wsignout1.0`  
 In the **X509 Certificate** area, paste the contents of the certificate you exported in Step 8 of the [General ADFS Setup](#) procedure. Following is an image of sample inputs in the

## FortiSOAR™ UI:

**Identity Provider Configuration**

Entity ID ⓘ

Single Sign On URL ⓘ

Single Logout Request URL ⓘ

X509 Certificate ⓘ  

```
-----BEGIN CERTIFICATE-----
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNDEwMTEyNTA4WhcNMjAwNDA5MTEyNTA4WjBF
1UBuDorUOA2NiH7M0NrnDylJp6l8aJnNGIGTJddOzPvnXFMH1Cafp0JmrK7dshwV.....
-----END CERTIFICATE-----
```

5. Map the user attributes received from the ADFS (IdP) with the corresponding attributes of FortiSOAR™.

Use the **User Attribute Map** to map the attributes received from the ADFS with the corresponding attributes required by FortiSOAR™. FortiSOAR™ requires the firstname, lastname and email attributes to be mapped. The ADFS attributes that you need to map are the names that you specify as values in the **Outgoing Claim Type** column in the management console of ADFS. For more information, see [Configuring ADFS Relying Party Claim Rules](#).

In the **User Attribute Map**, under **Fields**, click the editable field name (right side field name), to map it to the attribute that will be received from the IdP. The non-editable field name (left-side field name) is the FortiSOAR™ attribute. For example, in the following image, you map the FortiSOAR™ attribute **firstname** to the IdP attribute **First Name**.

**User Attribute Map** ⓘ

Tree ▾

Fields {4}

- firstName : **First Name**
- lastName : **Last Name**
- roles : **Roles**
- email : **Email**

If you want to set any of the optional configurations, see [Configuring SAML in FortiSOAR™](#).

6. Click **Save** to complete the SAML configuration in FortiSOAR™.

## Support for mapping roles and teams of SSO users in FortiSOAR™

You can map the role and team of SSO users in FortiSOAR™ based on their roles defined in the IdP. Thereby you can set the role of an SSO user in FortiSOAR™ based on the role you have defined in your IdP.

To achieve this FortiSOAR™ has added a new configuration in the **SSO Configuration** page where you can map the role that you have specified in the IdP to a FortiSOAR™ role and team. The relationship between the IdP role and the FortiSOAR™ role is one to many, i.e., one IdP role can map to multiple FortiSOAR™ roles.

SAML supports attribute-based authorization. Therefore, you should configure attribute **roles** in your IdP that will contain roles of your SSO users on the IdP.

If you have not set up mapped roles of SSO users in FortiSOAR™, or if FortiSOAR™ receives a response from the IdP that does not contain any roles, or receives a response that does not map to any of the FortiSOAR™ roles, then the SSO user will be assigned the default roles.

### Configuring IdPs to send the SSO user role information to FortiSOAR™

The following sections define how you can configure IdPs, i.e., **OneLogin**, **Okta**, or **Auth0** to send the SSO user role information to FortiSOAR™ when the user is logging on to FortiSOAR™ (SSO login).

For mapping of roles in ADFS, see the [Configuring ADFS Relying Party Claim Rules](#) section.

For any other IdP, configure roles as per the IdP requirements and contact the IdP support personnel if you face any issues.

#### *OneLogin*

1. Log on to OneLogin as an administrator.
2. Navigate to the SAML app that you have created by clicking **APPS** in the administration panel. Open the SAML app and in the App **Configuration** screen, go to the **Parameters** section and click **Add Field**, which displays the New Field dialog.

3. In the New Field dialog, in the Field name type **Roles**, ensure that you check **Include in SAML assertion** checkbox in the **Flags** section, and then click **Save**.

The screenshot shows the Fortinet management console interface. At the top, there are navigation tabs: USERS, APPS, DEVICES, ACTIVITY, SETTINGS, and DEVELOPERS. Below these, the main heading is 'SAML Test Connector (IdP w/ attr w/...'. To the right of this heading are two buttons: 'MORE ACTIONS' and 'SAVE'.

In the center, a 'New Field' dialog box is open. It has a title bar 'New Field'. Inside, there is a section for 'Field name' with a text input field containing the word 'Roles'. Below this, a note states: 'This is the name of the field in the application's API'. There is a horizontal separator line. Below the line, there is a section for 'Flags' with two checkboxes: 'Include in SAML assertion' (which is checked) and 'Multi-value parameter' (which is unchecked). At the bottom right of the dialog box are two buttons: 'CANCEL' and 'SAVE'.

In the background, partially obscured by the dialog box, is a table of SAML attributes. The table has two columns: 'Name' and 'Value'. The rows include: 'SAML Test Connector (IdP w/ attr w/...)' with value 'Field', 'E-mail (Attribute)' with value 'Email (SAML NameID)', 'First Name (Attribute)' with value 'First Name (Attribute)', 'Last Name (Attribute)' with value 'Last Name (Attribute)', 'Member of (Attribute)' with value 'Member of (Attribute)', 'PersonImmutableID' with value 'PersonImmutableID', 'roles' with value 'User Roles', and 'test\_roles' with value 'User Roles'. To the right of the table, there is a button 'Add parameter' and a list of 'custom parameter' entries.

4. In the next dialog, i.e., the **Edit Field Roles** dialog, from the **Value** drop-down list, select **User Roles** and click **Save**.

**Edit Field Roles**

Name	Roles	Flags
Value	User Roles	<input checked="" type="checkbox"/> Include in SAML assertion

CANCEL DELETE SAVE

## Okta

1. Log on to Okta as an administrator.
2. Navigate to the SAML app that you have created and edit the SAML settings.
3. In the **GROUP ATTRIBUTE STATEMENTS (OPTIONAL)** section set the following:  
**Name:** Set as **Roles**.  
**Filter:** Set as **Matches regex** \*.\*

**GROUP ATTRIBUTE STATEMENTS (OPTIONAL)**

Name	Name format (optional)	Filter
Roles	Unspecified	Matches regex *.*

Add Another X

4. Click **Next** and complete the setup.

## Auth0

1. Log on to Auth0 as an administrator and in the left menu click **Authorization**.
2. On the **Authorization Extension** page, create a new group and associate required members (users) and roles with this group.

The screenshot shows the Auth0 Authorization Extension interface. The top navigation bar includes the Auth0 logo, 'Authorization Extension', 'Help', 'Dashboard', and a user profile 'o10.auth0.com'. The left sidebar lists 'Users', 'Groups', 'Roles', and 'Permissions'. The main content area displays the 'QA' group (Qa Team) with edit and delete icons. Below this, there are tabs for 'Members', 'Roles', 'Nested Groups', and 'Group Mappings'. A message states: 'Add or remove roles to this group. Any member of this group will also be assigned to these roles.' with an '+ ADD ROLE' button. A table lists roles assigned to the group:

Name	Application	Description
ReadOnly	Cyber-QA :	ReadOnly


3. Navigate back to the main menu (**Dashboards** page) and click **Applications**.
4. Create a new application, or click on the **Settings** icon of the application whose settings you want to edit:

The screenshot shows the Auth0 Applications page. The top navigation bar includes the Auth0 logo, a search bar 'Search for users or applications', and links for 'Help & Support', 'Documentation', 'Talk to Sales', and a user profile 'o10'. The left sidebar lists 'Dashboard', 'Applications', 'APIs', 'SSO Integrations', 'Connections', 'Universal Login', 'Users & Roles', and 'Rules'. The main content area is titled 'Applications' with a '+ CREATE APPLICATION' button. Below the title, it says 'Setup a mobile, web or IoT application to use Auth0 for Authentication. [Learn more](#)'. A table lists applications:



Application Name	Type	Client ID	Actions
auth0-authz	GENERIC	9uFgK9ddGw3okU7mmepzUkYMamx	Settings, Code, Copy, Share
Cyber-QA	REGULAR WEB APPLICATION	6U48q1AnWn33GrTkQ1ZY3s1TIXkI	Settings, Code, Copy, Share





This opens the **Setting** page for the application:





Search for users or applications


 2 Help & Support Documentation Talk to Sales o10 


 Dashboard


 Applications


 APIs


 SSO Integrations


 Connections


 Universal Login


 Users & Roles


 Rules


 Hooks

 Multifactor Auth


 Emails

 Logs

 Anomaly Detection

 Extensions

← Back to Applications



## Cyber-QA

REGULAR WEB APPLICATION Client ID .....


Quick Start

Settings


Addons

Connections


Name

Cyber-QA 


Domain

o10.auth0.com 

Client ID

..... 

Client Secret

..... 

- Click the **Addons** tab and click **SAML2** and enter the required details on the **Settings** tab for the application you have created:

✕

**Addon: SAML2 Web App**

Settings
Usage

---

**Application Callback URL**

https://qa-cyber.net/api/public/saml/login

SAML Token will be POSTed to this URL.

**Settings**

```

1 {
2   "mappings": {
3     "user_id": "user_id",
4     "email": "email",
5     "name": "name",
6     "given_name": "fname",
7     "family_name": "lname",
8     "upn": "upn",
9     "Group": "groups"
10  },
11  "logout": {
12    "callback": "https://qa-
cyber.net/api/public/saml/logout"

```

- Click **Save** to save the settings of the application.

## Troubleshooting SAML issues

### Unable to login to FortiSOAR™ when ADFS SAML is configured

If you are unable to login to FortiSOAR™ when ADFS SAML is configured, and if you find the "The revocation function was unable to check revocation for the certificate." error in the ADFS logs, then you must turn off the certificate revocation check using the following steps:

- Enter **Powershell** in the "Administrator" mode of the ADFS system.

2. Run the following commands: (RelyingPartyTrustName should be in double quotes):  
`Set-AdfsRelyingPartyTrust -TargetName "<RelyingPartyTrustName>" -  
SigningCertificateRevocationCheck None`  
`Set-AdfsRelyingPartyTrust -TargetName "<RelyingPartyTrustName>" -  
EncryptionCertificateRevocationCheck None`  
This turns off the certificate revocation check and now you should be able to login to FortiSOAR™.

## Application Editor

Use the Application Editor to configure data models contained in modules, to export and import configurations, visually display the nodes related to a particular record, customize your Picklist values, and the left navigation bar.

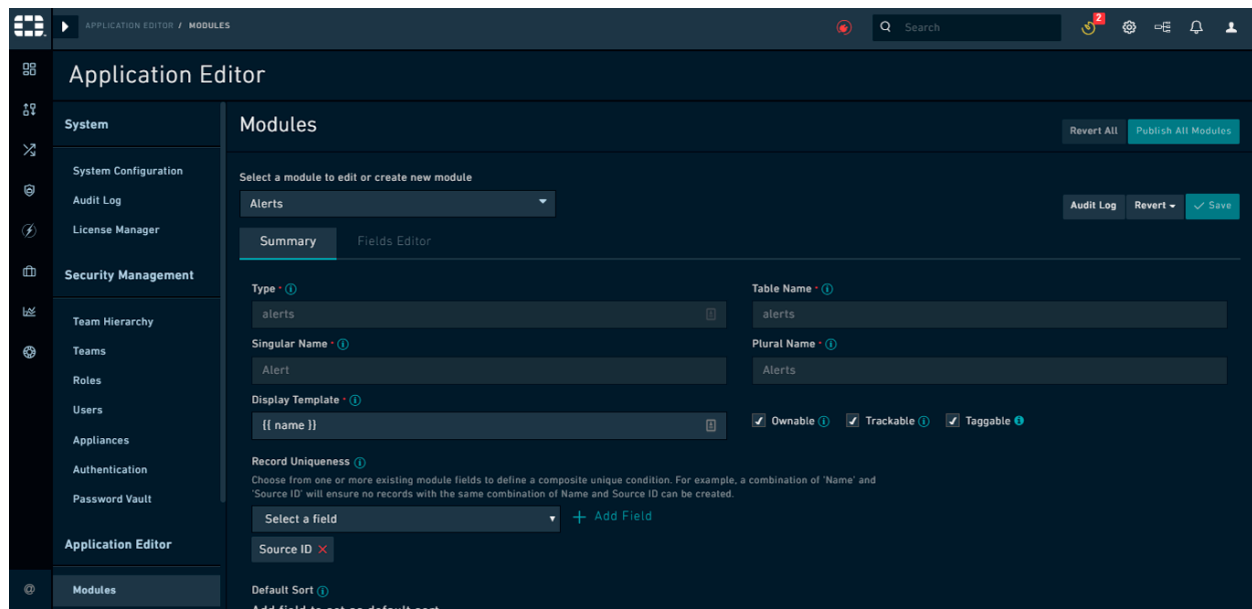
The Application Editor has following tools for this purpose:

- Module Editor - for editing the data models in a module
- Picklist Editor - for changing picklist values and color associations
- Navigation Editor - for modifying the navigation links and hierarchy in the left navigation bar
- Correlation Settings - for configure the display of the Visual Correlation widget.
- Configuration Manager - for exporting and importing configurations across environments

**Important:** To edit these settings, users must be assigned a role that has at a minimum of Read and Update permissions on the Application module. If you want a user to be able to add modules also, then those users must be assigned a role that has at a minimum of 'Read,' 'Create,' and 'Update' permissions on the Application module. To delete picklist or navigation items, you must have Delete permissions on the Application module. These privileges must be granted carefully as unintended application modification could result in data loss.

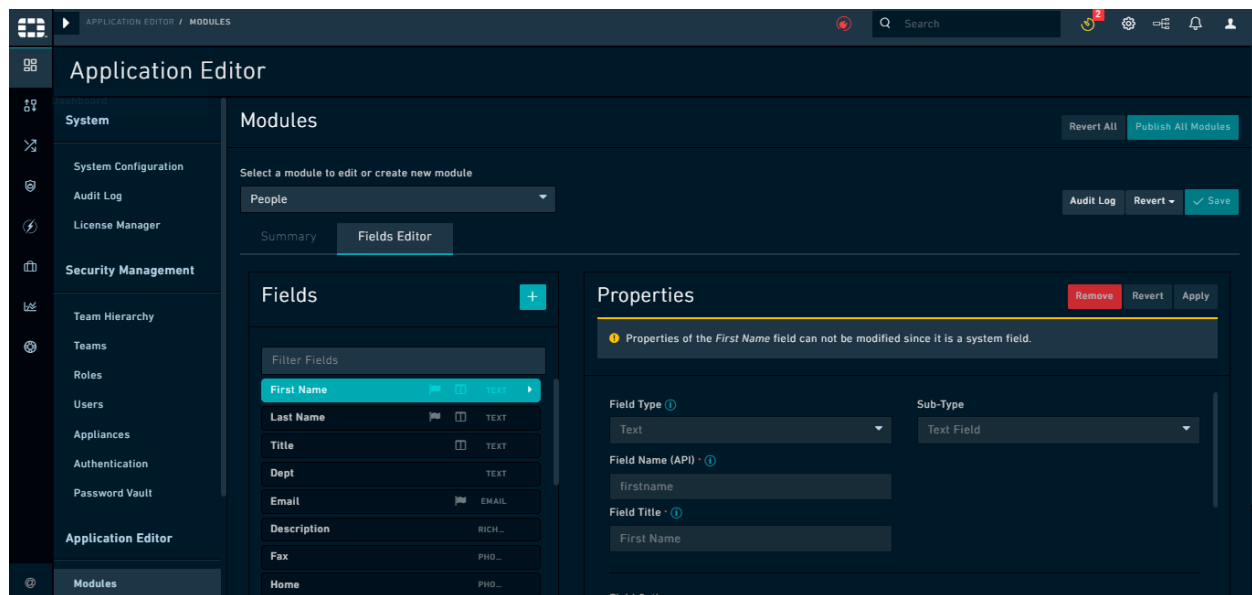
## Module Editor

Use the Module Editor to add new modules and to add new fields and edit existing fields within a module. You can open the module editor by clicking **Settings** and in the **Application Editor** section, click **Modules**. This displays the **Modules** page.



**Figure 64.** *Module Editor Interface*

**Important:** Some fields in some modules are system fields and only FortiSOAR™ can create system fields. Changing the properties of the system fields could lead to issues with the working of FortiSOAR™. Therefore, you cannot modify any properties of these fields, and they appear as read-only when you select them in the **Fields Editor** tab. An example of this type of field is the **First Name** field in the **People** Module as shown in the following image:

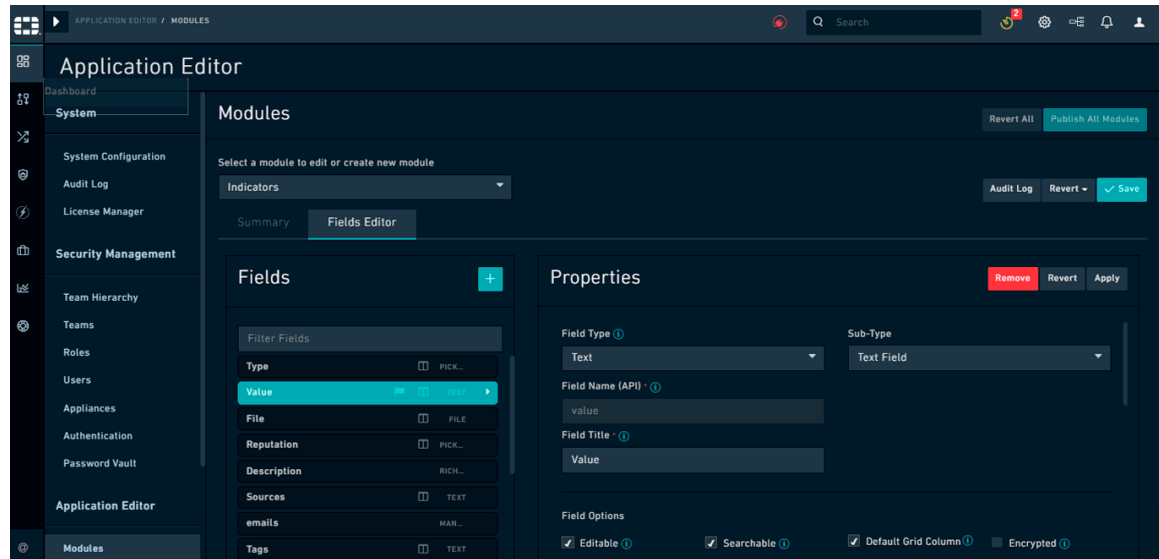


**Figure 65.** *Field Editor tab- Read-only fields*

## Modifying an existing module

To modify an existing module, do the following:

1. Click **Settings** and click **Modules** in the **Application Editor** section, to open the Module Editor.  
This displays the **Modules** page.
2. To edit an existing module, from the **Select a module to edit or create new module** drop-down list, select the module.  
For example, select **Alerts**.
3. To add a module, you have to specify the properties on the **Summary** tab. You can also add or modify any field in the summary view for a module, by updating the properties or adding fields on the **Summary** tab. To add any field to the **Summary** view, you must ensure that you have already added the field using the **Field Editor**. This step describes editing properties in the **Summary** view.
  - a. Edit properties on the summary view.  
You can configure the following fields for defining a module using the **Module Editor**:
    - **Type**: Type is similar to table name and is used to identify the module in the API. The Type name must be unique. The Type field must contain only lower-case alphabets, underscore characters `_`, and numbers, and it must start with a lower-case alphabet.
    - **Table Name**: The Table Name refers to the SQL table name generated. The table name must be unique and in lower-case. This generally matches the Type name. We recommend that you do not change the table name, or you risk data loss as the referenced table name changes, though the old table remains intact in the database.
    - **Singular Name**: The name of the module itself, when it is in the singular context (individual record). For example, an Incident refers to an individual record in a module, whereas the module is Incidents.
    - **Plural Name**: The name of the module itself when it is in the plural context. For example, Vulnerability is the singular version of the module and Vulnerabilities is the plural version of the module.
    - **Display Template**: This field uses an Angular Template expression to display a record appropriately. This template specifies the fields that will be displayed when a record from this module is referenced in the application. Fields of a module can be specified in the display template as `{{ field_name_api }}`.  
**Important:** Ensure that you add the fields that you specify in **Display Template** in the module that you are creating or updating. For example, if you have added `{{ value }}` in **Display Template**, then ensure that you have added **Value** as a field in the module, its **Field Name (API)** attribute will be set as `value`.



You can also add an attribute of a picklist as part of the Display Template. See the following *Display Template* section for more details.

- **Ownable:** Records that are ownable are owned by a Team or Teams. An example of a module that you should make ownable is Incidents. If you do not select this option, then the records are not ownable and are publicly available and visible to any system user, without consideration of the user's team. An example of a module that you could make not ownable is Addresses.

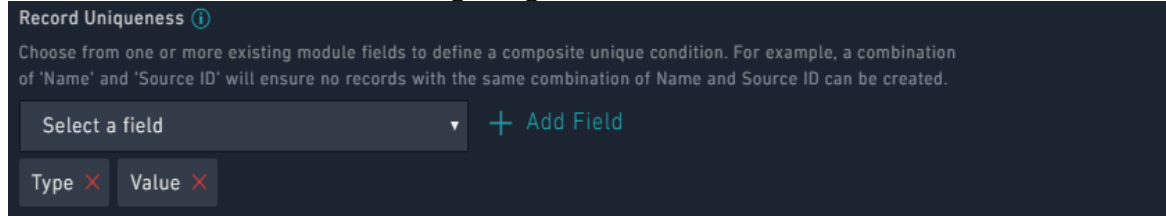
**Note:** Records that do not have any owners are visible to "All." If you change a module that was not ownable to ownable, then the records created before you have changed the ownership are visible to "All". However, until owners (teams) are assigned to the record, the record is read-only, i.e., fields in that record cannot be edited until a team is assigned to the record. Also, users' who are editing the same record (with no owners) must assign their team to the records to ensure that the records continue to be visible to those users and/or teams.

- **Trackable:** Selecting this option ensures that FortiSOAR™ tracks the date that the record was created, user who has created the record, date that the record was modified, and user who has modified the record on all records in the module.

**Important:** Once a module has been created, you must not modify the Type and Table Name fields. You can edit the Singular and Plural names whenever required. However, note that the Singular name plus an *s* is used for API endpoint generation during module creation. Changing the Singular name could disrupt existing API calls to the endpoint.

- **Taggable:** Selecting this option ensures that the selected module is taggable, i.e., you can enter tags to records in this module making it easier to search and filter records in the module.
- **Data Replication:** (Used in multi-tenant setups): Selecting this option enables replication of data for the selected module across peers' setups.

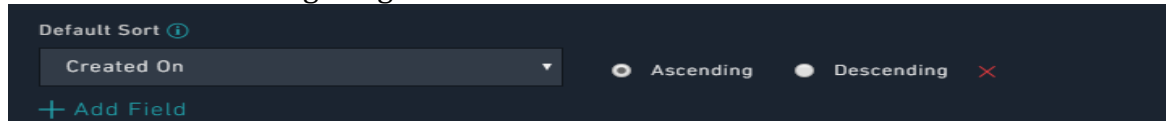
- **Record Uniqueness:** This section allows you to choose one or more published fields from the existing module that would be used to define a unique condition. This ensures that only unique records will be created in FortiSOAR™ and any record that matches the unique field or the combination of unique fields would not be created. For example, *Type + Value* is a unique combination in the **Indicators** module as shown in the following image:



This will ensure that indicator records will be created with unique “Type and Values” values.

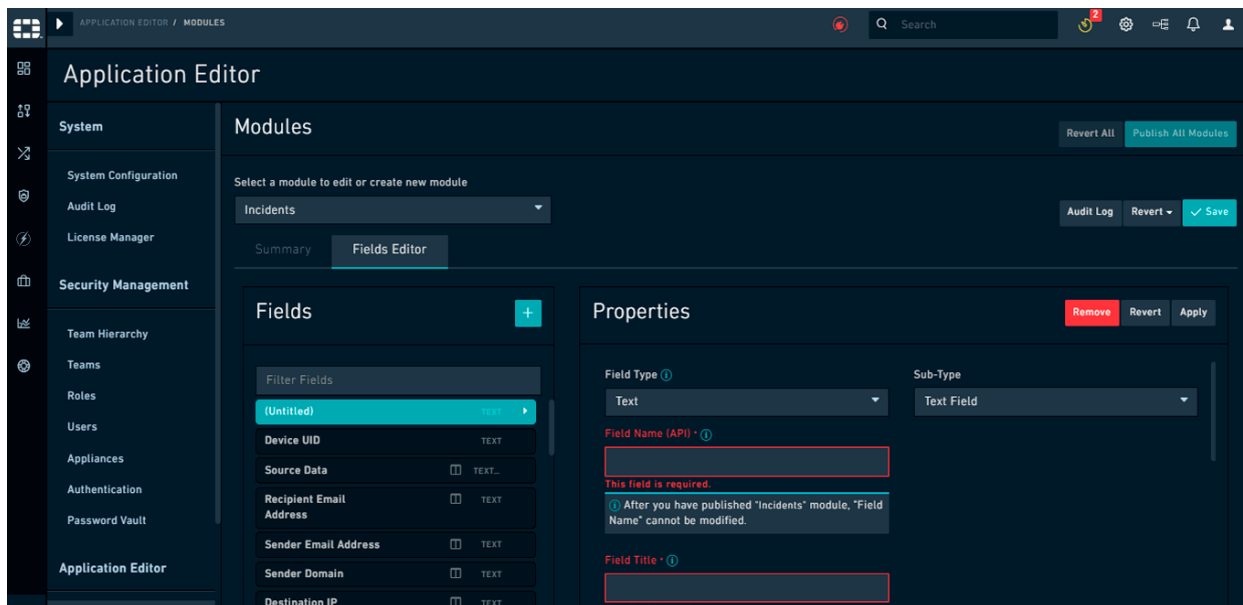
If you want to add any other field to for part of the unique combination of fields, then from the **Record Uniqueness** section, select that field from the **Select a Field** drop-down list, and then click **Add Field**. Similarly, if you want to remove any field from the unique combination, you need to click the red **X** on that field.

- **Default Sort:** Click **Add Field** to add a field based on which the list of records in the module will be sorted, either in the ascending or descending order. For example, indicators will be sorted based on when they were created, if you add **Created On** in the Default Sort section, as shown in the following image:



- b. Click **Save** to save the changes to the module or click **Revert** to clear any changes made in the interface since the last **Save** event. For information on the save and revert operations, see the *Saving your changes* section.
4. To add fields to the module, or to edit any of the fields belonging to the module, add or update the fields on the **Fields Editor** tab on the **Modules** page.

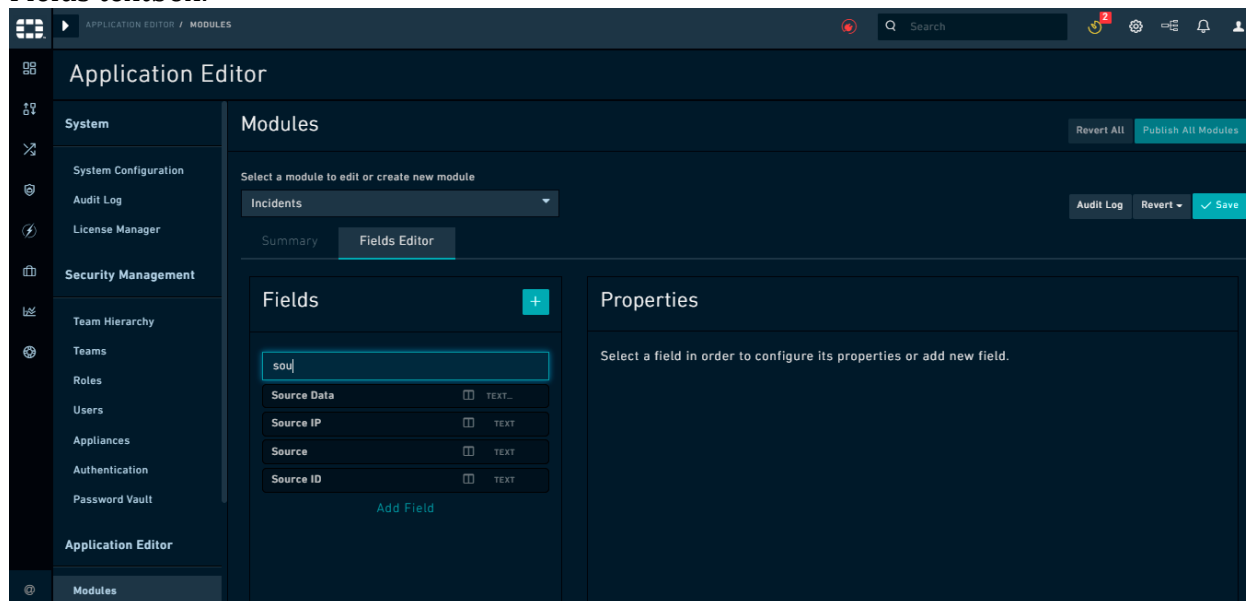




**Important:** Some fields in some modules are system fields and changing properties of these fields could lead to issues with the working of FortiSOAR™. Therefore, you cannot modify any properties of these fields and they appear as read-only when you select them in the **Fields Editor** tab. An example of this type of field is the **First Name** field in the **People** Module.

- a. To add fields, on the **Modules** page, click the **Fields Editor** tab and click the Add (+) icon beside **Fields**.

**Note:** The Fields Editor pane displays the list of fields that have been defined for the module. You can filter the fields by typing the search term in the Filter Fields textbox:



- b. Define the following properties for the newly added field:
  - **Field Type:** The type of field; it specifies the type of form used to render this attribute. Examples of field types are text, checkbox, integer,

decimal, date/time, picklist, and relationship fields.

It is recommended that when you create a field of type **Integer**, then you should set its default value as “zero”.

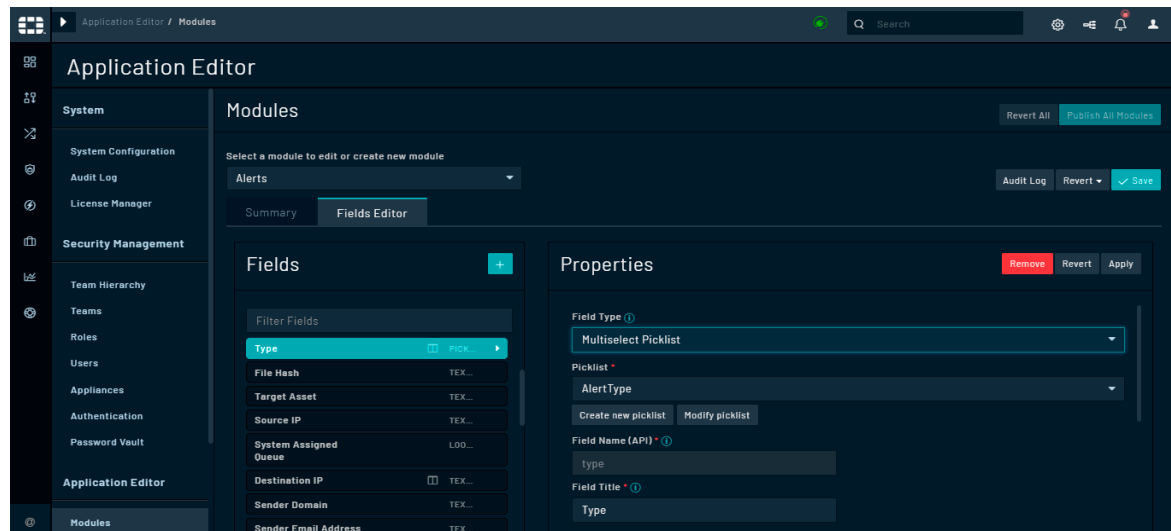
Use the **JSON** field type for fields such as, **Source Data**, which commonly store data in the JSON format to allow playbooks to get to the JSON data directly, without having to use a JSON parse step. You can also define the height of the JSON field in pixels by editing your record template.

Based on the **Field Type** that you select, you can see an additional field.

For example, if you select the field type as **Picklist**, a **Picklist** drop-down list will appear, and you must select the picklist associated with the field or click **Create new picklist** to add a new picklist. Use the **Configure Picklist Option Visibility** checkbox to filter a picklist field based on specified criteria. Once you check this checkbox, the picklist items are displayed and you can choose whether the item should be Visible, Disabled, Hidden, Conditionally Visible, or Conditionally Enabled. If you choose Conditionally Visible or Conditionally Enabled, you can then define the criterion when this item should be visible. An example would be displaying the Minimal option, in case of the Severity picklist, only if the type of alert is Other / Unknown:

The screenshot shows the FortiSOAR Fields Editor interface. On the left, under the 'Fields' tab, a list of fields is shown: Device UID, Name, Description, Assigned To, Severity (highlighted), Status, Type, File Hash, Target Asset, and Source IP. The 'Severity' field is selected, and its properties are shown on the right. The 'Properties' tab for 'Severity' includes a 'Create new picklist' button and a checked 'Configure Picklist Option Visibility' checkbox. Below this, the 'Minimal' option is set to 'Conditionally Visible'. A condition is defined: 'ALL OF THE BELOW ARE TRUE (AND)' with a single condition: 'Type' equals 'Other / Unknown'. The 'Low', 'Medium', and 'High' options are all set to 'Visible'.

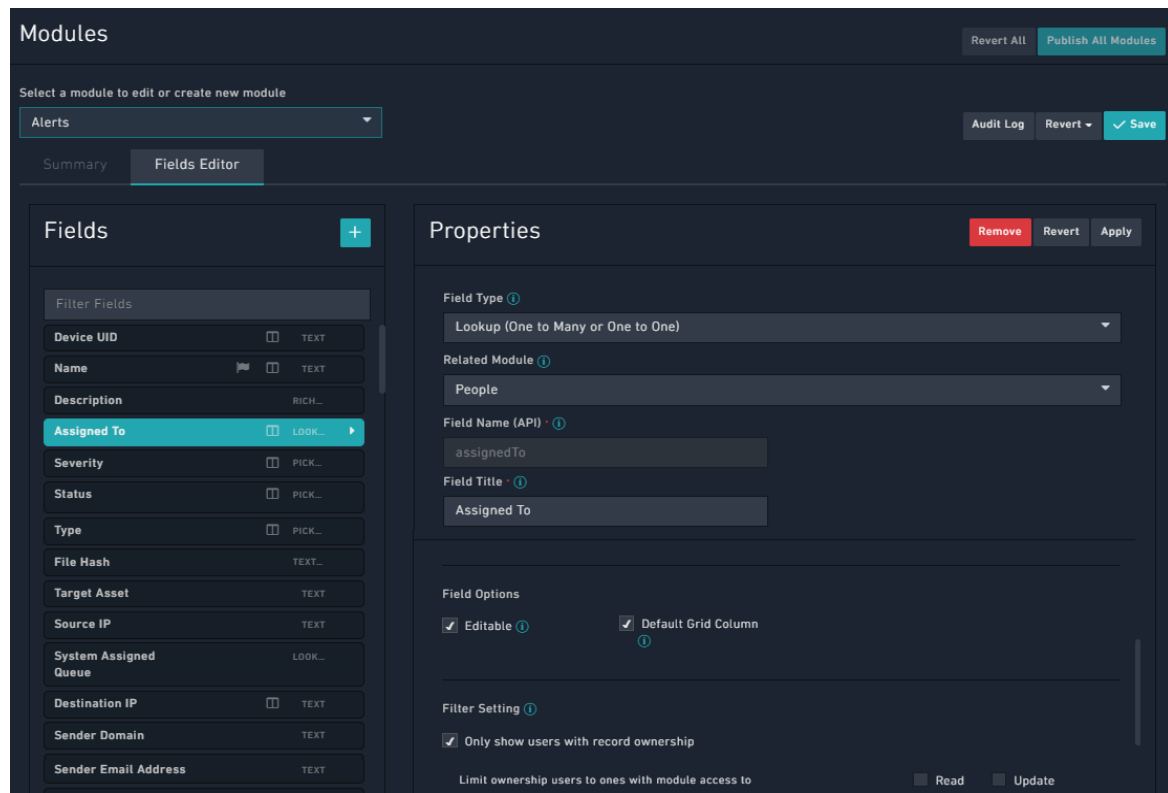
FortiSOAR™ also supports a special type of picklist, called “Multiselect Picklist”. You can use the multiselect picklist for fields that can contain more than one value. For example, you can have an alert be assigned more than one “Type”, i.e., an alert can be of type Brute Force Alert and Malware. In such a case you can assign **Multiselect Picklist** as the *Field Type* for the “Type” field. You can then select an existing picklist from the picklist drop-down list, for example **AlertType**, or click **Create new picklist** to create a new picklist. You can also click **Modify picklist** to modify the existing picklist, by adding or removing picklist items or changing the properties of the picklist items.



If you select Lookup (One to Many or One to One), Many to One, or Many to Many, a **Related Model** drop-down list will appear, and you must select the related module. The related module is the module for the source of the data, which is not explicitly defined, to which the fields points.

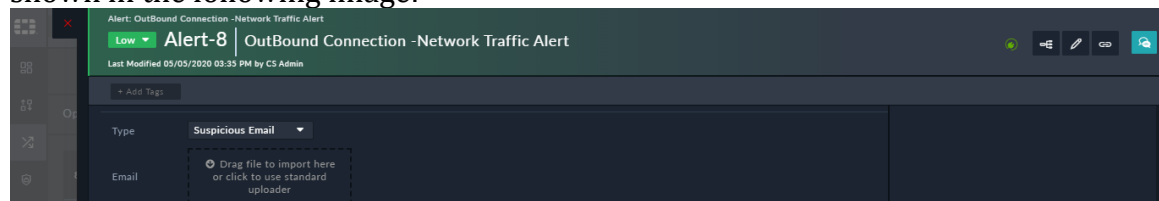
#### Notes with respect to Relationship fields:

- In the case of a Many to One, or a Many to Many field, you must select the appropriate field from the **Related Model** drop-down list, before you publish the module.
- In the case of Lookup (One to Many or One to One) fields that have People as a related module contain the Filter Setting section. If you select the **Only show users with record ownership** checkbox in the Filter Settings section, then the list of users displayed in the lookup on the UI is restricted to include only those users who have record ownership. Further, you can also limit the list of users displayed in the lookup based on permissions given to the user on the module using the Limit ownership users to ones with module access to option. In the **Limit ownership users to ones with module access to** option, you can choose to display users who have **Read** access or **Update (Read + Update)** access.



**Example:** In the Alerts module, we have an **Assigned To** field, which is of type Lookup (One to Many or One to One) , with **People** as the related module. In this case by default, all users will be displayed in the Assigned To lookup, when you open an alert record. However, this could include users who belong to other teams, and who, therefore, would not have access to the record, even if you assign that record to that user. Therefore, to restrict the users to only those users who have access to the record, you can select the **Only show users with record ownership** checkbox. You can further restrict users displayed in the **Assigned To** lookup based on the module access. For example, if you want to display only those users who can update the record, in the **Limit ownership users to ones with module access to field**, select the **Update** checkbox (once you select the Update checkbox, the Read checkbox is automatically checked).

You can drag and drop files in the "File Field" type field. An example of a "File Field" is "Email"; therefore, if you have an **Email** field in your record, then you can drag and drop an email to attach it to the record as shown in the following image:



- **Sub-Type:** The “Sub-Type” field can be used along with the **Text** field type. When you select **Text** in the **Field Type**, then an additional field named **Sub-Type** is displayed. You can select the sub-type such as, Text Field, Rich Text (Markdown), Rich Text (HTML), Text Area, IPv4, IPv6, Domain, URL, or Filehash. The sub-type field enforces the format of data that the user can enter in that field. For example, in a Rich Text (HTML) or Rich Text (Markdown) fields, you can use formatting options or you can use the IP address and domain field types to lookup threat intelligence tools and whois info.  
**Note:** For all modules, the default rich text editor is set to "Markdown", i.e., the Rich Text (Markdown) is selected for rich text fields. You can change the editor from markdown to HTML by selecting the appropriate sub-type for a field and then publish the module for the changes to reflect.
- **Field Name (API):** The name of the field. This is a required field. The Name field must be alphanumeric and must start with a lower-case alphabet. It cannot contain any spaces, underscores or any special characters.  
**Note:** You cannot change the name that you specify for the field once the field has been created and the module has been published. This is because there is no migration path from the old name to the new name, so you risk data loss if you change the field name.
- **Field Title:** A short descriptive name describing the item.  
**Note:** If you have a field, in a module, whose **Field Title (Singular Description)** attribute value contains a **.** or **\$**, then the Audit Logs replace the **.** or **\$** with an **\_**. For example, if you have a field **SourceID** whose singular description you have specified as **Source.ID**, then in this field will appear as **Source\_ID** in Audit Logs.
- **Editable:** Selecting this option allows you to modify the field after the creation of a module record. If this option is not selected, then you cannot modify the initial value after the record is created.
- **Delete Associations With Parent:** Selecting this option cascades the deletion of a parent record to all the associated records for the **Many to One** relation type fields. For example, **Events** and **Alerts** have a **Many to One** relationship, i.e., one alert could have many associated events. If you select this option, then if an alert is deleted all its associated events also get deleted. Another example would be the case where one alert has multiple comments, and selecting this option cascade deletes the comments that are associated with a deleted alert.  
**Warning:** Select this option with caution since RBAC is **Not** applied for child records. For example, if you have **Delete** permissions on the **Alerts** module but not on the **Events** module, and you have selected this option, then deleting an alert with associated events, leads to the associated events getting deleted, irrespective of the permissions on the **Events** modules.

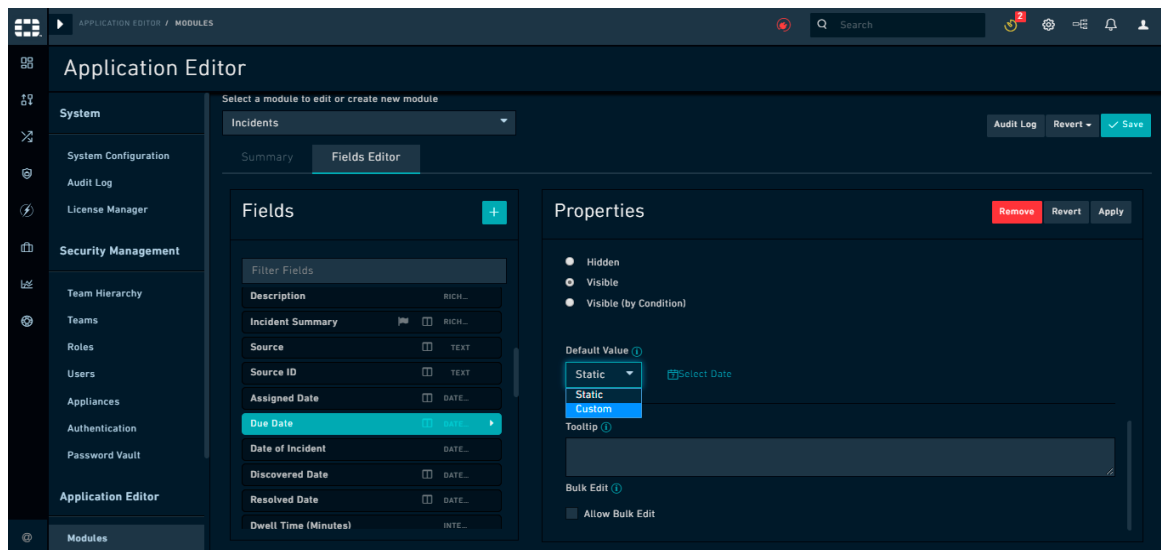
- **Searchable:** Selecting this option makes this field searchable in the grid view.
- **Default Grid Column:** Selecting this option makes the field appear as a column by default in the grid view. The order of the grid columns is defined by order of the fields in the Field Editor list. For information about grids, see the *Dashboards, Templates, and Widgets* section in the “User Guide.”
- **Encrypted:** Selecting this option enables encrypting of field values before storing in the database for enhanced security. FortiSOAR™ UI will continue to display the non-encrypted values. Currently, Text Fields, Email Fields, Rich Text Area and Text Area fields can be encrypted.  
**Important:** Once you enable encryption you cannot search the field values using FortiSOAR™ UI. Filters also will not work on encrypted fields. You also cannot use the upsert functionality for fields that are encrypted.
- **Required:** Specifies whether the field is a required field.  
The options are: **Not required**, **Required**, or **Required (by condition)**. Once you select **Required (by condition)**, FortiSOAR™ displays the Condition Builder options where you must add the necessary condition.  
**Note:** FortiSOAR™ also supports advanced date operations and nested conditions for the **Required (by condition)** fields i.e., the **Add Condition Group** link is now available for these fields.  
**Important:** Do not choose the **Visibility = Hidden** option for **Required (by condition)** fields.
- **Visibility:** Specifies whether the field is visible or not.  
The options are: **Hidden**, **Visible** and **Visible (by condition)**.  
If you select the **Hidden** option, then the field is only accessible at the API level and not shown in the UI.  
If you select the **Visible** option, then the field is displayed on the UI. If you select the **Visible (by condition)** option, then the field is displayed on the UI only if the specific conditions are met.  
Once you select **Visible (by condition)**, FortiSOAR™ displays the Condition Builder options where you must add the necessary condition.  
**Note:** FortiSOAR™ also supports advanced date operations nested conditions for the **Visible (by condition)** fields i.e., the **Add Condition**

**Group** link is now available for these fields:

- **Default Value:** Specifies the default value of this field. Once you specify a value in this field, then this value will be displayed, by default when you add a record in the selected module.  
For example, if you want the status of a newly created alert to be set to **Open**, by default, then select the **Status** field and from the **Default Value** drop-down list, select **Open** as shown in the following image:

Once you set the default value, then whenever you add a new record in the **Alerts** module (in our example), then by default **Open** will be displayed in the **Status** field.

In the **Default Value** field for the **Date/Time** field type you can specify either a **Static** date/time or a **Custom** date/time. If you select **Static**, click the **Select Date** icon to display the Calendar and select the required date/time. If you select **Custom**, then you can specify a date/time relative to the current date/time such as 1 hour from now, or 3 hours ago.



**Note:** In case you have upgraded to version 5.0.0 or later, then you will have to reselect your datetime default values, since the new datetime format is not backward compatible. You will be able to see the older applied datetime default value in the FortiSOAR™ fields. However, if you want to edit the default field, then you will have to specify the datetime again in the **Default Value** field.

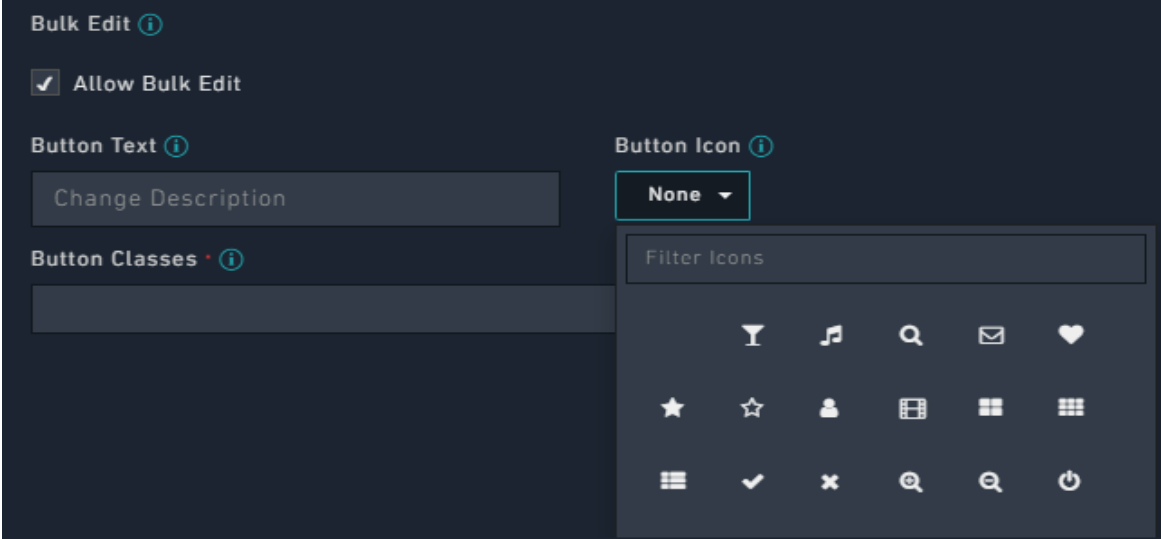
- **Tooltip:** Brief definitions that you can optionally add to fields. This definition is displayed when you click the information (i) icon of the field that has tooltip information added while creating, updating, or viewing records.
- **Length Constraints:** In case of a Text field with sub-type set as Text Field or Text Area, you can specify length constraints by clicking the **Add minimum/maximum range** checkbox, if you want to override the default field length constraints by providing a minimum-maximum range for a field. Once you select the **Add minimum/maximum range** checkbox, you can specify the minimum character length for the field in the **Minimum** field and the maximum character length for the field in the **Maximum** field. You can enter any number from 0 to the maximum character length that is applicable for that field in the database. FortiSOAR™ will display a validation message if the maximum character length for the field is exceeded, or if the minimum character length for the field is not met.
- **Bulk Edit:** Selecting the **Allow Bulk Edit** option to allow bulk edit operations on the selected field.  
For example, if you have selected the **Severity** field, in the **Alerts** module, and have clicked **Allow Bulk Edit**, this means the users can select multiple records in the grid view of the **Alerts** module and change the severity of those records to a particular severity level. You must enter the following details for the button that you want to use for the bulk edit operation:



**Button Text:** In the **Button Text** field, type the name of the label that will be displayed on the bulk action button. For example, type **Change Type**.

**Button Icon:** From the **Button Icon** drop-down list, select the icon that will be displayed on the bulk action button. If you do not want an icon to be displayed, select **None**.

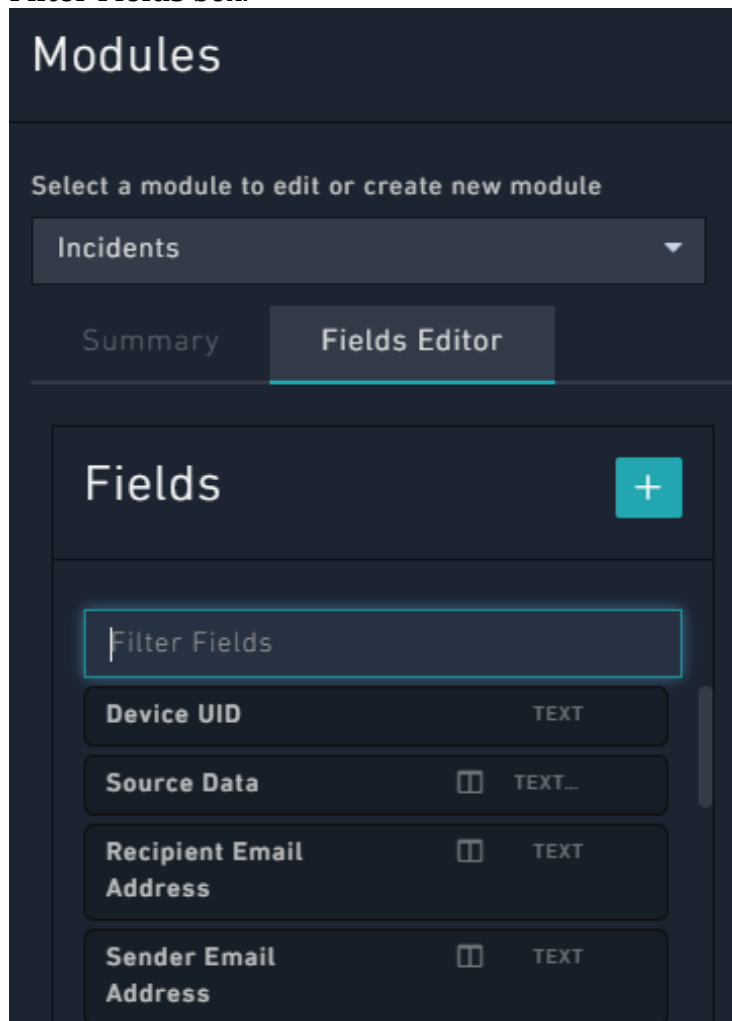
**Button Classes:** From the **Button Classes** drop-down list, select from the **Default**, **Primary**, **Danger**, or **Warning** styles.



Once you save the changes and publish the module, a **Change Severity** button is added to the **Alerts** module in the action bar. For more information on how to use the bulk action button, see *Working with Modules - Alerts & Incidents*. You can add the bulk edit action button for any other fields, such as **Status**, **Assigned To**, and **Type**.

- c. Click **Apply** to add the field or click **Revert** to clear any changes made to the field since the last **Save** event or click **Remove** to remove the field. For information on the save and revert operations, see the *Saving your changes* section.
5. You can also define the order of the default grid columns, which is defined by the order of the fields in the **Fields Editor** list. Fields are listed in the **Fields** column and you can drag-and-drop the fields to sequence the fields. You can also filter fields using the

Filter Fields box.



6. Click **Save** to save the changes to the module or click **Revert > Revert to last saved** to clear any changes made in the interface since the last **Save** event or click **Revert > Revert to last published** to clear any changes made since the last Publish event. For fields, you can revert only to the last published instance. For information on the save and revert operations, see the *Saving your changes* section.

Once you have completed making modifications to the module, you must publish the modules to reflect the changes in the system. This takes the system down for up to a few minutes while the changes are made. See the *Publishing Modules* section for more information.

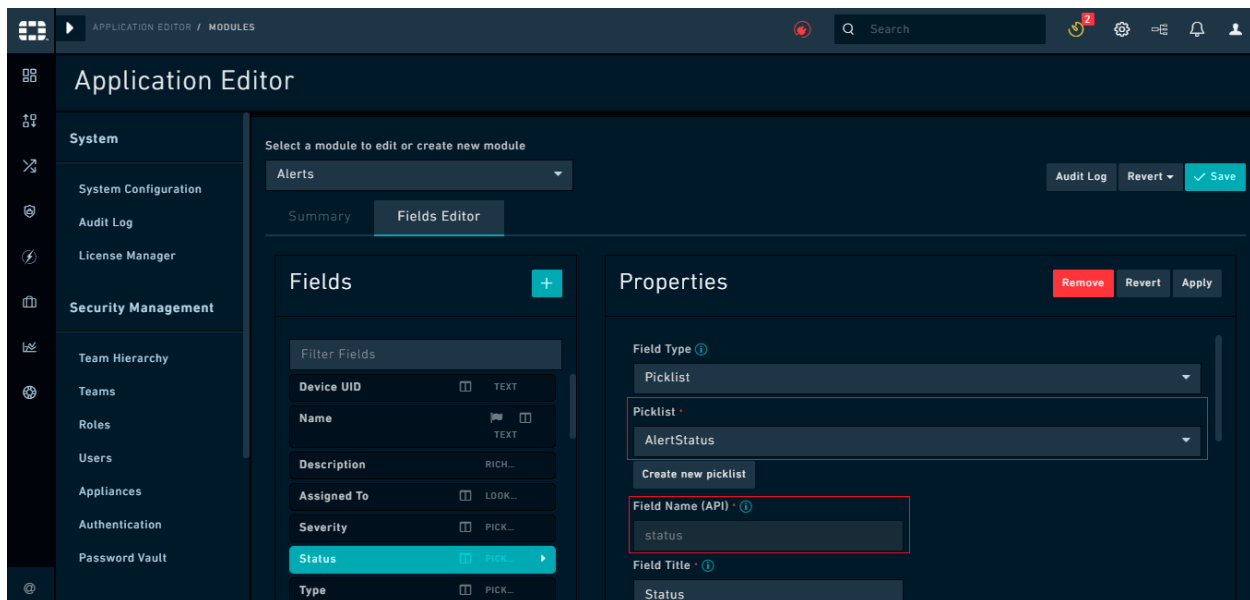
**Note:** The Module Editor changes the relational database schema, therefore for changes to go live in the environment, you must perform a Publish to the database. This temporarily takes the application offline while the database operations are being performed. All users in the application must save their work prior to this occurring before this occurs or you risk data loss.

## Display Template

A module's Display Template refers to one or more fields in the data model itself that is used to display a record in the general interface. Certain widgets, or visualizations in the interface, use the Display Template to identify records to the user. This template specifies the fields that will be displayed when a record from this module is referenced in the application. Fields of a module can be specified in the display template as `{{ <*name of the module's field*>_name }}`. If multiple fields are part of the display template, then you can specify multiple fields as `{{field_name1,field_name2,...}}`.

**Summary “FYI”:** If you were to use just the name of the module itself, such as Incidents, every Incident record in the interface would include a label named `Incident`. So, users see the Incident label with every record, which is not helpful. Therefore, we use Templates with a language to describe how to label your modules.

You can also include an attribute, such as `itemValue`, of a picklist field in the Display Template, add the following jinja: `{{picklistFieldName.itemValue}}`. For example if you want to include the status of the alert in the Display Template, then the picklist to be used would be `AlertStatus`, and the picklist field name would be `status`:



**Figure 66.** Example of adding jinja in Display template for picklists

Therefore you require to add the following jinja: `{{status.itemValue}}` in the Display Template.

### Example

We have taken the `Asset` module as an example. Assets represent computing resources, typically on the network. Assets generally have a hostname, IP Address, or MAC Address. We are using the hostname as an example.

To create a **Display Template** for the Assets module with the hostname, you must ensure that you have already added the `hostname` field using the **Field Editor**. Once the hostname is added as a field in the Assets module, use the following expression in the Display Template field:

```
{{ hostname }}
```

The double curly braces, `{{ }}`, is used to identify a variable, specifically a field name. In our case, we are calling the `hostname` field. Any expression in the Display Template field that uses a field from the module data fields must use the double curly braces surrounding the field name. When the record is displayed, the hostname of each asset is used in the interface, so users know the asset they are selecting. For example, a user can know that they are selecting an **HR Server**.

Assets have a unique situation. They might only have one of those pieces of identifiable information depending on what is known about a resource. A laptop on a DHCP network might have only a MAC address. If we set the Asset Display Template to always be a hostname, in many cases the asset might have a blank Display Template in the interface. For these situations, the Angular Template expression allows you the flexibility to modify the format of the Display Template in a way that can account for variation. Taking the asset example, asset information is used to help users identify the asset when in the interface. Because using only a single asset field could potentially lead to a lot of blank Display Templates, we use multiple fields such as hostname, IP address and Mac address:

```
{{ hostname }} {{ ip }} {{ mac }}
```

This Display Template expression instructs the system to use all three fields based on their field names. If a field is not present, it displays as blank. In some cases, depending on what is known about the asset, the Display Template will include all three pieces of information, in others just one.

You can further extend this to display static information that identifies the parts of the Display Template. The following example includes the static text of **Hostname:**, **IP:** and **MAC:** in every Display Template. This might be redundant but is an option.

```
Hostname:{{ hostname }} IP:{{ ip }} MAC:{{ mac }}
```

We recommend that to keep things simple, most of the time you would want to use the following expression for a Display Template, assuming you always create a `name` field for a module:

```
{{ name }}
```

This ensures that the Display Template points to whatever is in the `name` field on any module record. If you create `name` as a required field, then it will always be populated.

## Adding a related module to the related records for a module

1. Click **Settings** and click **Modules** in the **Application Editor** section, to open the Module Editor.

This displays the **Modules** page.

2. On the **Modules** page, from the **Select a module to edit or create new module** drop-down list, select the first module that you want to relate.  
For example, select **Alerts**.
3. Click the **Fields Editor** tab and click the Add (+) icon beside **Fields**.
4. Set the following values:  
Field Type: **Many to Many**  
Related Module: Module that you want to relate. For example, **Indicators**  
Related Field (Optional): blank (for now)  
Field Name (API): Exact name of the related model. For example, **indicators**  
Field Title: Name to describe the related model. For example, **Indicators**  
Editable: Select editable to allow the field to be modified after creation of a module record. If this is option is not selected, then the initial value of the field cannot be changed after the record is created.

Select a module to edit or create new module

Alerts

Audit Log Revert Save

Summary Fields Editor

Fields +

Filter Fields

(Untitled) TEXT

Device UID TEXT

Name TEXT

Description RICH...

Assigned To LOOK...

Severity PICK...

Status PICK...

Type PICK...

File Hash TEXT...

Target Asset TEXT

Properties Remove Revert Apply

Field Type ① Multiple Relationship (Many to Many)

Related Module ① Indicators

Related Field ① Select a Field to Relate

Field Name (API) ① indicators

This field must have a unique value.

① After you have published "Alerts" module, "Field Name" cannot be modified.

Field Title ①

5. Click **Save**.
6. On the **Modules** page, from the **Select a module to edit or create new module** drop-down list, select the other module to be related.  
For example, select **Indicators**.
7. Click the **Fields Editor** tab and click the Add (+) icon beside **Fields**.
8. Set the following values:  
Field Type: **Many to Many**  
Related Module: First module that was related. For example, **Alerts**  
Related Field (Optional): blank (for now)  
Field Name (API): Exact name of the first related module. For example, **alerts**  
Field Title: Name to describe the related model. For example, **Alerts**  
Editable: Select editable to allow the field to be modified after creation of a module record. If this is option is not selected, then the initial value of the field cannot be

changed after the record is created.

Select a module to edit or create new module

Indicators

Audit Log Revert Save

Summary Fields Editor

Fields +

Filter Fields

emails MAN...

Tags TEXT

UUID TEXT

Events MAN...

Alerts MAN...

Assets MAN...

Companies MAN...

Incidents MAN...

Properties Remove Revert Apply

Field Type ①

Multiple Relationship (Many to Many)

Related Module ①

Alerts

Related Field ①

Select a Field to Relate

Field Name (API) ①

alerts

Field Title ①

Alerts

9. Click **Apply**.
10. Select the same name and set the value **Related Field (Optional)** field to the related field in the other module. For example, **indicators**.

Select a module to edit or create new module

Indicators

Audit Log Revert Save

Summary Fields Editor

Fields +

Filter Fields

emails MAN...

Tags TEXT

UUID TEXT

Events MAN...

Alerts MAN...

Assets MAN...

Companies MAN...

Incidents MAN...

Properties Remove Revert Apply

Field Type ①

Multiple Relationship (Many to Many)

Related Module ①

Alerts

Related Field ①

Select a Field to Relate

Select a Field to Relate

Indicators

Field Name (API) ①

Field Title ①

Alerts

11. Click **Save**.
12. Select the first module, in our case Alerts, and then click the **Fields Editor** tab, and select the field that you had created.

13. Set the value **Related Field (Optional)** field to the related field in the other module. For example, **alerts**.

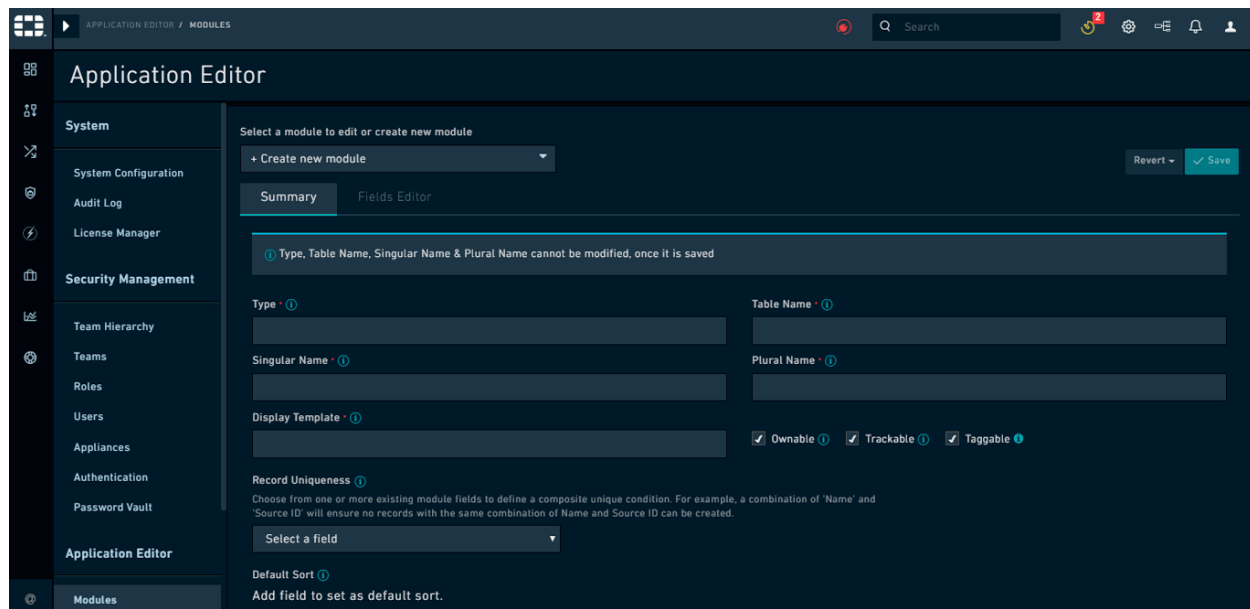
The screenshot shows the Fortinet Fields Editor interface. At the top, there's a dropdown menu for 'Alerts' and buttons for 'Audit Log', 'Revert', and 'Save'. Below this, there are tabs for 'Summary' and 'Fields Editor'. The 'Fields Editor' tab is active, showing a list of fields on the left and the 'Properties' panel on the right. The 'Fields' list includes 'Notes', 'Comments', 'Vulnerabilities', 'People', 'Emails', 'Indicators' (highlighted), 'Task', 'Events', and 'Alerts'. The 'Properties' panel shows the 'Field Type' as 'Multiple Relationship (Many to Many)', the 'Related Module' as 'Indicators', and the 'Related Field' as 'alerts'. There are also buttons for 'Remove', 'Revert', and 'Apply' in the top right of the 'Properties' panel.

14. Click **Save**.
15. Click **Publish All Modules** and wait for the publishing to complete. Now, the modules must show the relationship, i.e., both the **Indicators** and **Alerts** modules will have a tab to relate to each other.

**Note:** You must perform a similar procedure to relate two modules using the **Lookup (One to Many or One to One)** field type. If you add the related field to only one of the modules, you can get an error, while publishing, as follows: **Inversed field 'alert' does not exist on related model metadata. Module 'UUID of Module 1' Field 'UUID of Module 2' on 'inversedField'.**

## Creating a New Module

To create a new module, click **Settings > Modules**. This displays the **Modules** page. Use the **+Create new module** option that appears at the top of the editor to define the properties of the module. By default, when choosing the Module Editor, the ability to define the new modules is available.



**Figure 67.** Adding a new Module

Bear in mind there are requirements to realize the addition of the new module, notwithstanding the need to allow for the interface to recognize this module.

See the *Modifying an existing module* section for information on how to add and edit fields. After you have completed adding fields to the module, click **Save** to save the changes to the module and publish the module to reflect the changes in the system. For information on the Save operation, see the *Saving your changes* section. For information on publishing, see the *Publishing Modules* section.

## Saving your changes

Whenever you make any changes to a module or a field, you must stage those changes by saving. At the top-right of the Module Editor is the **Save** button, which applies any changes made to the staged data. To update the database and make your changes to go live, you must **Publish** the updated modules.

The **Revert** button clears any changes made in the interface since the last **Save** event. If you go into a module and realize that you have edited the wrong field, use **Revert** to clear the changes. However, once you press **Save**, you require to undo the changes manually.

## Viewing your changes

Editing any of the fields of a module does not mean those fields are accessible immediately within the UI or the API. The fields must be first represented in the database. The templates included might automatically discover these fields, or these fields might need to be added manually to the template to specify their location within the interface. However, you can set the grid defaults within the attribute data for the model itself.



To update the database and make your changes to go live, you must **Publish** the updated modules.

## Publishing modules

Whenever you change a field or a module and click **Save**, the change is staged but is not yet live in the system. You must perform a **Publish** to ensure that the changes are made in the system.

You initiate a publish action by clicking the **Publish All Modules** button at the top-right of the Module Editor page. Publishing pushes the changes that you have made to fields and modules to the database. Up until the Publish point, all changes to the data model in the Module Editor are saved as metadata, which is information that describes the structure of other information.

A Publish is the point at which the changes are truly irreversible, meaning that an unintended field deletion could cause irretrievable data loss. Use Publish carefully and verify changes before Publishing to avoid any problems.

**Warning “Publishing is a sensitive operation”:** We recommend that you send a prior notification to all users of a publish since while the publish is in progress users are unable to work. We also recommend reviewing each staged change to ensure that only the desired changes are going to take effect.

If there is any error during the publish operation, FortiSOAR™ displays a meaningful error message at the top of the module editor, so that it becomes easier for you to resolve issues.

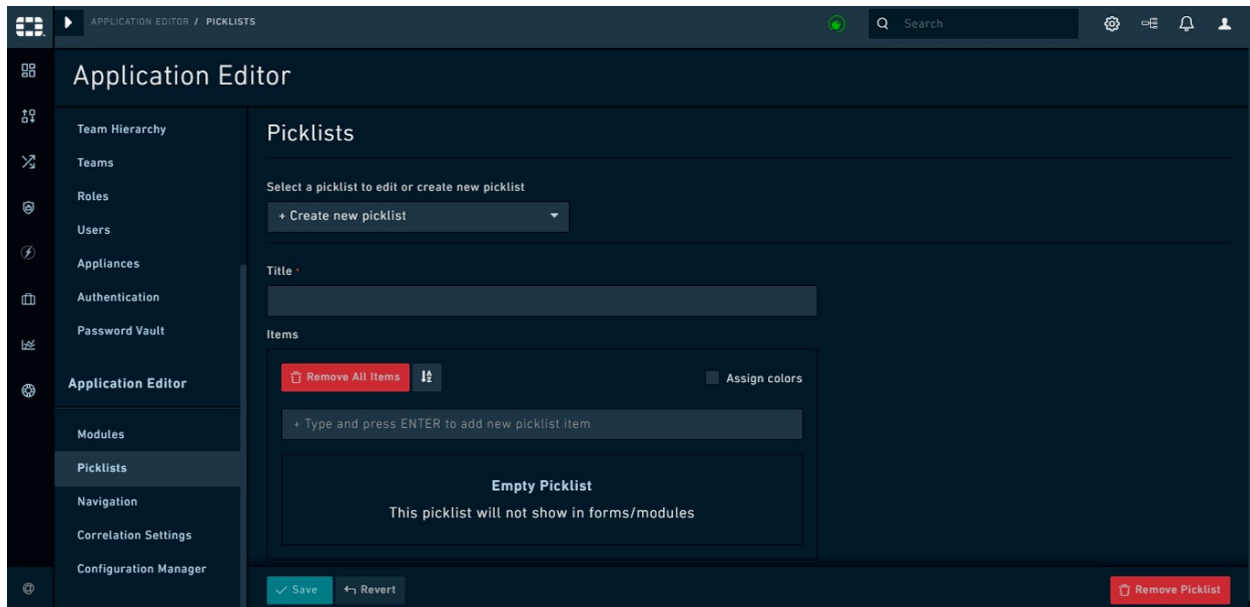
**Note:** If you have not selected an appropriate field from the **Related Model** drop-down list, for a **Many to One**, or a **Many to Many** field, then the publish operation will display an error.

## Picklist Editor

Use the Picklist Editor to change the values of any picklist within the modules and add new picklists that might be referenced by a field in any module.

Unlike the Module Editor, changes made in the Picklist Editor are immediately live once they are saved. This is because Picklists names and Picklist values are records in the database.

A UUID (Universally Unique Identifier) identifies picklist values, which means if you modify any of the names or colors of an existing picklist value, the original data is preserved. Therefore, all records that contain that picklist value retains a reference to the UUID for the picklist. This means that if you want to change an Incident Category of **Theft** to **Physically Stolen**, you could make that change on the existing **Theft** value and any records with the value of **Theft** would now display **Physically Stolen**.



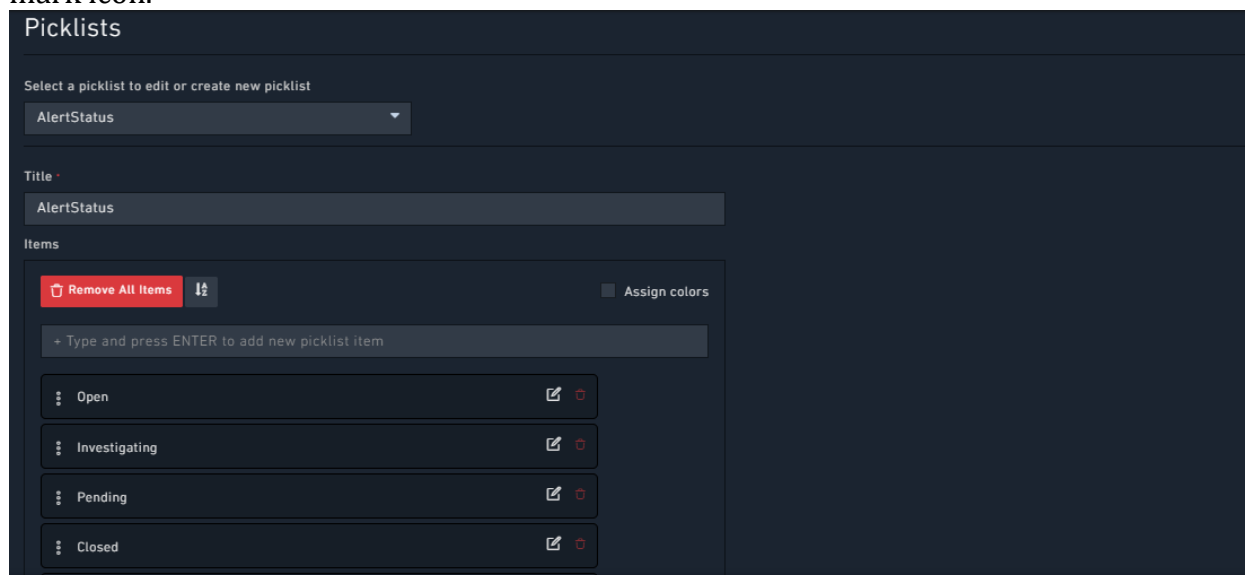
**Figure 68.** *Picklist Editor*

## Creating or modifying a picklist

To add or modify a picklist:

1. Click **Settings** and in the **Application Editor** section, click **Picklists**. This displays the Picklist Editor.
2. Add or edit an existing picklist. To add a picklist, use the **+Create new picklist** option that appears at the top of the editor to define the properties of the picklist. Start by entering a title for the new picklist in the **Title** field.  
Or To edit an existing picklist, from the **Select a picklist to edit or create new picklist** drop-down list, select the picklist.  
For example, select **AlertStatus**.
3. In the **Items** section, in the **+ Type and Press ENTER To Add New Picklist Item** field, enter the name of the new picklist item and press **Enter**.  
For example, for the **AlertStatus** picklist, add items such as **Open**, **False Positive**, and **Verified**.  
Or  
To edit a picklist item, click the **Edit** icon that appears on the item row, update the name of the item or the color assigned to the picklist, and then click the green tick

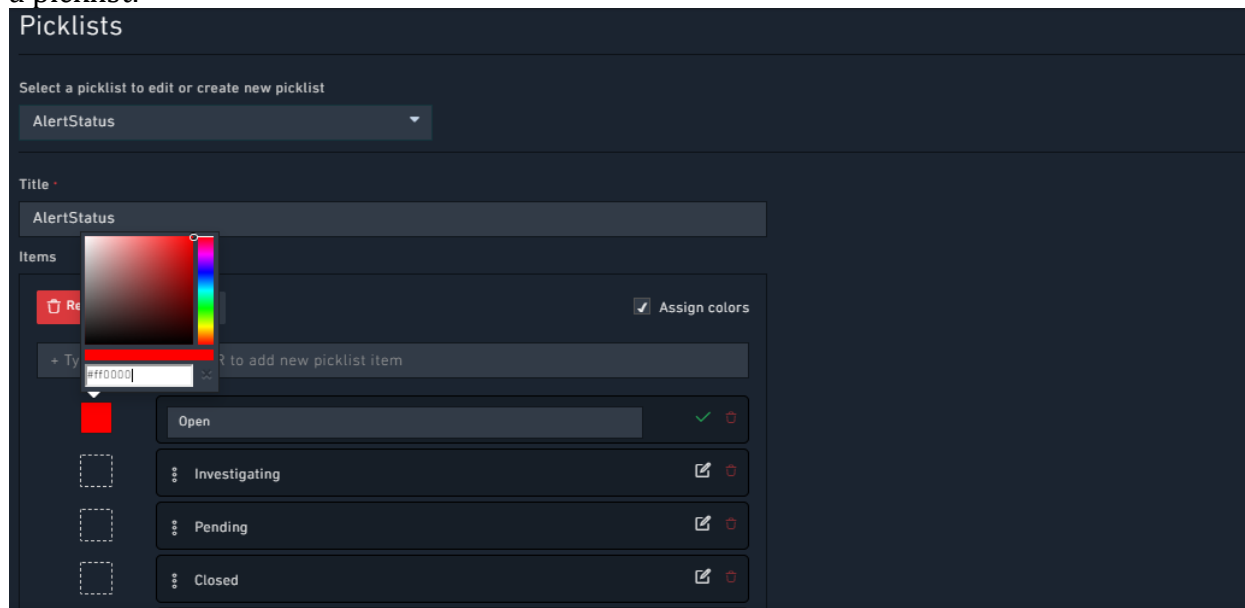
mark icon.




4. (Optional) You can add colors to any picklist, by checking the **Assign Colors** checkbox. Once the Assign colors checkbox is enabled, you can assign each item in the picklist a color.

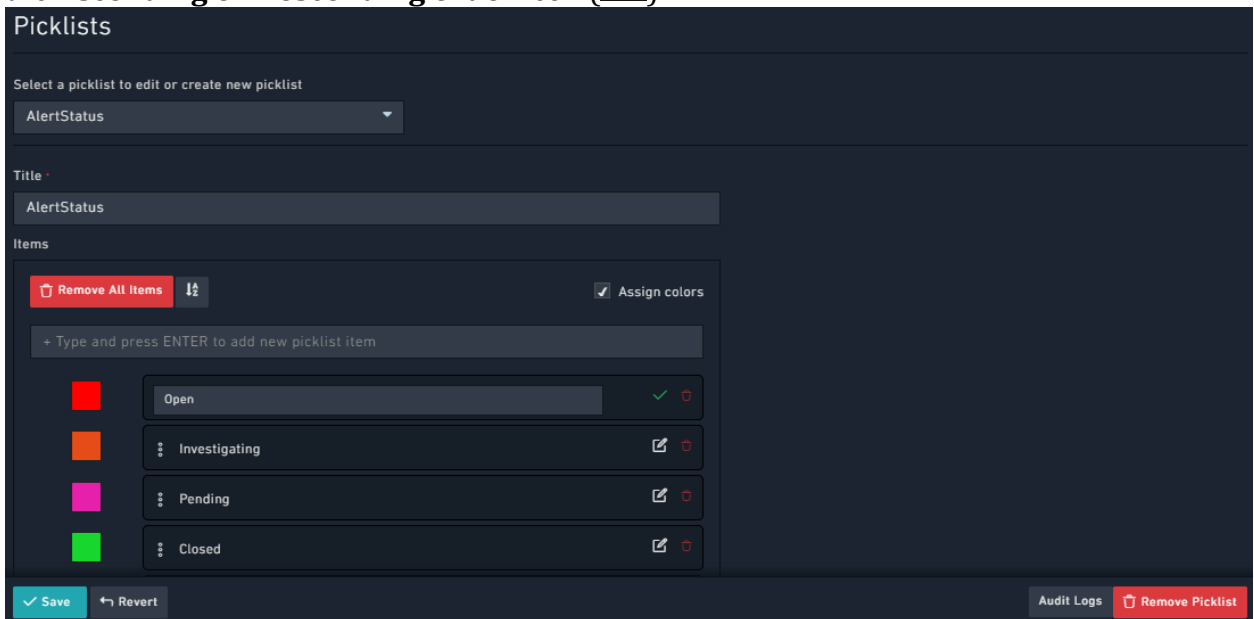
Use the color picker box that appears next to each item in the picklist or enter the hexadecimal code for the color to edit the colors. You can use any valid HTML color. You can set the picklist color by directly entering the hexadecimal code of the color and assigning that as the picklist color, or by using an API, or you could choose colors by clicking in the color picker.

The following image shows how to enter a hexadecimal code (#ff0000 for red color) in a picklist:



**Note:** Multiple items in a picklist can have the same color.

- (Optional) You can also remove all items from the picklist by clicking the **Removing All Items** button, and you can also change the sort order of the picklist items clicking the **Ascending or Descending order** icon (  ).



Picklists


Select a picklist to edit or create new picklist

AlertStatus













Title

AlertStatus

Items

Remove All Items  Assign colors

+ Type and press ENTER to add new picklist item

	Open		
	Investigating		
	Pending		
	Closed		

Save Revert

Audit Logs Remove Picklist

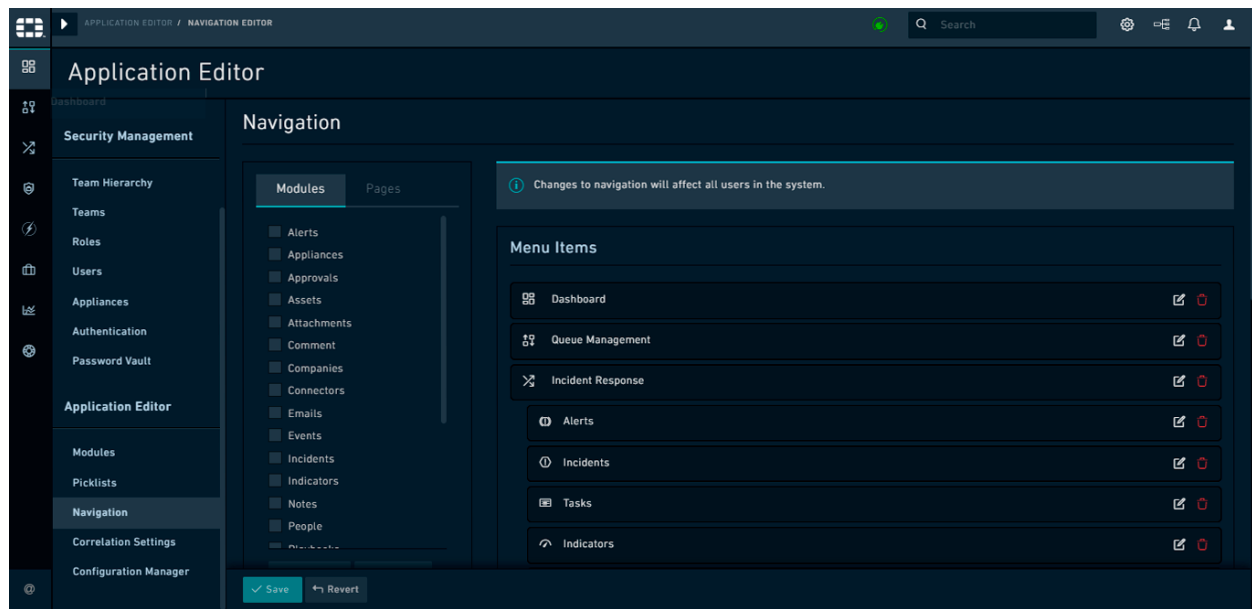
- Click **Save** to save the changes made to the picklist or click **Revert** to clear any changes made to the picklist since the last **Save** event or click **Remove Picklist** to remove the picklist.  
You can also click the **Audit Log** button to view logs specific to a particular picklist.  
For more information on Audit Logs, see the *System Configuration* chapter.

## Navigation Editor

Pages are iFramed resources that are accessible from the application interface by the user, such as resource pages and wikis within the local environment or on an accessible website link. Pages must currently be added in the `modules` API to be present to add in the Editor.

Use the Navigation Editor to modify the system Navigation bar, present on the left-side of the application interface.

**Note:** Changes that you make to the left navigation bar using the Navigation Editor affects all users. Currently, these changes cannot be made at a user-specific level.



**Figure 69.** *Navigation Editor*

There are two types of Navigation values:

- Single-level navigation item, in which case an icon and title on the Navigation bar represent a module or page
- Two-level navigation item, in which case an icon and title reveal a menu of additional options. Secondary navigation items might only have a name, not an icon.

You can add an external HTML page in an iFrame or a new tab and display that page as part of the left-navigation in FortiSOAR™.

## Modifying the Navigation bar

To modify the Navigation bar:

1. Click **Settings** and in the **Application Editor** section, click **Navigation**. This displays the **Navigation Editor**.
2. Add or modify the navigation bar:
 

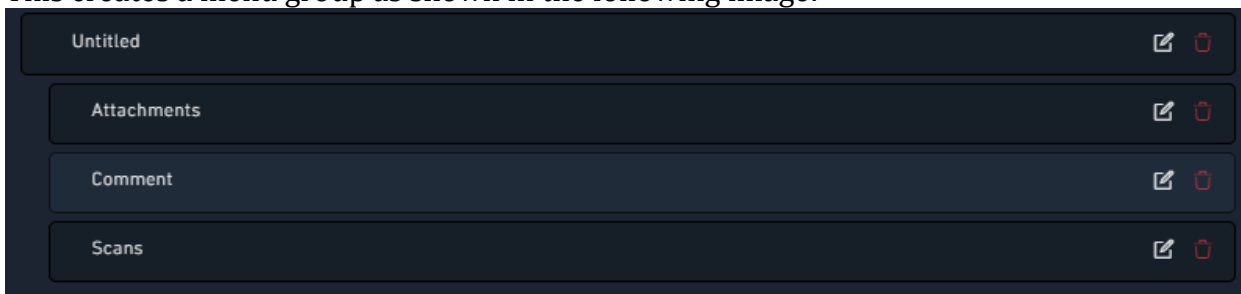
To add a single-level item, select module or pages by clicking the **Modules** or **Pages** tab, and click **Add To Menu**. Single level items on the menu must represent a 1:1 relationship with a module or page.

To add a two-level item, select modules or pages by clicking the **Modules** or **Pages** button, and click **Add As Group**.

The second-level navigation item is not a hyperlink or capable of referencing a given module or page. Only the sub-items in the group can be linked as a module or page. Clicking any two-level Navigation group shows and hides the sub-items.

For example, you want to create a menu-group named Artifacts Management that has Attachments, Comment, and Scans as the menu items. You select the Attachments, Comment, and Scans modules and click **Add As Group**.

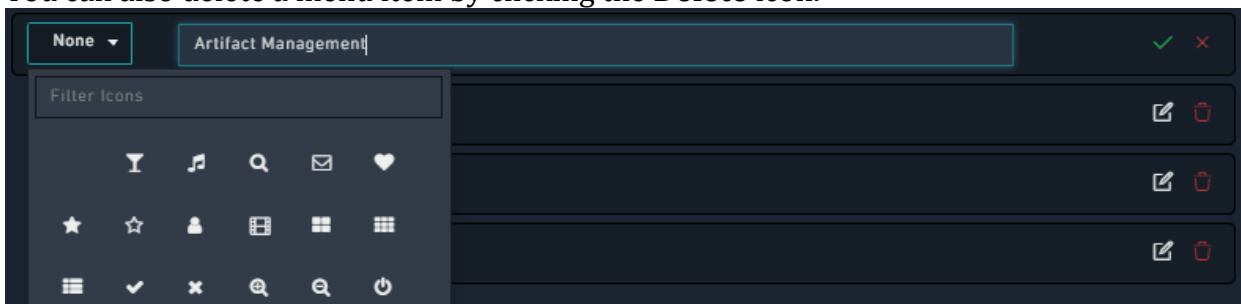
This creates a menu group as shown in the following image:



3. Edit the menu items by clicking the **Edit** icon that appears on the item row, update the name of the menu item or replace the icon of the first-level item in menu group, and click the green tick mark icon.

You can replace icons by choosing icons from the icon selector at the left of each Navigation item.

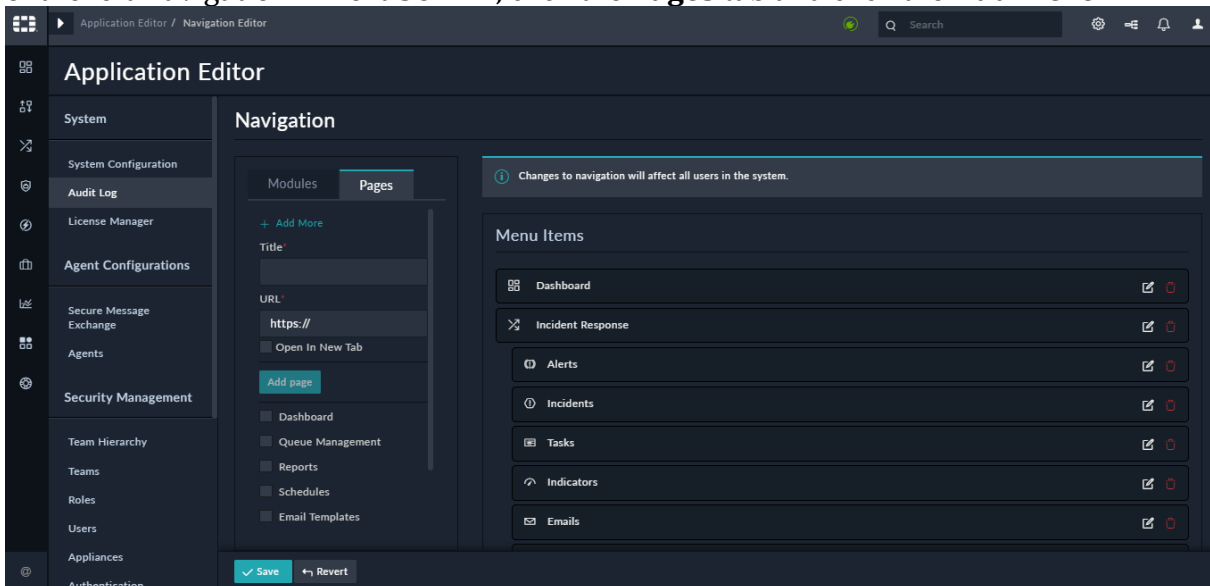
You can also delete a menu item by clicking the **Delete** icon.



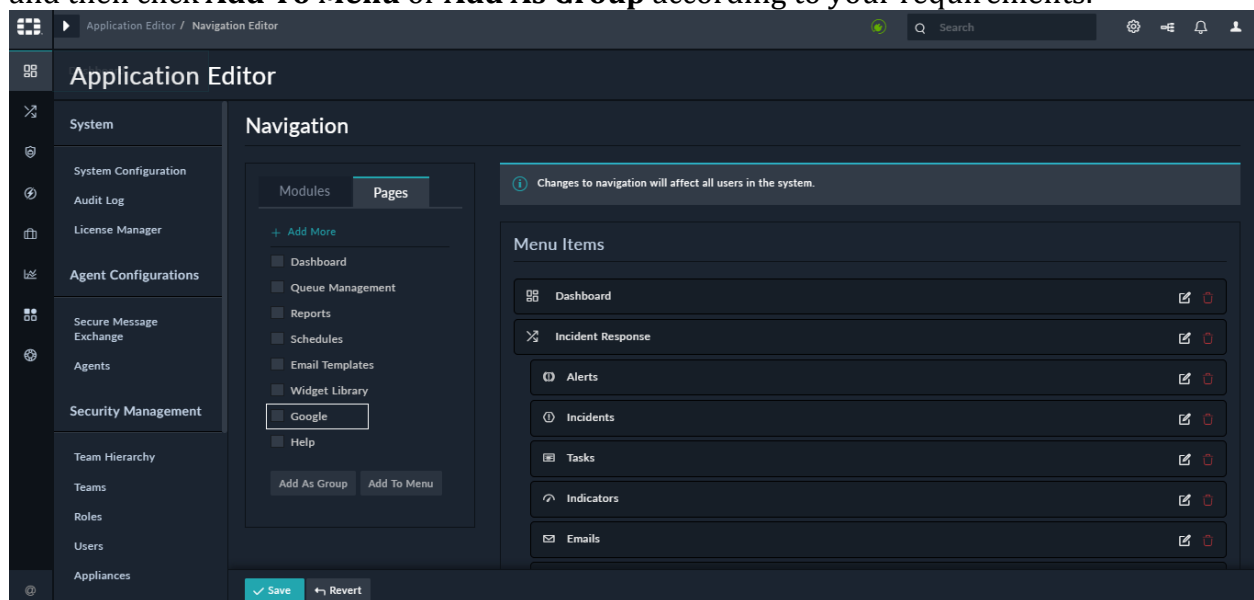
4. Drag-and-drop modules or module groups to change the order of the navigation items in the Navigation bar.

**Note:** The top item of the navigation is always the default login page. By default, this is the dashboard page. However, you can modify this to make any other page the home page.

5. To add an external HTML page in an iFrame or a new tab and display that page as part of the left-navigation in FortiSOAR™, click the **Pages** tab and click the **Add More** link.



- a. In the **Title** field, enter the name for the HTML page that you would want to display in the left navigation menu.  
For example, if you want to add a link to the Google website as part of your left-navigation in FortiSOAR™, enter **Google** in the title field.
- b. In the **URL** field, enter the URL for the HTML page that you want to display in an iFrame or new tab. For our example, enter <https://www.google.com>.
- c. (Optional) If you want to open the page in a new tab, click the **Open in New Tab** checkbox.  
If the **Open in New Tab** checkbox is unchecked (default) the page will open in an iFrame in FortiSOAR™.
- d. Click **Add Page**.
- e. On the **Pages** tab, select the page you have just added, **Google** in our example, and then click **Add To Menu** or **Add As Group** according to your requirements.



6. Click **Save** to save the changes made to the menu items or click **Revert** to clear any changes made to the menu items since the last **Save** event.

## Correlation Settings

If you want to use the Visual Correlation widget to visually display the nodes related to a particular record, then you have to configure the display of the various related nodes on the **Visual Correlation Setting** page.

The following procedure is an example where you are configuring the display of tasks that have associated records.

1. Click **Settings** and in the **Application Editor** section, click **Correlation Settings**.
2. On the **Visual Correlation Setting** page, from the **Choose Modules To Define Correlation View Configurations** drop-down list, select the module for which you want to define visual correlations and then click **Add and Configure**.

**Note:** FortiSOAR™ has pre-configured five modules, Alerts, Assets, Incidents, Indicators, and Vulnerabilities. The default depth of the nodes displayed is "3", i.e., if you start from the Alerts node, you view its related indicators and if those indicators have related assets, you can view those related assets. However, if that asset also has a related incident, then you can double-click on that asset node and see its related incident and so on.

3. To configure the **Tasks** module, from the **Choose Modules To Define Correlation View Configurations** drop-down list, select **Tasks** and click **Add and Configure**.
4. From the **Choose Related Modules** drop-down list, select the modules that should be shown in the correlation graph as linked modules, and then click **Add Related Modules**.

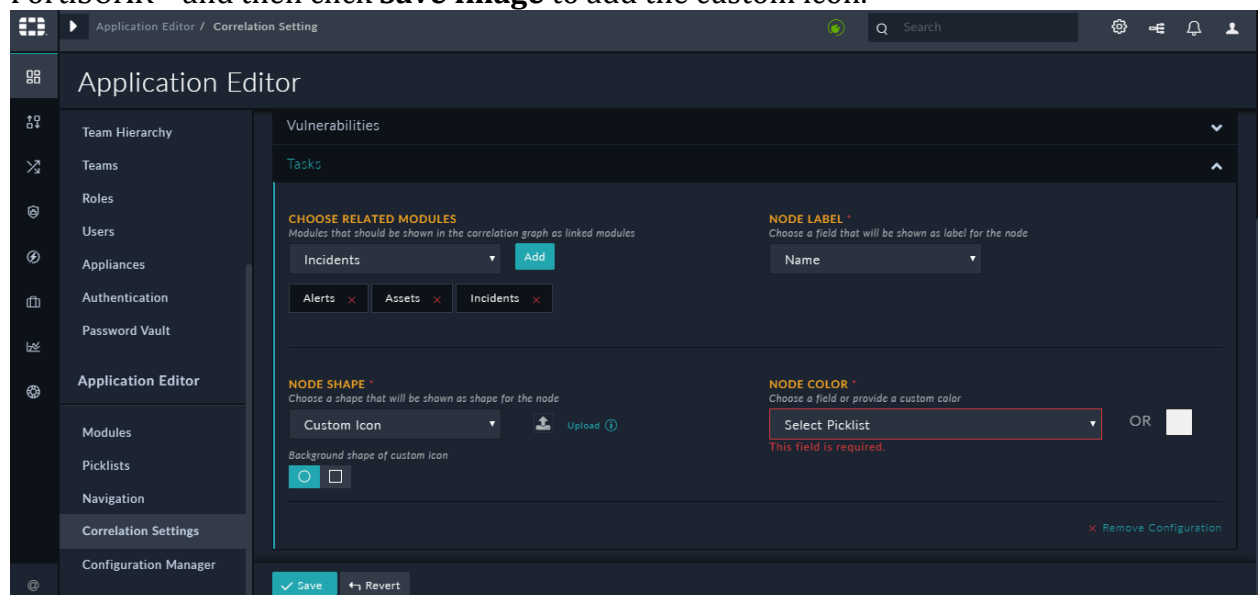
**Note:** The modules that are pre-configured already have related modules configured, for example, the Alert module has Alerts, Incidents, Indicators, Vulnerabilities, and Assets configured as related modules.

For our example, we require to add **Alerts**, **Assets**, and **Incidents**, as related modules to the **Tasks** module.

5. From the **Node Label** drop-down list, select the field that will be shown as a label for the node.  
For our example, choose **Name**.
6. From the **Node Shape** drop-down list, select a shape that will be shown as the shape of the node.

For our example, choose **Square**.

You can also choose to specify a custom icon as the shape of the node. In this case choose **Custom Icon** from the **Node Shape** drop-down list and click **Upload** to display the **Upload an Image** dialog. In the **Upload an Image** dialog, drag-and-drop the icon file, or click the **Import** icon and browse to the icon file to import the icon file into FortiSOAR™ and then click **Save Image** to add the custom icon.



You also require to change the background shape of the custom icon by clicking the shapes present under **Background shape of custom icon**.



You can also change the custom icon by clicking **Change**, which again displays the **Upload an Image** dialog.

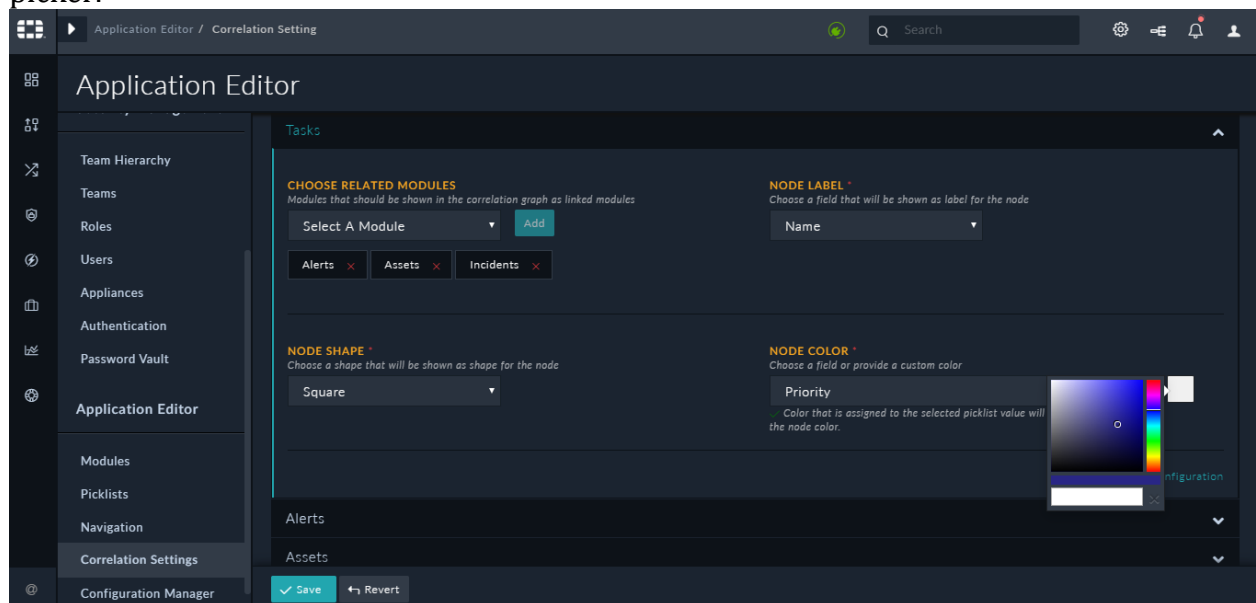
**Note:** The custom icon should be 15px X 15px and the file size must be less than 10KB. Also, once you select a custom icon, you cannot specify the node color.

7. From the **Node Color** drop-down list, select the field that will conditionally determine the color of the node.

For the pre-configured modules, such as alert, this field is set by default. For example, for the Alerts module, this is set as **Severity**. For the Tasks module, select **Priority**.

**Note:** In case of picklists the color of the node is determined by the color that you have assigned to the value of the picklist item. For example, if you have chosen the **Priority** as the picklist, then the colors that you have assigned to the selected picklist value will be used as the node color. For example, if the Priority is set as Urgent, then the node color will appear as Red, if its High, then the node color will appear as Orange, if its Medium, then the node color will appear as Yellow, etc. Therefore, if the task in which you have added the Visual Correlation widget is Critical, then its node color will be Red. For information on how to add the Visual Correlation widget in the records, see the *Dashboards, Templates, and Widgets* chapter in the "User Guide."

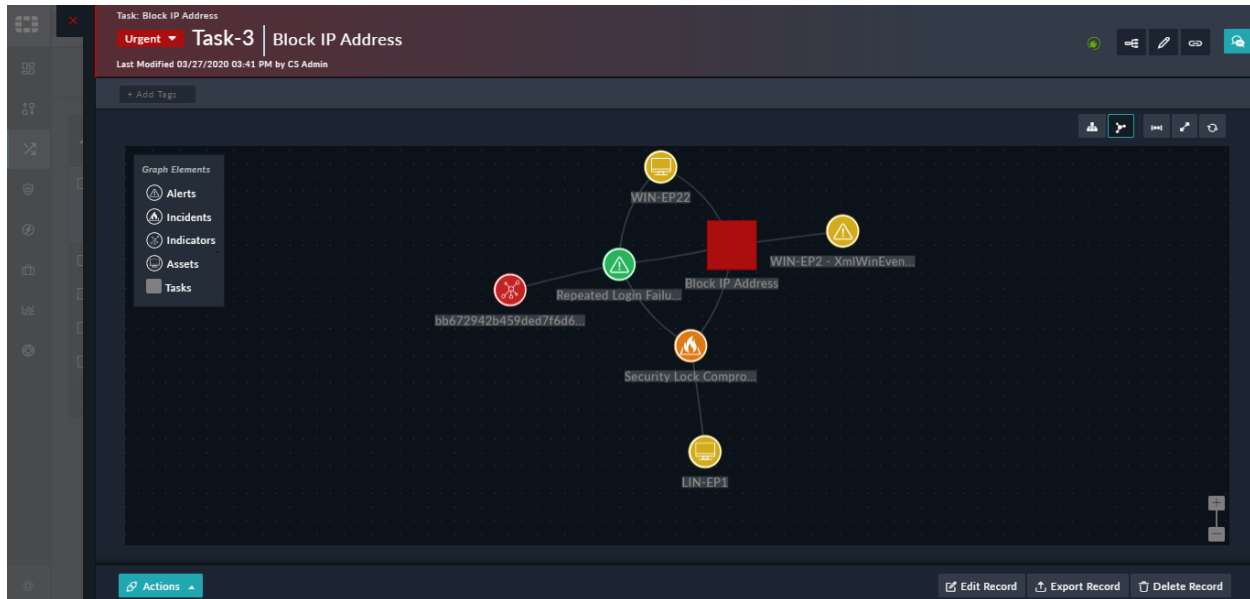
You can also assign a custom color for the node by using the **Choose custom color** picker.



If you do not specify any color, the node will appear with its default color.

8. Next, you require to define how the related record node will also be displayed. For our example, we have chosen Alerts, Incidents, and Indicators modules, as related modules all of which are pre-configured modules, so we do not require to configure any module.
9. Click **Save** to save the settings for visual correlation.

Now, if you have added the Visual Correlation Widget in the Tasks detail view (see the *Dashboards, Templates, and Widgets* chapter in the "User Guide"), it will display the "Visual Correlations" graph as shown in the following image:



**Figure 70.** Display of the configured Visual Correlation Widget in the Tasks Details view

As you can see in the above image, the Correlations graph has a title which is **Tasks: Correlated Records**. The title can be specified by the user when they are adding the Visual Correlation Widget. The task for which correlated records are displayed is shown as a square node, whose color is determined by its severity, Red in this case since the task has priority set as "Urgent". The name of the task displayed as the label of the node. The associated records are displayed as various nodes, which is determined by the legend given in the left of the graph. The color of the nodes is determined by their "Severity" in case of Incidents and Alerts and "Asset Criticality" in case of Assets. For example, linked records whose severity is critical appear in red, high appear in orange, those that are medium appear in yellow, those that are low appear in green, and so on.

## Configuration Export and Import

FortiSOAR™ provides you with a wizard-based export and import of configuration information, dashboards, application settings, etc., which enhances the user experience and improved architecture. These enhancements also allow for scheduled, API-based configuration export and imports. For information about the export and import APIs, see the *API Methods* chapter in the "API Guide."

## Permissions required

- To export and import configurations using the Wizards or APIs, users who will be performing the import/export operations must be assigned a role that has **Create**, **Read** and **Update** permissions on the **Application**, **Security**, and **Playbooks** modules. Users who require to import files must additionally be assigned a role that has **Create** and **Read** permissions on the **Files** module.

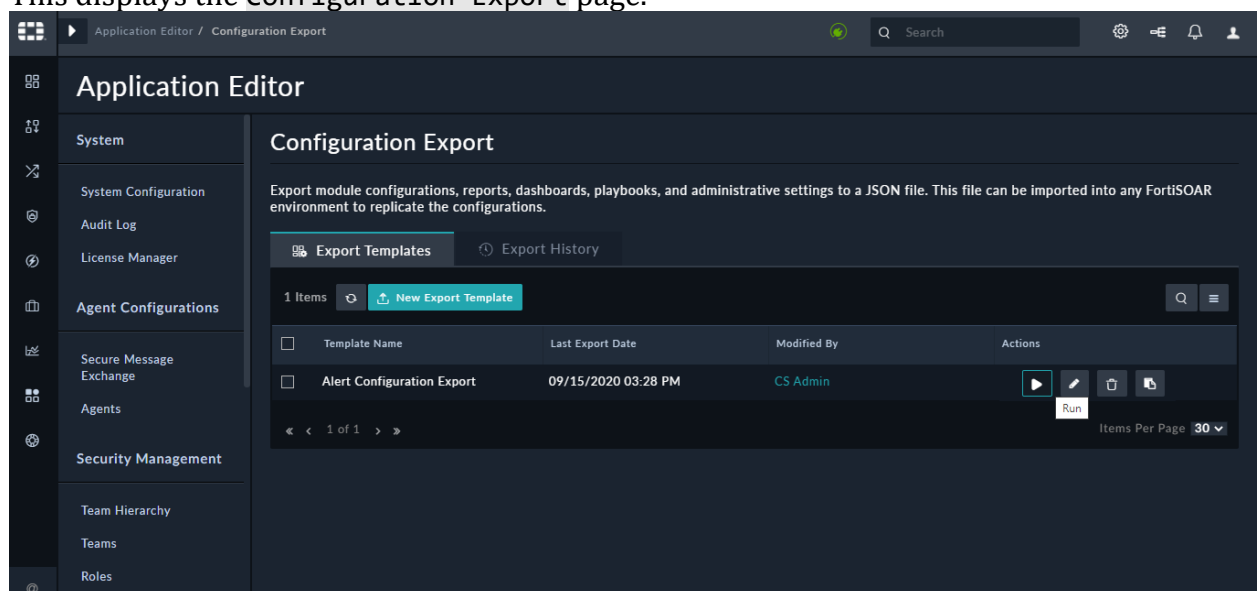
- If a playbook is running the import and export using the API, your playbook appliance also requires the same permissions.

## Configuration Export Wizard

You can use the Configuration Export Wizard to export module configuration information such as module metadata, field definitions, picklists, view templates, etc. of your modules. You can also export playbook collections, dashboards, reports, and administrative settings such as, application configuration, system views, etc.

To export configurations, do the following:

1. Click **Settings** and in the **Application Editor** section, click **Configuration Export**. This displays the **Configuration Export** page.



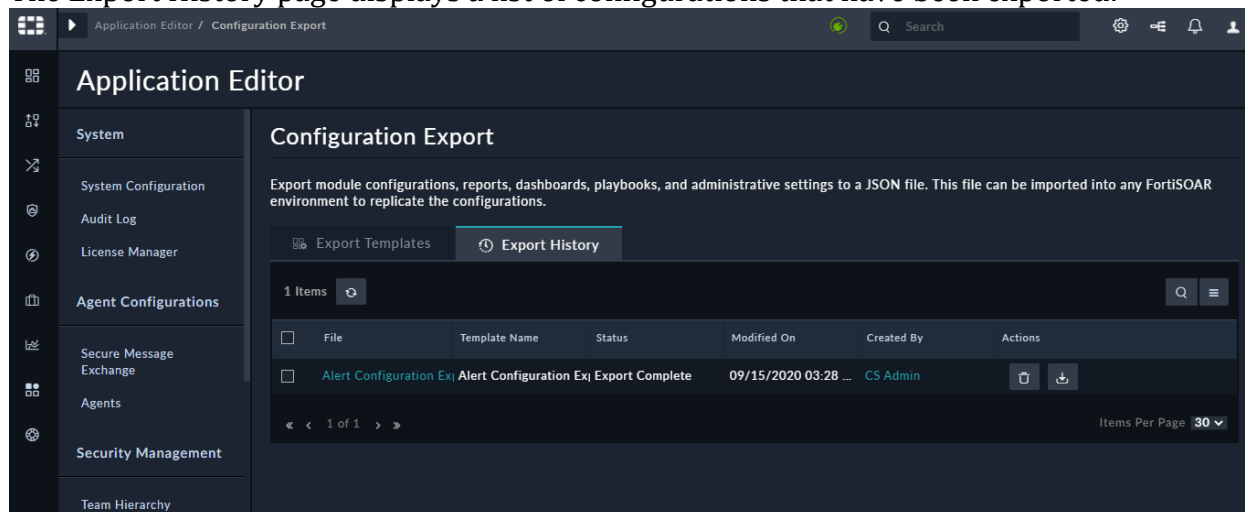
2. To begin a new export for configurations and create an export template, click the **Export Templates** tab, and then click **New Export Template**. This displays the **Choose Entities** page in the Export Wizard, in which you can choose all or any of the entities such as module configurations, playbooks, dashboards, etc. that you want to export.

To run an existing configuration again, click the **Run** icon in the **Actions** column, which displays the "Run Export" screen of the Export Wizard using which you can rerun an existing configuration.

To edit an existing configuration, click the **Edit** icon in the **Actions** column, which displays the "Choose Entities" screen of the Export Wizard using which you can edit the configurations you want to export as per your requirements. To delete an existing configuration template, click the **Delete** icon in the **Actions** column.

If you want to use a playbook to schedule exporting configurations using an existing export template, you will require to add the UUID of the export template in the playbook. You can get the UUID of the export template by click the **Copy UUID to Clipboard** icon in the **Actions** column.

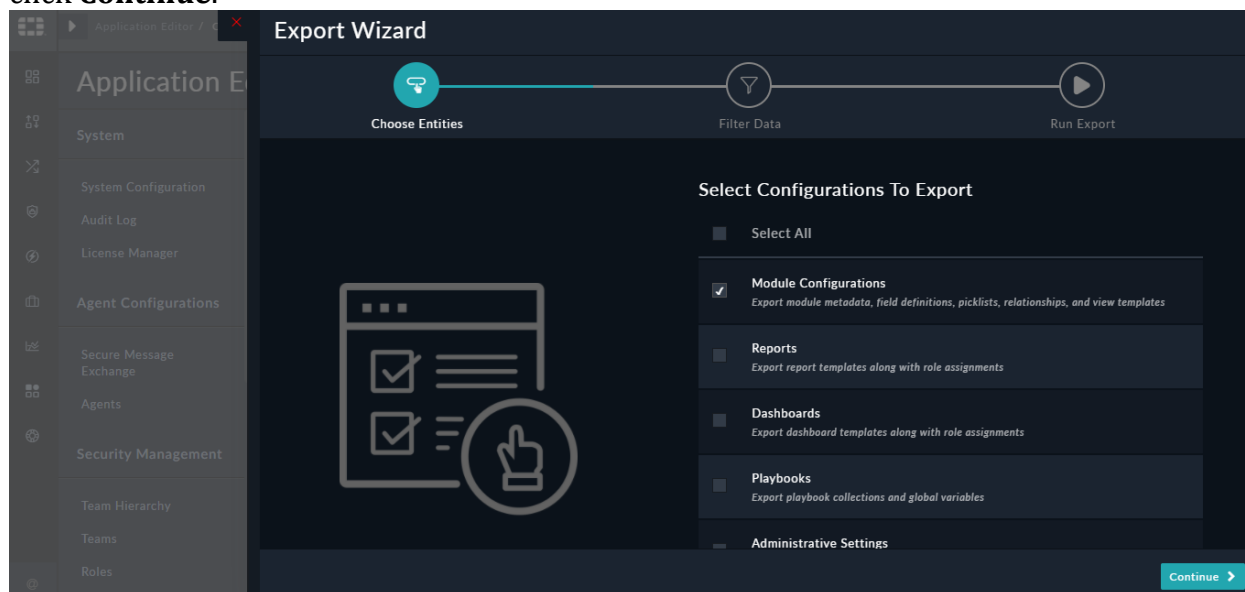
The Export History page displays a list of configurations that have been exported:



To download a configuration file in the JSON format, click the **Download** icon in the **Actions** column, and to delete a configuration file, click the **Delete** icon in the **Actions** column.

## Exporting Modules and/or picklists

1. On the **Choose Entities** page, in Export Wizard, select **Module Configurations** and click **Continue**.



**Note:** You can choose to export one, all, or multiple entities.

2. On the **Filter Data** page, click the Modules option, and select the modules that you want to export. You can choose to export one, all, or multiple modules. You can also choose to export all or any of the configuration information associated with a module, i.e., the module's schema, listing view, record view, and add views. The **Listing View**,

**Record View**, and **Add View** exports the configuration information of the templates that you have created for the selected module(s). To include all the selected entities, click the **Include Everything** checkbox. In this case it exports all the modules and all its associated configuration information including the module's schema, views, and all the picklists.

Click the **Modules** menu item, and in the **Choose Modules and Views to Export** table choose the modules and their related configurations you want to export. The **Auto-Select Required Picklists** checkbox is selected by default, since the picklists associated with the module must also be exported when you are exporting the configuration information for the modules to ensure there are no issues when you import the configuration to another environment. Therefore, for example, if you select **Schema** for the "Alerts" module, you will observe that "3" picklists that are required for the "Alerts" module are automatically selected.

Click the checkboxes in the header row to perform bulk actions. For example, clicking the **Export All** checkbox, selects all the modules their associated configurations. Similarly, clicking the **Schemas** checkbox in the header row, changes **Export to Yes** for all modules and selects the schema for all the modules.

To enable configuration export for a particular module, in that modules row, toggle the **Export** button to **Yes**, which selects all the configuration information associated with a module, i.e., the module's schema, listing view, record view, and add views. If you do not want to export some configuration information, for example add view, toggle the **Add View** button to disable exporting the add view configuration.

**Export Wizard**

Choose Entities | Filter Data | Run Export

☐ Include Everything

**Choose Modules And Views To Export** ☒ Auto-Select Required Picklists ⓘ

Modules (1/23)	Export All	Schema	List View	Detail View	Add View
Agents	<input type="button" value="Export"/> No	<input type="button" value="Schema"/>	<input type="button" value="List View"/>	<input type="button" value="Detail View"/>	<input type="button" value="Add View"/>
Alerts	<input type="button" value="Export"/> Yes	<input type="button" value="Schema"/>	<input type="button" value="List View"/>	<input type="button" value="Detail View"/>	<input type="button" value="Add View"/>
Appliances	<input type="button" value="Export"/> No	<input type="button" value="Schema"/>	<input type="button" value="List View"/>	<input type="button" value="Detail View"/>	<input type="button" value="Add View"/>
Approvals	<input type="button" value="Export"/> No	<input type="button" value="Schema"/>	<input type="button" value="List View"/>	<input type="button" value="Detail View"/>	<input type="button" value="Add View"/>
Assets	<input type="button" value="Export"/> No	<input type="button" value="Schema"/>	<input type="button" value="List View"/>	<input type="button" value="Detail View"/>	<input type="button" value="Add View"/>
Attachments	<input type="button" value="Export"/> No	<input type="button" value="Schema"/>	<input type="button" value="List View"/>	<input type="button" value="Detail View"/>	<input type="button" value="Add View"/>
Comment	<input type="button" value="Export"/> No	<input type="button" value="Schema"/>	<input type="button" value="List View"/>	<input type="button" value="Detail View"/>	<input type="button" value="Add View"/>

If you want to export only picklists, click the **Picklists** menu item, and select the picklists you want to export. Using this menu item, you can export those picklists that are not associated with any module.

**Note:** When you import a picklist, by clicking **Configuration Import** and if that picklist already exists on your system, then the "Import Wizard" replaces the existing picklist.

Once you have complete choosing the modules and picklists that you want to export, click **Continue**.

3. On the **Review Export** page, you can review the configuration information that you are exporting, and can also specify the name of the template that you are exporting as well as the name of the JSON file that you want export. If you change the template name, the file name automatically gets updated as per the template name specified. Once you have completed reviewing the information, click **Save & Run Export** to export the specified configuration information in a JSON file that you can download and use in another environment, or click **Save** to save the configuration information. FortiSOAR™ also displays warnings if there are any inconsistencies in the data, such as templates not found, to be exported. If you have clicked **Save & Run Export**, then the record of export configuration that has been run is added as an entry in both the **Export Templates** and **Export History** pages. If you have clicked **Save**, then FortiSOAR™ saves the specified configuration information as a record entry only in the **Export Templates** page. You can edit this configuration at any time by clicking the **Edit** icon in the **Actions** column, which again displays the Export Wizard in which you can edit the configurations you want to export as per your requirements.

## Exporting Playbooks and/or Global Variables

You can export playbook collections and global variables. Currently, you have to export the complete playbook collection, and cannot select specific playbooks to be exported from within a playbook collection.

1. On the **Choose Entities** page, in Export Wizard, select **Playbooks** and click **Continue**.
2. On the **Filter Data** page, select the playbook collections and/or global variables that you want to export.  
In the **Choose Playbook Collections and Global Variables To Export** page, in the **Playbook Collections** section, click the **Playbook Name** checkbox to select or deselect all the playbook collections. To export specific playbook collections, select those playbook collections. To include versions of your playbooks while exporting playbook collections, click the **Include Versions** checkbox.  
Similarly, in the **Global Variables** section, click the **Global Variable Name** checkbox to select or deselect all the global variables. To export specific global variables, select those global variables.  
To include all the selected entities, click the **Include Everything** checkbox. In this case it exports all the playbook collections and global variables.  
To include all the selected entities, click the **Include Everything** checkbox. In this case it exports all the playbook collections and global variables.  
Once you have complete choosing the playbook collections and/or global variables that you want to export, click **Continue**.

3. On the **Review Export** page, you can review the playbook collections/global variables that you are exporting, and can also specify the name of the template that you are exporting as well as the name of the JSON file that you want export. If you change the template name, the file name automatically gets updated as per the template name specified.

Once you have completed reviewing the information, click **Save & Run Export** to export the playbook collections/global variables in a JSON file that you can download and use in another environment or click **Save** to save the playbook collections/global variables. If you have clicked **Save & Run Export**, then the record of export configuration that has been run is added as an entry in both the **Export Templates** and **Export History** pages. If you have clicked **Save**, then FortiSOAR™ saves the playbook collections/global variables configuration as a record entry only in the **Export Templates** page. You can edit this configuration at any time by clicking the **Edit** icon in the **Actions** column, which again displays the Export Wizard using which you can edit the configurations you want to export as per your requirements.

**Note:** When you import a playbook collection, by clicking **Configuration Import**, and if that playbook collection exists, you can choose to either overwrite the existing playbook collection or create a new playbook collection and appending the original playbook collection name with a number. For more information, see [Importing configurations](#).

When you import a global variable, by clicking **Configuration Import** and if that global variable already exists on your system, then the "Import Wizard" replaces the existing global variable.

## Exporting Dashboards and/or Reports

1. On the **Choose Entities** page, in Export Wizard, select **Dashboards** and/or **Reports** and click **Continue**.

2. On the **Filter Data** page, select the dashboards and/or reports that you want to export.

Click the **Dashboards** menu item, and in the **Choose Dashboards To Export** table, click the **Dashboard Name** checkbox to select or deselect all the dashboards. To export specific dashboards, select those dashboards.

Similarly, click the **Reports** menu item, and in the **Choose Reports To Export** table, click the **Report Name** checkbox to select or deselect all the reports. To export specific reports, select those reports.

To include all the selected entities, click the **Include Everything** checkbox. In this case it exports all the dashboards and reports.

Once you have complete choosing the dashboards and/or reports that you want to export, click **Continue**.

3. On the **Review Export** page, you can review the dashboards/reports that you are exporting, and can also specify the name of the template that you are exporting as well as the name of the JSON file that you want export. If you change the template name, the file name automatically gets updated as per the template name specified.

Once you have completed reviewing the information, click **Save & Run Export** to



export the dashboard/report in a JSON file that you can download and use in another environment or click **Save** to save the dashboards/reports. If you have clicked **Save & Run Export**, then the record of export configuration that has been run is added as an entry in both the **Export Templates** and **Export History** pages. If you have clicked **Save**, then FortiSOAR™ saves the dashboard/report template as a record entry only in the **Export Templates** page. You can edit this configuration at any time by clicking the **Edit** icon in the **Actions** column, which again displays the Export Wizard using which you can edit the configurations you want to export as per your requirements.

**Note:** When you import a dashboard or report, by clicking **Configuration Import** and if that dashboard or report already exists on your system, then the "Import Wizard" replaces the existing dashboard or report.

## Exporting Roles and Administrative Settings

You can export roles, and settings and customizations that you have applied across your FortiSOAR™ instance. For example, you can export your system settings such as branding and notifications, SSO and LDAP configurations, High Availability configurations, proxy and environment variables, etc.

**Important:** Passwords are write-only fields and therefore they cannot be exported using Configuration Manager. Therefore, if for example, you have exported your LDAP configurations and imported that into another FortiSOAR™ system, then since the passwords are not copied, you have to manually enter the passwords for all the users to be able to perform any activity related to users, such as searching for users or updating details of users.

1. On the **Choose Entities** page, in Export Wizard, select **Settings** and click **Continue**.
2. On the **Filter Data** page, select the roles and/or settings that you want to export. Click the **Roles** menu item, and in the **Choose Roles To Export** table, click the **Role Name** checkbox to select or deselect all the roles. To export specific roles, select those roles. To export specific roles, select those roles. You can export roles such as **Full App Permissions, Application Administrator, T1 Analyst, Security Administrator**, etc. Click the **Settings** menu item, and in the **Choose Administrative Settings To Export** table, in the **Administrative Settings** section click the **Settings Name** checkbox to select or deselect all the administrative settings. To export specific administrative settings, select those administrative settings. Similarly, in the **System Views** section, click the **Settings Name** checkbox to select or deselect all the system views. To export specific system views, select those system views. To include all the selected entities, click the **Include Everything** checkbox. In this case it exports all the roles and system views. Once you have complete choosing the settings and roles that you want to export, click **Continue**.
3. On the **Review Export** page, you can review the settings/roles that you are exporting, and can also specify the name of the template that you are exporting as well as the name of the JSON file that you want export. If you change the template name, the file name automatically gets updated as per the template name specified.



Once you have completed reviewing the information, click **Save & Run Export** to export the settings/roles in a JSON file that you can download and use in another environment or click **Save** to save the settings/roles. If you have clicked **Save & Run Export**, then the record of export configuration that has been run is added as an entry in both the **Export Templates** and **Export History** pages. If you have clicked **Save**, then FortiSOAR™ saves the settings/roles template as a record entry only in the **Export Templates** page. You can edit this configuration at any time by clicking the **Edit** icon in the **Actions** column, which again displays the Export Wizard using which you can edit the configurations you want to export as per your requirements. When you import the exported configurations into a system, all the application settings that were applied on the system from which the application settings were exported get applied on the system where you import and install the settings. For example, if the system from which the application settings were exported had its "Audit Log Purge" enabled with the logs to be retained for the last month, the same Audit Log policy will apply on the system in which you import and install the application settings.

**Important:** If you have exported your SSO configuration and imported the SSO (SAML) configurations into a different FortiSOAR™ system, you require to make certain updates before SAML users can log into FortiSOAR™. For more information, see [Updates required to be done after importing SSO configurations](#).

**Note:** When you import a role, system view, or setting by clicking **Configuration Import**, and if that role, system view, or setting already exists on your system, the Import Wizard will overwrite the existing role, system view, or setting.

## Configuration Import Wizard

You can use the import wizard to import configurations or metadata information for modules, playbook collections, dashboards, etc. from other environments into FortiSOAR™. Using the import wizard, you can move model metadata, picklists, system view templates, dashboards, reports, roles, playbooks, and application settings across environments.

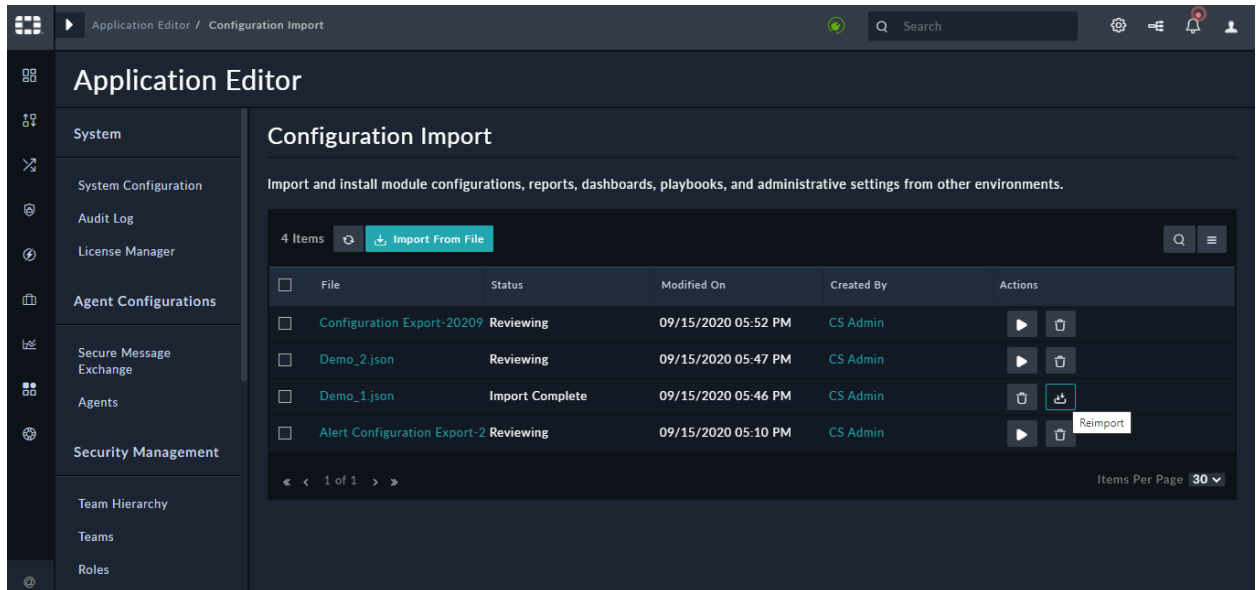
**Important:** It is advisable not to import MMDs between major releases of FortiSOAR™.

### Importing configurations

The following section provides an example of importing module configurations. You can import dashboard, system views, playbooks, etc., using the same method.

**Note:** To import configurations into FortiSOAR™ the configurations file must be in the JSON format. FortiSOAR™ ensures that you either revert or publish staged changes prior to importing configurations so that there are no issues during the import process.

1. Click **Settings** and in the **Application Editor** section, click **Configuration Import**. This displays the **Configuration Import** page.

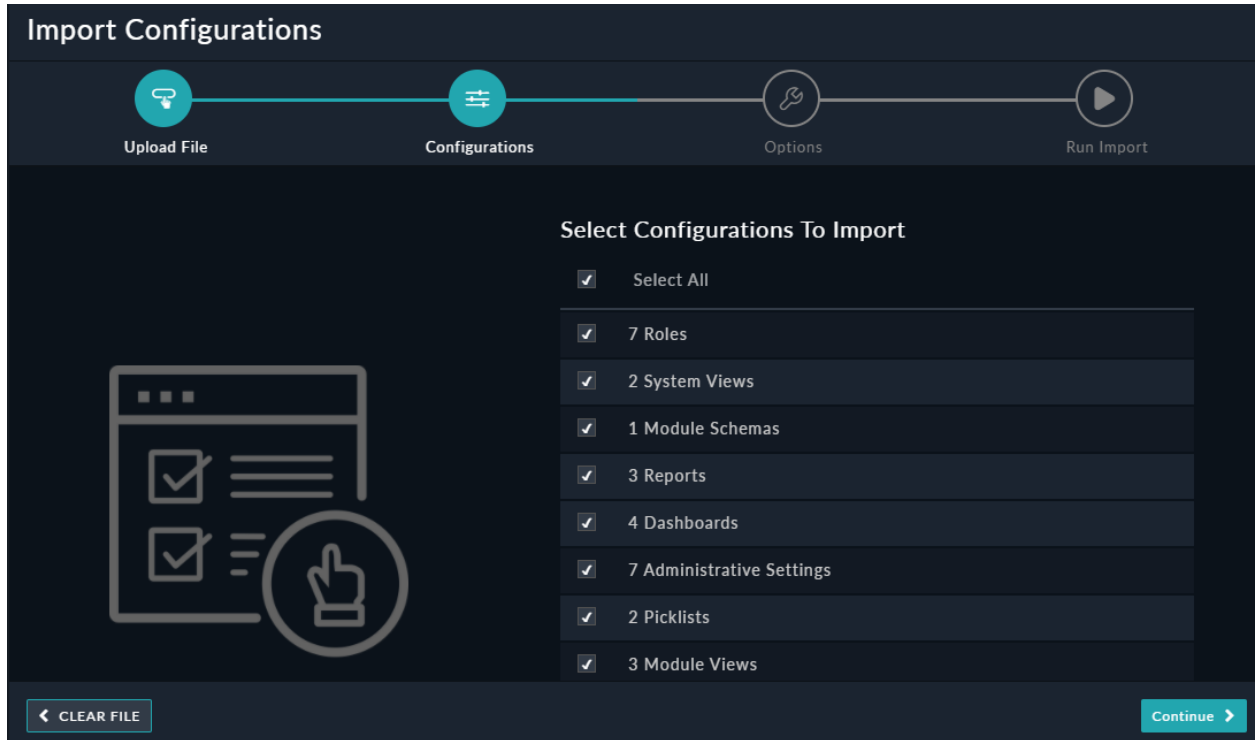


If you close the wizard without clicking **Run Import**, then the status of your import will display as "Reviewing", and you can click the **Continue** icon in the **Actions** column to display the "Configurations" screen of the Import Wizard, and you can continue review of the import configurations. If you have clicked **Run Import**, and the import process is completed, then the status of your import will display as "Import Complete". You can also the configuration at any time by clicking the **Reimport** icon in the **Actions** column to display the "Configurations" screen of the Import Wizard.

## 2. Click **Import From File**.

This displays the **Upload File** page in Import Wizard. On this page, drag and drop the JSON file, or click the **Download** icon and browse to the JSON file to import configurations into FortiSOAR™. If the JSON format is incorrect, FortiSOAR™ displays an error message and not import the file. If the JSON format is correct, FortiSOAR™ imports the configurations and displays details of what is being imported on the **Configurations** page.

- On the **Configurations** page, choose the configurations that you want to import, and click **Continue**.



- Importing Configurations:**

#### **Importing Dashboards, Reports, Picklists, Roles and Settings:**

To import Dashboards, on the **Options** page, click the **Dashboards** menu item, and the "Observation" column displays whether the dashboards that you are importing are "New" or "Existing". Click the **Dashboard Name** checkbox to select or deselect all the dashboards, or click the checkbox alongside the individual Dashboard name to import particular dashboards.

If you are importing Dashboards and or Reports, then apart from displaying whether it is an existing or new dashboard or report, you can assign a default role to the dashboard or report:

## Import Configurations

Upload File

Configurations

Options

Run Import

1 Module(s)	Choose Dashboards To Import		Choose a default role if no role is assigned
5 Picklist(s)	<input checked="" type="checkbox"/> Dashboard Name		Observation
7 Dashboard(s)	<input checked="" type="checkbox"/> Executive View	Assigned Roles: Security Administrator, Full App Permissions, FortiSOAR Agent, T1 Analyst, Playbook Administrator, T2 Analyst, Application Administrator	New dashboard
4 Report(s)	<input checked="" type="checkbox"/> ROI Summary	Assigned Roles: Security Administrator, Full App Permissions, Playbook Administrator, Application Administrator	Existing dashboard
7 Role(s)	<input checked="" type="checkbox"/> SOC Admin	Assigned Roles: Security Administrator, Full App Permissions, Playbook Administrator, Application Administrator	Existing dashboard
5 Playbooks Collection(s)	<input checked="" type="checkbox"/> System Dashboard	Assigned Roles: Security Administrator (default)	Existing dashboard
9 Settings(s)	<input checked="" type="checkbox"/> System Health Status	Assigned Roles: Security Administrator	Existing dashboard

BACK

Continue

The **Options** page for Picklists, Reports, Roles, Settings are similar, except that the Settings page does not have the "Observation" column, and the role assignment drop-down list is present only for the Dashboards and Reports page. Use the <Name of the Option> Name checkbox to select or deselect all the configurations of a particular type on their respective pages. For example, if you want to import all the administrative settings and system views, click the **Settings** menu item, and then in the **Administrative Settings** section, click the **Settings** checkbox to select or deselect all the administrative settings, and in the **System Views** section, click the **View Name** checkbox to select or deselect all the system views.

**Important:** If picklists, dashboards, reports, global variables, roles, system views, or administrative settings that you are importing already exist in your system, then the Import Wizard overwrites the configurations of these entities in your system.

### Importing Playbook Collections and Global Variables:

To import playbook collections, on the Options page, click the **Playbook Collections** menu item. Currently, you have to import the complete playbook collection, and cannot select specific playbooks to be imported from within a playbook collection. The playbook collections and global variables page displays the list of "New Playbook Collections", "Existing Playbook Collections", "New Global Variables" and "Existing Global Variables". In case of new playbook collections and global variables, click the **Import All** checkbox in their respective sections to select or deselect all the new playbook collections and global variables. To import particular playbook collections or global variables, click the checkbox alongside the individual playbook collections or global variables.

In case of existing playbook collections, apart from the **Import All** checkbox in the header, the Import Wizard also displays the following the "Bulk Actions" that you can

take for the playbook collections: **Overwrite Existing**, which is the default option, or **Rename (append number)**. You can choose to apply this action across all the playbook collections you are importing or you can choose the action to be performed for each playbook collection that you are importing. If you retain the **Overwrite Existing** action, then the Import Wizard overwrites the playbook collections in your system. If you select **Rename (append number)**, then the Import Wizard creates a new playbook collection and appends the original playbook collection name with a number. For example, if you have exported a playbook collection named "Demo" and you are importing the same playbook collection with **Rename (append number)** selected, then the imported collection will automatically be created as a new playbook collection named as "Demo (1)".

**Import Configurations**

Upload File | Configurations | Options | Run Import

Item	Name	Import	Action
1 Module(s)	Choose Playbooks and Global Variables to Import		
5 Picklist(s)		<input type="checkbox"/> Import All	
7 Dashboard(s)			
4 Report(s)	Demo	Import Yes	
7 Role(s)	Sample - BPMN - 1.0.2	Import No	
4 Playbooks Collection(s)	<b>Existing Playbook Collections (3)</b>		
9 Settings(s)		<input checked="" type="checkbox"/> Import All	Overwrite Existing
	Sample - Code Snippet - 1.2.4	Import Yes	Overwrite Existing
	Sample - IMAP - 3.5.4	Import Yes	Overwrite Existing
	Sample - System Monitoring - 1.3.0	Import Yes	Overwrite Existing

BACK Continue

## Importing Modules:

When you import existing modules, and if the modules that you are importing contain fields that conflicts with the existing fields that prevent some fields from being imported, then those modules are displayed in Existing Modules With Conflicts section as shown in the following image:.

## Import Configurations

Upload File

Configurations

Options

Run Import

1 Module(s)

Choose Modules and Views to Import

Existing Modules With Conflicts (1)

These modules match existing modules, and contain field conflicts that prevent some fields from importing. Please review conflicts before importing.

Modules

☒ Import All
☒ Schema

Merge With Existing

☒ List View
☒ Detail View
☒ Add View

Demo

Import

Yes

Schema

Merge With Existing

List View

Detail View

Add View

Action Preset: Merge

Sort: Default

Overwrite existing fields, add new fields, and keep non-imported fields

Name	Type	Observation	Actions
Name name	Lookup (One to Many or One to One)	Matching Field Found	<div>Keep old version</div> <div>Cannot change type from string to alerts.</div>

BACK

Continue

Modules whose fields have no conflicts with existing fields are displayed in the Existing Modules Without Conflicts section as shown in the following image:

## Import Configurations

Upload File

Configurations

Options

Run Import

3 Module(s)

22 Picklist(s)

Choose Modules and Views to Import

Existing Modules Without Conflicts (3)

These modules match existing modules, but no conflicts have been detected. Expand to review.

Modules

☐ Import All
☐ Schema

Merge With Existing

☐ List View
☐ Detail View
☐ Add View

Alerts

Import

Yes

Schema

Merge With Existing

List View

Detail View

Add View

Assets

Import

No

Schema

Merge With Existing

Replace Existing

List View

Detail View

Add View

Comment

Import

No

Schema

List View

Detail View

Add View

Incidents

Import

Yes

Schema

List View

Detail View

Add View

Indicators

Import

Yes

Schema

List View

Detail View

Add View

BACK

Continue

Choose the options in the header row to perform bulk actions. For example, if you

want to import all the modules, click the **Import All** checkbox, etc.

For schemas of the modules that you are importing, you can choose if you want to **Merge With Existing** or **Replace Existing** configurations. You can click the **Review Field Level Actions** icon to view the detailed schema of the module you are importing. **Merge**, merges then the configurations, i.e., for example if you are importing an existing module, say Alerts, which has 3 new fields in the configuration that you are importing and 10 existing fields and you choose **Merge**, then post-import the Alerts modules will have 13 fields.

**Replace**, replaces the existing configuration with the imported configuration.

**Review Field Level Actions**, provides you with the module schema details and includes information about fields such as which fields are replaced and which fields are retained, and which fields are going to be created. Users can also decide what they want to do with fields that are different in the existing modules and in the configuration that you want to import by selecting options such as **Keep old version**, or **Delete field**, or **Replace with new version**, etc., which are present in the **Actions** column.

You can choose to sort how the fields are displayed in the grid by clicking the **Sort** drop-down list. The Sort drop-down list has the **Default**, **A-Z**, or **Z-A** options.

Module(s)	Field Name	Field Type	Matching Field Found	Actions	Status
4 Module(s)	Resolved Date resolveddate	Date/Time Field	Matching Field Found	Keep old version	Keep Existing
22 Picklist(s)	Closure Notes closureNotes	Rich Text (Markdown)	New Field Found	Create field	Create
	Closure Reason closureReason	Picklist	Matching Field Found	Ignore field	Overwrite
	Notes notes1	Text Field	No Match Found	Keep field	No change
	escalationReason		Found	Delete field	
	Source Type sourceType	Text Field	Matching Field Found	Keep old version	Keep Existing
	MITRE ATT&CK ID mitreattackid	Text Field	Matching Field Found	Replace with new version	Keep Existing
	ATT&CK Techniques mitrelink	Many to Many	Matching Field Found	Keep old version	Keep Existing

Observations displayed for various fields:

- **New Field Found:** Fields that are present only in the configuration that you want to import, i.e., fields that are newly added to the configuration. Available user actions are **Create field** or **Ignore field**.

**Note:** If you select **Ignore field** then the newly added field is not included in the mmd when you import the configuration.

- **No Match Found:** Fields that are present only in the existing module and not in the configuration that you want to import, i.e., fields that are deleted from the configuration. Available user actions are **Keep field** or **Delete field**.  
**Note:** Delete field will delete the field from the mmd file.
- **Matching Field Found:** Fields that are present in both the configuration that you want to import and in the existing module, but which have *different properties* in the configuration that you want to import and in the existing module. These are fields that a user should replace with the newer version of the field. However, ensure that you review all the fields before choosing the import option since replacing a field with its newer version should not result in the publish failing due to for example, conversion of the field to an Unsupported type. Available user actions are **Replace with new version** or **Keep old version**.
- **System Field:** Fields whose properties cannot be changed by users. An example of a system field would be the **First Name** field in the **People** module, which cannot be changed by users. For more information on system fields, see [Module Editor](#).  
**Note:** The name and properties of the Lookup (One to Many or One to One), Many to Many, and Many to One fields must not be changed once they have been defined. For example, the Alerts module contains a Many to Many with the **Indicators** field, and if in the configuration that you are importing the name of this field is changed to Indicator1 then the new field Indicator1 will not be imported.

Once you have completed reviewing the import options, click **Continue**.

5. On the **Review Import** page, you can review the details of the import. Once you have reviewed the import details displayed by the Import Wizard, click **Run Import** to begin the import process or you can close the wizard. Clicking **Run Import** displays a configuration dialog, where you can click, **I have reviewed the changes - Publish** to import and publish the configuration into your FortiSOAR™ environment. Once the configuration publish begins, FortiSOAR™ displays the list of configurations being imported along with progress of the import. For example, **Publishing Modules (36%)**, etc and displays a message **Import Process Completed Successfully**. If there are any issues with the configuration that you are trying to import then "Publish" operation fails and the wizard displays a message containing information about which configuration has failed such as **Error while Importing Picklists**, and also the details of the error that caused the failure.

## Points to be considered while importing module configurations

- If you have edited a picklist on an environment (Env)1 and you import the Env1 configuration into Env2, in this case, the edited picklist items will be replaced.
- If you have added a field, say **test1**, to Env1 and added a field, say **test2**, to Env2, to the **Alerts** module in both environments. Now, if you export the **Alerts** module from Env1 and import the **Alerts** module to Env2, then the **Alerts** module in Env2 gets completely overridden, i.e., the **Alerts** module in Env2 will now only contain the **test1** field, and the **test2** field gets overridden.



You can also select the **Merge** check box to retain fields that were present in an existing module but which are not present in the exported (new) module.

## Updates required to be done after importing SSO configurations

If you have exported your SSO configuration and imported the SSO (SAML) configurations into a different FortiSOAR™ system, you require to make the following updates to the service provider portal, before SAML users can log into FortiSOAR™:

1. Update the "Single Sign On URL" to the URL of the system that is importing the SSO configuration.
2. Update any other field in the service provider's portal that mentions the FortiSOAR™ system URL.
3. Generate the X509 certificate for the FortiSOAR™ system that is importing the SSO configuration.

Once you have generated the X509 certificate, you must update the newly generated X509 certificate details on the **SSO Configuration** page in the FortiSOAR™ system that is importing the SSO configuration. To open the **SSO Configuration** page, click **Settings > Authentication > SSO Configuration**. In the **Identity Provider Configuration** section, in the **X509 Certificate** field update the details of the newly generated X509 certificate.

# SLA Management

## Overview

FortiSOAR™ provides you with a SLA Templates module using which you can create in-built SLA management for incidents and alerts.

You can define SLAs for incidents and alerts at varying degrees of severity and track whether those SLAs are met or missed.

**Important:** To use the SLA feature, you must Install the FSR-IR-CONTENT-PACK on a fresh installation of FortiSOAR™. You must deploy your FortiSOAR™ license before installing the FSR-IR-CONTENT-PACK. Also, NEVER install the content pack after you have modified any data or have any existing data. If you proceed with installing the FSR-IR-CONTENT-PACK after you have modified or added data, then the customizations or data might be lost.

The FSR-IR-CONTENT-PACK contains the "Case Management" playbooks collection that automatically tracks the SLAs of the case management workflows and other OOB playbooks that demonstrate various use cases. For more information on the FSR-IR-CONTENT-PACK, see the [FSR-IR-CONTENT-PACK](#) article present in the Fortinet Knowledge Base. You can also use the SLA Calculator connector and playbooks associated with the same to calculate when the SLAs are due based on the locale and work hours that you have specified. For more information on the SLA calculator, see the SLA calculator documentation on the [FortiSOAR™ Connectors](#) page.

**Note:** To view automatic tracking of SLAs on your incident or alert records, you do not need to modify the "Case Management" playbooks collection. However, you require to schedule some playbooks in this collection. For more information, see the [Scheduling SLAs](#) article present in the Fortinet Knowledge Base.

## Permissions required for managing SLAs

To create and manage SLAs, you must be assigned a role with a minimum of **Create**, **Read**, and **Update** permission on the **SLA Templates** module and **Playbooks** modules along with the default **Read** permission on the **Application** module.

## Creating SLA Templates

You can create SLA templates for each level of severity of incidents or alerts. You can set SLAs for both alerts and incidents using the same SLA Template.

For example, you can create 5 SLAs for incidents at severity levels: Critical, High, Medium, Low, and Minimal.

1. Click **Automation > SLA Templates** in the left navigation bar.
2. To add a new SLA Template, click **Add**.
3. In the **Create New SLA Template** dialog, enter the following details:
  - a. From the **Severity** drop-down list, select the severity level of the incident for which you are defining the SLAs.  
For example, if you select severity as "Critical", and you specify the acknowledgement time as 10 minutes and response time as 15 minutes, this means that to meet the SLA, users must acknowledge incidents within 10 minutes and respond to the incident within 15 minutes of the incident getting created.  
**Note:** You can update the default **Severity** picklist and then choose any severity (including custom) parameter.
  - b. (Optional) To make it easier to search and filter SLA templates, in the **Add Tags** field, you can enter appropriate tags.
  - c. From the **Incident Ack SLA Tracked On** drop-down list, select the status in which the incident will be marked as acknowledged. For example, select **In Progress**.  
**Note:** You can update the default **Status** picklist and then choose any status (including custom) parameter.
  - d. From the **Incident Response SLA Tracked On** drop-down list, select the status in which the incident will be marked as responded. For example, select **Resolved**.
  - e. In the **Incident Ack Time** field, add the number of minutes within which users must acknowledge an incident.
  - f. In the **Incident Response Time** field, add the number of minutes within which users must respond to an incident.  
You can similarly set SLAs for alerts.

- Click **Save** to save the SLA Template.

The screenshot shows the 'SLA Templates' section in the FortiSOAR interface. The main heading is 'Create New SLA Template'. Below this, there are several fields and sections:

- Severity:** A dropdown menu set to 'Critical'.
- Tags:** A field with a plus icon and the text '+ Add Tags'.
- Incident SLA:**
  - Incident Ack SLA Tracked On:** A dropdown menu set to 'In Progress'.
  - Incident Response SLA Tracked On:** A dropdown menu set to 'Resolved'.
  - Incident Ack Time:** A text input field with the value '0'.
  - Incident Response Time:** A text input field with the value '0'.
- Alert SLA:**
  - Alert Ack Tracked On:** A dropdown menu set to 'Select'.
  - Alert Response Tracked On:** A dropdown menu set to 'Select'.
  - Alert Ack Time:** A text input field.
  - Alert Response Time:** A text input field.

At the bottom of the form, there are two buttons: 'Save' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

## Viewing SLAs

You can view fields related to SLAs in the detail view of your alert or incident record, where you will see fields such as Ack Due Date, Ack Date, Ack SLA, Response Due Date, etc. using which you can track whether or not the SLAs have been met.

To automate the management of SLA workflows, you require to do the following:

1. Install the FSR-IR-CONTENT-PACK. This would import the "Case Management" playbooks collection into your FortiSOAR™ instance. For more information on the FSR-IR-CONTENT-PACK, see the [FSR-IR-CONTENT-PACK](#) article present in the Fortinet Knowledge Base.
2. Schedule the SLAs. For more information, see the [Scheduling SLAs](#) article present in the Fortinet Knowledge Base.

**Important:** Records must be in the "Open" state along with a proper severity set for the acknowledgement and response SLAs to be calculated.

Once you have installed the FSR-IR-CONTENT-PACK and scheduled the SLAs, whether the SLAs have been met or missed in the incident and alert records as shown in the following image:

The screenshot displays the Fortinet FortiSIEM interface for an alert titled "Alert-60 | Outbound File Transfer". The alert is categorized as "Medium" and was last modified on 04/19/2020 at 10:25 PM by a user named "Playbook". The interface includes tabs for "Alert Details", "Playbooks", and "Audit Logs".

**Description:**  
 sentBytes:64:12408696,  
 destipAddr:172.16.1.10,

**Assigned To:** Abhishek Narula  
**Status:** Investigating  
**Source:** FortiSIEM  
**Source ID:** 445  
**Detection Date:** 04/18/2020 01:44 AM  
**Assigned Date:** 04/18/2020 01:45 AM  
**Escalated:** No  
**Resolved Date:** [Select Date](#)

**Type Details:**  
**Type:** Data Exfiltration  
**Source IP:** --  
**Computer Name:** --  
**Destination IP:** 10.0.1.1  
**Target Asset:** --

**SLA Details:**

Ack Due Date	04/18/2020 02:24 AM
Ack Date	04/19/2020 10:25 PM
Ack SLA	Missed
Response Due Date	04/18/2020 02:34 AM
Response Date	-NA-
Response SLA	Met

At the bottom of the interface, there are tabs for "Indicators", "Correlations", "Tasks", "Source Data", and "Access Control".

**Figure 71.** Sample alert record with SLAs set

## FortiSOAR™ Admin CLI

### Overview

An administrator can use FortiSOAR™ Admin CLI (`csadm`) to perform various functions such as backing up and restoring data and run various FortiSOAR™ commands such as starting and stopping services and collecting logs.

### Prerequisites

To run `csadm` you must login as `root` or have `sudo` permissions.

### FortiSOAR™ Admin CLI - Usage

Once you type `# csadm` on the command prompt, the usage and subcommands of the FortiSOAR™ Admin CLI are displayed as shown in the following image:

```
[root@fortisoar csadmin]# csadm
usage: csadm [<subcommand> <options>]      Run subcommand
        [<subcommand> --help]              Show detailed help of subcommand
        [--help]                            Show this message

csadm subcommands are:
  ha          - Manage HA cluster
  certs       - Generate and deploy certificates
  db          - Manage database
  hostname    - Change hostname
  license     - Manage license
  log         - Collect logs
  mq          - Manage message queue
  network     - Manage network
  services    - Manage services
[root@fortisoar csadmin]#
```

**Figure 72.** FortiSOAR™ Admin CLI command prompt

To perform a particular task in FortiSOAR™ using `csadm`, you must type `# csadm` and then its subcommand and the subcommand's arguments (if any). For example, to change a hostname use the following command: `# csadm hostname --set [<hostname to be set>]`

You can get help for a particular subcommand by running following command:

```
# csadm <subcommand>
```

OR

```
# csadm <subcommand> --help
```

`csadm` supports the following subcommands:

## Subcommand Description

certs	<p>Generates and deploys your certificates. You can use the following options with this subcommand:</p> <ul style="list-style-type: none"> <li><code>--deploy</code>: Deploys SSL certificates. For more information, see the <i>Updating the SSL certificates</i> section in the <i>Additional configuration settings for FortiSOAR™</i> chapter in the “Deployment Guide.”</li> <li><code>--generate &lt;host name&gt;</code>: Generates and deploys self-signed certificates. You can use the <code>--no-replace-nginx-cert</code> option with this command, if you do not want to replace your nginx self-signed certificates.</li> </ul>
db	<p>Performs operations related to database. You can use the following options with this subcommand:</p> <ul style="list-style-type: none"> <li><code>--change-passwd</code>: Changes the password of your PostgreSQL database. Once you run this command, you will be prompted to enter the password of your choice and confirm the password, which will then update your PostgreSQL database password to the new password.</li> <li><code>--backup [&lt;BACKUP_DIR_PATH&gt;]</code>: Performs an encrypted backup of your FortiSOAR™ system, including backup of both data and configuration files. From version 6.4.3 onwards, you can optionally use the <code>--exclude-workflow</code> option to exclude all the “Executed Playbook Logs” from the backup. For more information, see the <i>Backing up and Restoring FortiSOAR™</i> chapter.</li> <li><code>--backup-config [&lt;BACKUP_DIR_PATH&gt;]</code>: Performs an encrypted backup of only your configuration files.</li> <li><code>--restore</code>: Performs data restore from a locally stored file (<code>/home/csadmin/db_backup/DR_BACKUP_&lt;yyyymmdd_hhmmss&gt;.tar</code>). For more information, see the <i>Backing up and Restoring FortiSOAR™</i> chapter.</li> <li><code>--encrypt</code>: Generates an encrypted version of the text that you have specified on the prompt. Use this command to generate an encrypted version of the password that you have set for your PostgreSQL database.</li> <li><code>--externalize</code>: Performs externalization of your FortiSOAR™ PostgreSQL data. You must provide the path in which you want to save your database backup file. For more information, see the <i>Externalization of your FortiSOAR™ PostgreSQL database</i> chapter.</li> <li><code>--check-connection</code>: Checks the connection between FortiSOAR™ and the external PostgreSQL database.</li> <li><code>--getsize</code>: Displays the size of the primary data and the audit and workflow logs in your database. This enables you to see the current usage and calculate usage over time based on your purging policy.</li> </ul>
ha	<p>Manages your FortiSOAR™ High Availability cluster. For more information about HA and its commands, see the <i>High Availability support in FortiSOAR™</i> chapter.</p>
hostname	<p>Changes the name of the host and Fully Qualified Domain Name (FQDN) based on the parameters you have specified. You can use the following options with this subcommand:</p>

	<p><code>--set [&lt;hostname&gt;]</code>: If you specify a new hostname, then this changes your current hostname to the new hostname that you have specified, sets up the message broker, regenerates certificates, and restarts FortiSOAR™ services.</p> <p>If you do not specify a hostname, then this sets up the message broker, regenerates certificates using the existing hostname, and restarts FortiSOAR™ services.</p> <p><b>Note:</b> Before you run this command, you must ensure that the specified hostname is resolvable.</p> <p><code>--dns-name &lt;DNS_SERVER_IP&gt;</code>: Adds the DNS server entry to the <code>/etc/resolv.conf</code> file.</p>
license	<p>Manages your FortiSOAR™ license. You can use the following options with this subcommand:</p> <p><code>--get-device-uuid</code>: Retrieves the Device UUID for your FortiSOAR™ instance.</p> <p><code>--deploy-enterprise-license &lt;License File Path&gt;</code>: Deploys your FortiSOAR™ enterprise license. For example, <code>csadm license --deploy-enterprise-license temp/&lt;Serial_No&gt;.lic</code>.</p> <p><code>--deploy-multi-tenant-license &lt;License File Path&gt;</code>: Deploys your FortiSOAR™ multitenancy license.</p> <p><code>--show-details</code>: Displays details of the installed license such as, type of license, Device UUID, expiry date of the license, etc. If you add the [License File Path] parameter to this subcommand, for example, <code>--show-details /home/&lt;Serial_No&gt;.lic</code>, then this displays the contents of the license file.</p>
log	<p>Performs log collection and forwarding of syslogs. You can use the following options with this subcommand:</p> <p><code>forward</code>: Forwards FortiSOAR™ logs to your central log management server that supports a Rsyslog client. For the options that you can use with this subcommand see the <a href="#">CLI commands used for forwarding syslogs</a> section. You can also configure syslog forwarding using the FortiSOAR™ UI, details of which are in the <i>System Configuration</i> chapter.</p> <p><code>--collect [&lt;LOG_PATH&gt;]</code>: Collects logs and bundles them up into a <code>fortisoar-logs.tar.gz.gpg</code> file. You must specify the path where the logs should be collected. If you do not specify a path, then the logs will be collected in the current working directory.</p>
mq	<p>FortiSOAR™ message queue controller (RabbitMQ) functions.</p> <p><code>--flush-db</code>: Deletes and recreates the rabbitmq database.</p>
secure-message-exchange	<p>Manages the default secure message exchange server available with a FortiSOAR™ node. A secure message exchange establishes a secure channel that is used to relay information to the agents or tenant nodes.</p> <p><b>Note:</b> For a production setup, it is recommended that you add and configure a separate secure message exchange for handling scale and high availability.</p> <p>You can use the following options with this subcommand:</p>



**enable:** Enables the secure message exchange on your FortiSOAR™ instance if you want to use localhost, i.e., the Default (Embedded) secure message exchange to connect to an external agent or in case of a dedicated tenant.

You must specify the **password**, which is the admin password that is used for setting up a communication channel for every tenant or agent node that will connect to this FortiSOAR™ instance using this local secure message exchange. All the other parameters are optional and if they are not specified, then the default values are set. If you do specify the values for any parameter, then the default values are replaced by the user-specified values.

The following parameters are used with this subcommand:

**--name:** Name that you want to set for the secure message exchange. By default, this is set to **Default (Embedded)**.

**--user:** Admin username that will be used to login to the secure message exchange management console and perform tasks such as configuring tenants and agents on the secure message exchange. Default value is **admin**.

**--password:** Admin password that will be used to login to the secure message exchange management console.

**--vhost:** Virtual host for running admin commands on the secure message exchange. Default value is **cyops-admin**.

**--api-port:** RabbitMQ API port that should be enabled for configuring tenants and agents on the secure message exchange. Default value is **15671**.

**--tcp-port:** RabbitMQ TCP port that should be enabled for data exchange with tenants and agents. Default value is **5671**.

**disable:** Disables the secure message exchange that you had enabled on your FortiSOAR™ instance for using localhost to connect to an external agent.

**show-config:** Displays the configuration details of your secure message exchange, such as the name of the secure message exchange, username used to login to the secure message exchange, the TCP port and API port that is configured for your secure message exchange, etc.

## services

FortiSOAR™ services controller (RabbitMQ) functions. You can use the following options with this subcommand:

**--start:** Starts all FortiSOAR™ services in their respective order.

**--stop:** Stops all FortiSOAR™ services in their respective order.

**--restart:** Restarts all FortiSOAR™ services in their respective order.

**--status:** Displays the status, i.e., Running or Not Running of all FortiSOAR™ services.

## network

Manages network operations. You can use the following options with this subcommand:

**ipv6 --enable :** Enables the IPv6 protocol on your FortiSOAR™ system. The system will reboot as part of the execution.

`set-https-proxy --host<proxy_hostname> --port<proxy_port> --protocol<proxy_protocol> --user<proxy_username> --password<proxy_password>`: Configures an https proxy server to serve all https requests from FortiSOAR™. To configure an https proxy, you must specify the hostname and the port number of the HTTPS proxy server. You must also specify the protocol to be used to communicate with the HTTPS proxy server. You can also optionally specify the username and password used to access the HTTPS proxy server.

`set-http-proxy --host<proxy_hostname> --port<proxy_port> --protocol<proxy_protocol> --user<proxy_username> --password<proxy_password>`: Configures an http proxy server to serve all http requests from FortiSOAR™. To configure an http proxy, you must specify the hostname and the port number of the HTTP proxy server. You must also specify the protocol to be used to communicate with the HTTP proxy server. You can also optionally specify the username and password used to access the HTTP proxy server.

`list-proxy`: Lists the proxies that are configured.

`set-no-proxy --host<hostname>`: Configures a comma-separated list of hostnames that do not require to be routed through a proxy server.

**Note:** Review the existing no-proxy list using the `list-proxy` option. You can add or remove proxies from the existing list by specifying a *complete comma-separated list of proxies* that you want to configure using the `set-no-proxy` option. For example, if you have added hostname1 to the no-proxy list and you want to add hostname2 to the no-proxy list, then you must run the command as: `csadm network set-no-proxy --host "hostname1, hostname2"`

### Notes with respect to FortiSOAR™ Admin CLI:

- In case of FortiSOAR™ **Secure Message Exchange** instance all subcommands work as per the enterprise edition. However, the `mq` subcommand only supports the `--generate-certs` option:  
`csadm mq --generate-certs`: Generates the SSL certificate. This generates the cyopsca certificate, then creates the updated `.pem` file, and then restarts the rabbitmq-server.  
**Note:** A `.key` file has the path to a PEM encoded file containing the private key. A `.pem` file has the path to a PEM encoded file containing the certificate (or certificate chain) that will be presented when requested.
- After you run the `csadm certs --generate <hostname>` or `csadm mq --flush-db` commands for troubleshooting purposes, you must ensure that you restart all FortiSOAR™ services using the `csadm services --restart` command.
- If you have upgraded your system, you must close and logout of your existing SSH session and login to your upgraded instance again to run the `csadm` commands and perform any operations.

## CLI commands used for forwarding syslogs

Use the `csadm log forward` command to forwards FortiSOAR™ logs to your central log management server that supports a Rsyslog client. You can use the following options with this subcommand:

- `add-config - csadm log forward add config`: Adds configuration details for the syslog server to which you want to forward the FortiSOAR™. You can use the following options with this subcommand:
  - `--server`: Hostname of the syslog server to which you want to forward the FortiSOAR™ logs.
  - `--port`: Port number that you want to use to communicate with the syslog server.
  - `--protocol`: Protocol that you want to use to communicate with the syslog server. You can specify `tcp`, `udp`, or `relp`.
  - `--tls`: To securely communicate with the syslog server, set `-tls` to **true**. If you enable TLS, then in the `--ca-cert` option, you must specify the path to the CA certificate PEM file which contains the complete chain of CA certificates including the filename. If you have a client certificate for your FortiSOAR™ client, then in the `--client-cert` option, you must specify the path to the client certificate PEM file including the filename, and in the `--client-key` option, you must specify the path to the client key PEM file including the filename.
  - `--filter`: Comma-separated list of filters to specify the type of logs that you want to forward to your syslog server. Valid filters are `application`, `audit`, `none`, and by default, all the logs, i.e., application and audit logs are forwarded. If for example, if you want to forward audit logs only then specify `--filter=audit`. If you specify `--filter=none`, then no logs are forwarded, i.e., log forwarding is temporarily disabled. To enable the log forwarding again, use the `update-config` subcommand with the `--filter` option. For example, `csadm log forward update-config -uuid < UUID of configuration > --filter <audit,application>`.

**Note:** You can define the rules to forward audit logs using the FortiSOAR™ UI. For more information, see the *System Configuration* chapter.

  - `--config-name`: Name of the configuration in which you want to store the log forwarding configuration details.

**Note:** Validation checks such as, whether the syslog server is reachable on the specified port etc. are run before adding the syslog server, and the syslog server is added only if the configuration details entered are valid.
- `show-config - csadm log forward show-config`: Displays configuration details of the syslog server such as the server's IP address, protocol, TLS information, UUID of the configuration, etc.
- `remove-config - csadm log forward remove-config -uuid < UUID of configuration >`: Removes the syslog configuration based on the configuration UUID

you have specified. To know the UUID of your configuration use the `show-config` subcommand.

- `update-config -csadm log forward remove-config -uuid < UUID of configuration >`: Updates the syslog configuration based on the configuration UUID you have specified. To know the UUID of your configuration use the `show-config` subcommand. You can update any or all of the options as mention in the `add-config` subcommand.

Use the `update-config` subcommand with the `--filter` option, to enable temporarily disabled log forwarding.

**Note:** You can configure only a single syslog server. If you have already configured a syslog server and you try to add a new one, then FortiSOAR™ displays appropriate warning messages informing you that a syslog server is already configured, and adding a new syslog server will remove already configured one. Further processing is done based on your response (yes/no) to the messages.

# High Availability support in FortiSOAR™

## Overview

High Availability (HA) can be achieved using the following methods:

- **Nightly database backups and incremental VM snapshots:** FortiSOAR™ provides backup scripts that are scheduled to run at pre-defined intervals and take full database backup on a shared or backed up drive. The full backups have to be supplemented with incremental Virtual Machine (VM) snapshots whenever there are changes made to the file system, such as connector installation changes, config file changes, upgrades, schedule changes, etc. For more information, see the *Backing up and Restoring FortiSOAR™* chapter.
- **HA provided by the underlying virtualization platform:** Your Virtualization platform also provides HA, such as VMware HA and AWS EBS snapshots. This method relies on your expertise and infrastructure.
- **Externalized Database:** This method allows you to externalize your PostgreSQL database and uses your own database's HA solution. VM snapshots have to be taken when there are changes made to the file system, such as connector installation changes, config file changes, upgrades, schedule changes, etc. For more information on externalizing PostgreSQL database, see the *Externalization of your FortiSOAR™ PostgreSQL database* chapter.
- **HA clusters:** FortiSOAR™ provides a clustering solution with more than one FortiSOAR™ node joined to form an HA cluster. When you deploy FortiSOAR™ instance, the FortiSOAR Configuration Wizard configures the instance as a single node cluster, and it is created as an active primary node. You can join more nodes to this node to form a multi-node cluster. This method is explained in detail in this chapter.

FortiSOAR™ implements HA Clustering with the use of PostgreSQL database clustering. It supports Active/Active and Active/Passive configurations with both internal and external PostgreSQL databases. HA clusters can be used to fulfill the following two use cases: Disaster Recovery (DR) and Scaling. For DR you can configure an Active/Passive cluster that has the passive node located in a remote datacenter. For scaling workflow execution across multiple nodes, you can use co-located Active/Active cluster nodes.

## High Availability Types supported with FortiSOAR™

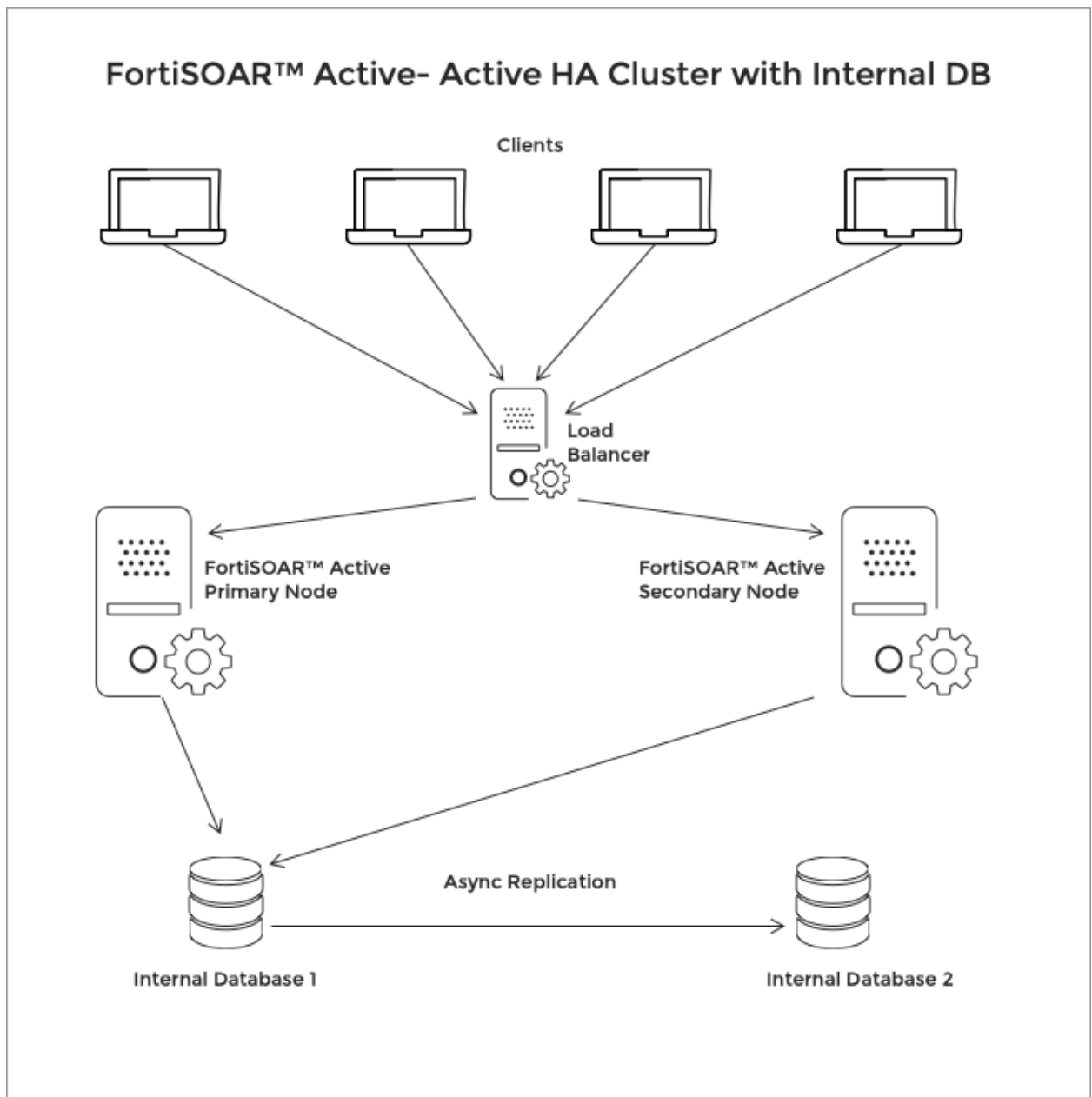
You can configure FortiSOAR™ with either an externalized PostgreSQL database or an internal PostgreSQL database. For both cases you can configure Active-Active or Active-Passive high availability clusters.

## High Availability with an internal PostgreSQL database

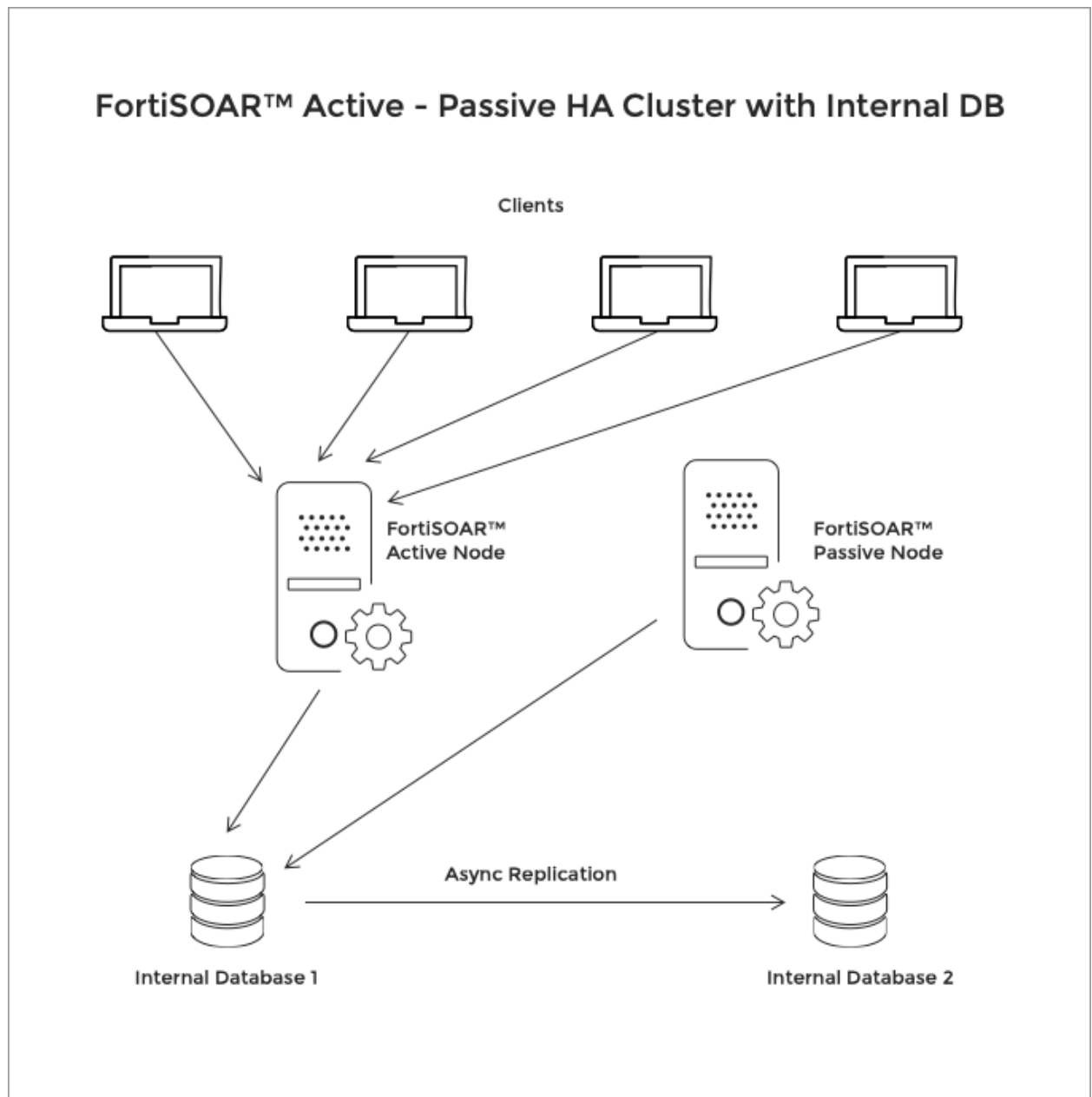
FortiSOAR™ HA/DR is based on internal clustering that takes care of replicating data (PostgreSQL) to all cluster nodes, and provides an administration CLI (csadm) to manage the cluster and perform the "Takeover" operation, when necessary. FortiSOAR™ uses PostgreSQL streaming replication, which is asynchronous in nature. For more information, see [PostgreSQL: Documentation](#).

You can configure FortiSOAR™ for high availability (HA) with an internal PostgreSQL database in the following two ways:

- In an Active-Active HA cluster configuration, at least two nodes are actively running the same kind of service simultaneously. The main aim of the active-active cluster is to achieve load balancing and horizontal scaling, while data is being replicated asynchronously. You should front multiple active nodes with a proxy or a load balancer to effectively direct requests to all nodes.



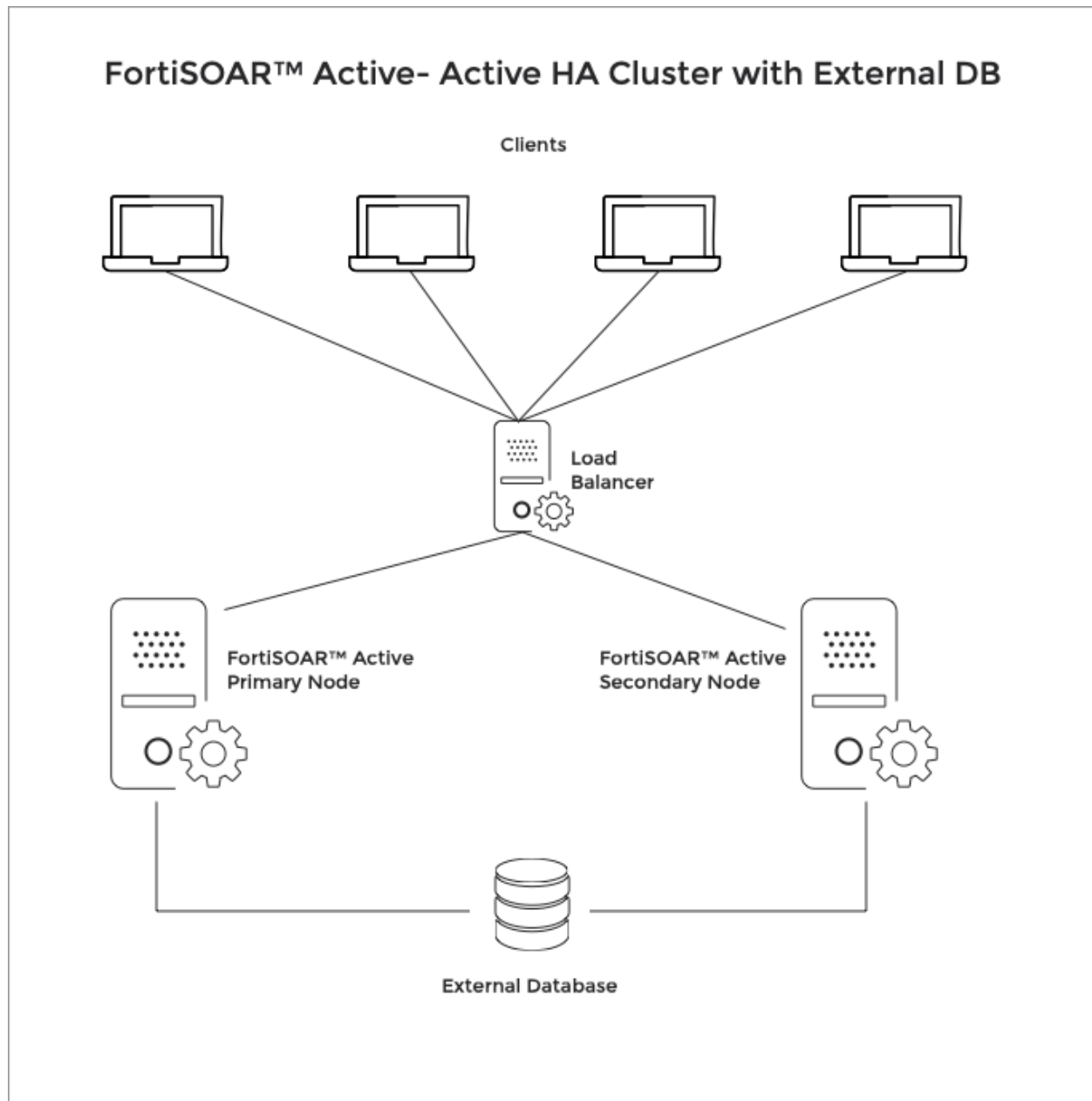
- In an Active-Passive HA cluster configuration, one or more passive or standby nodes are available to take over if the primary node fails. Processing is done only by the primary node. However, when the primary node fails, then a standby node can be promoted as the primary node. In this configuration, you can have one active node and one or more passive nodes configured in a cluster, which provides redundancy, while data is being replicated asynchronously.



## High Availability with an externalized PostgreSQL database

In case of an externalized database, the user will use their own database's HA solution. FortiSOAR™ ensures that changes done in the file system of any of the cluster nodes arising from the connector install/uninstall or any changes in the module definitions are synced across every node so a secondary or passive node can takeover in the least time in case of a failure of the primary node.





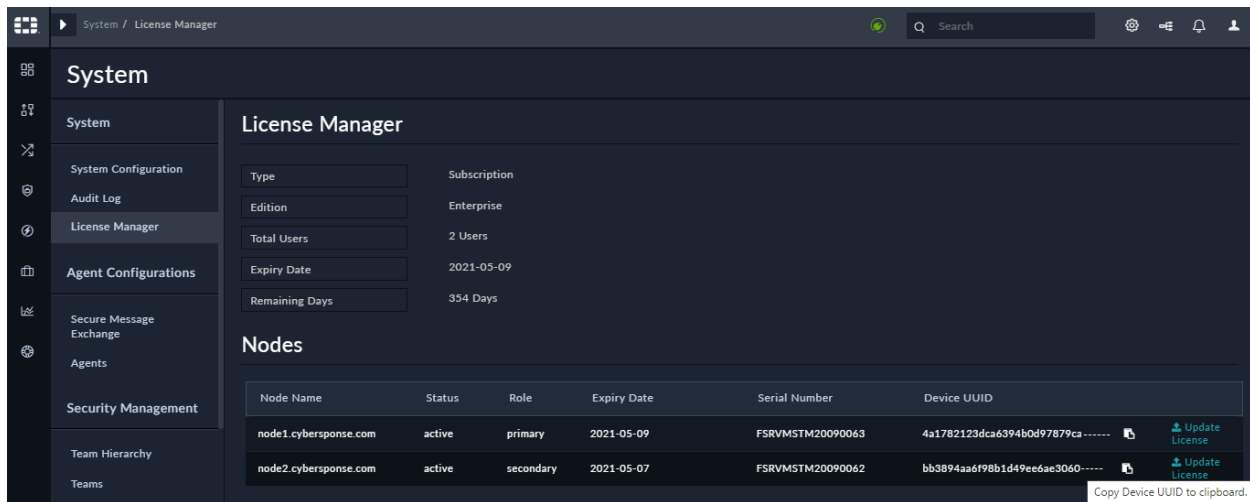
**Figure 73.** *FortiSOAR™ with an external database and an Active/Active configuration*

## Cluster Licensing

FortiSOAR™ version 6.4.4 and later does not mandate 'Additional Users' entitlement to be the same across all cluster nodes, i.e., you do not require to buy additional user licenses for clustered nodes. User count entitlement will now always be validated from the primary node. The secondary nodes can have the basic two-user entitlement.

## Viewing and updating the license of an HA cluster

In case your FortiSOAR™ instance is part of a High Availability cluster, the **License Manager** page also displays the information about the nodes in the cluster, if you have added secondary node(s) as shown in the following image:



**Figure 74.** License Manager Page in case of your FortiSOAR™ instance is part of a High Availability cluster

As shown in the above image, the primary node is Node 2 and that node is licensed with 7 users, therefore the total user count displays as 7 users.

To update the license for each node, click **Update License** and upload the license for that node.

**Note:** If you update a license that does not match with the system UUID, then you will get a warning on UI while updating the license. If you update the same license in more than one environment then the license is detected duplicate and you require to correct the license, else your FortiSOAR™ UI will be blocked in 2 hours.

## Prerequisites to configuring High Availability

- Your FortiSOAR™ instance must be a 5.0.0 and later instance, either a fresh install of 5.0.0 and later or your instance must be upgraded to 5.0.0 and later.
- All nodes of a cluster should DNS resolvable from each other.
- Ensure that the **ssh** session does not time out by entering into the **screen** mode. For more information, see the [Handle session timeouts while running the FortiSOAR™ upgrade](#) article present in the Fortinet Knowledge Base.
- If you have a security group (AWS) or an external firewall between the HA nodes, then you must open the following ports between HA nodes on AWS or the external firewall: For PostgreSQL: 5432, for Redis: 6379, and for ElasticSearch: 9200

- Fronting and accessing the FortiSOAR™ HA Cluster with a Load Balancer such as HAProxy or a Reverse Proxy is recommended so that the address remains unchanged on takeover.

## Process for configuring High Availability

### Steps to configure FortiSOAR™ HA cluster with an internal PostgreSQL database

If you are configuring HA with an internal PostgreSQL database, ensure that you have met all the Prerequisites criteria (see the [Prerequisites to configuring High Availability](#) section) and then perform the following steps:

**Important:** You must join nodes to a HA cluster in a sequentially order.

1. Use the FortiSOAR™ Admin CLI (`csadm`) to configure HA for your FortiSOAR™ instances. For more information, see the *FortiSOAR™ Admin CLI* chapter. Connect to your VM as a `root` user and run the following command:

```
# csadm ha
```

This will display the options available to configure HA:

```
[root@cybersponse csadmin]# csadm ha
usage: csadm ha [-h]
               {join-cluster,export-conf,whitelist,list-nodes,leave-cluster,list-commands,takeover,firedrill,restore,get-replication-stat}
               ...
subcommand options are:
  join-cluster      Join the HA cluster
  export-conf       Export the configuration file
  whitelist         Whitelist secondary/passive server
  list-nodes        List HA cluster details
  leave-cluster     Leave HA cluster
  list-commands     List pending cluster commands
  get-replication-stat Get the replication statistics
  takeover         Perform takeover
  firedrill         Test DR
  restore           Restore the server to either passive/secondary after firedrill
subcommand options are:
-h, --help         show this help message and exit
```

2. To configure a node as a secondary node, ensure that all HA nodes are resolvable through DNS and then SSH to the server that you want to configure as a secondary node and run the following command:

```
# csadm ha join-cluster --status <active, passive> --role secondary --primary-node <DNS_Resolvable_Primary_Node_Name>
```

Once you enter this command, you will be prompted to enter the SSH password to access your primary node.

In case of a cloud environment, where authentication is key-based, you require to run the following command:

```
# csadm ha join-cluster --status <active, passive> --role <primary, secondary> --primary-node <DNS_Resolvable_Primary_Node_Name> --primary-node-ssh-key <Path_To_Pem_File>
```

This will add the node as a secondary node in the cluster.

**Note:** When you join a node to an HA cluster, the `list-nodes` command does not display that a node is in the process of joining the cluster. The newly added node will

be displayed in the `list-nodes` command only after it has been added to the HA cluster.

**Note:** If you have upgraded FortiSOAR™ and are joining a freshly provisioned node using the `join-cluster` operation to a cluster having some connectors installed, then you are required to manually reinstall the connectors that were present on the existing node on the new node.

Also, note that if you have built your own custom connector, then you must upload the .tgz file of the connector on all the nodes within the HA cluster.

When you are uploading the .tgz file on all the nodes, you must ensure that you select the **Delete all existing versions** checkbox. You must also ensure that you have uploaded the same version of the connector to all the nodes.

## Steps to configure FortiSOAR™ HA cluster with an external PostgreSQL database

If you are configuring HA with an external PostgreSQL database, perform the following steps:

1. Externalize the PostgreSQL database for the primary node of your HA configuration. For the procedure for externalizing PostgreSQL databases, see the *Externalization of your FortiSOAR™ PostgreSQL database chapter*.
2. Add the hostnames of the secondary nodes to the allowlist in the external database.
3. Add the hostnames of the secondary nodes to the `pg_hba.conf` (`/var/lib/pgsql/12/data/pg_hba.conf`) file in the external database. This ensures that the external database trusts the FortiSOAR™ server for incoming connections.
4. Ensure that you have met all the Prerequisites criteria (see the [Prerequisites to configuring High Availability](#) section)
5. Create the HA cluster by following the steps mentioned in the [Steps to configure FortiSOAR™ HA cluster with an internal PostgreSQL database](#) section.

## Takeover

Use the `csadm ha takeover` command to perform a takeover when your active primary node is down. Run this command on the secondary node that you want to configure as your active primary node.

If during takeover you specify **no** to the `Do you want to invoke 'join-cluster' on other cluster nodes?` prompt, or if any node(s) is not reachable, then you will have to reconfigure all the nodes (or the node(s) that were not reachable) in the cluster to point to the new active primary node using the `csadm ha join-cluster` command.

During the takeover operation, if the secondary node license user entitlement is lesser than that on the primary node, then the licenses get swapped between the new primary node (node B) and the old primary node (node A). To prevent any undesirable node lockouts,

FortiSOAR™ checks the user count entitlement of both licenses before exchanging the licenses between Node A and Node B. If Node B already has a higher user entitlement, then the licenses are not swapped. Therefore, no duplicate license violation will occur once Node A comes back online in case of matching user entitlements of cluster nodes.

The swapping of licenses during takeover leads to the following scenarios:

- If Node A is alive at the time of the takeover operation, then whether Node A joins back the HA cluster or not, it synchronizes to the Fortinet Licensing Portal with the license previously associated with Node B.
- If Node A is not alive at the time of the takeover operation, then it synchronizes with FDN with its old license, which is being used by Node B as well; and this might cause a node lockout, if this is not corrected manually, by deploying the old Node B license onto Node A, in the grace window of two hours. Note, that FortiSOAR™ allows a grace period of two hours even when FDN reports a duplicate license.

**Important:** After you have performed takeover and configured a secondary node as the active primary node, then you will observe that the log forwarder configurations are not present on the new primary node. This is because Syslog settings are not replicated to the passive node since the passive node could be in a remote datacenter and with network latencies between datacenters. Also, the same Syslog server might not be the ideal choice for log forwarding from the DR node. If you want to forward logs from the passive node, you must enable it manually using the `csadm log forward` command. For more information, see the FortiSOAR™ Admin CLI chapter.

## Usage of the `csadm ha` command

Certain operations, such as takeover, join cluster, etc. might take a longer period of time to run, therefore you must ensure that your ssh session does not timed out by entering into the `screen` mode. For more information, see the [Handle session timeouts while running the FortiSOAR™ upgrade](#) article present in the Fortinet Knowledge Base.

You can get help for the `csadm ha` command and subcommands using the `--help` parameter.

**Note:** It is recommended that you perform operations such as join-cluster, leave-cluster, etc sequentially. For example, when you are adding nodes to a cluster, it is recommended that you add the nodes one after the other rather than parallelly.

The following table lists all the subcommands that you can use with the `csadm ha` command:

Subcommand	Brief Description
list-nodes	Lists all the nodes that are available in the cluster with their respective node names and ID, status, role, and a comment that contains information about which nodes have joined the specific HA cluster and the primary server.

```
[root@cluster-node5 csadmin]# csadm ha listnodes
nodeId      nodeName      status  role  comment
-----
* bddacf7748866c9b6f35d4a812785f04 cluster-node5.net active primary primary server
21cd1ae33bab8e8509274cb8f74cc25b cluster-node6.net active secondary joined cluster with cluster-node5
0b1cb2516e25d03168054d23a72c6b20 cluster-node7.net active secondary joined cluster with cluster-node5
```

You can filter nodes for specific status, role, etc. For example, if you want to retrieve only those nodes that are active use the following command: `csadm ha list-nodes --active`, or if you want to retrieve secondary active nodes, then use the following command: `csadm ha list-nodes --active --secondary`.

**Note:** The `list-nodes` command will not display a node that is in the process of joining the cluster, i.e., it will display the newly added node only after it has been added to the HA cluster.

**export-conf** Exports the configuration of details of the active primary node to a configuration file named `ha.conf`. For more details on `export-conf`, see the [Process for configuring HA](#) section.

**allowlist** Adds the hostnames of the secondary nodes in the HA cluster to the allowlist on the active primary node. For more details on `allowlist`, see the [Process for configuring HA](#) section.

**Important:** Ensure that incoming TCP traffic from the IP address(es) [xxx.xxx.xx.xxx] of your FortiSOAR™ instance(s) on port(s) **5432**, **9200**, and **6379** is not blocked by your organization's firewall.

**join-cluster** Adds a node to the cluster with the role and status you have specified. For more details on `join-cluster`, see the [Process for configuring HA](#) section.

**get-replication-stat** Displays the replication statistics, i.e., the replication lag and status between cluster nodes.

In the case of secondary nodes, information about total lag and time elapsed from last sync is displayed. In the case of the primary node, information about sending lag, receiving lag, relaying lag, and total lag is displayed.

You can use the following option with this subcommand:

`--verbose`: Displays detailed replication statistics.

In the case of secondary nodes, information about receive lsn, replay lsn, total lag, and time elapsed from last sync is displayed.

Do not use this subcommand on the primary node since no additional details are displayed for the primary node when you use the `--verbose` subcommand.

**Note:** If you have configured FortiSOAR™ with an externalized PostgreSQL database, then replication statistics will not be displayed for the cluster nodes.

**show-health** Displays the health information for the current node. You can use the following option with this subcommand:

`--all nodes`: Displays the health information for all the nodes in an HA cluster.

`--json`: Displays the health information in the JSON format.

**firedrill** Tests your disaster recovery configuration.  
You can perform a firedrill on a secondary (active or passive) node only.

Running the firedrill suspends the replication to the node's database and sets it up as a standalone node pointing to its local database. Since the firedrill is primarily performed to ensure that the database replication is set up correctly, hence it is not applicable when the database is externalized. Once you have completed the firedrill, ensure that you perform restore, to get the nodes back to replication mode.

## **Licenses on a firedrilled node:**

- If the node license had a user license entitlement matching the primary node user entitlement, all users can login to the firedrilled node.
- If the node license had a basic user entitlement and the HA cluster had more active users, then only the `csadmin` user can login to the UI of the firedrilled node. The `csadmin` user can then activate two users who need to test the firedrill and make the rest of the users inactive.

**Note:** This does not cause any impact to the primary node or other nodes in the HA cluster. Post-restore, the firedrilled node will join the cluster back and maximum active users as per the entitlement will be honored.

## **Schedules on a firedrilled node:**

The node on which a firedrill is being performed will have their schedules and playbooks stopped, i.e., `celerybeatd` will be disabled on this node. This is done intentionally as any configured schedules or playbooks should not run when the node is in the firedrill mode.

restore	Restores the node back to its original state in the cluster after you have performed a firedrill. That is, <code>csadm ha restore</code> restores the node that was converted to the active primary node after the firedrill back to its original state of a secondary node. The restore command discards all activities such as record creation, that is done during the firedrill since that data is assumed to be test data. This command will restore the database from the content backed up prior to firedrill.
takeover	Performs a takeover when your active primary node is down. Therefore, you must run the <code>csadm ha takeover</code> command on the secondary node that you want to configure as your active primary node.
leave-cluster	Removes a node from the cluster and the node goes back to the state it was in before joining the cluster.

## Overview of nodes in a FortiSOAR™ HA cluster

- One FortiSOAR™ cluster can have only one active primary node, all the other nodes are either active secondary nodes or passive nodes. Uniqueness of the primary node is due to the following:
  - In case of an internal database, all active nodes talk to the database of the primary node for all reads/writes. The database of all other nodes is in the read-only mode and setup for replication from the primary node.



- Although the queued workflows are distributed amongst all active nodes, the Workflow scheduler runs only on the primary node.
- All active nodes index the data for quick search into Elasticsearch at the primary node.
- All integrations or connectors that have a listener configured for notifications, such as IMAP, Exchange, Syslog, etc run the listeners only on the primary node. Therefore, if the primary node goes down, one of the other nodes in the cluster must be promoted as the new primary node and the other nodes should rejoin the cluster connecting to the new primary.
- Active secondary nodes connect to the database of the active primary node and serve FortiSOAR™ requests. However, passive nodes are used only for disaster recovery and they do not serve any FortiSOAR™ requests.

## Checking replication between nodes in an active-passive configuration

When using an active-passive configuration with internal databases, ensure that replication between the nodes is working correctly using the following steps:

- Perform the **firedrill** operation at regular intervals to ensure that the passive node can takeover successfully, when required.
- Schedule full nightly backups at the active primary node using the FortiSOAR™ backup and restore scripts. For more information on backup and restore, see the *Backing up and Restoring FortiSOAR™* chapter.

## Upgrading an HA cluster

For the procedure on how to upgrade a FortiSOAR™ High Availability Cluster to 6.4.4, see the *Upgrading a FortiSOAR™ High Availability Cluster to 6.4.4* section in the "Upgrade Guide."

## Load Balancer

The clustered instances should be fronted by a TCP Load Balancer such as HAProxy, and clients should connect to the cluster using the address of the proxy.

## Setting up HAProxy as a TCP load balancer fronting the two clustered nodes

The following steps list out the steps to install "HAProxy" as a load balancer on a CentOS Virtual Machine:



1. `# yum install haproxy`
2. In the `/etc/haproxy/haproxy.cfg` file, add the policy as shown in the following image:

```
listen logyank_cluster
bind ha.directponse.net:8443
mode tcp
option tcplog
balance roundrobin
cookie SERVERUSED insert indirect nocache
server cocache-node2.directponse.net 192.168.5.221 :443 check inter 5000 downinter 500 cookie cluster-node1.downinponse.net
server socache-node2.directponse.net 192.168.5.101 :443 check inter 5000 downinter 500 cookie cluster-node2.downinponse.net
server socache-node3.directponse.net 192.168.5.101 :443 check inter 5000 downinter 500 cookie cluster-node3.downinponse.net
```

3. To reload the firewall, run the following commands:  
`$ sudo firewall-cmd --zone=public --add-port=<portspecifiedwhilebindingHAProxy>/tcp --permanent`  
`$ sudo firewall-cmd --reload`
4. Restart haproxy using the following command:  
`# systemctl restart haproxy`
5. Use the bind address (instead of the IP address of the node in the cluster) for accessing the FortiSOAR™ UI.

## Behavior that might be observed while publishing modules when you are accessing HA clusters using a load balancer

When you have initiated a publish for any module management activity and you are accessing your HA cluster with one or more active secondary nodes using a load balancer such as “HAProxy”, then you might observe the following behaviors:

- While the Publish operation is in progress, you might see many publish status messages on the UI.
- If you have added a new field to the module, or you have removed a field from the module, then you might observe that these changes are not reflected on the UI. In such cases, you must log out of FortiSOAR™ and log back into FortiSOAR™.
- After a successful publish of the module(s), you might observe that the **Publish** button is yet enabled and the modules yet have the asterisk (\*) sign. In such cases, you must log out of FortiSOAR™ and log back into FortiSOAR™ to view the correct state of the Publish operation.

## Tunables

You can tune the following configurations:

- `max_wal_senders = 10`  
This attribute defines the maximum number of walsender processes. By default, this is set as 10.
- `wal_keep_segments = 320`  
This attribute contains a maximum of 5 GB data.

**Important:** Both `max_wal_senders` and `wal_keep_segments` attributes are applicable when the database is internal.

Every secondary/passive node needs one wal sender process on the primary node, which means that the above setting can configure a maximum of 10 secondary/passive nodes.

If you have more than 10 secondary/passive nodes, then you need to edit the value of the `max_wal_senders` attribute in the `/var/lib/pgsql/12/data/postgresql.conf` file on the primary node and restart the PostgreSQL server using the following command: `systemctl restart postgresql-12`

**Note:** You might find multiple occurrences of `max_wal_senders` attribute in the `postgresql.conf` file. You always need to edit last occurrence of the `max_wal_senders` attribute in the `postgresql.conf` file.

The `wal_keep_segments` attribute has been set to 320, which means that the secondary nodes can lag behind by the maximum of 5GB. If the lag is more than 5GB, then replication will not work properly, and you will require to reconfigure the secondary node by running the `join-cluster` command

Also note that Settings changes that are done in any configuration file on an instance, such as changing the log level, etc., apply only to that instance. Therefore, if you want to apply the changed setting to all the node, you have to make those changes across all the cluster nodes.

## Best Practices

- Fronting and accessing the FortiSOAR™ HA cluster with a Load Balancer or a Reverse Proxy is recommended so that the address remains unchanged on takeover.
- You must ensure that the SIEM and other endpoints that FortiSOAR™ connects to are reachable on the virtualized host name (DNS) that would remain intact even after a failover (local or geo wide).
- The FortiSOAR™ node connects outbound to the SIEM, to periodically pull the "Alerts" (Terminology for this would differ for each SIEM, Eg, 'Offense', 'Corelated Event', 'Notable'). The "pull" model also ensures resiliency. In the case of downtime, once the FortiSOAR™ node comes back up, it would pull the alerts from last pulled time, ensuring there is no data loss even during down time.
- Tune the `wal_keep_segments` setting in the `/var/lib/pgsql/12/data/postgresql.conf` file. When you have a heavy write on the primary node, for example, a lot of playbooks are being run or a lot of alerts are created, then there is a lot of data to be replicated. If the secondary node is in a distant data center, the replication speed might not be able to cope up with the write on the primary node. There is a fixed size for the buffer data (default is 5 GB) that the primary node keeps for data replicated, after which the data rolls over. If a secondary node has not yet copied the data before the data has rolled over, it can become 'out of sync' and require a full synchronization, and then this would cause failures.

You might want to increase the `wal_keep_segments` setting in the following scenarios:

- The secondary node is in a distant datacenter and the network speed is slow.
- The secondary node is offline for a very long time due to some issues or for maintenance, etc.
- The secondary node is firedrilled and you want the restore operation to be faster using a differential sync instead of a full sync.

It is recommended to increase the `wal_keep_segments` settings to 20 GB (instead of the default, i.e., 5GB) in the `/var/lib/pgsql/12/data/postgresql.conf` file as follows:

The `wal_keep_segments` settings in the `/var/lib/pgsql/12/data/postgresql.conf` file appears as follows:

```
wal_keep_segments = 320 # in logfile segments, 16MB each; 0 disables;  
keeps upto 5GB wal
```

**Note:** `postgresql.conf` can set the `wal_keep_segments` value multiple times in the file. You must change the last occurrence of the `wal_keep_segments` setting in the `postgresql.conf` file.

To increase the last occurrence of the `wal_keep_segments` setting to 20 GB change it as follows:

```
wal_keep_segments = 1280 # in logfile segments, 16MB each; 0 disables;  
keeps upto 20GB
```

## Monitoring health of HA clusters

All secondary nodes in the cluster exchange HA heartbeat packets with the primary node so that the primary node can monitor and verify the status of all the secondary nodes and the secondary nodes can verify the status of the primary node.

Your system administrator can configure the monitoring of heartbeats on the **System Configuration > Application Configuration > System & Cluster Health Monitoring > Cluster Health** section. Once you have configured monitoring of heartbeats and if any node in the HA cluster is unreachable, then the other active nodes in the cluster, which are operational, send email notifications and write log messages to alert the system administrator that a failure has occurred. For more information, see the [Configuring System and Cluster Health Monitoring](#) topic in the *System Administration* chapter.

## Understanding HA Cluster Health Notifications

### HA cluster health notification checks on the primary node

On every scheduled monitoring interval, which defaults to 5 minutes on the primary node for every secondary/passive node, the HA cluster health notifications checks:

- If there is a heartbeat miss from the secondary/passive node(s) in the last 15 minutes by taking the default values of monitoring interval (5 minutes) \* missed heartbeat count (3). If there is a missed heartbeat, then the health notification check sends a "heartbeat failure" notification and exits.

- If the data replication from the primary node is broken. If yes, then the health notification check sends a notification containing the replication lag with respect to the last known `replay_lsn` of secondary node and exits.

Following is a sample notification:

Following secondary FortiSOAR node(s) seem to have failed -

Node: hasecondary.myorgdomain

Current lag with primary node is 97 kB

Failure reason:

1. The postgres database replication to the secondary node is not working due to data log rotation at the primary node.
2. The secondary node has been shutdown/halted.
3. PostgreSQL not running on node(s).
4. nodeName from 'csadm ha list-nodes' differs from actual FQDN used during join-cluster.

If node is up and running,

1. Check the status of PostgreSQL service using 'systemctl status postgresql-<postgresql-version-here> -l' on node to get more details.

2. If you see 'FATAL: could not receive data from WAL stream: requested WAL segment has already been removed' in the PostgreSQL service status, you need to re-join the cluster using 'csadm ha join-cluster --fetch-fresh-backup'

- If the replication lag reaches or crosses the set threshold specified, then the health notification check sends a notification containing the replication lag as shown in the following sample notification:

Replication lag threshold is reached on following node(s):

Node: hasecondary.myorgdomain

Current lag with primary node : 3431 MB

Configured WAL size : 5120 MB

Configured Threshold : 3072 MB (60% of the Configured WAL size)

- If any service is not running, then the health notification check sends a "service failure" notification and exits.
- If a firedrill is in progress on a secondary/passive node. If yes, then the health notification check sends the following notification and exits.

Firedrill is in progress on following node(s):

Node: hasecondary.myorgdomain

Current lag with primary node : 52 kB

You can ignore the lag that is displayed in this case since this lag indicates the amount of data the firedrill node needs to sync when `csadm ha restore` is performed.

You can also check the lag using the `get-replication-stat` command on the primary node.

## HA cluster health notification checks on the secondary node

On every scheduled monitoring interval, which defaults to 5 minutes on the secondary node, the HA cluster health notifications checks:

- If there is a heartbeat miss from the primary node in the last 15 minutes by taking the default values of health beat interval (5minutes) \* missed heartbeat count (3). If there is a missed heartbeat, then the health notification check sends a "heartbeat failure" notification and exits.
- If there is no heartbeat failure but there is a service failure, then the health notification check sends a "service failure" notification and exits.

## HA cluster health notification checks when the HA cluster is set up with an external PostgreSQL database

If the PostgreSQL database is externalized, the email notifications generated by the primary node are different from when the PostgreSQL database is not externalized. On the primary node for every secondary/passive node, the HA cluster health notifications checks:

- If there is a heartbeat miss from the secondary/passive node(s) in the last 15 minutes by taking the default values of health beat interval (5 minutes) \* missed heartbeat count (3). If there is a missed heartbeat, then the health notification check sends a "heartbeat failure" notification as follow and exits:  
Following secondary FortiSOAR node(s) seem to have failed -  
Node: hasecondary.myorgdomain  
Failure reason: Heartbeat failure. Check if the 'cyops-ha' service is running or not using 'systemctl status cyops-ha'.
- If any service is not running, then the health notification check sends a "service failure" notification as follows and exits:  
Following secondary FortiSOAR node(s) seem to have failed -  
Node: hasecondary.myorgdomain  
Failure reason: cyops-auth service(s) not running.

## HA cluster health notification checks when a secondary node is firedrilled

- When a firedrill is in progress on a secondary/passive node, then you do not receive any 'out of sync' notification, instead the health notification check sends the following email notification and exits.  
Firedrill is in progress on following node(s):  
Node: hasecondary.myorgdomain  
Current lag with primary node : 52 kB  
You can ignore the lag that is displayed in this case since this lag indicates the amount of data the firedrill node needs to sync when `csadm ha restore` is performed.  
You can also check the lag using the `get-replication-stat` command on the primary node. If a firedrill is in progress on a secondary/passive node, then you can ignore the lag displayed. This is because the 'total\_lag' that gets shown in the `get-replication-stat` messages indicates the amount of data the secondary/passive node will need to sync when the `csadm ha restore` operation is performed on the node once the firedrill completes.

## HA cluster health notification checks during takeover

1. When takeover is in progress, the previous primary node might send 'out of sync' email notifications for the node that is taken over, because the previous primary sees it as not replicating data anymore. These can be ignored. After the takeover is completed, we mark the previous primary node as `faulted`. Therefore, you will not see any replication statistics on the old primary node.
2. After the takeover is performed, you can ignore the messages of the `get-replication-stat` command on the new primary node. You can also ignore the 'out of sync' email notification that is generated by the new primary node since when we perform the takeover, the entries of all the nodes in the cluster are yet included in `csadm ha list-nodes`, and because the remaining nodes yet require to join the new primary node, this new primary node keeps generating the notification for all those nodes.
3. When all the other nodes of a HA cluster join back to the new primary node, then the health notification check starts to work and there will not be any ignorable notification.

## Troubleshooting issues based on the notifications

The following section provides details on how to check and fix the possible reasons of failures that are listed in the email notifications sent by the HA cluster check.

To troubleshoot HA issues, you can use the HA log located at: `/var/log/cyops/cyops-auth/ha.log`.

### Heartbeat Failure

#### Resolution:

When you get a heartbeat failure notification on a secondary/passive node or on an active node, then do the following:

1. Check if the `cyops-ha` service is running on that node, using the `systemctl status cyops-ha` command.
2. If it is not running, then you must restart the `cyops-ha` service.

### Node name differs from actual FQDN

#### Resolution:

Correct the notification such as `nodeName` from '`csadm ha list-nodes`' differs from actual FQDN used during `join-cluster`, using the following steps:

1. Login on the node for which you are receiving the above notification using SSH.
2. Use the following command to correct the FQDN of the node:  
`csadm ha set-node-name <enter-correct-FQDN-here>`

## Secondary/Passive node is out of sync with the Primary node

This issue could occur due to the following reasons:

- PostgreSQL service status shows `requested WAL segment <some-number-here> has already been removed`

OR

The `csadm ha get-replication-stat` command shows a higher time lapsed from the last sync when compared to the general time lapsed.

### Resolution:

In these cases, since the secondary/passive node is completely out of sync with the primary node, you need to perform the following steps on the secondary/passive node:

- Run the `touch /home/csadmin/.joincluster_in_progress` command to create the `.joincluster_in_progress` file.
- Rejoin the cluster as follows:  
`csadm ha join-cluster --status active/passive --role secondary --primary-node <Primary-node-FQDN> --fetch-fresh-backup`
- When there is heavy write on the primary node and the secondary node has not yet copied the data before the data has rolled over, it will be 'out of sync' and a full synchronization is needed, which can cause the above failures.

### Resolution:

Increase the `wal_keep_segments` setting in the `/var/lib/pgsql/12/data/postgresql.conf` file as described in the [Best Practices](#) section.

## PostgreSQL service is down on the primary node or PostgreSQL service is down on the externalized database host

If PostgreSQL service is down on the primary node, then the `cyops-ha service` on all the nodes will be down and there will be no notifications generated since the whole cluster is down; due to this you will also not be able to login to the FortiSOAR™ UI.

1. Check the reason for the failure using the `systemctl status postgresql-<postgresql-version-here> -l` on the primary node or the externalized database host.
2. Fix the issue based on the reason for failure.

## Higher time lapsed from the last sync when compared to the general time lapsed

When you run the `csadm ha get-replication-stat` command on the secondary node you might get a `'time_elapsed_from_last_sync'` value is higher than usual message.

- PostgreSQL down on the primary server.
- No activity on primary server.
- Secondary node is out of sync with the Primary node.



## Resolution:

1. Run the `systemctl status postgresql-12` command and ensure that you are not getting the `FATAL: could not receive data from WAL stream: requested WAL segment has already been removed.` message.
2. Run the `csadm ha get-replication-stat` command and check its results:
  - If you get the Value of 'sending\_lag' is higher than usual on primary when checked message, this means that there is load on the primary node. Run the `top` command to check which process is taking more CPU time. You can also use the following command for a quick check:  
`ps -eo pid,cmd,%mem,%cpu --sort=-%mem | head`
  - If you get the Value of 'replaying\_lag' is higher than usual on primary when checked message, this means that there is load on the secondary node. Run the `top` command to check which process is taking more CPU time. You can also use the following command for a quick check:  
`ps -eo pid,cmd,%mem,%cpu --sort=-%mem | head`

Sample scale test that were done in the lab to understand the behavior of 'csadm ha get-replication-stat'

## What was done before observing the behavior:

First we stopped the PostgreSQL service on the secondary/passive node.

Next, generated data on the primary node using the following script. You need to kill the script after some time when enough data is generated on the primary node.

```
[root@cybersponse csadmin]# cat data_load.sh
#!/bin/sh

psql -U cyberpgsql -d das -c "CREATE TABLE scale_data (
    section NUMERIC NOT NULL,
    id1      NUMERIC NOT NULL,
    id2      NUMERIC NOT NULL
);"

psql -U cyberpgsql -d das -c "
INSERT INTO scale_data
SELECT sections.*, gen.*
    , CEIL(RANDOM()*100)
  FROM GENERATE_SERIES(1, 300)    sections,
       GENERATE_SERIES(1, 900000) gen
 WHERE gen <= sections * 3000;"
[root@cybersponse csadmin]#
```



During the data generation process, we ran the `csadm ha get-replication-stat` on the primary node and you can observe that the secondary node is lagging with 4702 MB.

```
get-replication-stat on the primary node:

[root@cybersponse csadmin]# csadm ha get-replication-stat
-----
Warning:
Warning:
Following could be the issues with the nodes:
1. The postgres database replication to the secondary node is not
   working due to data log rotation at the primarynode.
2. The secondary node has been shutdown/halted.
3. PostgreSQL not running on node(s).
4. nodeName from 'csadm ha list-nodes' differs from actual FQDN u
   sed during join-cluster.
5. If a firedrill is in progress on the node, no action is requir
   ed. The 'lag' that is displayed indicates the amount of data the
   firedrill node needs to sync when 'csadm ha restore' will be perf
   ormed.

If node is up and running,
1. Check the status of PostgreSQL service using 'systemctl statu
   s postgresql-12 -l' on node to get more details.
2. If you see 'FATAL: could not receive data from WAL stream: req
   uested WAL segment has already been removed' in the PostgreSQL se
   rvice status, you need to re-join the cluster using 'csadm ha joi
   n-cluster --fetch-fresh-backup' for this node.
-----

nodeId                      nodeName                      status
  role      comment                      total
_lag
-----
--
-----
469c6330613a332c30dd4d8e3a607cf2  hasecondary.myorgdomain  active
      secondary  Joined cluster with haprimary.myorgdomain  4702 MB
[root@cybersponse csadmin]#
```

Next, start PostgreSQL on the secondary node and observed the 'replication-stat' on both the primary and secondary nodes

```
On the Primary node:

Every 2.0s: csadm ha get-replication-stat
                        Tue May 12 05:27:31 2020
-----
```

Note:

'sending\_lag' indicates load on the primary node

'receiving\_lag' indicates network delay or load on the passive/secondary node

'replaying\_lag' indicates load on the passive/secondary node

```
-----
node_hostname      sending_lag    receiving_lag    replayin
g_lag    total_lag
-----
-----
hasecondary.mydomain 4458 MB        11 MB           213 MB
4683 MB
```

On the Secondary node:

```
primary_hostname    total_lag    time_elapsed_from_last_syn
c
-----
---
haprimary.mydomain 287 MB      00:07:59.113185
```

On the Primary node:

Note:

'sending\_lag' indicates load on the primary node

'receiving\_lag' indicates network delay or load on the passive/secondary node

'replaying\_lag' indicates load on the passive/secondary node

```
-----
node_hostname      sending_lag    receiving_lag    replayin
g_lag    total_lag
-----
-----
hasecondary.mydomain 3600 MB        3456 kB          727 MB
4330 MB
```

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:27:49 2020

```
primary_hostname      total_lag      time_elapsed_from_last_syn
c
-----
haprimary.mydomain    854 MB        00:08:18.360359
```

On the Primary node:

```
Every 2.0s: csadm ha get-replication-stat
                Tue May 12 05:28:05 2020
```

Note:

```
'sending_lag' indicates load on the primary node
'receiving_lag' indicates network delay or load on the passive/se
condary node
'replaying_lag' indicates load on the passive/secondary node
```

```
node_hostname      sending_lag      receiving_lag      replayin
g_lag      total_lag
-----
hasecondary.mydomain 2774 MB        5632 kB        1273 MB
                4052 MB
```

On the Secondary node:

```
Every 2.0s: csadm ha get-replication-stat
                Tue May 12 05:28:07 2020
```

```
primary_hostname      total_lag      time_elapsed_from_last_syn
c
-----
haprimary.mydomain    1486 MB        00:07:35.238068
```

On the Primary node:

```
Every 2.0s: csadm ha get-replication-stat
                Tue May 12 05:28:28 2020
```

Note:

```
'sending_lag' indicates load on the primary node
```

'receiving\_lag' indicates network delay or load on the passive/secondary node

'replaying\_lag' indicates load on the passive/secondary node

```
-----
node_hostname      sending_lag    receiving_lag    replayin
g_lag    total_lag
-----
-----
hasecondary.mydomain 1910 MB        6784 kB        1803 MB
3719 MB
```

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:28:29 2020

```
primary_hostname    total_lag    time_elapsed_from_last_syn
c
-----
---
haprimary.mydomain 1952 MB        00:07:56.70475
```

On the Primary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:28:44 2020

Note:

'sending\_lag' indicates load on the primary node

'receiving\_lag' indicates network delay or load on the passive/secondary node

'replaying\_lag' indicates load on the passive/secondary node

```
-----
node_hostname      sending_lag    receiving_lag    replayin
g_lag    total_lag
-----
-----
hasecondary.mydomain 1153 MB        1408 kB        2278 MB
3433 MB
```

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:28:39 2020

primary_hostname	total_lag	time_elapsed_from_last_sync
-----	-----	-----
---		
haprimary.mydomain	2286 MB	00:07:04.28739

On the Primary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:29:00 2020

Note:

'sending\_lag' indicates load on the primary node

'receiving\_lag' indicates network delay or load on the passive/secondary node

'replaying\_lag' indicates load on the passive/secondary node

node_hostname	sending_lag	receiving_lag	replaying_lag
total_lag			
-----	-----	-----	-----
-----			
hasecondary.mydomain	452 MB	3200 kB	2726 MB
3181 MB			

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:29:12 2020

primary_hostname	total_lag	time_elapsed_from_last_sync
-----	-----	-----
---		
haprimary.mydomain	2941 MB	00:07:33.857054

On the Primary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:29:25 2020

-----  
Note:

'sending\_lag' indicates load on the primary node

'receiving\_lag' indicates network delay or load on the passive/secondary node

'replaying\_lag' indicates load on the passive/secondary node  
-----

node_hostname	sending_lag	receiving_lag	replaying_lag	total_lag
hasecondaory.mydomain	0 bytes	0 bytes	2658 MB	2658 MB

-----

-----

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:29:30 2020

primary_hostname	total_lag	time_elapsed_from_last_sync
haprimary.mydomain	2519 MB	00:06:48.870481

-----

-----

On the Primary node:

Every 2.0s: csadm ha get-replication-stat

Tue May 12 05:29:46 2020

-----  
Note:

'sending\_lag' indicates load on the primary node

'receiving\_lag' indicates network delay or load on the passive/secondary node

'replaying\_lag' indicates load on the passive/secondary node  
-----

node_hostname	sending_lag	receiving_lag	replaying_lag	total_lag
hasecondaory.mydomain	0 bytes	154 kB	2172 MB	2172 MB

-----

-----

On the Secondary node:

```

Every 2.0s: csadm ha get-replication-stat
                Tue May 12 05:29:53 2020

primary_hostname      total_lag      time_elasped_from_last_syn
c
-----
---
haprimary.mydomain  1985 MB      00:07:11.244842

On the Primary node:

Every 2.0s: csadm ha get-replication-stat
                Tue May 12 05:30:06 2020

-----
Note:
'sending_lag' indicates load on the primary node
'receiving_lag' indicates network delay or load on the passive/se
condary node
'replaying_lag' indicates load on the passive/secondary node
-----

node_hostname      sending_lag      receiving_lag      replayin
g_lag      total_lag
-----
-----
hasecondary.mydomain  0 bytes      0 bytes      1687 MB
1687 MB

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat
                Tue May 12 05:30:11 2020

primary_hostname      total_lag      time_elasped_from_last_syn
c
-----
---
haprimary.mydomain  1552 MB      00:06:25.877238

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat
                Tue May 12 05:30:57 2020

```

```

primary_hostname      total_lag      time_elapsed_from_last_syn
c
-----
---
happrimary.mydomain  2288 bytes    00:00:55.861428

On the Secondary node:

Every 2.0s: csadm ha get-replication-stat
                        Tue May 12 05:31:23 2020

primary_hostname      total_lag      time_elapsed_from_last_syn
c
-----
---
happrimary.mydomain   0 bytes       00:00:19.235799

```

## Troubleshooting

To troubleshoot HA issues, you can use the HA log located at: `/var/log/cyops/cyops-auth/ha.log`. To understand and troubleshoot the HA cluster health notifications, see the [Monitoring health of HA clusters](#) section.

### Failure to create an HA cluster

If the process to configure HA using the automated join cluster fails, and the HA cluster is not created due to reasons such as, proxies set up etc, you can perform the steps mention in the following procedure and configure HA:

1. Connect to your VM as a *root* user and run the following command:  
`# csadm ha`  
 This will display the options available to configure HA.
2. To configure a node as a secondary node, perform the following steps:
  - a. SSH to the active primary node and run the `csadm ha export-conf` command to export the configuration details of the active primary node to a configuration file named `ha.conf`.  
 You must copy the `ha.conf` file from the active primary node to the node that you want to configure as a secondary node.
  - b. On the active primary server, add the hostnames of the secondary nodes to the allowlist, using the following command:  
`# csadm ha allowlist --nodes`  
 Add the comma-separated list of hostnames of the cluster nodes that you want to add to the allowlist after the `--nodes` argument.  
**Important:** In case of an externalized database, you need to add all the nodes in a cluster to the allowlist in the `pg_hba.conf` file.



- c. Ensure that all HA nodes are resolvable through DNS and then SSH to the server that you want to configure as a secondary node and run the following command:  

```
# csadm ha join-cluster --status <active, passive> --role <primary, secondary> --conf <location of the ha.conf file>
```

  
For example, 

```
# csadm ha join-cluster --status passive --role secondary --conf tmp/ha.conf
```

  
This will add the node as a secondary node in the cluster.  
**Note:** If you run the `csadm ha join-cluster` command without adding the hostnames of the secondary nodes to the allowlist, then you will get an error such as, `Failed to verify...`  
Also, when you join a node to an HA cluster, the `list-nodes` command does not display that a node is in the process of joining the cluster. The newly added node will be displayed in the `list-nodes` command only after it has been added to the HA cluster.

## Unable to add a node to an HA cluster using join-cluster, and the node gets stuck at a service restart

This issue occurs when you are performing `join-cluster` of any node and that node sticks at service restart, specifically at PostgreSQL restart.

### Resolution

Terminate the `join-cluster` process and retry `join-cluster` using an additional parameter `--fetch-fresh-backup`.

## Fixing the HA cluster when the Primary node of that cluster is halted and then resumed

If your primary node is halted due to a system crash or other such events, and a new cluster is made with the other nodes in the HA cluster, the `list-nodes` command on other nodes will display that the primary node is in the `Faulted` state. Since the administrator has triggered takeover on other cluster nodes, the administrator will be aware of the faulted primary node. Also, note that even after the primary node resumes, post the halt, the primary node still remains the primary node of its own cluster, and therefore, after the resume, the `list-nodes` command on the primary node will display this node as `Primary Active`.

### Resolution

To fix the HA cluster to have only one node as primary active node, do the following:

1. On the primary node, which got resume, run `leave-cluster`, which will remove this node from the HA cluster.

2. Run `join-cluster` command to join this node to the HA cluster with the new primary node.

## Unable to join a node to an HA cluster when a proxy is enabled

You are unable to join a node to an HA cluster using the `join-cluster` command when you have enabled a proxy using which clients should connect to the HA cluster.

### Resolution

Run the following commands on your primary node:

```
$ sudo firewall-cmd --zone=trusted --add-source=<CIDR> --add-port=<ElasticSearchPort>/tcp --permanent
```

```
$ sudo firewall-cmd --reload
```

For example,

```
$ sudo firewall-cmd --zone=trusted --add-source=64.39.96.0/20 --add-port=9200/tcp --permanent
```

```
$ sudo firewall-cmd --reload
```

## Changes made in nodes in an active-active cluster fronted with a load balancer take some time to reflect

In the case of a FortiSOAR™ active-active cluster that is fronted with a load balancer or reverse proxy such as an HAProxy, changes such as, adding a module to the FortiSOAR™ navigation, updating or adding the permissions of the logged-in user, or updates done to the logged-in user's parents, child, and sibling hierarchy, do not get reflected immediately.

These issues occur due to local caching of these settings at the individual cluster nodes.

### Resolution

Log off and log back into the FortiSOAR™ user interface after ten minutes to see the recent updates.

### OR

If you want the settings to reflect immediately, run the following command on the "active" nodes in the cluster:

```
php /opt/cyops-api/app/console --env=prod redis:flushdb --env=prod --quiet
```

**Important:** You do not require to run the above command on the "passive" nodes of the cluster.

## Post Takeover the nodes in an HA cluster do not point to the new active primary node

This issue occurs when during the takeover process either the previous primary node is down or automatic join-cluster fails. In case of an internal database cluster, when the failed primary node comes online after the takeover, it still thinks of itself as the active primary node with all its services running. In case of an external database cluster, when the failed primary node comes online after the takeover, it detects its status as "Faulted" and disables all its services.

### Resolution

Run the `csadm ha join-cluster` command to point all the nodes to the new active primary node. For details on `join-cluster`, see [Process for configuring HA](#).

# Elasticsearch Configuration

## Introduction

FortiSOAR™ leverages the fast search capability of Elasticsearch for quick text search across all records and files in the FortiSOAR™ database. FortiSOAR™ supports externalization of Elasticsearch data. Externalization is indexing of data to an Elasticsearch instance that has the same or higher version of Elasticsearch outside of the FortiSOAR™ virtual appliance; the steps for which are covered in this chapter.

**Important:** The minimum version of your Elasticsearch cluster must be 7.0.2, if you want to externalize your ElasticSearch data.

If you want to externalize your other FortiSOAR™ PostgreSQL database, see the *Externalization of your FortiSOAR™ PostgreSQL database* chapter.

## Externalization and Authentication of Elasticsearch

If you require to change the location of your Elasticsearch instance from your local instance to a remote machine, you need to update the `db_config.yml` file, which is located at: `/opt/cyops/configs/database/db_config.yml`

In the `db_config.yml` file, you require to update the host and port (if needed) in the `elasticsearch` section that appears as follows:

```
elasticsearch:
  es_host: localhost
  es_port: 9200
  es_user: None
  initial_backoff: 60
  max_backoff: 6000
  secret: None
  ssl_cert_path: ""
  use_ssl: false
```

To change the location of your Elasticsearch instance from your local instance to a remote machine:

`es_host: localhost` > Update host value with the hostname or IP address of the remote Elasticsearch machine.

`es_port: 9200` > Update the port required to access the remote Elasticsearch machine, if required.

For authentication of Elasticsearch (require X-Pack License):

`es_user: None` > Update the username that is used to access the remote Elasticsearch machine, if Authentication is enabled on the remote Elasticsearch machine

`secret: None` > Update the secret (password) that is used to access the remote Elasticsearch machine, if Authentication is enabled on the remote Elasticsearch machine.

You also require to assign `nginx` permission to the SSL certificate that you have specified in the `db_config.yml` file using the following command:

```
chown nginx:nginx filename.pem
```

## Migration of Elasticsearch data

Once you complete the externalization of Elasticsearch, you will require to migrate your data from your local instance to the remote Elasticsearch machine.

To migrate the remote Elasticsearch machine run the following command on your FortiSOAR™ instance as a `root` user:

```
$ sudo -u nginx php /opt/cyops-api/app/console cybersponse:elastic:create --env="prod"
```

## Troubleshooting

### FortiSOAR™ Search Errors

FortiSOAR™ Search performs indexing in an asynchronous fashion in the backend. Users could be faced with certain scenarios that could lead to a restart of services, which can cause indexing to stop. In this case, FortiSOAR™ might display any of the following errors when users are performing a search operation on FortiSOAR™:

- Search indexing is in progress. Partial results are returned.
- Search indexing has stopped. You must manually rerun indexing (see product documentation for instructions) or raise a support ticket for the same.
- We are sorry, but the server encountered an error while handling your search request. Please contact your administrator for assistance.

In this case, use the `/var/log/cyops/cyops-search/falcon.log` log file to check which modules are published and indexed and which modules are yet to be published (pending).

For example, the `/var/log/cyops/cyops-search/falcon.log` log file will display results as follows:

```
2019-02-13,11:00:44 INFO blocking_connection: _dispatch_events():  
1445: Module Currently Getting Published: ['attachments']
```

```
2019-02-13,11:00:44 INFO blocking_connection: _dispatch_events():
1445: Indexing for Module: 'attachments' started Total Records to
be indexed: '1'
2019-02-13,11:00:49 INFO blocking_connection: _dispatch_events():
1445: Module: 'attachments' Successful Total Records indexed: '1'
,
2019-02-13,11:00:49 INFO blocking_connection: _dispatch_events():
1445: on_publish_message called
2019-02-13,11:00:53 INFO blocking_connection: _dispatch_events():
1445: creating index with mapping
2019-02-13,11:01:00 INFO blocking_connection: _dispatch_events():
1445: Module Currently Getting Published: ['emails']
2019-02-13,11:01:02 INFO blocking_connection: _dispatch_events():
1445: Indexing for Module: 'emails' started Total Records to be
indexed: '1'
2019-02-13,11:01:04 INFO blocking_connection: _dispatch_events():
1445: Module: 'emails' Successful Total Records indexed: '1'
```

The above example shows the `attachments` and `emails` modules currently being indexed and its total number of records. Any failure in indexing any modules will be logged here. You can monitor the progress of this file while the indexing is in progress.

If any module(s) are missing from the published list or if any module has the `Publish Module: '<name of module>' Unsuccessful` listed in the `/var/log/cyops/cyops-search/falcon.log` log file; the `indicators` and `tasks` modules in our example, then you must manually run the indexing for those module(s) using the following command:

```
$ sudo -u nginx php app/console cybersponse:elastic:create --env="prod" --
index='{ "type":["<list of comma-seperated module names that require to be
indexed>"] }
```

For our example, run the following command:

```
$ sudo -u nginx php app/console cybersponse:elastic:create --env="prod" --
index='{ "type":["indicators","tasks"] }'
```

## Externalization of your FortiSOAR™ PostgreSQL database

This chapter explains the steps required to externalize your FortiSOAR™ PostgreSQL database. For information about ElasticSearch configuration, including ElasticSearch externalization, see the *ElasticSearch Configuration* chapter.

Externalization is migration of data from your local database instance to a remote database instance that has same version of PostgreSQL, outside of the FortiSOAR™ virtual appliance.

To externalize your FortiSOAR™ PostgreSQL database you must have *root access* on your FortiSOAR™ system and you must use the FortiSOAR™ Admin CLI (`csadm`). For more information on `csadm`, see the *FortiSOAR™ Admin CLI* chapter in the “Administration Guide.”

### Prerequisites

- Prepare your Remote instance:
  - Remote instance must allow inbound communication from your FortiSOAR™ local Virtual Machine.
  - Remote instance must have PostgreSQL version 12.
- Prepare your Local FortiSOAR™ instance:
  - Ensure that port 5432 is opened for PostgreSQL to allow inbound and outbound communication with the remote instance.
- Ensure that the connectivity between your FortiSOAR™ local instance and remote PostgreSQL instance is established.
- If the FortiSOAR™ instance was connected previously to the same instance of the database that is being externalized, it could lead to a stale connection being 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>`
- Ensure that you have stopped all your schedules and that you have no playbooks in the running state.

**Note:** Ensure that you have enough disk space available to perform DB externalization tasks. It is recommended that you have available disk space of around 3X of the data size, for example, if your data size is 2GB, then you should have around 6GB of available disk space, to ensure that the processes do not stop or fail.

## Externalizing FortiSOAR™ databases

1. Create the `db_external_config.yml` file at the following location  
`/opt/cyops/configs/database/`  
Use the following command to create the `db_external_config.yml` file:  

```
# cp /opt/cyops/configs/database/db_config.yml  
/opt/cyops/configs/database/db_external_config.yml
```
2. Update the newly created `db_external_config.yml` file for PostgreSQL as follows:  
In the `postgres` section:
  - a. Set the `pg_external` parameter to "true".  
This parameter determines whether or not the postgres database needs to be externalized. If it is set to "true", then the postgres database is externalized, and if set to "false" (default), then the postgres database is not externalized.
  - b. Update the value of the postgres host (`pg_host`) and postgres port (`pg_port`) (if needed) parameters.
  - c. Add the encrypted password that you have set on your remote PostgreSQL server in the `pg_password` parameter.  
You can encrypt your PostgreSQL passwords by running the `csadm db --encrypt` command as a `root` user. For more information on `csadm`, see the *FortiSOAR™ Admin CLI* chapter.
3. On the externalized PostgreSQL database run the following commands:
  - a. To ensure that the PostgreSQL server allows connections, open the firewall port:  

```
# firewall-cmd --add-service=postgresql --permanent  
# firewall-cmd --reload
```
  - b. To ensure that the `pg_hba.conf` file, trusts the FortiSOAR™ server for incoming connections:  
Add the following entry to the file `/var/lib/pgsql/12/data/pg_hba.conf` file:  

```
host    all         all         ip/subnetmask      trust
```

  
For example, if the ip/subnetmask of your externalized PostgreSQL database is `xxx.xxx.xxx.xxx/xx` then add the following to the `pg_hba.conf` file:  

```
host    all         all         xxx.xxx.xxx.xxx/xx trust
```
  - c. To ensure that the `postgresql.conf` file, trusts the FortiSOAR™ server for incoming connections:  
Make the following changes to the `/var/lib/pgsql/12/data/postgresql.conf` file:  

```
listen_addresses = '*'  
port = 5432
```
  - d. Restart PostgreSQL using the following command:  

```
# systemctl restart postgresql-12
```
  - e. Create a `cyberpgsql` user using the following commands:  

```
# psql -U postgres -c "CREATE USER cyberpgsql WITH SUPERUSER  
PASSWORD '<password>'"
```
4. SSH to your FortiSOAR™ VM and login as a `root` user.



5. Check the connectivity between the FortiSOAR™ local instance and remote PostgreSQL database using the `csadm db --check-connection` command.
6. To externalize the PostgreSQL database, type the following command:  
`# csadm db --externalize`  
Once you run the above command, you will be asked to provide the path in which you want to save your database backup file.  
**Note:** If you run the `# csadm db --externalize` option more than once (i.e., you are running the option again after the first time), then `csadm` will display a message such as:  
The databases already exist in postgresql, do you want to delete these databases (y/n): If you want to externalize your PostgreSQL database again you must type y.
7. After you have completed externalizing your PostgreSQL database, you should restart your schedules.

## Setting up an externalized database on the cloud

If you want to set up your externalized database on the cloud, for example AWS, do the following:

1. Set up your AWS RDS with its default port, i.e., **5432** and **postgresql-12.1**.
2. Setup the master password for the PostgreSQL user.
3. Ensure that your FortiSOAR™ system is able to access the RDS system using RDS endpoint, for which you might have to update security groups in AWS RDS. Check the connectivity between FortiSOAR™ and RDS systems using the `telnet` command and using the following psql command:  
`psql -h <pg_hostname> -U <pg_username> -p <port_no> -l postgres`
4. Once the connectivity is verified, create the `db_external_config.yml` file at the following location:  
`/opt/cyops/configs/database/`
5. Navigate to `/opt/cyops/configs/database/` and then run the following command:  
`cp db_config.yml db_external_config.yml`
6. Edit the `db_external_config.yml` file and update the postgres section as mentioned in the [Externalizing FortiSOAR™ databases](#) section.  
You need to encrypt the password using the following command:  
`csadm db -encrypt`
7. Connect to the RDS system to create a user:  
`psql -h <pg_hostname> -U <pg_username> -p <port_no> -d postgres`
8. Create the `cyberpsql` user in the RDS system using the following command:  
`CREATE USER cyberpsql WITH PASSWORD '<your password>' CREATEROLE CREATEDB`
9. Grant appropriate access to the `cyberpsql` user using the following command:  
`GRANT cyberpsql TO postgres;`
10. Exit the psql shell.

11. To externalize the PostgreSQL database, type the following command:

```
# csadm db --externalize
```

This command takes some time for completion.

**Note:** Performance differences might be seen in cases where there is high network latency between the FortiSOAR™ and RDS systems.

## Troubleshooting DB Externalization issues

### Unable to log onto FortiSOAR™ if the IP of the externalized PostgreSQL database changes

If the IP of the externalized PostgreSQL database has changed, in cases such as crashing of the Postgres server, then you might not be able to log onto FortiSOAR™.

#### Resolution

1. Update the PostgreSQL database IP to the new IP in the `db_config.yml` and the `db_external_config.yml` files. These files are present in the `/opt/cyops/configs/database` folder.
2. Update the PostgreSQL database IP to the new IP in the `appProdProjectContainer.php` file located at `/opt/cyops-api/app/cache/prod/appProdProjectContainer.php`.
3. Run the following command:  

```
$ sudo -u nginx php /opt/cyops-api/app/console cache:clear --env=prod
```

## Backing up and Restoring FortiSOAR™

This chapter describes the process of backing up and restoring FortiSOAR™, whether or not you have not externalized your PostgreSQL database.

### Prerequisites

You must have the `root` or `sudo` permissions to perform backup and restore.

**Note:** Ensure that you have enough disk space available to perform backup and restore tasks. It is recommended that you have available disk space of around 3X of the data size, for example, if your data size is 2GB, then you should have around 6GB of available disk space, to ensure that the processes do not stop or fail.

### Backup Process

Use the FortiSOAR™ Admin CLI (`csadm`) `data` option to regularly perform backups and restore, which restores the data seamlessly to a new FortiSOAR™ environment. To perform backup and restore, you must have *root access* on your FortiSOAR™ system. For more information on `csadm`, see the *FortiSOAR™ Admin CLI* chapter in the “Administration Guide.”

The FortiSOAR™ Admin CLI performs a full database backup of your FortiSOAR™ server each time and the backup is an encrypted backup. There is no provision of incremental backups. Backups are performed for a particular version of FortiSOAR™, and backups should be restored on the exact versions of FortiSOAR™. If a newer version of FortiSOAR™ is available and you want to move to that newer version of FortiSOAR™, you must restore the backed-up version only and then upgrade to the latest FortiSOAR™ version. This is to ensure that all the new changes will be present.

**Important:** The FortiSOAR™ Admin CLI backs up the latest three backups every time it creates a new backup. Any backups older than the latest three backups are deleted.

### Data that is backed up during the backup process

The FortiSOAR™ Admin CLI backs up the following files, configurations, and data during the backup process:

- site-packages
- connectors
- application.conf
- db\_config.yml
- pg\_hba.conf

- PostgreSQL database backups as per requirements

**Note:** Backup of the configuration files are taken only in case of localized databases.

## Prerequisites to running the backup process

You must have the NFS or local backup storage path.

## Performing a backup

To perform a backup run the `csadm` command on any FortiSOAR™ machine using any terminal. A user who has `root` or `sudo` permissions can run the `csadm` command.

1. SSH to your FortiSOAR™ VM and login as a `root` user.
2. To perform a backup, type the following command:  

```
# csadm db --backup [<BACKUP_DIR_PATH>]
```

[<BACKUP\_DIR\_PATH>] is the directory where backup files will be created. If you do not specify the path of the backup file in the above file, then the CLI will interactively ask you to provide the path of the backup file. If you do not specify any path, then by default, the backup file is stored in the current working directory.

Optionally, from version 6.4.3 onwards, you can specify the `--exclude-workflow` option to exclude all the "Executed Playbook Logs" from the backup. Executed playbook logs are primarily meant for debugging so they are not a very critical component to be backed up. However, they constitute a major part of the database size, so excluding them from the backup reduces time and space needed for the backup. To exclude all the "Executed Playbook Logs" from the backup, type the command as follows:  

```
# csadm db --backup [<BACKUP_DIR_PATH>] --exclude-workflow
```

**Important:** FortiSOAR™ backs up the latest three backups every time it creates a new backup. Any backups older than the latest three backups are deleted.
3. (Optional) If you only want to backup only your configuration files, then type the following command:  

```
# csadm db --backup-config [<BACKUP_DIR_PATH>]
```

Once you run the above command, you will be asked to provide the path of the configuration backup file. If you do not specify any path, then by default, the backup file is stored in the current working directory

## Running a backup as a scheduled job

Following is an example of running a backup as a scheduled cron job, on your FortiSOAR™ system, that will run at 12:30 am every day. You can schedule the backup process based on your requirements.

Add the cron job to run at 12:30 am every day as follows:

```
$ sudo crontab -e
30 00 * * * csadm db --backup <path_of_backup_file>
```

Once the backup process is successfully completed, the final `DR_BACKUP_<FortiSOAR_version>_timestamp.tgz` file is located in the directory where the backup files are created. It would be the same directory that you have specified when you ran the `csadm db --backup <path_of_backup_file>` command. The `DR_BACKUP_<FortiSOAR_version>_timestamp.tgz` file includes the timestamp on when the backup is created.

The `DR_BACKUP_<FortiSOAR_version>_timestamp.tgz` file includes all the backup files. You can run the following command to check the contents of the `DR_BACKUP_<FortiSOAR_version>_timestamp.tgz` file:

```
# tar -tvf <DR_BACKUP_<FortiSOAR_version>_timestamp.tgz>
```

## Restore process

To restore the data on a new FortiSOAR™ server run the `csadm` command on any FortiSOAR™ machine using any terminal. A user who has `root` or `sudo` permissions can run the `csadm`

### Restoring data

1. Move the backup file to the new FortiSOAR™ server.
2. SSH to the new FortiSOAR™ VM and login as a `root` user.
3. To restore the data, type the following command:

```
# csadm db -restore
```

Once you hit enter after this command, you have to provide the the path of the database backup file. Note that the backup process stores the backup in a locally saved file: `/home/csadmin/db_backup/DR_BACKUP_<yyyymmdd_hhmmss>.tgz`

**Important:** Once you have restored FortiSOAR™, you are required to get and deploy a new license for this FortiSOAR™ instance. Your existing license will not work on the restored instance. For the procedure to get a new license, see the *Licensing FortiSOAR™* chapter in the "Deployment Guide."

If you have backed up a FortiSOAR™ instance has a Secure Message Exchange enabled and is using a signed certificate, then you would need to re-apply the signed certificate on the new instance. For steps on how to replace certificates, see the *Replacing the self-signed certificates on the secure message exchange with signed certificates* topic in the "Multi-tenancy support in FortiSOAR™ Guide."

If the restore is done on a machine that has a different FQHN, you will need to update the master FQHN at any tenant nodes or agents, which are connected through this secure message exchange. You can either update the tenant nodes or agents manually on the respective remote nodes, or download the installer file again from the master

and apply on the remote nodes. For more information, see the *Segmented Network support in FortiSOAR™* chapter.

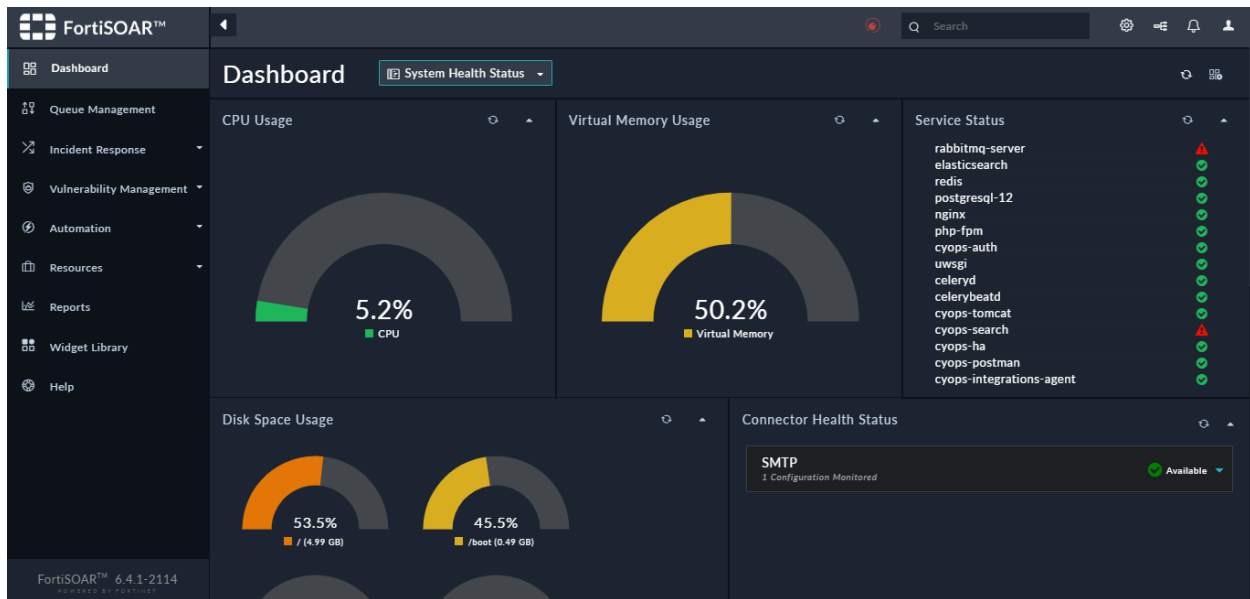
## Backup and Restore process for FortiSOAR™ High Availability systems

You can backup and restore your High Availability (HA) systems, if for example, your primary database gets corrupted, using the following steps:

1. Configure backup on your primary database. Steps for which are mentioned in the [Backup Process](#) section.
2. Remove the secondary nodes from the HA cluster using the `csadm ha leave-cluster` command. For more information on the HA and the `csadm ha` CLI, see the High Availability support in FortiSOAR™ chapter in the "Administration Guide."
3. Restore the primary database. Steps for which are mentioned in the [Restore Process](#) section.
4. Add the secondary nodes back to the HA cluster using the `csadm ha join-cluster` command.

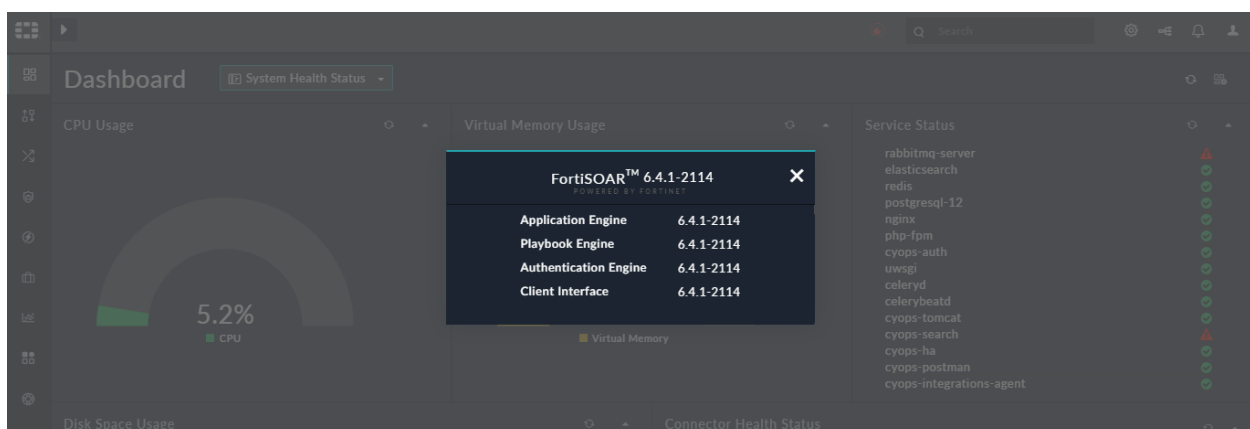
## About FortiSOAR™

The left-navigation panel contains a link that includes the version and build number of FortiSOAR™ that is installed in your environment. For example, in the following image, the version of FortiSOAR™ installed is 6.4.1, and the build number is 2114:



**Figure 75.** *About FortiSOAR™ link*

Clicking on the **FortiSOAR™ Version Number Build number** link, for example, **FortiSOAR™ 6.4.1-2114** link in the above image displays the version information of four major components of FortiSOAR™, which are: Application Engine, Playbook Engine, Authentication Engine, and Client Interface.



**Figure 76.** *About FortiSOAR™ dialog*

You can use the information presented in the FortiSOAR™ dialog, in the following cases:

- If you require some issue resolution or feature enhancement, then you might need to know the exact version of FortiSOAR™ installed in your environment, since the fix or enhancement might vary based on the version.
- There can be instances where you require only a component, for example, Client Interface, within FortiSOAR™ to be updated. In such cases, you might need to know the versions of all the components in your FortiSOAR™ system.



## Monitoring FortiSOAR™

### Overview

Administrators can monitor various important aspects of their FortiSOAR™ system such as uptime (availability) of FortiSOAR™, monitoring databases, services, disk space utilization, CPU and Memory utilization, etc.

The "System Health Status" Dashboard, monitoring playbooks, and the High Availability (HA) notifications that FortiSOAR™ sends already monitor various elements of the FortiSOAR™ system and also send appropriate notifications to users. This chapter intends to provide more details on what are the various aspects that can be monitored in case you want to fine tune the monitoring and/or setup monitoring using custom tools.

You can set up the system monitoring and purging of audit and playbook logs as part of your initial deployment and configuration process. For more information, see the *Setting up monitoring for your FortiSOAR™ system* in the *Additional configuration settings for FortiSOAR™* chapter of the "Deployment Guide."

You can also set up system monitoring for FortiSOAR™, both in case of a single node system and High Availability (HA) clusters. You can also receive monitor the system and get email notifications for failures of any FortiSOAR™ service, or if any monitored thresholds exceed the set threshold. In case of HA clusters, in addition, you can also monitor and get notified in case of heartbeat failures and high replication lags between nodes of your HA cluster. For more information, see the *Configuring System and Cluster Health Monitoring* topic in the *System Configuration* chapter.

For the list of logs that you can use for troubleshooting FortiSOAR™, see the *Debugging, Troubleshooting, and optimizing FortiSOAR™* chapter.

For information on monitoring the secure message exchange, see the *Monitoring the connectivity of the different nodes at the secure message exchange* topic in the "Multi-tenancy support in FortiSOAR™ Guide."

### Benefits of monitoring

Implementing effective application monitoring offers the following benefits:

- Increased server, services, and application availability.
- Faster detection of network outages and protocol failures.
- Faster detection of failed services, processes, and scheduled jobs.

## Setting up monitoring

To monitor various components of your FortiSOAR™ system, you need to SSH to your FortiSOAR™ VM and login as a user who has `root` or `sudo` permissions and then run the commands mentioned in the following sections.

### Monitoring uptime of FortiSOAR™

Run the `uptime` command.

You can also get the latest health check details for your FortiSOAR™ system. By default, the FortiSOAR™ health check runs every 5 minutes. For more information, see the System Configuration chapter.

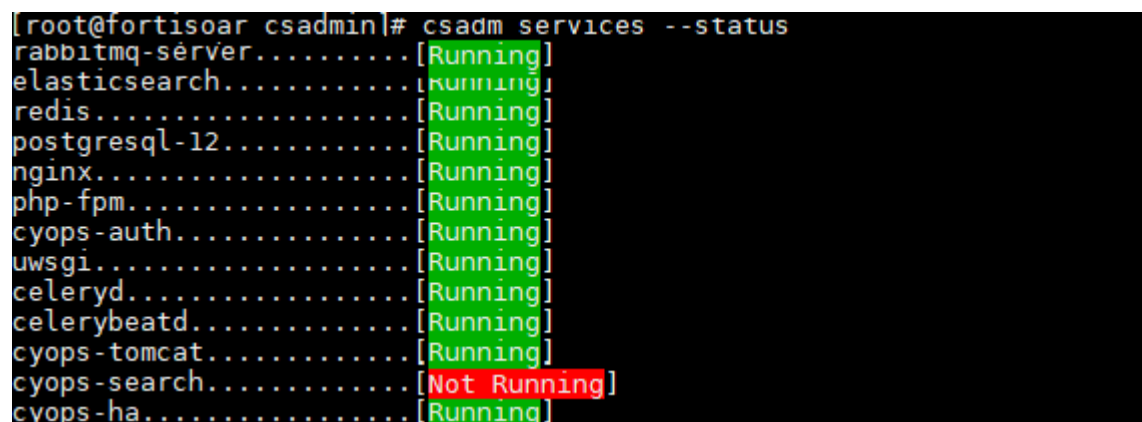
### Monitoring FortiSOAR™ services

To know the status of all FortiSOAR™ services run the `# csadm services --status` command.

To view the status of individual FortiSOAR™ services, run the `# systemctl status <service_name>` command. For example, to see the status of the `nginx` service, use the `# systemctl status nginx` command.

When you run `# csadm services --status` command the status of FortiSOAR™ services are displayed with a background color so that you can quickly and easily identify which services are running and which are not running. The status of services that are running are displayed in a Green background, and the status of services that are not running are displayed in a Red background.

Following image displays how the statuses of FortiSOAR™ services are displayed when some services are running, and some are not running:



```
[root@fortisoar csadmin]# csadm services --status
rabbitmq-server.....[Running]
elasticsearch.....[Running]
redis.....[Running]
postgresql-12.....[Running]
nginx.....[Running]
php-fpm.....[Running]
cyops-auth.....[Running]
uwsgi.....[Running]
celeryd.....[Running]
celerybeatd.....[Running]
cyops-tomcat.....[Running]
cyops-search.....[Not Running]
cyops-ha.....[Running]
```

**Figure 77.** Status of FortiSOAR™ services

You can also use the "System Monitoring" widget to monitor various FortiSOAR™ system resources such as CPU, Disk Space and memory utilization and status of various FortiSOAR™ services. FortiSOAR™ includes a default system monitoring dashboard, the "System Health Status" Dashboard, that displays the usage and health of various components in your FortiSOAR™ system. For more information on the System Monitoring widget, see the *Dashboards, Templates, and Widgets* chapter in the "User Guide."

## Monitoring databases

To know the status of your PostgreSQL database run the `systemctl status postgresql-$(psql --version | egrep -o '[0-9]{1,}\.' | cut -d'.' -f1) -l` command.

To know the status of your Elasticsearch database run the `systemctl status elasticsearch` command.

## Monitoring Disk Space Utilization

```
$ sudo df -H | grep -vE '^Filesystem|tmpfs|cdrom' | awk '{ print $5 " " $1 }'  
44% /dev/mapper/cybersponse-root  
10% /dev/mapper/cybersponse-var  
2% /dev/mapper/cybersponse-tmp  
16% /dev/mapper/rpmdata-cs--apps  
2% /dev/mapper/cybersponse-log  
1% /dev/mapper/esdata-search  
1% /dev/mapper/pgdata-relations  
1% /dev/mapper/cybersponse-redis  
1% /dev/mapper/cybersponse-rabbitmq  
8% /dev/mapper/cybersponse-audit  
17% /dev/sda1  
1% /dev/mapper/cybersponse-home  
$
```

You can also use the System Monitoring widget and the "System Health Status" Dashboard to monitor the disk space utilization.

## Monitoring CPU and Memory Utilization

```
#Top 50 process with memory and CPU usage
$sudo ps -eo pid,cmd,%mem,%cpu --sort=-%mem | head -50

#RAM and Swap memory usage command
free -m
```

You can also use the System Monitoring widget and the "System Health Status" Dashboard to monitor the CPU and memory utilization.

## Monitoring connectors

Use the "Connector Health" widget to track the health of all the configurations of all your configured connectors. You can view the status of your connector configurations using the "System Health Status" Dashboard.

You can also retrieve the health status of any connector configuration using the following API call:

```
GET
/api/integration/connectors/healthcheck/<name>/<version>/?config=<config_id>
For example, GET
/api/integration/connectors/healthcheck/smtp/2.3.3/?config=88c3d39c-2fa9-4731-b00d-29815008f17c
```

Following are additional APIs around connectors and configurations:

- GET /api/integration/connectors: Use this API to list all connectors installed on a FortiSOAR™ instance
- GET /api/integration/connectors/<name>/<version>: Use this API to list all configurations for a connector

For information on authenticating and invoking FortiSOAR™ APIs, see the "API Guide."

## Monitoring workflows

To know the number of workflows that are queued and not yet picked up for execution use the following command:

```
redis-cli -n 11 -h localhost -p 6379 -a $hkey llen celery
```

The number returned by this command should be 0, or at the maximum within two digits. If this number remains high for long, it means that the workflow engine is not able to cope up with the requests and requires to be tuned or you need to scale horizontally. For

information on tuning workflows, see the Debugging, Troubleshooting, and optimizing FortiSOAR™ chapter and Debugging and Optimizing Playbooks in the "Playbooks Guide."

# Debugging, Troubleshooting, and optimizing FortiSOAR™

## Overview

Administrators can use various logs that FortiSOAR™ generates to troubleshoot FortiSOAR™ issues. This chapter lists the key FortiSOAR™ services and processes and also provides some troubleshooting tips. This chapter also provides some additional configuration settings so that you can tune the results that get displayed by FortiSOAR™ for record similarity and field prediction. For more information on record similarity and field prediction, see the *Working with Modules - Alerts & Incidents* chapter in the “User Guide.”

If you face any issues while deploying or upgrading FortiSOAR™, see the *Troubleshooting FortiSOAR™* chapter in the “Deployment Guide.” If you face deployment or upgrade failures due to insufficient space, or if you face issues while using FortiSOAR™ that might be caused due to insufficient space, like you are unable to log into FortiSOAR™ or FortiSOAR™ services stop working, then see the *Issues occurring in FortiSOAR™ due to insufficient space* section in the *Troubleshooting FortiSOAR™* chapter in the “Deployment Guide.”

## List of logs used for troubleshooting FortiSOAR™

FortiSOAR™ log files are stored in the following location: `/var/log/cyops`. You will find the following directories in the `/var/log/cyops` location:

### Log Name

`cyops-api/ssl_cyops_api_access.log`

`cyops-api/ssl_cyops_api_error.log`

`cyops-api/prod.log`

`cyops-api/last_system_publish.log`

`cyops-auth/das.log`

### Purpose

Used for troubleshooting web (nginx) UI or API access issues.

Used for troubleshooting API errors.

Used for troubleshooting FortiSOAR™ PHP related issues.

Used for troubleshooting publishing issues. It captures the output when a publish is fired from the UI after MMD changes.

Used for troubleshooting FortiSOAR™ authentication

`cyops-auth/fdn.log`

issues.

Used for troubleshooting FortiSOAR™ license synchronization issues with FortiGuard Distribution Network (FDN).

`cyops-auth/ha.log`

Used for troubleshooting FortiSOAR™ High Availability issues.

`cyops-gateway/auditlog.log`

Used for troubleshooting FortiSOAR™ audit log issues.

`cyops-gateway/etl.log`

Used for troubleshooting FortiSOAR™ application and system-level issues.

`cyops-gateway/saml.log`

Used for troubleshooting FortiSOAR™ SAML issues.

`cyops-search/falcon.log`

Used for troubleshooting FortiSOAR™ Search issues. If you get any error when you are indexing or searching for a record in FortiSOAR™, you can use the `falcon.log` file to troubleshoot ElasticSearch issues. This log is also used for checking the status of ElasticSearch indexing.

`cyops-gateway/gateway.log`

Used for troubleshooting FortiSOAR™ Gateway issues such as, audit log page failing to load or the SSO configuration page failing to load.

`cyops-notifier/notifier.log`

Used for troubleshooting FortiSOAR™ Web Socket issues.

`cyops-workflow/beat.log`

Used for troubleshooting issues of the FortiSOAR™ Scheduler.

`cyops-workflow/celeryd.log`

Used for troubleshooting FortiSOAR™ playbook runtime issues.

`cyops-workflow/sealab.log`

Used for troubleshooting FortiSOAR™ playbook

`cyops-workflow/ssl_cyops_workflow_access.log`

`cyops-workflow/ssl_cyops_workflow_error.log`

`cyops-workflow/uwsgi.log`

`cyops-integrations/connectors.log`

`cyops-integrations/integrations.log`

`cyops-integrations/integrations/imap/listener.log`

`cyops-integrations/ssl_cyops_integrations_access.log`

`cyops-integrations/ssl_cyops_integrations_error.log`

`csadm/db.log`

`install` For example, `6.4.1-2133.log`.

`install/connectors.log`

`upgrade_fortisoar_<version_number>-<timestamp>.log` For example,  
`upgrade_fortisoar_6.4.1-2020-02-18-1558604373.log`

`install/config-vm-<timestamp>.log` For example,  
`install/config-vm-27_Nov_2018_18h_14m_34s.log`

For troubleshooting FortiSOAR™ audit log issues use the `tomcat.log` located at `/opt/cyops-tomcat/tomcat.log`.

For Centos OS level errors, use the `Messages` logs located at `/var/log/messages`.

framework issues.

Used for troubleshooting  
playbook access issues.

Used for troubleshooting  
playbook errors.

Used for troubleshooting  
FortiSOAR™ playbook and  
connector issues.

Used for troubleshooting  
FortiSOAR™ connector related  
issues.

Used for troubleshooting  
FortiSOAR™ connector  
framework issues.

Used for troubleshooting the  
IMAP connector issues.

Used for troubleshooting  
connector access issues.

Used for troubleshooting  
connector errors.

Used for troubleshooting  
database externalization  
errors.

Used for troubleshooting  
FortiSOAR™ installation  
issues.

Install logs are named  
according to the FortiSOAR™  
version and build number.

Used for troubleshooting  
connector installation issues.

Stores upgrade console log  
and you can use it to  
troubleshoot FortiSOAR™  
upgrade issues.

Used for troubleshooting  
FortiSOAR Configuration  
Wizard issues.



For troubleshooting issues related to dedicated tenant nodes or FortiSOAR agents, see the following logs:

`var/log/cyops/cyops-routing-agent/postman.log`, `var/log/cyops/cyops-routing-agent/uwsgi.log`, `var/log/cyops/cyops-routing-agent/ssl_cyops_routing_agent_error.log`, and `var/log/cyops/cyops-routing-agent/ssl_cyops_routing_agent_access.log`.

## Logging Levels

You can set the following logging levels in the log files:

- **DEBUG:** Low-level system information for debugging purposes.
- **INFO:** General system information.
- **WARNING:** Information describing a minor problem that has occurred.
- **ERROR:** Information describing a major problem that has occurred.
- **CRITICAL:** Information describing a critical problem that has occurred.

## Changing the logging levels

- For **sealab** or **workflow**:
  - a. Open the `/opt/cyops-workflow/sealab/sealab/config.ini` file and set the `WORKFLOW_LOG_LEVEL` parameter to the required logging level. For example, `WORKFLOW_LOG_LEVEL = 'INFO'`
  - b. Restart the `uwsgi` service.
- For **integrations**:
  - a. Open the `/opt/cyops-integrations/integrations/configs/config.ini` file and set the `connector_logger_level` parameter to the required logging level. For example, `connector_logger_level= 'INFO'`
  - b. Restart the `uwsgi` service.
- For **celeryd**:
  - a. Open the `/etc/celery/celeryd.conf` file and set the `CELERYD_LOG_LEVEL` parameter to the required logging level. For example, `CELERYD_LOG_LEVEL = 'INFO'`
  - b. Restart the `celeryd` service.
- For **nginx (UI), API, or php**:
  - a. Open the `/opt/cyops-api/app/config/config_prod.yml` file and set the `level` parameter to the required logging level. For example, `level = 'INFO'`
  - b. Run the `# systemctl restart php-fpm nginx` command.

## List of key FortiSOAR™ services and processes

Name of Services/Processes	Description
redis	Caching service used by the playbook engine. To know the status of this service, use the <code># systemctl status redis</code> command.
postgresql-12	Service for all application data stored in postgresql DB. To know the status of this service, use the <code># systemctl status postgresql-12</code> command.
elasticsearch	Service to bring up the elasticsearch service. To know the status of this service, use the <code># systemctl status elasticsearch</code> command.
php-fpm	Service for PHP FastCGI implementation. To know the status of this service, use the <code># systemctl status php-fpm</code> command.
uwsgi	Software application that aims at developing a full stack for building hosting services. uWSGI is named after the Web Server Gateway Interface. We host our playbook execution engine application and connector integrations applications on a uWSGI server. To know the status of uwsgi use the <code># systemctl status uwsgi</code> command.
celeryd	celeryd is used to run the playbooks asynchronously in the FortiSOAR™ playbook execution engine. To know the status of celeryd use the <code># systemctl status celeryd</code> command.
celerybeatd	celerybeatd is a playbook scheduler; used to kick off tasks at regular intervals, that are then executed by available worker nodes in the cluster. To know the status of use the <code># systemctl status celerybeatd</code> command.
cyops-auth	Service used for FortiSOAR™ authentications. To know the status of this services, use the <code># systemctl status cyops-auth</code> command.
cyops-tomcat	Service used for SSO, auditing, and websocket. To know the status of this services, use the <code># systemctl status tomcat</code> command.
cyops-search	Service used for full-text searching, finding similar records and predicting the value of fields based on similarity.
cyops-ha	Service is responsible for setting up High Availability in the FortiSOAR™ environment

cyops-postman	Service is responsible for setting up and managing FortiSOAR™'s distributed multi-tenant setup.
cyops-integrations-agent	Service is responsible for running actions on remote FortiSOAR agents.
rabbitmq-server	Service is responsible to send audit and live sync notifications. This service is also responsible for data transfer in a distributed environment.
nginx	Service used for Web UI. To know the status of this services, use the <code># systemctl status nginx</code> command.

If you want to restart, start, or stop all the services together, use FortiSOAR™ Admin CLI (`csadm`). For more information on `csadm`, see the *FortiSOAR™ Admin CLI* chapter.

You can run the `csadm` command on any FortiSOAR™ machine using any terminal. Any user who has `root` or `sudo` permissions can run the `csadm` command.

To restart FortiSOAR™ services, type: `# csadm services --restart`

To start FortiSOAR™ services, type: `# csadm services --start`

To stop FortiSOAR™ services, type: `# csadm services --stop`

To know the status of all FortiSOAR™ services type: `# csadm services --status`

To know more about monitoring services, see the *Monitoring FortiSOAR™* chapter.

## Additional settings for record similarity and field predictions

FortiSOAR™ supports "Record Similarity" i.e., FortiSOAR™ displays records that are similar to the record on which you are working. FortiSOAR™ also supports "Record Field Value Prediction" i.e., FortiSOAR™ predicts values of fields of your choice within a record from the values of fields of existing records based on the criteria you have defined, making it easier for analysts to make informed decisions. For more information, see the *Working with Modules - Alerts & Incidents* chapter in the "User Guide."

This section provides information on how you can tune the results that are displayed by FortiSOAR™ for record similarity and field predictions using the following parameters in the `/opt/cyops/config/cyops-search/config.yml` file:

- `minimum_should_match: <percentageValue>`: This setting defines that a record will be considered similar only if there is a match of at least the percentage value that you have specified on the related fields. This is especially true for similarity based on related records. For example, if you set this parameter as `minimum_should_match: 10%` (default), then if you have defined similarity for alerts based on related indicators, then FortiSOAR™ will display only those records as similar that match a minimum of 10% of the indicators. Therefore, for an alert that has 10 related indicators, FortiSOAR™

similarity results will display alerts that even have one common indicator; but if an alert has 20 related indicators, then FortiSOAR™ similarity results will display only those alerts that have at least 2 indicators in common.

- **max\_query\_terms:** <numberOfItems>: This setting defines how many terms of the parent record will be looked up for similarity in other records. Continuing the same example as above, if you set this parameter as **max\_query\_terms: 25** (default), then if an alert has more than 25 indicators, only 25 of them will be checked for similarity in other records. Note that increasing the value of this setting will increase the time FortiSOAR™ takes to return similarity and suggestion results.

For more information on the above parameters and other parameters, refer to the Elasticsearch reference at:

<https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-mlt-query.html>

## Troubleshooting Tips

### Your Workflow data size has increased

Increase in your Workflow data can cause performance bottlenecks.

#### Resolution:

You can purge Executed Playbook Logs using the **Purge Logs** button on the top-right of the **Executed Playbook Logs** dialog. For more information on purging, see the *Debugging and Optimizing Playbooks* chapter in the “Playbooks Guide.”

### Change the default value of some of the user profile parameters

An administrator with CRUD permissions on the **Security** module can change the default value of the following user-profile related parameters:

Parameter Name	Description	Default Value
<b>max_reset_attempts</b>	Maximum number of times users' can click the <b>Reset Password</b> link before actually resetting their password. If the user exceeds the value set in this parameter, then users' will not get a new link to reset their password based on the number of hours specified in the <b>reset_locktime</b> parameter. By default, the <b>max_reset_attempts</b> is set to 10 times and the <b>reset_locktime</b> is set to 12 hours, therefore, if a user clicks the <b>Reset Password</b> 11 times without actually resetting their password, then the user will not	10 times

	get a new link to reset their password for 12 hours.	
<code>reset_locktime</code>	Number of hours that users' will not get a new link to reset their password if they exceed the value set in the <code>max_reset_attempts</code> parameter.	12 hours
<code>max_failed</code>	Number of times that users' can enter an incorrect password, while logging into FortiSOAR™, before their account gets locked. If the user exceeds the value set in this parameter, then the user will get locked out based on the number of minutes specified in the <code>lock_minutes</code> parameter. By default, the <code>max_failed</code> is set to 5 times and the <code>lock_minutes</code> is set to 30 mins, therefore, if a user enters an incorrect password 6 times, then their account gets locked for 30 mins.	5 times
<code>lock_minutes</code>	Number of minutes that users' account gets locked if they exceed the value set in the <code>max_failed</code> parameter.	30 mins

To change the value of the `max_reset_attempts` parameter, the administrator should run the following curl command on their FortiSOAR™ system:

```
curl -X PUT \
  https://<FORTISOAR_HOSTNAME/IP>/api/auth/config \
  -H 'Authorization: <Bearer Token>' \
  -d '{
    "option": "max_reset_attempts",
    "value": 5
  }'
```

The above command changes the number of times users' can click the **Reset Password** link to 5 times, i.e., a user can click the **Reset Password** link 5 times without actually setting the new password. However, if the user clicks the **Reset Password** link for the 6th time, the user will be blocked.

Similarly, to change the value of the `reset_locktime`, `max_failed`, and `lock_minutes` parameters, the administrator should run the same curl command on their FortiSOAR™ system, but after changing the option and value parameter values:

```
curl -X PUT \
  https://<FORTISOAR_HOSTNAME/IP>/api/auth/config \
  -H 'Authorization: <Bearer Token>' \
  -d '{
    "option": "reset_locktime",
    "value": 2
  }'
```

The above command changes the number of hours that users' will not get a new link to reset their password to 2 hours if they have exceeded the value set in the `max_reset_attempts` parameter.

```
curl -X PUT \
  https://<FORTISOAR HOSTNAME/IP>/api/auth/config \
  -H 'Authorization: <Bearer Token>' \
  -d '{
    "option": "max_failed",
    "value": 3
  }'
```

The above command changes the number of times that users' can enter an incorrect password while logging into FortiSOAR™ before their account gets locked to 3, i.e., users' account will be locked if they enter an incorrect password 4 times while logging into FortiSOAR™.

```
curl -X PUT \
  https://<FORTISOAR HOSTNAME/IP>/api/auth/config \
  -H 'Authorization: <Bearer Token>' \
  -d '{
    "option": "lock_minutes",
    "value": 15
  }'
```

The above command changes the number of minutes that users' account will be locked to 15 minutes if they have exceeded the value set in the `max_reset_attempts` parameter.

## Error displayed while performing a search operation in FortiSOAR™

### Resolution:

If you get any error while performing a global search in FortiSOAR™, check that the `elasticsearch.service` and the `cyops-search.service` are running.

If these are not running, then start these services using the following commands:

```
# systemctl start elasticsearch
```

```
# systemctl start cyops-search
```

For more information, see the `FortiSOAR™ Search Errors` topic in the *Elasticsearch Configuration* chapter.

## Reindexing FortiSOAR™ modules for search

Partial indexing of a module, or when a module does not get indexed, can lead to errors in FortiSOAR™ search. You can manually reindex any skipped or unsuccessfully indexed modules. For more information, see the [FortiSOAR™ Search Errors](#) topic in the *Elasticsearch Configuration* chapter.

### Resolution:

To reindex all the FortiSOAR™ modules, run the following command:

```
$ sudo -u nginx php /opt/cyops-api/app/console cybersponse:elastic:create --env="prod"
```

To reindex specific FortiSOAR™ modules, run the following command:

```
$ sudo -u nginx php /opt/cyops-api/app/console cybersponse:elastic:create --env="prod" --index='{ "type": "type of the module(s)" }'
```

For example:

```
$ sudo -u nginx php /opt/cyops-api/app/console cybersponse:elastic:create --env="prod" --index='{ "type": "indicators", "tasks" }'
```

## FortiSOAR™ crashing with "out of memory" errors

By default, FortiSOAR™ configures Elasticsearch to use 4 GB of RAM. If there are too many records or any very heavy records (such as large files uploaded) created per day on the system, it might crash with "out of memory" errors. To fix this, you must increase the memory allocated to Elasticsearch.

### Resolution

1. Change the following entry in `/etc/elasticsearch/jvm.options` to a higher value based on memory available on your server:  
-Xms4g  
-Xmx4g
2. Restart Elasticsearch using the following command:  
`systemctl restart elasticsearch`

## Changing Postgres worker memory

When the primary data in the system becomes large (eg, over million alerts) and you notice that the system is slow to respond. The slowness could be caused due to database queries taking longer with the increased database size. You can fine tune this behavior by increasing the following Postgres settings based on the available free memory on the system:

1. Increase the shared buffer and worker memory in the `/var/lib/pgsql/12/data/postgresql.conf` file:  
`shared_buffers = 2048MB`  
`work_mem = 16MB`
2. Restart Postgres using the following command:  
`systemctl restart postgresql-12`

## Issues while accessing FortiSOAR™ UI while using Chrome on MacOS Catalina

When you try to access FortiSOAR™ UI using Chrome on MacOS Catalina, a "NET::ERR\_CERT\_INVALID" error is displayed and there is no option to "Proceed" to the web page. You will face this issue only if you use default self-signed certificates. Once you replace the default self-signed certificates with your organization's signed certificates you will not face this issue.

**Note:** This issue will be faced by users who are on versions older than FortiSOAR™ 6.4.1.

This issue occurs when the self-signed certificate not being trusted by the OS, and therefore, you can perform the following steps to add the certificates to trust:







## cybersponse.localhost

Issued by: fortisoar.localhost

Expires: Friday, June 10, 2022 at 4:59:17 PM India St

+ This certificate is marked as trusted for this accou

### ▼ Trust

When using this certificate:  (

**Secure Sockets Layer (SSL)**

**Secure Mail (S/MIME)**

**Extensible Authentication (EAP)**

**IP Security (IPsec)**

**Code Signing**

**Time Stamping**

**X.509 Basic Policy**

### ▼ Details

**Subject Name** \_\_\_\_\_