ADMINISTRATION GUIDE 6.0.0

VERSION 1.0

FEBRUARY 2020

Copyright

Trademark

Table of Contents

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
- Secrets management - Deprecated in version 5.0.0
- 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	Permissions required on the module
System configuration: Customizing FortiSOAR™ and configure several default options used throughout the system, including setting up	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.	CRUD permissions on `Security` module. Default Role - Security Administrator. **Note**: From version 4.12.0 onwards, the security administrator role also has CRUD permissions on the `Secure Message Exchange` and `Tenants` modules, so that this role can configure multi-tenanted systems.
User management: Adding and removing users and editing their permissions.	CRUD permissions on `People` module.
Appliances management: Configuring data models, including picklist values and system navigation.	CRUD permissions on `Appliances` module.
Secrets management: Managing the Secrets store. (Deprecated in version 5.0.0)	CRUD permissions on `Secrets` module.
Playbook management: Configuring playbook collections and playbooks	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 health of HA clusters
- 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.

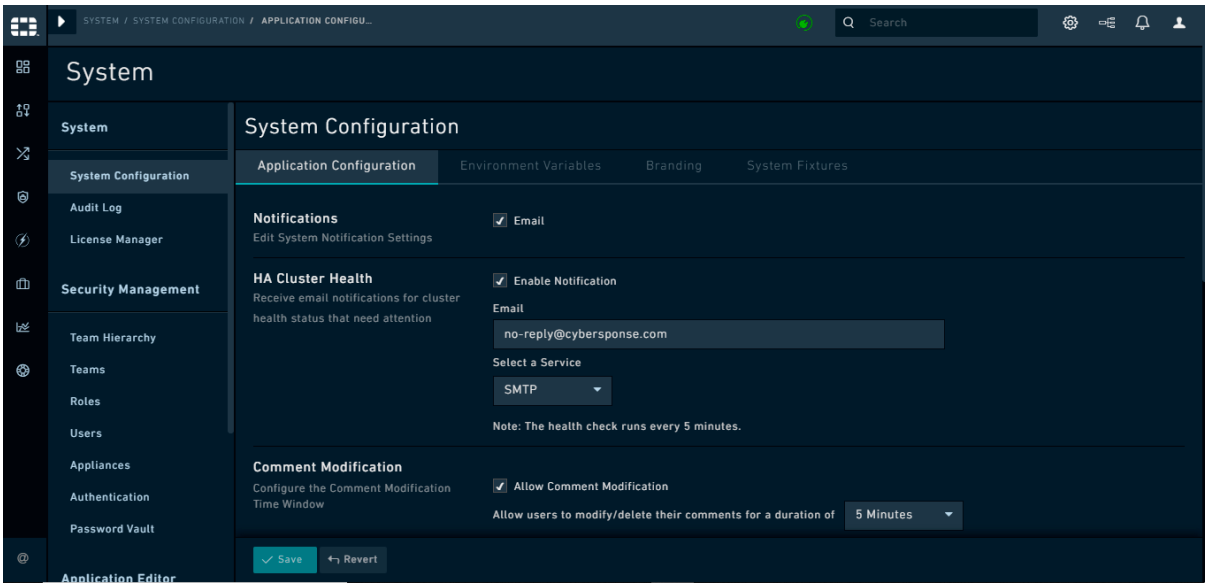


Figure 1. *System Configuration Menu - Application Configuration tab*

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 present on the support site. You must log onto the support site to view this information.

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 present on the support site. You must log onto the support site to view this information.

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 Notifications for health of HA cluster

To receive email notifications for failures of services within your High Availability (HA) cluster, in the `HA Cluster Health` section, click the **Enable Notification** checkbox.

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

Note: By default, the HA cluster health check runs every 5 minutes.

Configuring Comments

Users can edit and delete their own comments, 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 (by default, this is checked in case of a fresh installation of version 5.0.0 and later). 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.

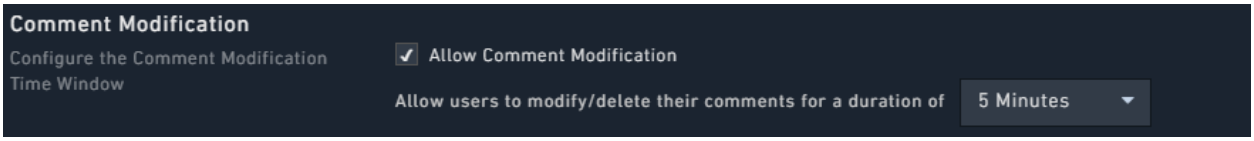


Figure 2. *Comments Modification section*

Users can edit or delete their comments in the collaboration window or in the `Comments` widget.

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.

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 both Audit Logs and Executed Playbook Logs. By default, audit logs and executed playbooks logs are not 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` page once you enable purging of the 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 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.

To enable purging of Audit logs and Executed Playbook Logs, you require to select the **Enable Purging** checkbox that appears in the `Audit Logs` and `Executed Playbook Logs` sections respectively.

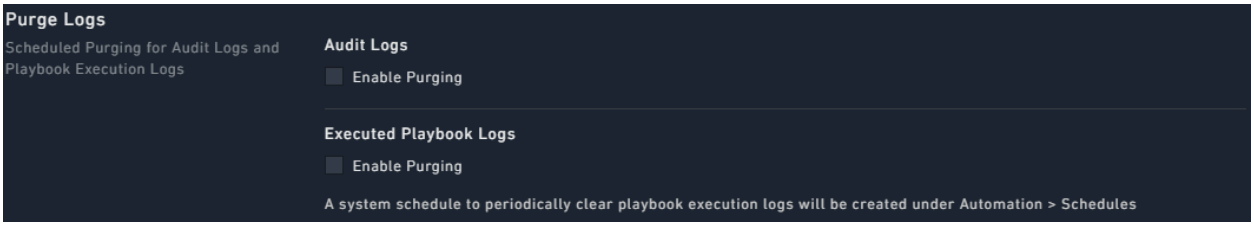


Figure 3. *Purge Logs Section*

Once you select the **Enable Purging** checkbox, you require to define the schedule for purging of audit log and executed playbook 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:

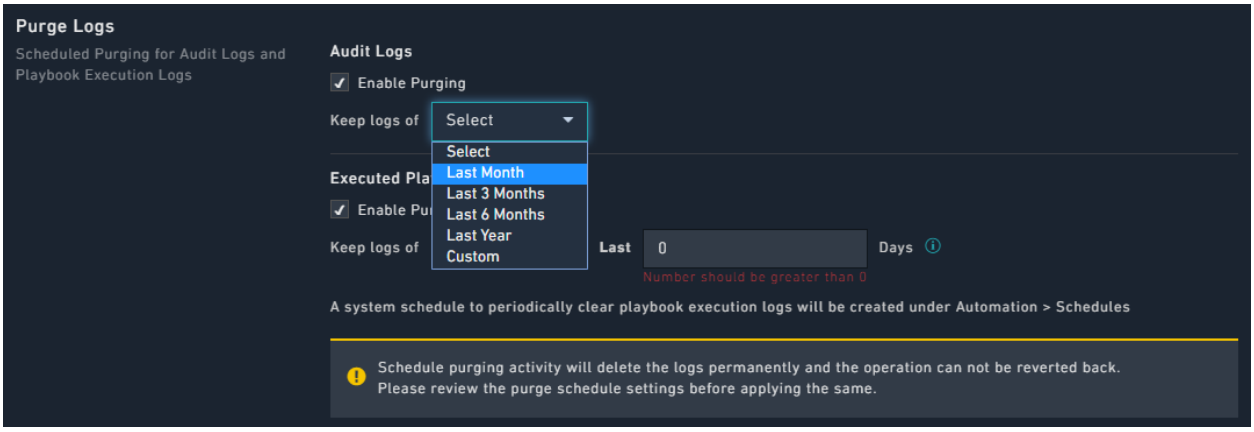


Figure 4. *Purge Logs - Specifying time to retain audit logs*

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.

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

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.

Similarly, define a schedule for purging of executed playbook logs, in the `Purge Logs - Executed Playbook Logs` section. Once you enable purging of executed playbook logs, a system schedule to periodically clear playbook execution logs is created in **Automation > Schedule**. Once you save the setting, a link to the **View System Schedule** will be created using which you can view the schedule.

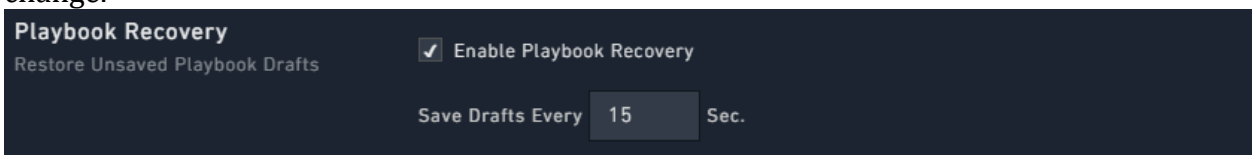
Configuring Playbook Recovery

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:

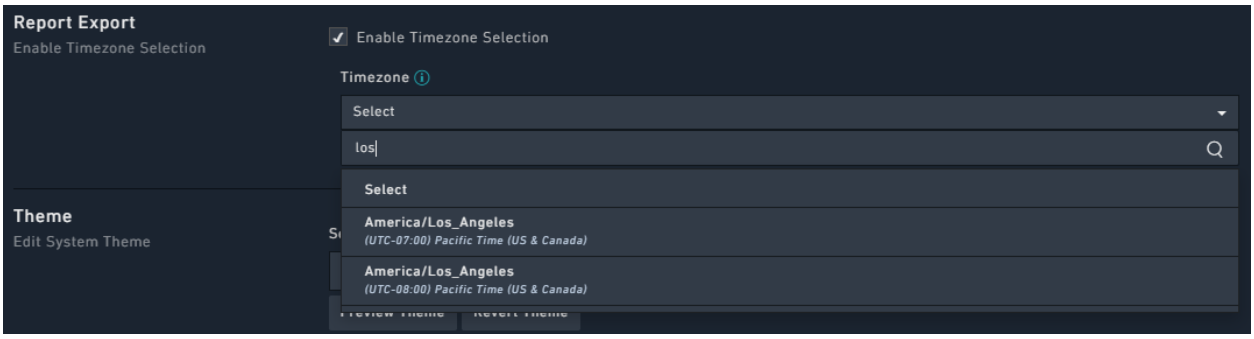


Figure 5. *Selecting the default Timezone for exporting reports*

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.

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 **uswgi** services for the changes to take effect. Use the `# systemctl restart celeryd` and `# systemctl restart uwsgi` commands to restart the celeryd and uswgi services.

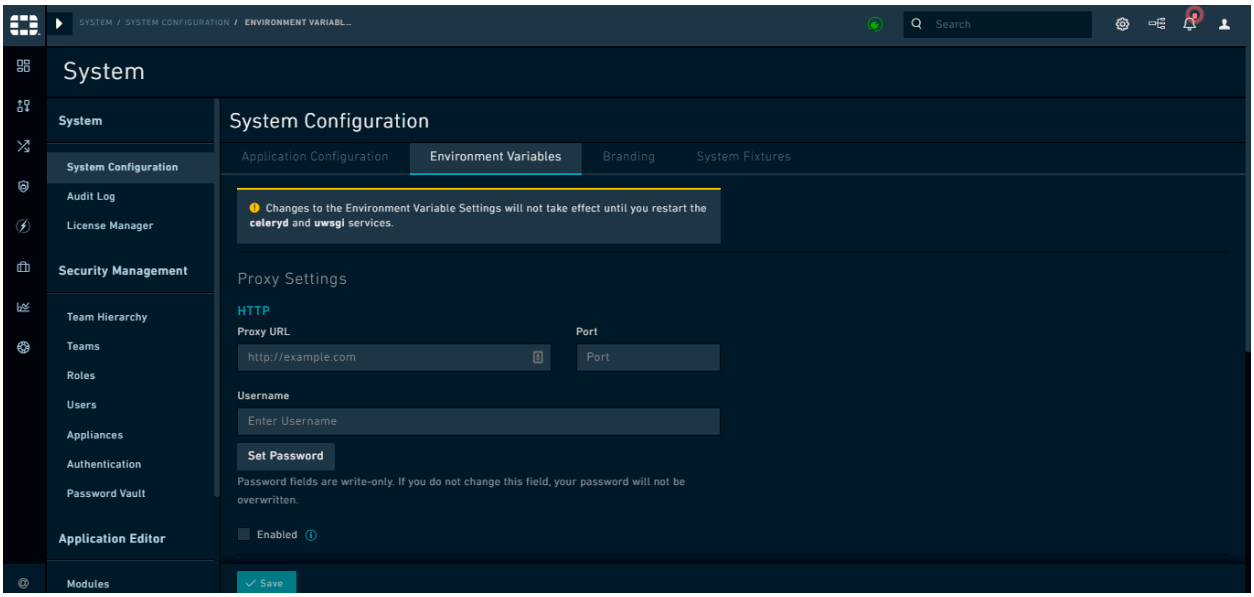


Figure 6. *System Configuration Menu - Proxy Configuration tab*

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, if your FortiSOAR™ license that has been enabled with *Advanced Branding*.

If your FortiSOAR™ license is not enabled with Advanced Branding, then you will only be able to customize the message that appears to all users on the login screen:

Login Message: You can enter a customized message that appears to all users on their login screen and click **Save**. Or, click **Reset To Default** to revert to the original message.

Contact your FortiSOAR™ Customer Success representative if you want your FortiSOAR™ license to be enabled with Advanced Branding.

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.

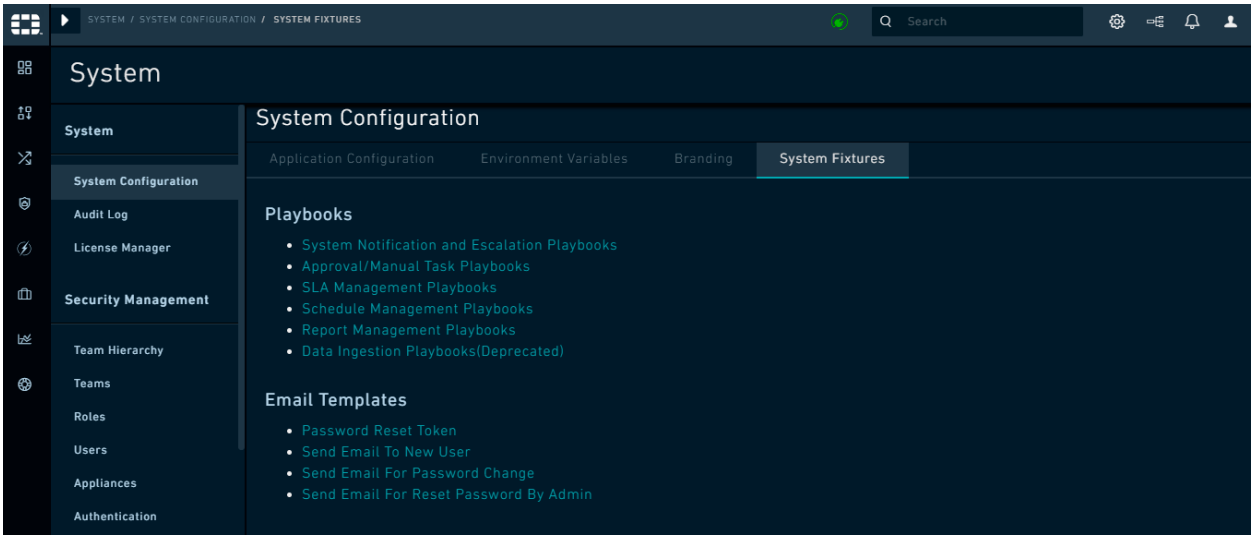


Figure 7. *System Fixtures tab*

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, etc.
- Report Management Playbooks collection: Includes a collection of system-level playbooks that are used to manage generation of FortiSOAR™ Reports.
- 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.

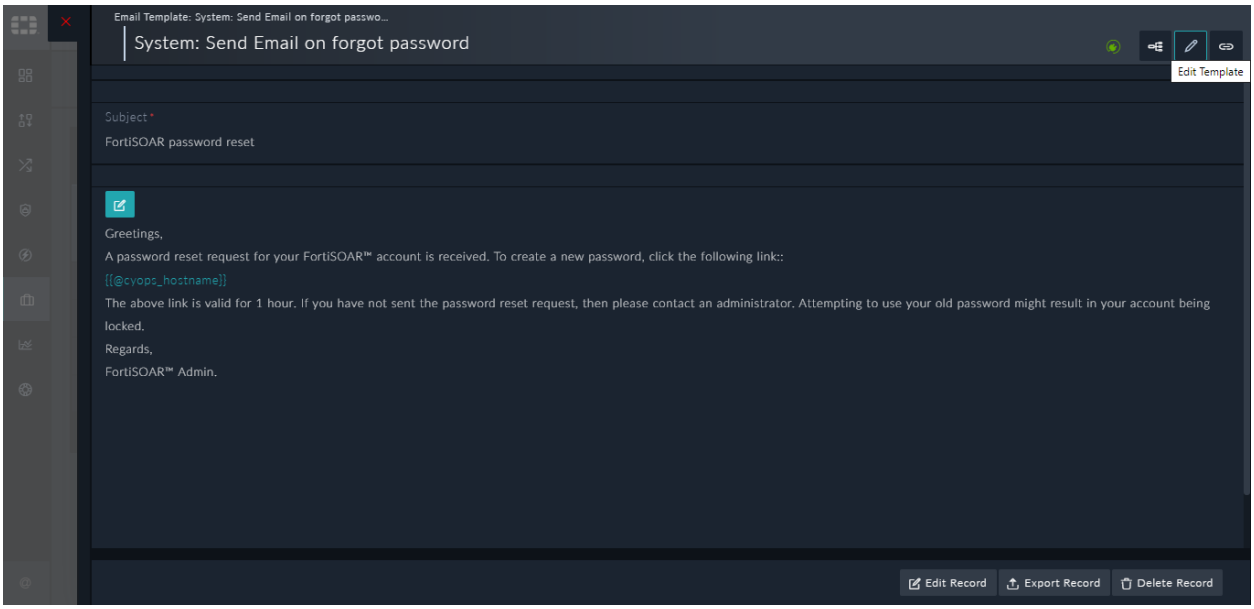


Figure 8. *Opening the Password Reset Token Email Template*

Clicking **Edit Record** opens the email template in a form format using which you can change the contents of the email as per your requirement, and then click **Save** to save your changes.

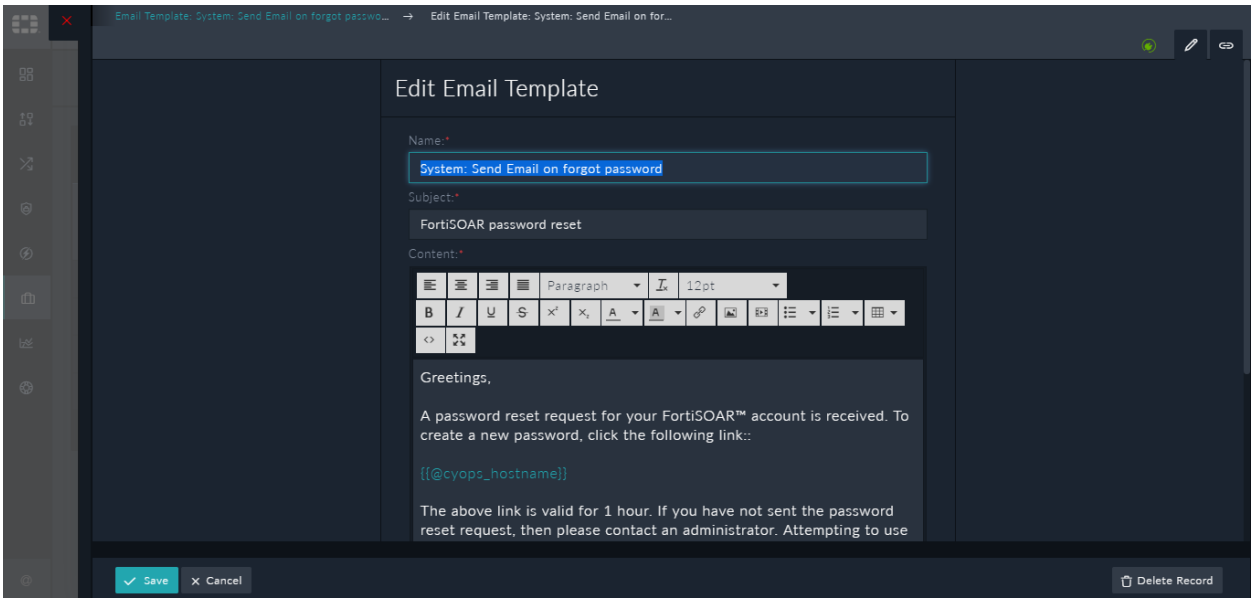


Figure 9. *Editing the Email Template in the Form Format*

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. From version 5.1.0 onwards, the audit logs also contain terminate and resume playbook events.

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.
  For version 5.0.0 or later installation, 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:

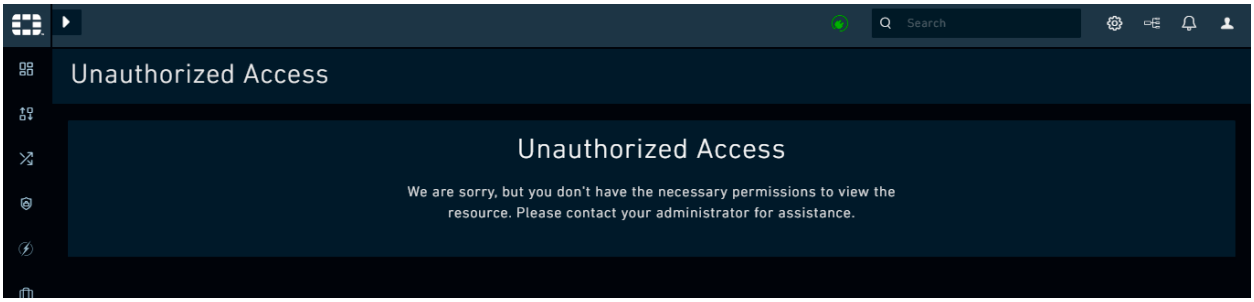


Figure 10. *Audit Log - No access error message*

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 also include data such as playbook events, 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.

The data included in the audit log has been further enhanced to 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.

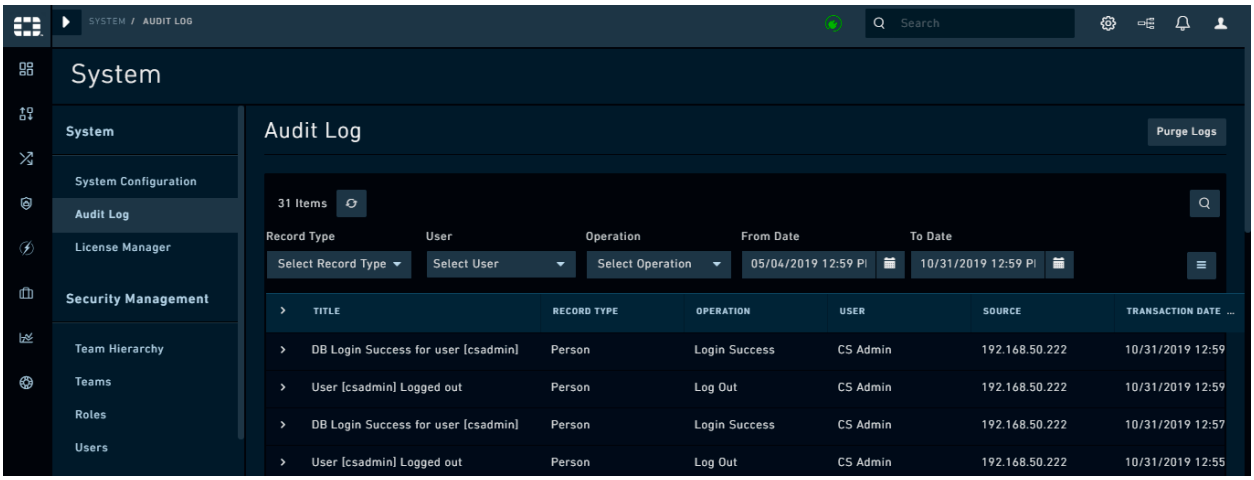


Figure 11. *Audit Logs - Purge Logs*

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.

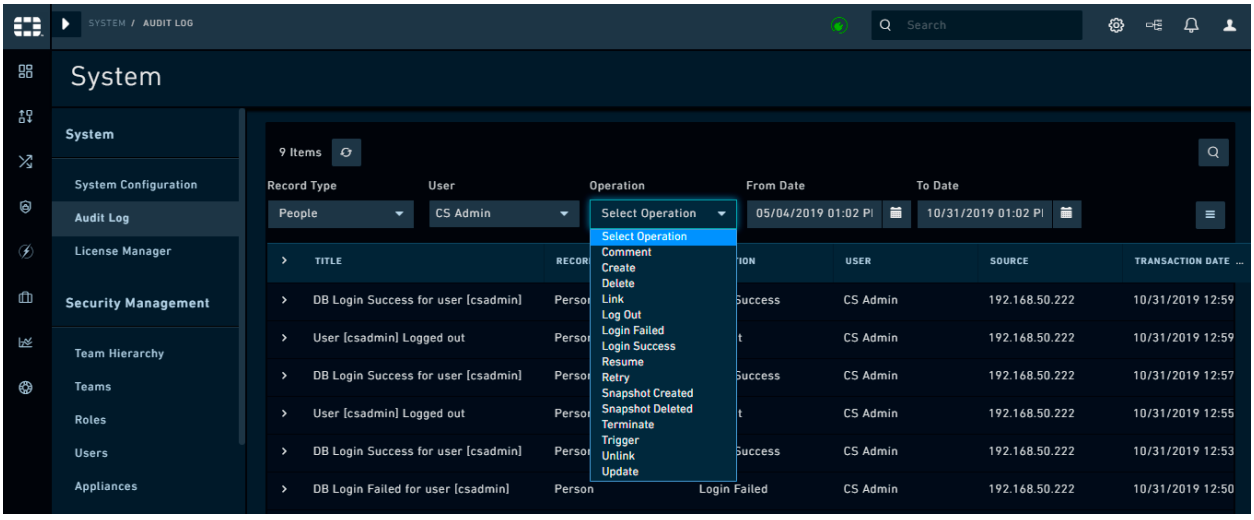


Figure 12. *Audit Log*

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`. For playbook audit log entries that were created prior to upgrading to version 4.11.0, then these entries will have blank approval names.
- `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.

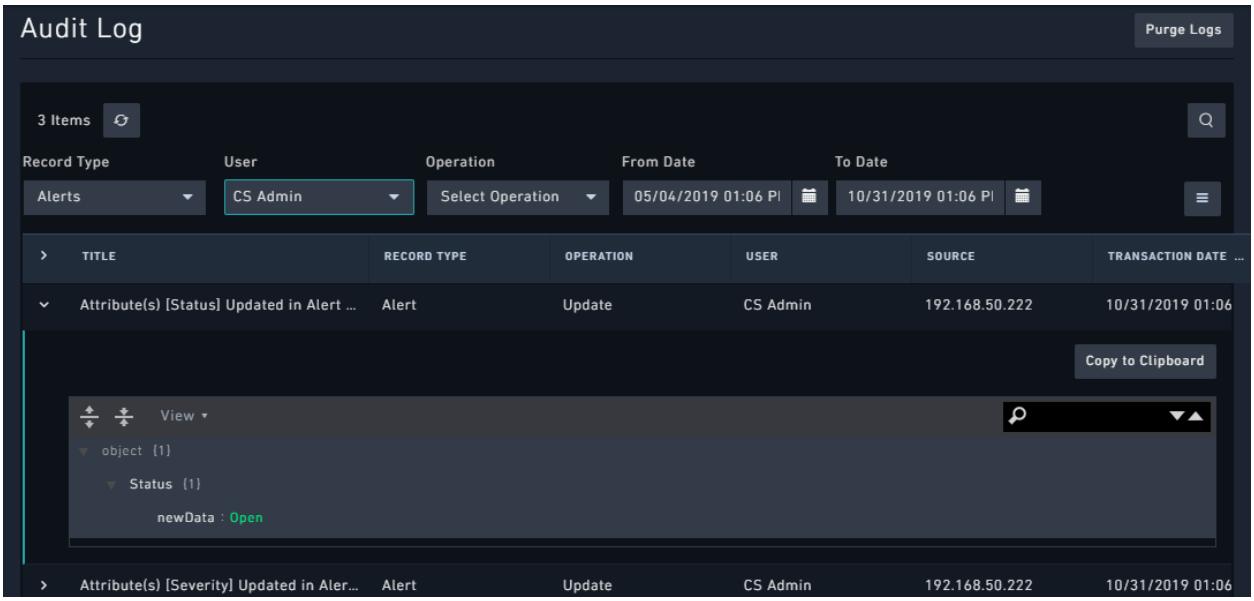
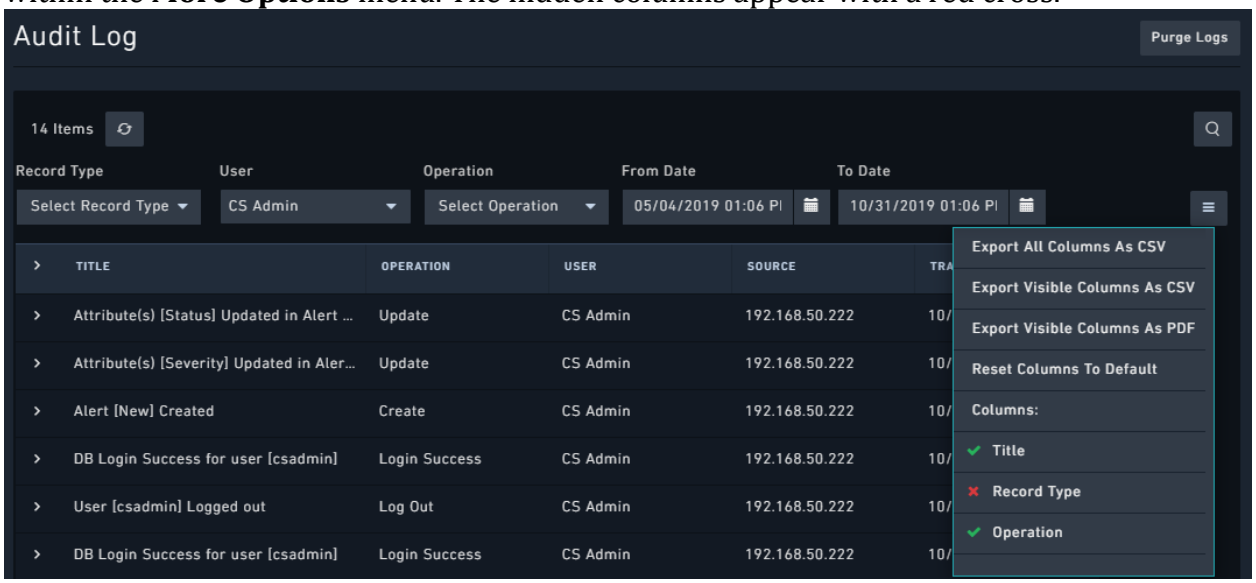


Figure 13. *Audit Log: Log Details*

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.

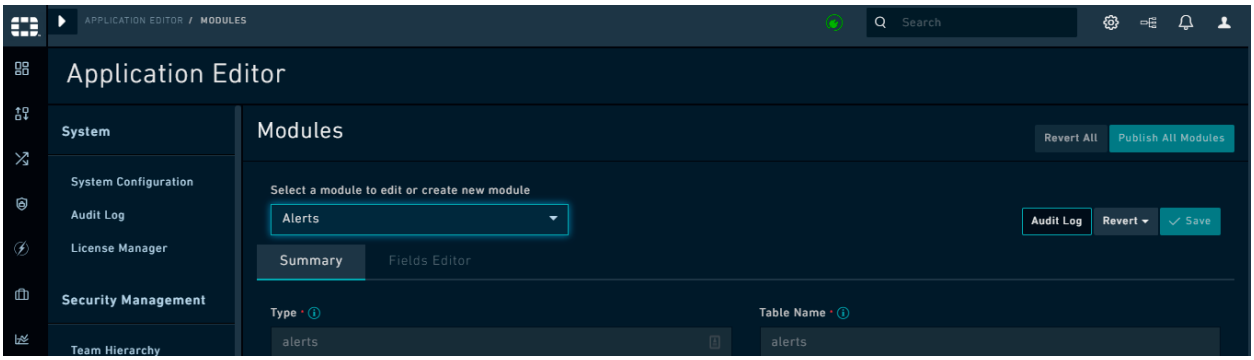


Figure 14. *Audit Log for a particular module*

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:

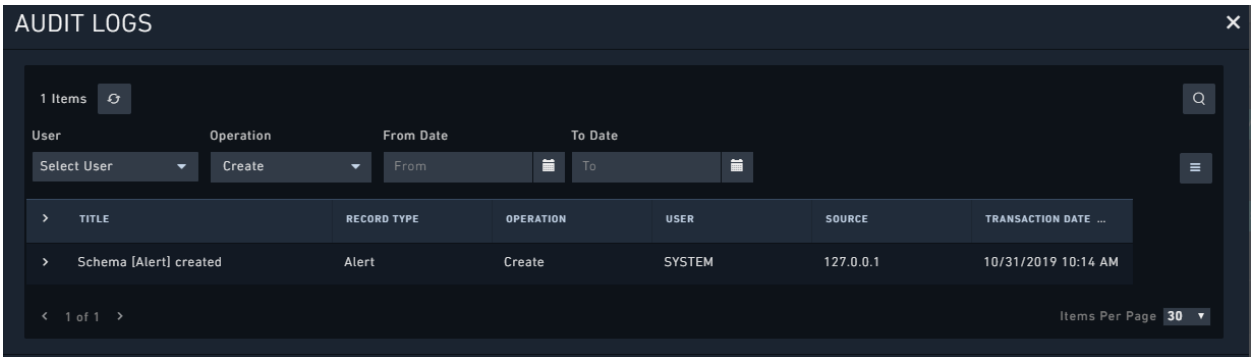


Figure 15. *Audit Logs: Alert Module Audit log*

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.

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.

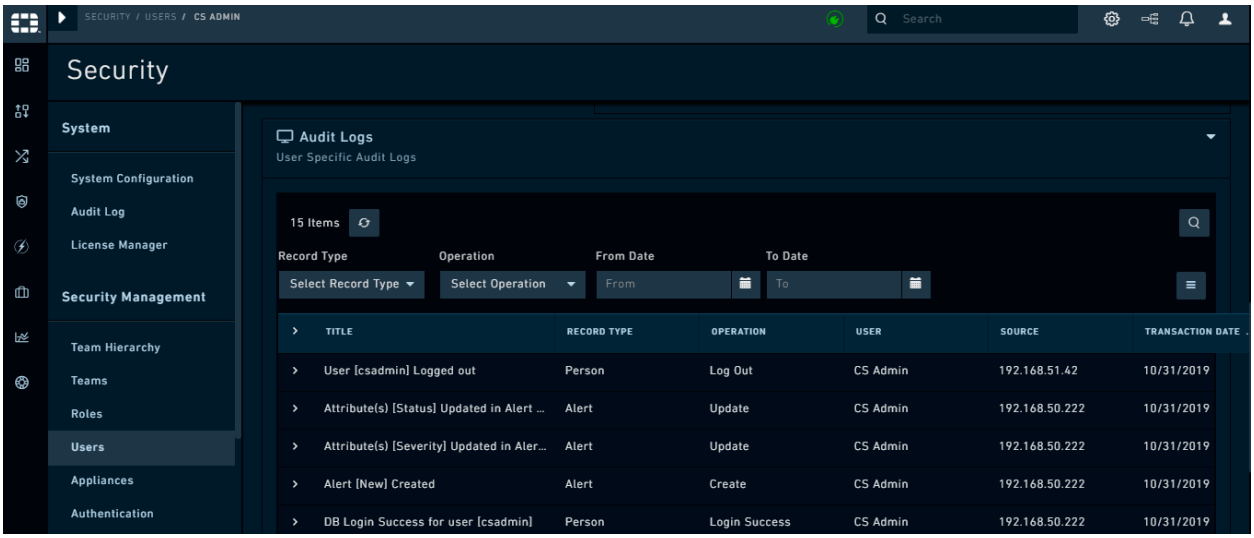


Figure 16. *User-Specific Audit Logs*

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:

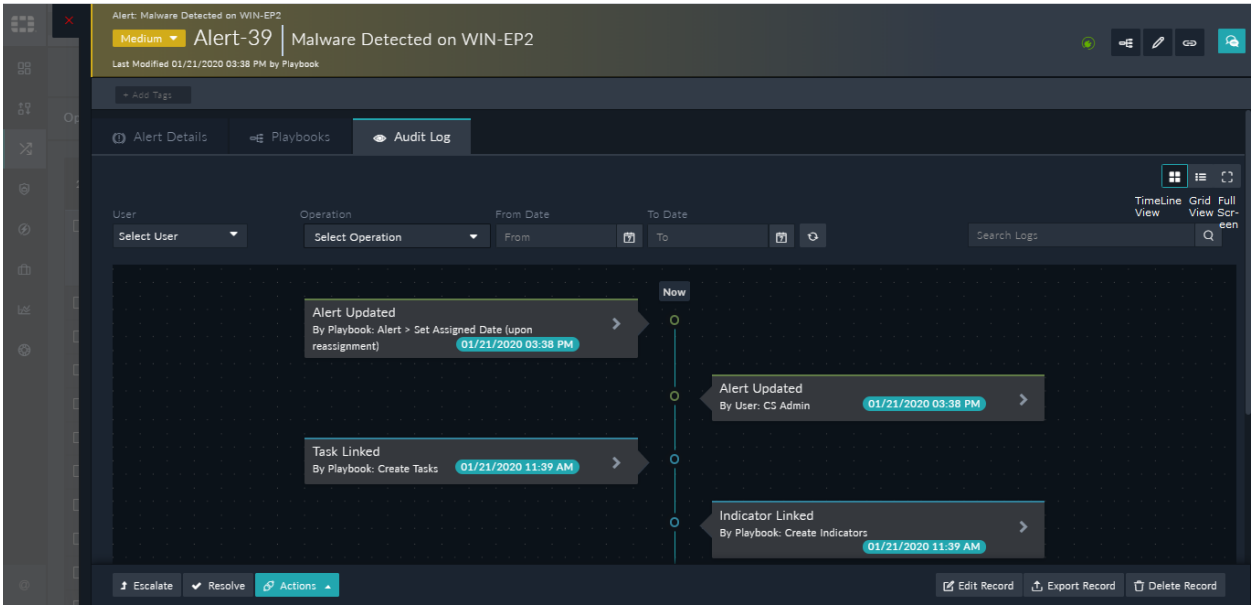


Figure 17. *Timeline Widget output on the Detail View page*

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:

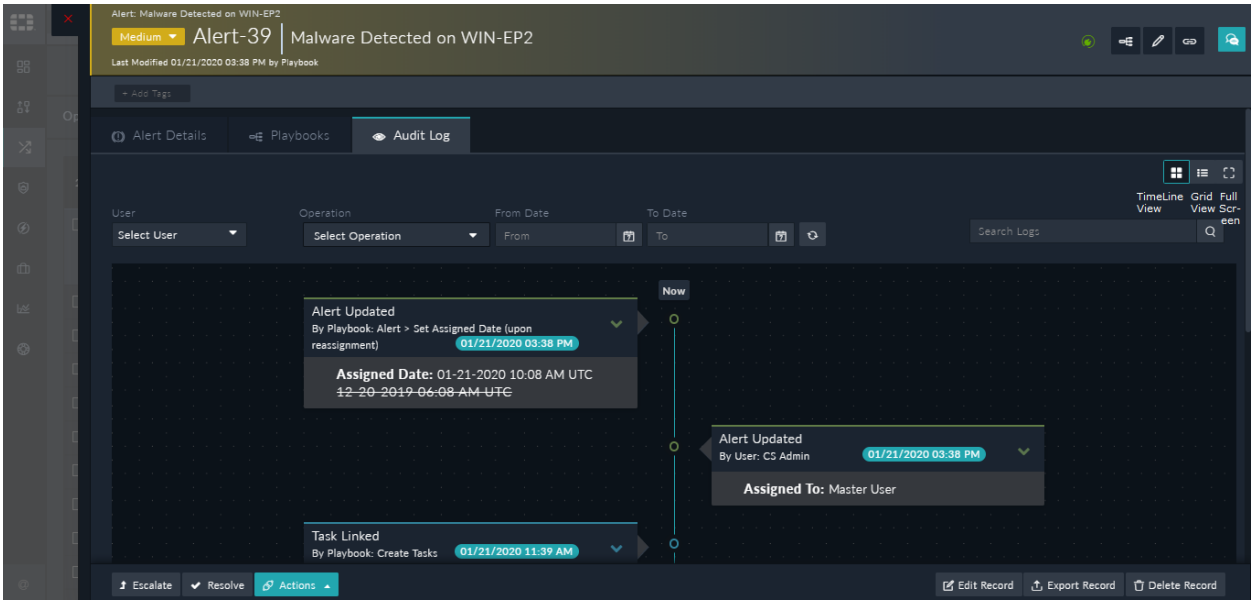


Figure 18. *Detailed timeline item*

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:

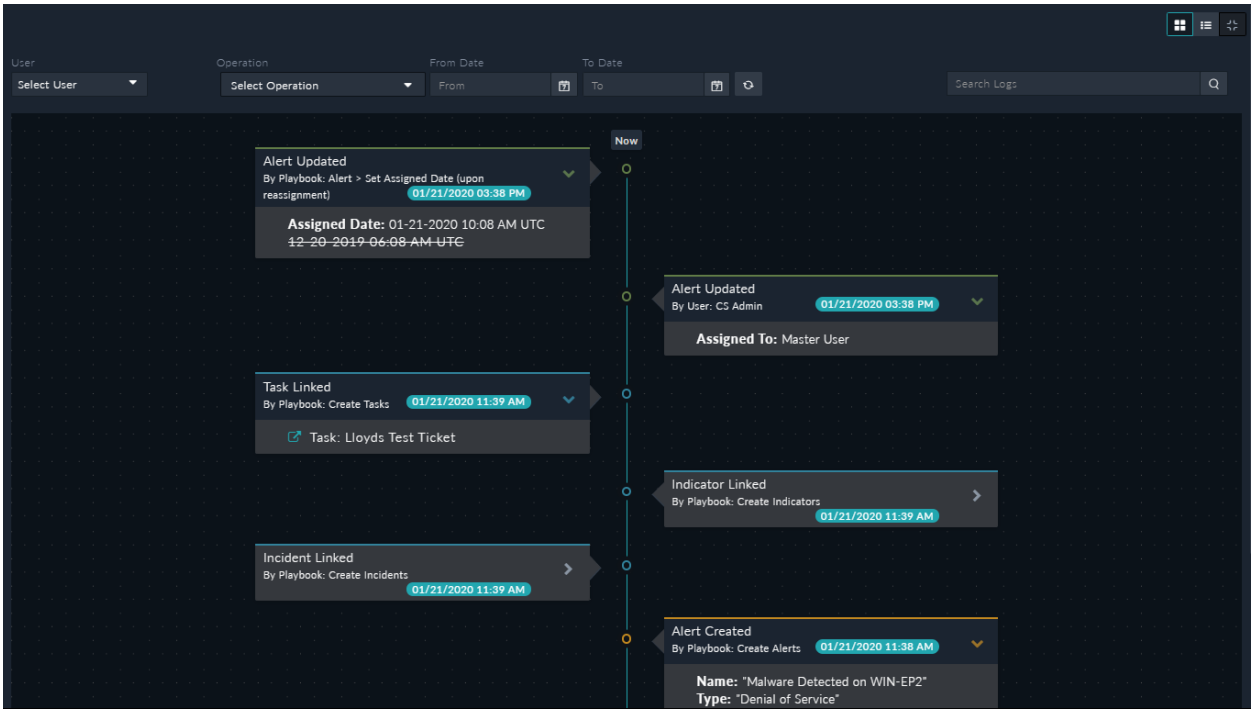


Figure 19. *Audit log in full screen*

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:

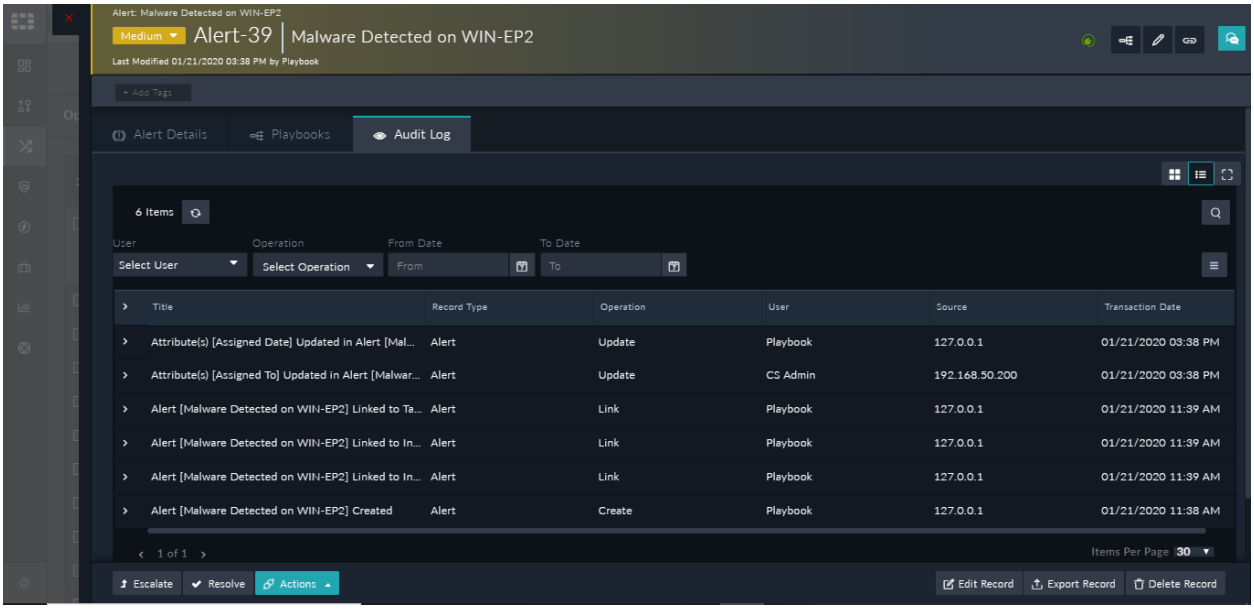


Figure 20. *Grid Widget output on the Detail View page*

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 Activies` module.

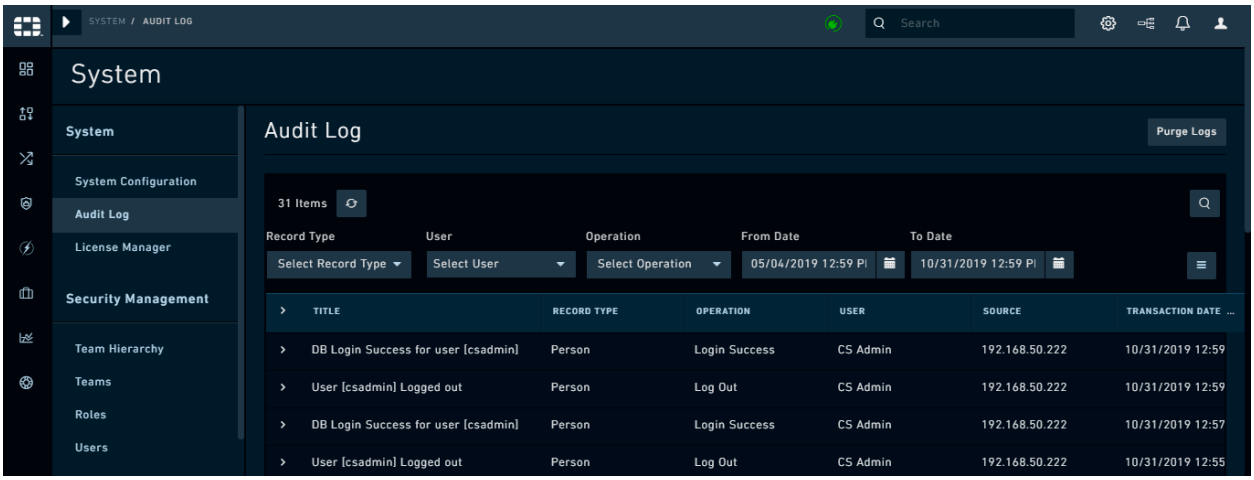


Figure 21. *Audit Logs - Purge Logs*

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

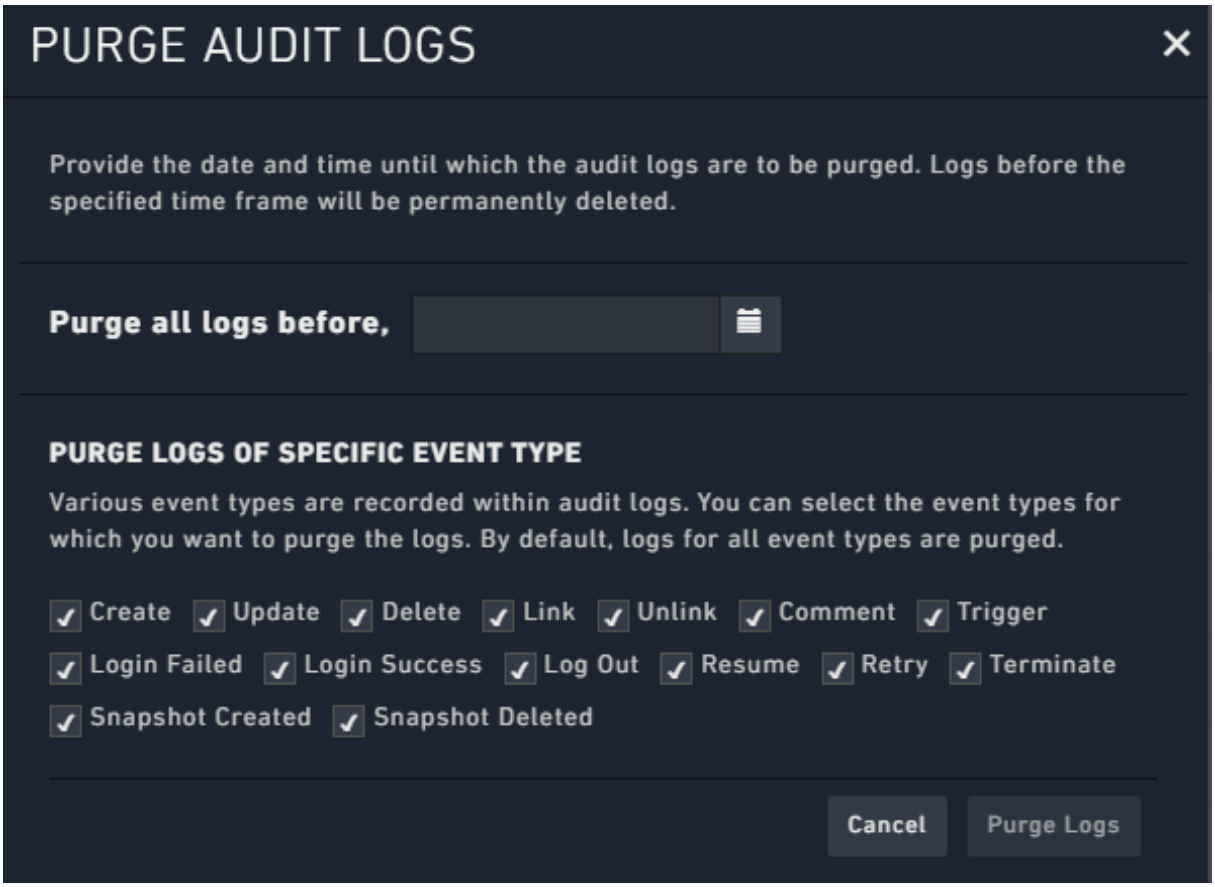


Figure 22. *Purge Logs Dialog - Date and Time Selection*

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.

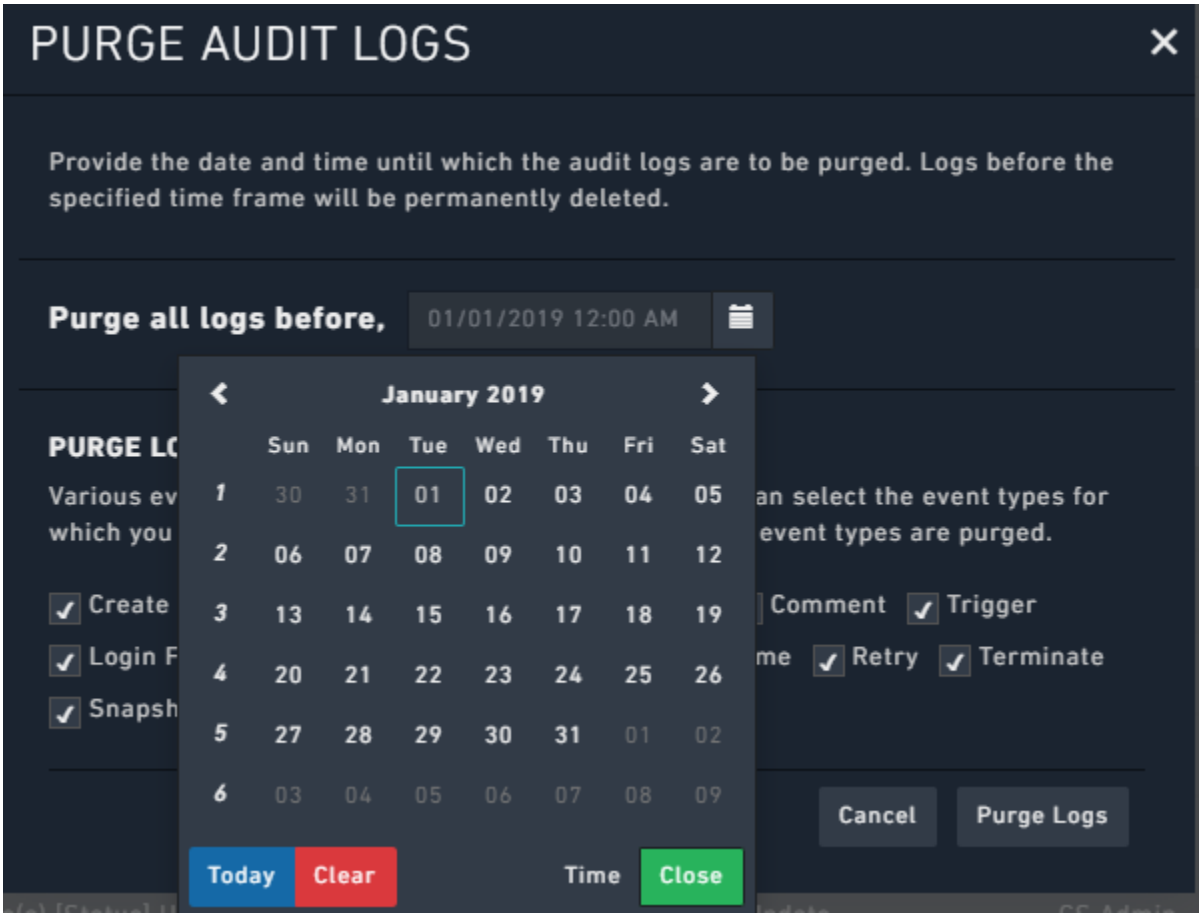


Figure 23. *Purge Logs Dialog - Date and Time Selection*

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:

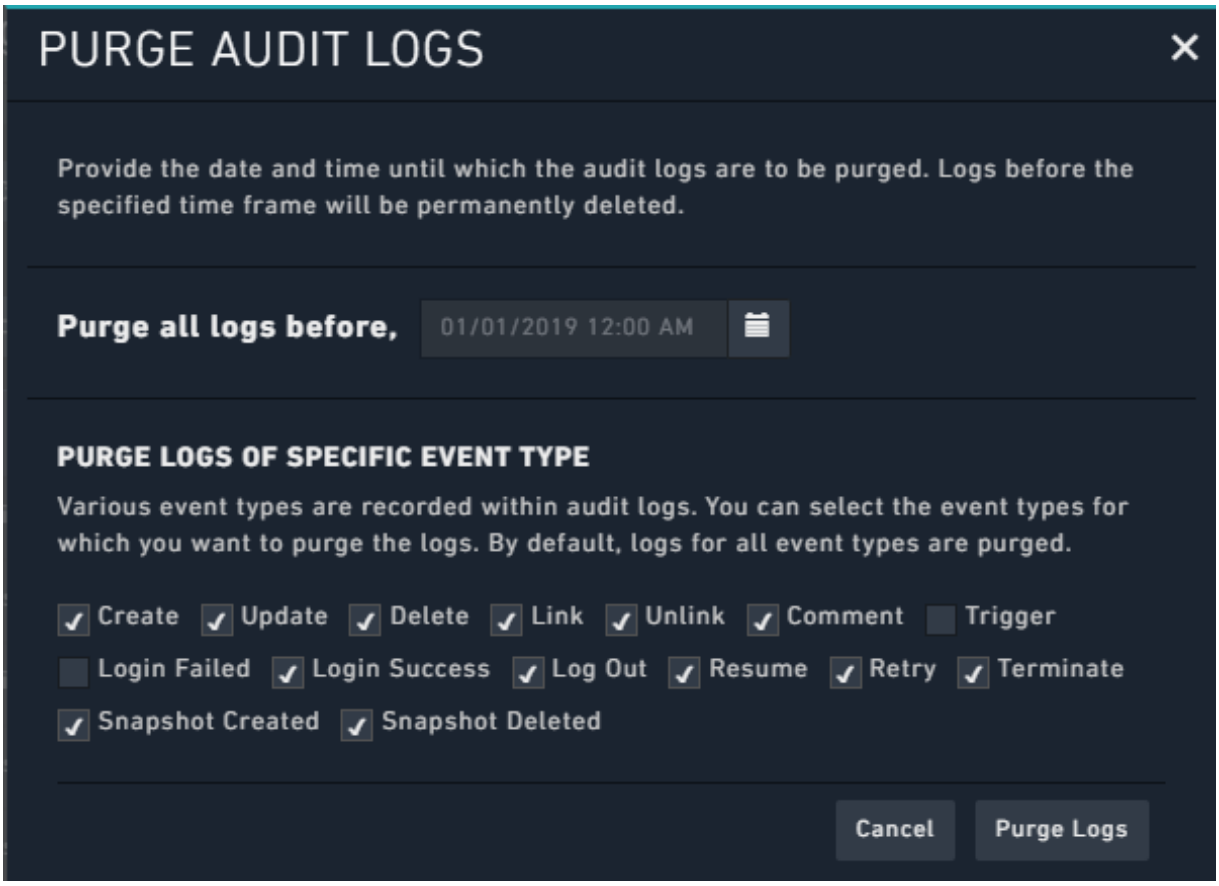


Figure 24. *Purge Logs Dialog - Choosing Events to Purge*

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

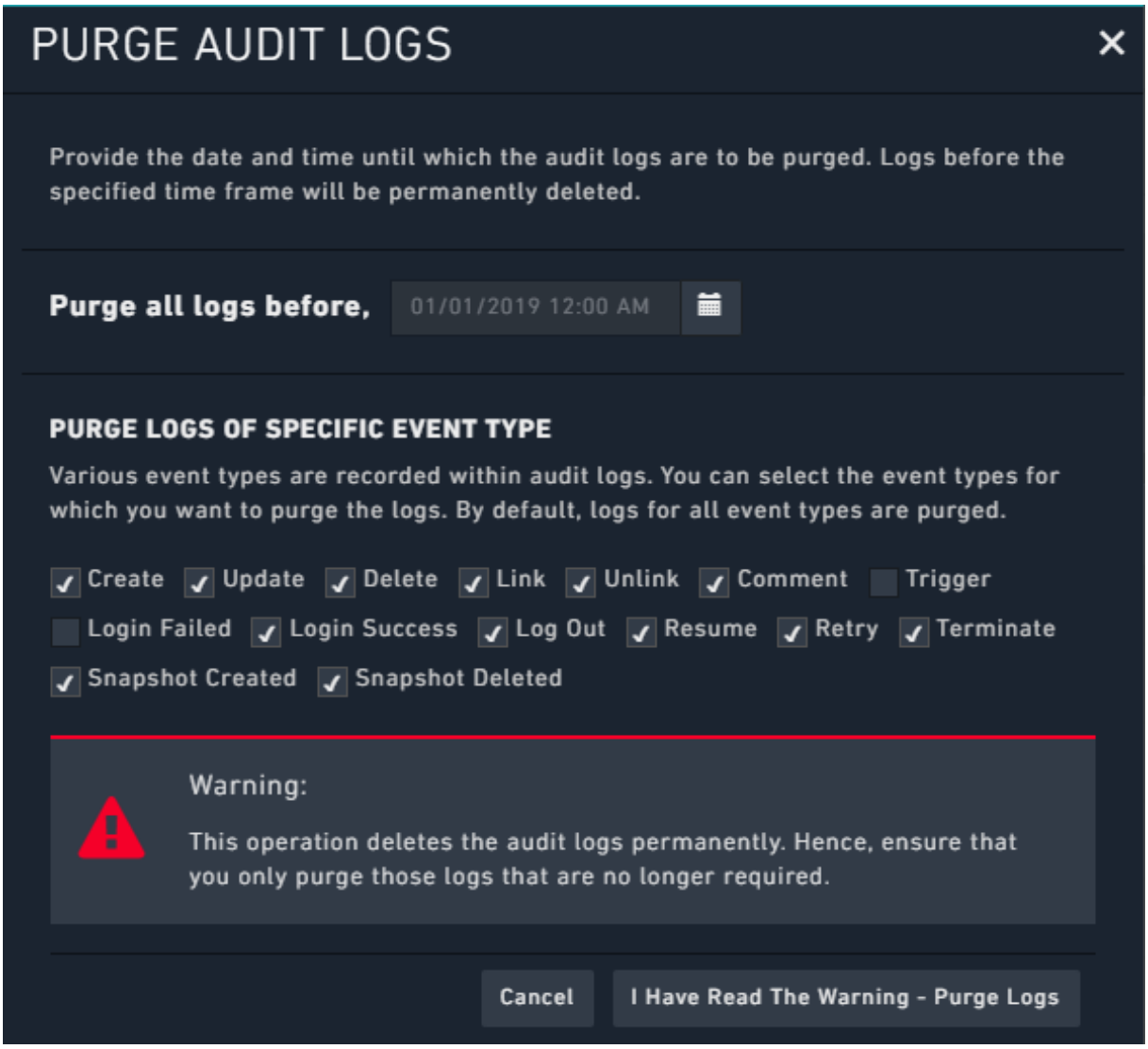


Figure 25. *Purge Audit Log Dialog Warning*

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 expiry date of the license.

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

You can use the License Manager to view your license details and for updating your license. FortiSOAR™ displays a message about the expiration of your license 30 days prior to the date your license is going to expire. You must update your license within 30 days if you want to keep using FortiSOAR™.

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

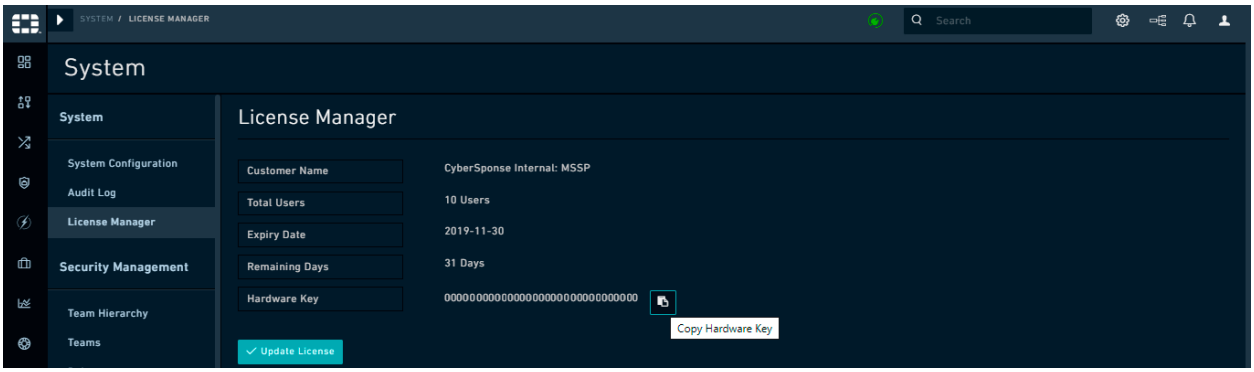


Figure 26. *License Manager*

Customer Name displays the name on whose name the license is issued.

Total Users displays the number of users that can use FortiSOAR™. You cannot create more users, in your FortiSOAR™ environment, than the value specified in this field. For example, if the Total Users field is set to 50, you cannot create a 51st active user in FortiSOAR™.

Expiry Date displays the date at which your FortiSOAR™ license will expire and **Remaining Days** displays the number of days left for your license to expire.

FortiSOAR™ starts displaying a message about the expiration of your license 30 days prior to the date your license is going to expire. Request your FortiSOAR™ CS representative to generate a new license for you within 30 days of your license expiration. You must provide your hardware key to your FortiSOAR™ CS representative for license generation. For more information about how to retrieve your hardware key and the FortiSOAR™ License Process, see *Licensing in FortiSOAR™*.

Once your FortiSOAR™ CS representative has generated a license for you, then you can install the license for the first time by clicking **Import License** and either drag-and-drop your newly generated license or click and browse to the location where your license file is located, then select the file and click **Open**.

If you want to update your license, and you have asked your FortiSOAR™ CS representative to generate a new license for you and your FortiSOAR™ CS representative has generated a license for you, then you can update your license by clicking **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**.

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 seven 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.

Version 5.0.0 implements RBAC for playbooks. Prior to version 5.0.0, users who were assigned roles with just `Read` permission on the `Playbooks` module could execute playbooks. However, from version 5.0.0 administrators require to assign roles that have the `Execute` permission on the `Playbooks` module to users who would be executing playbooks. `Execute` is a new permission added to the `Playbooks` and `Connector` modules.

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 from FortiSOAR™. However, you can make a user "Inactive" to stop that user from using the system. From version 5.0.0 onwards, you can delete users using a script. For more information, see Delete Users.

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.

Note: Version 5.1.0 onwards FreeIPA LDAP authentication is supported.

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.

Secrets

Use the `Secrets` menu to manage the Secrets store. Use the Secrets store to securely store and manage sensitive data, such as keys and credentials, which might further be used for 3rd party integrations. This feature has been deprecated in version 5.0.0. 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.

From version 4.11 onwards, 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.

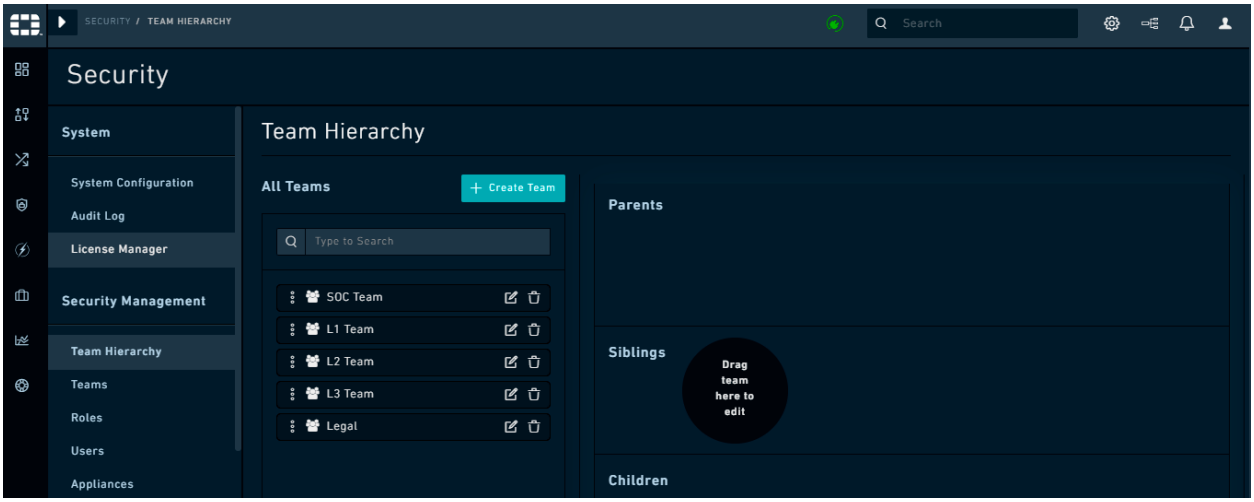


Figure 27. *Team Hierarchy Editor*

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.

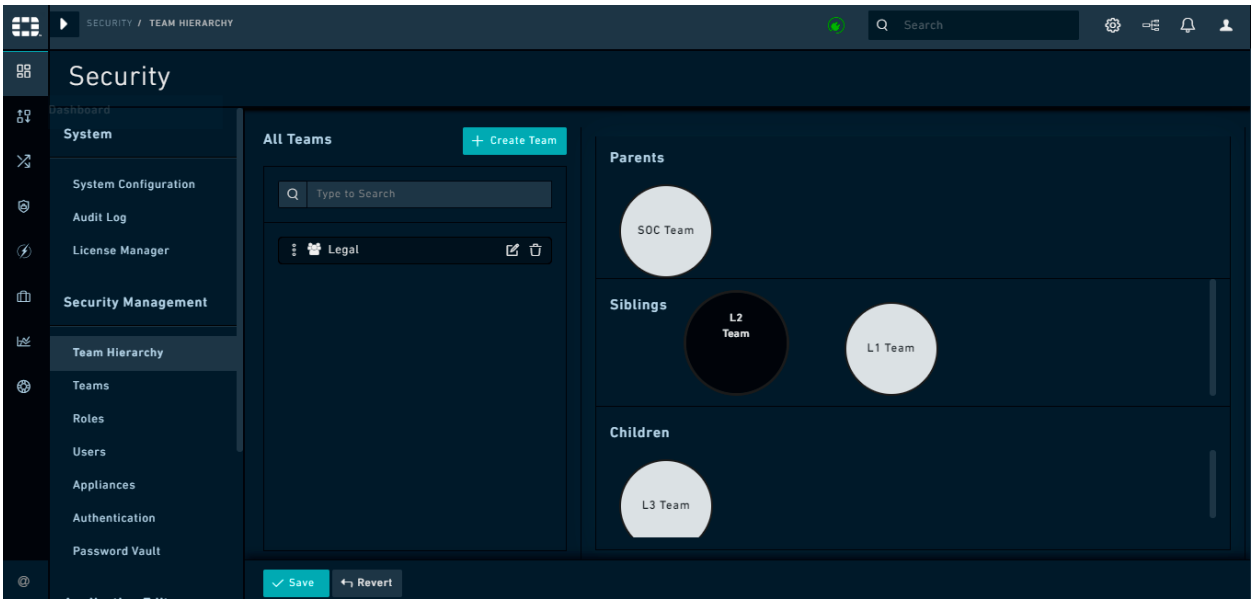


Figure 28. *Team Hierarchy Editor-Team in focus*

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.

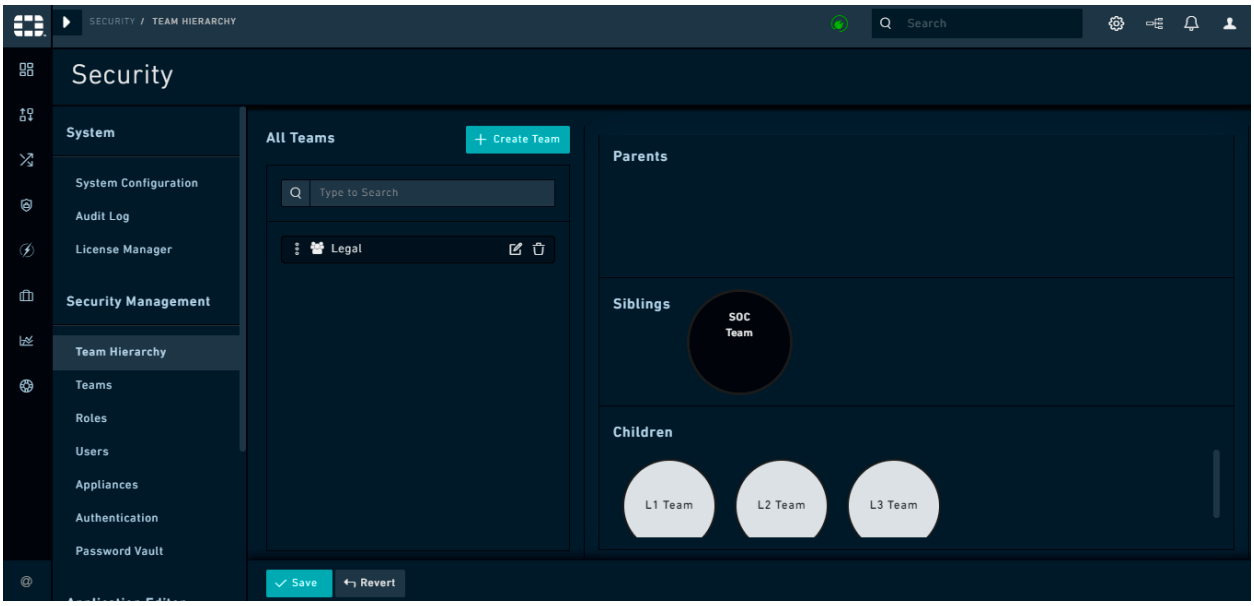


Figure 29. *SOC Management Team*

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.

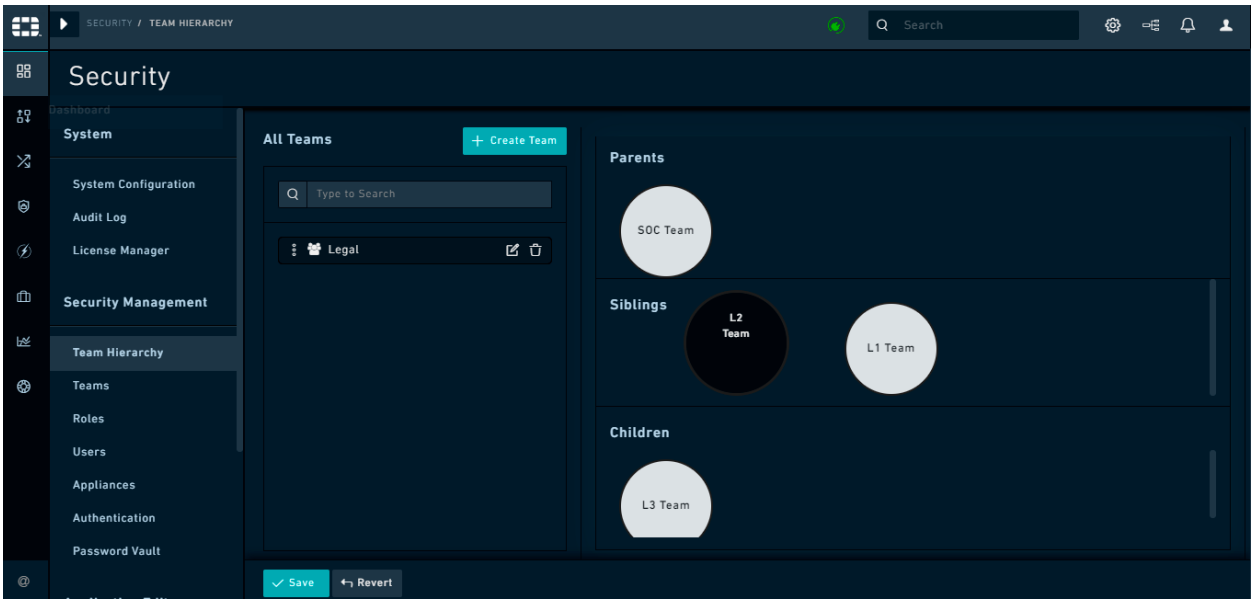


Figure 30. *L2 Team*

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.

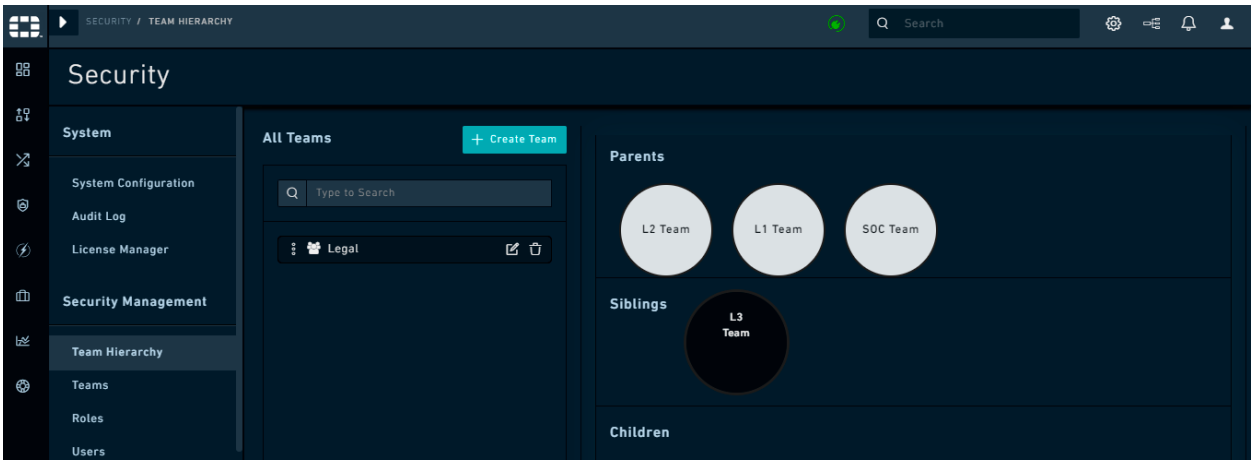


Figure 31. *L1 Team*

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 L1 Team can:

1. Effectively own only their own records
2. Own none of SOC Managers, L2, or L3 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.

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.

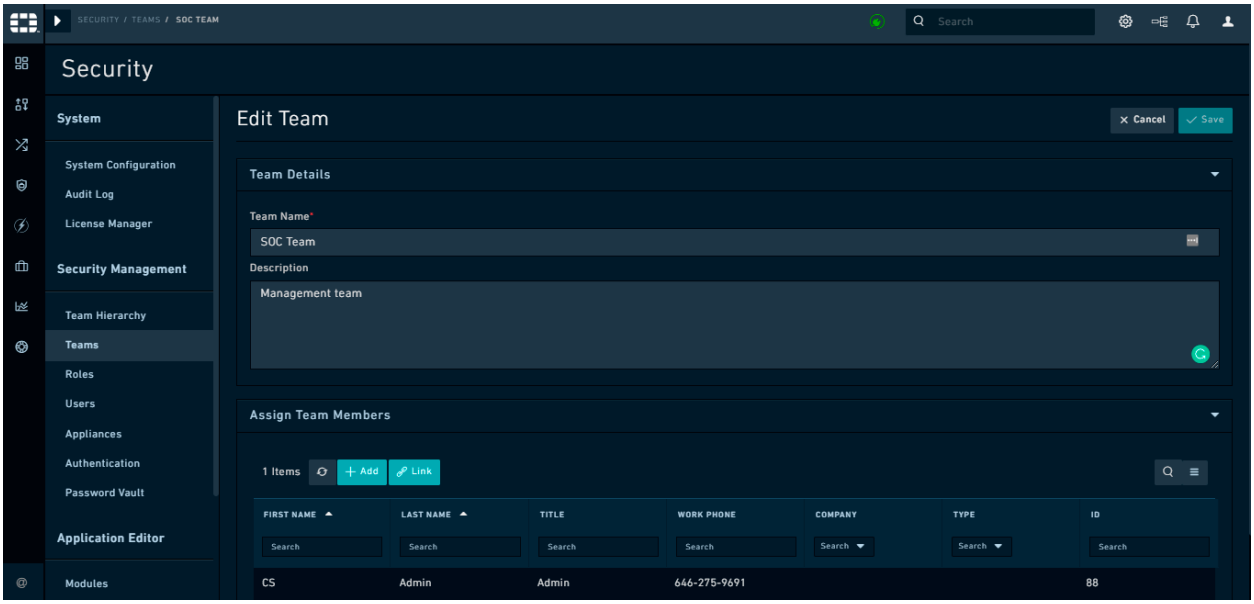


Figure 32. *Team membership page*

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.

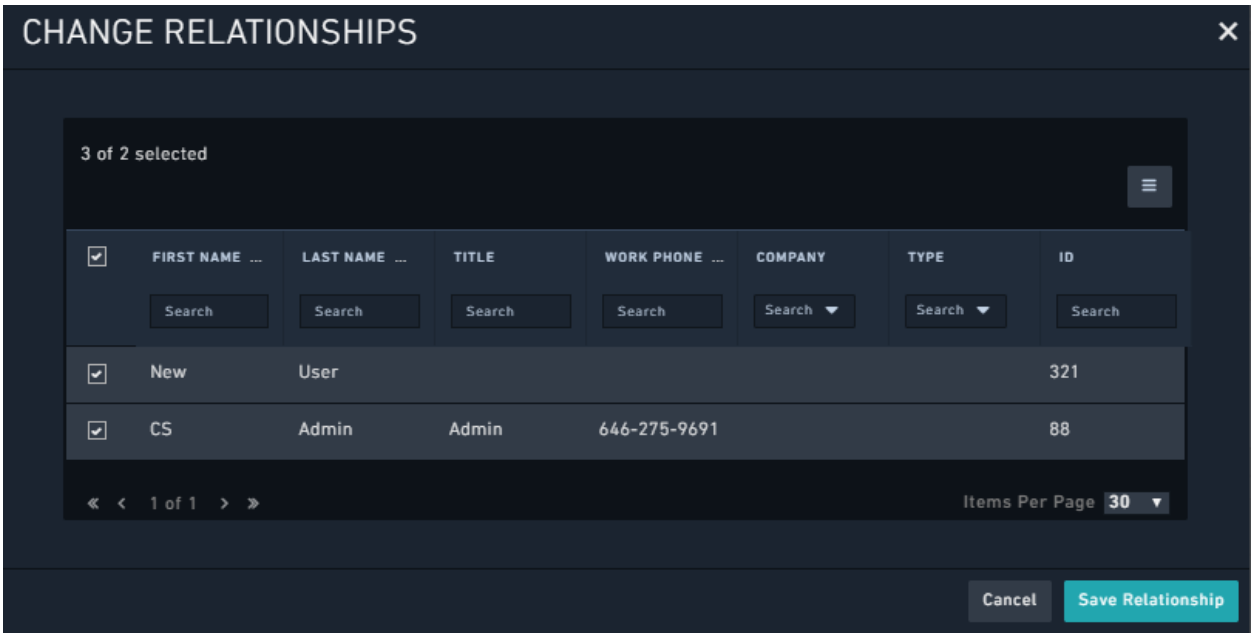


Figure 33. *Team membership editing*

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-tenanted 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.

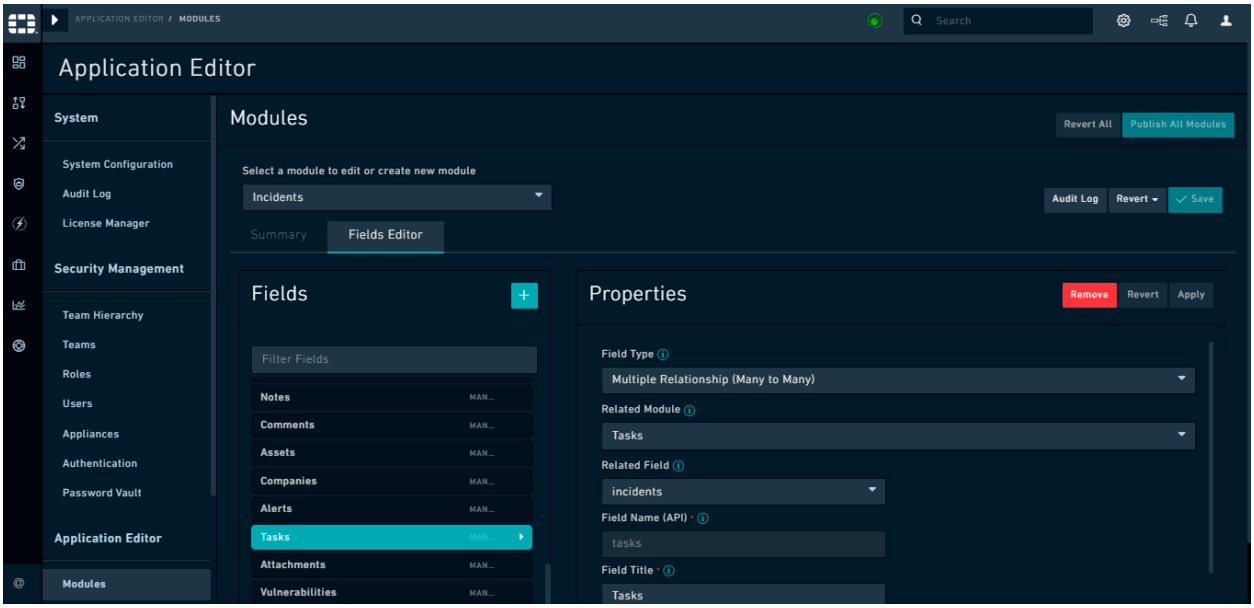


Figure 34. *Fields Editor - Incident Module*

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.

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 the default roles and instead add new roles, 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-tenanted 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.

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.
- **Secret** - the ability to manage the secrets from the **Secrets** item.
- **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:

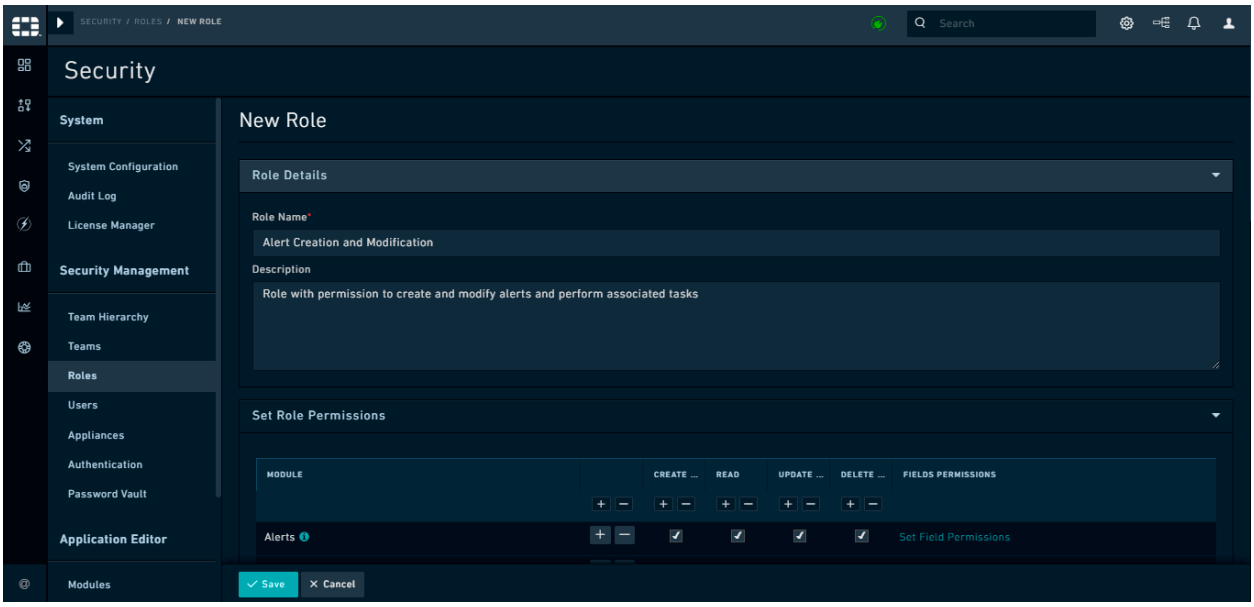


Figure 35. *Role Editor Page with Alerts and Incidents modules selected*

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:

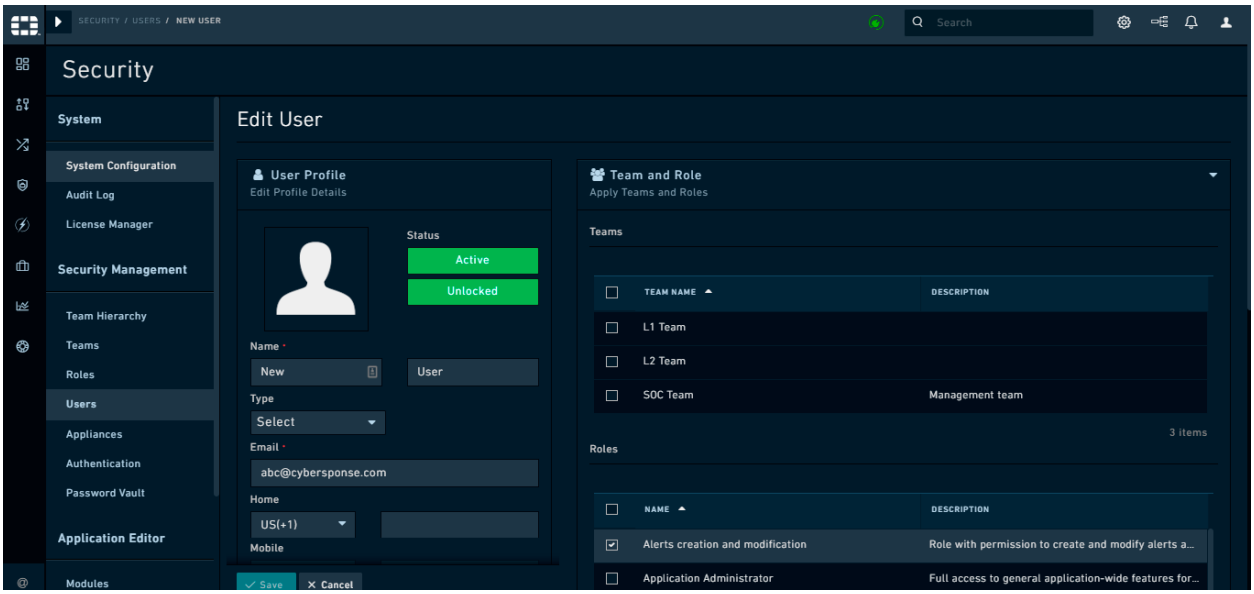


Figure 36. *User Profile page with User A assigned the Alerts and Incidents role*

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.

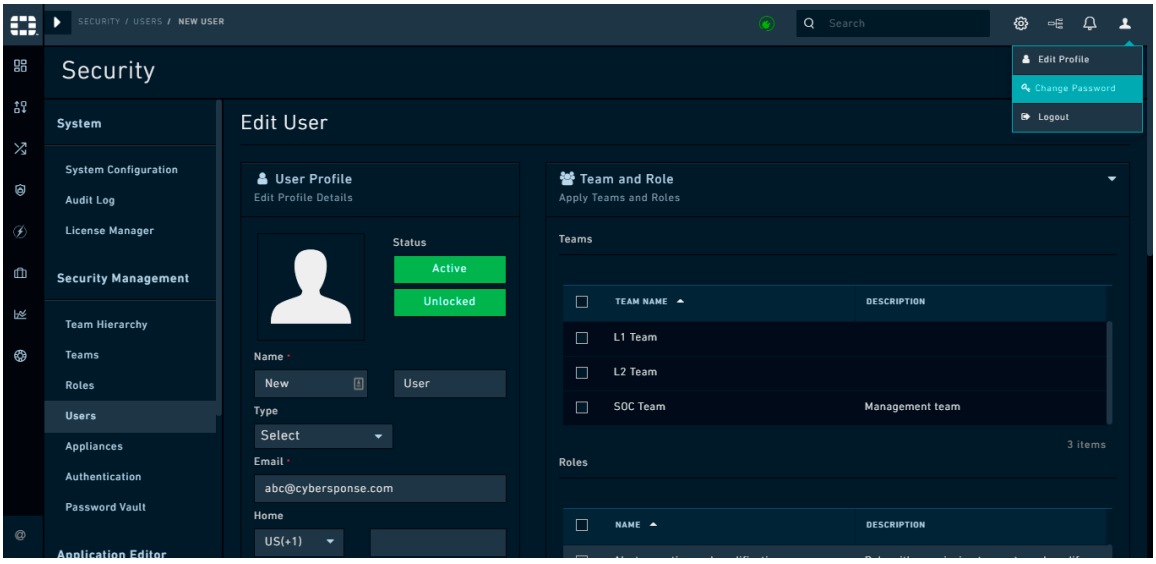


Figure 37. *User Profile Page*

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: You might face issues with user preferences such as applying filters on the grid or column formatting within a grid after you have upgraded FortiSOAR™ between major releases such as 5.x.x to 6.x.x. To resolve these issues, 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.

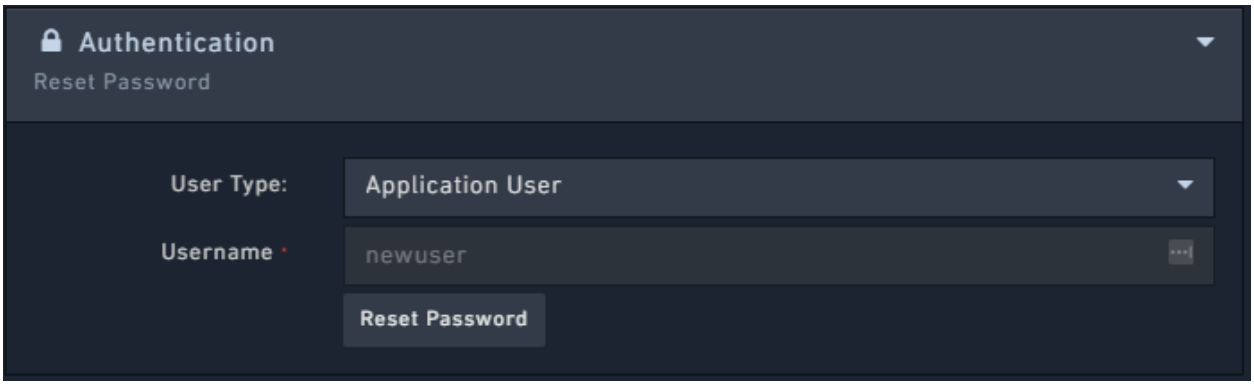


Figure 38. *User Profile Page: Authentication Section*

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.

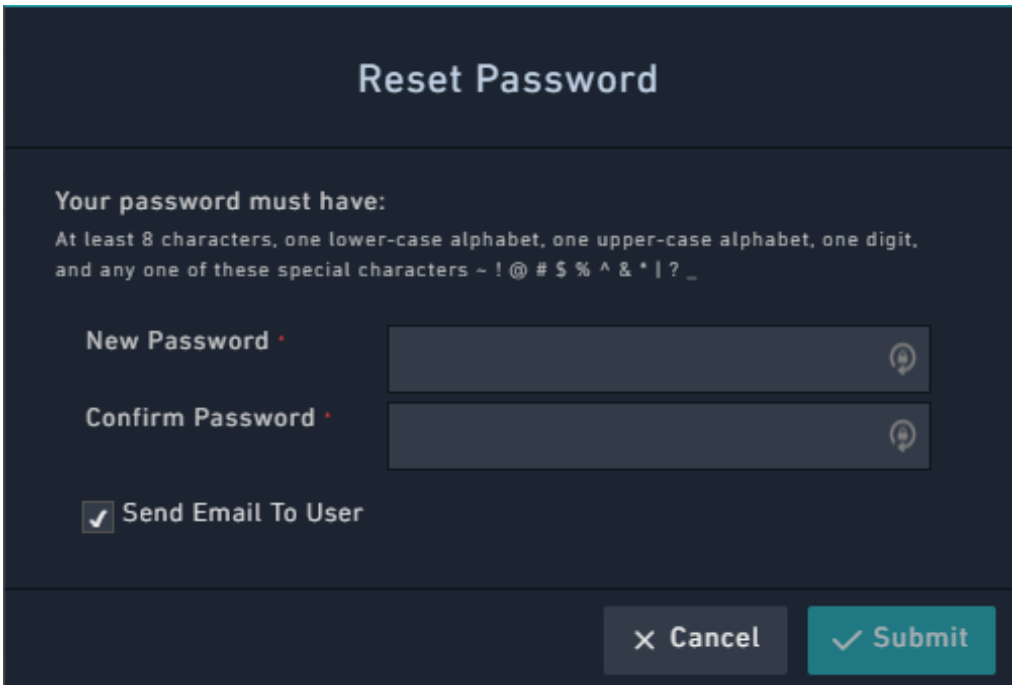


Figure 39. *Reset Password Dialog*

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.
Version 5.1.0 has provided Security Administrators with the ability to enforce 2FA across all FortiSOAR™ users. Therefore, this option will be 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. From version 5.1.0 onwards, the audit log 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.

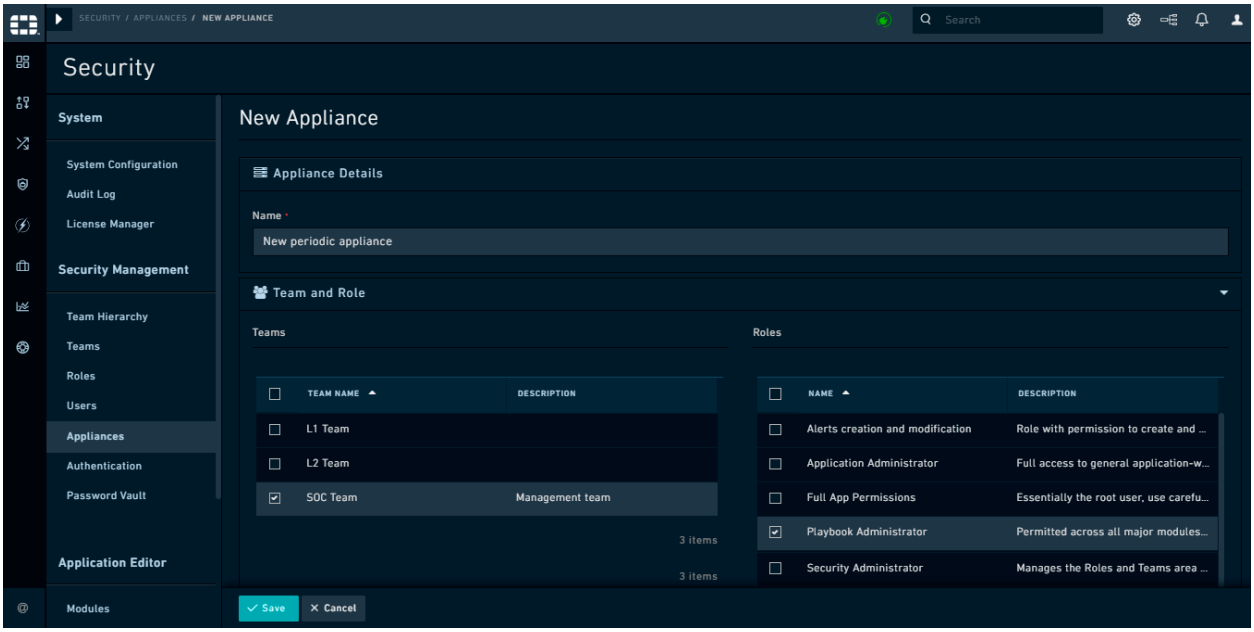


Figure 40. *Creating a New Appliance*

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.

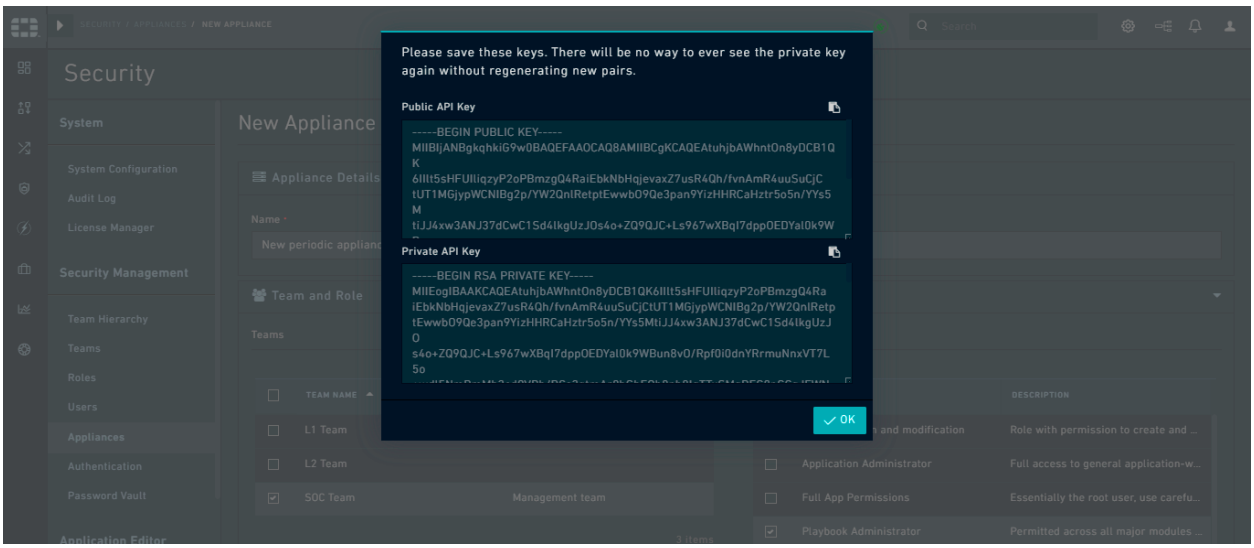


Figure 41. *Cryptographic Keys*

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.

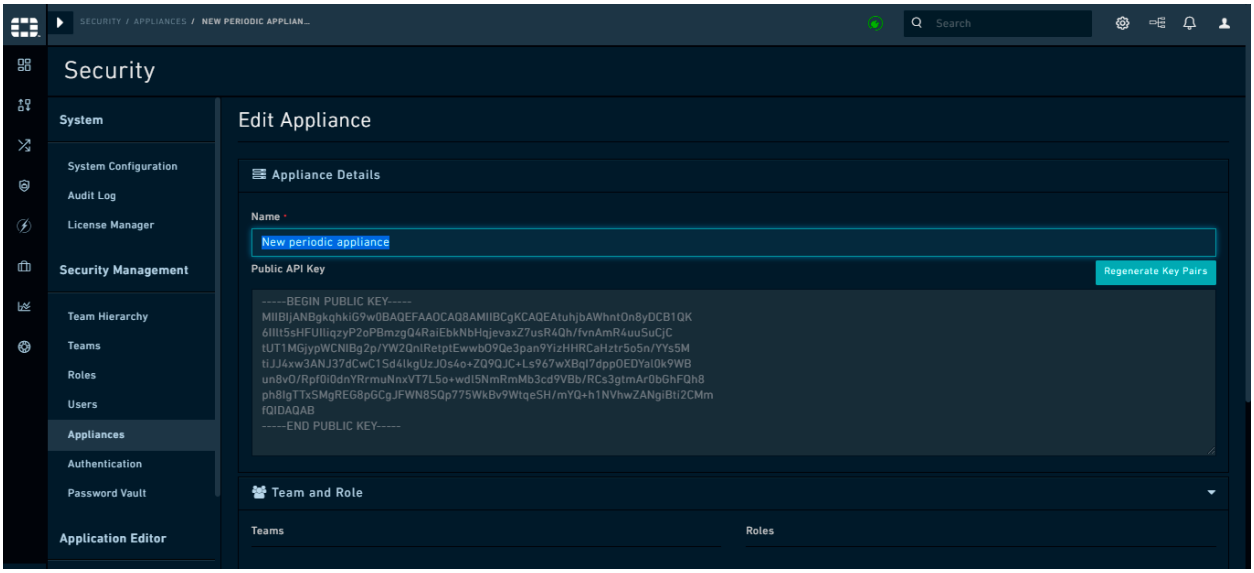


Figure 42. *Appliance Profile*

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.

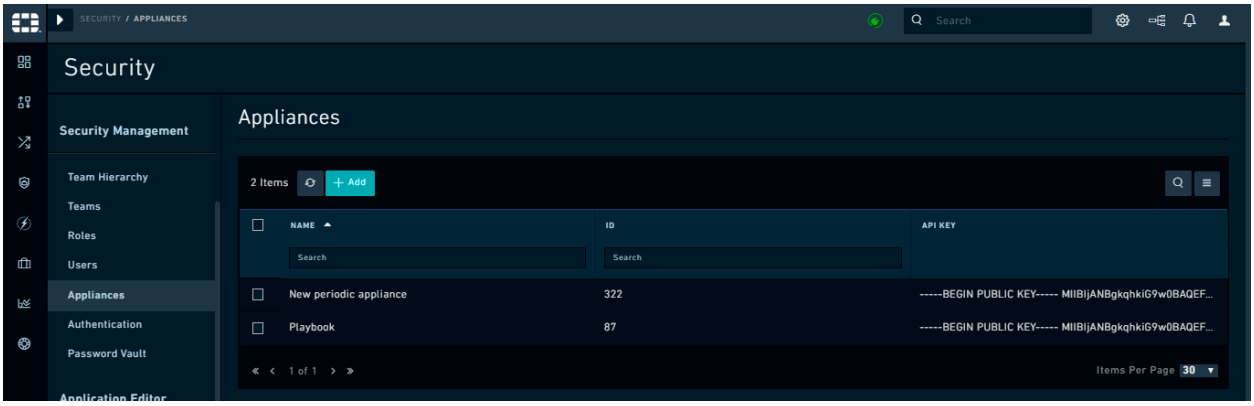


Figure 43. *Appliances Overview Screen*

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

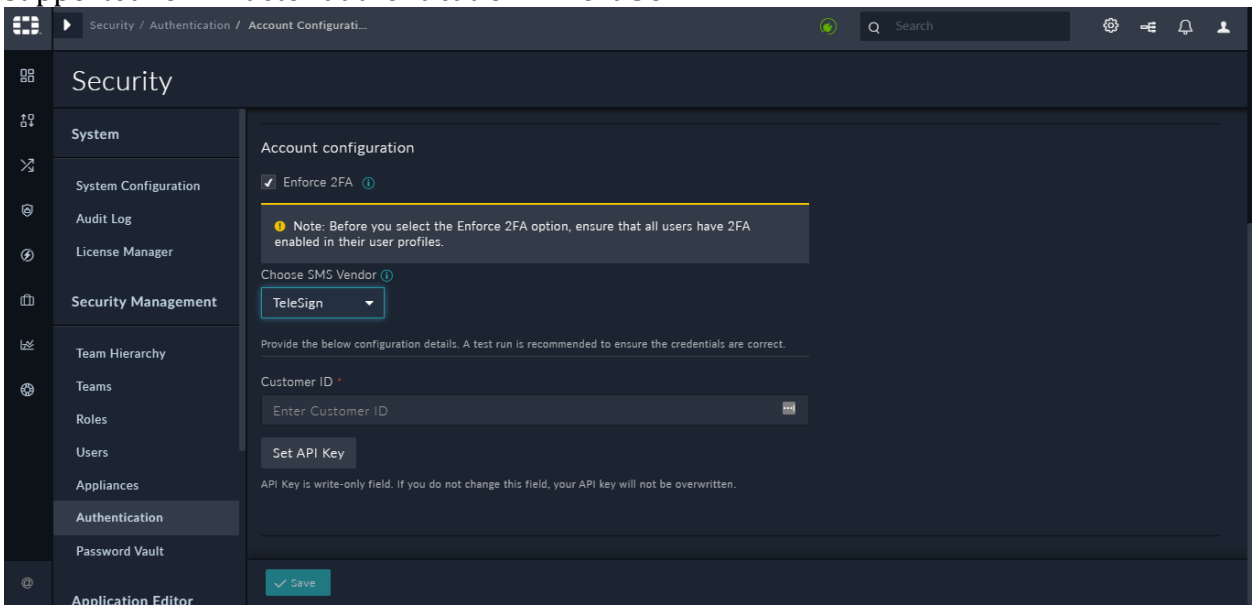
Click **Settings** > **Authentication** to open the `Account Configuration` page. On the `Account Configuration` page, you can configure the following option for user accounts:

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.

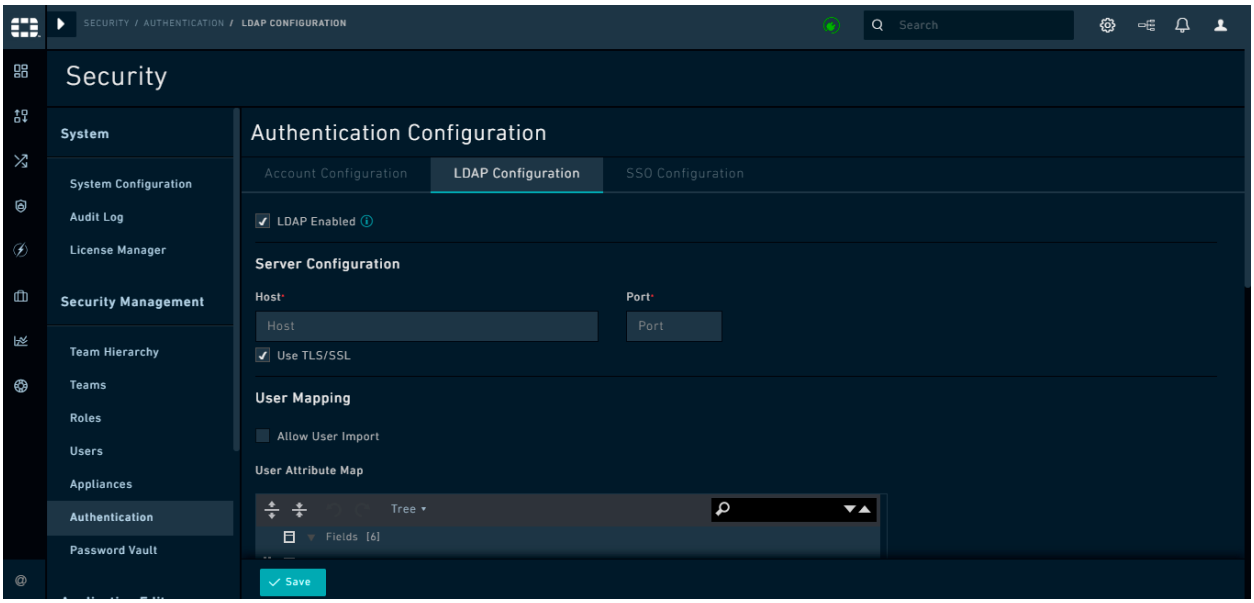


Figure 44. *Authentication Administration Menu*

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.

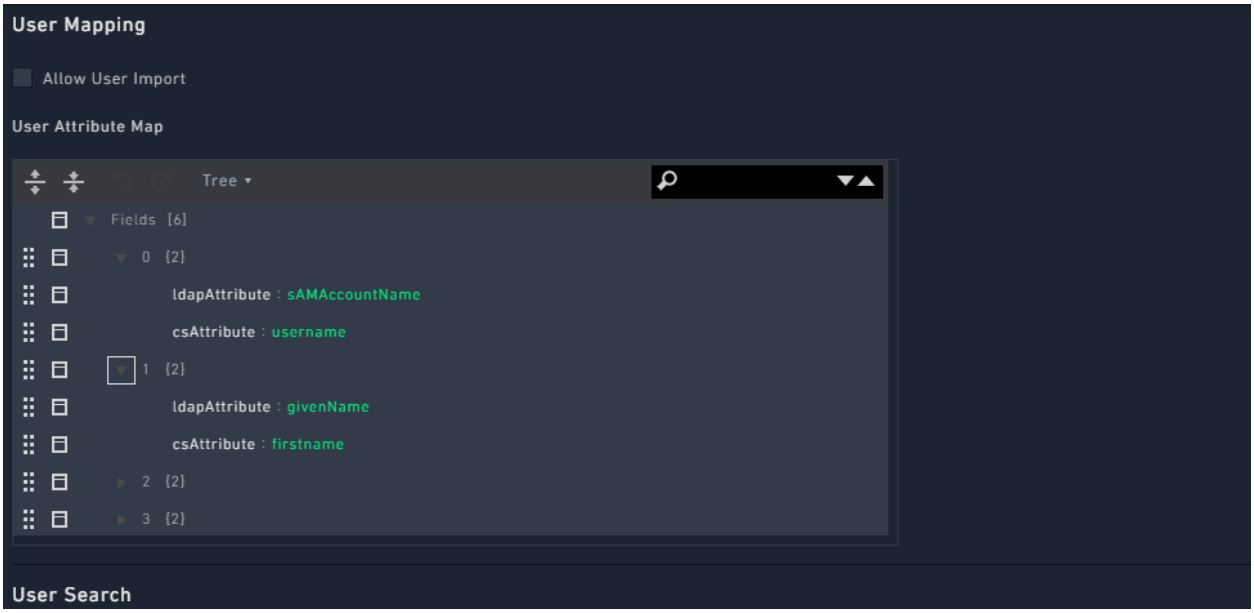


Figure 45. *User Attribute Map*

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.

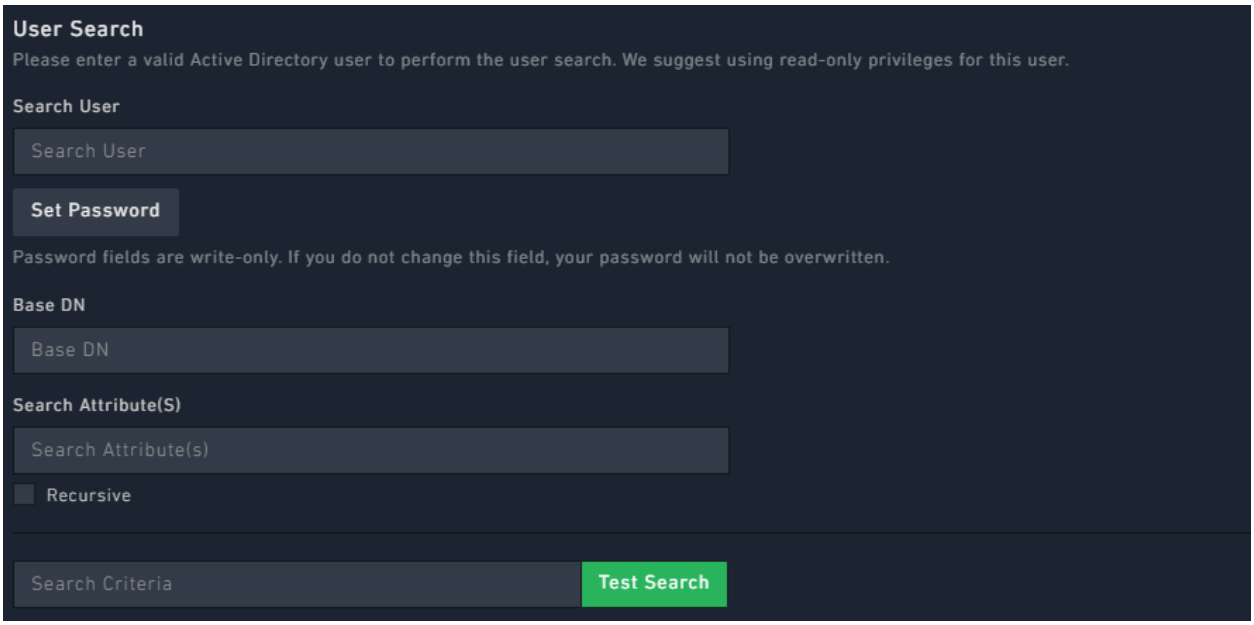


Figure 46. *User Search*

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™ 6.0.0 introduces integration 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™. In FortiSOAR™ 6.0.0, we have 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:

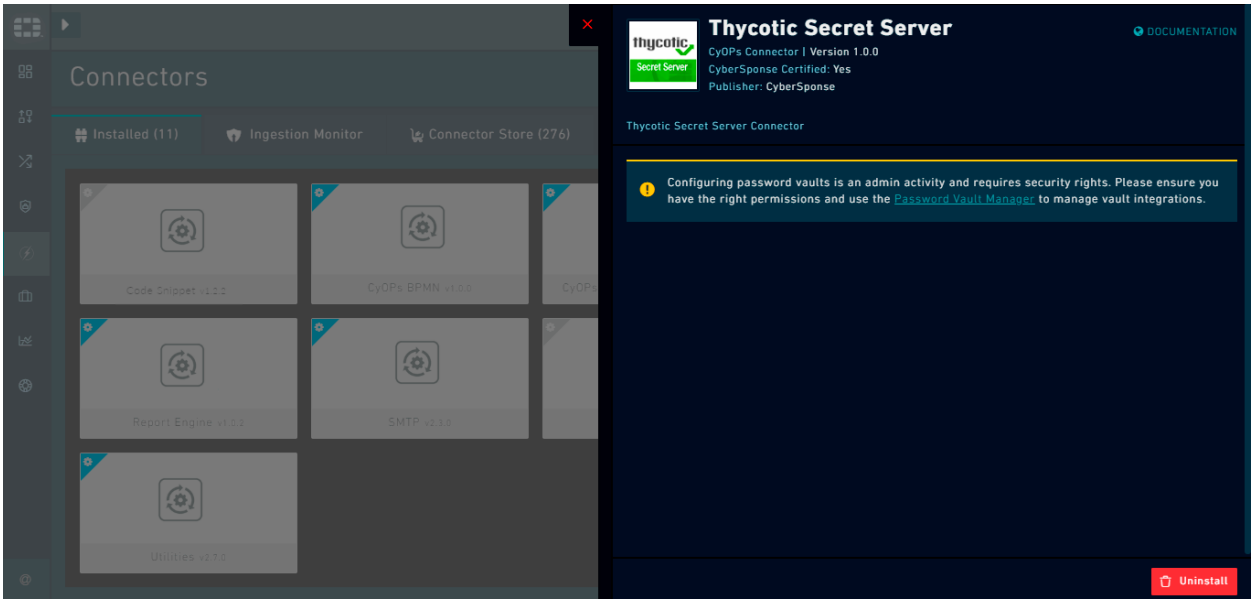


Figure 47. *Connector Configuration dialog in case of connectors that integrate with external vaults*

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.

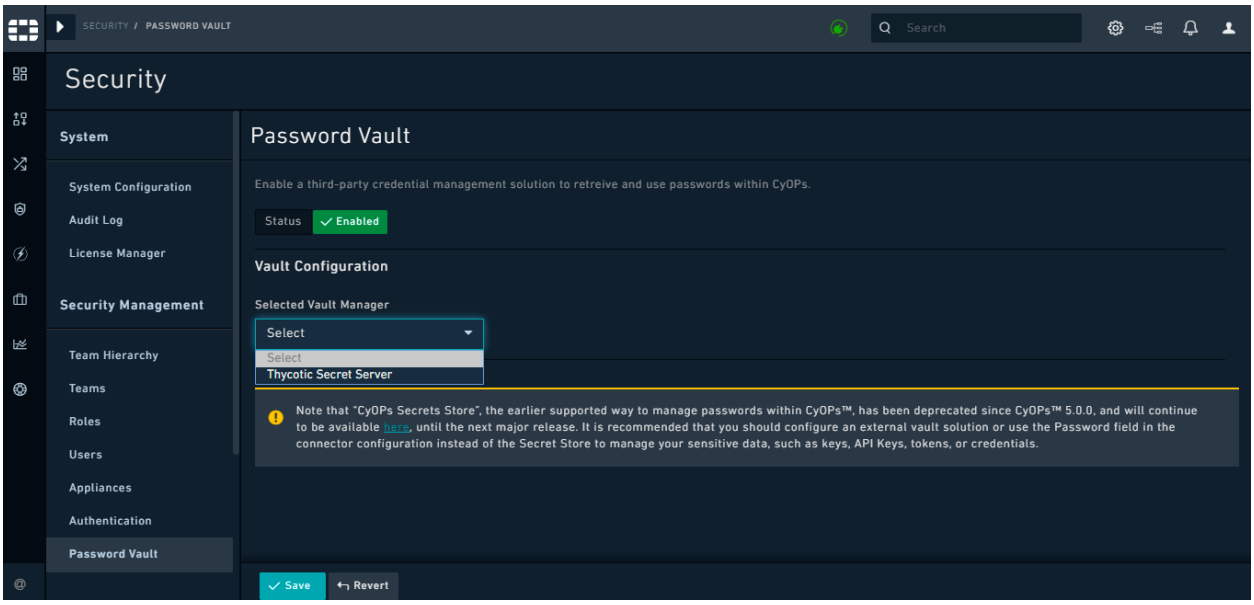


Figure 48. *Password Vault Manager - Enabling the integration*

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

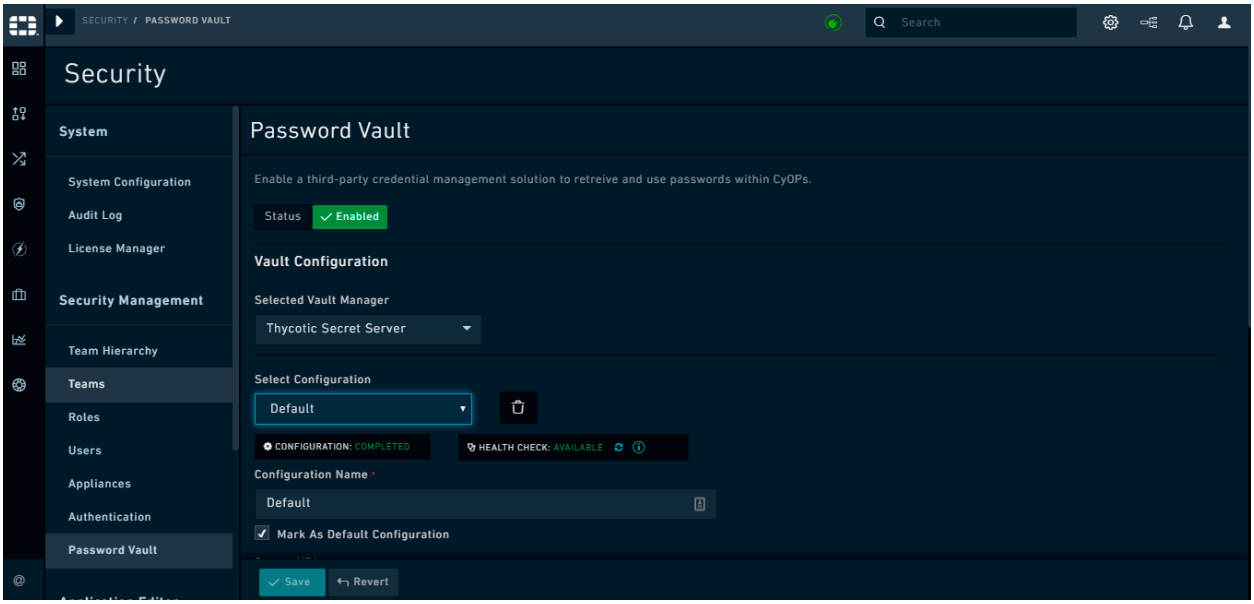


Figure 49. *Password Vault - Configure the vault connector*

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 3rd 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:

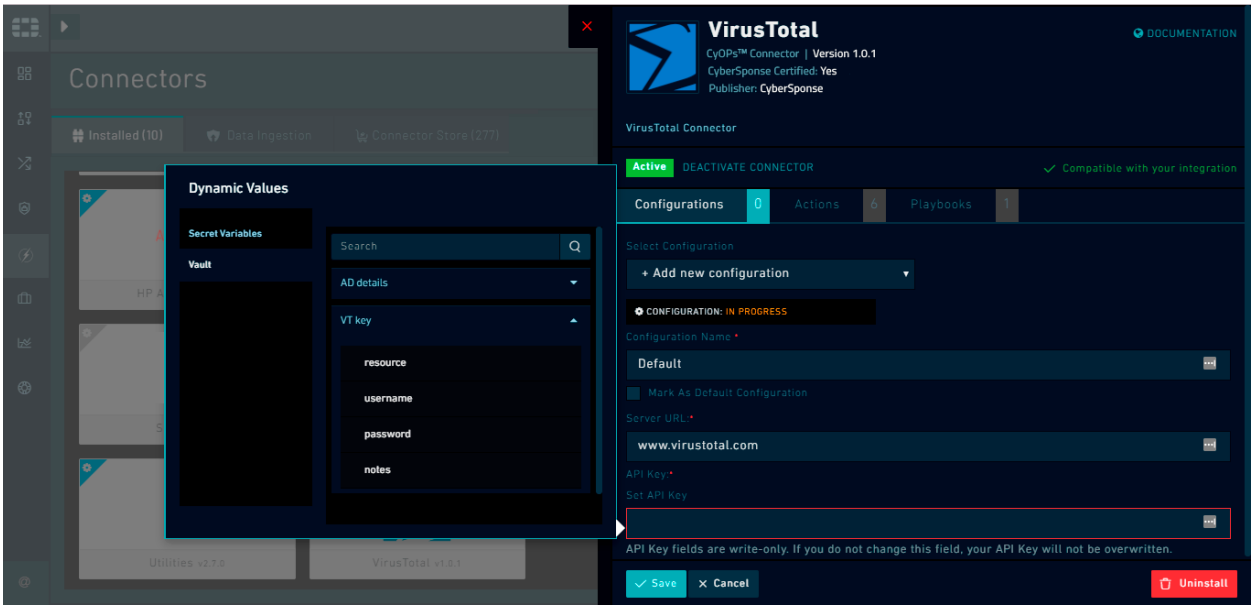


Figure 50. *Connector Configuration - Vault Option*

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 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:

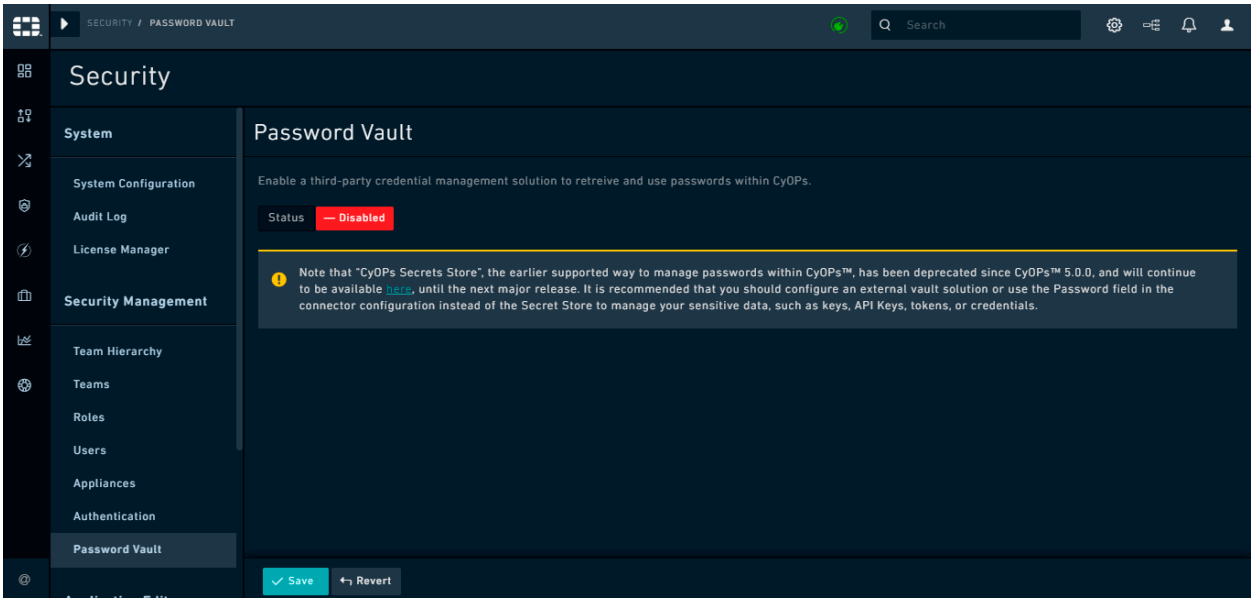


Figure 51. *Password Vault - Link to Secrets Store*

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.

Warning "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:

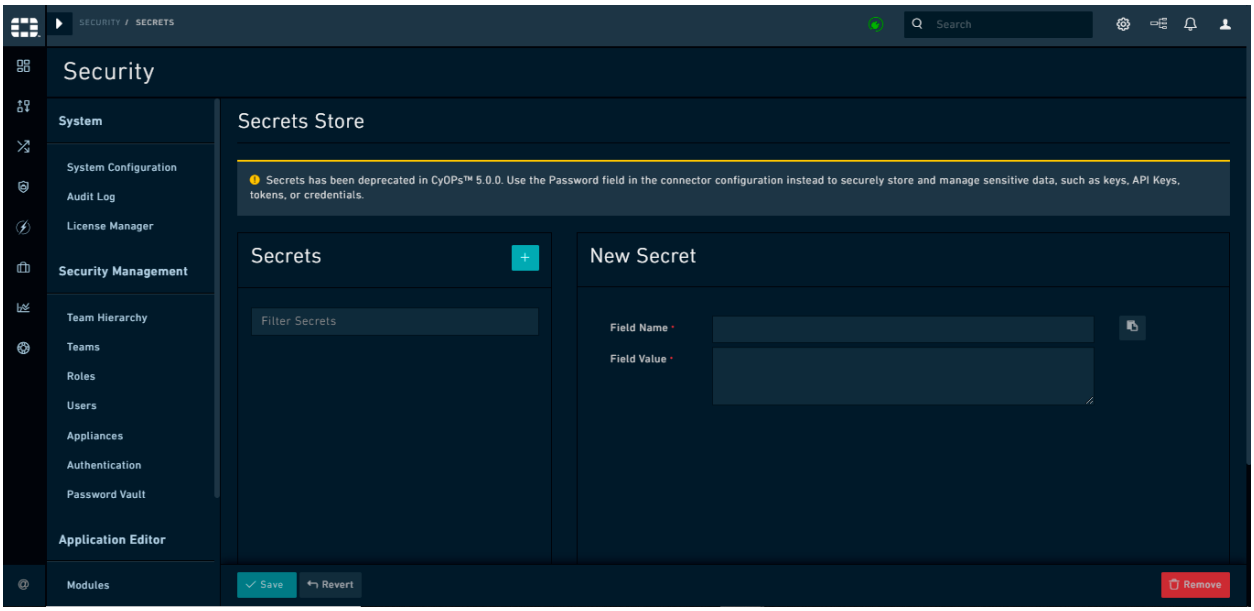


Figure 52. *Deprecated Secrets Store page*

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

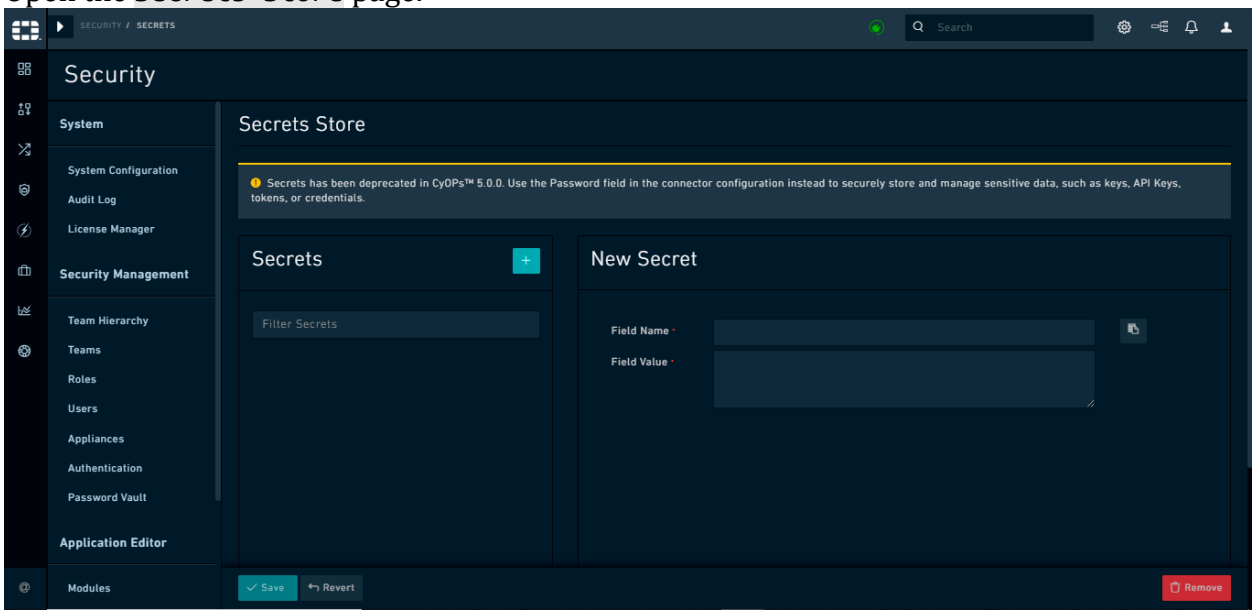
If you have a user who is creating a playbook that requires access to JIRA, a 3rd party integration, and you do not want to provide the JIRA credentials (username-password pair) to users, you can add a secret to store the credentials. FortiSOAR™ stores the secret fields' variable reference in a jinja 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

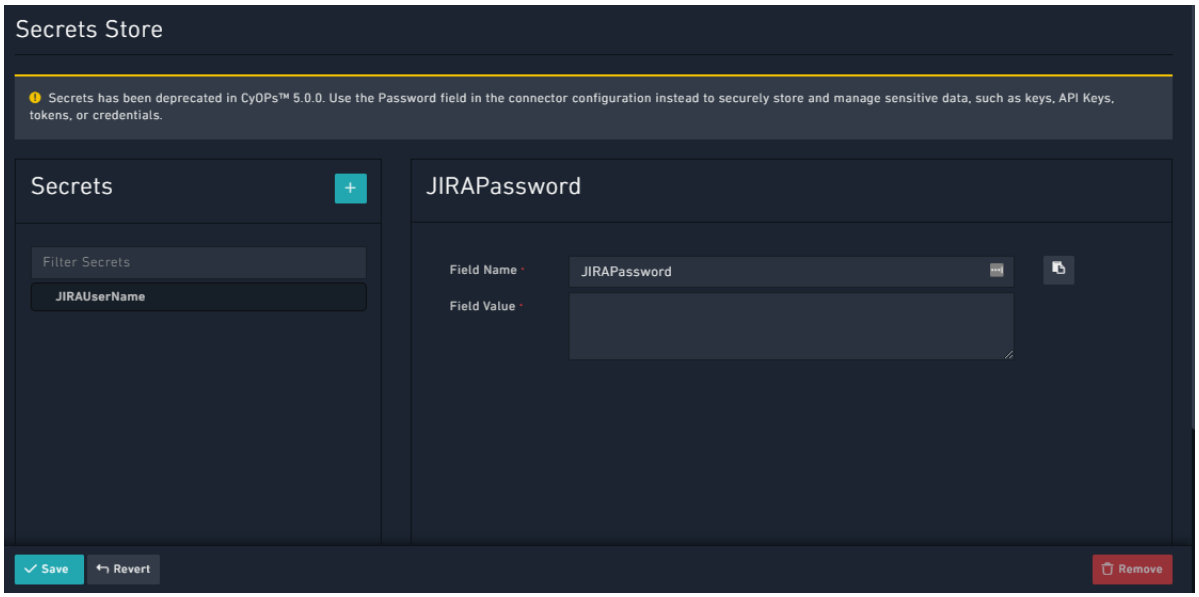
Note: The following procedure details the method of adding a secret in version 5.0.0 and later, though this is **not recommended**.

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:

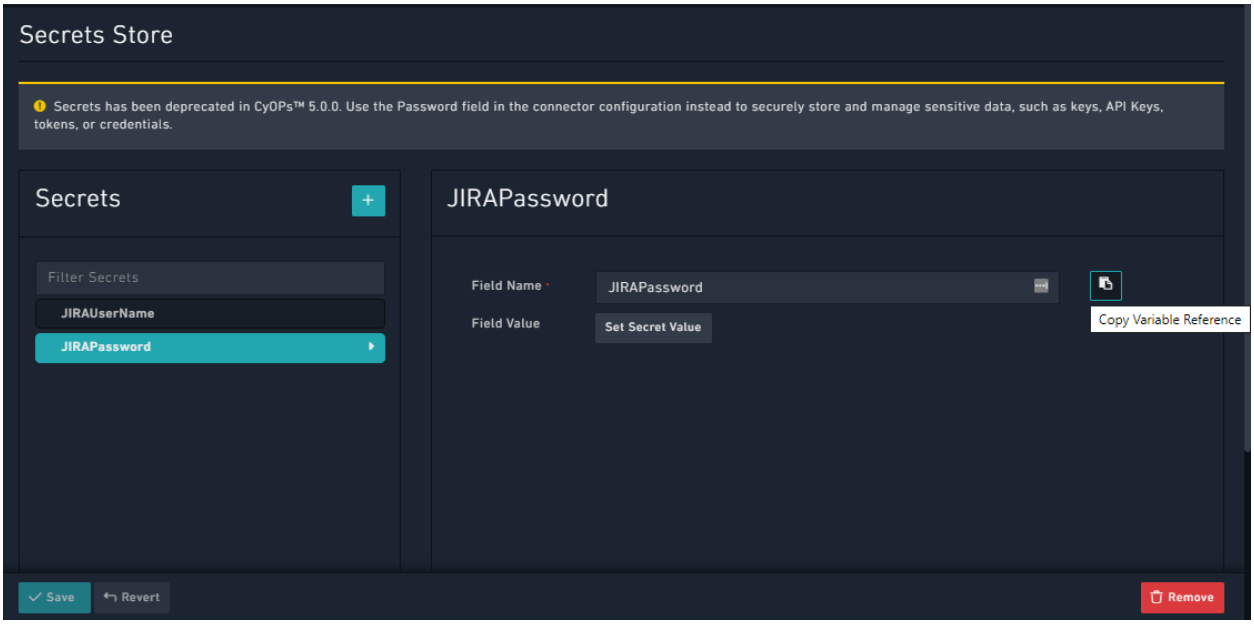


Figure 53. *Secrets - Copy Variable Reference icon*

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 in version 5.0.0 and later 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 UUID of the user(s) that you want to delete in the `usersToDelete.txt` file, which is located at `/opt/cyops/configs/scripts/`.
   The `usersToDelete.txt` file is an empty text file in which you can enter the users UUIDs.
2. SSH to your FortiSOAR™ VM and login as a *root* user.
3. 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.

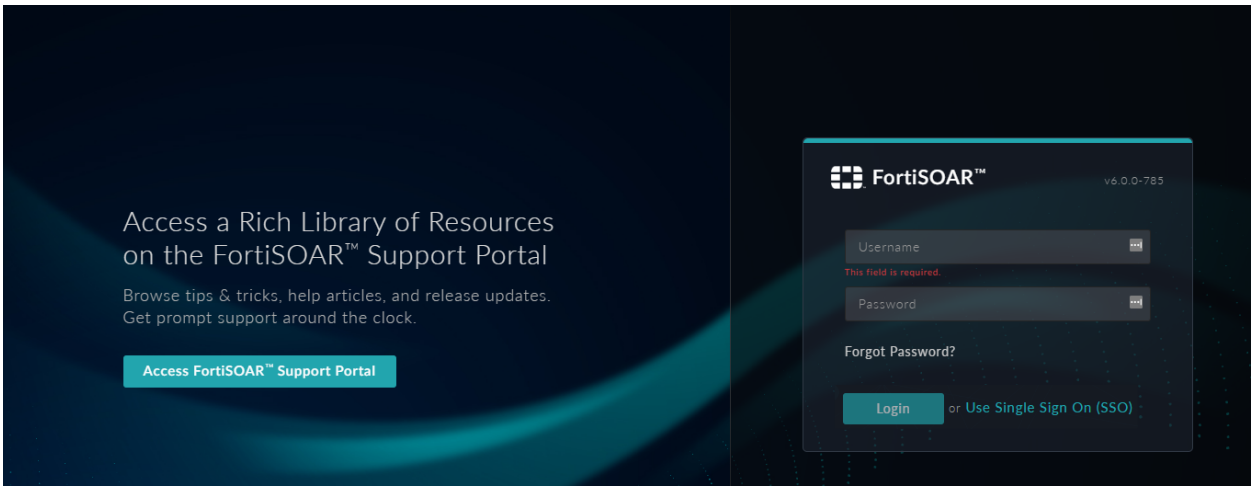


Figure 54. *FortiSOAR™ login page with Single Sign-On*

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.

Version 5.0.0 and later provides you with the ability to 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™

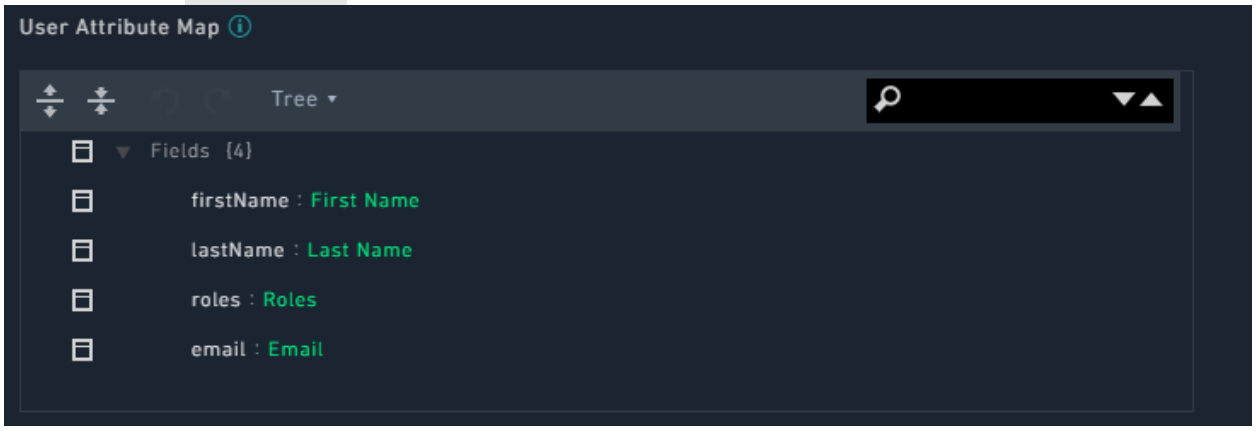
Configuring SAML is a two-way process. The SP configuration that is present in the FortiSOAR™ UI must be made at the IdP. Similarly, the IdP configuration must be added to the FortiSOAR™ UI.

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.

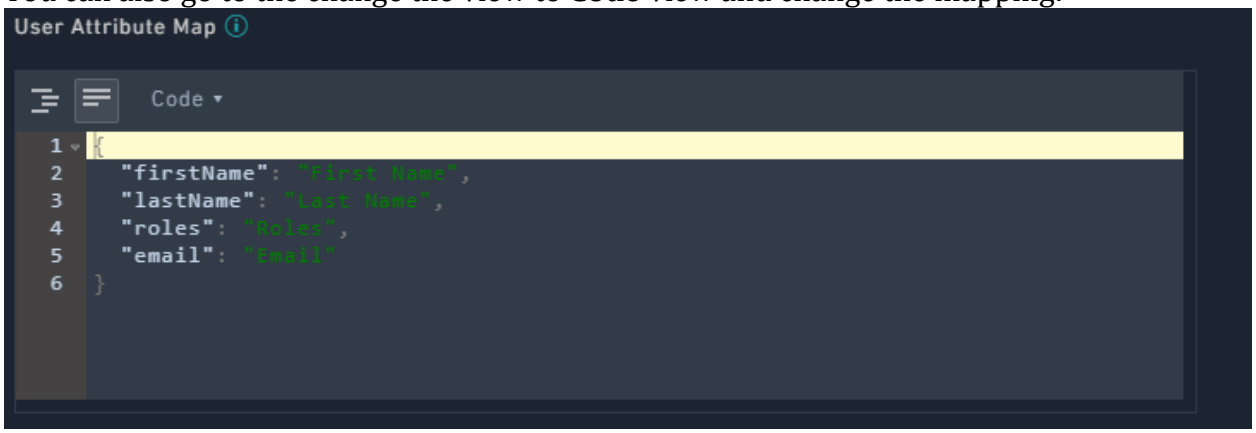
1. Log on to FortiSOAR™ as an administrator.
2. Click **Settings** > **Authentication** > **SSO Configuration**.
3. To enable SAML for FortiSOAR™, click the **SAML Enabled** check box.
4. In the `Identity Provider Configuration` section, enter the IdP details.
   Get the details for OneLogin from the 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`.

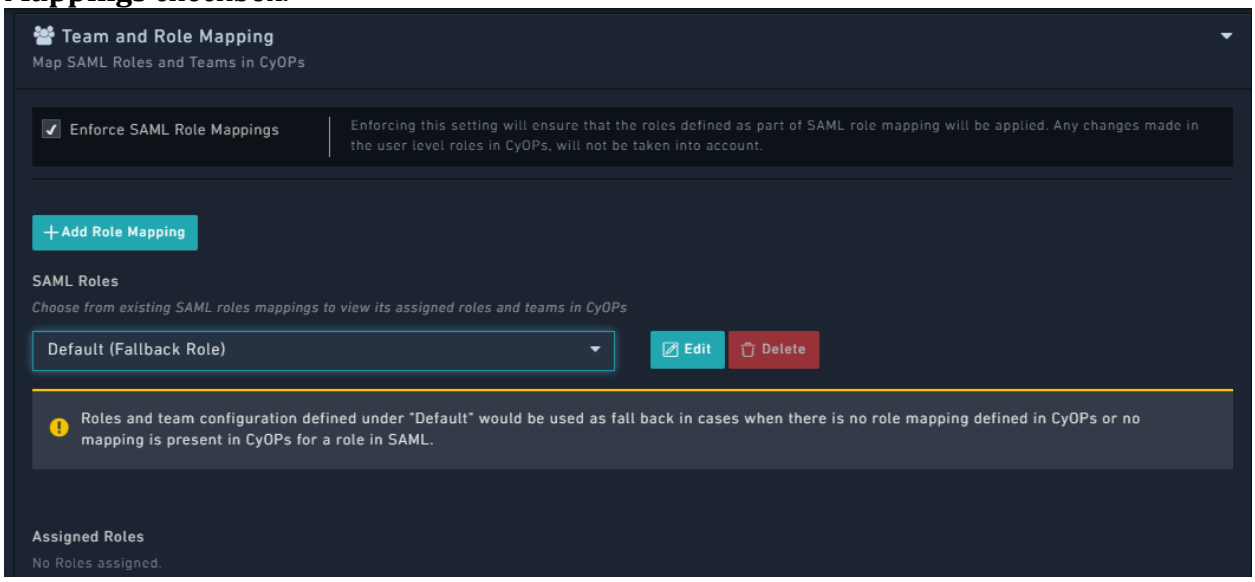


   You can also go to the change the view to **Code** view and change the mapping:



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.



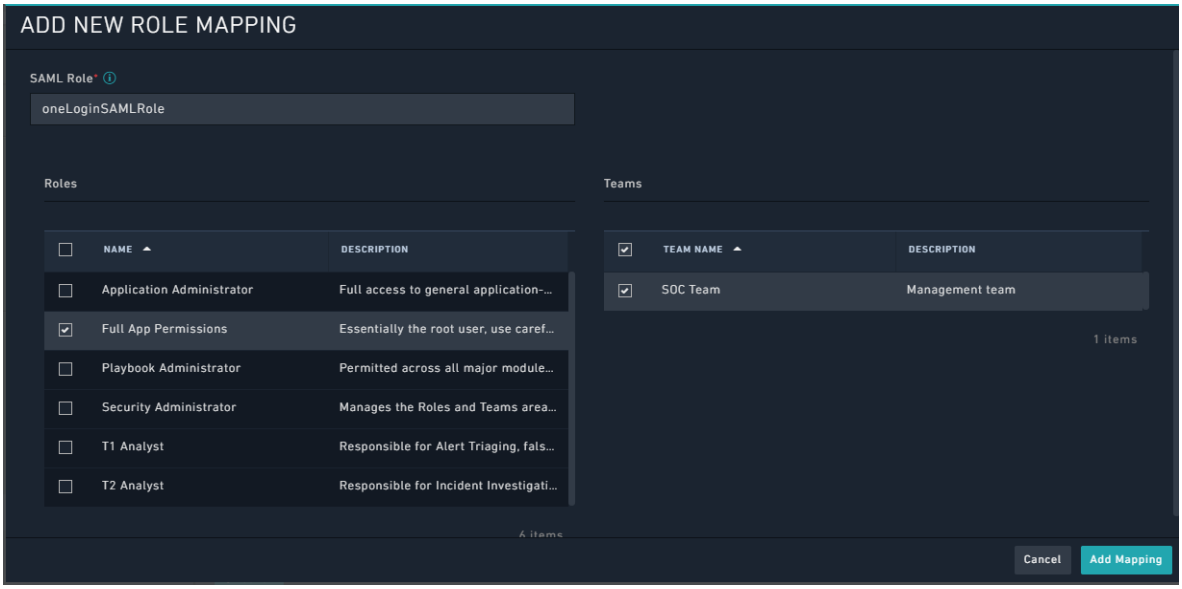
b. To map a role in the IdP to a FortiSOAR™-role and optionally a team in FortiSOAR™, in the `Team and Role Mapping` section, click **Add Role Mapping**.

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.

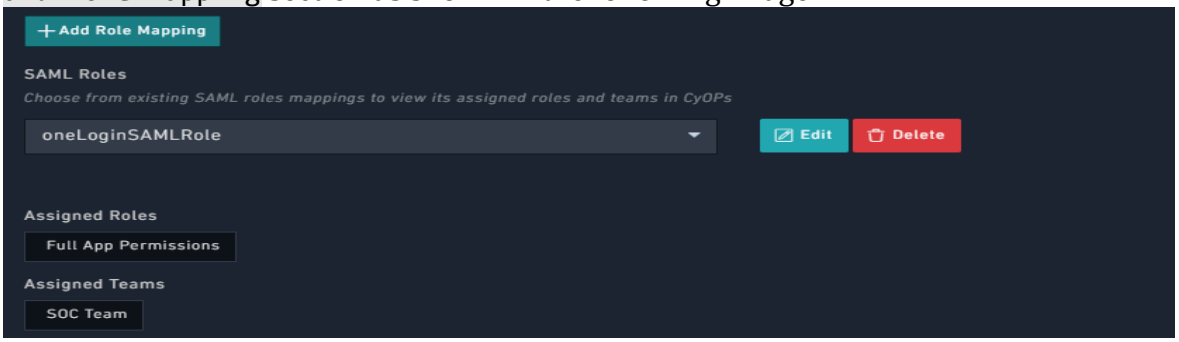
   ii. From the `Roles` column, select the FortiSOAR™ role(s) that you want to assign to the role that you have specified in the SAML Role field.

   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.



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 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:

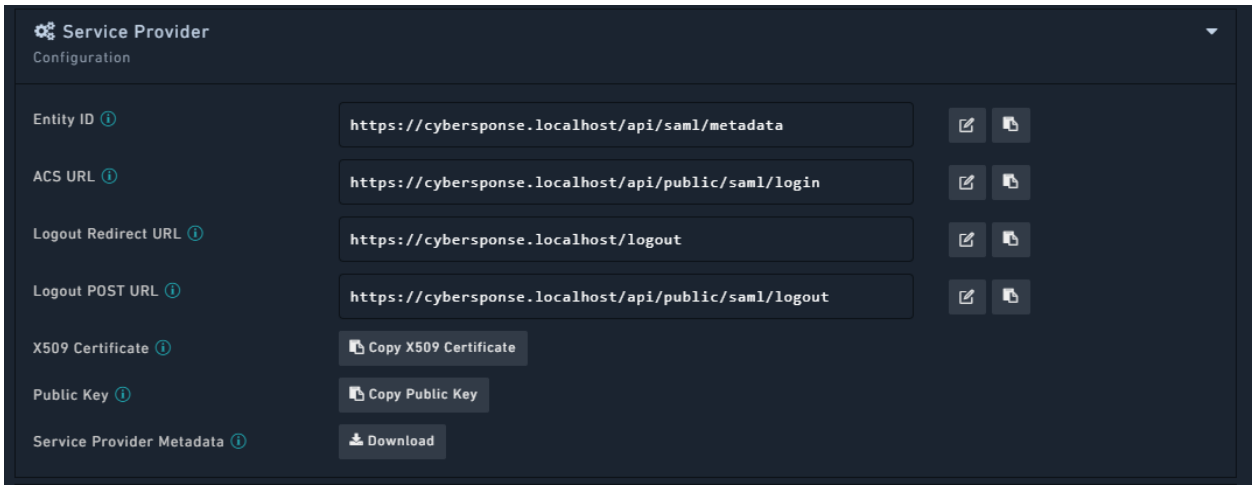


As shown in the above image, the `oneLoginSAMLRole`, i.e., the role defined in the IdP has been mapped to the `Application Administrator` role and the `SOC Team` in FortiSOAR™.

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**.

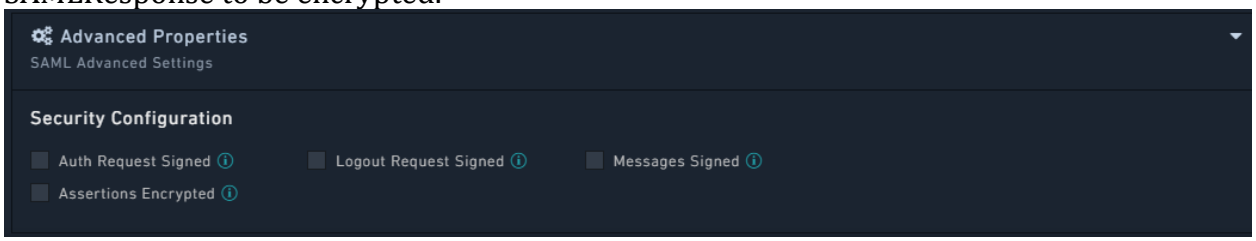
FortiSOAR™ displays a confirmation dialog, click **Confirm** to delete the role.

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™.



   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.

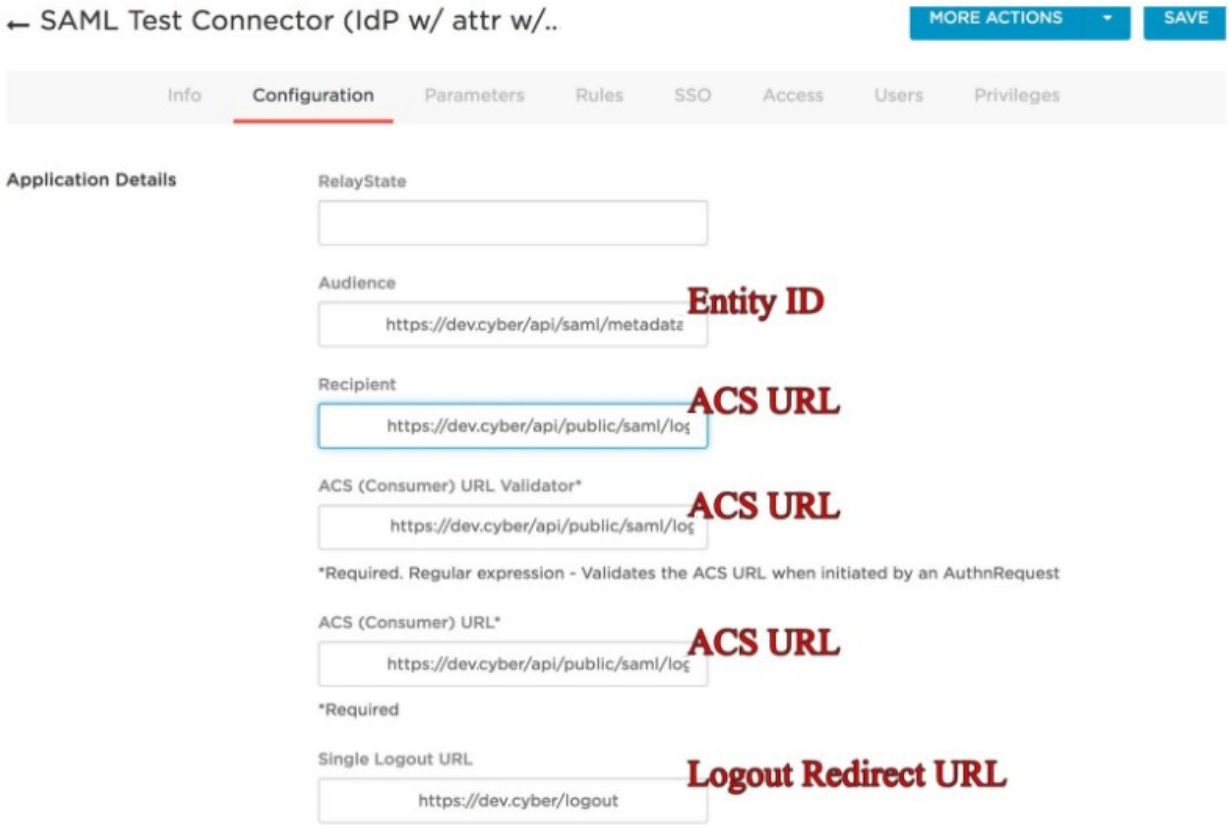


9. Click **Save** to complete the SAML configuration in FortiSOAR™.

Configuring SAML in OneLogin

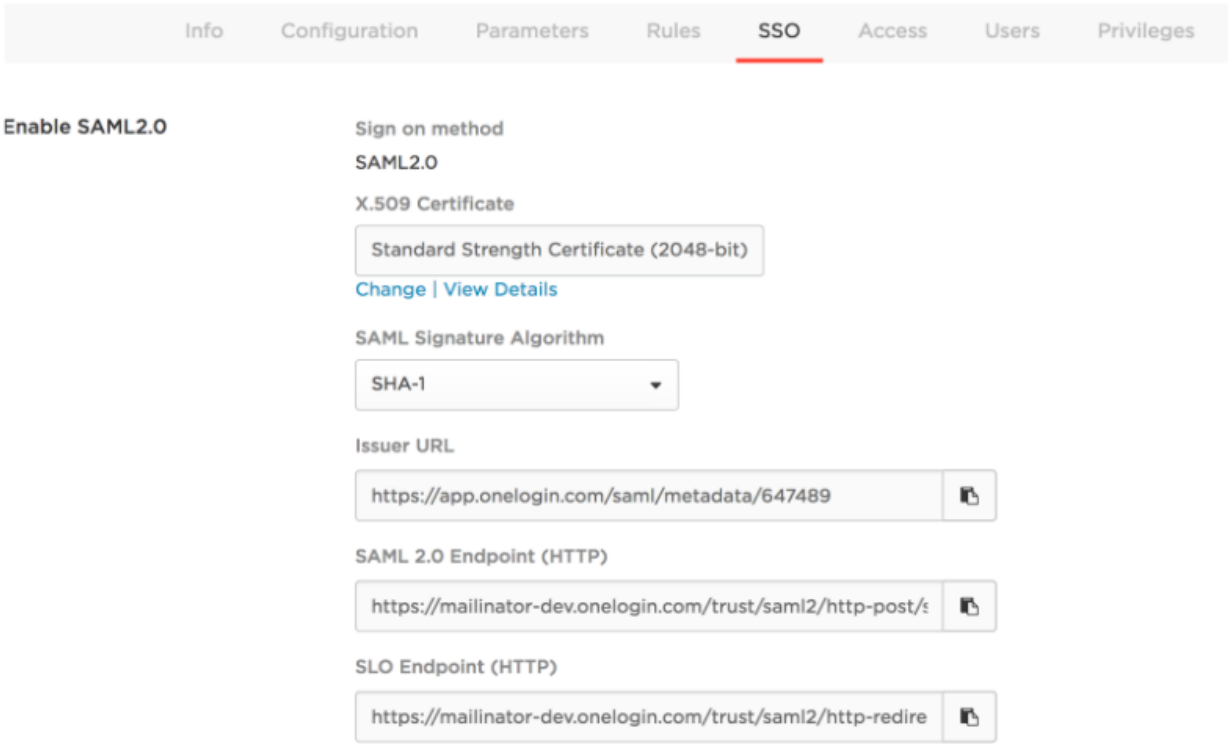
1. Log on to OneLogin as an administrator.
2. Create a new application in OneLogin. Navigate to **APPS** > **Company Apps** > **ADD APP**. In the Find Applications section, search for `saml` and select **SAML Test Connector (IDP w/attr w/sign response)**. Save the application.

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:



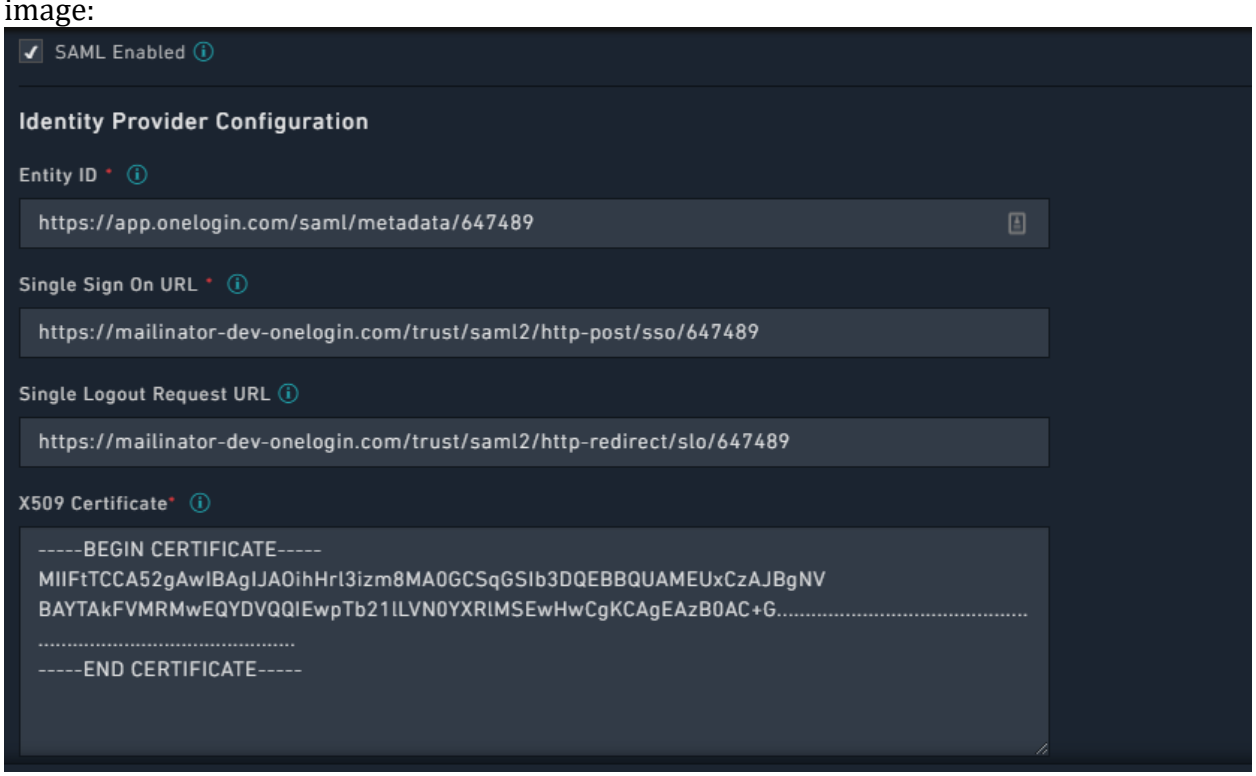
4. Get SSO details. On the SAML Test Connector (IDP w/attr w/sign response), click the **SSO** tab and you will see the SSO details of OneLogin (IdP) as shown in the following

image:

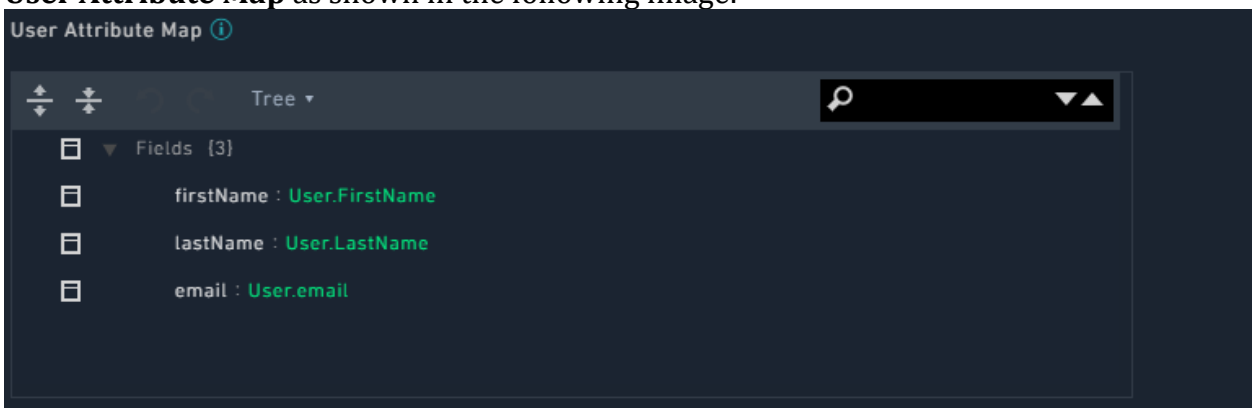


5. Add the SSO details shown in step 4 in FortiSOAR™. To add the SSO details, log on to FortiSOAR™, click **Settings** > **Authentication** > **SSO Configuration**. In the `Identity Provider Configuration` section, enter the IdP details as shown in the following

image:

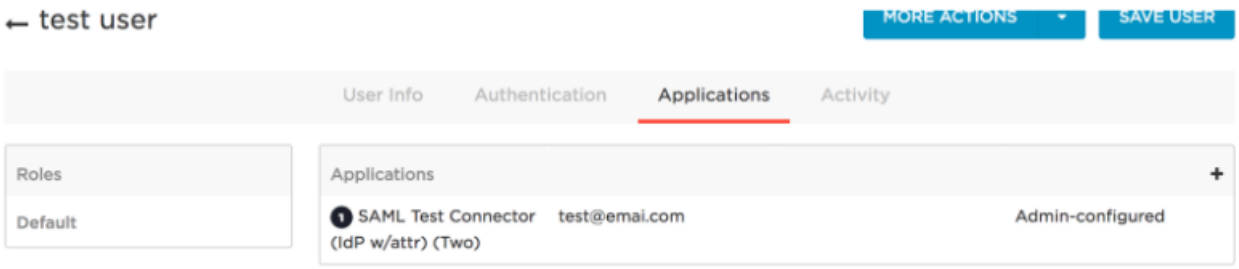


6. Add the default user attribute mapping for OneLogin in FortiSOAR™ by updating the **User Attribute Map** as shown in the following image:



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.

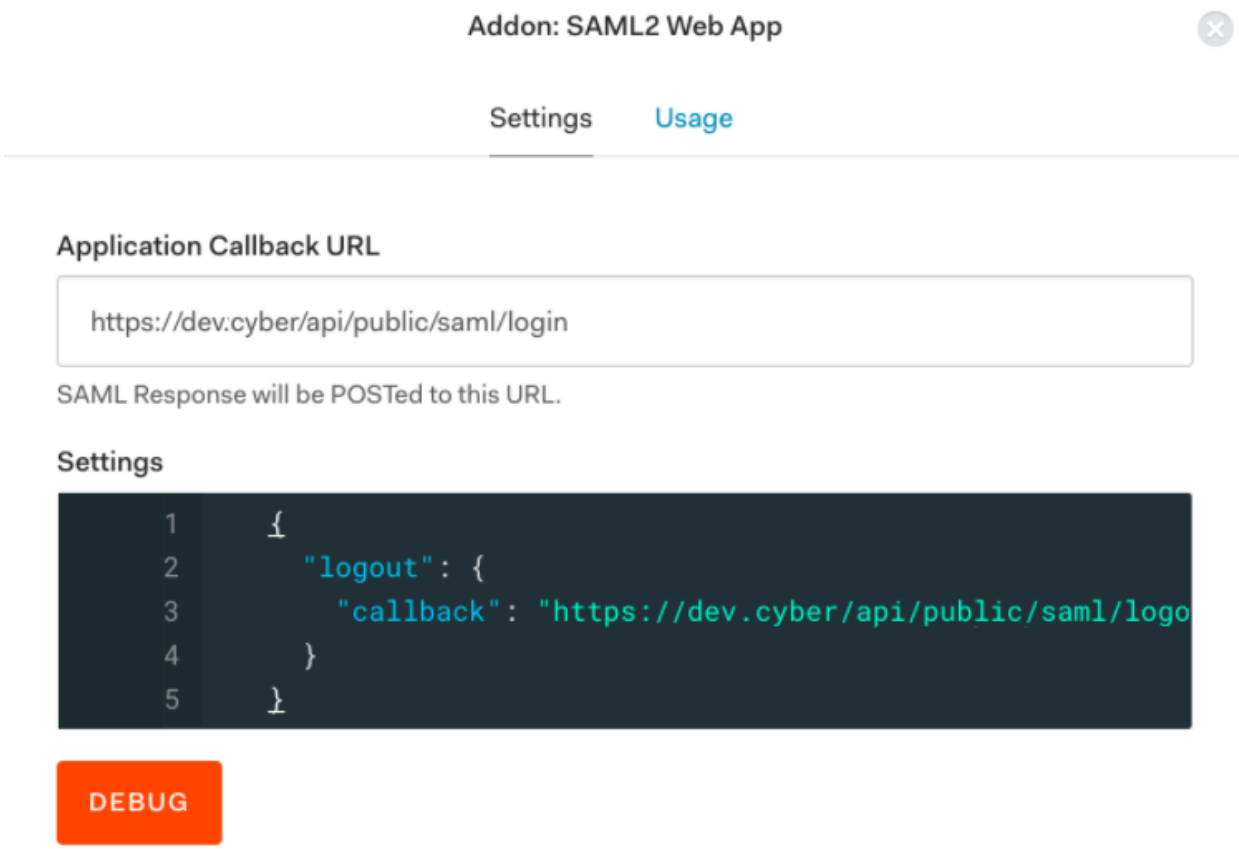


Once the user is created, you must assign the user a password by clicking **MORE ACTIONS**.

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`

section on the FortiSOAR™ `SSO Configuration` page, as shown in the following image:



4. Get SSO details. Download `Identity Provider Metadata`, by navigating to **App configuration** > **Addons** > **SAML2** > **Usage** > **Identity Provider Metadata**. Click **Download**. The Identity Provider Metadata appears as shown in the following image:

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:

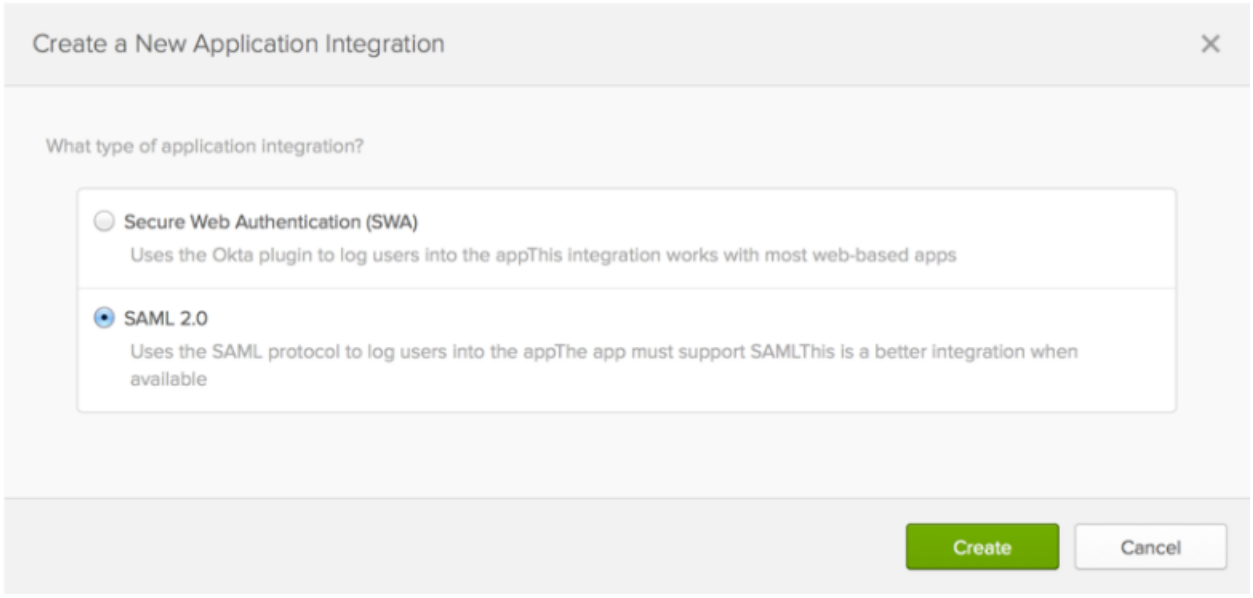
     ```
     zCCAeegAwIBAgIJZAzJWzHeGWUiMA0GCSqGSIb3DQEBCwUAMB0xGzAZBgNVBAMTEm8xMDg0MzYwLmF1dGgwLmNvbTAeFw0xNzA0MDEwNzMwMDBaFw0zMDEyMDkwNzMwMDBaMB0xGzAZBgNVBAMTEm8xMDg0
     MzYwLmF1dGgwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKhOggZ4r3jq2iAgrFNZv0IoEJZVKA6mhmpfFiqsBvAliUbtEireTpSfSO1SP/
     YaW7ODamSBZrb06VRCmt+LzsGwsXPJTZDwqORYraA3w4dSp5mnC7VLjyTrmMazRbcWo6Egq6N6v+OE48z0Qtd/
     Fb5wTdi8yKmxVV8xNYIEhRdcTIRoTjYZ0oc1j26BX7xOe3wYBIzly0JzkRCkZjpEOFZMIeC8cmMEJdDS3UEV/4nYsgLVi4CB/Y9Wwf4kbyLE1pTAKWBsbdgbBk5aYRxu1qNhu3ZuUT7AV/
     PEgXoBJIsFJiru37ORVp0Smi4F/Ji2rZk85Loj3hG0+G6CFYkzKnMCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUuRCNNTfAOfiQNeZdDE0nQUwza9QwDgYDVR0PAQH/
     BAQDAgKEMA0GCSqGSIb3DQEBCwUAA4IBAQBDGs3tN5W9wByql+hHZ83268Cow3t8iTeWmkWG9PLYZIL6AviKgN7Xa8vHos05/
     Kf0p5A1MoXKJ46QkUIEhusDIufBGNC7i3c3UpZYgaLcIDrf5BXPjUYCQW+ogiQPCuadrZjeImgAmaMsV/ChEucbYUD/
     mDwUqLc3RQ+O+cBHtfQ0eGSivAogmObbkoB3xWwL1hUn+XI3UEC3zlLTNj72FXadDtS7Pp9p4acIOnmlkR/
     YnqOB1MxUNLcM7ainvSwgwSU6zu81PUZkhufbBVnVA2QXHx0zrKVENWhLBBf2Dbn9W0kPychGxDrGmTCBF+VZTqdZf/n9a7EO0AGbK7Nw
     ```

   - Click **Save** in FortiSOAR™ to save the changes to the IdP configuration and user attribute mapping.

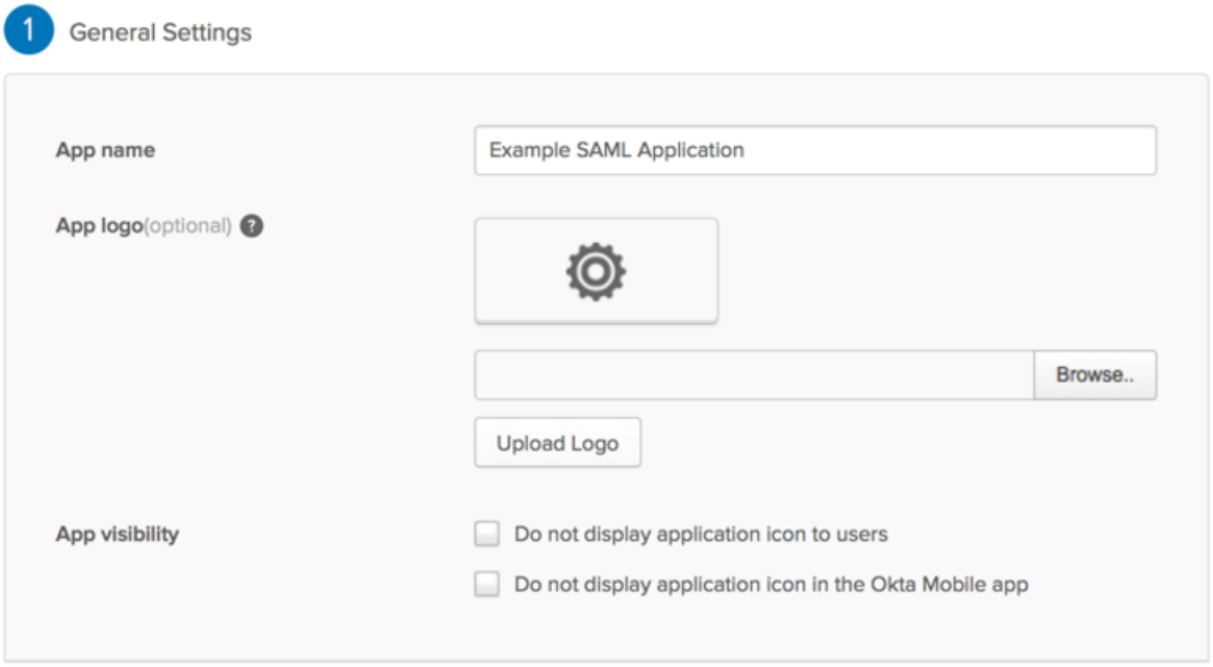
Configuring SAML in Okta

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**.

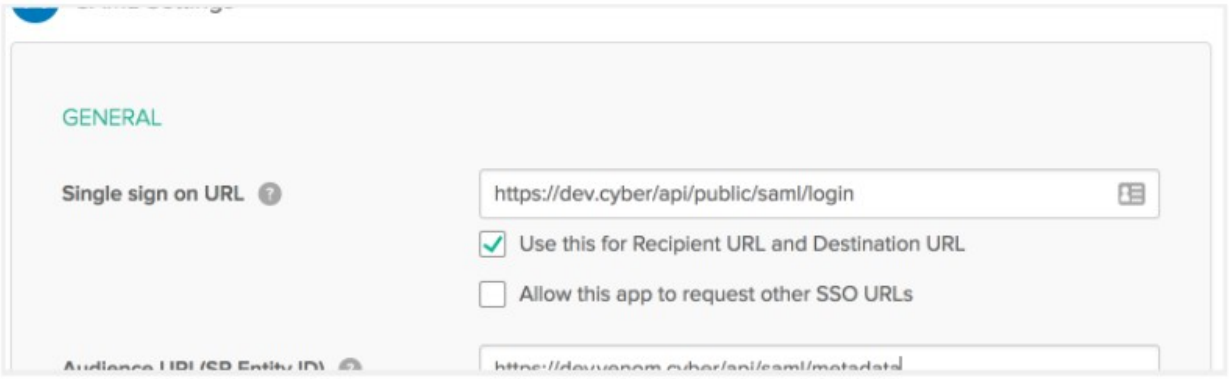


3. Configure IdP.
   - In the newly created application, on the `General Settings` dialog, in the **App name** field, enter the application name and click **Next**.

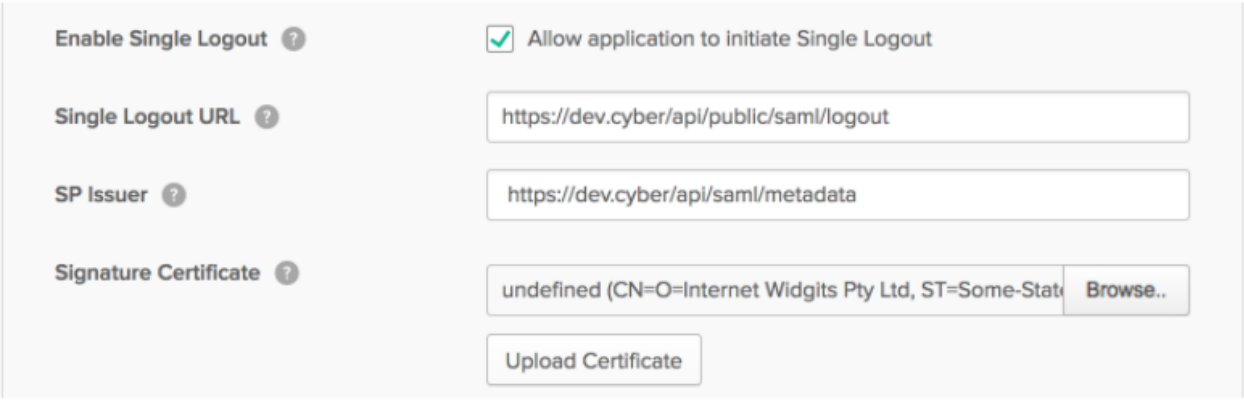


   - On the `Configure SAML` dialog, in the `SAML Settings` section, in the **Single Sign On URL** field, enter or paste the `SP ACS URL` and in the **Audience URI** field,

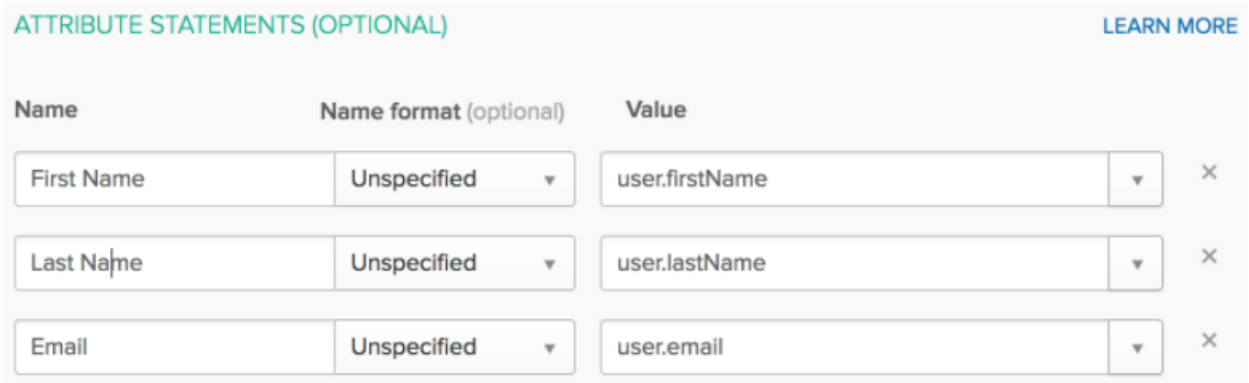
enter or paste the `SP Entity ID`.



- 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**.



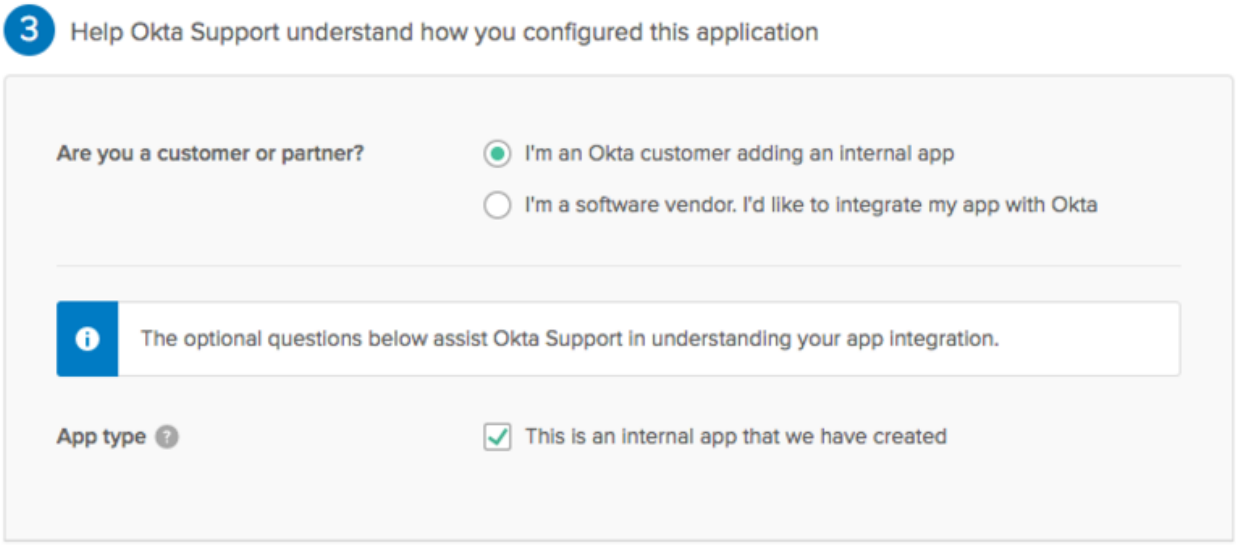
- In the `ATTRIBUTE STATEMENTS (OPTIONAL)` section, set the mapping as shown in the following image:



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™.

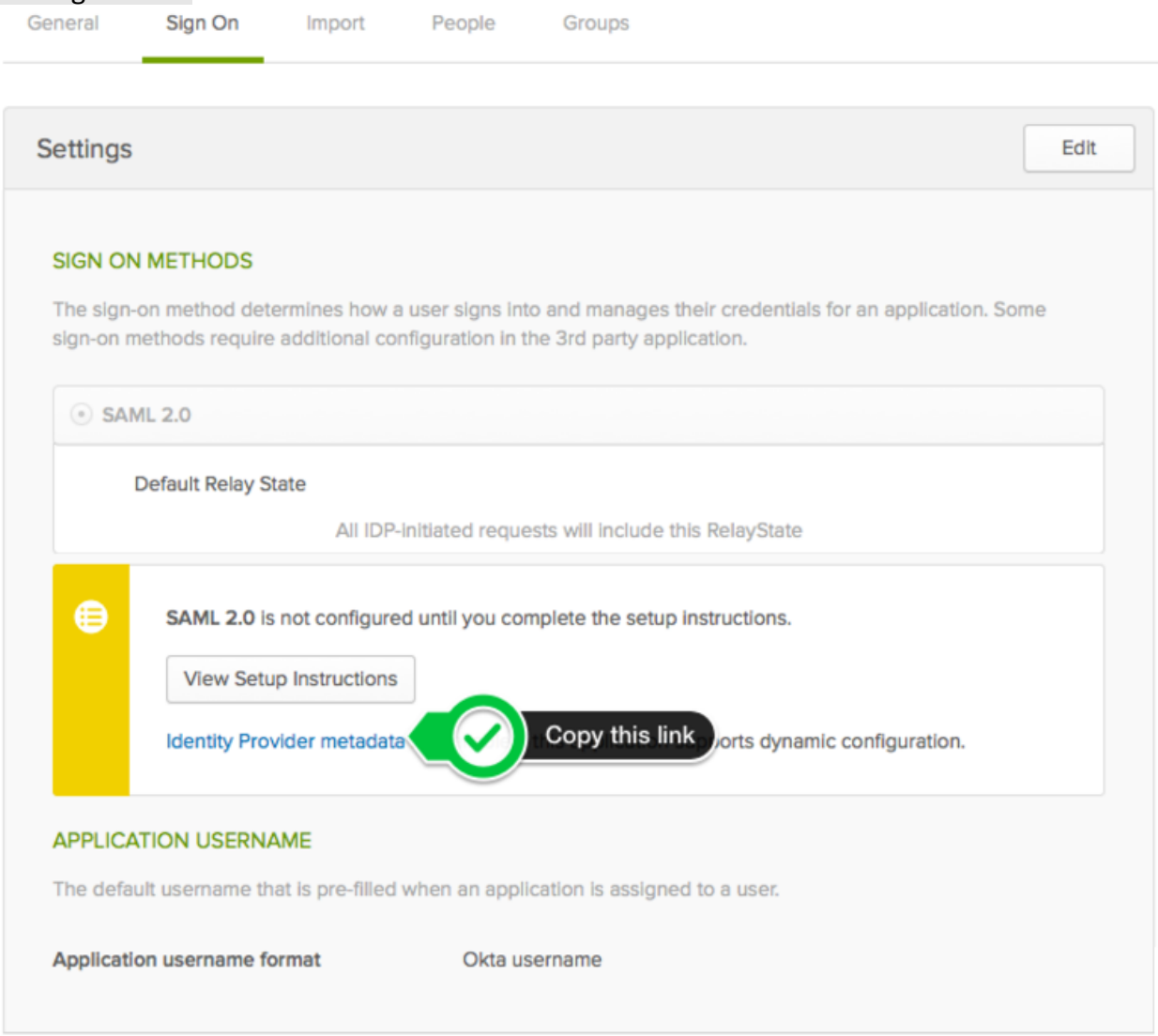
- Click **Next**.

- 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**.

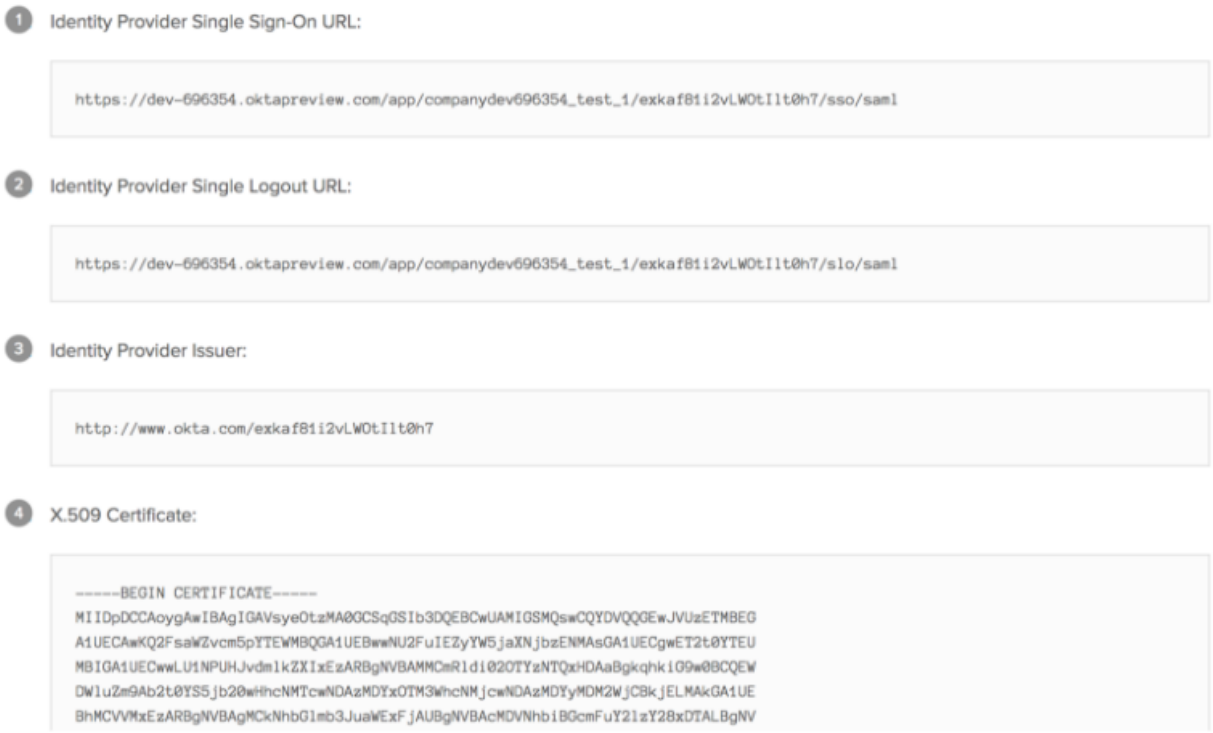


- Click **Finish**.
  The `Sign On` tab of your newly created SAML application gets displayed. Keep this page open in a separate tab or browser window as you will require the information present on this page to complete the `Identity Provider`

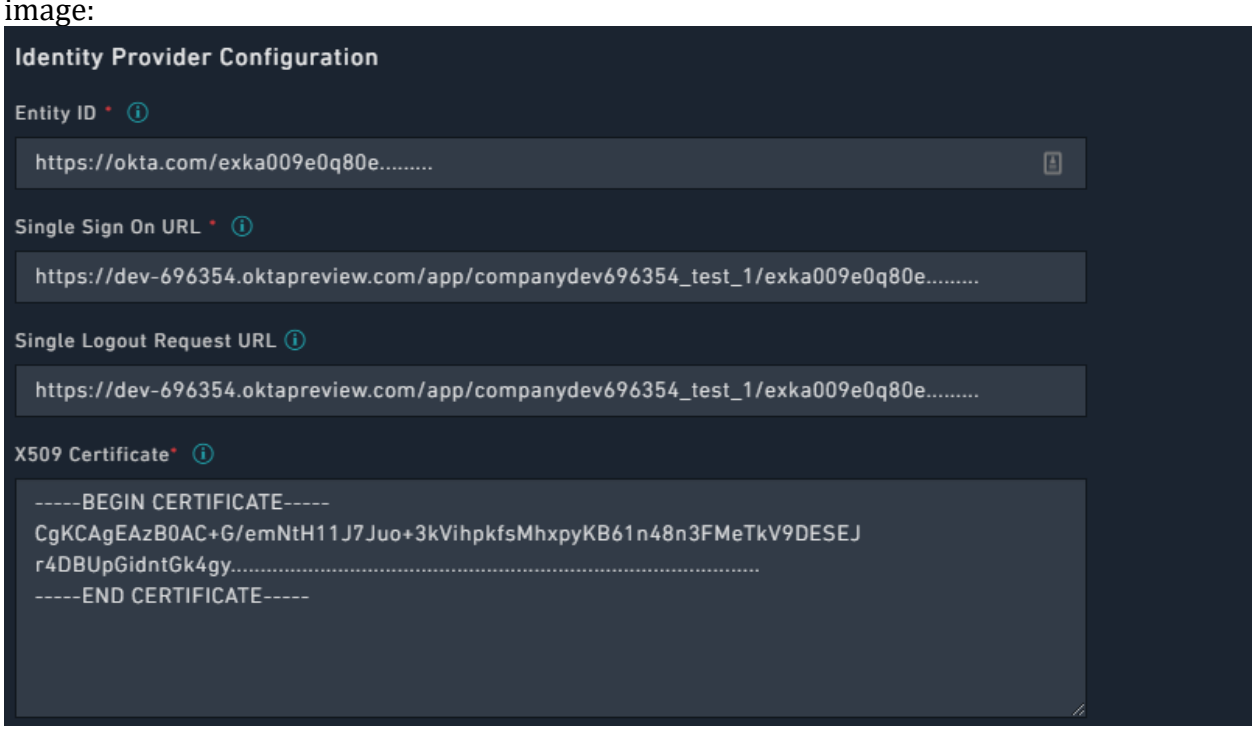
`Configuration` section in FortiSOAR™.



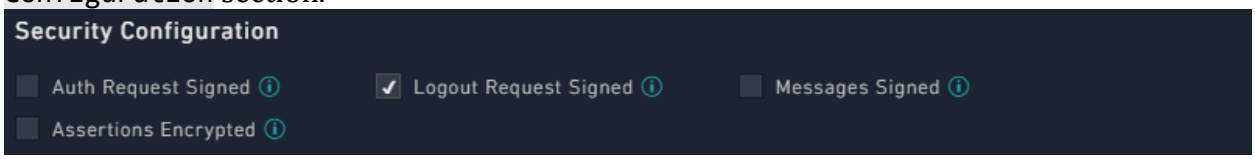
4. Get SSO details. Click **View Setup Instructions** and information as shown in the following image:



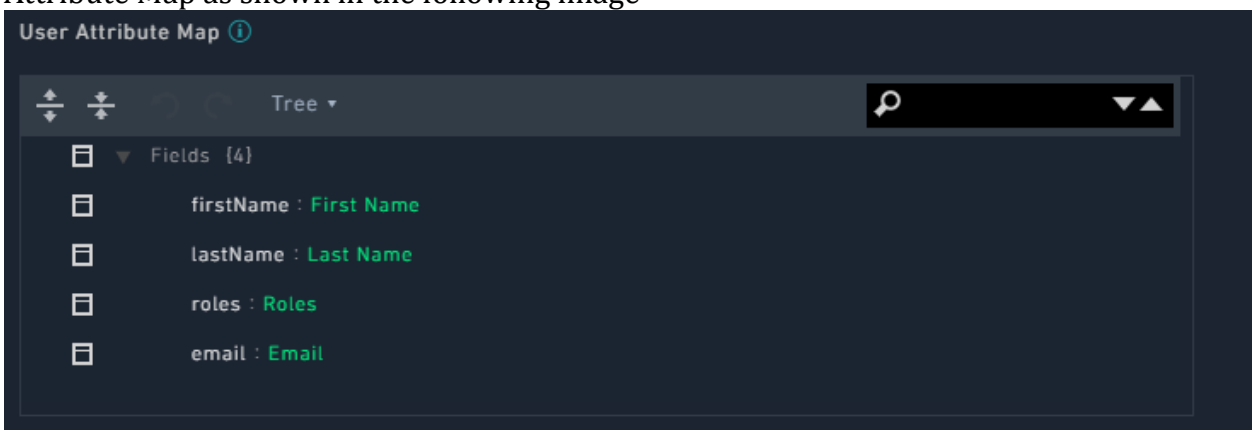
5. Add the SSO details shown in step 4 in FortiSOAR™. To add the SSO details, log on to FortiSOAR™, click **Settings** > **Authentication** > **SSO Configuration**. In the `Identity Provider Configuration` section, enter the IdP details as shown in the following image:



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.

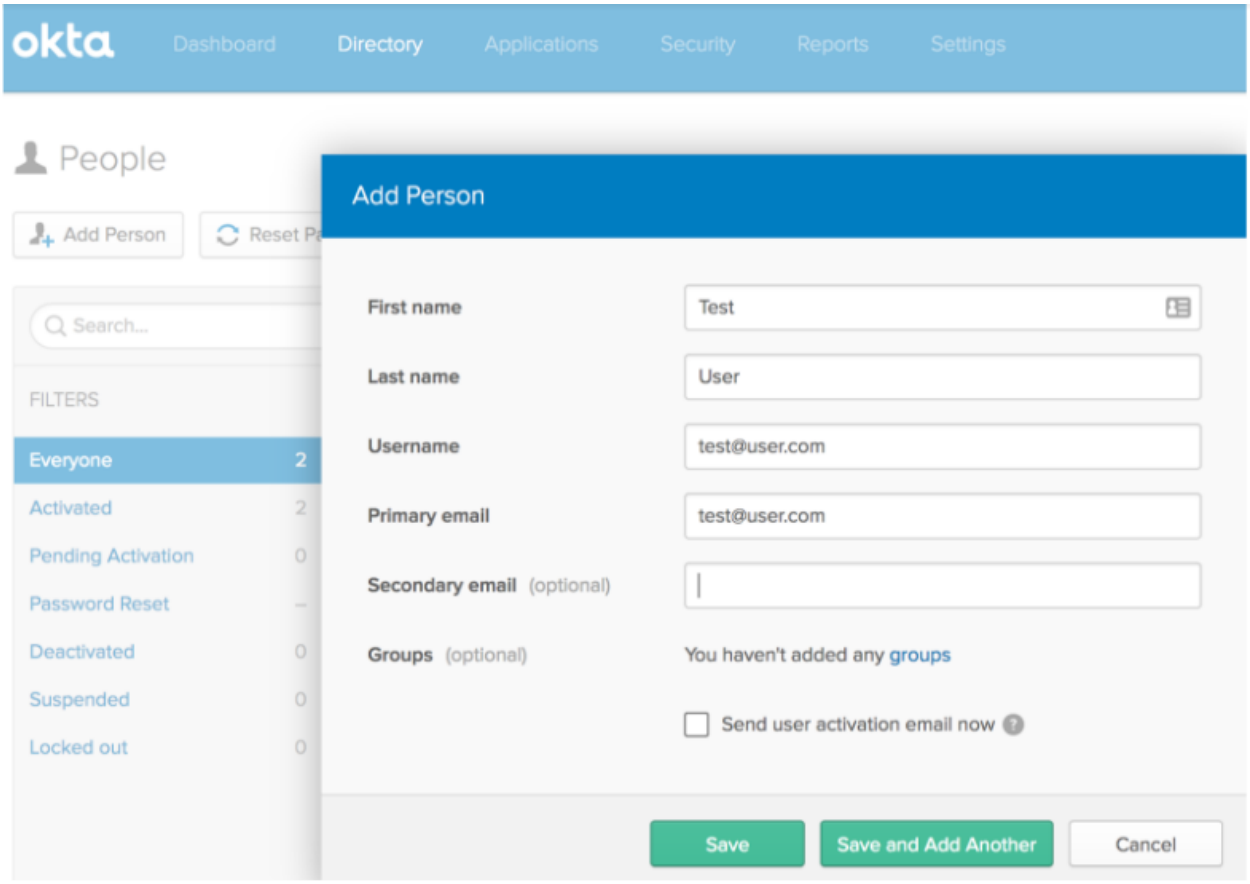


6. Add the default user attribute mapping for Okta in FortiSOAR™ by updating the User Attribute Map as shown in the following image

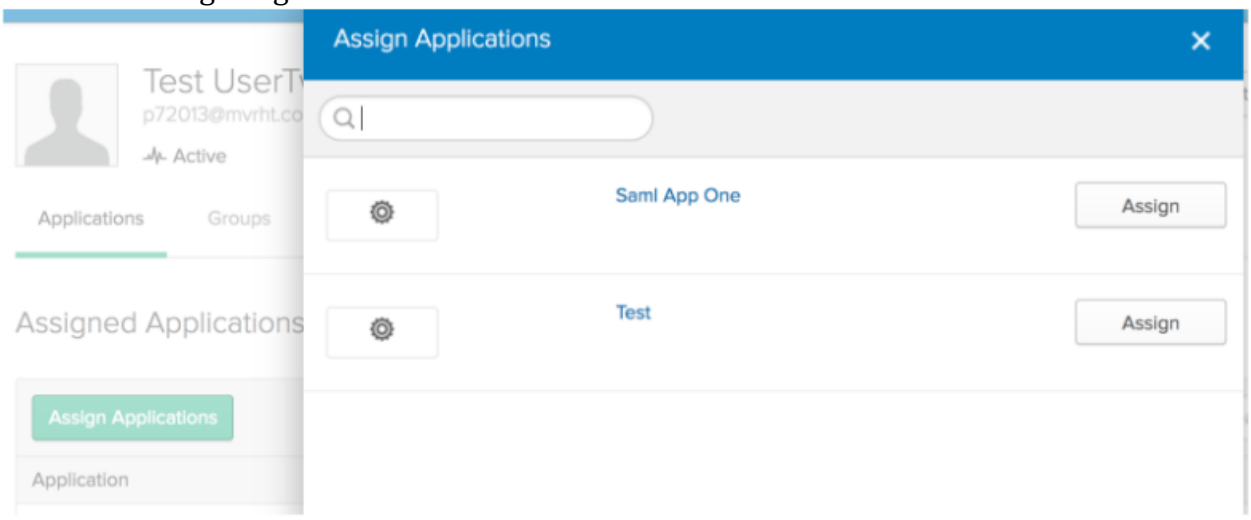


Note: The IdP keys, the keys on the right side, are obtained from the `ATTRIBUTE STATEMENTS (OPTIONAL)` section in Okta, as specified in step 3. You can change the default user attribute mapping later if required.

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.

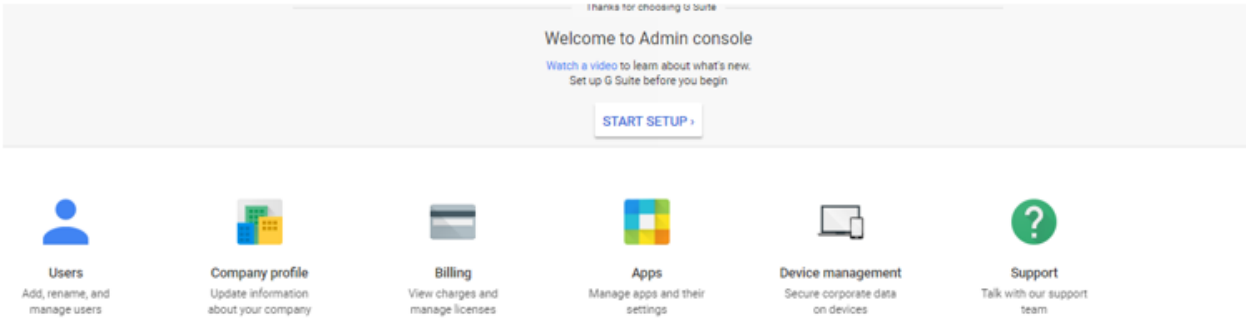


Once the user is created and activated successfully, you can assign this user to the SAML application that you have created. Click on a user to get the user details, and then assign the user to an application using the `Assign Applications` dialog as shown in the following image:

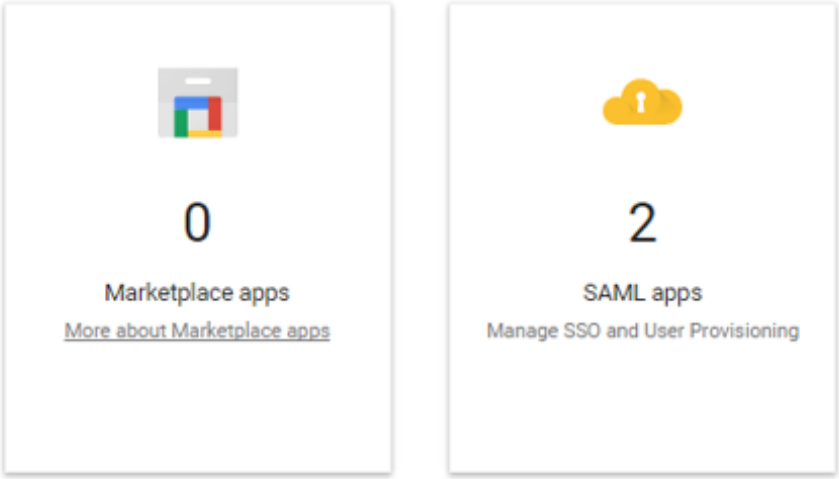


Configuring SAML in Google

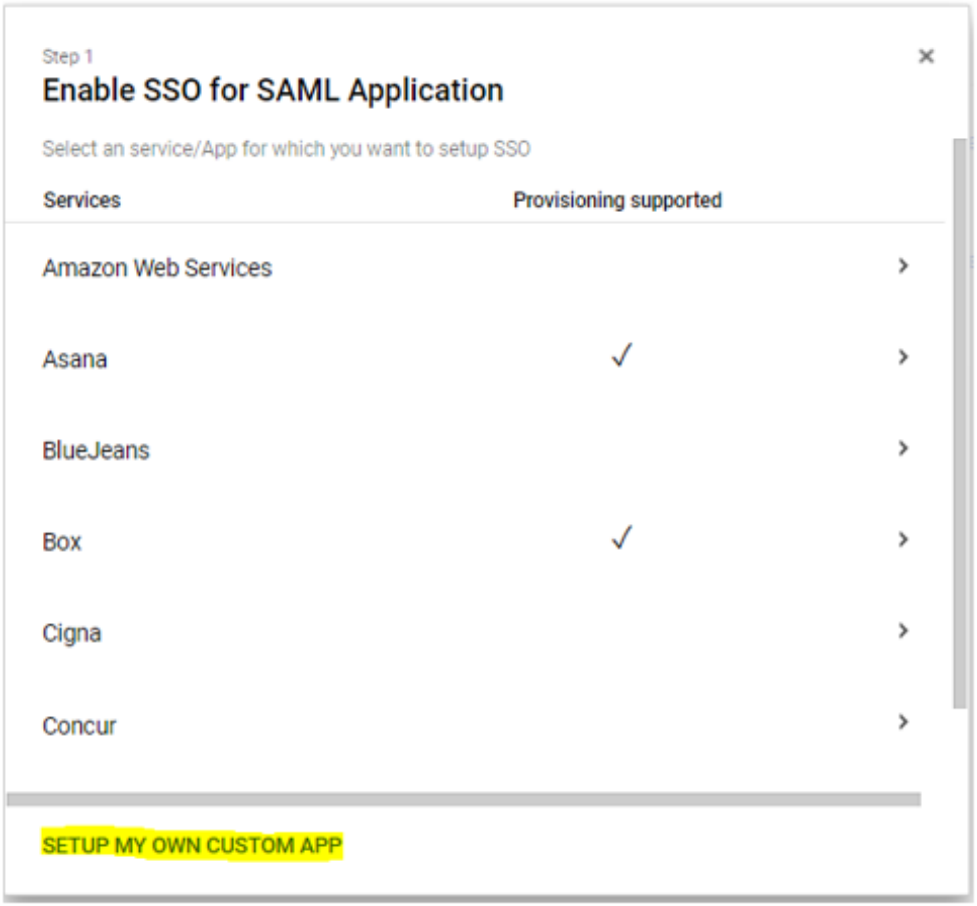
1. Ensure that you have Administrator access for your G Suite account and log on to G Suite using the admin account.
2. Configure IdP.
   - On your `Admin` console, click **Apps**.



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

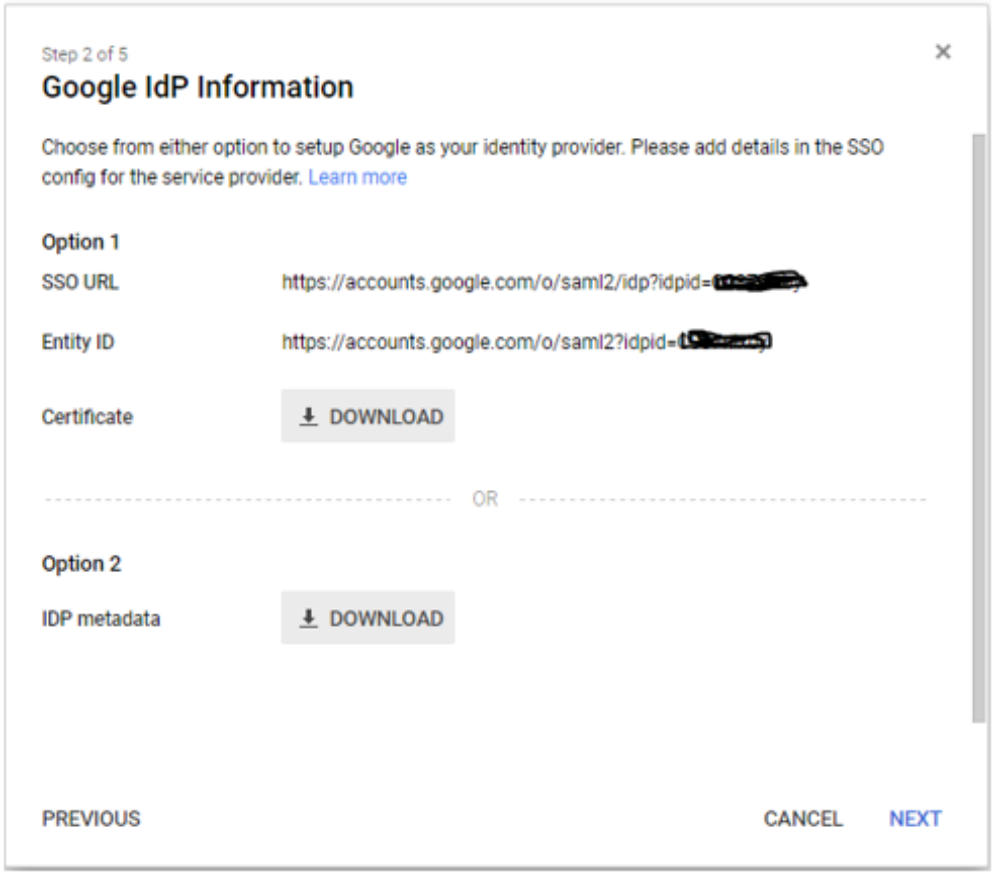


- On the `Enable SSO for SAML Application` page, click **SETUP MY OWN CUSTOM APP**.



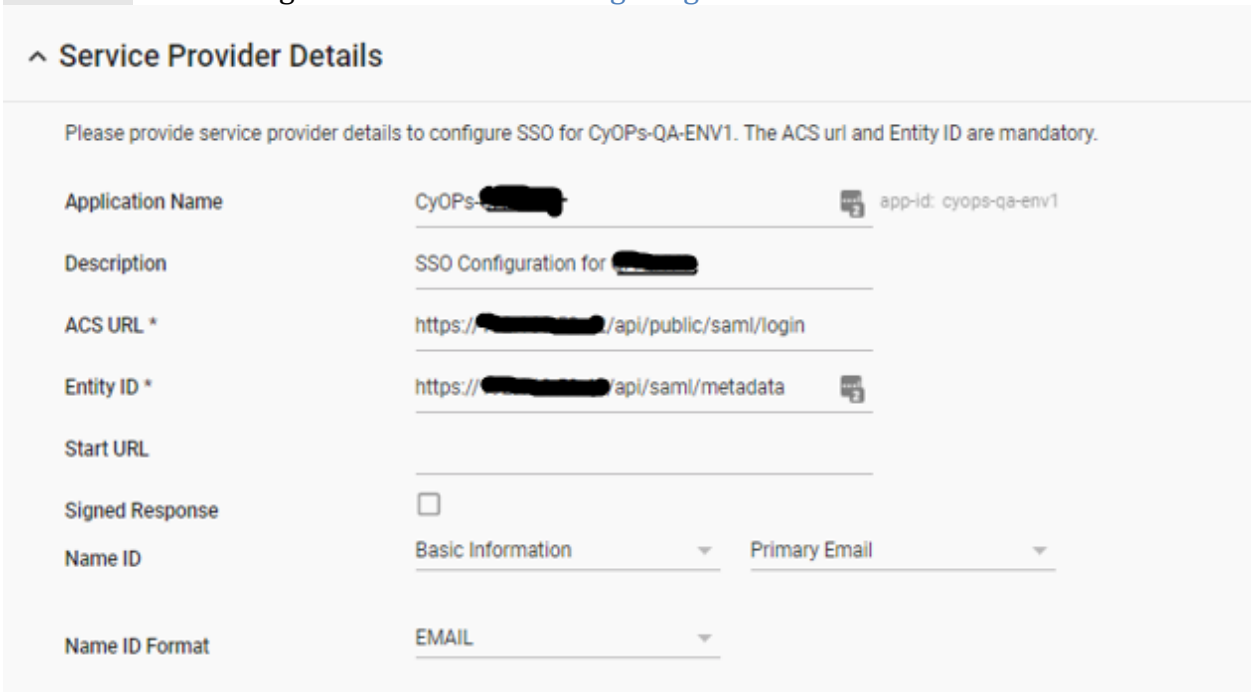
- Click **Next** to display the Google IdP information. Save the Google IdP information and download the `Certificate`.
  You will require the IdP information for Google to configure SSO within

FortiSOAR™.

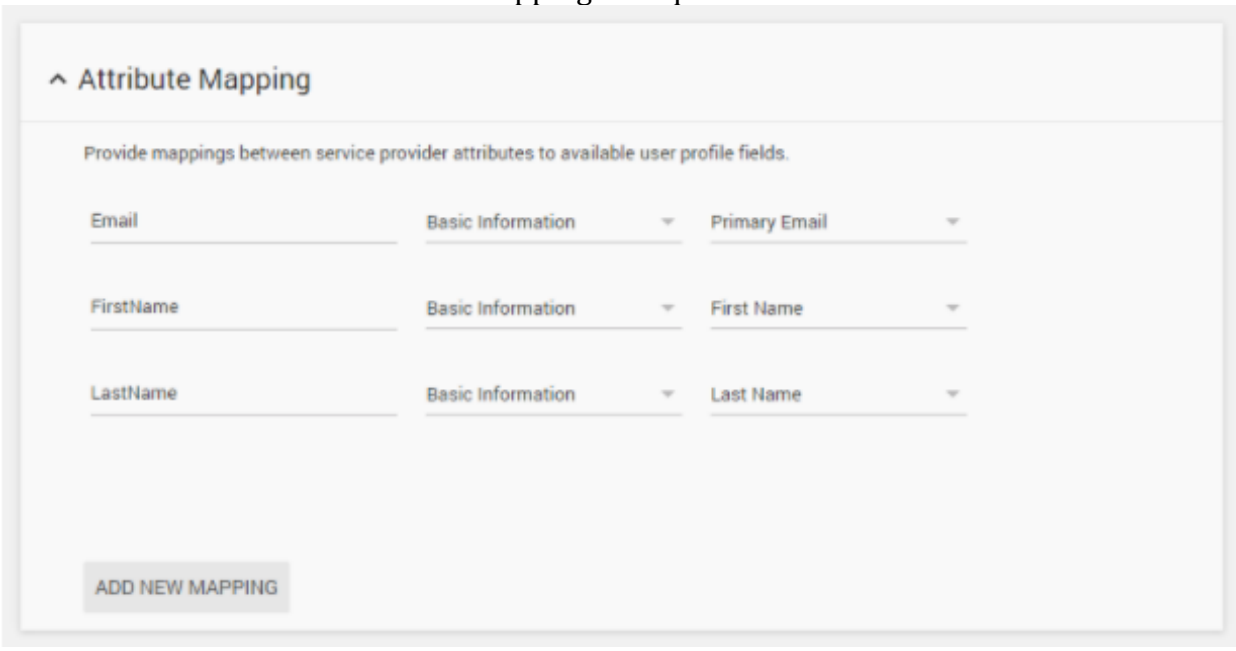


- Click **Next** and add basic information about the App, such as **Name** and Description and then click **Next**.
- On the `Service Provider Details` page, enter the **Entity ID** and **ACS URL** from the `Service Provider` section in FortiSOAR™. Log on to FortiSOAR™ and navigate to **Settings** >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

`Provider` section to get the details. See Configuring SAML in FortiSOAR™.



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

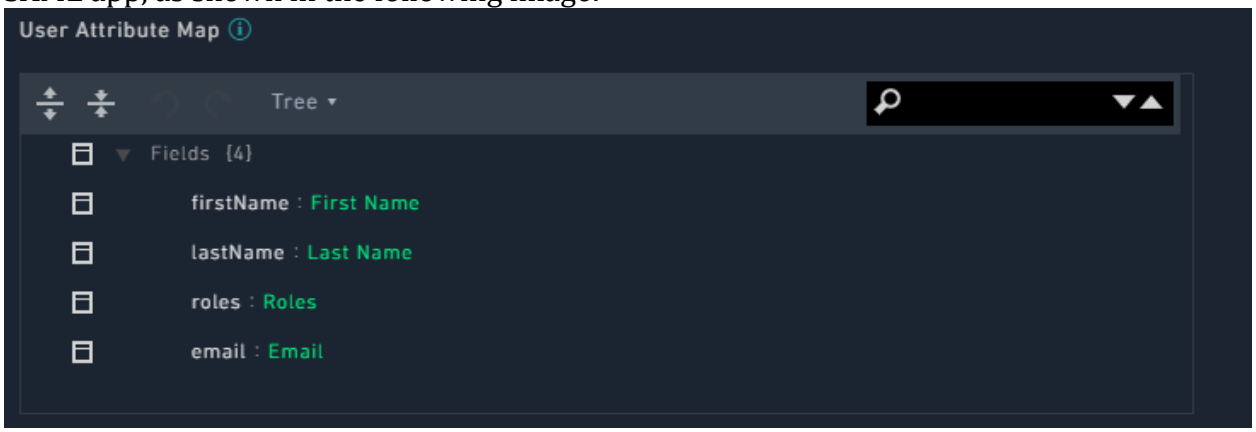


- Save the app configuration and click **Exit**.
- Set up user access for the Google SAML App, see Set up your own custom SAML application.

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:

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:



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

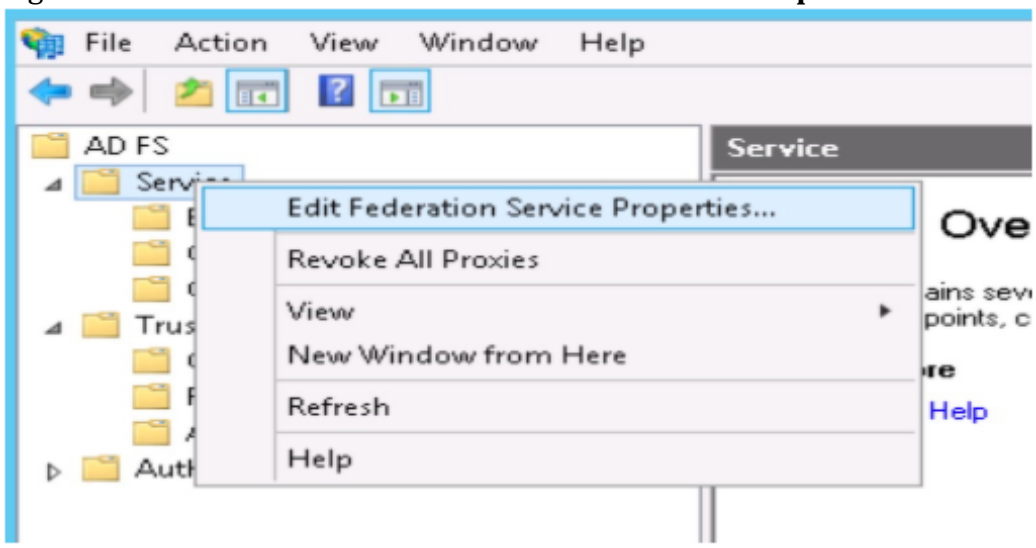
Configuring SAML in ADFS

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

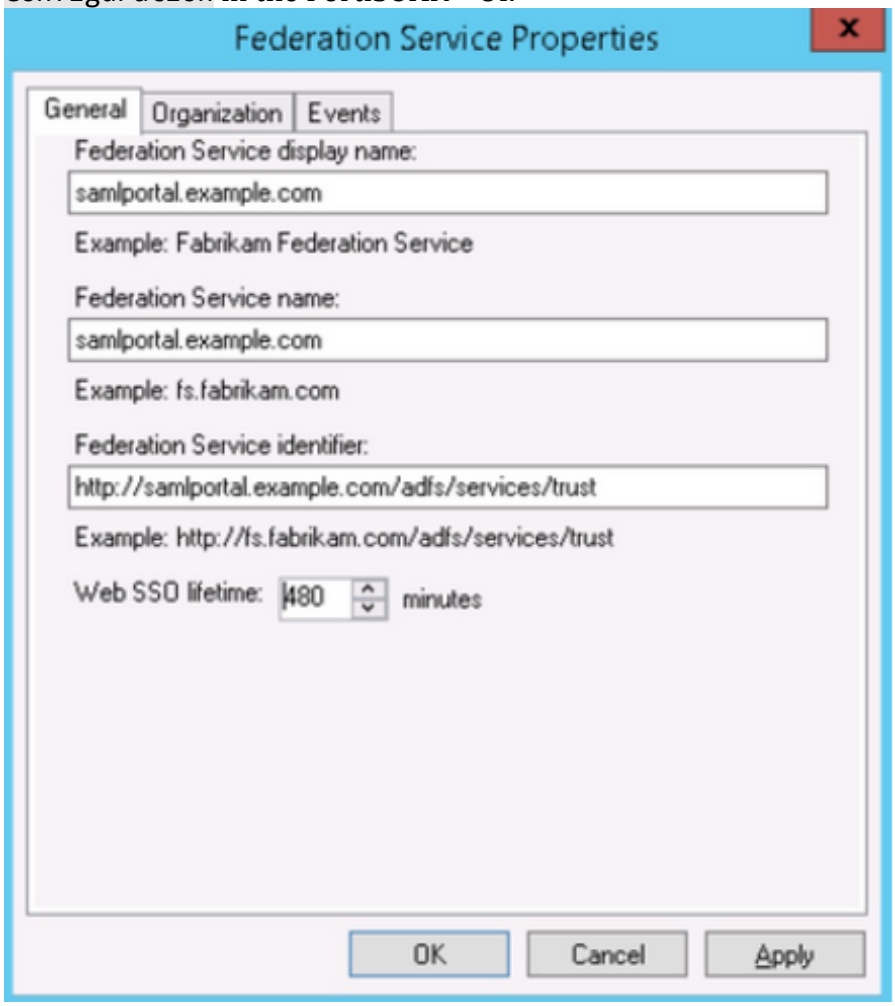
This procedure uses `ADFS 3.0` and uses `samlportal.example.com` as the ADFS website. The values you use in your setup will be based on your ADFS website address. See ADFS integration with SAML 2.0 for more information.

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`

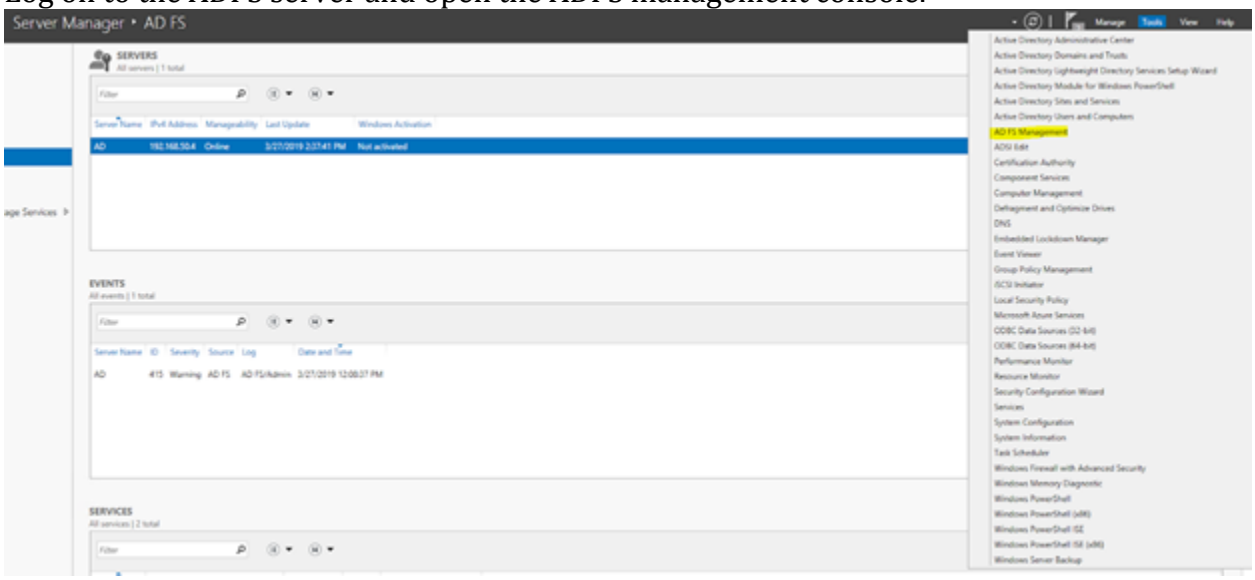
Configuration in the FortiSOAR™ UI.



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. Ensure that the **No, do not export the private key** option is selected, and then click **Next**.
    e. Select **Base-64 encoded binary X.509 (.cer)**, and then click **Next**.
    f. Select where you want to save the Token-Signing certificate and provide a name to the certificate, and then click **Next**.
    g. Click **Finish**.
    h. 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.

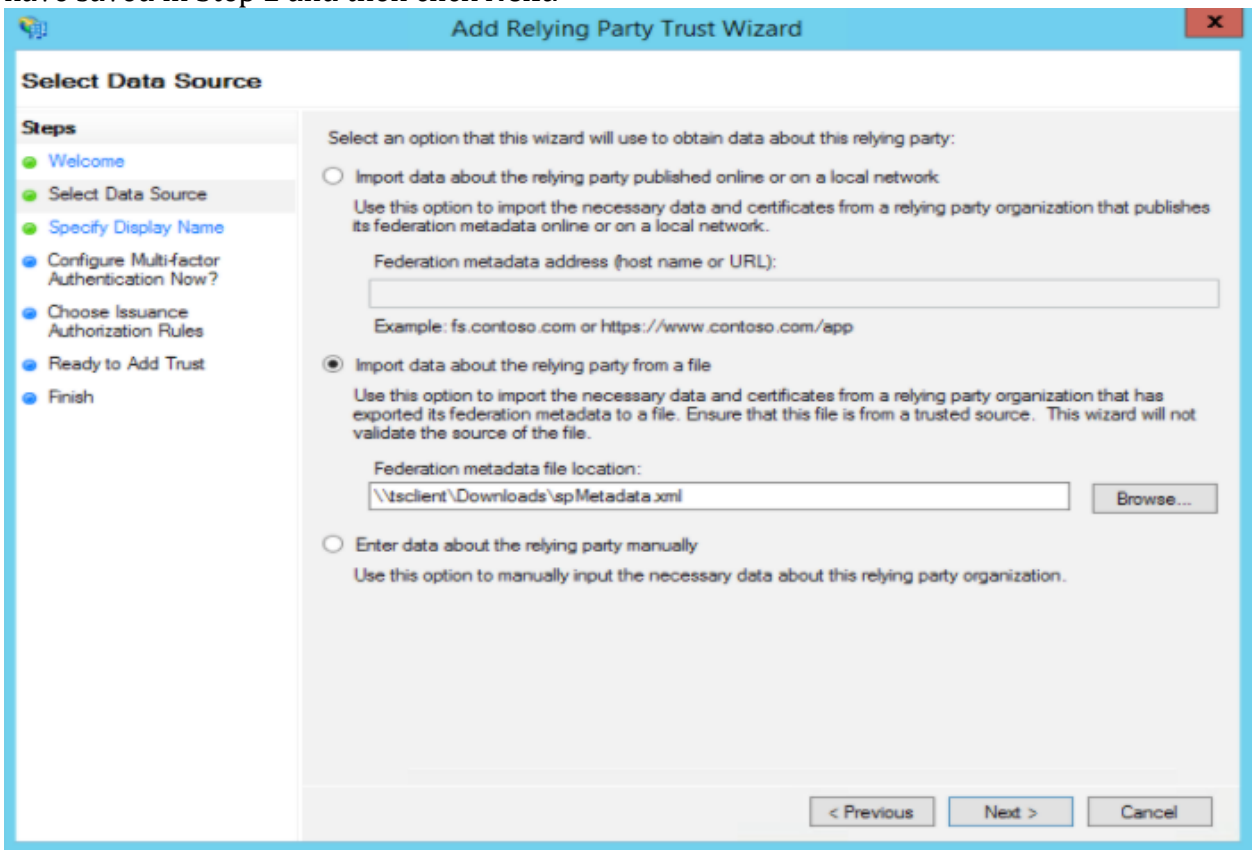
Configuring ADFS Relying Party Trust

1. Log on to FortiSOAR™ as an administrator.
2. Click **Settings** > **Authentication** > **SSO Configuration** and download the SAML metadata file by clicking **Download** in the `Service Provider Configuration` section.
3. Log on to the ADFS server and open the ADFS management console.



4. Expand **Trust Relationships** and right-click **Relying Party Trust** and select **Add**.
5. On the `Add Relying Party Trust Wizard` click **Start**.
6. 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`.

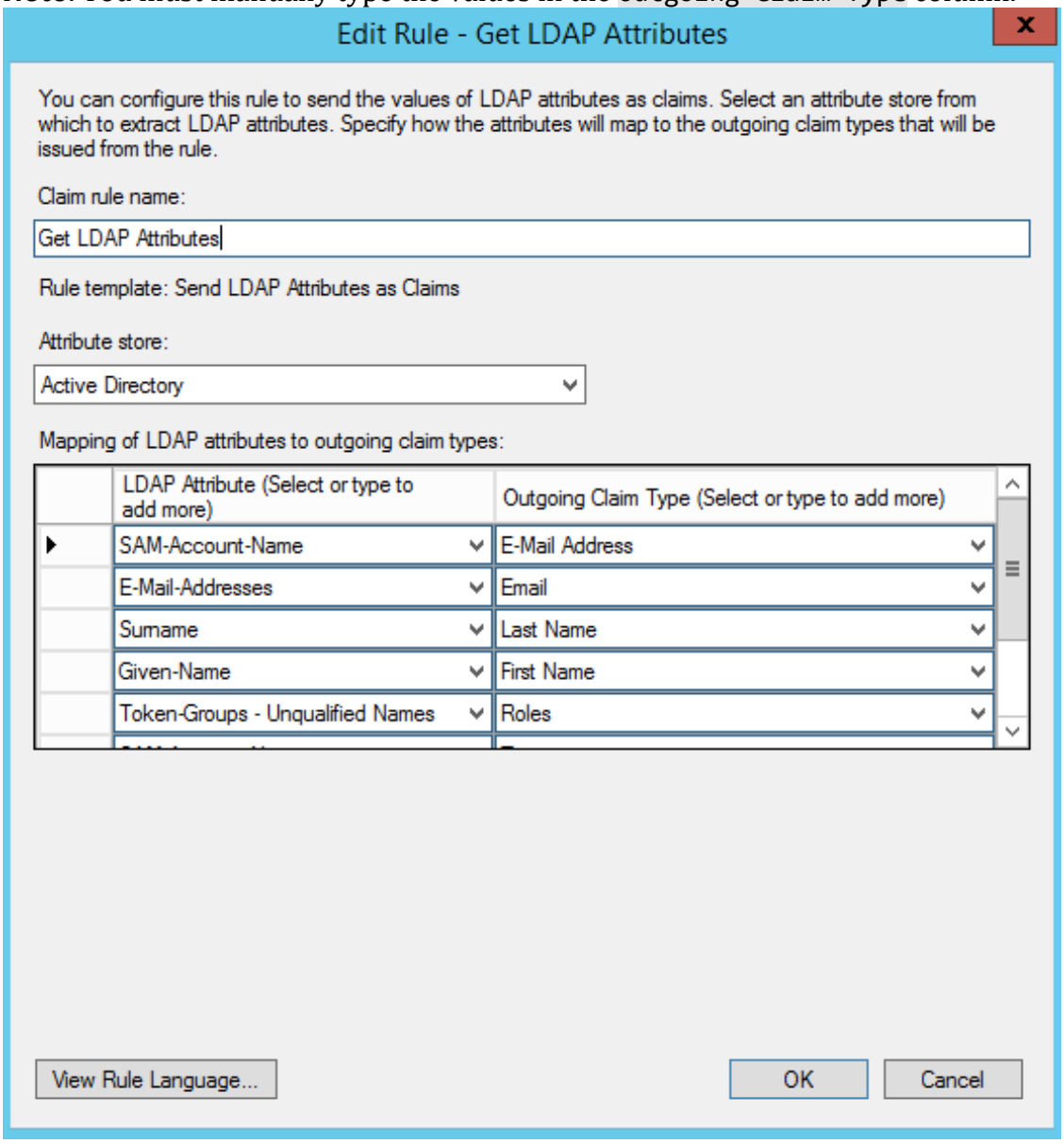
Configuring ADFS Relying Party Claim Rules

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`.

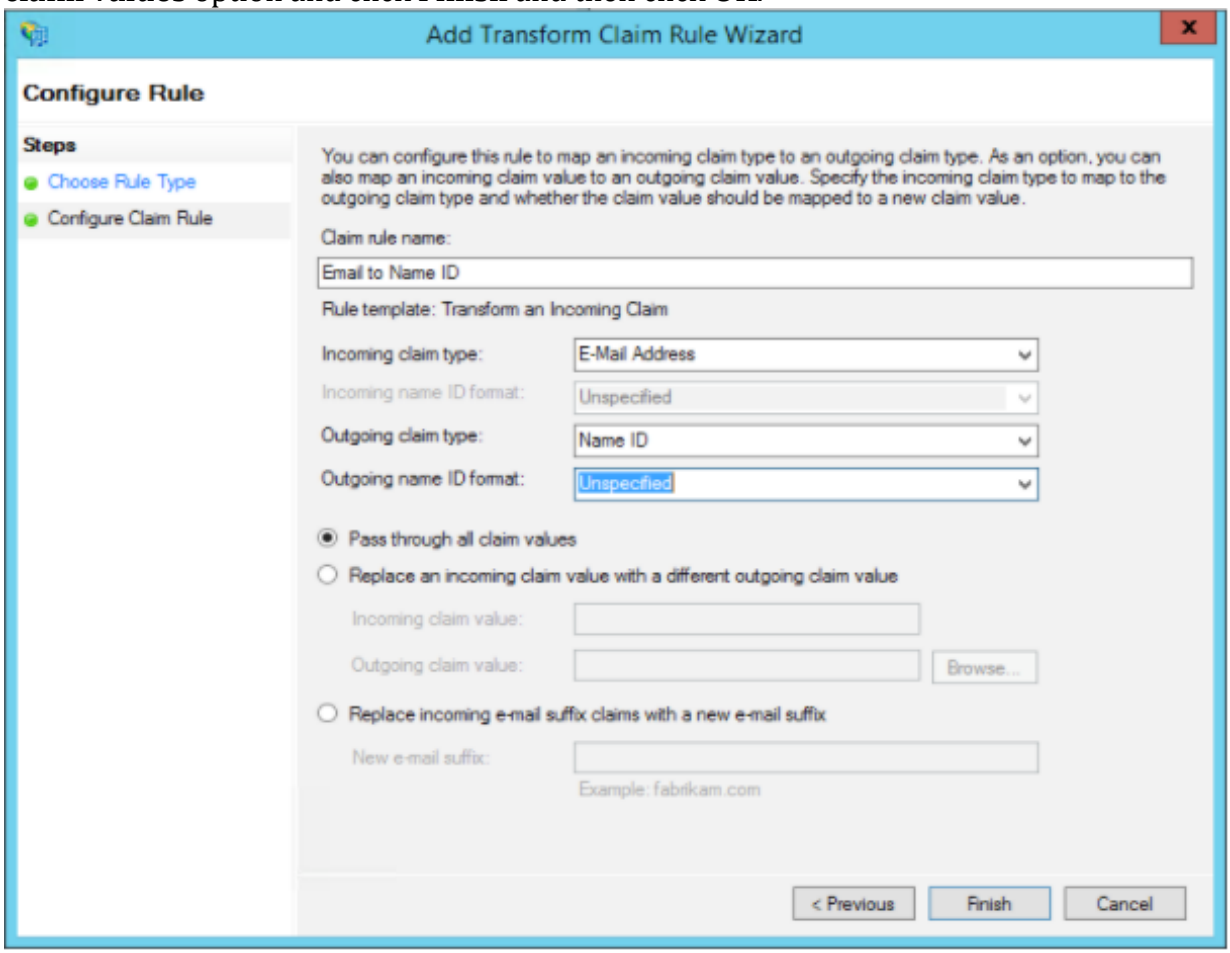
6. From the Attribute store drop-down list, select Active Directory.
7. In the Mapping of LDAP attributes to outgoing claim types section, map the following values:
    a. Select **SAM-Account-Name** from the `LDAP Attribute` column and map that to **E-Mail Address** in the `Outgoing Claim Type` column.
    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.



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**.

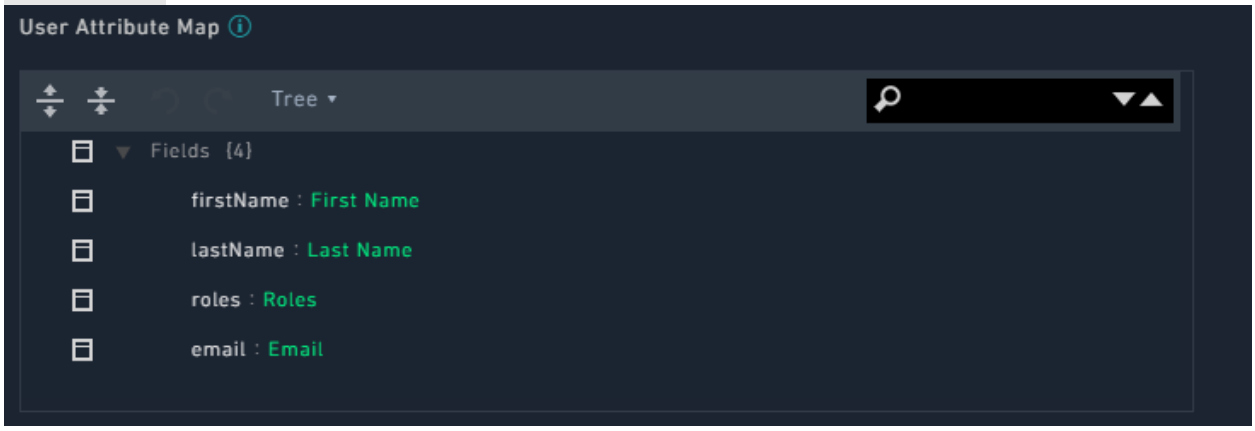


Configuring FortiSOAR™ for ADFS

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:

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`.



   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™

Version 5.0.0 and later provides you with the ability to 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).

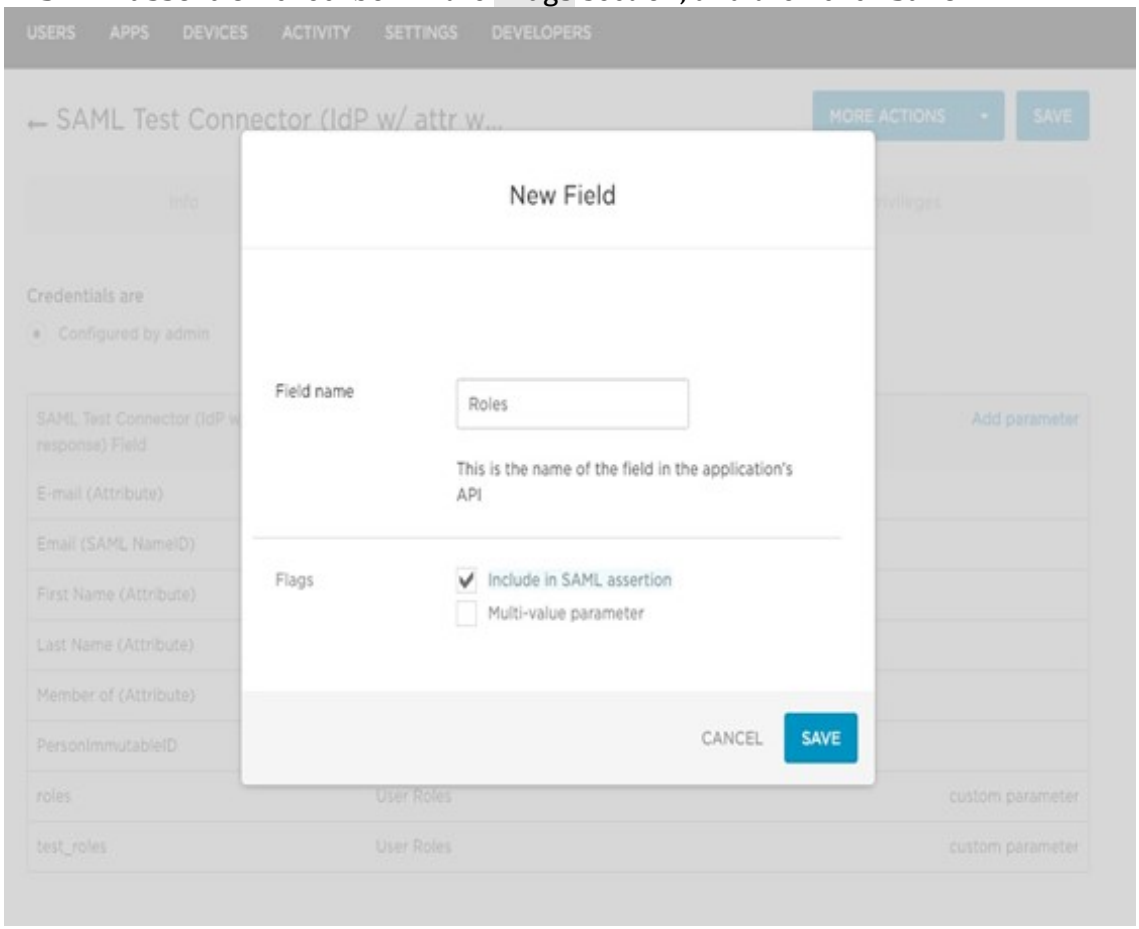
For mapping of roles in ADFS, see the Configuring ADFS Relying Party Claim Rules section.

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

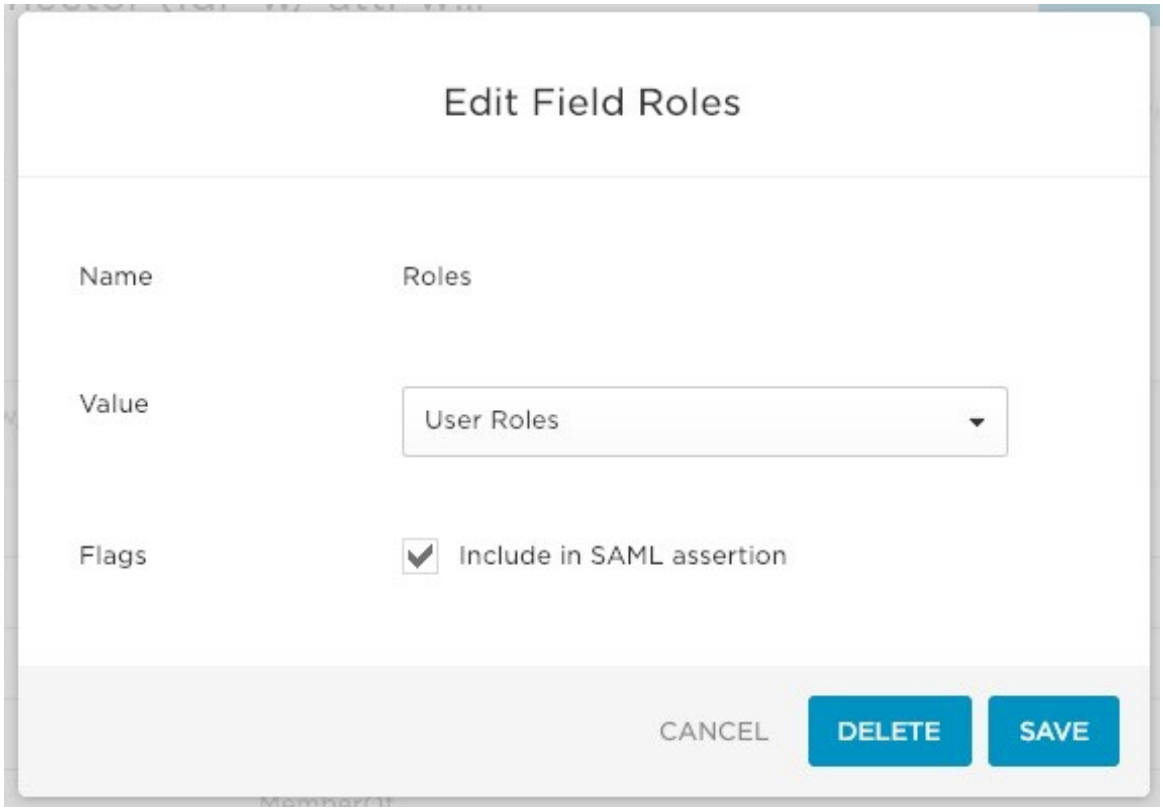
OneLogin

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**.

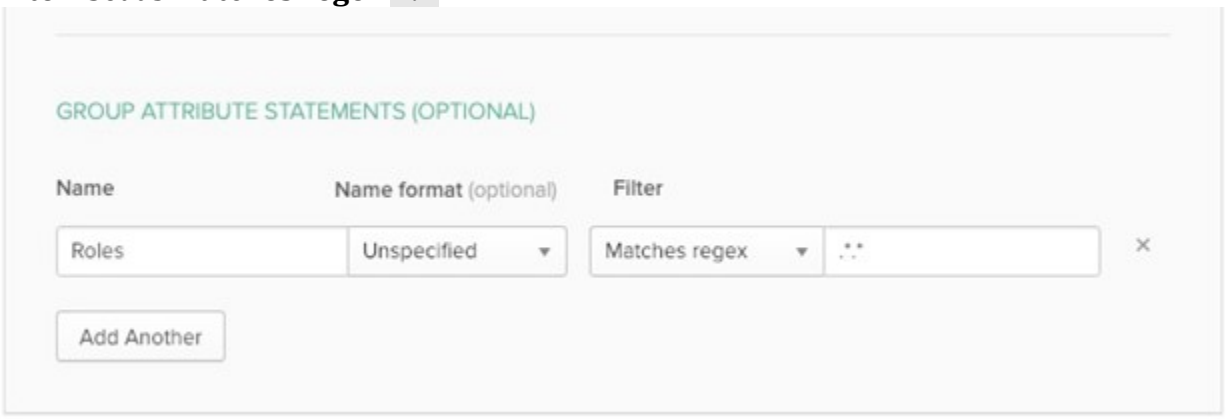


4. In the next dialog, i.e., the `Edit Field Roles` dialog, from the **Value** drop-down list, select **User Roles** and click **Save**.



Okta

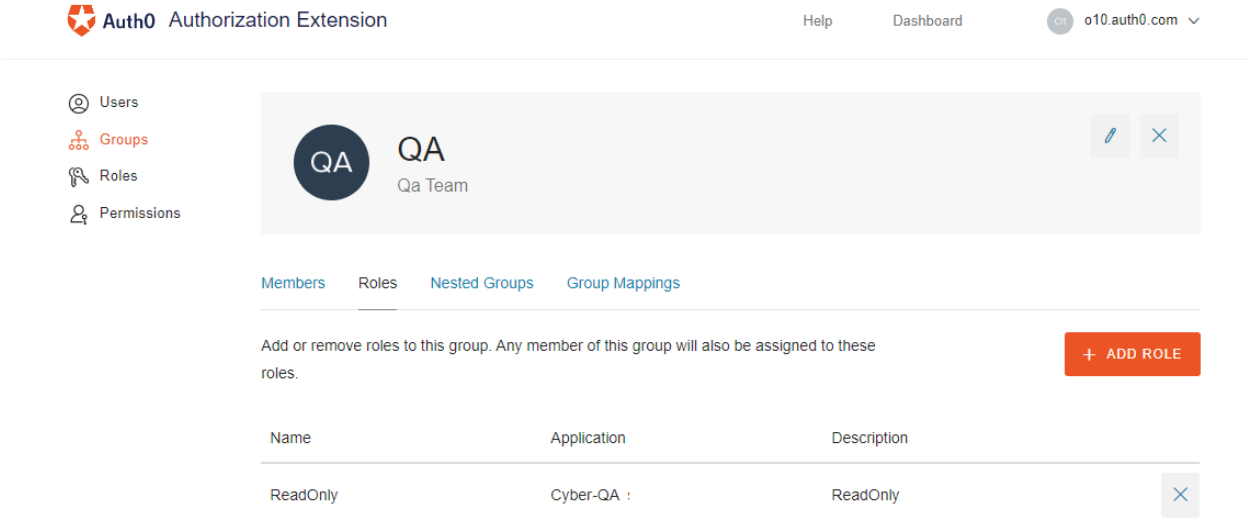
1. Log on to Okta as an administrator.
2. Navigate to the SAML app that you have created and edit the SAML settings.
3. In the GROUP ATTRIBUTE STATEMENTS (OPTIONAL) section set the following:
   Name: Set as **Roles**.
   Filter: Set as **Matches regex** `*.*`



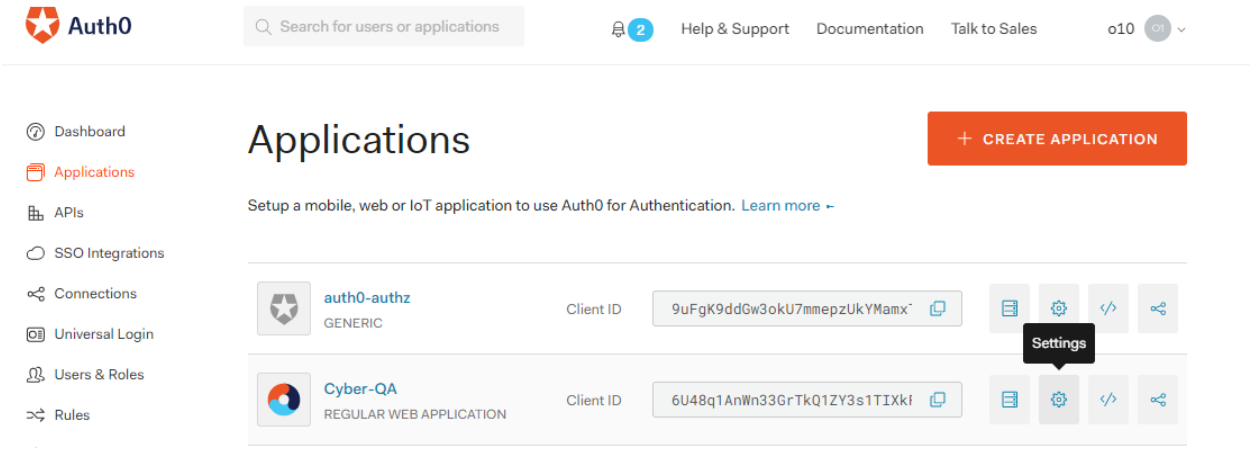
4. Click **Next** and complete the setup.

Auth0

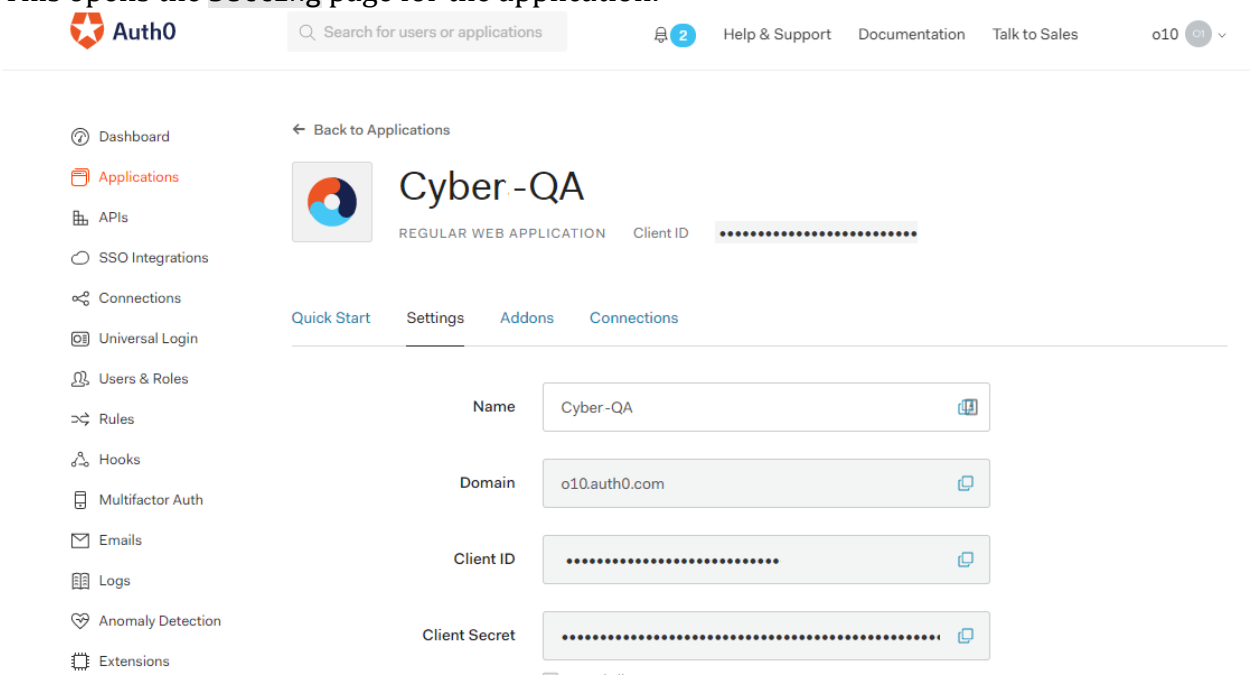
1. Log on to Auth0 as an administrator and in the left menu click **Authorization**.
2. On the `Authorization Extension` page, create a new group and associate required members (users) and roles with this group.



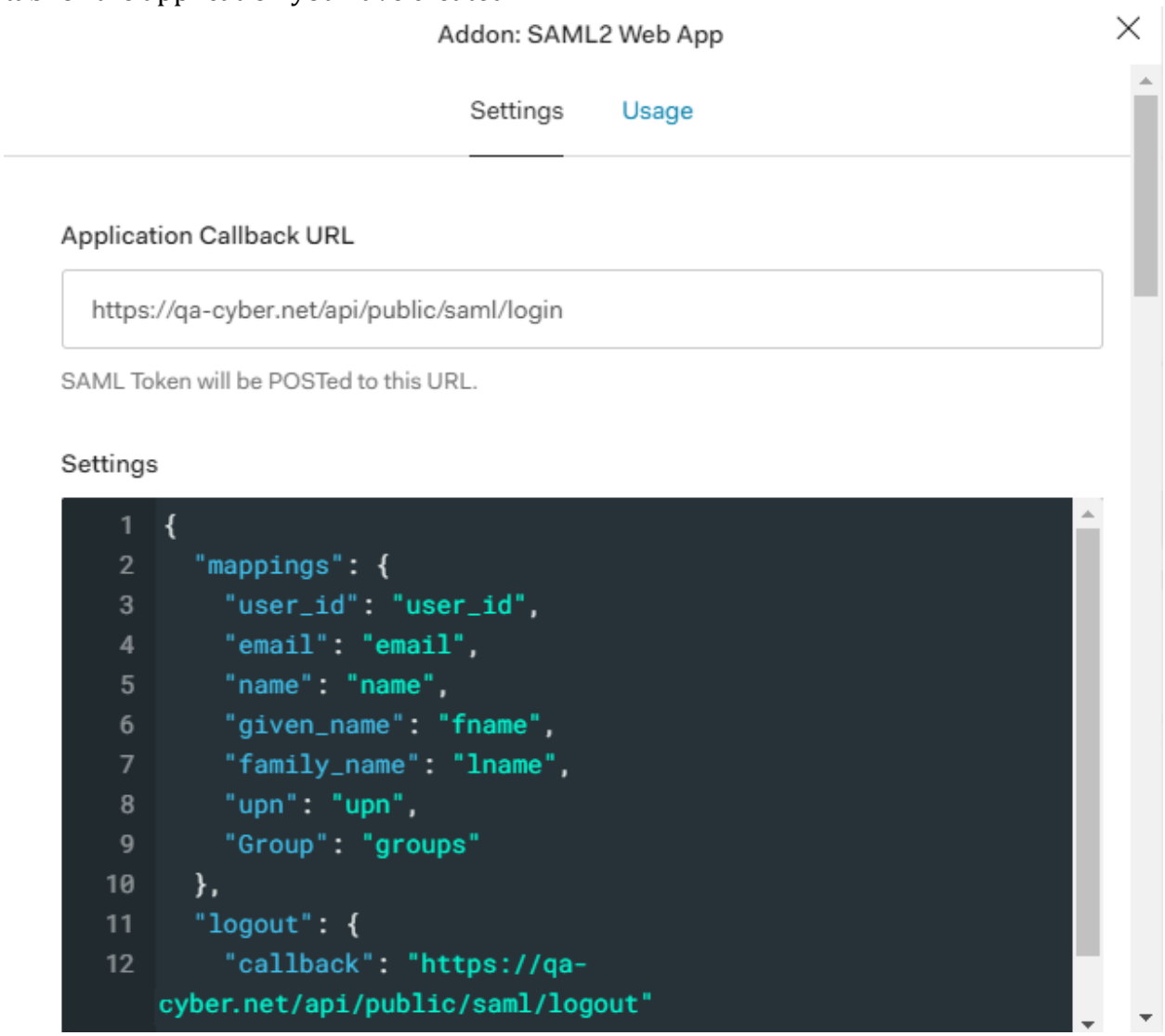
3. Navigate back to the main menu (`Dashboards` page) and click **Applications**.
4. Create a new application, or click on the **Settings** icon of the application whose settings you want to edit:



This opens the `Setting` page for the application:



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



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

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.

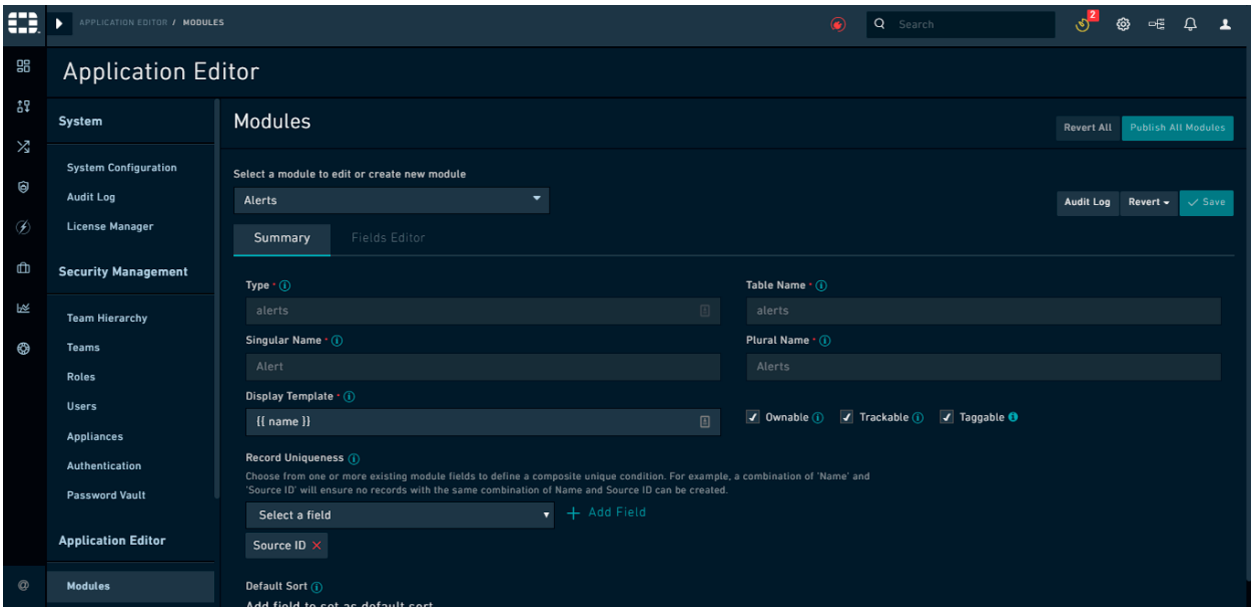


Figure 55. *Module Editor Interface*

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:

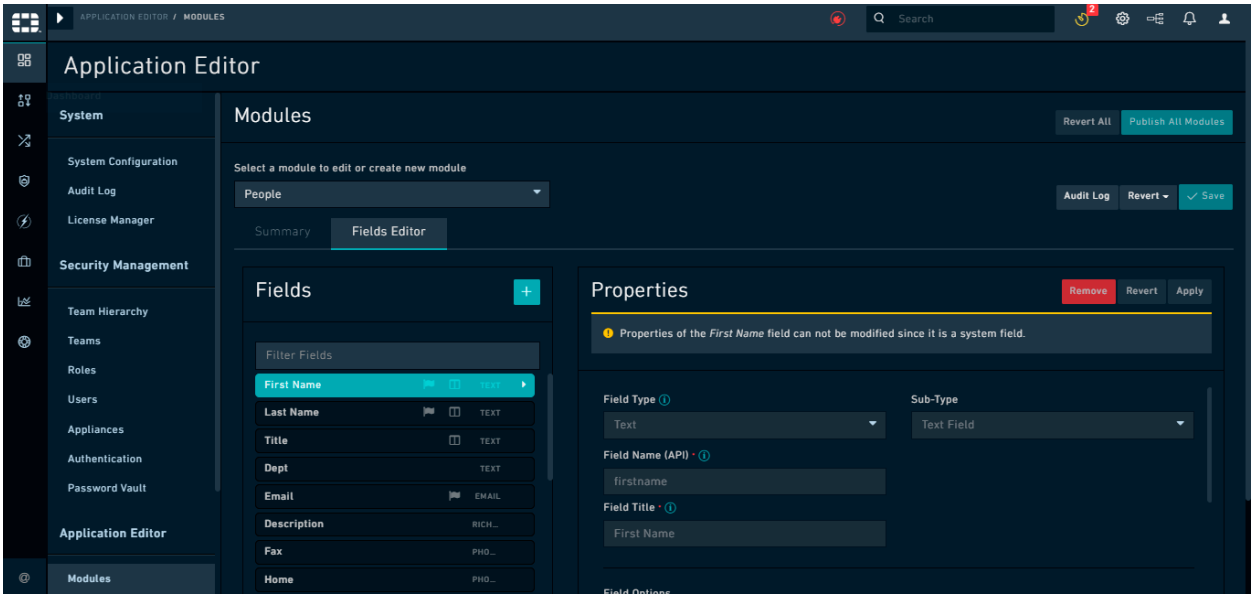
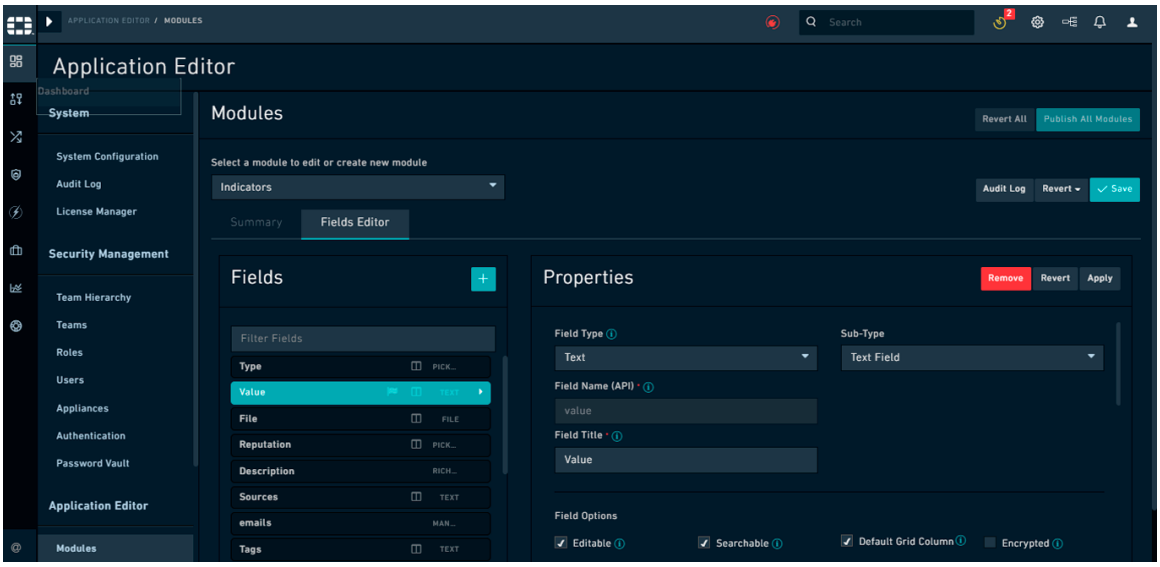


Figure 56. *Field Editor tab- Read-only fields*

Modifying an existing module

To modify an existing module, do the following:

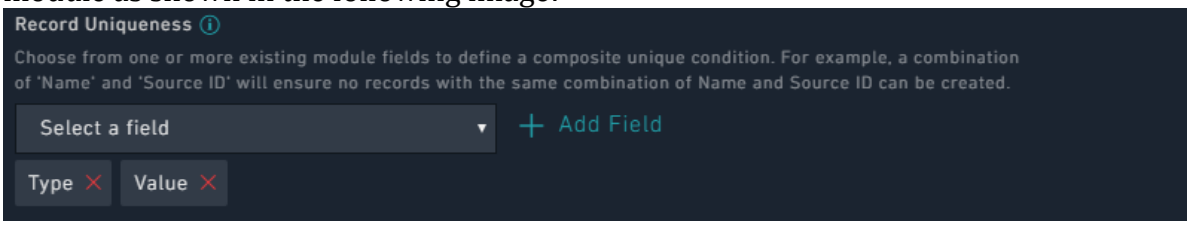
1. Click **Settings** and click **Modules** in the `Application Editor` section, to open the Module Editor.
   This displays the `Modules` page.
2. To edit an existing module, from the **Select a module to edit or create new module** drop-down list, select the module.
   For example, select `Alerts`.
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`.



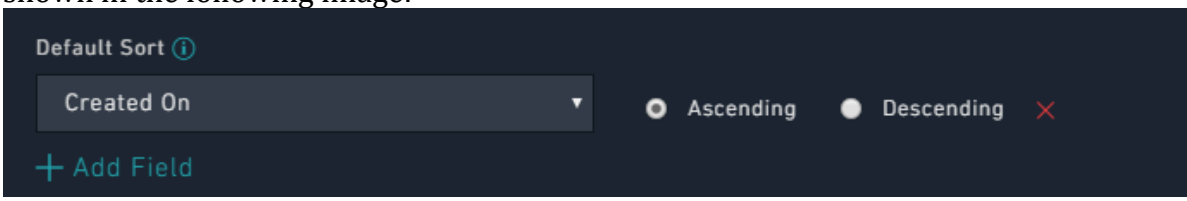
You can also add an attribute of a picklist as part of the Display Template. See the following *Display Template* section for more details.

- **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**: (Introduced in FortiSOAR™ 6.0.0 for MSSP 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:

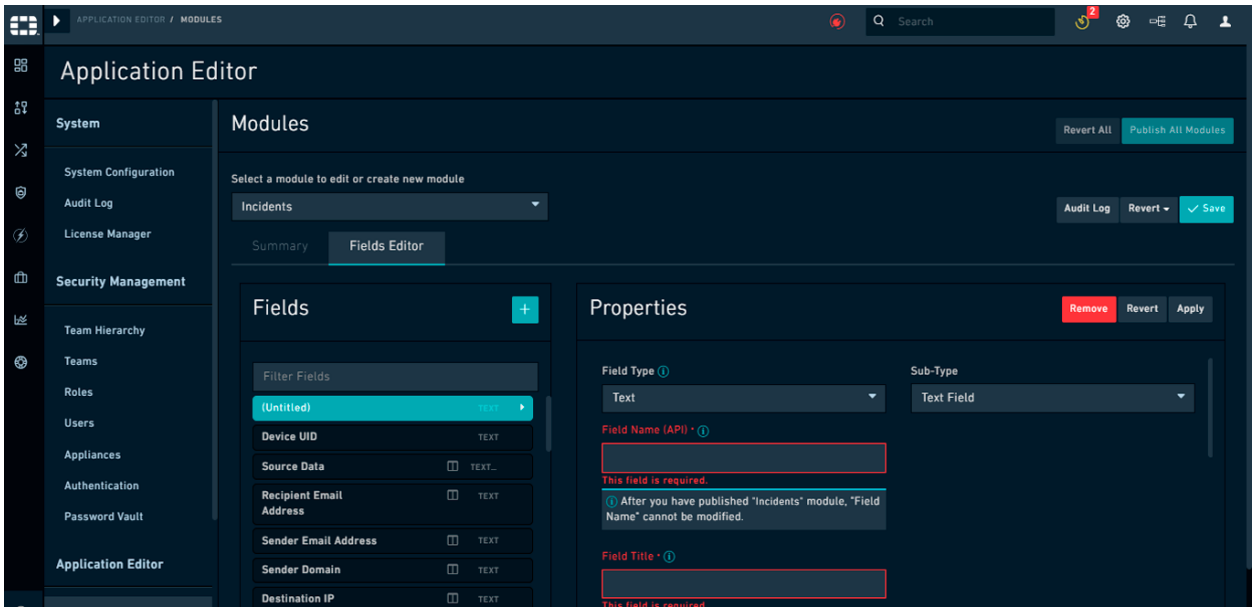


  This will ensure that indicator records will be created with unique "Type and Values" values.
  If you want to add any other field to for part of the unique combination of fields, then from the `Record Uniqueness` section, select that field from the **Select a Field** drop-down list, and then click **Add 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:



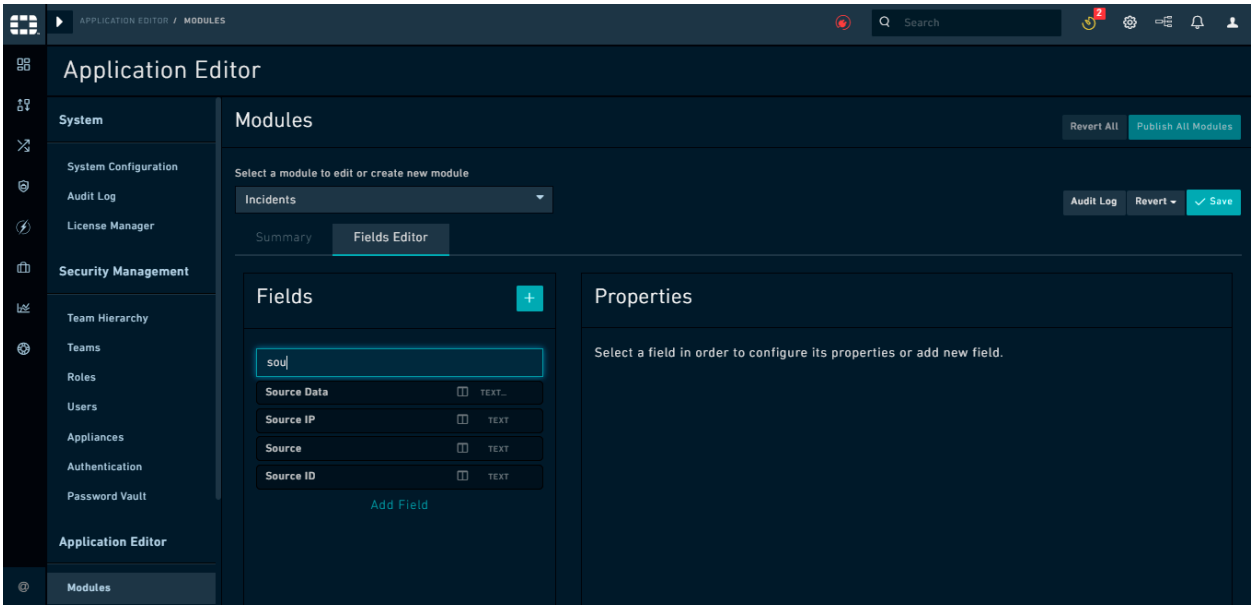
b. Click **Save** to save the changes to the module or click **Revert** to clear any changes made in the interface since the last `Save` event. For information on the save and revert operations, see the *Saving your changes* section.

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.



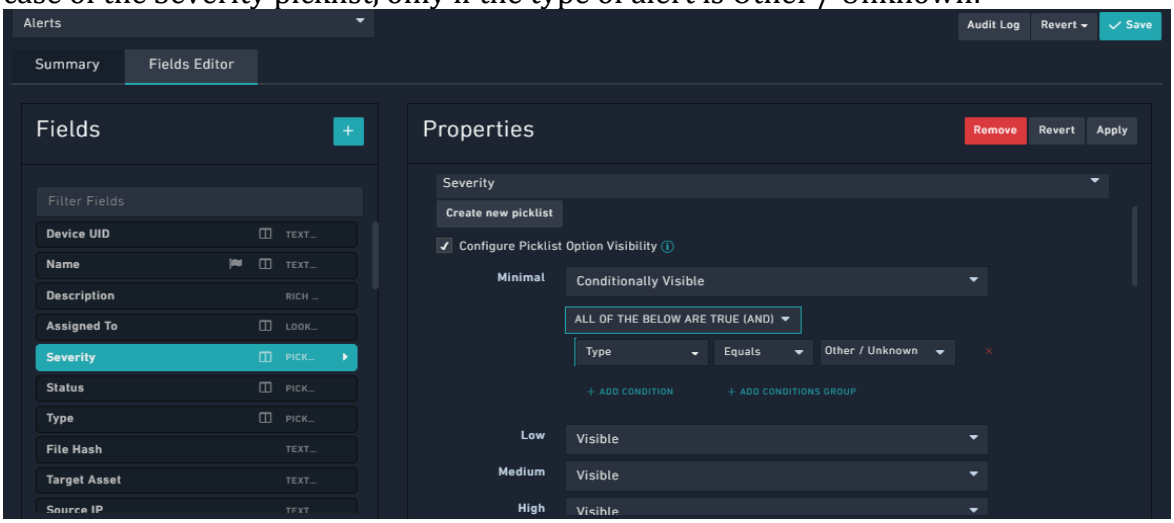
Important: Some fields in some modules are system fields and changing properties of these fields could lead to issues with the working of FortiSOAR™. Therefore, you cannot modify any properties of these fields and they appear as read-only when you select them in the **Fields Editor** tab. An example 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:

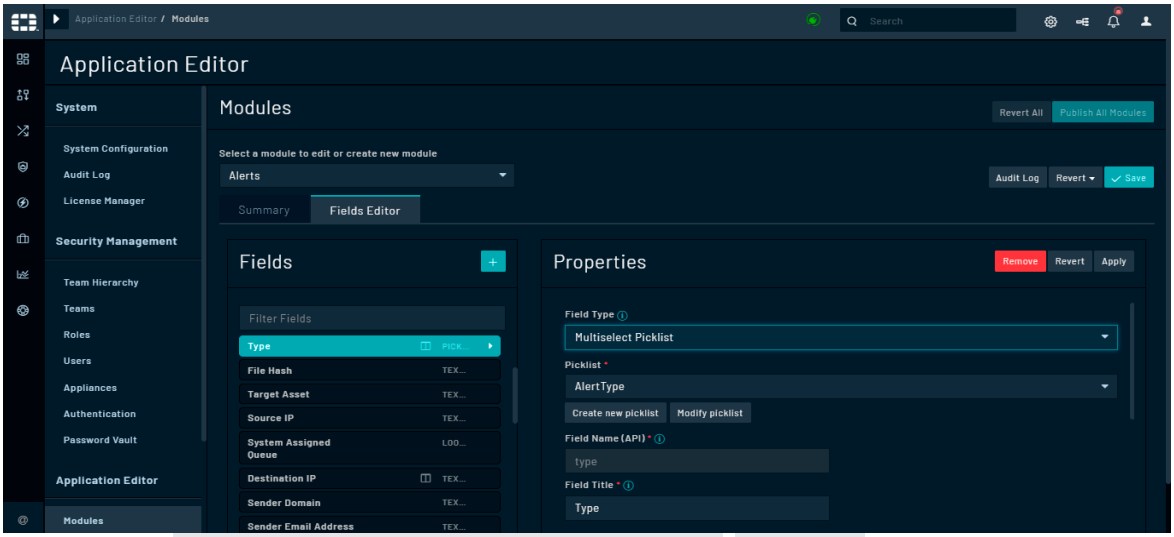


b. Define the following properties for the newly added field:
   - **Field Type**: The type of field; it specifies the type of form used to render this attribute. Examples of field types are text, checkbox, integer,

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".
FortiSOAR™ 6.0.0 introduces the JSON field type, which can be used for fields such as `Source Data` that commonly store data in the JSON format. Using JSON as a field type for such fields allows 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. FortiSOAR™ 6.0.0 introduces a **Configure Picklist Option Visibility** checkbox using which can 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:



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.

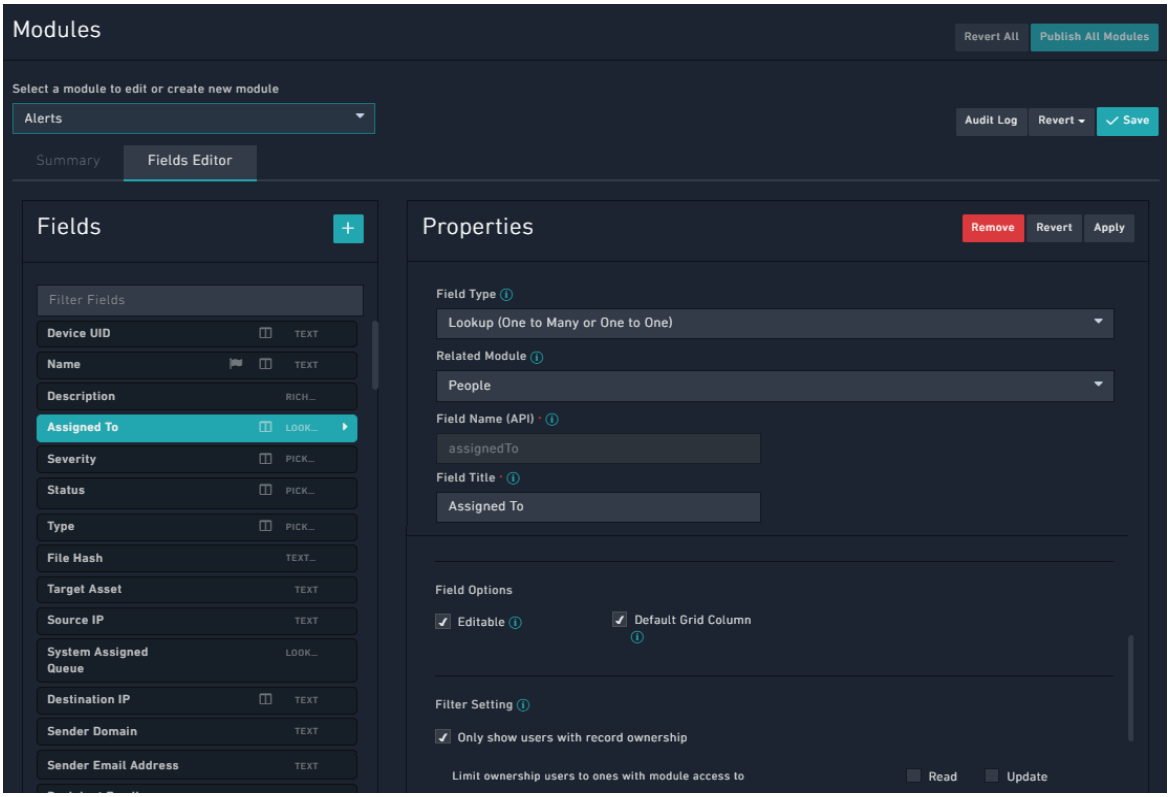


If you select `Lookup (One to Many or One to One)`, `Multiple Relationship (Many to One)`, or `Multiple Relationship (Many to Many)`, a **Related Model** drop-down list will appear, and you must select the related module. The related module is the module for the source of the data, which is not explicitly defined, to which the fields points.

Notes with respect to Relationship fields:

– In the case of a `Multiple Relationship (Many to One)`, or a `Multiple Relationship (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.



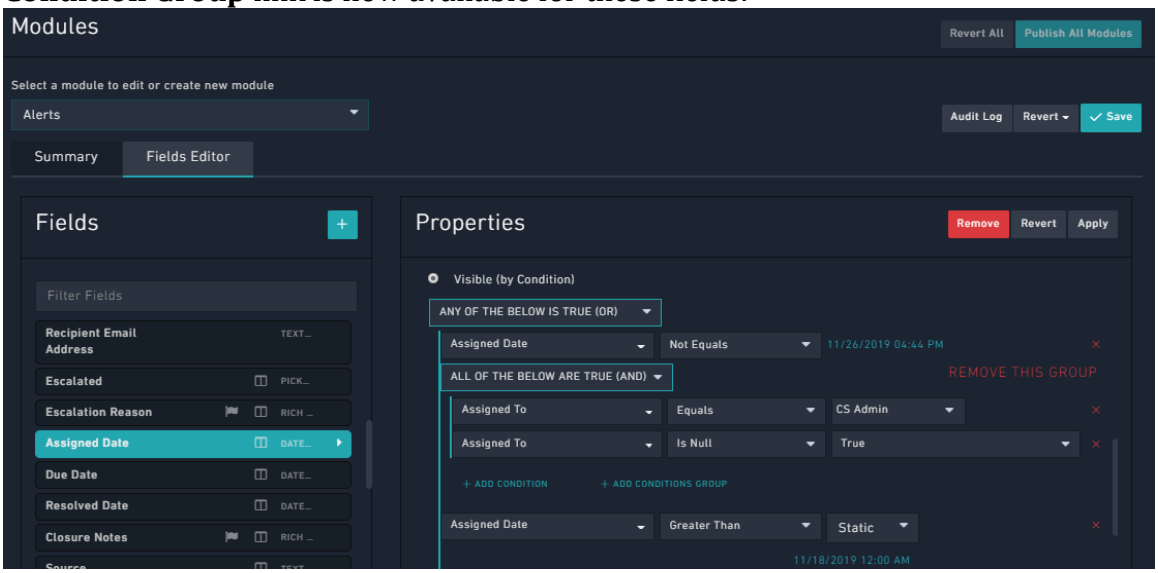
Example: In the Alerts module, we have an **Assigned To** field, which is of type `Lookup (One to Many or One to One)`, with **People** as the related module. In this case by default, all users will be displayed in the Assigned To lookup, when you open an alert record. However, this could include users 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).

- **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, 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 field, you can can use formatting options or you can use the IP address and domain field types to lookup threat intelligence tools and whois info.
- **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

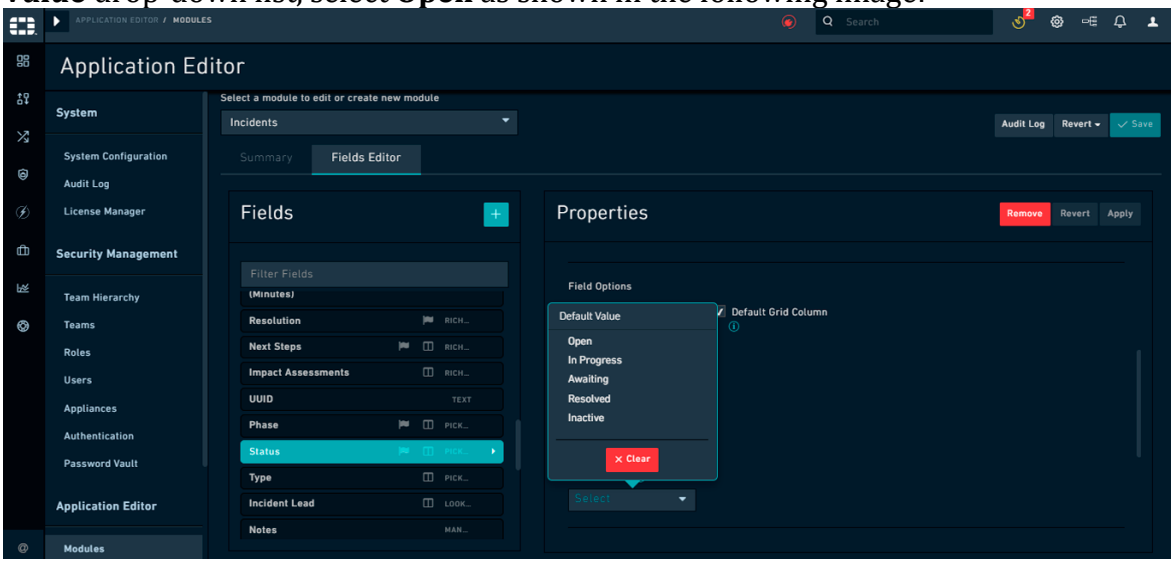
alphabet. It cannot contain any spaces, underscores or any special characters.
Note: You cannot change the name that you specify for the field once the field has been created and the module has been published. This is because there is no migration path from the old name to the new name, so you risk data 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.
- **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™ 6.0.0 adds support for 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™ 6.0.0 adds support for advanced date operations nested conditions for the **Visible (by condition)** fields i.e., the **Add Condition Group** link is now available for these fields:

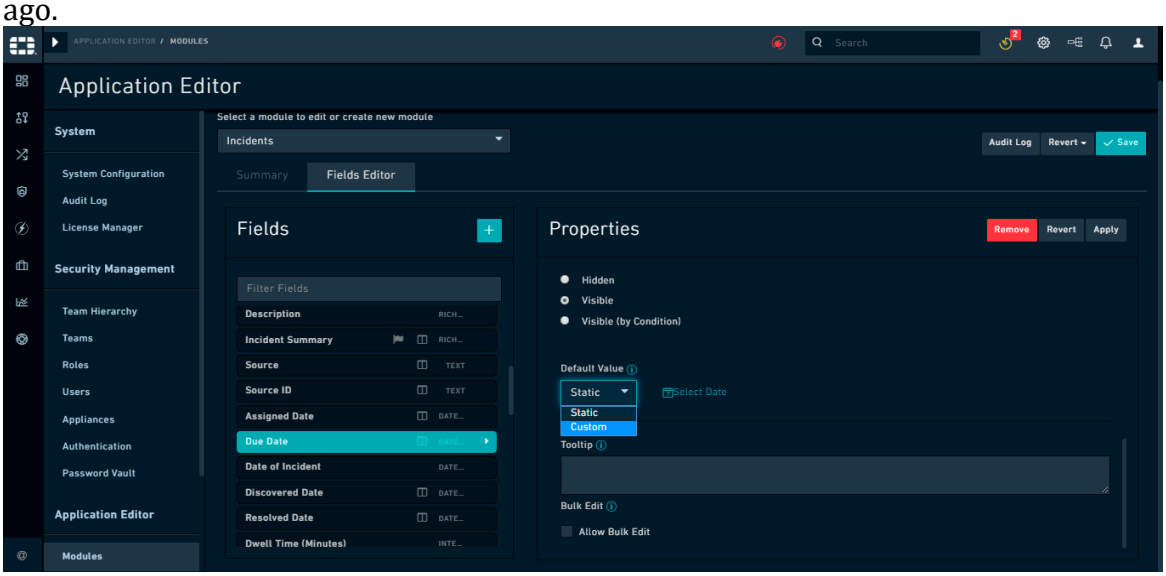


- **Default Value**: Specifies the default value of this field. Once you specify a value in this field, then this value will be displayed, by default when you add a record in the selected module.
For example, if you want the status of a newly created alert to be set to **Open**, by default, then select 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

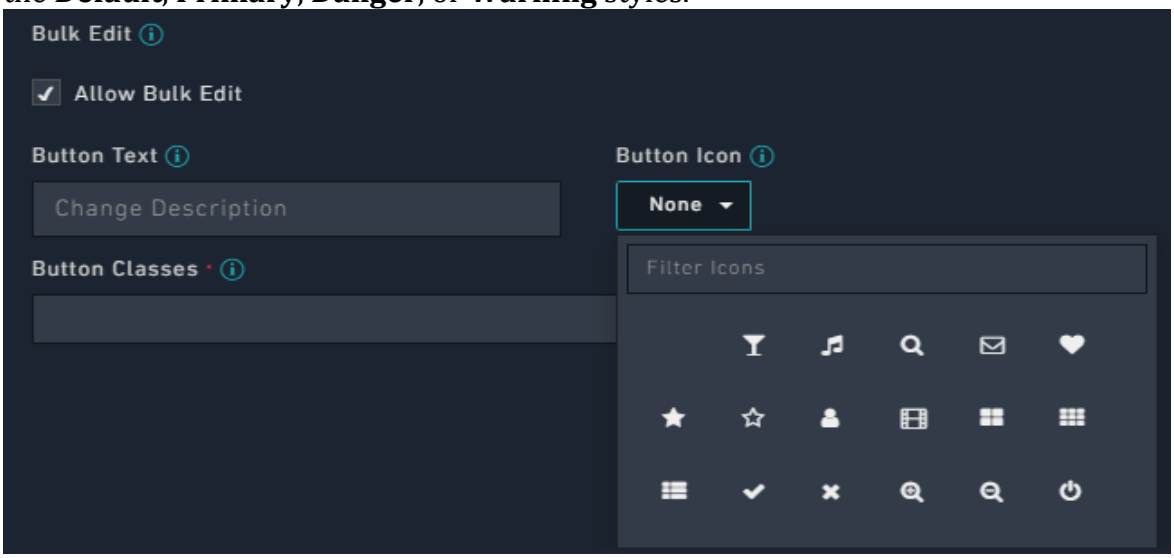
either a Static date/time or a Custom date/time. If you select **Static**, click the **Select Date** icon to display the Calendar and select the required date/time. If you select **Custom**, then you can specify a date/time relative to the current date/time such as 1 hour from now, or 3 hours ago.



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, 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.

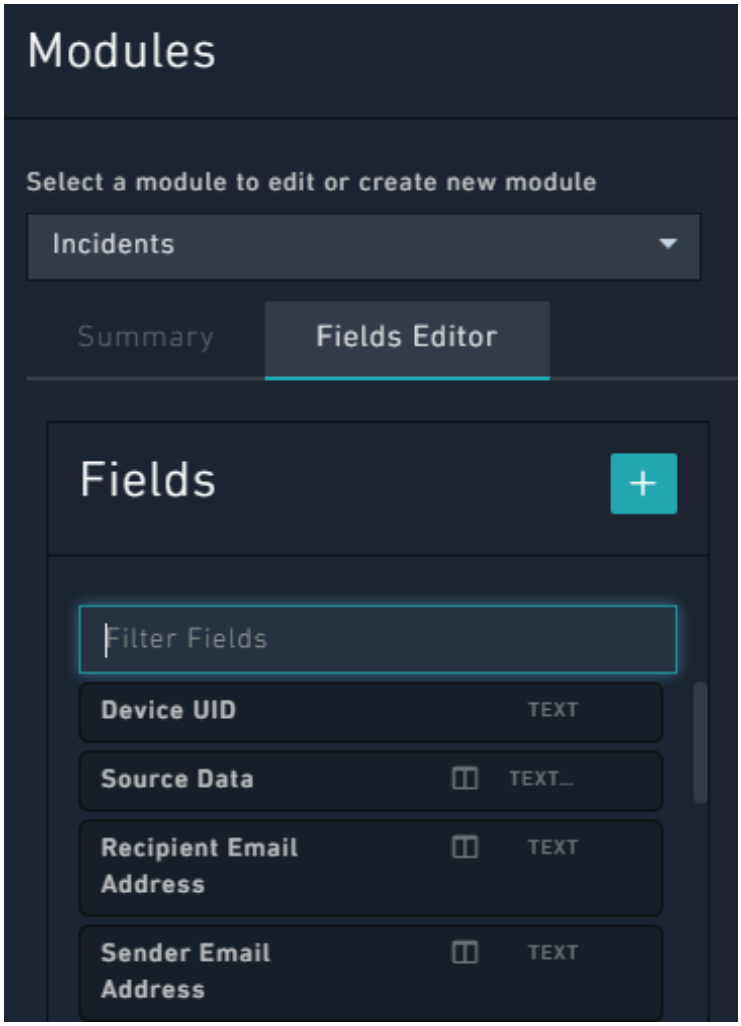


Once you save the changes and publish the module, a **Change Severity** button is added to the `Alerts` module in the action bar. For more information on how to use the bulk action button, see *Working with Modules - Alerts & Incidents*. You can add the bulk edit action button for any other fields, such 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`:

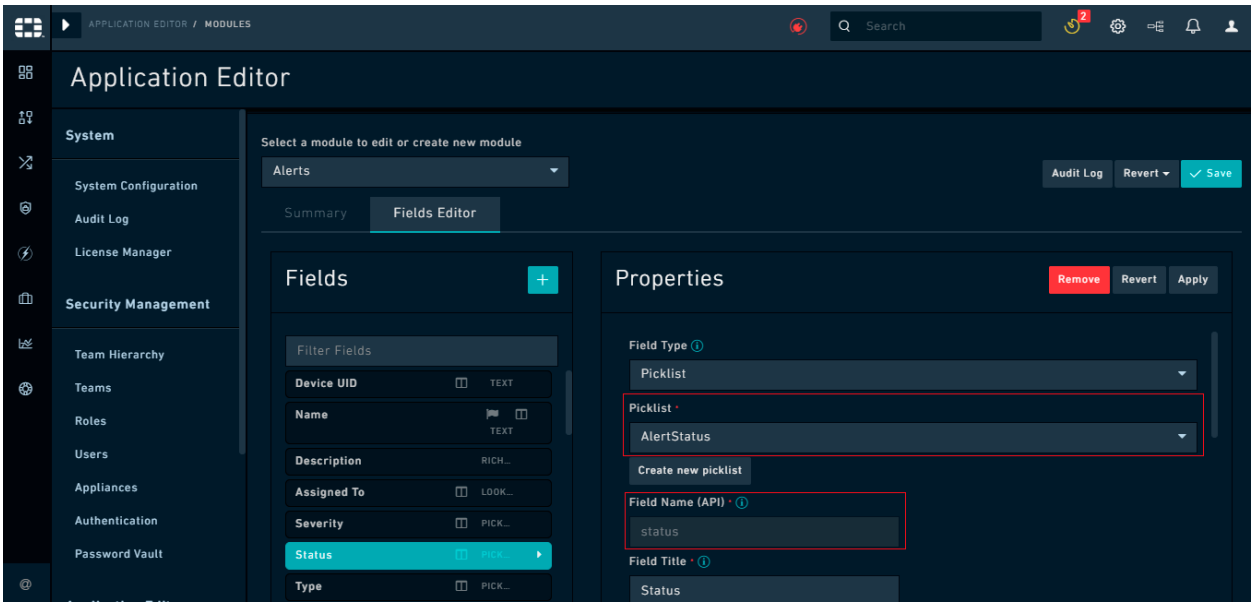


Figure 57. *Example of adding jinja in Display template for picklists*

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 }}`

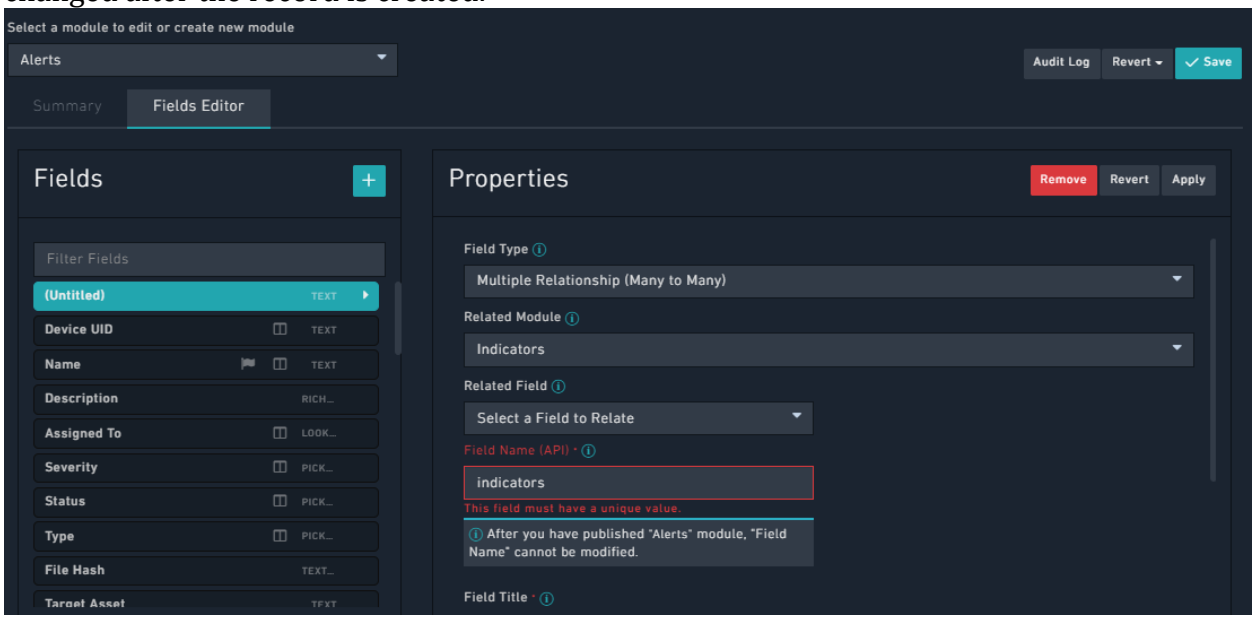
We recommend that to keep things simple, most of the time you would want to use the following expression for a Display Template, assuming you always create a `name` field for a module:
`{{ name }}`

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

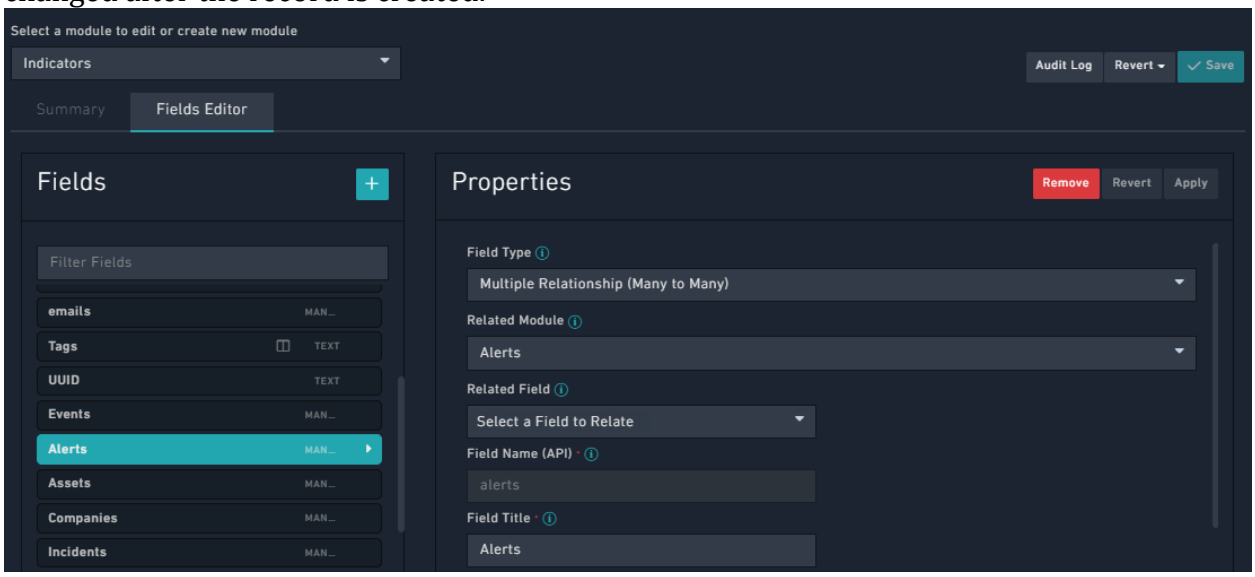
1. Click **Settings** and click **Modules** in the `Application Editor` section, to open the Module Editor.
   This displays the `Modules` page.

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: **Multiple Relationship (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.

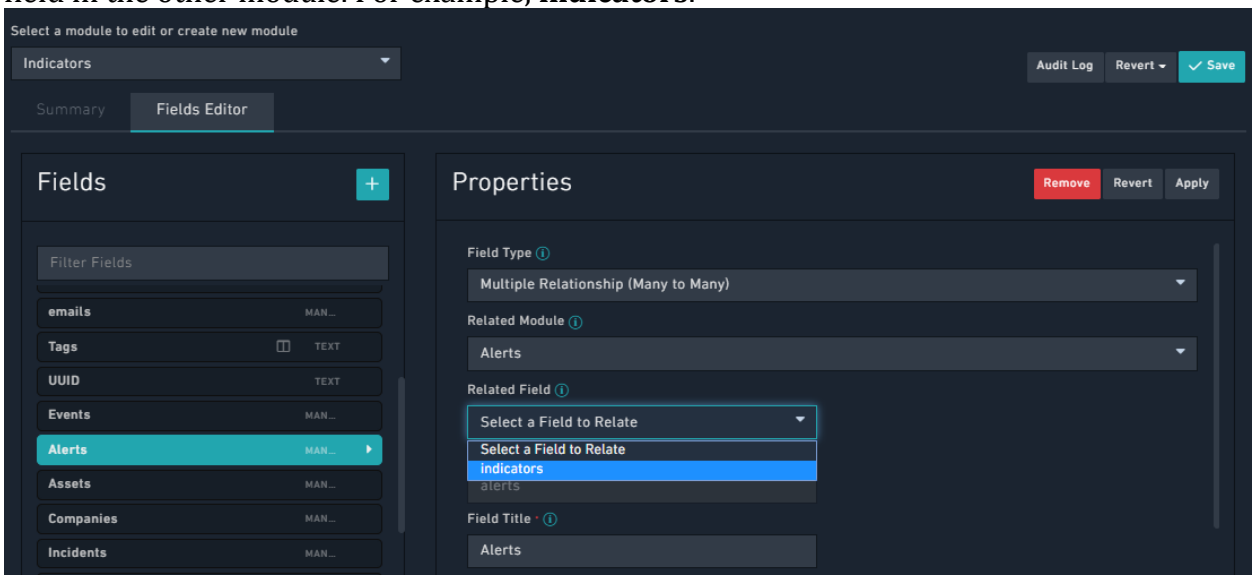


5. Click **Save**.
6. On the `Modules` page, from the **Select a module to edit or create new module** drop-down list, select the other module to be related.
   For example, select `Indicators`.
7. Click the **Fields Editor** tab and click the Add (**+**) icon beside `Fields`.
8. Set the following values:
   Field Type: **Multiple Relationship (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.

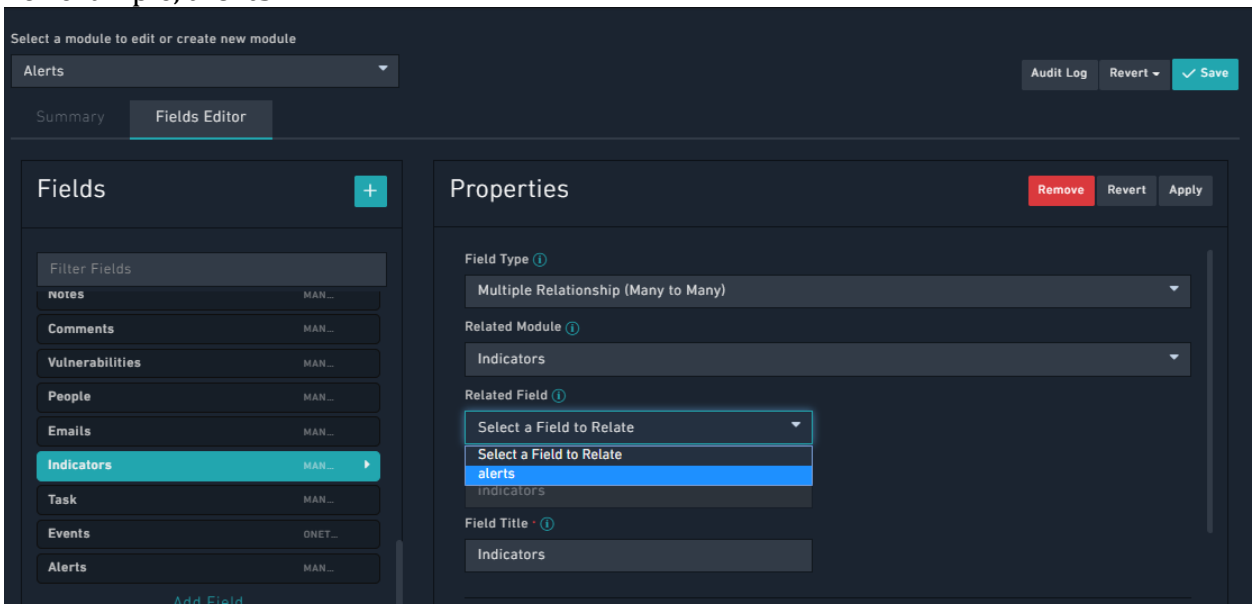


9. Click **Apply**.
10. Select the same name and set the value **Related Field (Optional)** field to the related field in the other module. For example, **indicators**.



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**.



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.

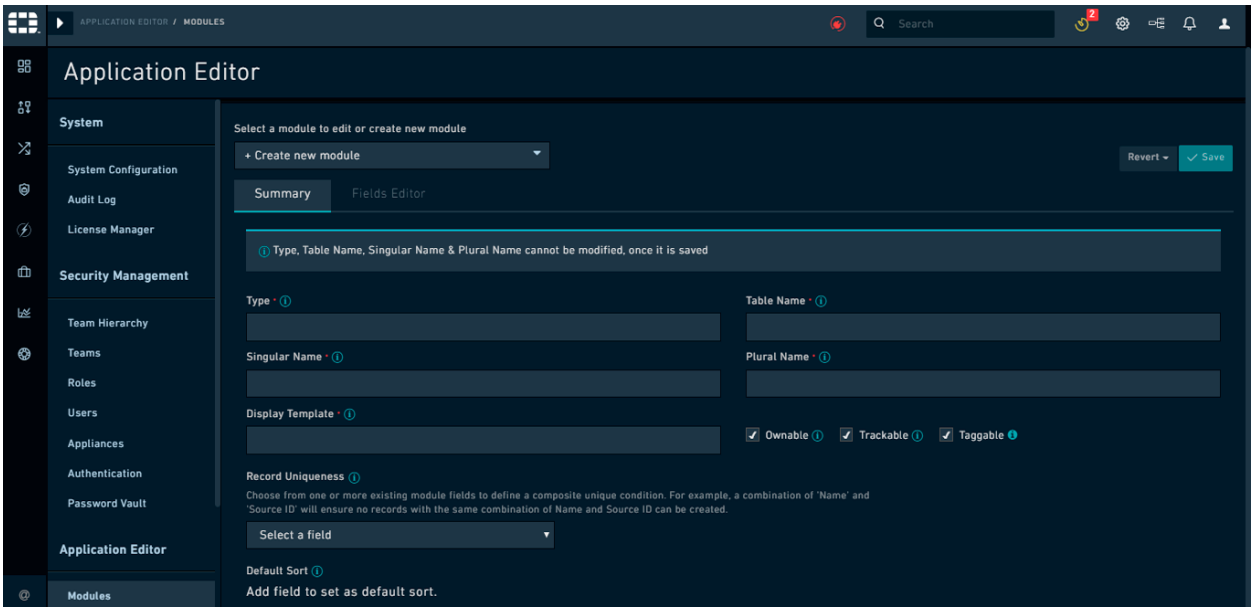


Figure 58. *Adding a new Module*

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 `Multiple Relationship (Many to One)`, or a `Multiple Relationship (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`.

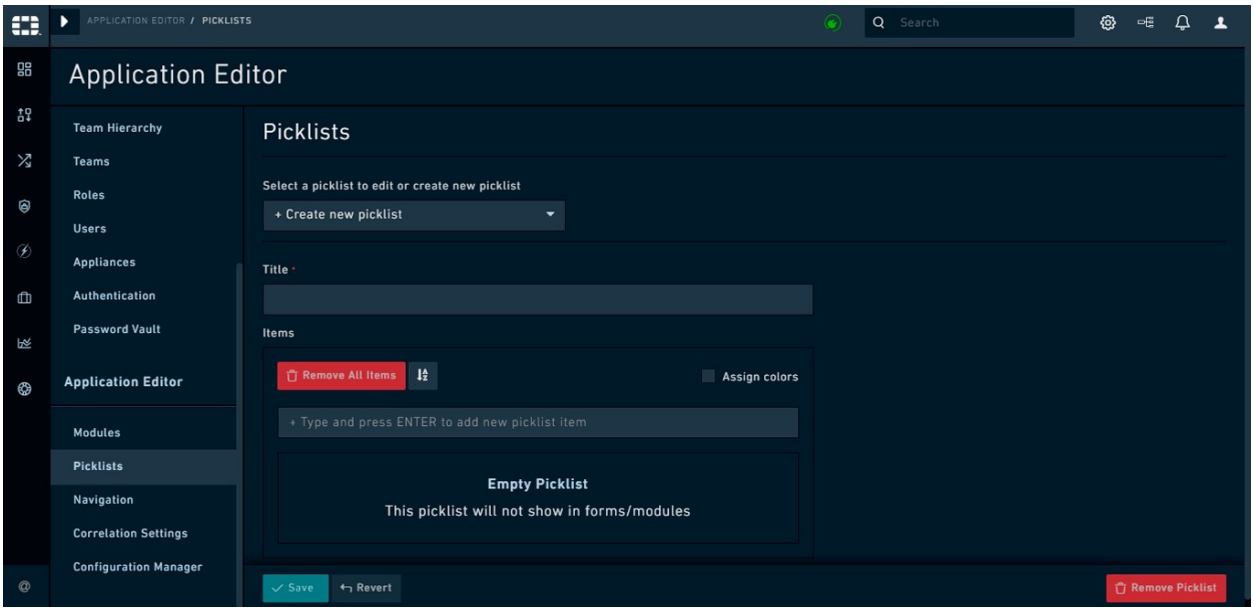


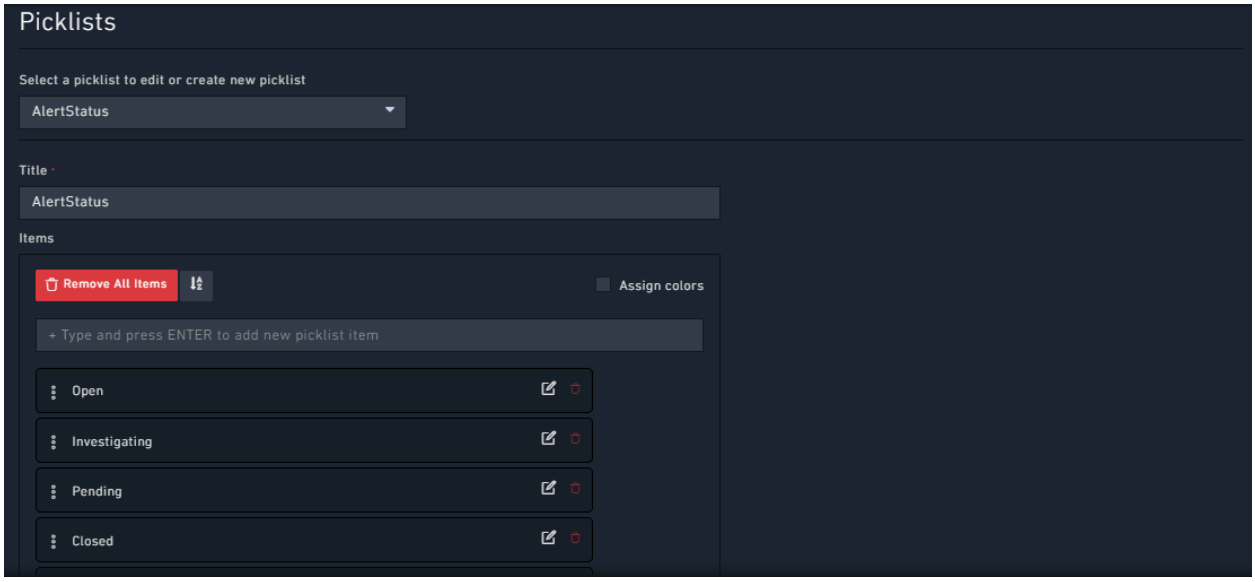
Figure 59. *Picklist Editor*

Creating or modifying a picklist

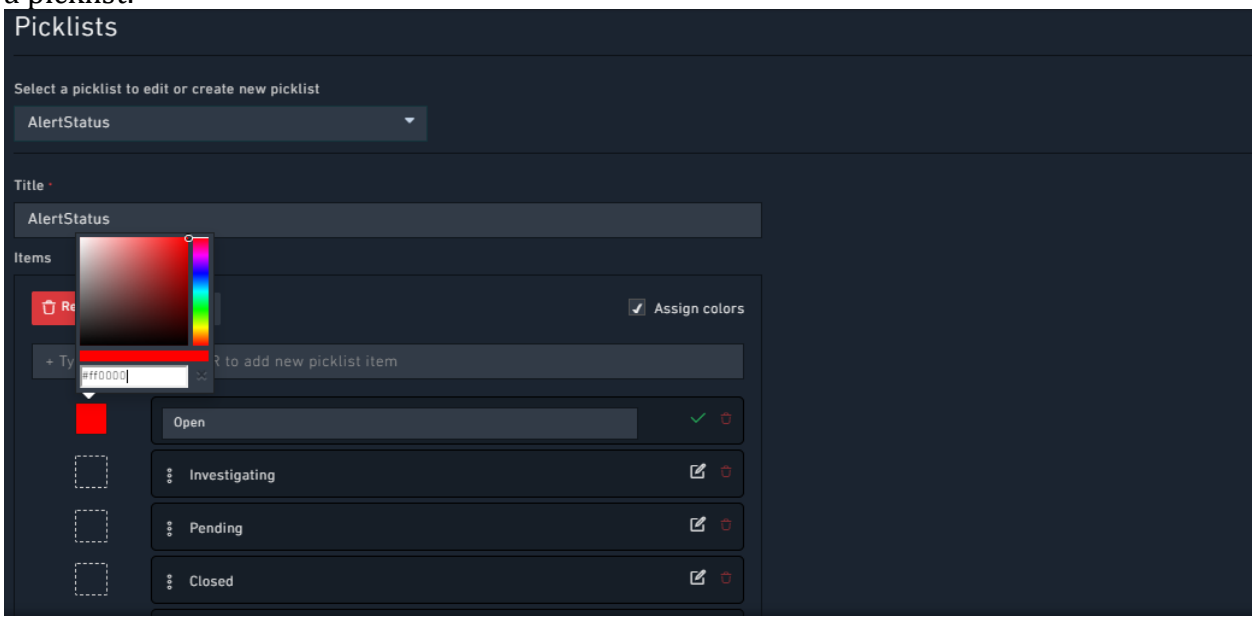
To add or modify a picklist:

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.

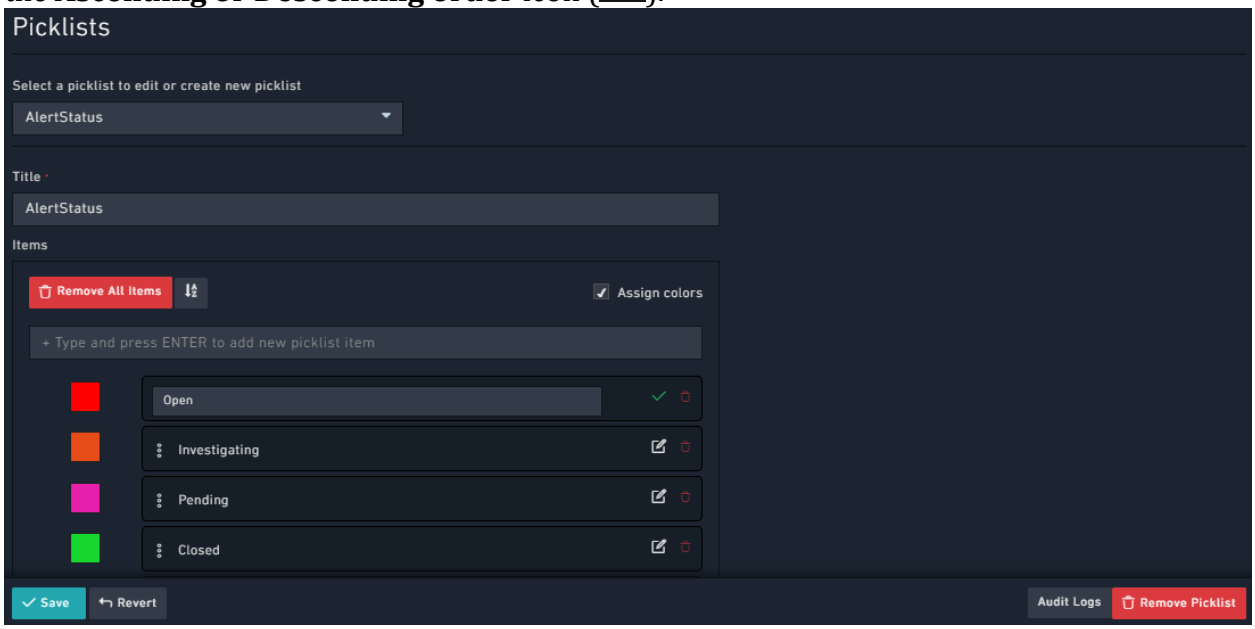


4. (Optional) You can add colors to any picklist, by checking the **Assign Colors** checkbox. Once the Assign colors checkbox is enabled, you can assign each item in the picklist a color.
Use the color picker box that appears next to each item in the picklist or enter the hexadecimal code for the color 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.

5. (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 ( ).



6. 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 to the left navigation bar using the Navigation Editor affects all users. Currently, these changes cannot be made at a user-specific level.

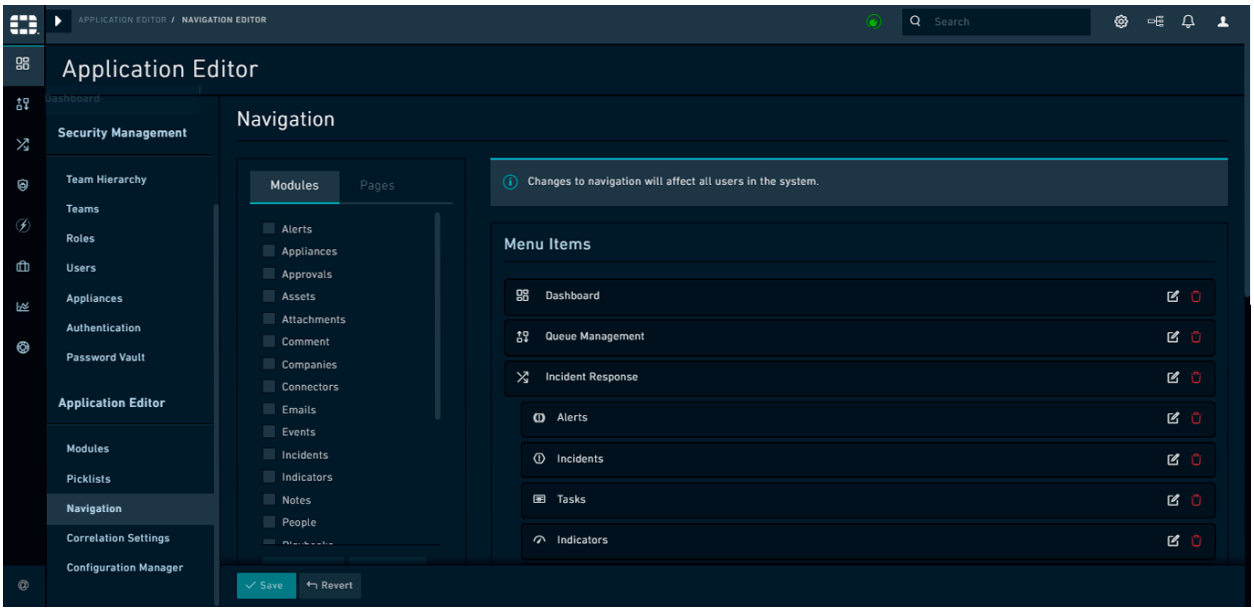


Figure 60. *Navigation Editor*

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.

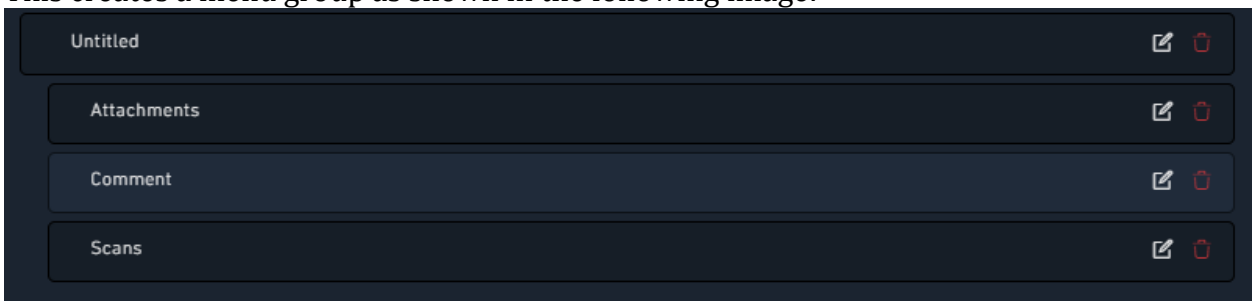
You can add an external HTML page in an iFrame and display that page as part of the left-navigation in FortiSOAR™.

Modifying the Navigation bar

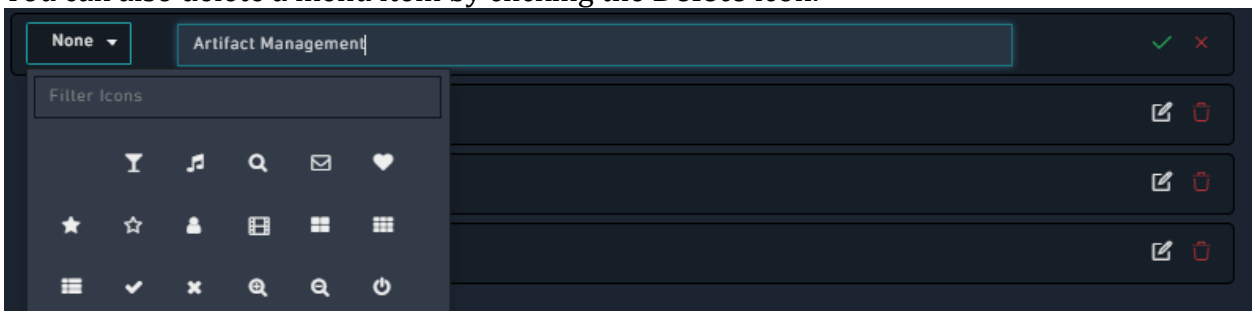
To modify the Navigation bar:

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:

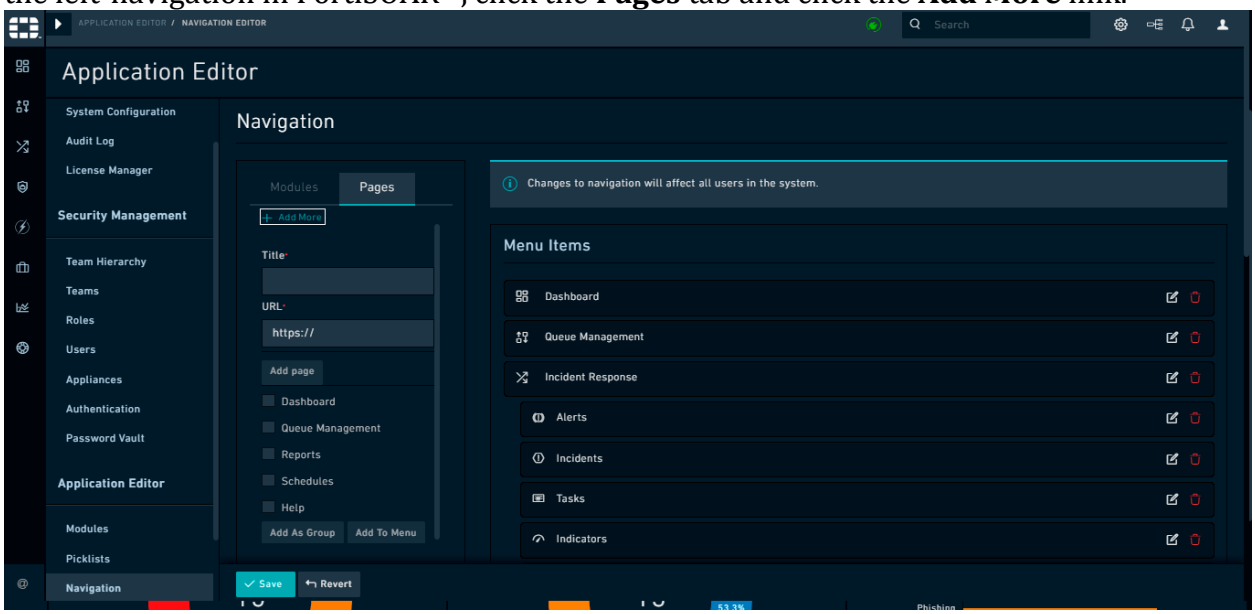


3. Edit the menu items by clicking the **Edit** icon that appears on the item row, update the name of the menu item or replace the icon of the first-level item in menu group, and click the green tick mark icon.
   You can replace icons by choosing icons from the icon selector at the left of each Navigation 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.

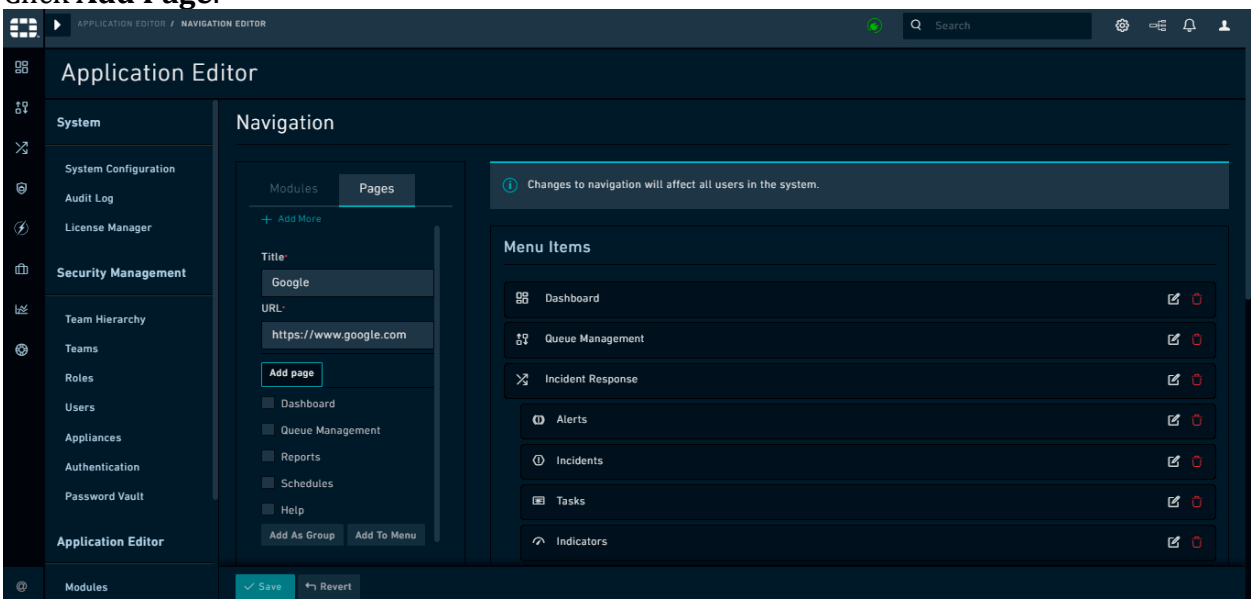
5. (Optional) To add an external HTML page in an iFrame and display that page as part of the left-navigation in FortiSOAR™, click the **Pages** tab and click the **Add More** link.



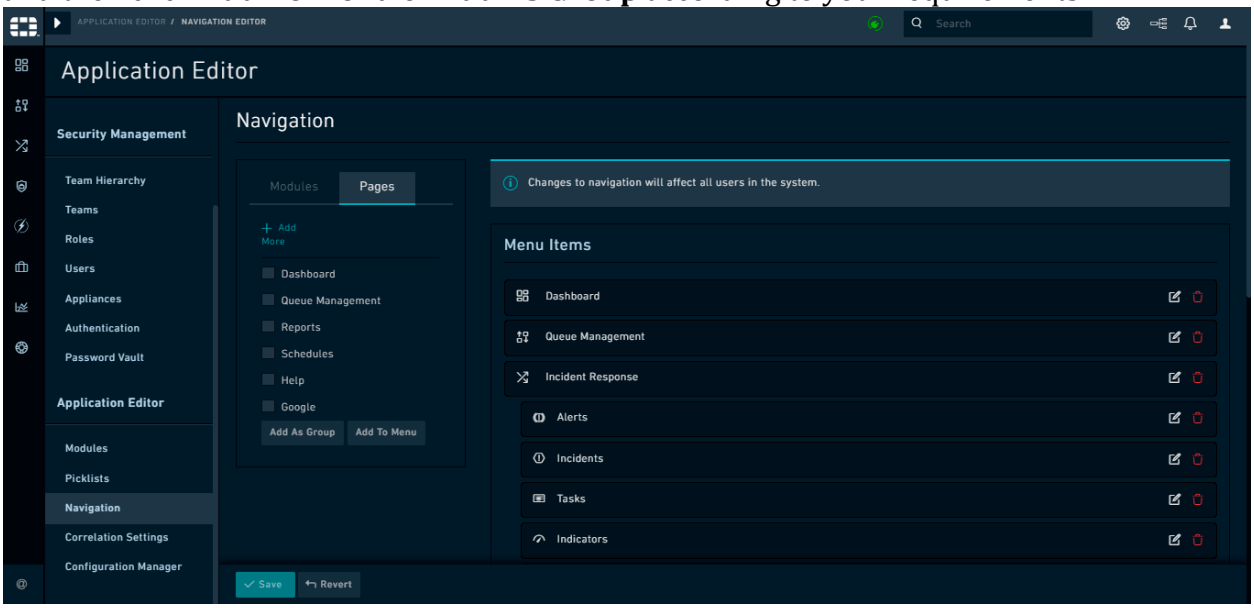
a. In the **Title** field, enter the name for the HTML page that you would want to display in the left navigation menu.
For example, if you want to add a link to the Google website as part of your left-navigation in FortiSOAR™, enter `Google` in the title field.

b. In the **URL** field, enter the URL for the HTML page that you want to display in an iFrame. For our example, enter `https://www.google.com`.

c. Click **Add Page**.



d. 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 alert nodes that has associated indicator nodes:

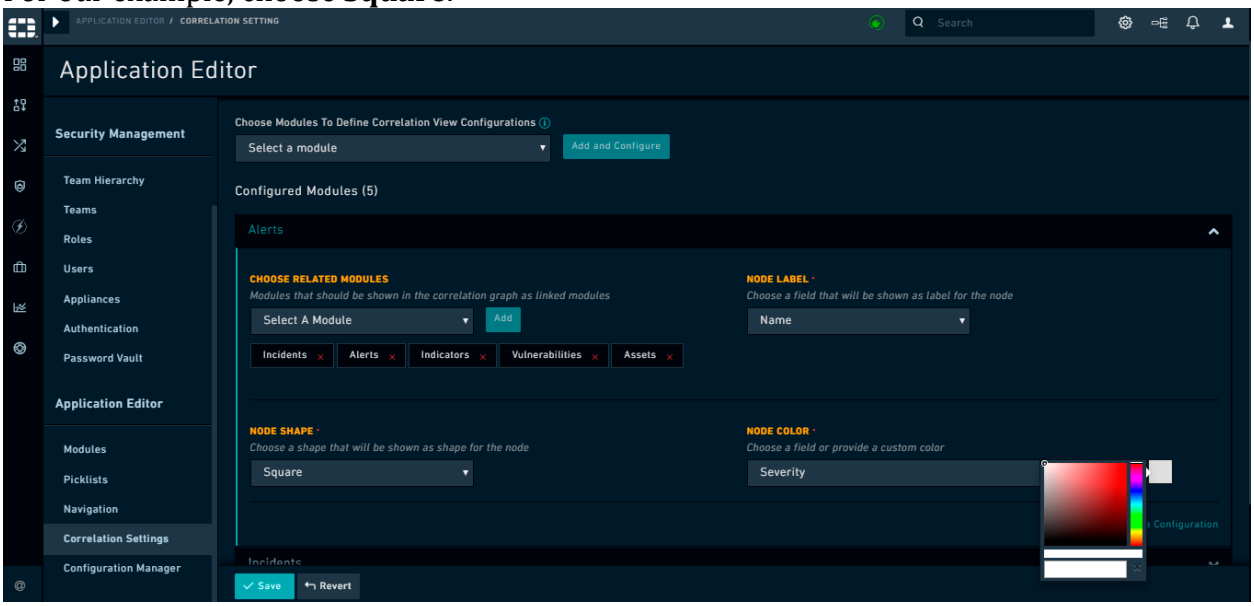
1. Click **Settings** and in the `Application Editor` section, click **Correlation Settings**.
2. On the `Visual Correlation Setting` page, from the **Choose Modules To Define Correlation View Configurations** drop-down list, select the module for which you want to define visual correlations and then click **Add and Configure**.
   Note: FortiSOAR™ has pre-configured five modules, Alerts, Incidents, Indicators, Vulnerabilities, and Assets. 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.
   For our example, we require the `Alerts` module, so we do not require to perform this step.
3. On the **Alerts** bar, click the down arrow and then configure the following parameters:
   a. From the **Choose Related Modules** drop-down list, select the module that should be shown in the correlation graph as linked modules and then click **Add Related Modules**.
   Note: There are some modules that are pre-configured as related modules for

the Alert module such as, Alerts, Incidents, Indicators, Vulnerabilities, and Assets.
For our example, we require to add `Indicators` as a related module to the `Alerts` module, so we do not require to perform this step.

b. From the **Node Label** drop-down list, select the field that will be shown as a label for the node.
By default, this is set as **Name**.
For our example, choose **ID**.

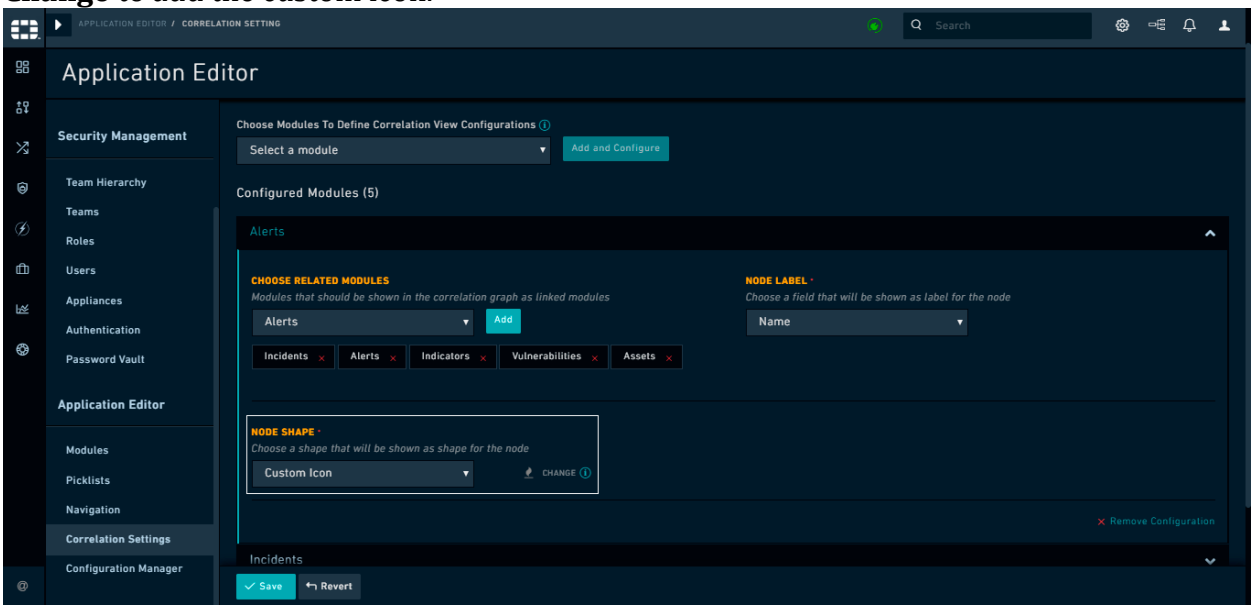
c. From the **Node Color** drop-down list, select the field that will conditionally determine the color of the node.
By default, this is set as **Severity**, which is what we need for our example. You can also choose Status, Type, or Escalated.
Note: In case of a picklists the color of the node is determined by the color that you have assigned to the value of the picklist item. For example, if you have chosen the **Severity** 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 Severity is set as Critical, 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 alert in which you have added the visual correlation widget is Critical, then its node color will be Red.
You can also determine a custom color for the node by using the **Choose custom color** picker.
If you do not specify any color, the node will appear as black.

d. 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

Change to add the custom icon.



Clicking **Change** displays the `Upload an Image` dialog, and then drag-and-drop the icon file, or click the **Import** icon and browse to the icon file XML file to import the icon file into FortiSOAR™ and then click **Save Image**.
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.

4. Next, you require to define how the related record node will also be displayed. For our example, we have to configure the `Indicator` module, which is a pre-configured module, so we do not require to add this module.
5. On the **Indicators** bar, click the down arrow and then check the pre-configured parameters and change them as per your requirements:
   a. From the **Choose Related Modules** drop-down list, select the module that should be shown in the correlation graph as linked modules and then click **Add Related Modules**.
   Note: The Alerts module is already added as a related module to the Indicators module.
   b. From the **Node Label** drop-down list, select the field that will be shown as a label for the node.
   By default, this is set as **Value**.
   c. From the **Node Color** drop-down list, select the field that will conditionally determine the color of the node.
   By default, this is set as **Reputation**.
   From the **Node Shape** drop-down list, select a shape that will be shown as the shape of the node.
   By default, this is set as **Circle**.
6. Click **Save** to save the settings for visual correlation.

Now if you have added the Visual Correlation Widget in the Alerts detail view (see *Dashboards, Templates, and Widgets* chapter in the "User Guide"), it will display as shown in the following image:

Figure 61. *Display of the configured Visual Correction Widget in the Alerts Details view*

As you can see in the above image, the Correlations graph has a title which is **Indicators associated with the Alert**. The title can be specified by the user when they are adding the Visual Correlation Widget. The alert for which the associated indicators are displayed is shown as a square node, whose color is determined by its severity, Orange in this case since the alert has severity set as High. The ID of the alert displayed as the label of the node. The associated indicators are displayed as circular nodes, whose colors are determined by their reputation, hence one circles are red (reputation set as malicious), one is yellow (reputation set as suspicious), one is light green (reputation not available), and one as grey (reputation TBD). The value of the indicator displayed as the label of the node.

Configuration Manager

Use the Configuration Manager to export configuration or metadata information of your models, view templates, and picklists from FortiSOAR™. You can also import configurations or metadata information for modules from other environments into FortiSOAR™ using Configuration Manager. Configuration Manager, therefore, enables you to move model metadata, picklists, and system view templates across environments.

Important: Do not import MMDs between major releases of FortiSOAR™. For example, do not import an MMD from version 5.x into version 6.x.

Using the Configuration Manager, you can export and import dashboards, reports, system views, roles, and picklists not related to modules. The system views that you can export, and import are for Queue Management Configuration and Navigation.

Using the Configuration Manager, you can replace picklist items during import instead of skipping them. You can also select the **Keep Existing Fields By Default** check box to retain fields that were present in an existing module, but which are not present in the exported (new) module. For example, if you have an **Alerts** module existing on your FortiSOAR™ Env1 having a field named **Notes** and you have exported the **Alerts** module from FortiSOAR™ Env2, which does not have the field named Notes. Now, when you import the Alerts module configuration from FortiSOAR™ Env2 to FortiSOAR™ Env1, the Notes field is retained in FortiSOAR™ Env1 if you have checked the **Keep Existing Fields By Default** check box.

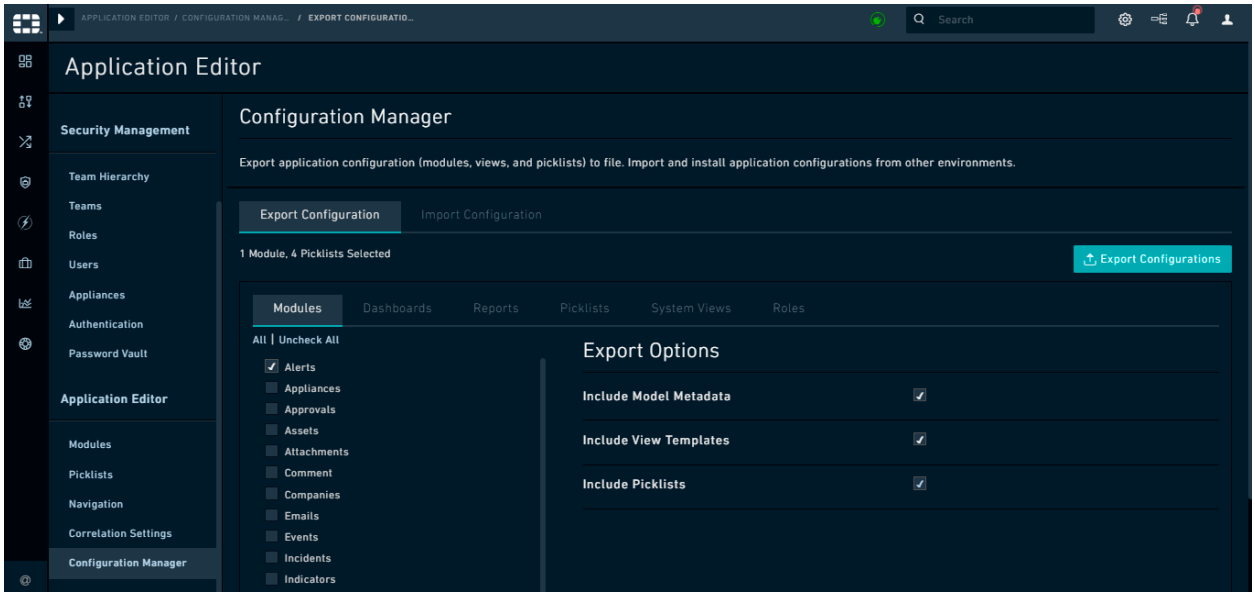
Note: FortiSOAR™ ensures that you either revert or publish staged changes prior to importing configurations so that there are no issues during the import process.

Exporting configurations

To export configuration or metadata information of your models, view templates, and picklists from FortiSOAR™:

Exporting Modules:

1. Click **Settings** and in the `Application Editor` section, click **Configuration Manager**. This displays the `Configuration Manager` page.
2. On the **Export Configuration** tab, on the **Modules** tab, you can select the module (s) that you want to export.
3. In the `Export Options` section, select the configurations that you want to export.
   Click the **Include Model Metadata** option to export configuration information of the modules that you have selected.
   Once you click the **Include Model Metadata** option, the **Include Picklists** option is automatically selected, 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.
   Click the **Include View Templates** option to export configuration information of the templates that you have created for the selected module(s).
   Click the **Include Picklists** option to export configuration information of the picklists that you have created for the selected module(s).
   Note: Once you select a specific module then the picklists associated with that particular module are automatically selected For example, if you select the **Alerts** module, the **AlertStatus**, **AlertType**, and **EscalatedToIncident** picklists are automatically selected.
   By default, all the export options are selected.
4. Click the **Export Configurations** button to export the specified configuration information of the modules that you have selected.
   FortiSOAR™ exports the specified configuration information in the JSON format.
   FortiSOAR™ displays warnings if there are any inconsistencies in the data, such as templates not found, to be exported.



You can now use the JSON file containing the exported configurations in another environment.

Exporting Dashboards and Reports:

1. Click **Settings** and in the `Application Editor` section, click **Configuration Manager**. This displays the `Configuration Manager` page.
2. On the **Export Configuration** tab, click the **Dashboards** tab or the **Reports** tab and select the dashboards or reports that you want to export.
   Click **All** to select all the dashboards or click **Uncheck All** to deselect all the dashboards.
3. Click the **Export Configurations** button to export the specified configuration information that you have selected in the JSON format.

Exporting Picklists:

1. Click **Settings** and in the `Application Editor` section, click **Configuration Manager**. This displays the `Configuration Manager` page.
2. On the **Export Configuration** tab, click the **Picklist** tab and select the picklist (s) that you want to export.
   Click **All** to select all the reports or click **Uncheck All** to deselect all the reports.
   Using this tab, you can export those picklists that are not associated with any module.
3. Click the **Export Configurations** button to export the specified configuration information that you have selected in the JSON format.

Exporting System Views:

1. Click **Settings** and in the `Application Editor` section, click **Configuration Manager**. This displays the `Configuration Manager` page.
2. On the **Export Configuration** tab, on the **System Views** tab, you can select the system views that you want to export.

You can export the **Queue Management Configuration** and **Navigation** system views.
Click **All** to select all the system views or click **Uncheck All** to deselect all the system views.

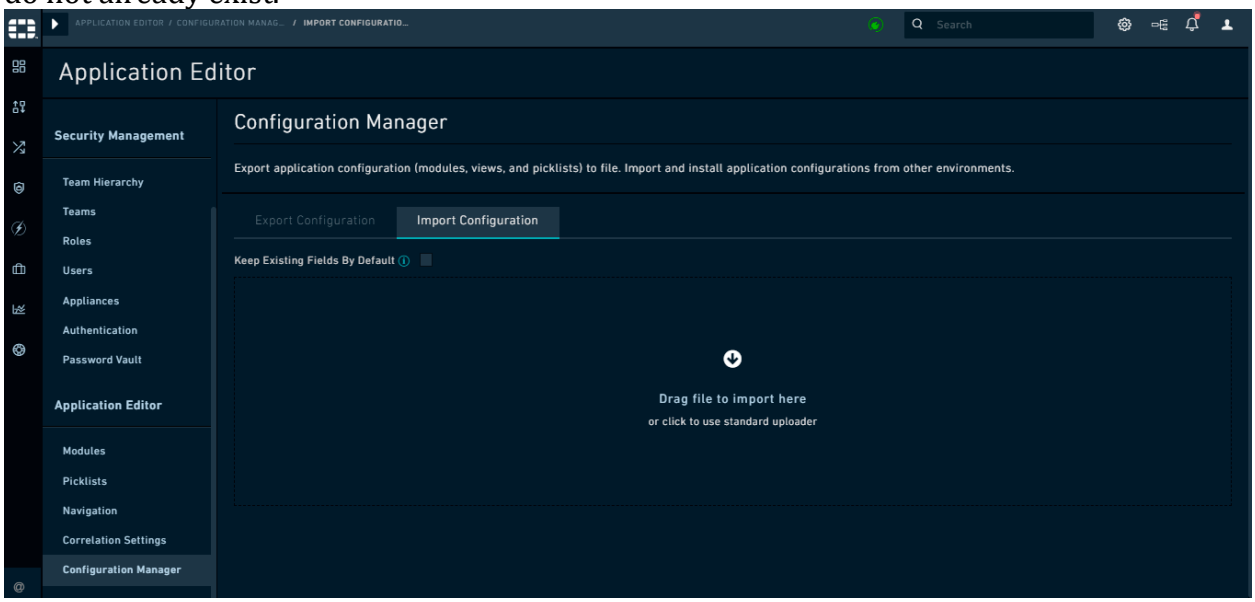
3. Click the **Export Configurations** button to export the specified configuration information that you have selected in the JSON format.

Exporting Roles:

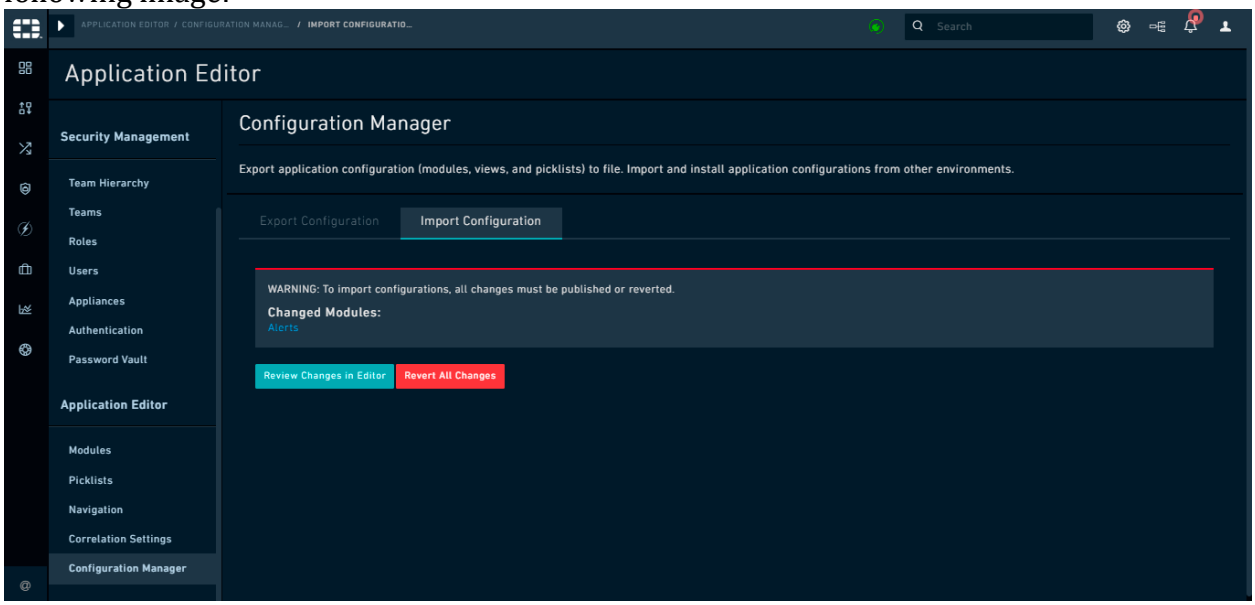
1. Click **Settings** and in the `Application Editor` section, click **Configuration Manager**. This displays the `Configuration Manager` page.
2. On the **Export Configuration** tab, on the **Roles** tab, you can select the role(s) that you want to export.
   You can export roles such as **Full App Permissions**, **Application Administrator**, **T1 Analyst**, **Security Administrator**, etc.
   Click **All** to select all the roles or click **Uncheck All** to deselect all the roles.
3. Click the **Export Configurations** button to export the specified configuration information that you have selected in the JSON format.

Importing configurations

1. Click **Settings** and in the `Application Editor` section, click **Configuration Manager**.
2. On the `Configuration Manager` page, click the **Import Configuration** tab.
   Note: To import module configurations into FortiSOAR™ the configurations file must be in the `JSON` format.
   You will also see a **Keep Existing Fields By Default** checkbox on the `Import Configuration` page. If you select this option, then fields that are present in existing modules will be retained. This option does not affect new modules, i.e., modules that do not already exist.

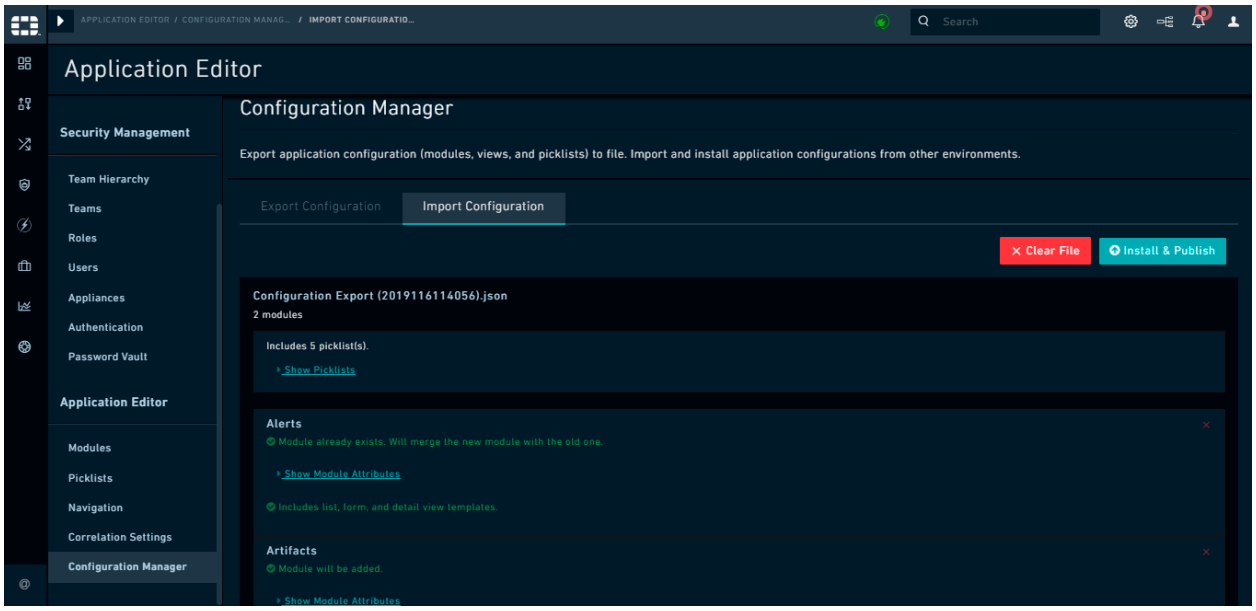


3. Before you can import any configuration, you must ensure that all staged changes are either published or reverted. The Import Configuration tab displays a warning that displays which module(s) have been changed and not published, as shown in the following image:

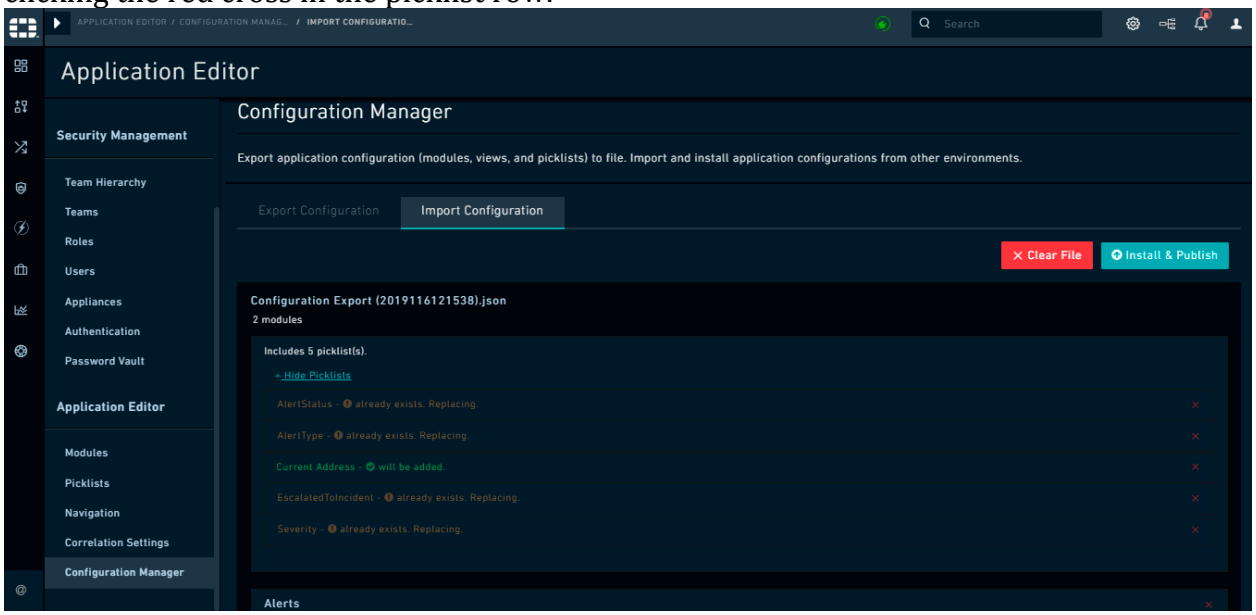


Click the **Review Changes in Editor** button to open the module editor and review the changes in the Module Editor. After reviewing the changes, you can choose to **Publish** the changed modules and then import the modules. Else, you can also choose to revert the changes made in the module by clicking the **Revert All Changes** button and then import the modules (if required).

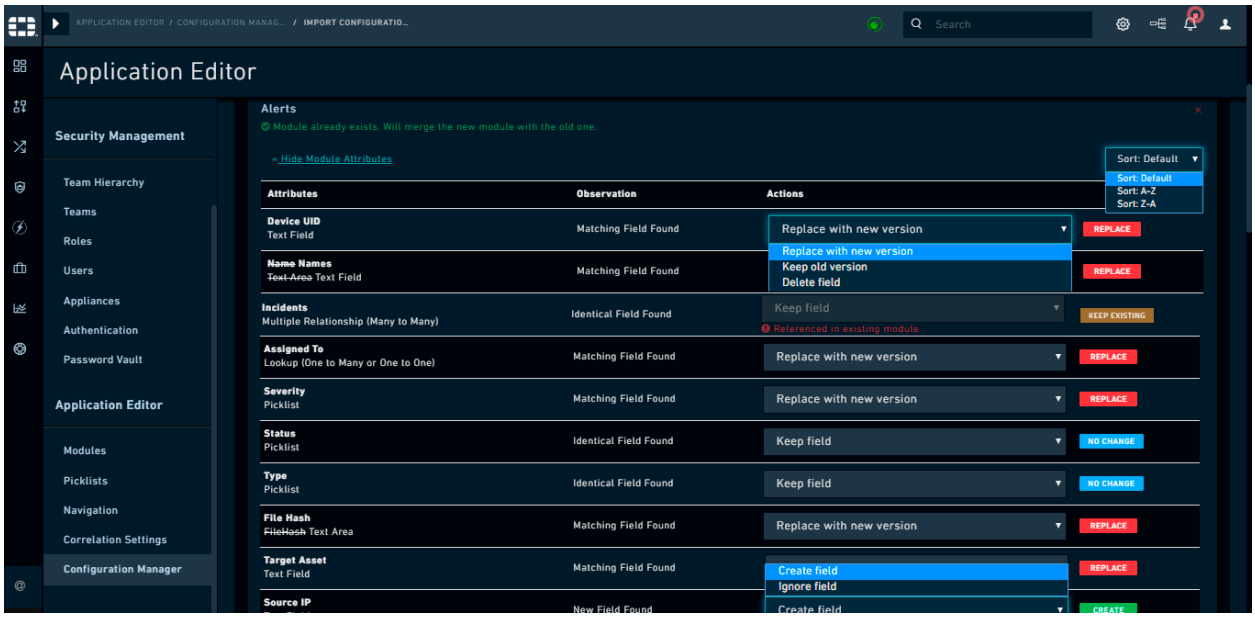
4. Drag and drop the JSON file, or click the **Download** icon and browse to the JSON file to import configurations into FortiSOAR™.
   If the JSON format is incorrect, FortiSOAR™ displays an error message and not import the file.
   If the JSON format is correct, FortiSOAR™ imports the configurations and displays details of what is being imported.



Click **Clear File** to clear the imported JSON file details from Import Configuration FortiSOAR™ displays the count of all configuration items like SVTs, dashboards, roles along with picklists and modules that are going to be imported. If you are importing a new module, then FortiSOAR™ displays a `Module will be added` message. For example, in the above image, **Artifacts** is a new module that you are importing. If you are importing configuration for an existing module, then FortiSOAR™ displays a `Module already exists. Will merge the new module with the old one`. For example, in the above image, **Alerts** is an existing module that you are importing. Click the **Show Picklists** link to display the picklists details that are going to be imported, such as which picklist are going to be replaced or added after the import. You can choose not to import a picklist, and retain the current existing picklist, by clicking the red cross in the picklist row.



Click the **Show Module Attributes** link to display information module attribute details that are going to be imported. Module attribute details display the following field details:



Module attribute details include 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**, 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.

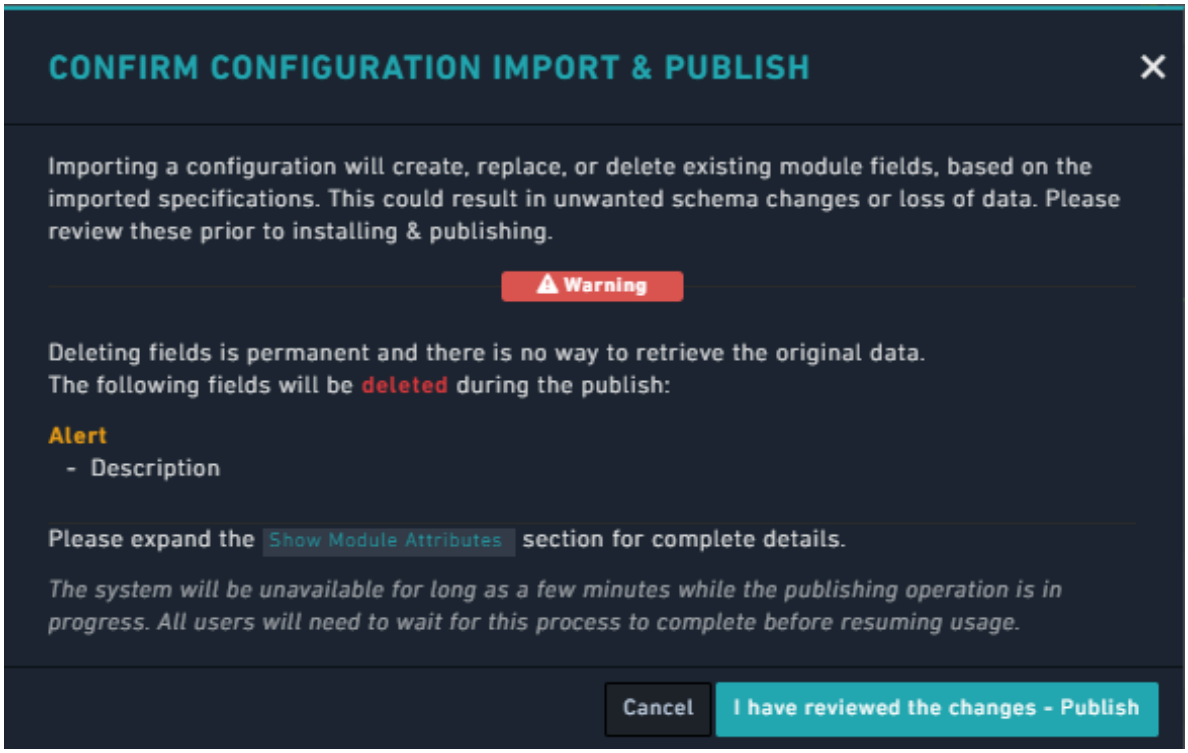
- **No Change (Identical Field Found)**: Fields that present in both the configuration that you want to import and in the existing module and which have *identical* properties in the configuration that you want to import and in the existing module. Available user actions are **Keep field** or **Delete field**. **Note**: Delete field will delete the field from the mmd file.
- **Replace (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 can and ideally, should replace with the newer version of the field. Available user actions are **Replace with new version**, **Keep old version**, or **Delete field**.
- **Keep Existing (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 not replace, for example, in cases where the change made to the field resulted in an Unsupported type conversion and which could result in the Publish failing. Available user actions are **Keep old version** or **Delete field**.

This **Keep Existing** option is also present in cases of fields that are referenced in the existing module and therefore must not be changed. The Action column, in this case, is read-only and cannot be changed by users. This **Keep Existing** option will also be present for system fields, whose properties cannot be changed by the user. An example of a system field would be the **First Name** field in the `People` module. In this case, as well the Action column will be read-only and 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), Multiple Relationship (Many to Many), and Multiple Relationship (Many to one) fields must not be changed once they have been defined. For example, the Alerts module contains a Multiple Relationship (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.

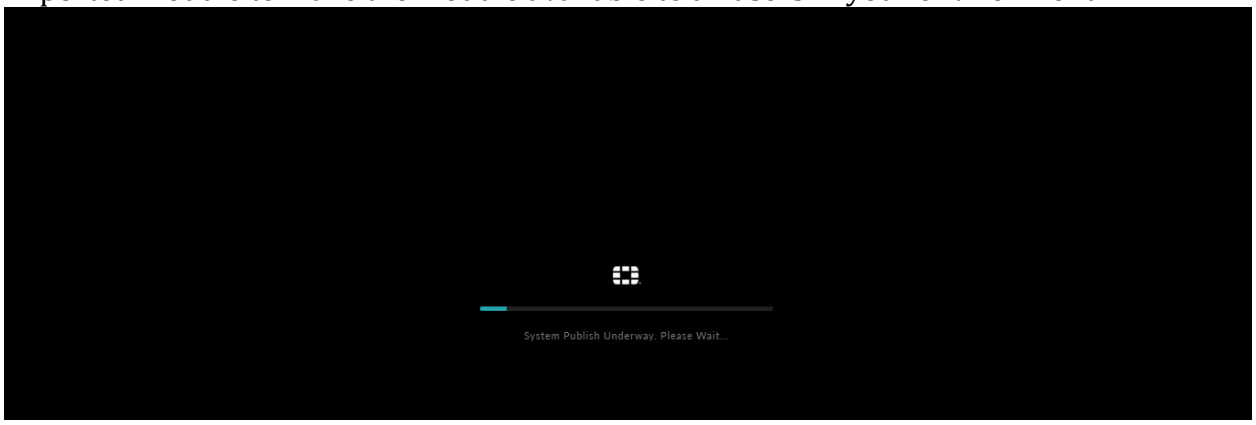
- **Create (New Field Found)**: Fields that are present only in the configuration that you want to import, i.e., fields that are newly added to the configuration. Available user actions are **Create field** or **Ignore field**.
  Note: If you select Ignore field then the newly added field is not included in the mmd when you import the configuration.

- **Delete (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 old version** or **Delete field**.

5. The import details include details about what configurations are being imported and also `Log` messages that defines what changes will be made to your configuration after the import. Once you have reviewed the import details displayed by FortiSOAR™, click **Install & Publish** to copy and publish the configuration into your FortiSOAR™ environment.
   FortiSOAR™ will display a warning message asking to confirm whether you have reviewed the changes:



Click **I have reviewed the changes - Publish** on this dialog to copy and publish the configuration into your FortiSOAR™ environment. FortiSOAR™ will then display, a `Model Metadata added. Publishing changes...` message and publishes the newly imported module to make the module available to all users in your environment.



Note: If there are any issues with the configuration that you are trying to import the Publish operation fails. In this case, there is no change to your existing module configuration. However, changes related to configurations of components other than modules, such as dashboards, picklist, or roles are imported, and if you require to update them, then those changes will have to be done manually.

- 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 **Keep Existing Fields By Default** check box to retain fields that were present in an existing module but which are not present in the exported (new) module.

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:

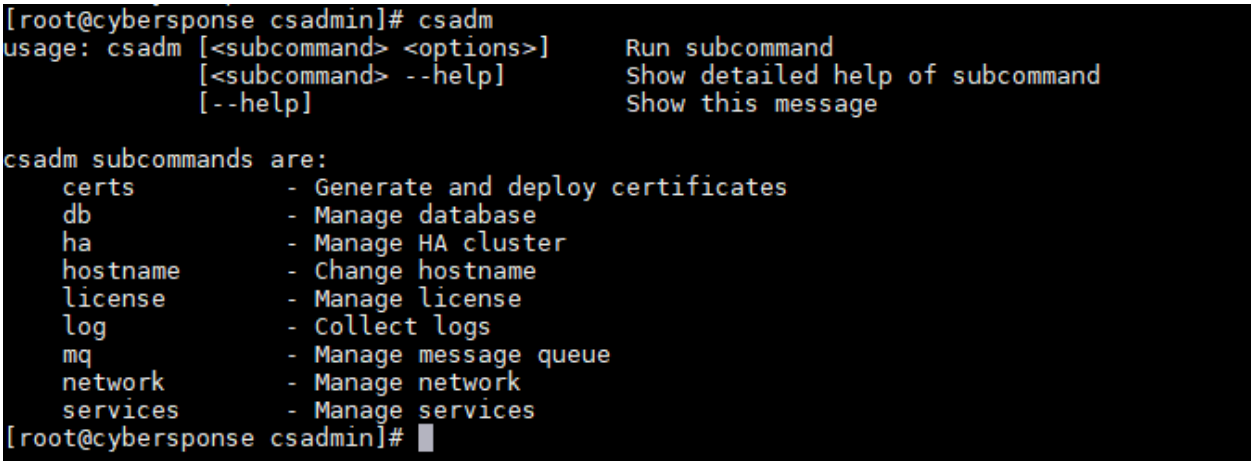


Figure 62. *FortiSOAR™ Admin CLI command prompt*

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	Generates and deploys your certificates. You can use the following options with this subcommand: `--deploy`: Deploys SSL certificates. For more information, see the `Replacing FortiSOAR™ self-signed certificates with your own signed certificates` section in the *Additional configuration settings for FortiSOAR™* chapter in the "Deployment Guide." `--generate <host name>`: Generates and deploys self-signed certificates. You can use the `--no-replace-nginx-cert` option with this command, if you do not want to replace your nginx self-signed certificates.
db	Performs operations related to database. You can use the following options with this subcommand: `--change-passwd`: 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. `--backup`: Performs an encrypted backup of your FortiSOAR™ system. For more information, see the *Backing up and Restoring FortiSOAR™* chapter. `--restore`: Performs data restore from a locally stored file (`/home/csadmin/db_backup/DR_BACKUP_<yyyymmdd_hhmmss>.tar`). For more information, see the *Backing up and Restoring FortiSOAR™* chapter. `--encrypt`: 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. `--externalize`: 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 *Externalization of your FortiSOAR™ PostgreSQL database* chapter. `--check-connection`: Checks the connection between FortiSOAR™ and the external PostgreSQL database.
ha	Manages your FortiSOAR™ High Availability cluster. For more information about HA and its commands, see the *High Availability support in FortiSOAR™* chapter.
hostname	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: `--set [<hostname>]`: 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 but does not replace nginx certificate, and restarts FortiSOAR™ services. If you do not specify a hostname, then this sets up the message broker, regenerates certificates using the existing hostname but does not replace nginx certificate, and restarts FortiSOAR™ services. **Note**: Before you run this command, you must ensure that the specified hostname is resolvable.

	`--dns-name [<FQDN>]`: Changes the FQDN. **Note**: Before you run this command, you must ensure that the specified hostname is resolvable.
license	Manages your FortiSOAR™ license. You can use the following options with this subcommand: `--get-hkey` : Retrieves the hardware key for your FortiSOAR™ instance. `--deploy-enterprise-license <License File Path>`: Deploys your FortiSOAR™ enterprise license. For example, `csadm license --deploy-enterprise-license temp/12344.lic`. `--deploy-multi-tenant-license <License File Path>`: Deploys your FortiSOAR™ multitenancy license.
log	Performs log collection. You can use the following options with this subcommand: `--collect`: Collects logs and bundles them up into a `cyops-logs.tar.gz.gpg` file. You must specify the path where the logs should be collected. By default, the logs are collected in the `/tmp/` folder.
mq	FortiSOAR™ message queue controller (RabbitMQ) functions. `--flush-db`: Deletes and recreates the rabbitmq database.
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.
- Once your system is upgraded to version 6.0.0, you must close and logout of your existing SSH session and relogin to your version 6.0.0 instance to run the `csadm` commands and perform any operations.

High Availability support in FortiSOAR™

Overview

FortiSOAR™ supports High Availability (HA) clusters that support both Active-Passive and Active-Active configurations.

FortiSOAR™ supports the following High Availability (HA)/Disaster Recovery (DR) options:

Method	Brief Description
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.
High Availability (HA) clusters	This chapter describes this method of HA/DR.

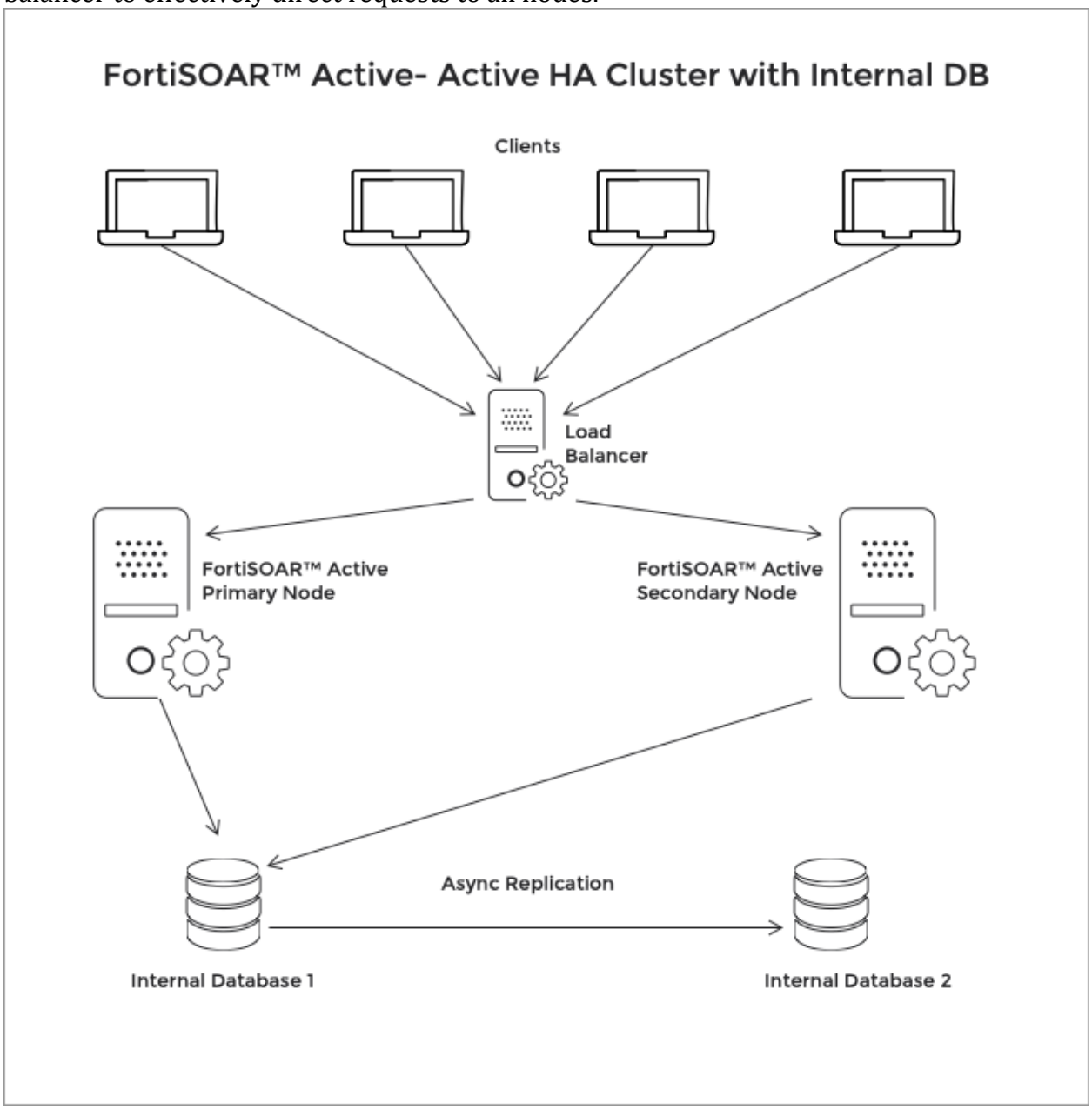
FortiSOAR™ High Availability Scenarios

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

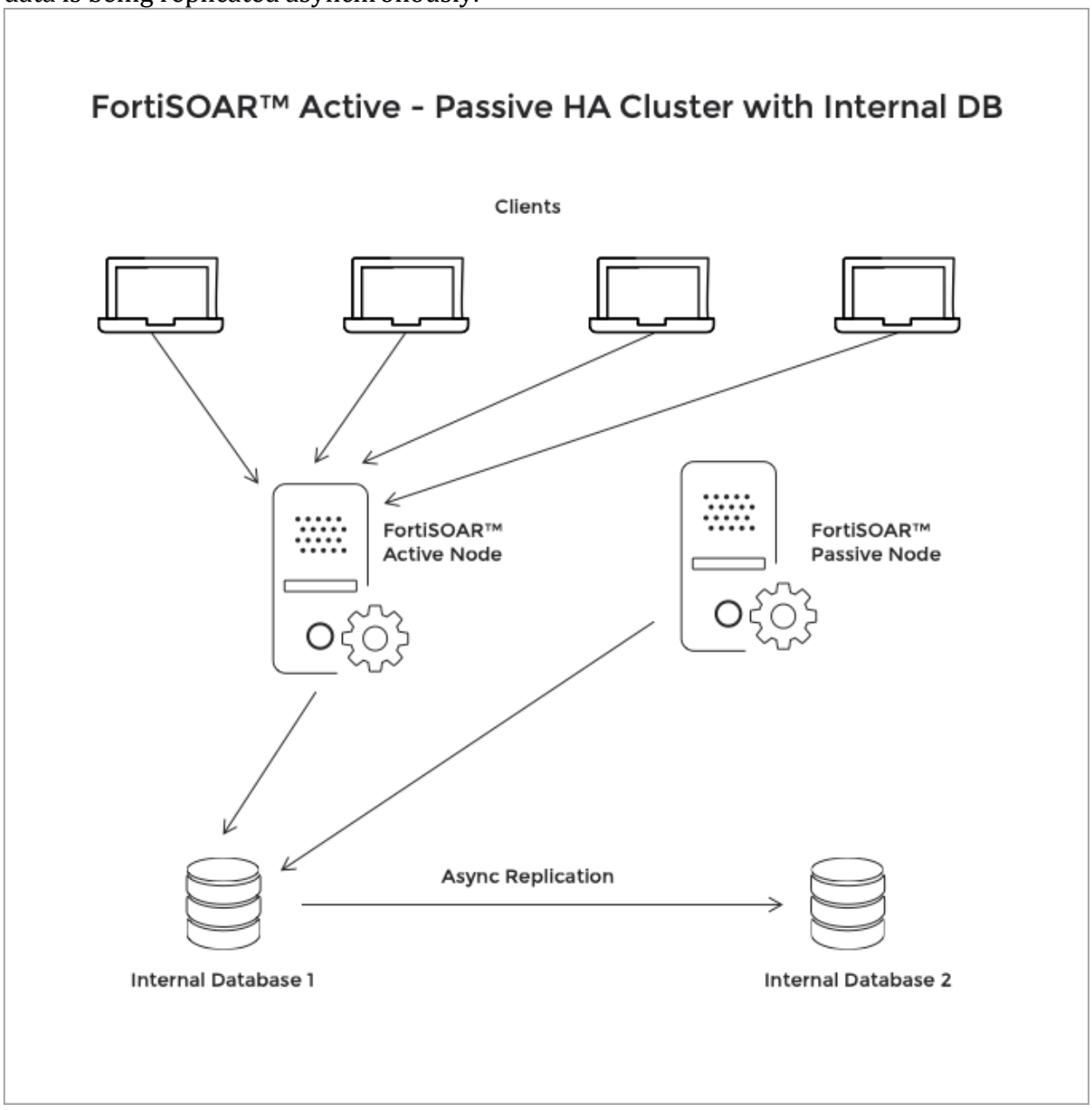
You can configure FortiSOAR™ for high availability (HA) with an internal PostgreSQL database in the following two ways:

- 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.

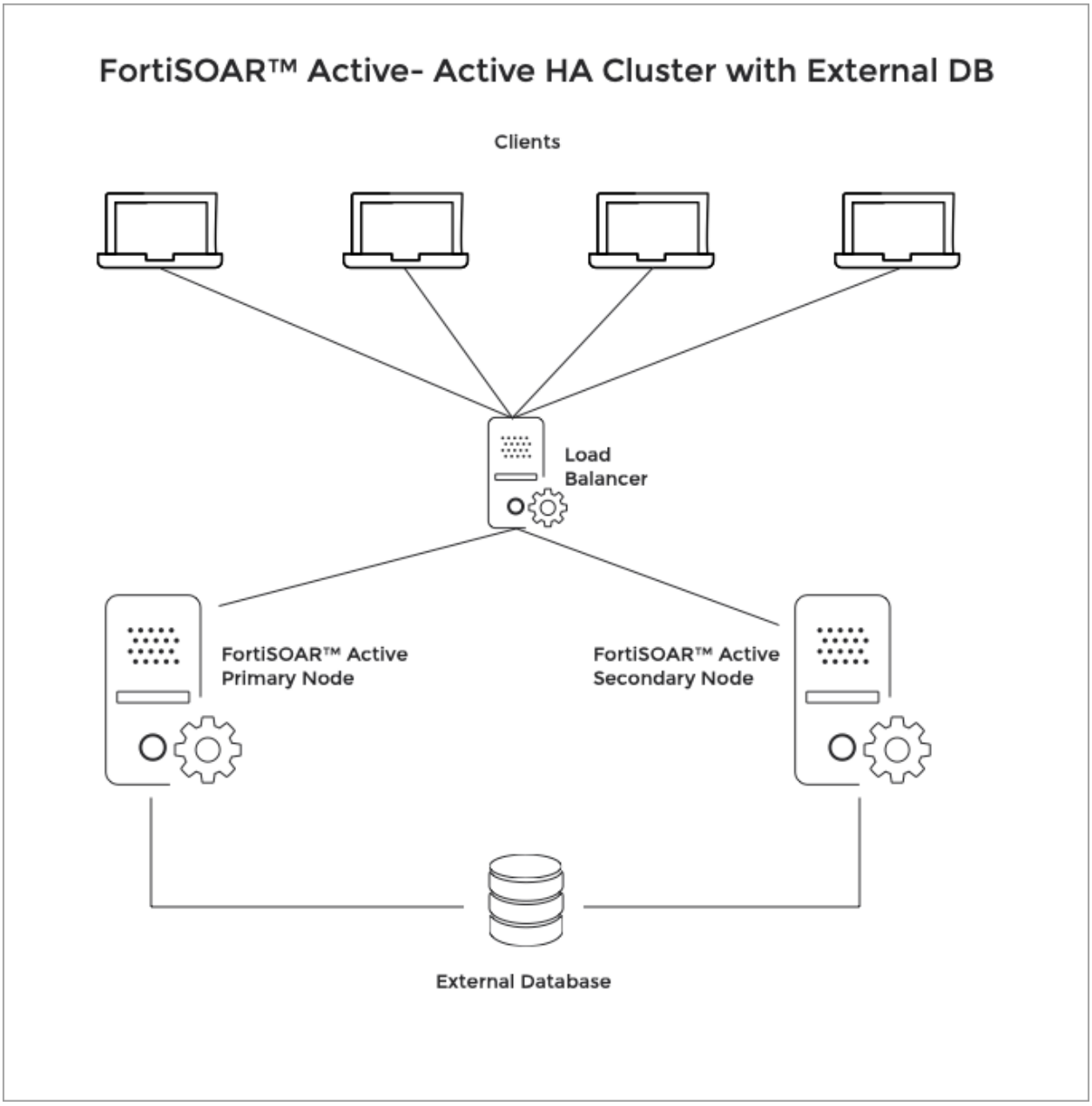


Figure 63. *FortiSOAR™ with an external database and an Active/Active configuration*

From version 5.0.0 onwards, 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. For more information on the FortiSOAR Configuration Wizard, see the *Deploying FortiSOAR™* chapter in the "Deployment Guide."

Notes for FortiSOAR™ HA clusters:

- 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.

Prerequisite 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 Handling session timeouts.
- All nodes that are part of a HA cluster must have a similar license in terms of user count, multitenancy support and entitlements.

Handling session timeouts

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. It is possible that your ssh session will time out since generally the timeout set for an ssh session is 5 minutes, and some of FortiSOAR™ operations can take up to 15-20 minutes, depending on the data volume. This also ensures that ensure the session runs smoothly even the terminal session gets deactivated.

To ensure that your session does not timeout, use the `screen` command that maintains the session until you manually terminate the session.
Command to install `screen` is `# yum install screen`.

For more information of the screen mode and to avoid issues due to session timeouts, see A Basic understanding of screen on Centos.

In cases where yet your current ssh session gets disconnected, then do the following:

1. To list the current session, type the `# screen -ls` command.
2. To restore the session, type `# screen -r XXXX`, where `XXXX` is the last session ID of the last screen.

Process for configuring High Availability

From version 5.1.0 onwards, the process for configuring HA has been simplified, i.e., the join-cluster operation is now a single step operation, which does not require you to perform the following steps:

1. Export the configuration details of the active primary node to a configuration file named `ha.conf`, and then copy the `ha.conf` file to the node that you want to configure as a secondary node.
2. Whitelist the hostnames of the secondary nodes on the active primary server.

Important: You cannot parallelly join nodes to a HA cluster in version 5.1.0. Therefore, in version 5.1.0 you can only join nodes sequentially to a HA cluster.

Process that you can use for configuring HA for version 5.1.0 and later:

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}
                ...

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
  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
[root@cybersponse csadmin]#
```

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 <primary, 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.

3. If you have upgraded to version 5.0.0 and later and are joining a freshly provisioned 5.0.0 (or later) node (with 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.

Alternative process that can be followed to 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, whitelist the hostnames of the secondary nodes, using the following command:
   `# csadm ha whitelist --nodes`
   Add the comma-separated list of hostnames of the cluster nodes that you want to whitelist after the `--nodes` argument.
   Important: In case of an externalized database, you need to whitelist all nodes in a cluster 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 whitelisting the hostnames of the secondary nodes, 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.

3. If you have upgraded to version 5.0.0 or later and are joining a freshly provisioned 5.0.0 (or later) node (with 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.

Important: In the case of an HA cluster, proxy settings get replicated only for FortiSOAR™ services on the secondary/passive nodes. OS services or commands such as 'yum', 'curl', or 'wget' do not honor the proxy settings of the primary node. Therefore, to configure proxy settings on the secondary node, you can either configure the proxy setting when the FortiSOAR Configuration Wizard is run on the first login of the 'csadmin' user (using SSH) or by using the `csadm network {set-https-proxy|set-http-proxy|set-no-proxy}` command.

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 Handling session timeouts.

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:

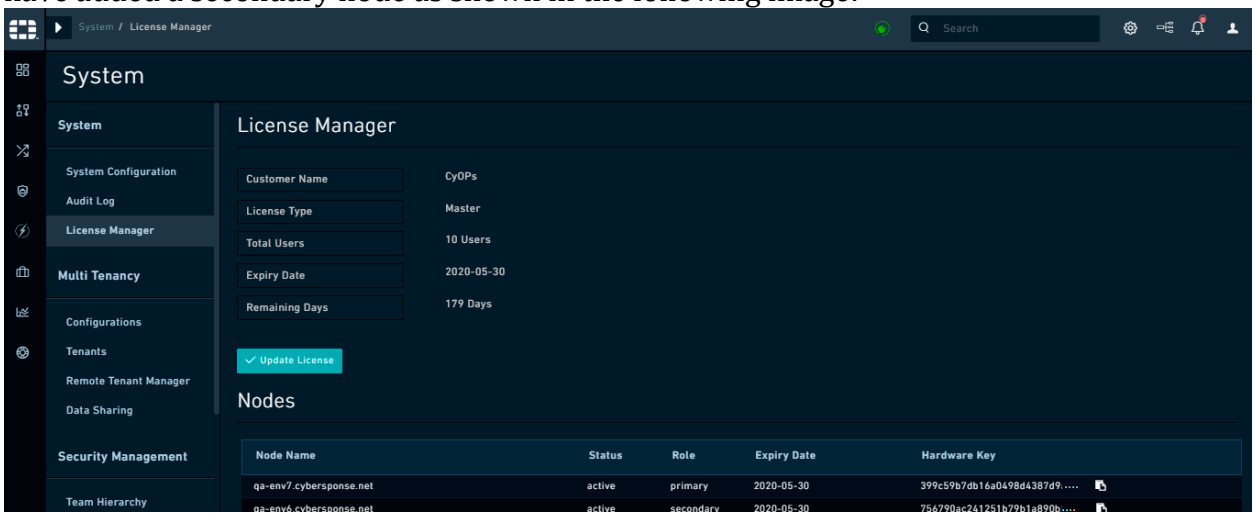
Subcommand	Brief Description
list-nodes	Lists all the nodes that are available in the cluster with their respective node names and ID, status, role, and a comment that contains information about which nodes have joined the specific HA cluster and the primary server.  You can filter nodes for specific 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.
whitelist	Whitelists the hostnames of the secondary nodes in the HA cluster on the active primary node. For more details on `whitelist`, 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.
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. **Important**: 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. Once you have completed the firedrill, ensure that you perform restore, to get the nodes back to replication mode.
restore	Restores the node back to its original state in the cluster after you have performed a firedrill. That is, `csadm ha restore` 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 `csadm ha takeover` command on the secondary node that you want to configure as your active primary node.
list-commands	Lists all pending, in-progress, or failed commands that were propagated across the cluster nodes. You can filter this command for a specific nodeID or state. For example, if you want to retrieve a list of failed commands use the following command: `csadm ha list-commands --status failed`. In case of failed commands, you must check the reason for failure and re-run the failed command manually after resolving the error.
leave-	Removes a node from the cluster and the node goes back to the state it was

cluster in before joining the cluster.

Points to be considered while working with High Availability configurations

- 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.
- In case your FortiSOAR™ instance is part of a High Availability cluster, the `License Manager` page, you will display the information about the nodes in the cluster, if you have added a secondary node as shown in the following image:



- 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.
- For the procedure on how to upgrade a FortiSOAR™ High Availability Cluster to 6.0.0, see the Upgrading a FortiSOAR™ High Availability Cluster to 6.0.0 article.

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.

From version 5.1.0 onwards, `takeover` is a single-step operation, i.e., you do not need to manually reconfigure all the nodes in the cluster to point to the new active primary node. The takeover operation reconfigures the nodes to point to the new active primary node during the process.

However, 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.

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. In both cases, 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.

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.

HAProxy

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 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 the HAProxy

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 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.

Troubleshooting HA Issues

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
```

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: Version 5.1.0 uses Elasticsearch version 7.0.2. Therefore, if you are externalizing ElasticticSearch data, you must ensure that the minimum version of your Elasticsearch cluster is 7.0.2.

If you want to externalize your other FortiSOAR™ PostgreSQL database, see the *Externalization of your FortiSOAR™ PostgreSQL database* chapter.

Externalization and Authentication of Elasticsearch

Version 4.12.0 onwards

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 `ngnix` 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 FortiSOAR™ 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 t
o 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/db_external_config.yml`
   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, update the host (`pg_host`) and port (`pg_port`) (if needed). You must also 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.

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 <path_of_backup_file>`
   `<path of backup file>` is the directory where backup files will be created. If you do not specify the path of backup file in the above file, then the CLI will interactively ask you to provide the path of backup file.
   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`
   Once you run the above command, you will be asked to provide the path of the configuration backup file.

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 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`

Note: The restore process restores data from the following locally saved file: `/home/csadmin/db_backup/DR_BACKUP_<yyyymmdd_hhmmss>.tar`

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
   ```

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 6.0.0, and the build number is 769:

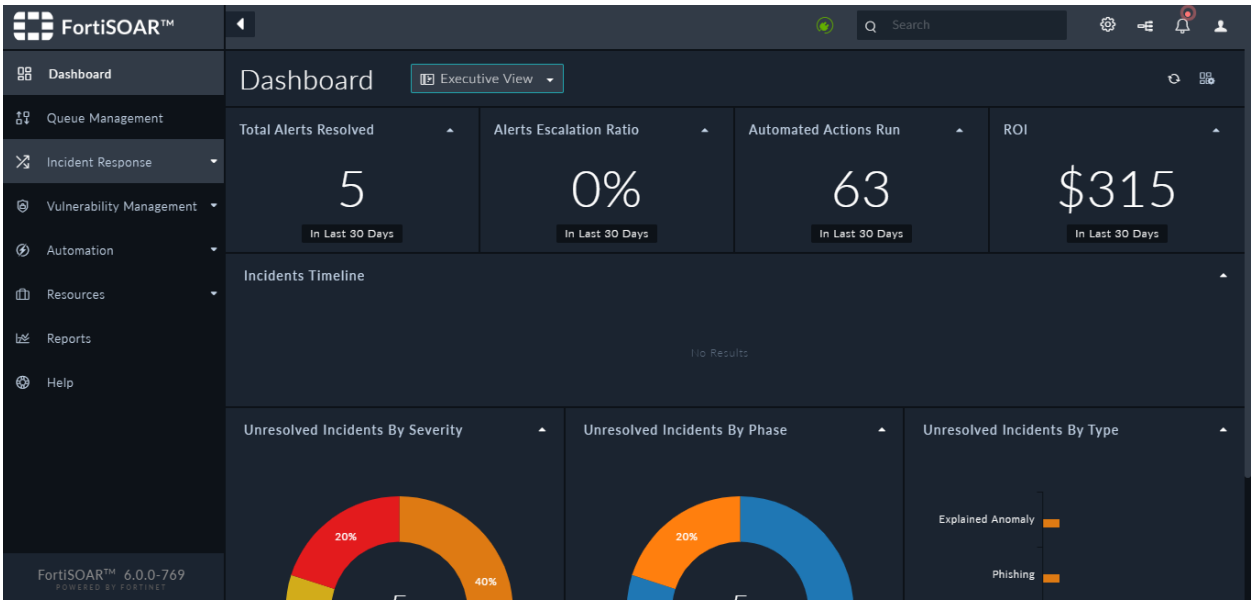


Figure 64. *About FortiSOAR™ link*

Clicking on the **FortiSOAR™ Version Number Build number** link, for example, **FortiSOAR™ 6.0.0-769** 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.

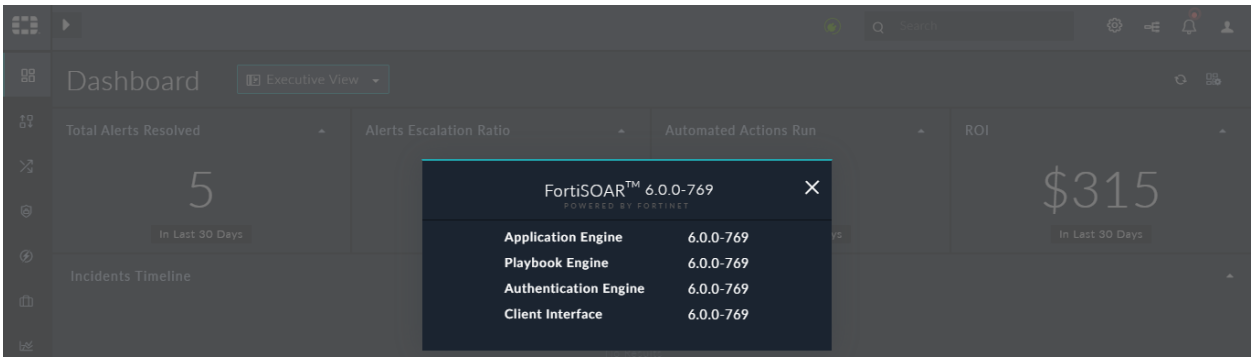


Figure 65. *About FortiSOAR™ dialog*

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.

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	Purpose
`cyops-api/ssl_cyops_api_access.log`	Used for troubleshooting web (nginx) UI or API access issues.
`cyops-api/ssl_cyops_api_error.log`	Used for troubleshooting API errors.
`cyops-api/prod.log`	Used for troubleshooting FortiSOAR™ PHP related issues.
`cyops-auth/das.log`	Used for troubleshooting FortiSOAR™ authentication 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 framework issues.
`cyops-workflow/ssl_cyops_workflow_access.log`	Used for troubleshooting playbook access issues.
`cyops-workflow/ssl_cyops_workflow_error.log`	Used for troubleshooting playbook errors.
`cyops-workflow/uwsgi.log`	Used for troubleshooting FortiSOAR™ playbook and connector issues.
`cyops-integrations/connectors.log`	Used for troubleshooting FortiSOAR™ connector related issues.
`cyops-integrations/integrations.log`	Used for troubleshooting FortiSOAR™ connector

	framework issues.
`cyops-integrations/integrations/imap/listener.log`	Used for troubleshooting the IMAP connector issues.
`cyops-integrations/ssl_cyops_integrations_access.log`	Used for troubleshooting connector access issues.
`cyops-integrations/ssl_cyops_integrations_error.log`	Used for troubleshooting connector errors.
`install` For example, `5.0.0-855.log`.	Used for troubleshooting FortiSOAR™ installation issues. Install logs are named according to the FortiSOAR™ version and build number.
`install/connectors.log`	Used for troubleshooting connector installation issues.
`upgrade_cyops_<version_number>-<timestamp>.log` For example, `upgrade_cyops_5.0.0-2019-05-23-1558604373.log`	Stores upgrade console log and you can use it to troubleshoot FortiSOAR™ upgrade issues.
`install/config-vm-<timestamp>.log` For example, `install/config-vm-27_Nov_2018_18h_14m_34s.log`	Used for troubleshooting FortiSOAR Configuration Wizard issues.

For troubleshooting FortiSOAR™ audit log issues use the `tomcat.log` located at `cyops/tomcat.log`.

For Centos OS level errors, use the `Messages` logs located at `/var/log/messages`.

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 `# systemctl status redis` command.
postgresql-12	Service for all application data stored in postgresql DB. To know the status of this service, use the `# systemctl status postgresql-12` command.
elasticsearch	Service to bring up the elasticsearch service. To know the status of this service, use the `# systemctl status elasticsearch` command.
php-fpm	Service for PHP FastCGI implementation. To know the status of this service, use the `# systemctl status php-fpm` 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 `# systemctl status uwsgi` command.

celeryd	celeryd is used to run the playbooks asynchronously in the FortiSOAR™ playbook execution engine. To know the status of celeryd use the `# systemctl status celeryd` 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 `# systemctl status celerybeatd` command.
cyops-auth	Service used for FortiSOAR™ authentications. To know the status of this services, use the `# systemctl status cyops-auth` command.
cyops-tomcat	Service used for SSO, auditing, and websocket. To know the status of this services, use the `# systemctl status tomcat` 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.
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 `# systemctl status nginx` 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 in the "Administration Guide."

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 view the status of individual FortiSOAR™ services use 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:

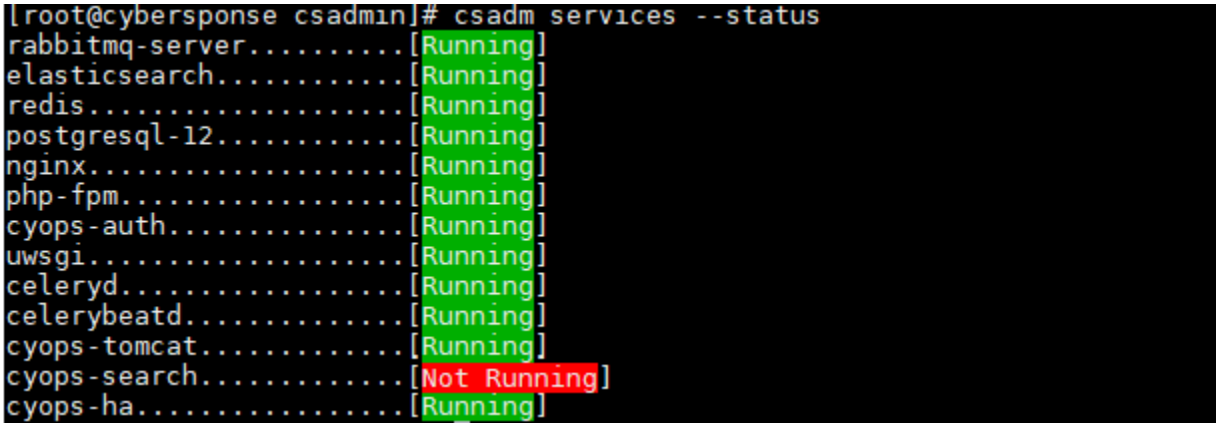


Figure 66. *Status of FortiSOAR™ services*

Additional settings for record similarity and field predictions

FortiSOAR™ 6.0.0 introduces "Record Similarity" i.e., FortiSOAR™ displays records that are similar to the record on which you are working. Version 6.0.0 also introduces "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 ElastiSearch 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
`max_reset_attempts`	Maximum number of times users' can click the **Reset Password** 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 `reset_locktime` parameter. By default, the `max_reset_attempts` is set to 10 times and the `reset_locktime` is set to 12 hours, therefore, if a user clicks the **Reset Password** 11 times without actually resetting their password, then the user will not get a new link to reset their password for 12 hours.	10 times
`reset_locktime`	Number of hours that users' will not get a new link to reset their password if they exceed the value set in the	12 hours

	`max_reset_attempts` parameter.	
`max_failed`	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 `lock_minutes` parameter. By default, the `max_failed` is set to 5 times and the `lock_minutes` 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
`lock_minutes`	Number of minutes that users' account gets locked if they exceed the value set in the `max_failed` 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://<CyOPs™ 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://<CyOPs™ 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://<CyOPs™ 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://<CyOPs™ 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"}
```