BEGINNERS TUTORIAL TO FORTISOAR™ FOR ADMINISTRATORS 6.0.0

VERSION 1.0

FEBRUARY 2020

Copyright

Trademark

Table of Contents

Introduction 4

Authentication 4

Default Roles 6

Security Administrator Role 6

Teams, Roles, and Users 7

Add a new role 7

Add a new user and assign the role to a user 8

Create your first record 10

Next Steps 11

Introduction

Welcome to Fortinet Orchestration Platform (FortiSOAR™). FortiSOAR™ allows you to manage the entire lifecycle of a threat or breach within your organization.

This Beginners Tutorial to FortiSOAR™ is designed to help you get acquainted with the application and start exploring some of the key functionality that FortiSOAR™ offers. For more detailed information on FortiSOAR™ and the full range of features and functionality, refer to the “Administration” and “User” guides.

Authentication

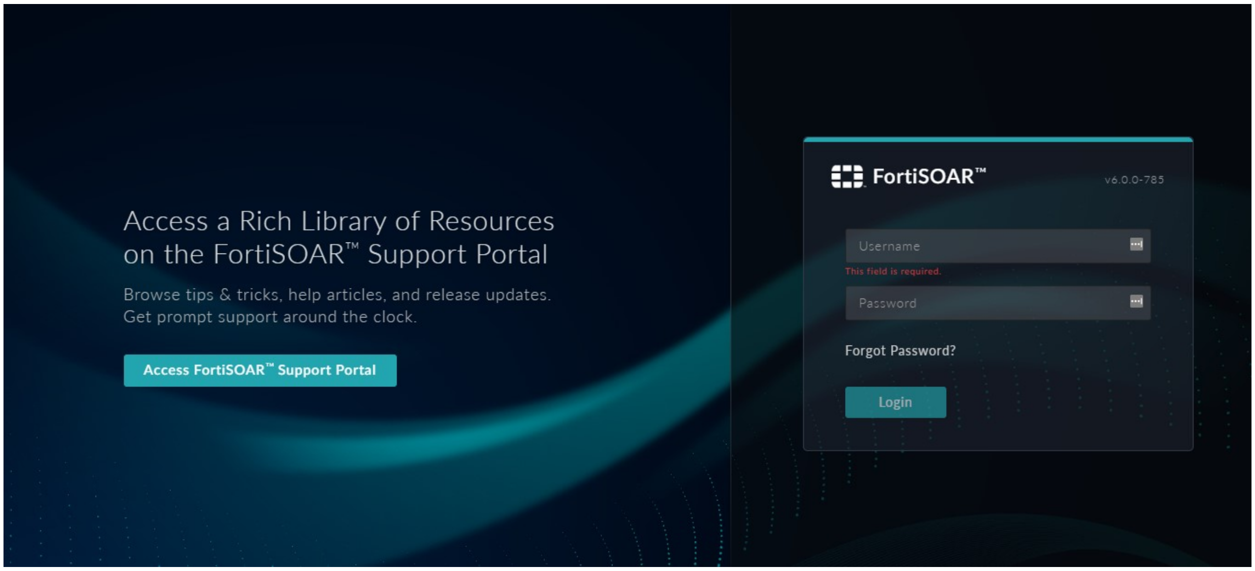
A FortiSOAR™ Customer Success Representative will create an initial Security Administration credential and provide a valid username and password to access the FortiSOAR™ application. Thus, each FortiSOAR™ instance will have at least one role (Security Administrator - csadmin) created by default after installation.

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.

If you are accessing the FortiSOAR™ login screen for the first time, you will be presented with the Fortinet End-User License Agreement (EULA). You must accept the EULA before you can log onto FortiSOAR™.

Upon accessing the FortiSOAR™ login screen, enter your login credentials.



Access a Rich Library of Resources on the FortiSOAR™ Support Portal

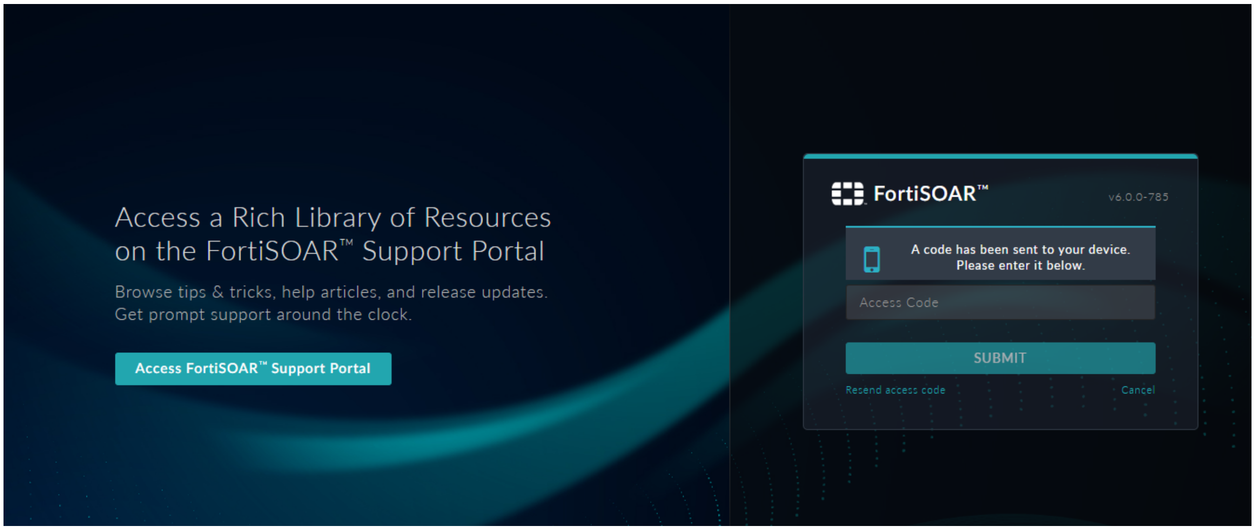
Browse tips & tricks, help articles, and release updates. Get prompt support around the clock.

This field is required.

Figure 1. *FortiSOAR™ Login Screen*

Once valid login credentials have been entered, you might be redirected to a second screen requesting a 2-Factor Authentication (2FA) code.

The authentication code consists of a six-digit number sent to the mobile phone number associated with the account using SMS or a five-digit number sent using a voice message. This authentication works in over 200 countries and territories and in 87 different languages. Users can determine the method by which the authentication code is sent to your mobile phone using their user profile.



Access a Rich Library of Resources on the FortiSOAR™ Support Portal

Browse tips & tricks, help articles, and release updates. Get prompt support around the clock.

A code has been sent to your device. Please enter it below.

Figure 2. *FortiSOAR™ Login Screen with 2FA*

The initial login to the application opens your Dashboard. Your Dashboard is based on your role.

Note: The dashboard displays "No Results" for modules, such as Incidents and Alert and there will be no module icons in the left navigation bar. This is because the default Security

Administrator's role does not provide module-level access to those entities. The Security Administrator will need to create a role that provides access to the modules and then assign that role to either themselves or to a new user.

Once you log on to FortiSOAR™, you must change your password by clicking the User Profile icon (👤) and then selecting the **Change Password** option.

Default Roles

In FortiSOAR™, modules are applied to roles. For example, the `Security` module is applied to the Security Administrator role. Therefore, you can assign the role of Security Administrator to any other user in the system.

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:

- An `Application Administrator` role has full permissions to modify or customize FortiSOAR™ features and configure your FortiSOAR™ system.
- A `Full App Permissions` role is essentially a *root* user and has full permissions across FortiSOAR™. Use this role with care.
- A `Playbook Administrator` role has full permissions to the Playbook Engine and all the major modules in FortiSOAR™ and also has **Read** access to the Security module.
- A `Security Administrator` (csadmin) role has the permissions to assign privileges to other roles and teams.
- A `T1 Analyst` role has access to major modules in FortiSOAR™ and is responsible for alert triaging and escalating potentially malicious alerts to indicators for review by T2 analysts.
- A `T1 Analyst` role has access to major modules in FortiSOAR™ and is responsible incident investigation and other remediation and containment related tasks.

Refer to the "Administration Guide" for a detailed description of the default roles.

Security Administrator Role

If you are a Security Administrator, the default Security Administrator role allows access to create the following:

- Teams - establish the ownership/viewership of data within FortiSOAR™
- Roles - establish the permissions of a user within FortiSOAR™
- Users - establish individual accounts for members of your organization to access FortiSOAR™

Note: From 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-tenant systems

Teams, Roles, and Users

Click the **Settings** (⚙) icon in the upper right corner of the screen and click **Team Hierarchy** in the `Security Management` section to open the `Team Hierarchy` page. The Team Hierarchy Editor is an interface that allows you to define the data ownership structure within your organization. By default, your FortiSOAR™ installation might have several default teams. You can choose to keep these Teams or to remove them.

Warning: Deleting a team can result in orphaned data. FortiSOAR™ recommends you rename teams or remove members but leave the team itself intact to prevent any problems accessing data that might be owned by a team.

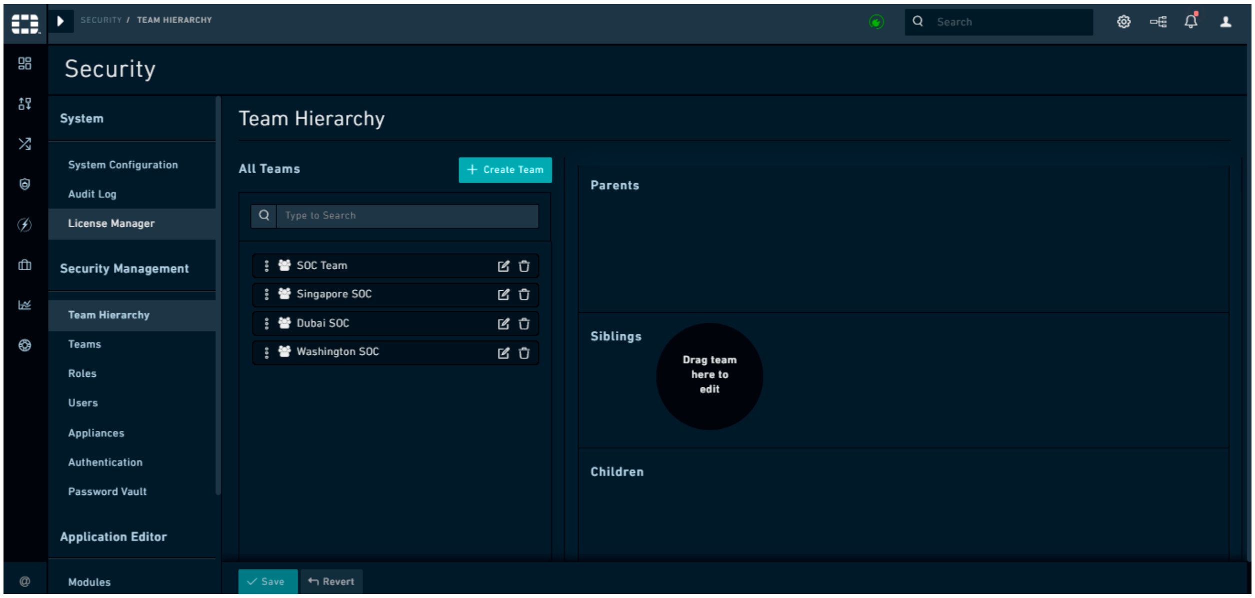
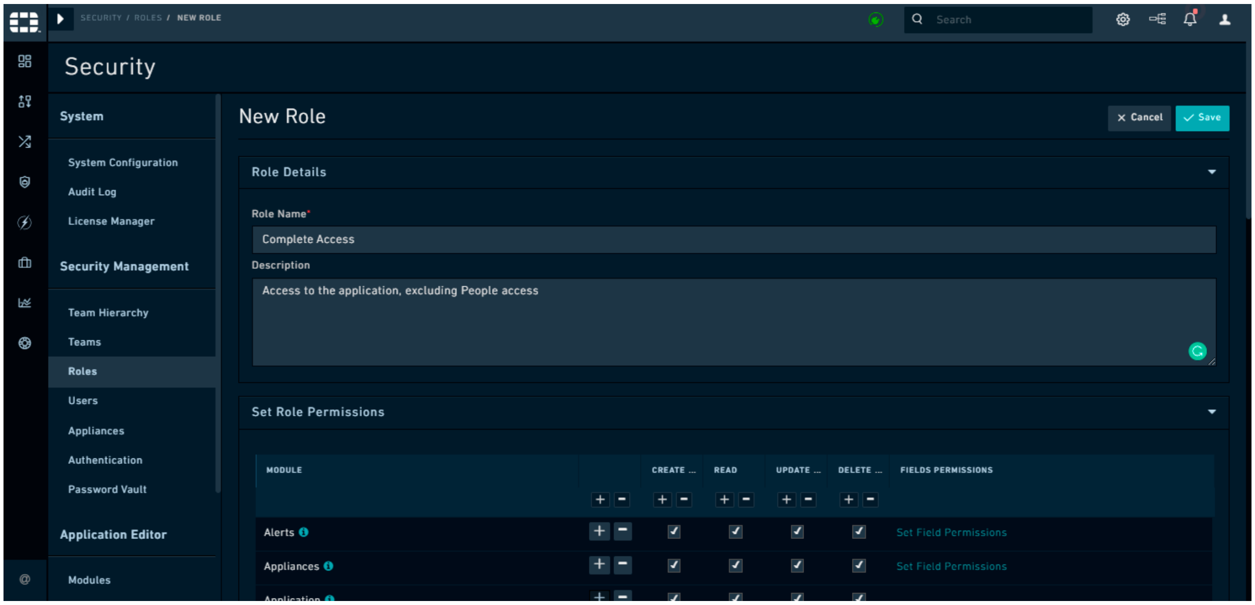


Figure 3. *Security Management Administration Page*

Add a new role

To open the `Role Editor`, click **Roles** in the `Security Management` section. The Role Editor lists the roles that exist within the organization. You can modify the existing roles or add new ones. Refer to the Default Roles section for information on default roles.

To add a new role, click **Add Role** to display the **New Role** form.



Role Name*

Complete Access

Description

Access to the application, excluding People access

MODULE		CREATE ...	READ	UPDATE ...	DELETE ...	FIELDS PERMISSIONS
	+ −	+ −	+ −	+ −	+ −	
Alerts	+ −	☑	☑	☑	☑	Set Field Permissions
Appliances	+ −	☑	☑	☑	☑	Set Field Permissions
Application	+ −	☑	☑	☑	☑	

Figure 4. *Quick Admin - New Role*

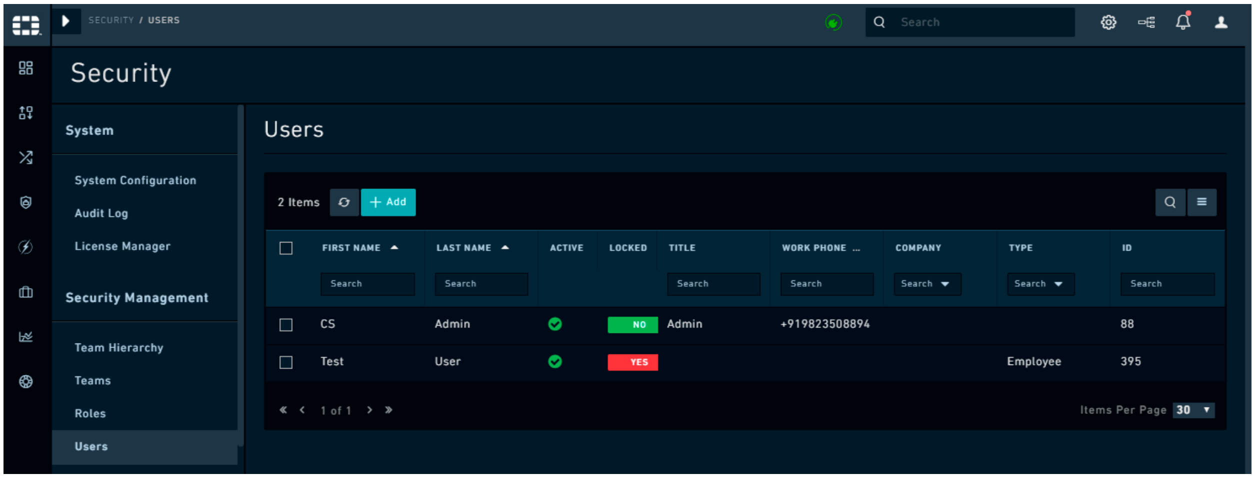
In the `Set Role Permissions` grid, the **Module** column displays the name of the various modules to which you can assign permissions. Each of the `Create`, `Read`, `Update`, and `Delete` columns have checkboxes that allow you to assign specific permissions for each module. The Playbooks module has an additional permission named `Execute`, which should be assigned to users who should have the right to run playbooks and actions.

To create a role that has full access to the application and all permissions, click on the **+** button in the column header between `Module` and `Create`. This selects all permissions and all modules. Click **Save** to create the newly-created `Complete Access` role. You can either assign the role to yourself, the Security Administrator, or create a user to whom you assign this role.

Warning: A Role with ALL permissions granted can affect security settings for current users, roles, and teams. Do not grant that role access to someone who should not be making security decisions for your organization.

Add a new user and assign the role to a user

Click the **Settings** (⚙) icon and click **Users** in the `Security Management` section to open the `Users` page. The `Users` page displays a list of users (active and inactive) for the organization. Use the `Users` page to add additional users and assign roles and teams to users.



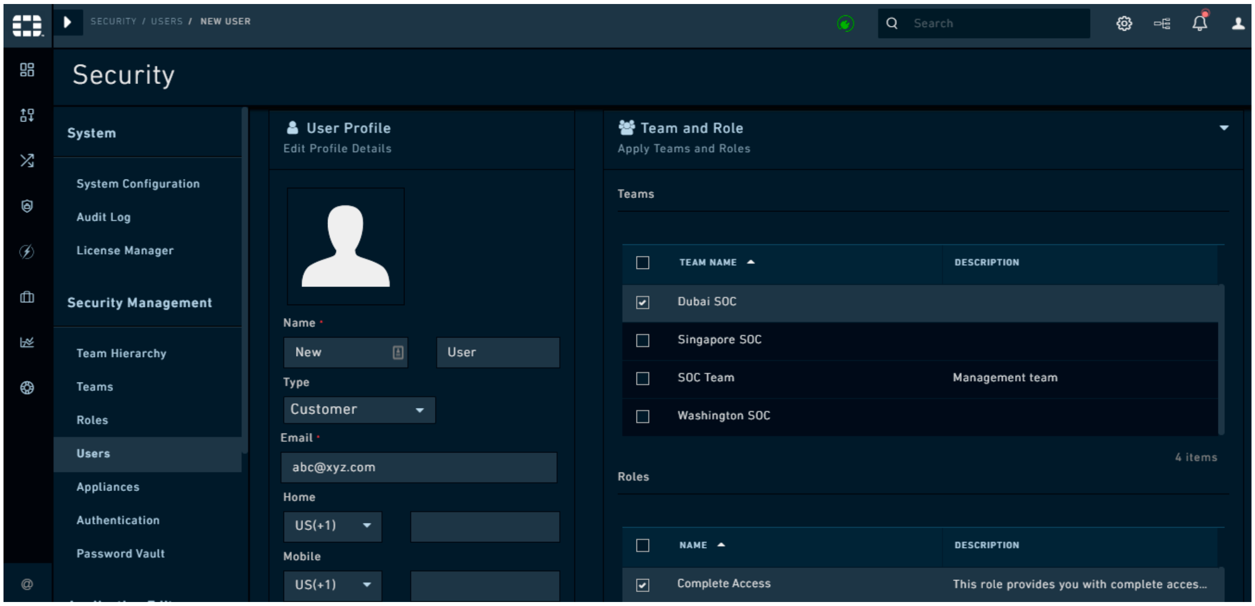
☐	FIRST NAME	LAST NAME	ACTIVE	LOCKED	TITLE	WORK PHONE ...	COMPANY	TYPE	ID
☐	CS	Admin	✓	NO	Admin	+919823508894			88
☐	Test	User	✓	YES				Employee	395

Figure 5. *User management grid*

To add a new user, click **Add Person** to display the **New User** form. Enter the user details on the `New User` page and click **Save** to save the new user profile. Refer to the *Configuring User and Appliance Profiles* section in the "Administration" guide for more information.

Note: The **Username** field is mandatory, case sensitive and cannot be changed once it is set.

To assign the newly created `Complete Access` role to a user, click on the username. On the `Edit User` page, in the `Roles` section, click the checkbox for the newly created role and then click **Save**. The selected user now has full access to the FortiSOAR™ application, except for the `People` module.



Name: New User
Type: Customer
Email: abc@xyz.com
Home: US(+1)
Mobile: US(+1)

Teams

☐	TEAM NAME	DESCRIPTION
☑	Dubai SOC	
☐	Singapore SOC	
☐	SOC Team	Management team
☐	Washington SOC	

4 items

Roles

☐	NAME	DESCRIPTION
☑	Complete Access	This role provides you with complete acces...

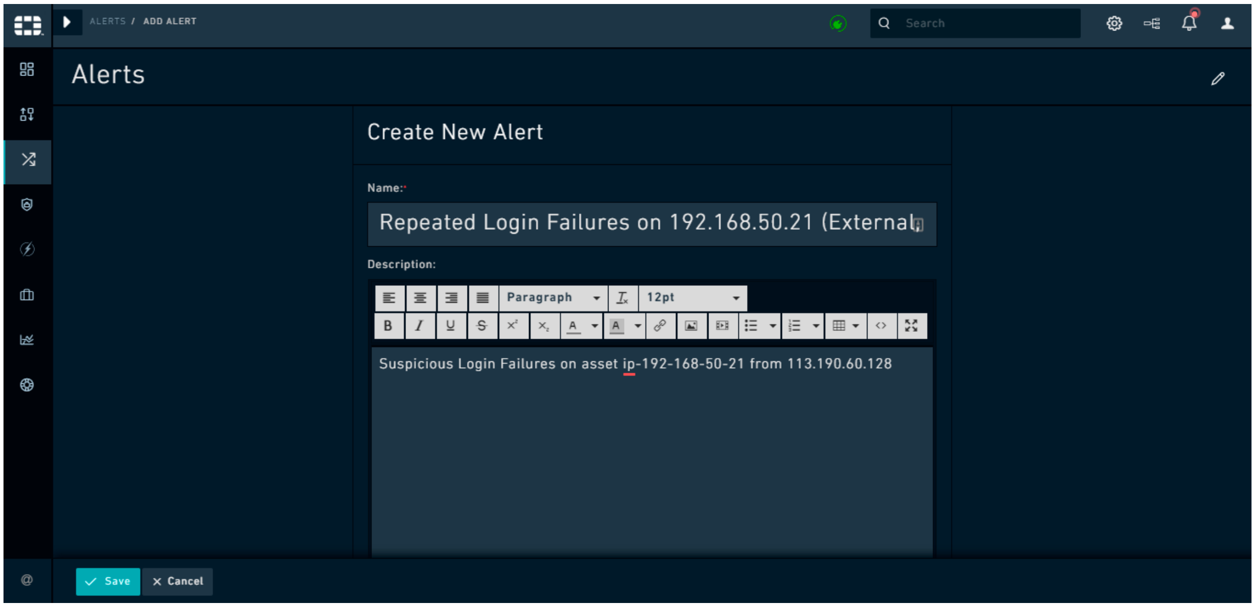
Figure 6. *Editing a User Profile*

Note: Users might already have permissions for full application access. Users are not affected if they have more than one role with the same permissions. Permissions always aggregate across your roles when determining your authorization level. Refer to the *Security Management* chapter in the "Administration Guide" for more information regarding security management.

Create your first record

Now that you have created a user with a role that gives you full access to FortiSOAR™, you can test your access and FortiSOAR™ by creating your first record. We recommend you try creating an Alert.

Click **Incident Response > Alerts** in the left menu and click the **Add** button in the `Alerts` module, to open the **Create New Alert** dialog. Enter data for the new record and click **Save** to save the record.

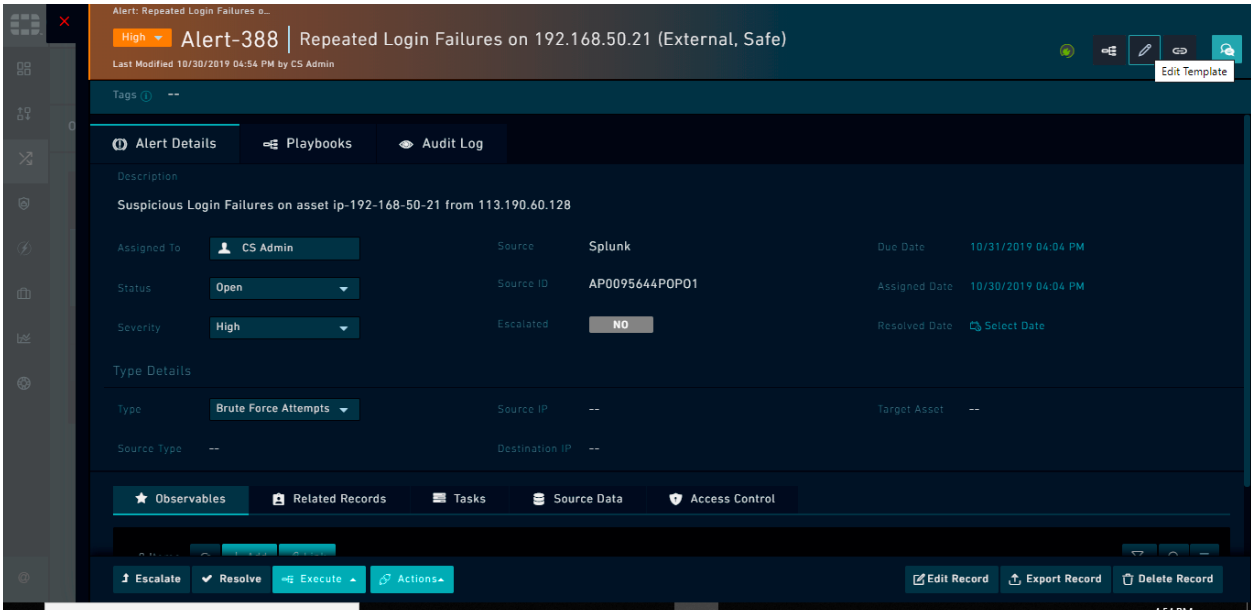


Name:* Repeated Login Failures on 192.168.50.21 (External

Description: Suspicious Login Failures on asset ip-192-168-50-21 from 113.190.60.128

Figure 7. *Create New Alert Dialog*

The following image displays an example of a completed record in the default Alert Template. You can modify this template by clicking the **Edit Template** icon on the top right of the page.



Alert: Repeated Login Failures o...

High Alert-388 | Repeated Login Failures on 192.168.50.21 (External, Safe)

Last Modified 10/30/2019 04:54 PM by CS Admin

Tags --

Description

Suspicious Login Failures on asset ip-192-168-50-21 from 113.190.60.128

Assigned To	CS Admin	Source	Splunk	Due Date	10/31/2019 04:04 PM
Status	Open	Source ID	AP0095644POP01	Assigned Date	10/30/2019 04:04 PM
Severity	High	Escalated	NO	Resolved Date	Select Date

Type Details

Type	Brute Force Attempts	Source IP	--	Target Asset	--
Source Type	--	Destination IP	--		

Figure 8. *Newly created Alert record*

Note: You, or users, who are assigned the role of Application Administrator, can modify the fields of any record in the application using the Module Editor and the Picklist Editor. Refer to the *Application Editor* chapter in the "Administration Guide" for more information.

Next Steps

Now that you have an introduction to the system, we recommend you review the "Administration Guide" to learn more about how to further configure your system.

If you have any questions, please do not hesitate to reach out to your FortiSOAR™ Customer Success representative for further assistance.