ANLYZ®

SOAR - SPORACT

ADMIN GUIDE

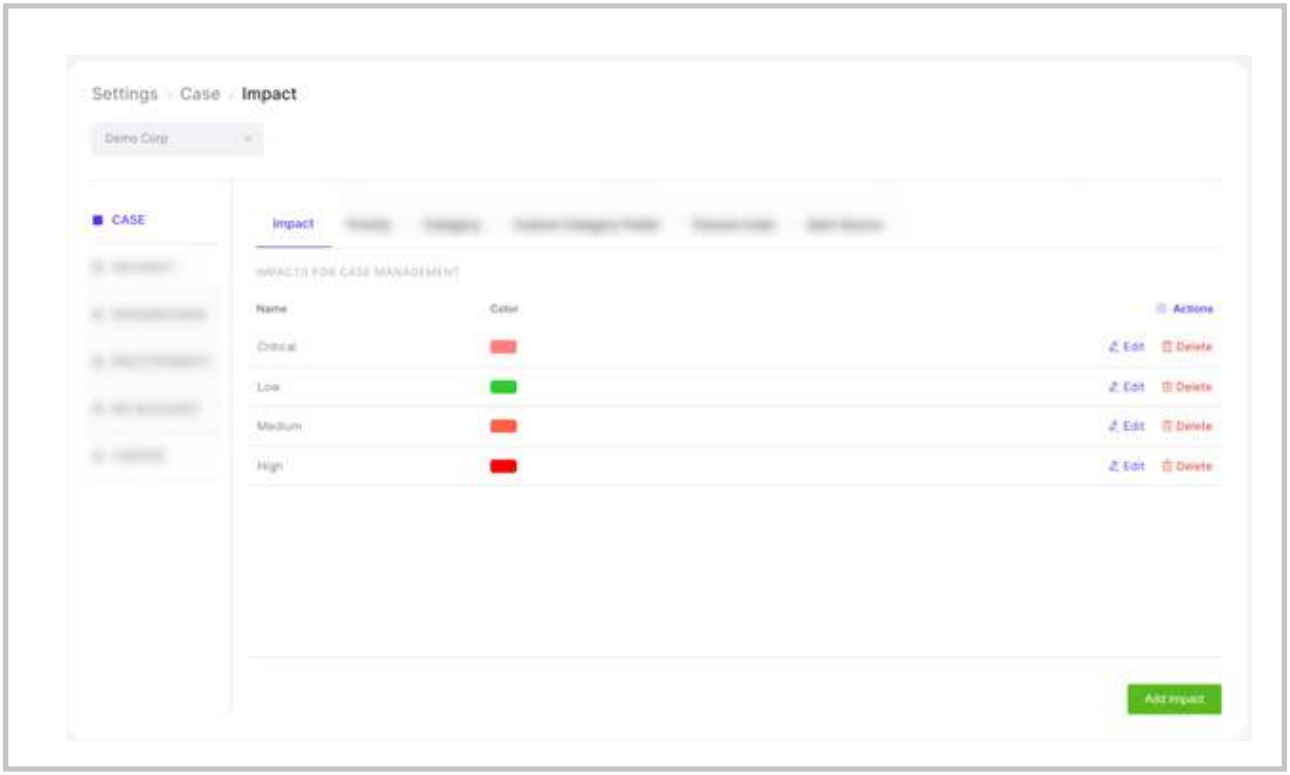
CONTENTS

Settings

Case

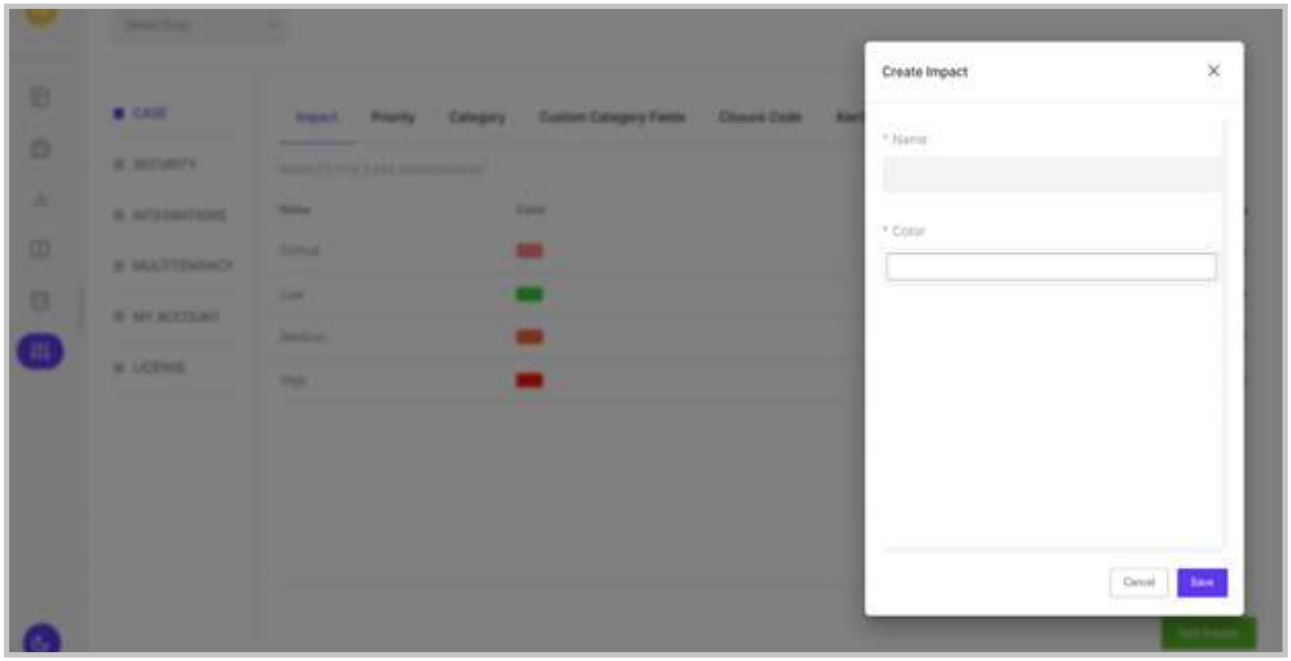
Impact

An impact is the magnitude of harm that can be expected to result from the consequences of an incident and is used to enrich a case.



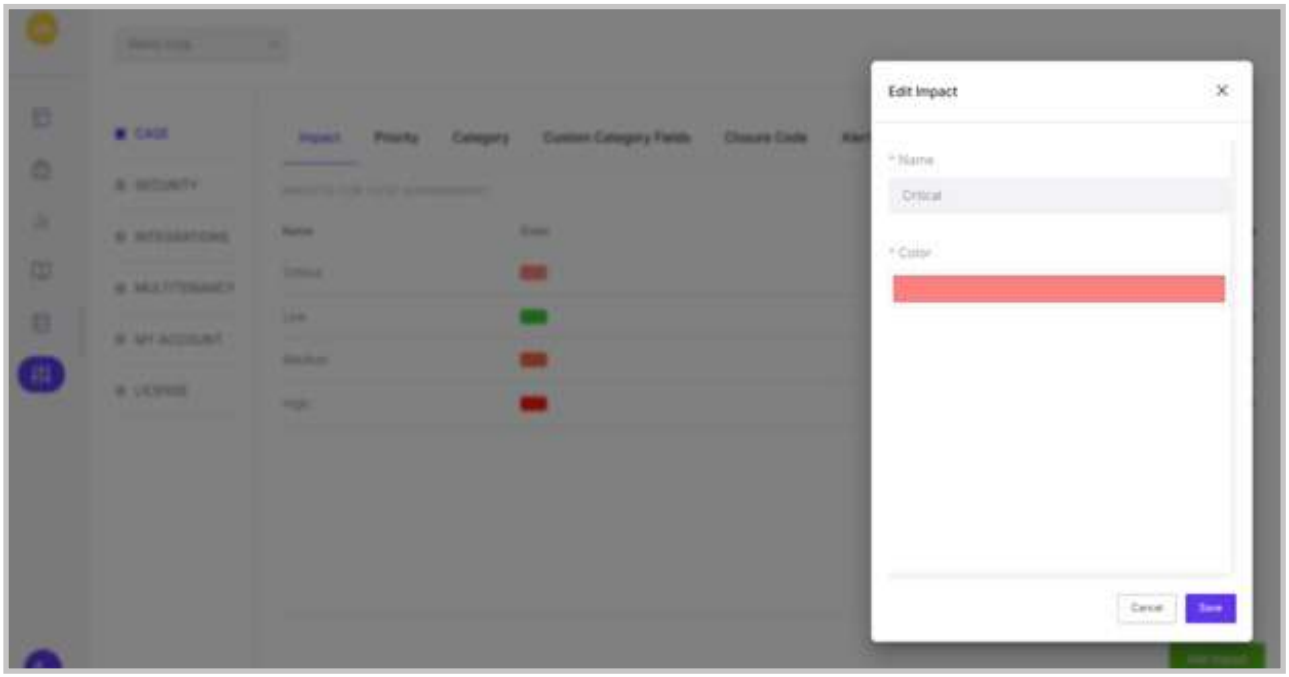
Add an impact

Impacts can be added as and required by the user. A specific colour can be assigned to the impact as well.



Edit an impact

A user can edit an existing impact as depicted in the image below.



Delete an impact

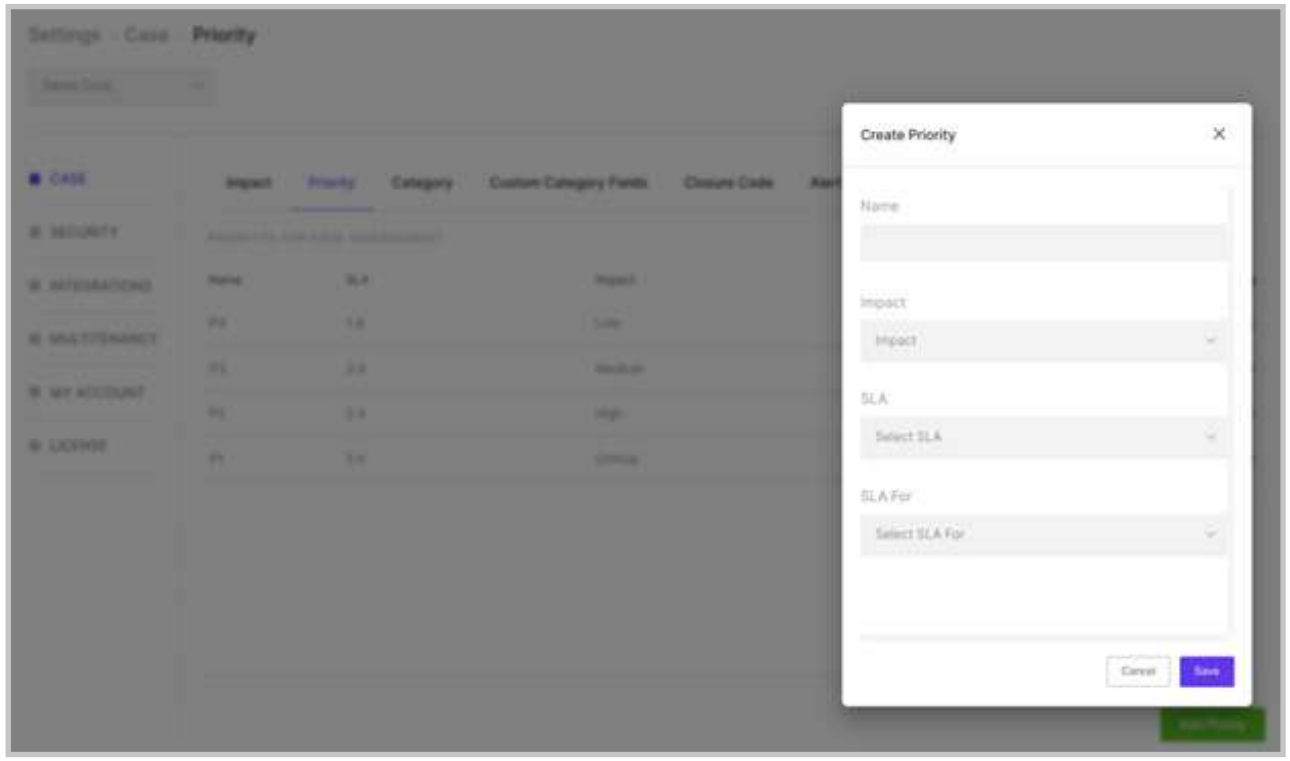
An impact can be deleted as depicted below.

Priority

Priority helps the user in identifying cases which have to be taken care of first. A case can be allotted various priorities, based on which a user can work on it. A case with the highest priority will be considered first.

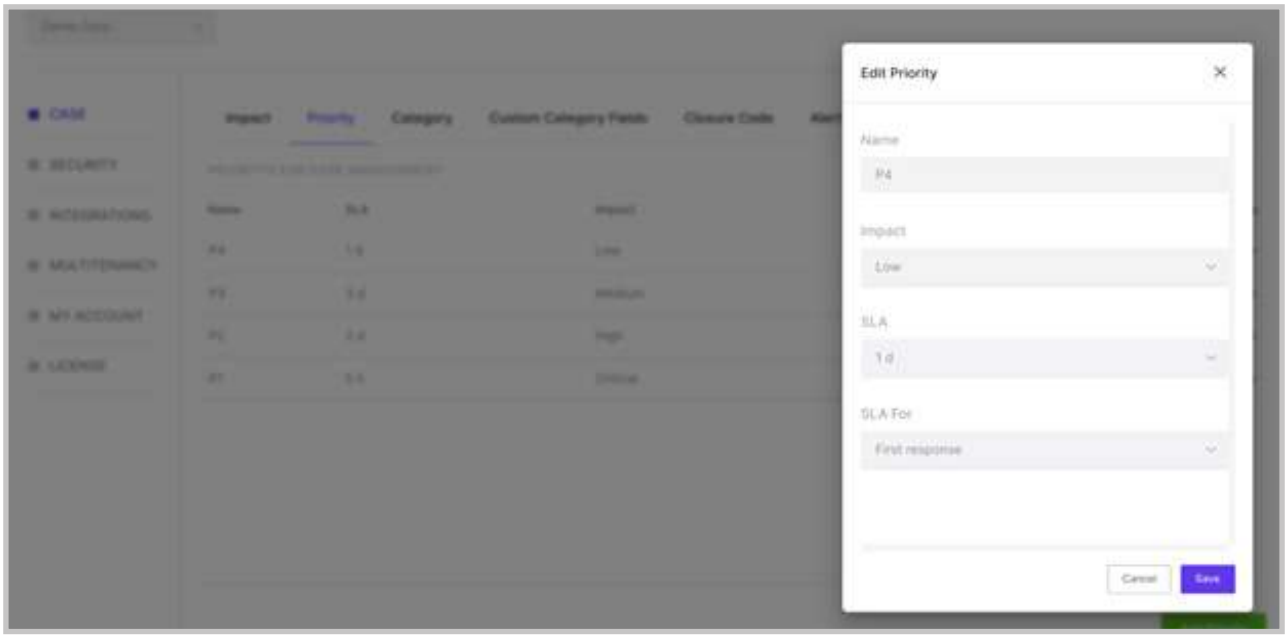
Add a priority

A user can create a priority as depicted below. The priorities are assigned based on the impacts described.



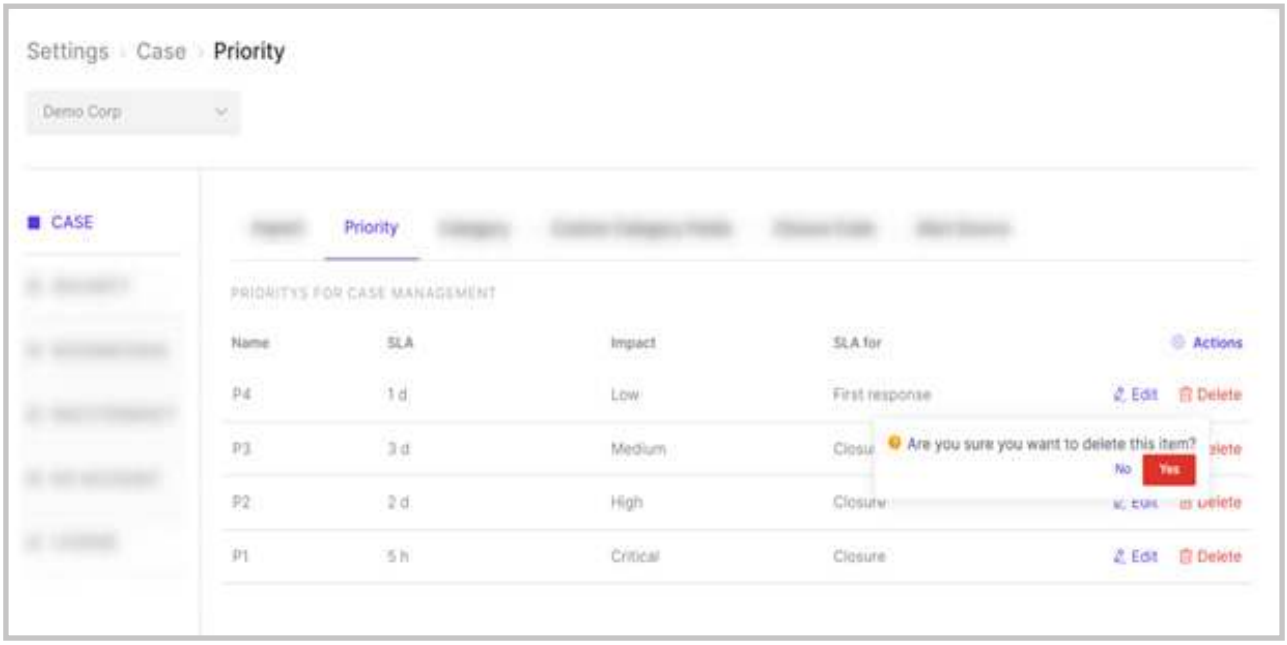
Edit a priority

A priority can be edited as shown below in the image.



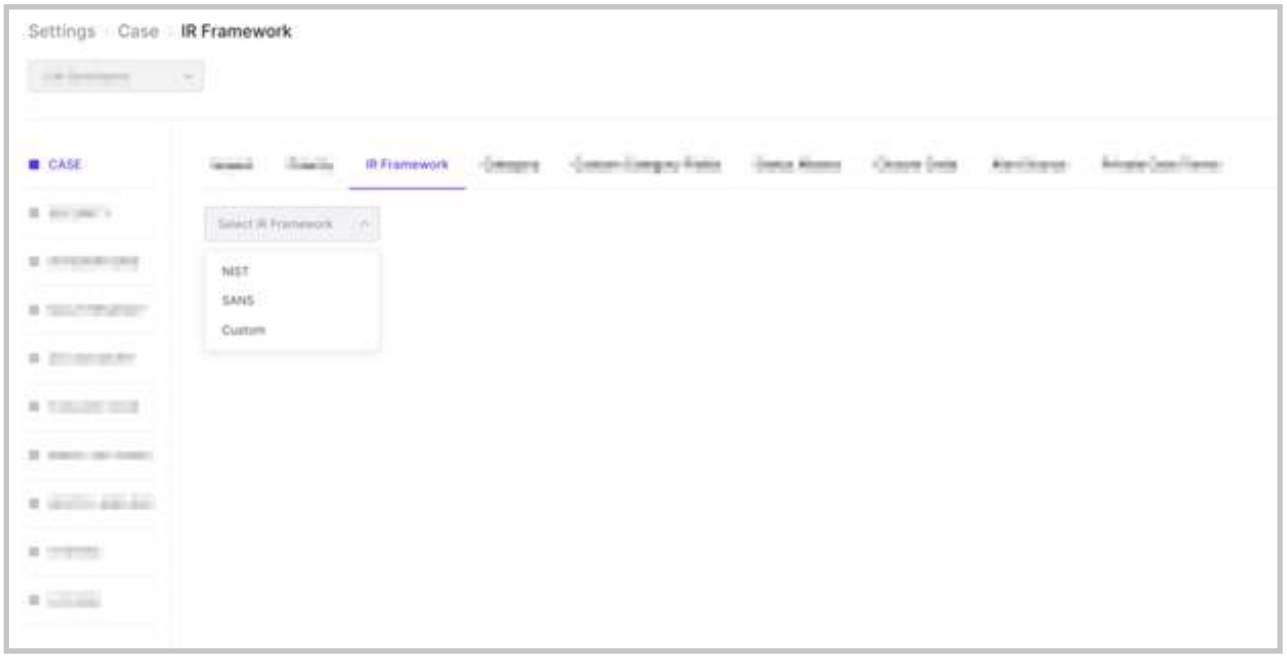
Delete a priority

The user can delete a priority as depicted in the image below.



IR Framework

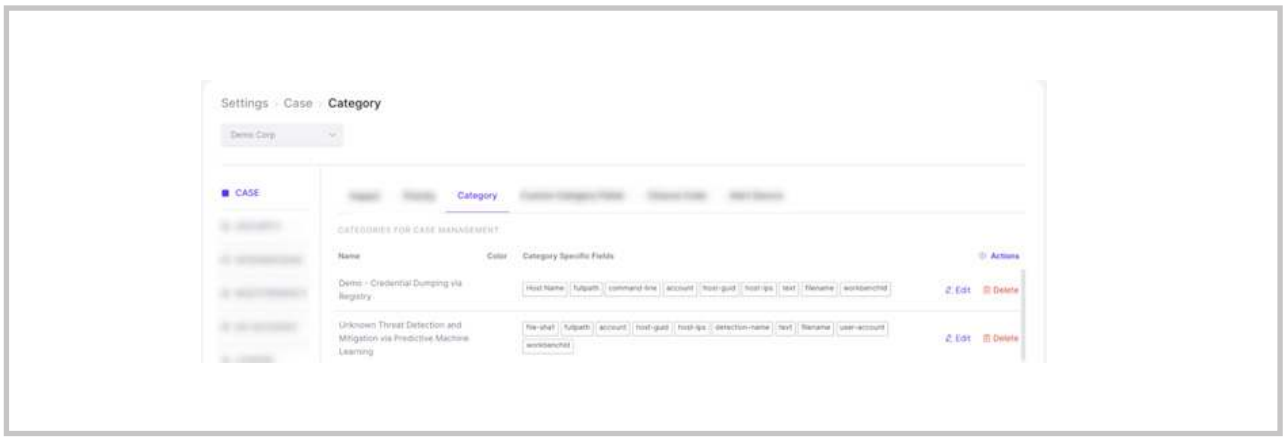
The IR or Incident Response framework consists of steps to methodically respond to any cybersecurity threat or incident. The industry has two main standards for the framework: NIST and SANS. Sporact provides the option to select a framework based on the requirement of the organization. A customer has the option to customize it as well.



The user can select NIST, SANS or Custom from the list of options. If Custom is selected, the user can add the customized phases. Once a framework is selected and saved, it's permanent and cannot be changed.

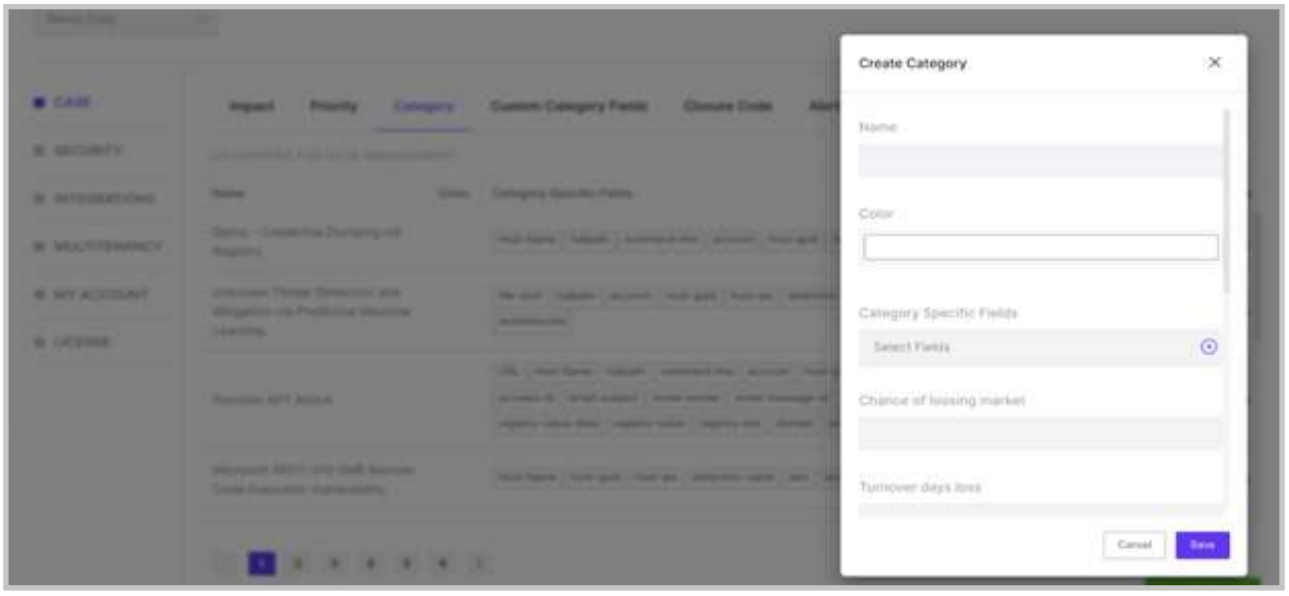
Category

Categories help the user to classify cases based on the type of incidents and attacks described in the specific case. For example, a case that deals with a system affected by a corrupted file can be categorized as Malware. Each and every category can be assigned a colour and custom fields to have a detailed description.



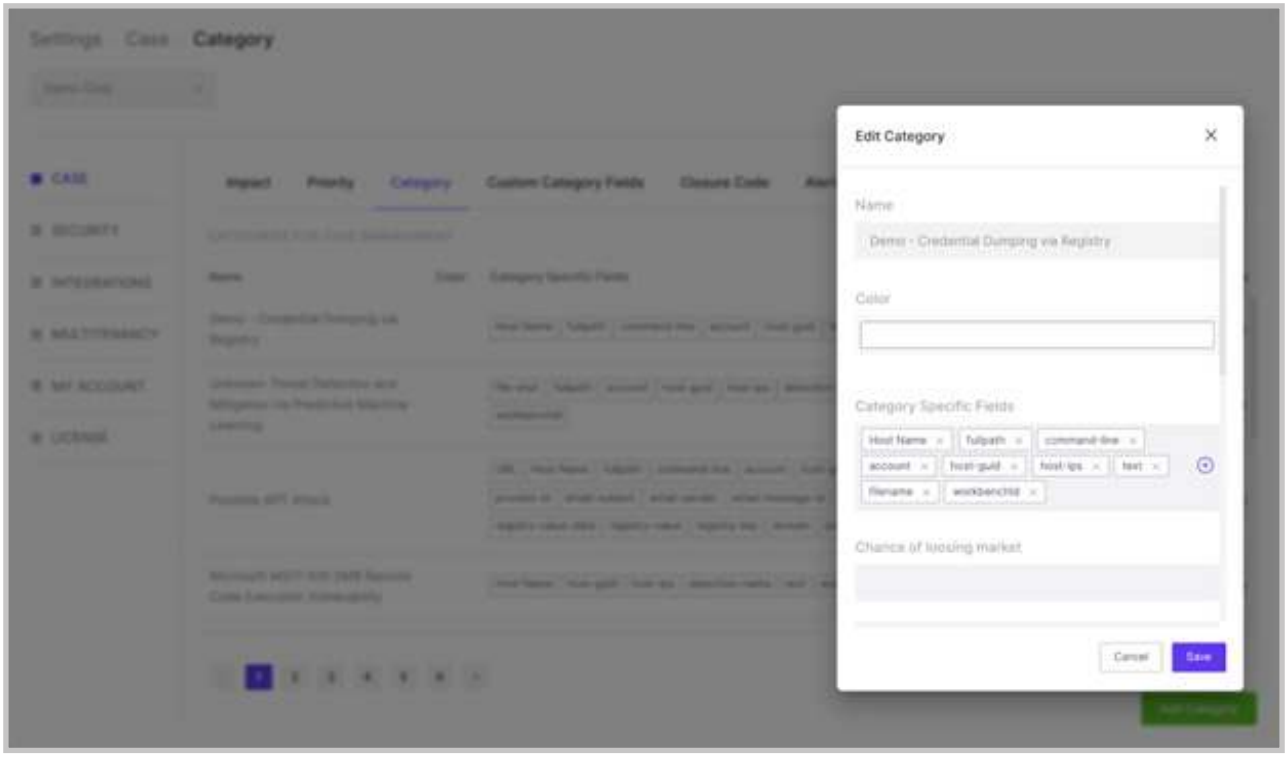
Add a category

Sporact provides the option to create a category when deemed necessary by the user. The user can select the 'add category' option to create a new category.



Edit a category

A category can be edited if any changes are to be made by clicking on the ‘edit’ option.

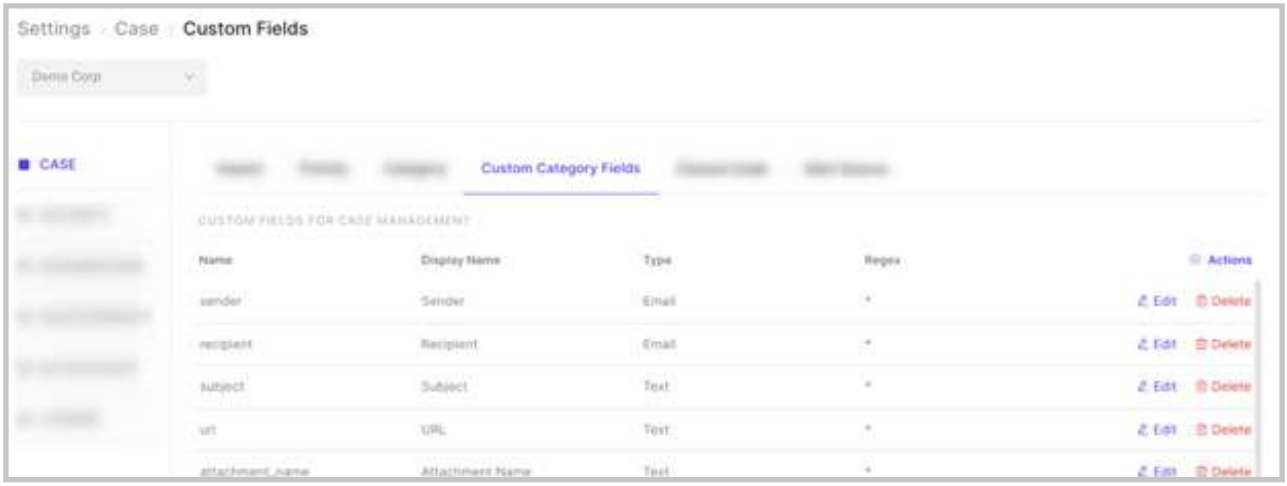


Delete a category

A category can be deleted by the user as shown below.

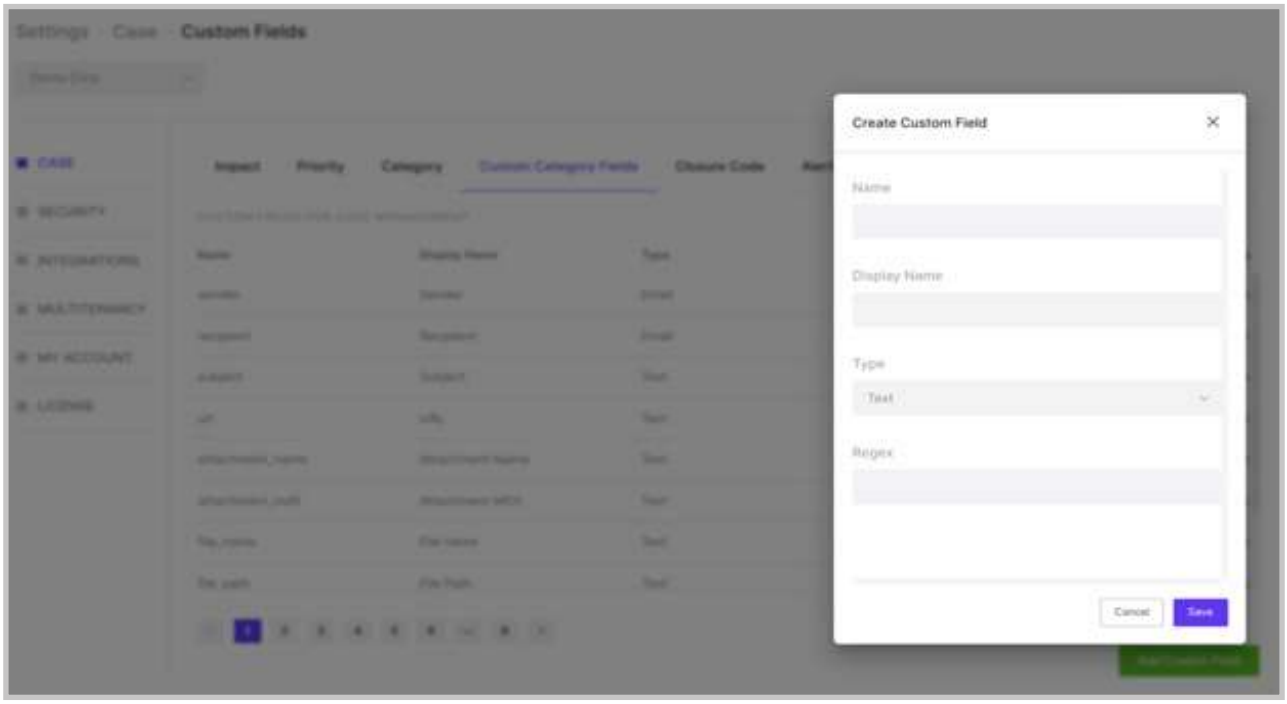
Custom Category Fields

A custom category field allows the user to customize fields pertaining to categories, to provide additional details about the incident described in the case.



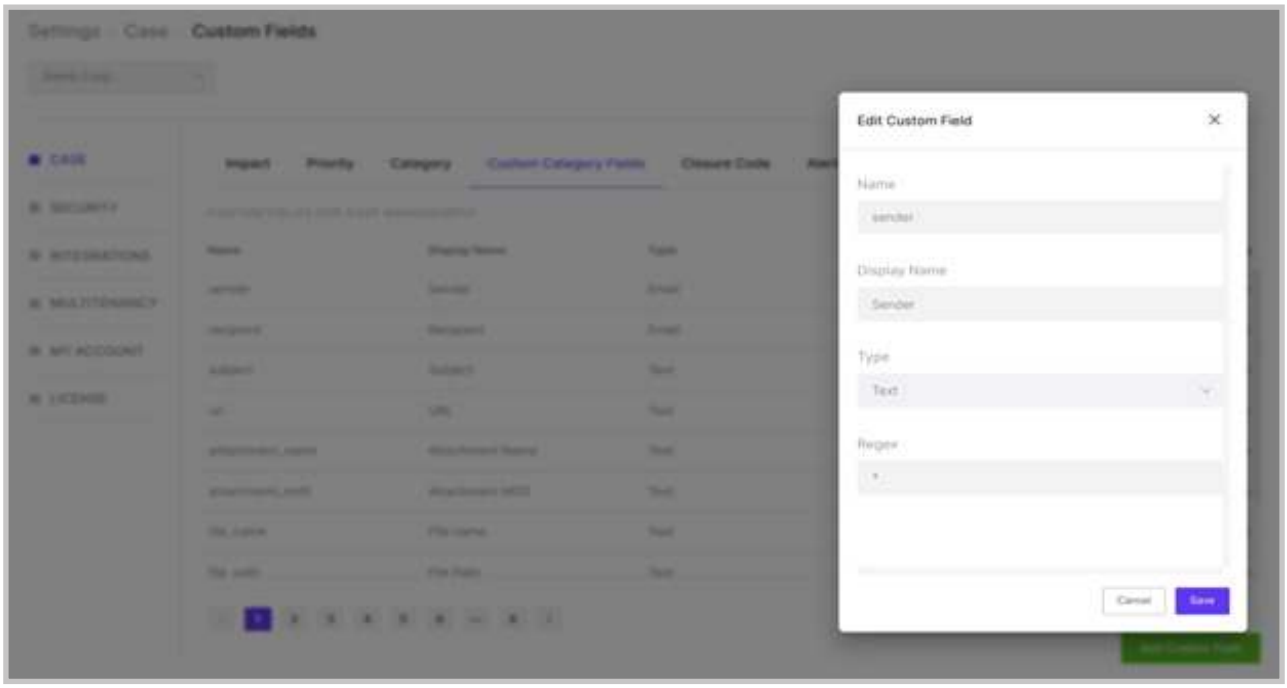
Add a custom field

The user can create additional custom fields as shown below.



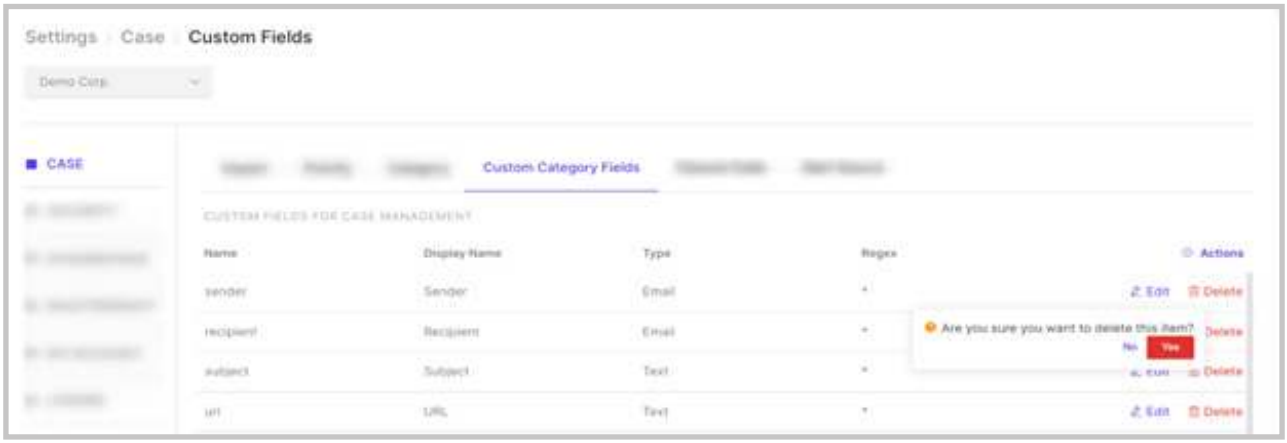
Edit a custom field

As shown in the image below, a custom field can be edited by the user.



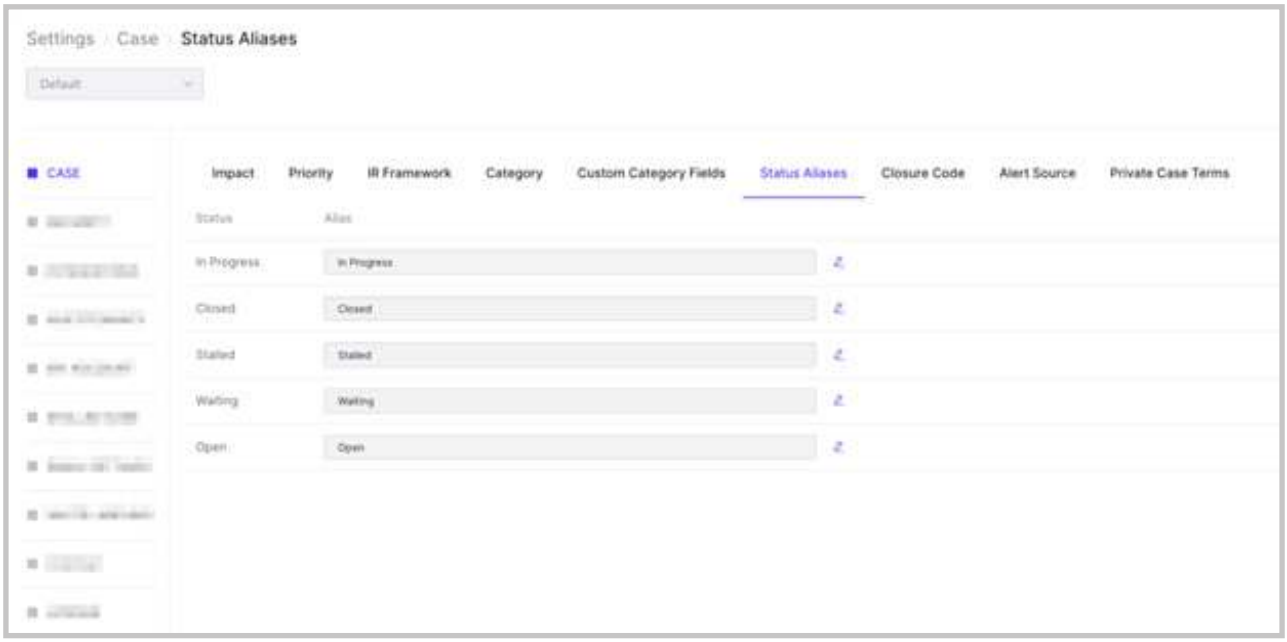
Delete a custom field

A user can delete a custom field as well.



Status Aliases

The status of the case lets the user know in what state the case is currently. Sporact has the default status as open, in progress, waiting, stalled and closed. Sporact provides the option to customize these statuses.



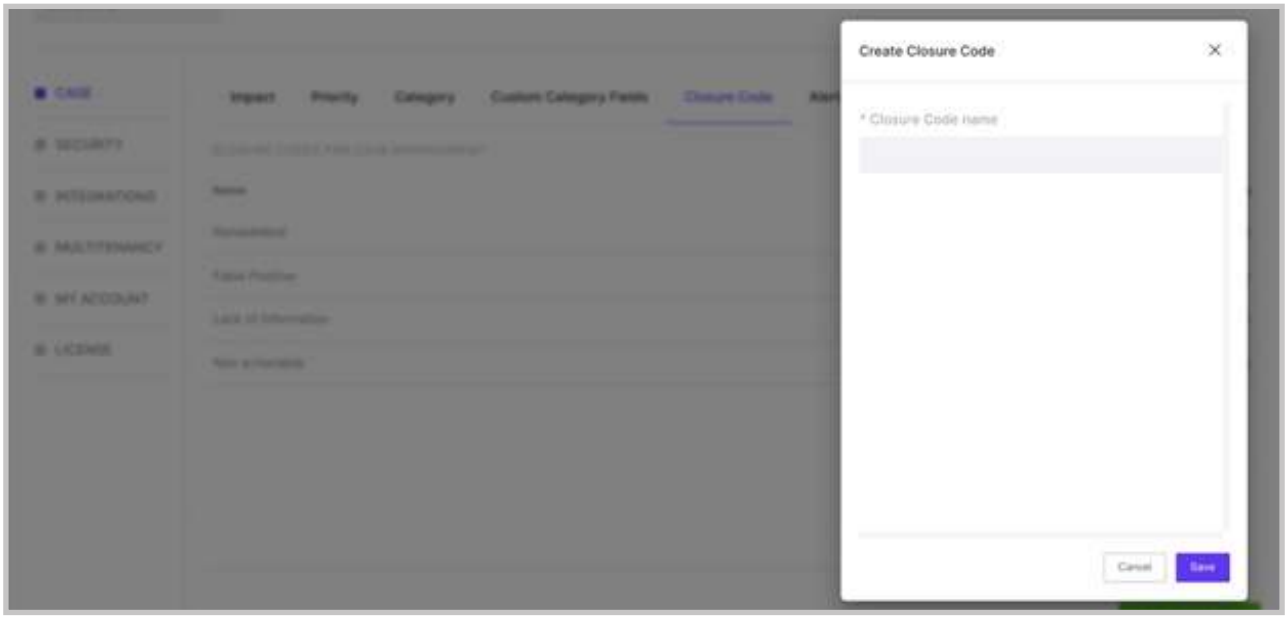
The user can click on the edit icon to customize the status. Once done, the user can click on the save icon the save the changes.

Closure Code

When a case has been analyzed and is ready to be closed, an appropriate closure code is used to describe how the case has been closed. Remediated indicates that a proper solution has been used to prevent any damage from the incident, false-positive indicates that an incident that was thought to be threatening isn't one and is safe, and so on.

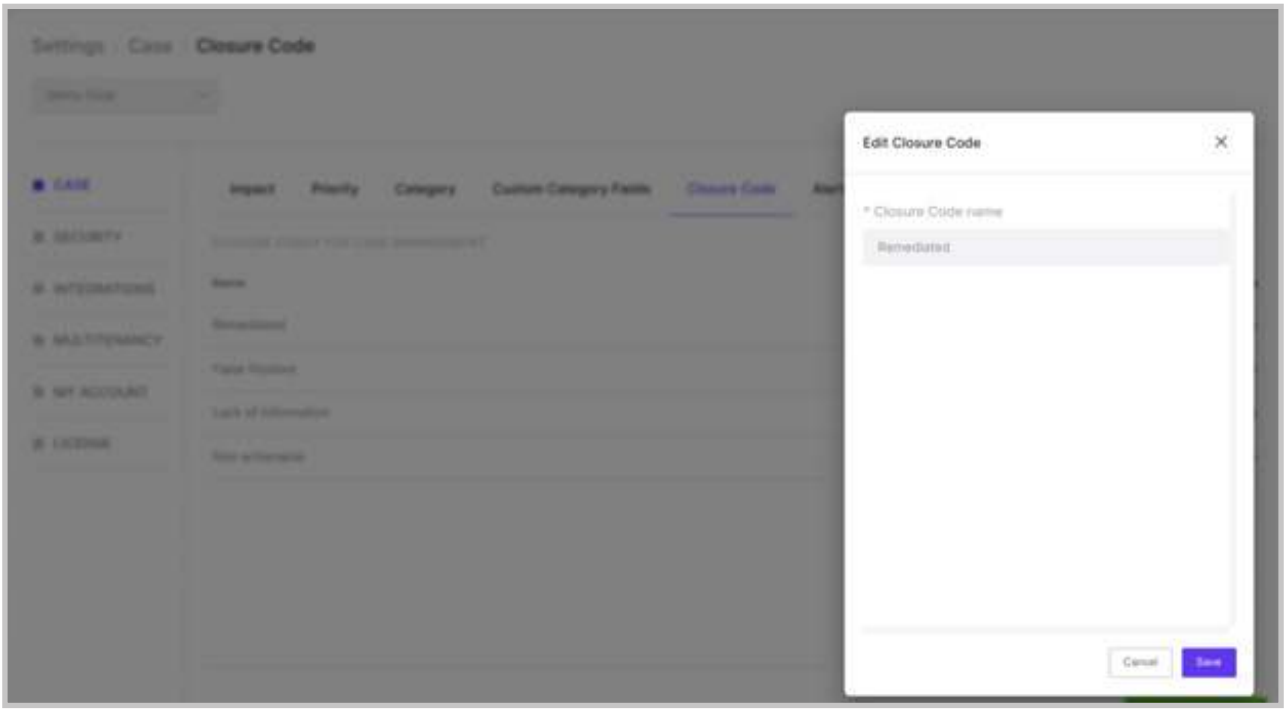
Add closure code

A user has the option to create a closure code as and when required which is shown below.



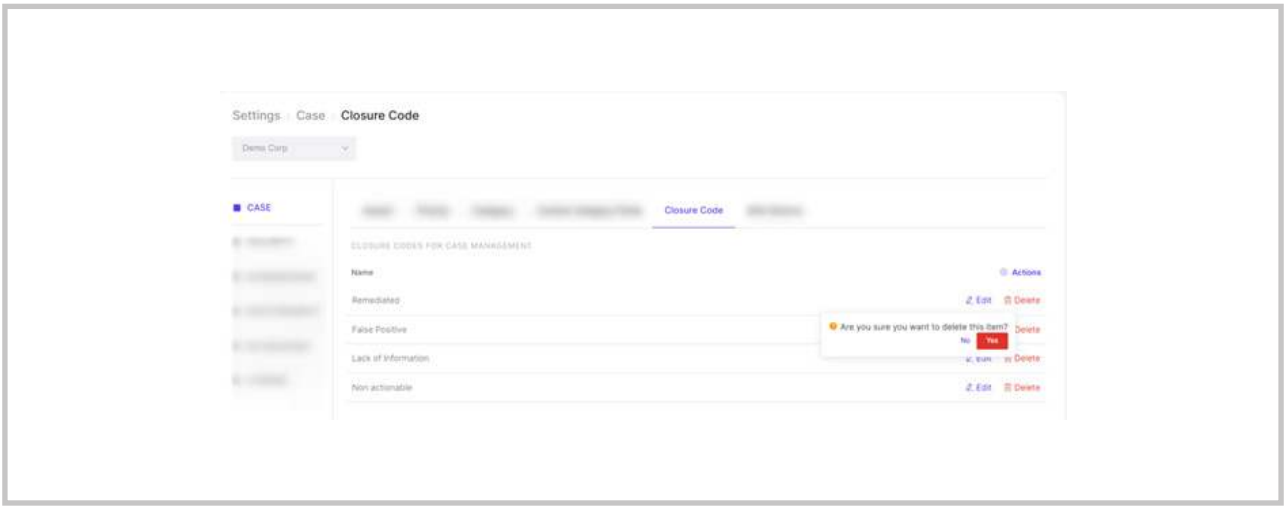
Edit a closure code

Closure codes can be edited by the user as shown below.



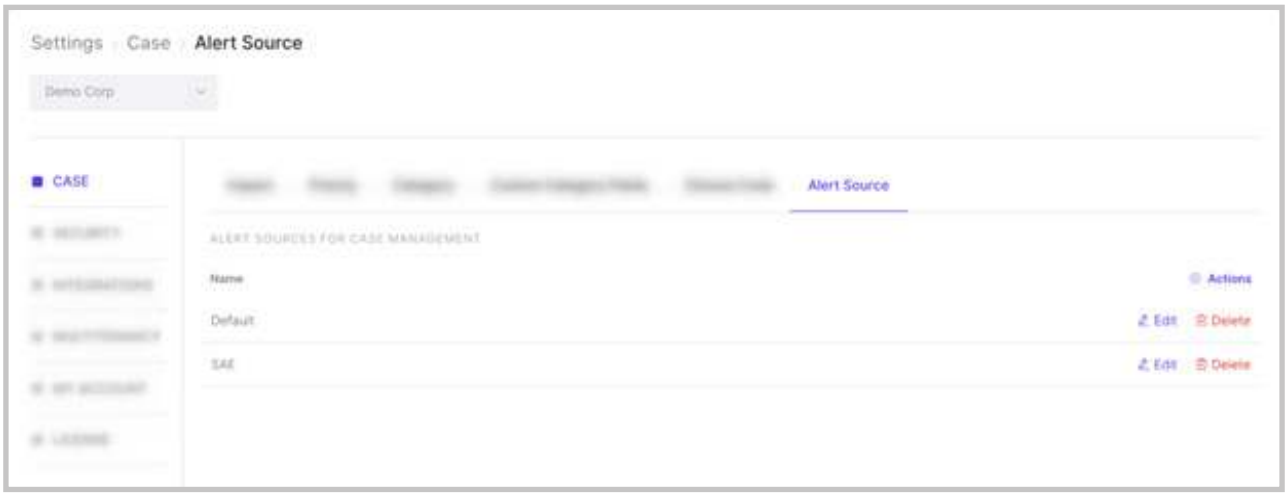
Delete a closure code

A user can also delete a closure code as shown below.



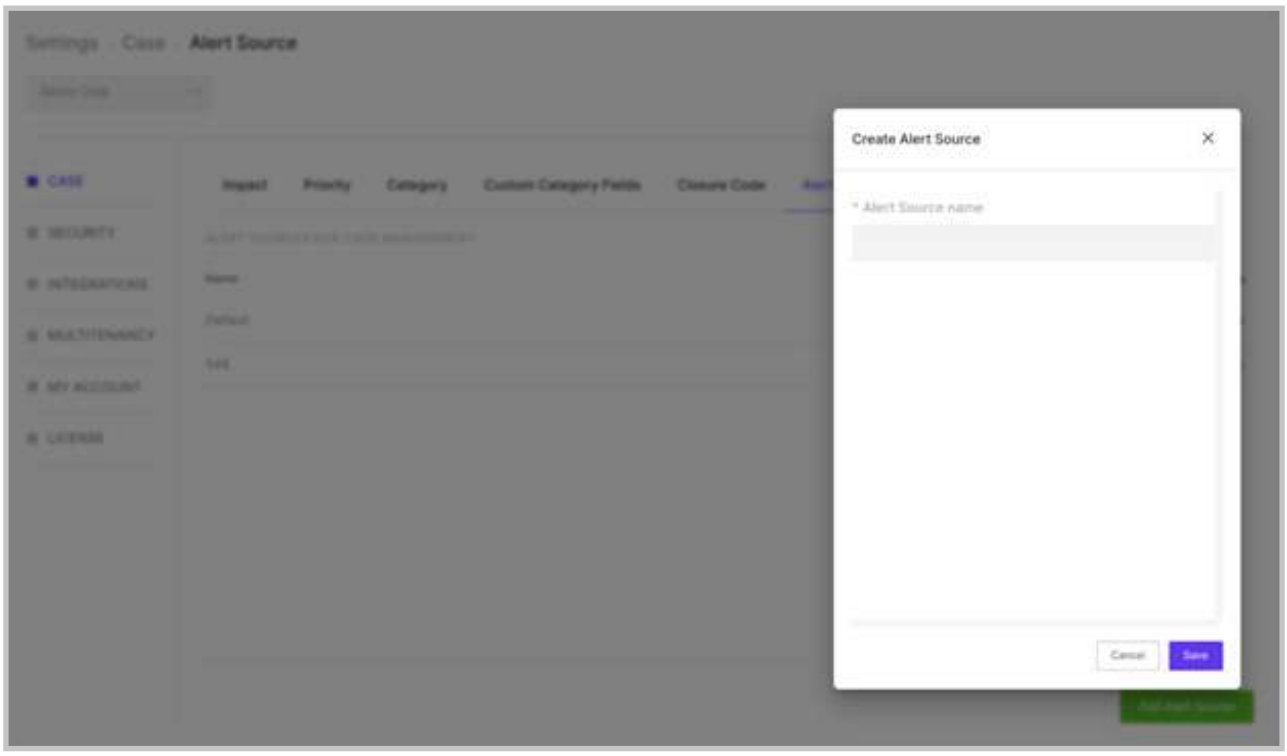
Alert Source

An alert is a technical notification identifying threats and incidents related to a case. Alert source is meant to describe the source of such alerts.



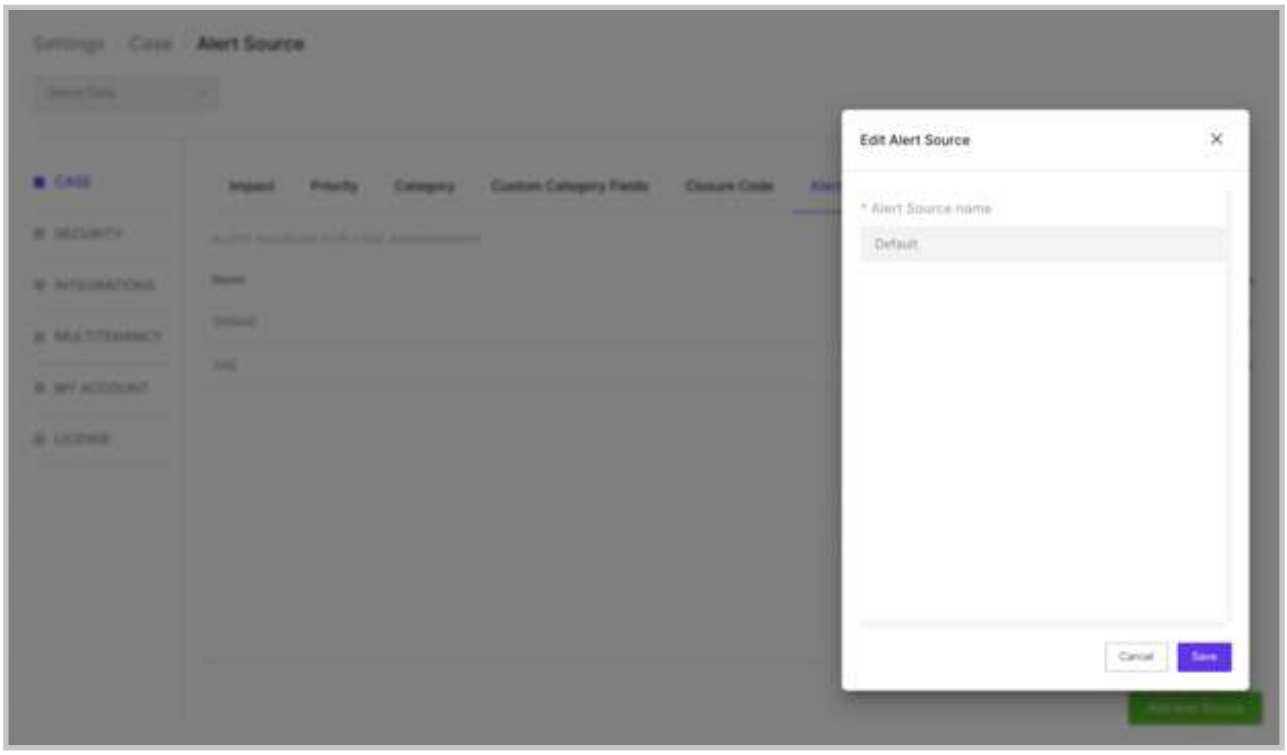
Add alert source

A user has the option to create or add an alert source as depicted below.



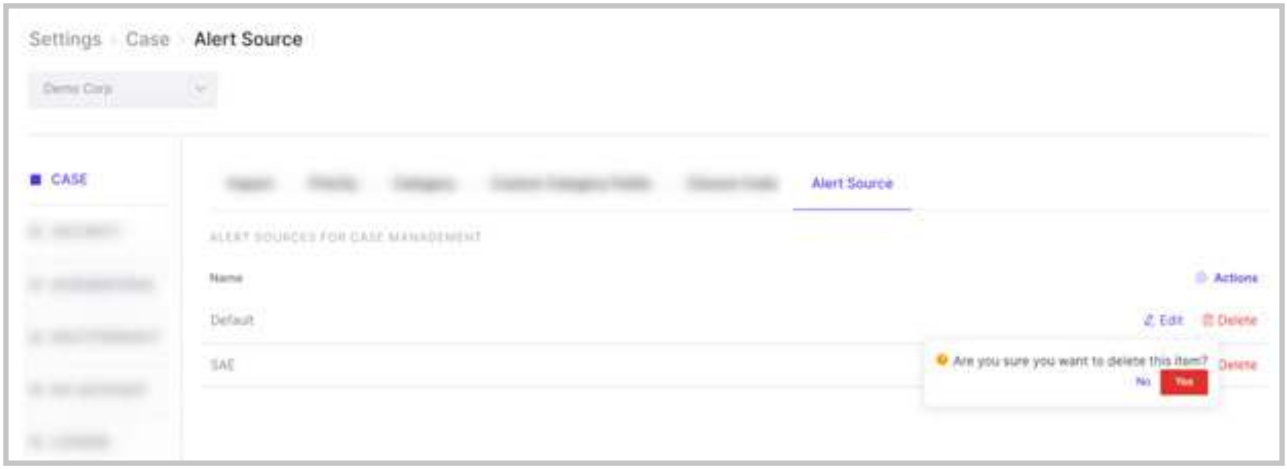
Edit alert source

A user can edit and make changes to an alert source whenever the situation arises for the same.



Delete alert sourcet

A user can also delete an alert source as depicted in the image below.



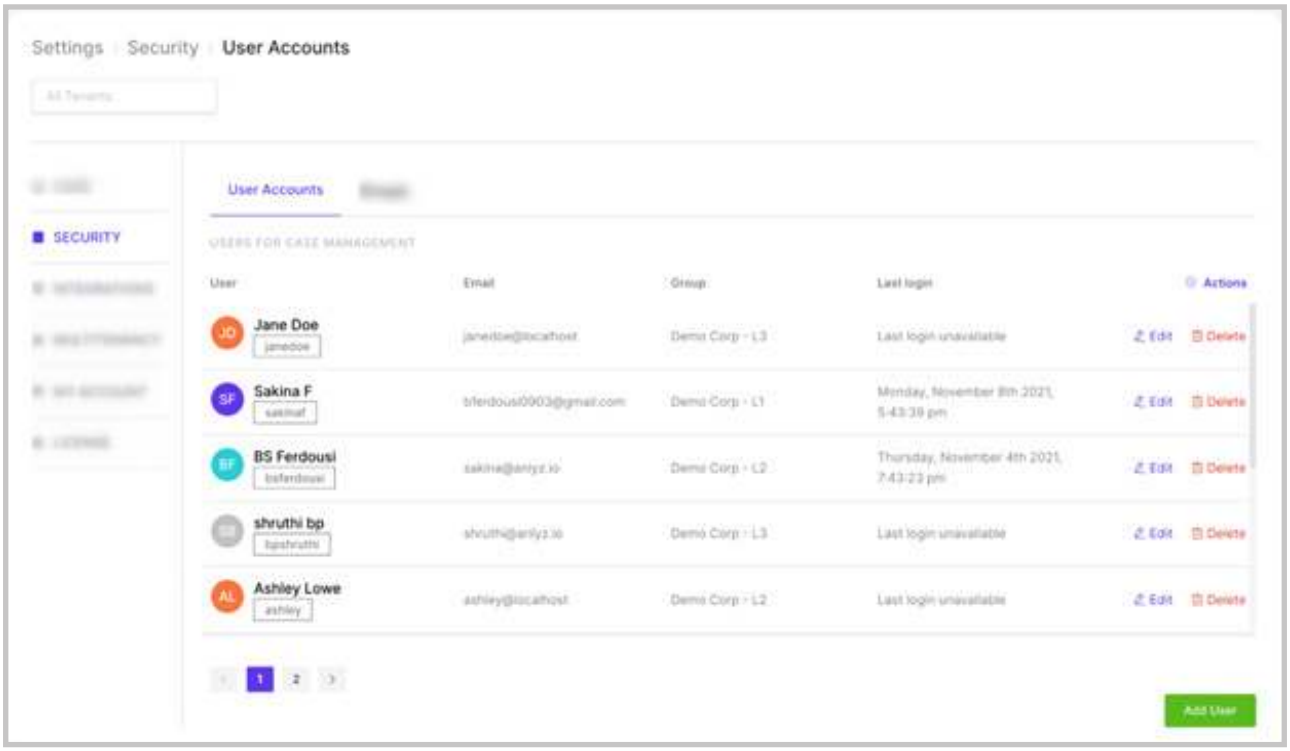
Private Case Terms

When a case is made private, only the user who created the case and the user who is assigned the case can see it. The private case terms can be set by the user as required. Once the terms are set, the user can save them. Every time the assigned user opens the private case, they have to accept the said private terms to get access to the case.

Security

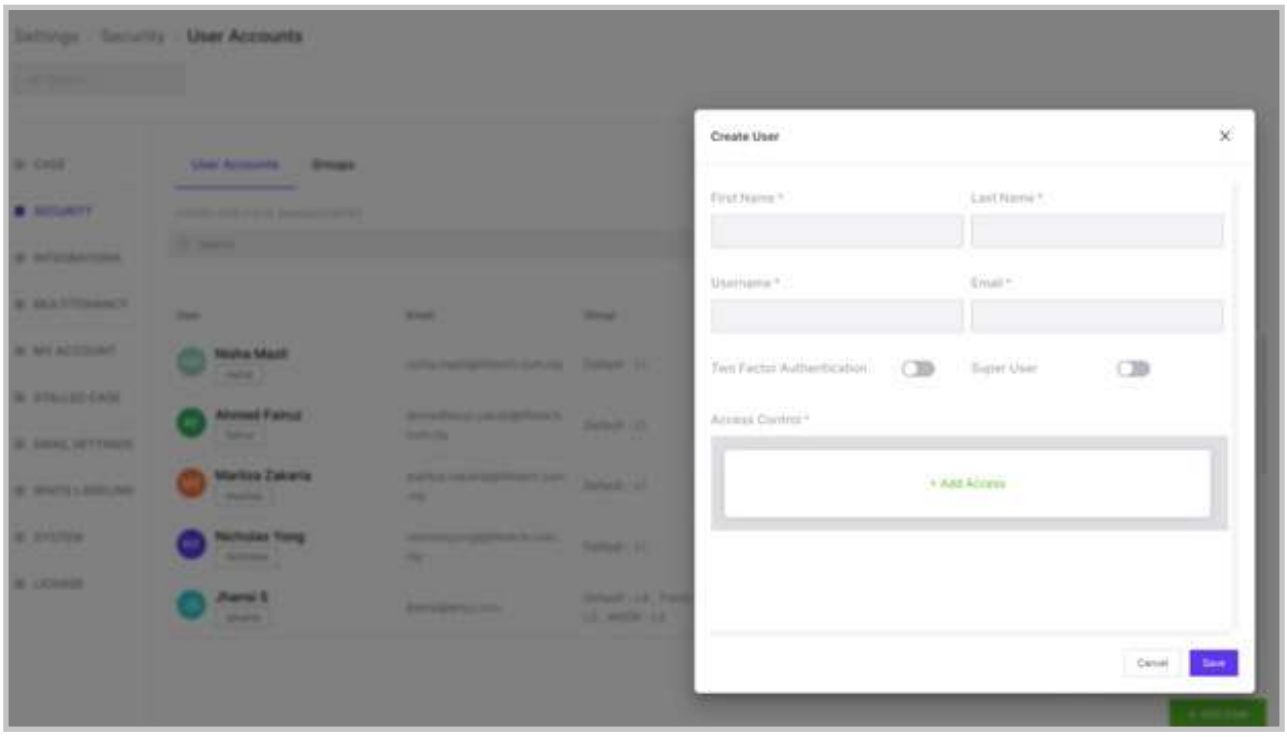
User Accounts

All the users in the team or organization can be seen under the User Accounts section. Details like the email id of the user, the group and the tenants the user belong to and the last login time by the user can be seen under User Accounts.

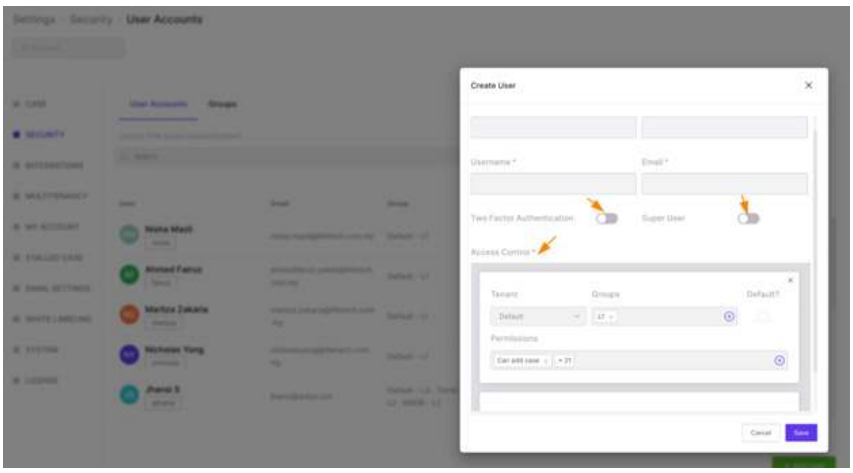


Add User

User accounts can be created with a registered email-id. A password link is generated and sent to the new user's email-id from where a password can be created to log in. While the user is being created, the new user is assigned to the respective tenants, groups and permissions. Here, please note that the permissions are granular. Depending on the situation, a user can be assigned extra permissions or a few permissions can be removed, irrespective of the group/groups assigned. Also, a two-factor authentication option is provided. A user can be made a super user as well.



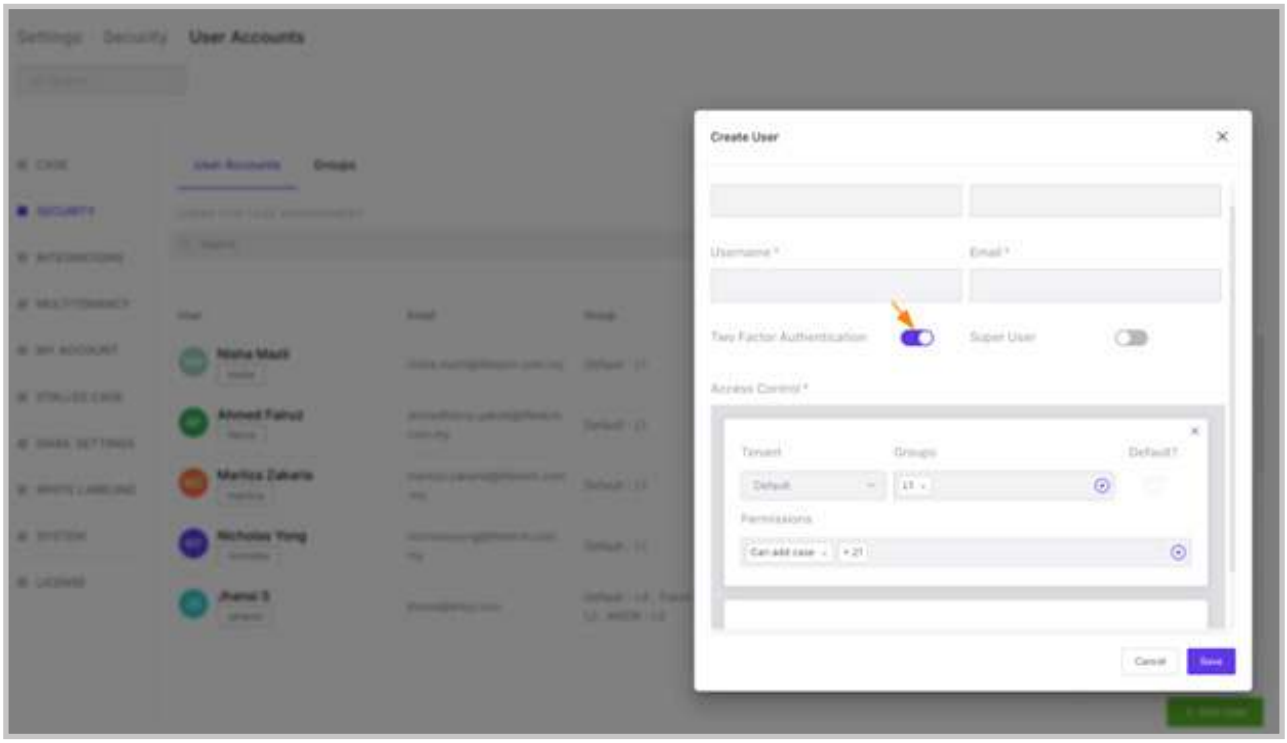
Access control is done as shown below.



Super user – Once a super user is created, that user account cannot be deleted or edited. Hence refrain from creating super users without necessary approvals (Kindly follow the process defined by TM if any). The super user is meant to be only with one or two people in the team (like leads). If others need all permissions, assign them all permissions; however, do not make them super

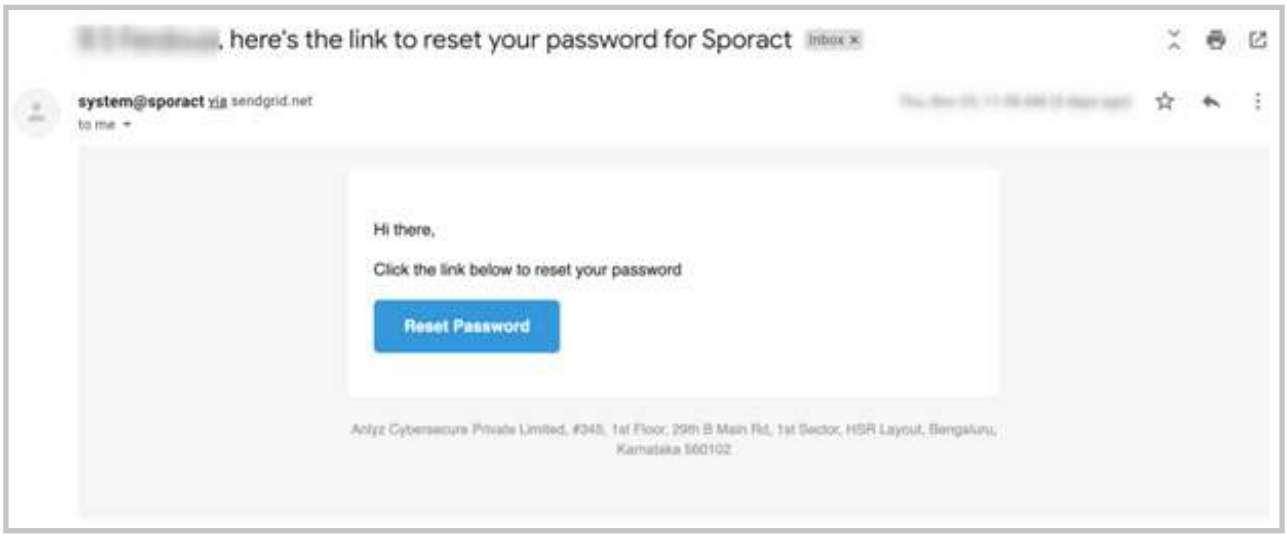
Add User with Two Factor Authentication

A user can be created with two-factor authentication. Click on the 'Add User' to create a new user.

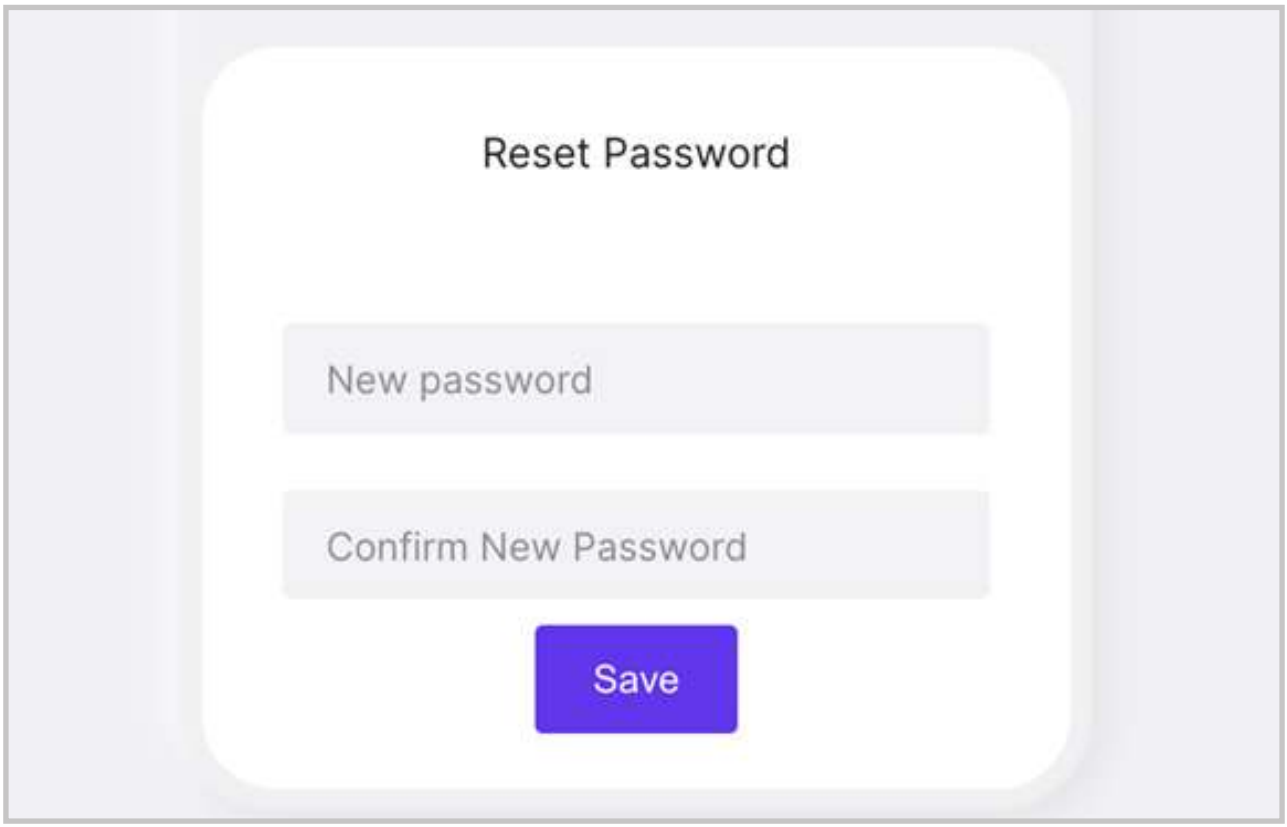


The option Two Factor Authentication can be selected as shown.

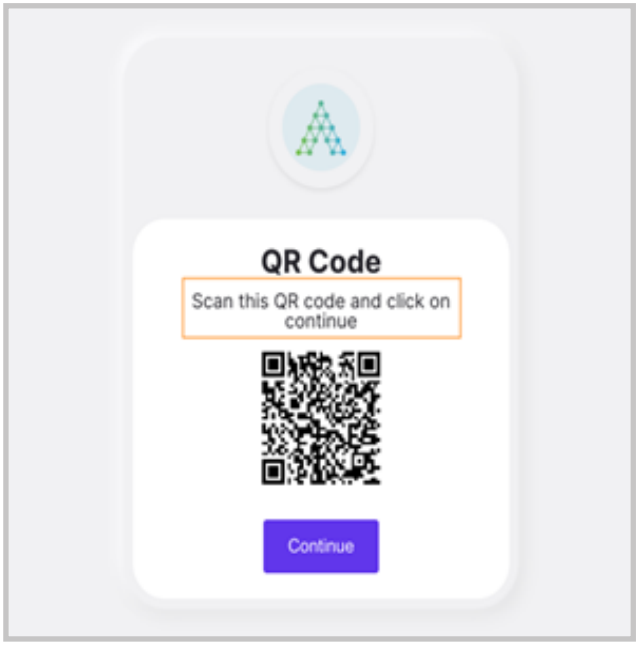
Once a new user is created, a reset password link is sent to the registered email address.

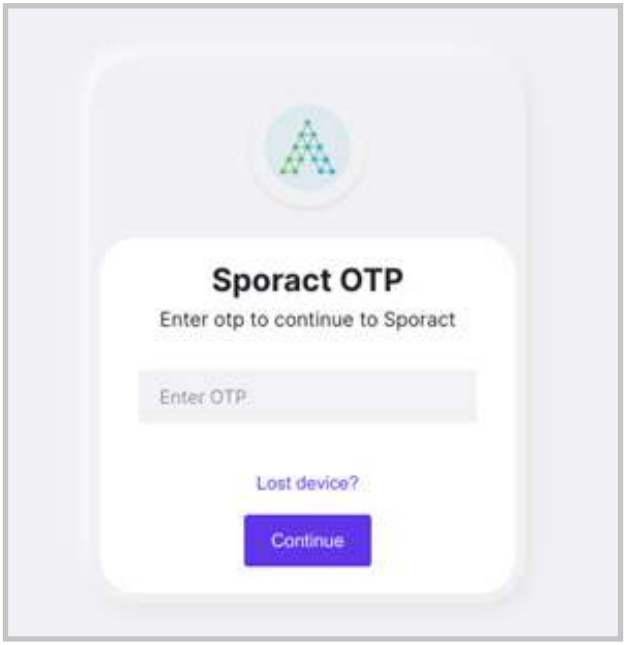


The new user can set the password, and then try logging in to the account.



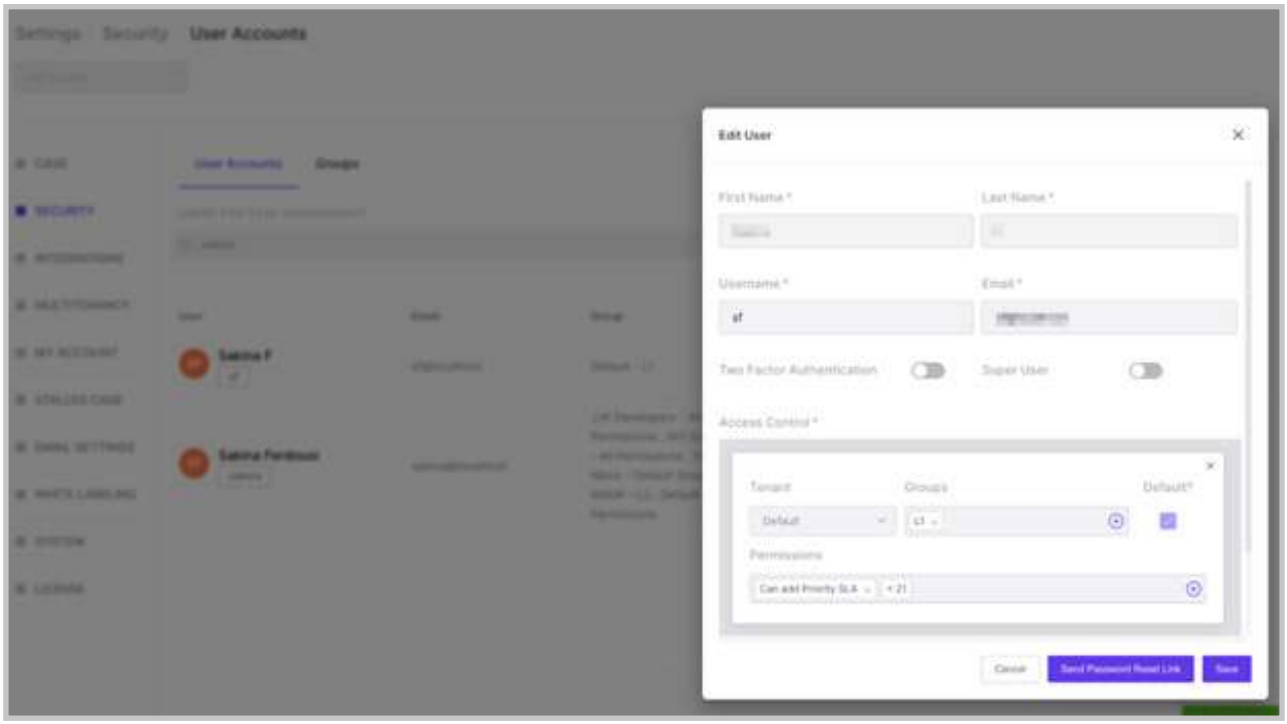
While logging in, the new user has to scan a QR code (use the Google Authenticator app or Microsoft Authenticator app, which gives a 6-digit OTP which changes every 30 seconds). The user has to use this OTP to log in to their account. A token is also generated which can be used by the user for security purposes.





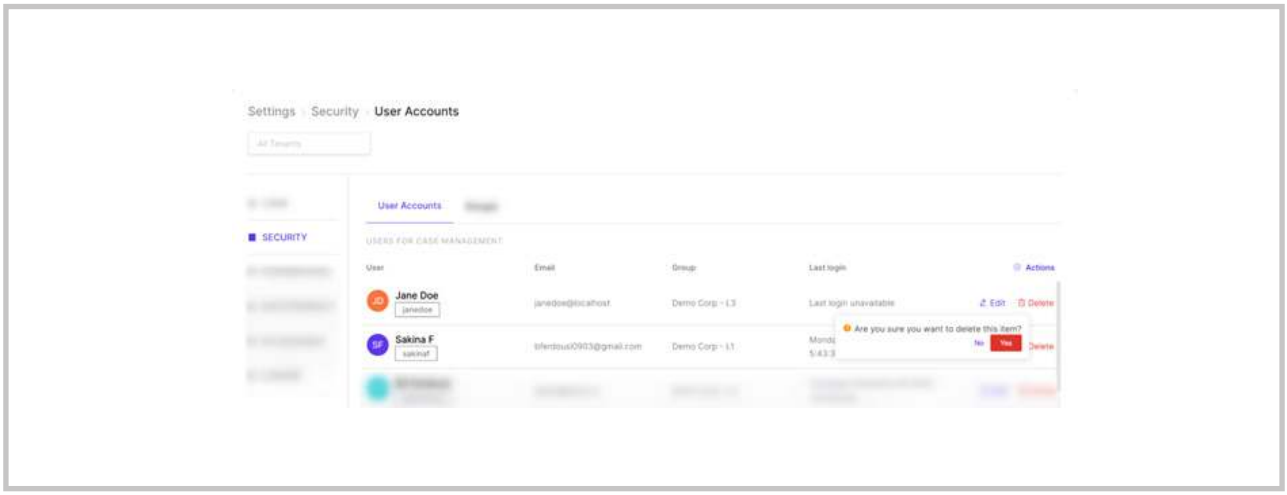
Edit user

Changes can be made to the users whenever required. The password reset link can be sent as well.



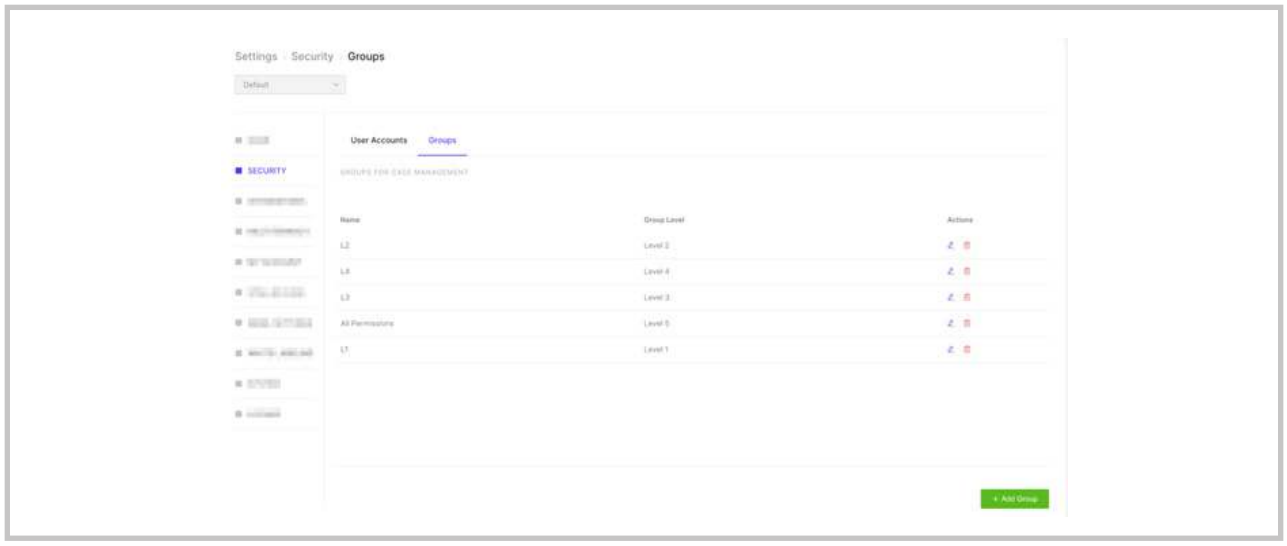
Delete a user

A user can also be deleted by clicking on the ‘delete’ option as shown below.



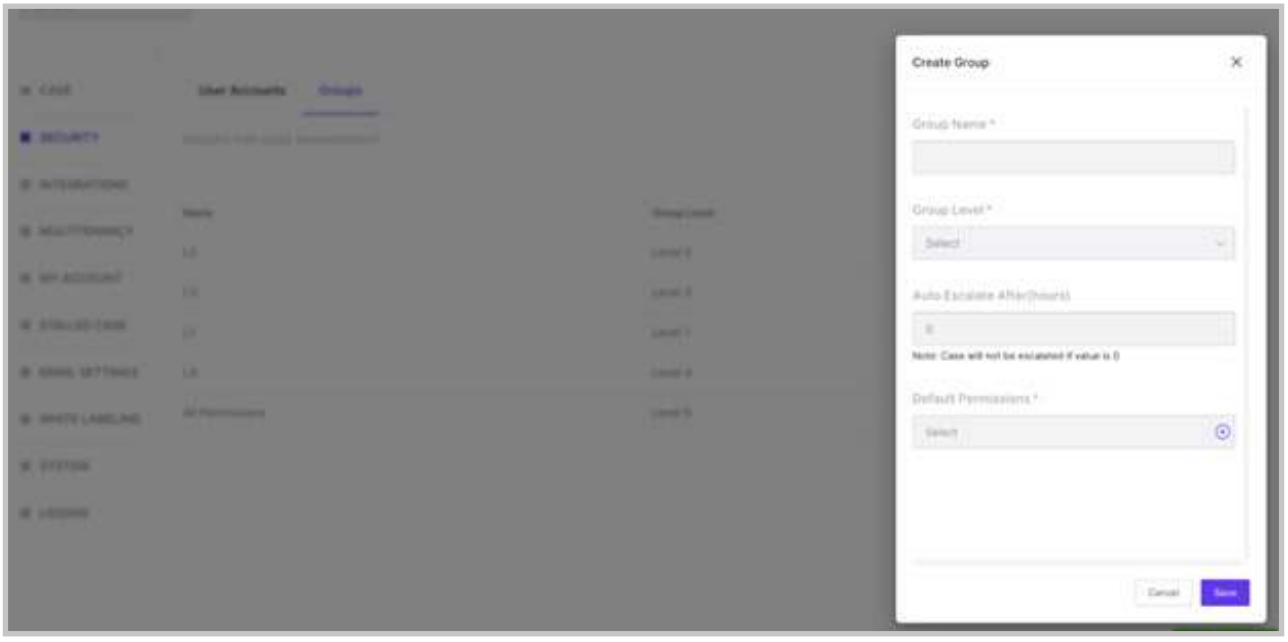
Groups

Groups are meant for access controls. Different groups can have different privileges. Only a group with special privileges can perform specific tasks. For example, only an administrator can create a tenant or delete a tenant.



Add group

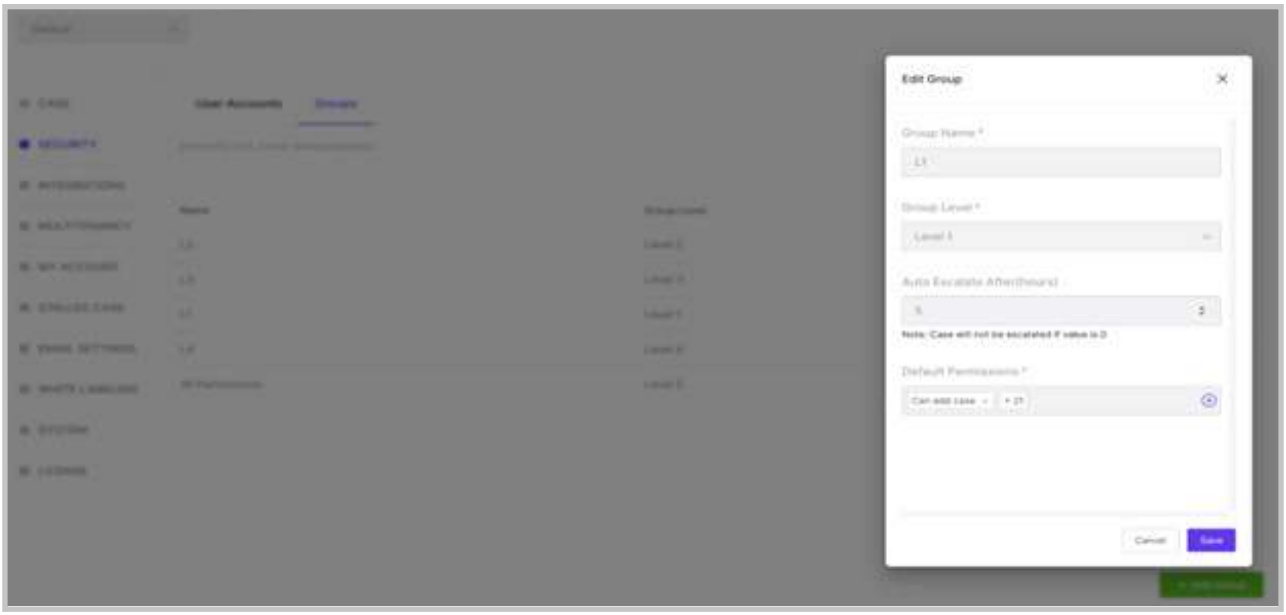
A group can be created by clicking on Add User and specific permissions can be assigned to the said group.



Auto-escalate after (hours) automatically escalates a case to the immediate higher-level group after the specified hours, on the condition that the case remains idle for the said hours. For example, if a group has 1 hour to auto-escalate, after 1 hour of inactivity, it will escalate the case to the next level group.

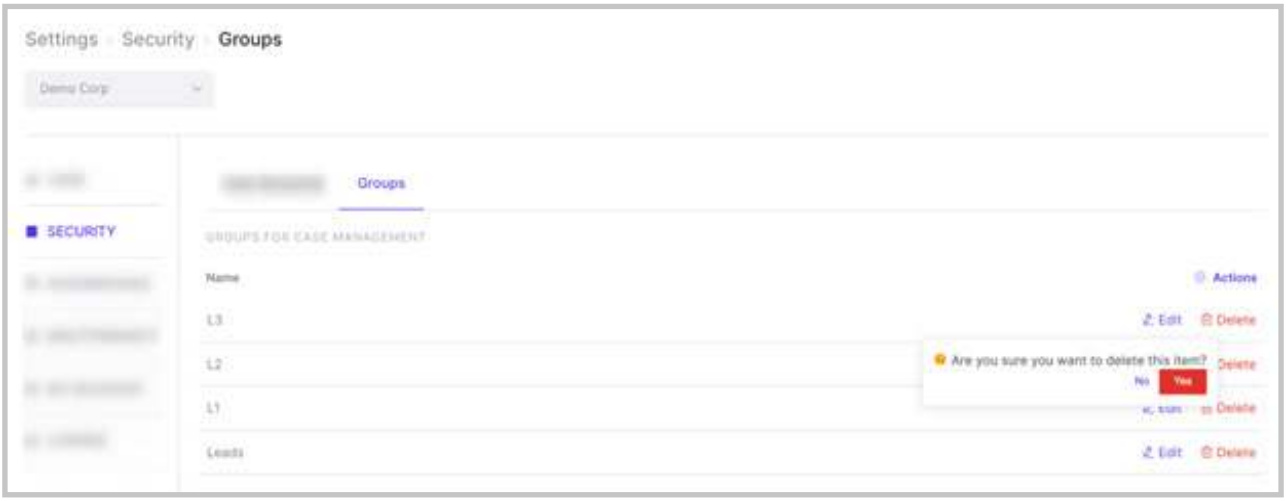
Edit group

Changes pertaining to the name and permissions can be made.



Delete group

A user can delete a group as shown below

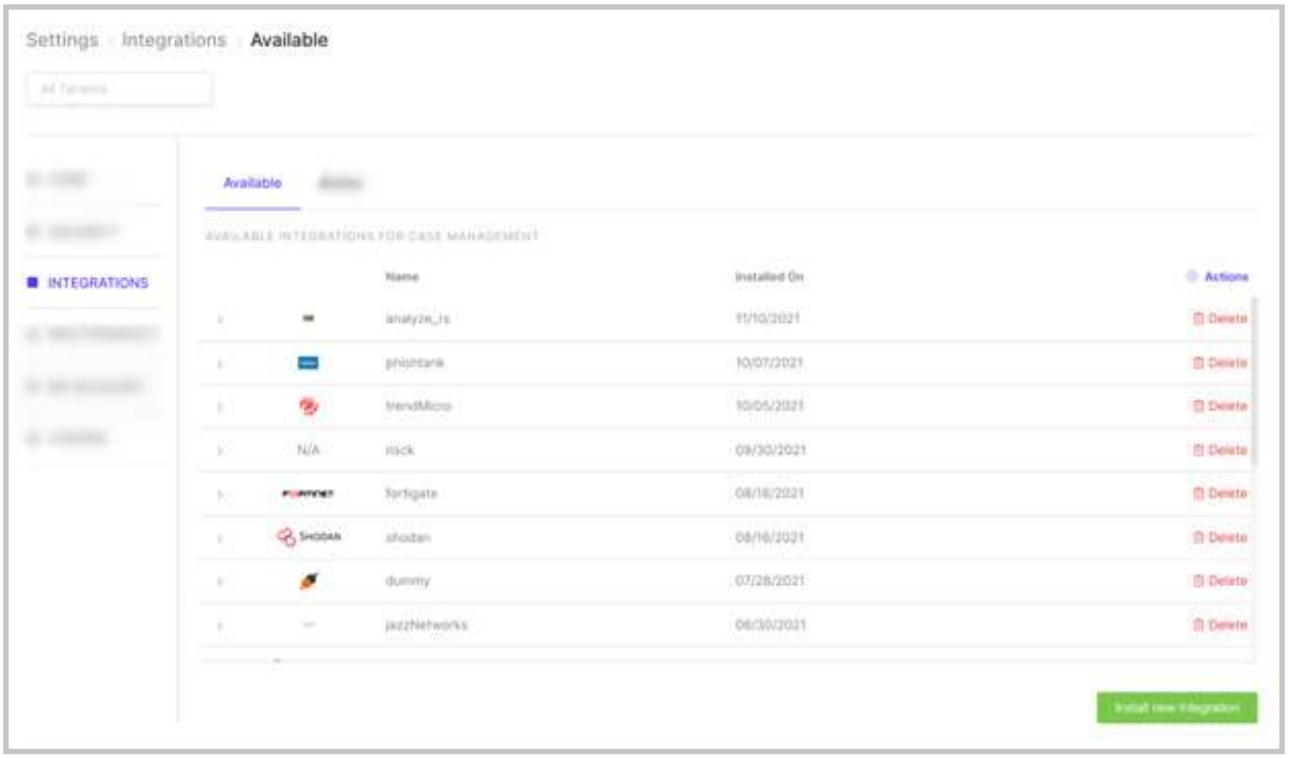


Integrations

Sporact provides multiple integrations which help in creating playbooks and thus help in automating various actions required for incident response. These integrations are a collection of security tools which are incorporated in Sporact and can be open-source or third-party tools.

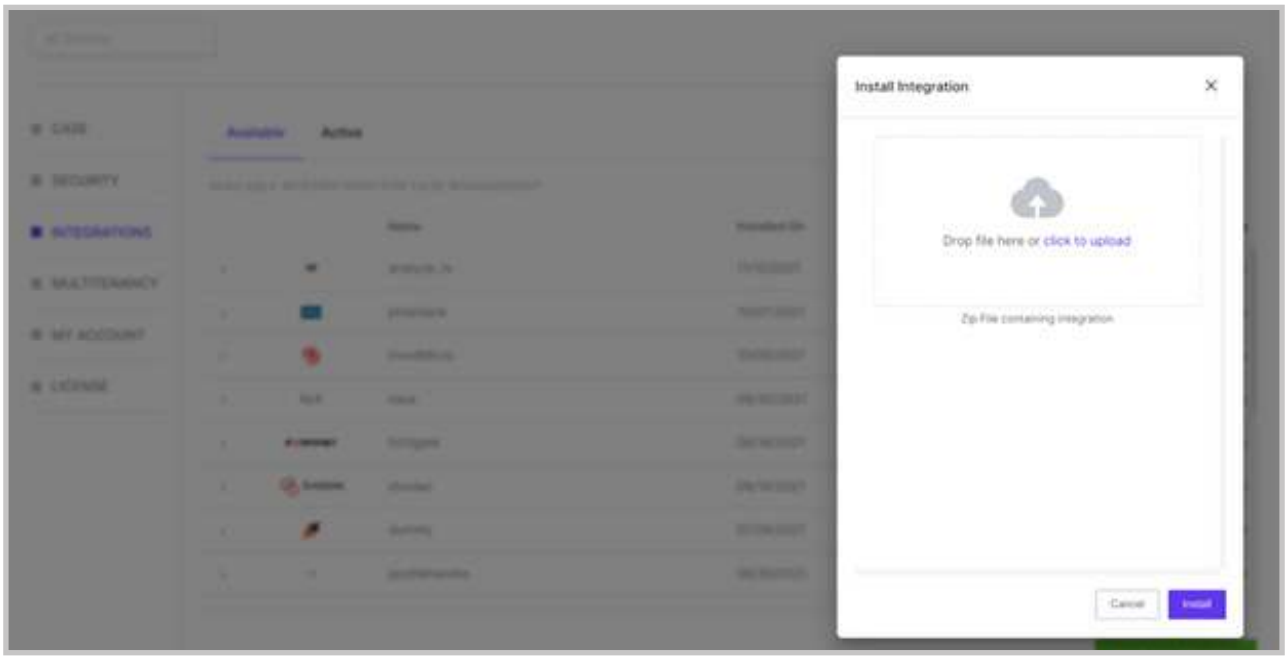
Available Integrations

These integrations are those which are already available in Sporact.



Install new integration

A user can install an integration by uploading the file containing the integration as shown below.

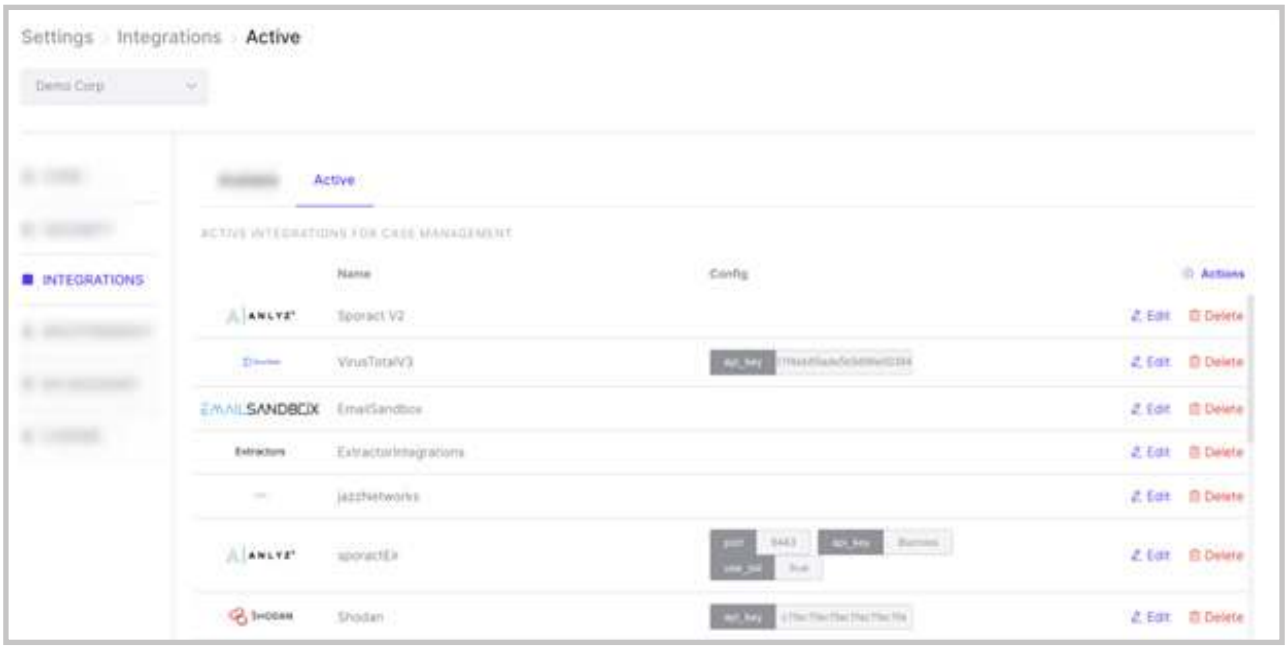


Delete an integration

An integration can be deleted by a user if the need arises.

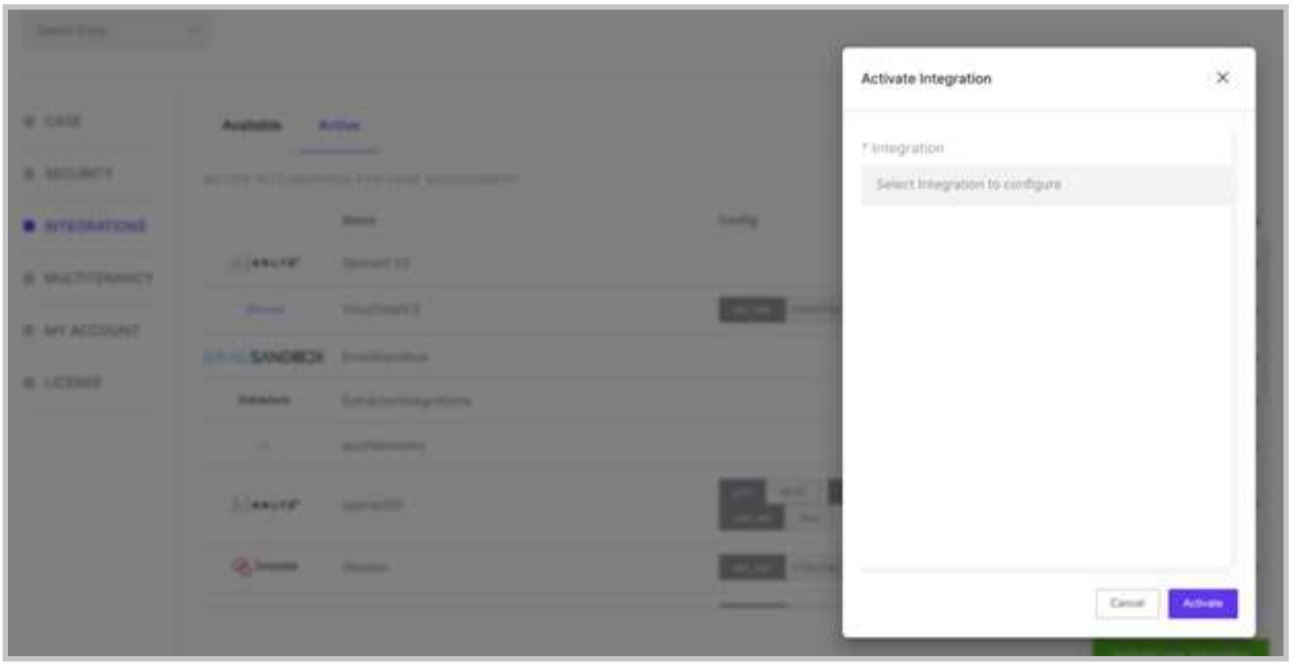
Active Integrations

Active integrations are those that are actively used by the customer or user. These are configured by the user and can be used for creating dynamic playbooks.



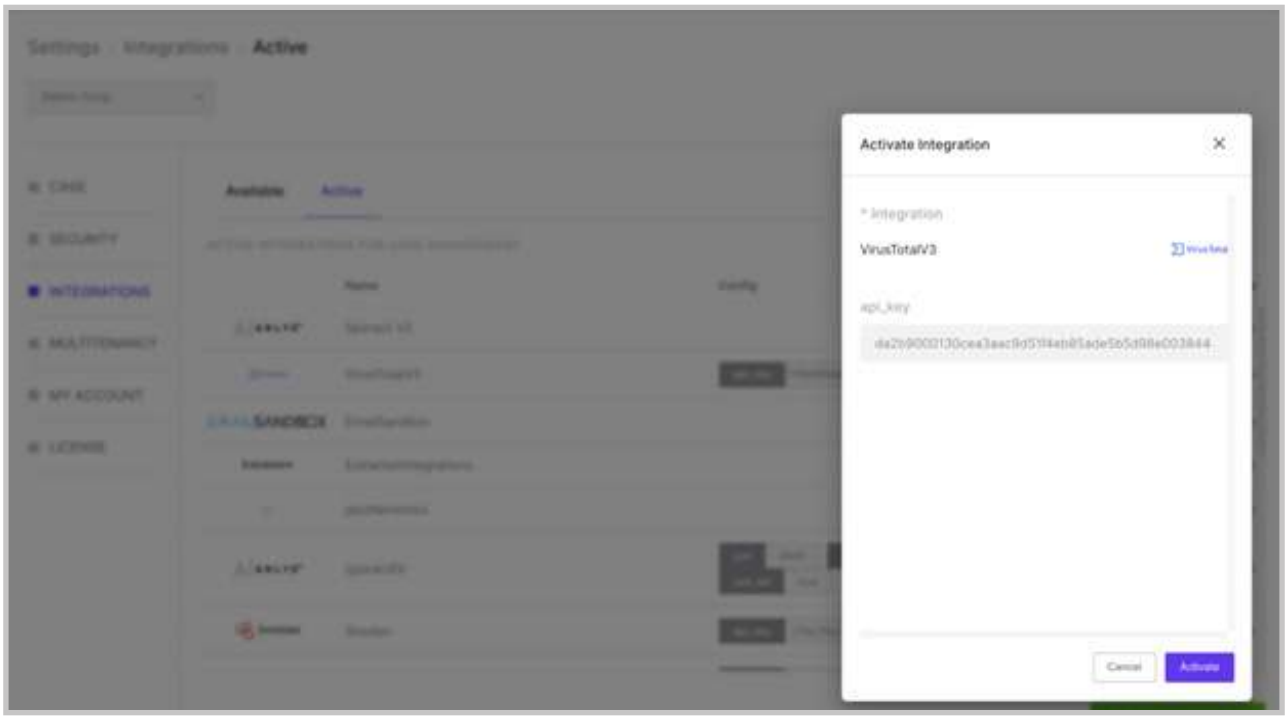
Active Integration

An integration can be activated by providing API keys where required.



Edit active integration

Changes can be made to any integration as shown in the image below.



Delete active integration

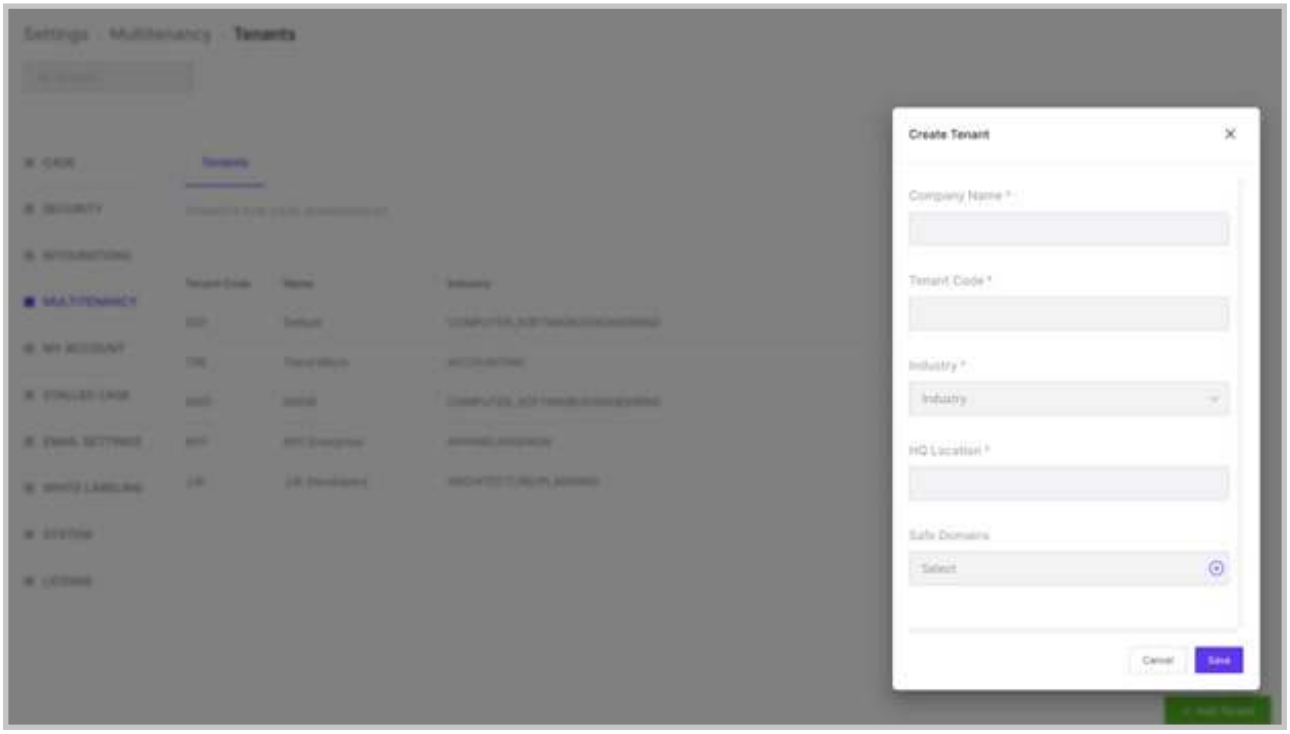
An active integration can be deleted as shown below.`

Multitenancy

Multitenancy allows the same instance of the product to be used by multiple users. A tenant is a group of users that have access to Sporact with specific privileges.

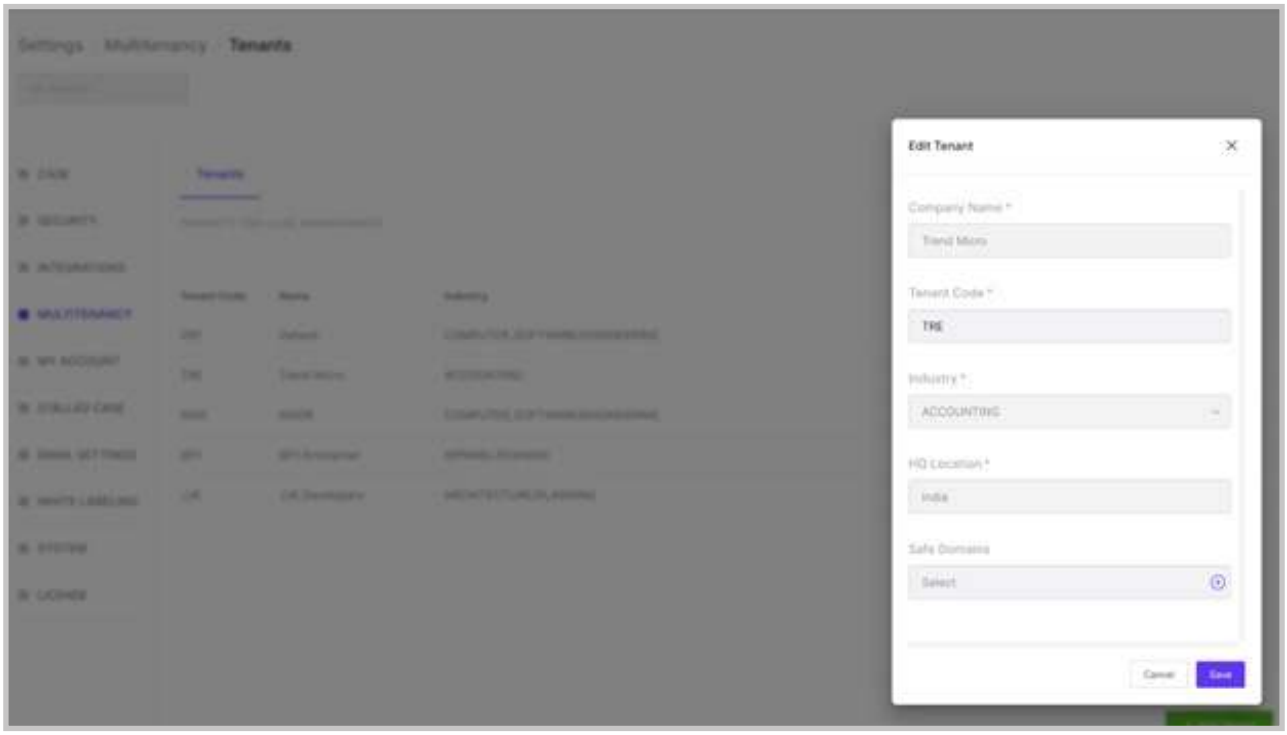
Add tenant

A new tenant can be created by a user with specific privileges as shown below.



Edit tenant

Once a tenant is created, changes can be made to these tenants by using the ‘edit’ option available.



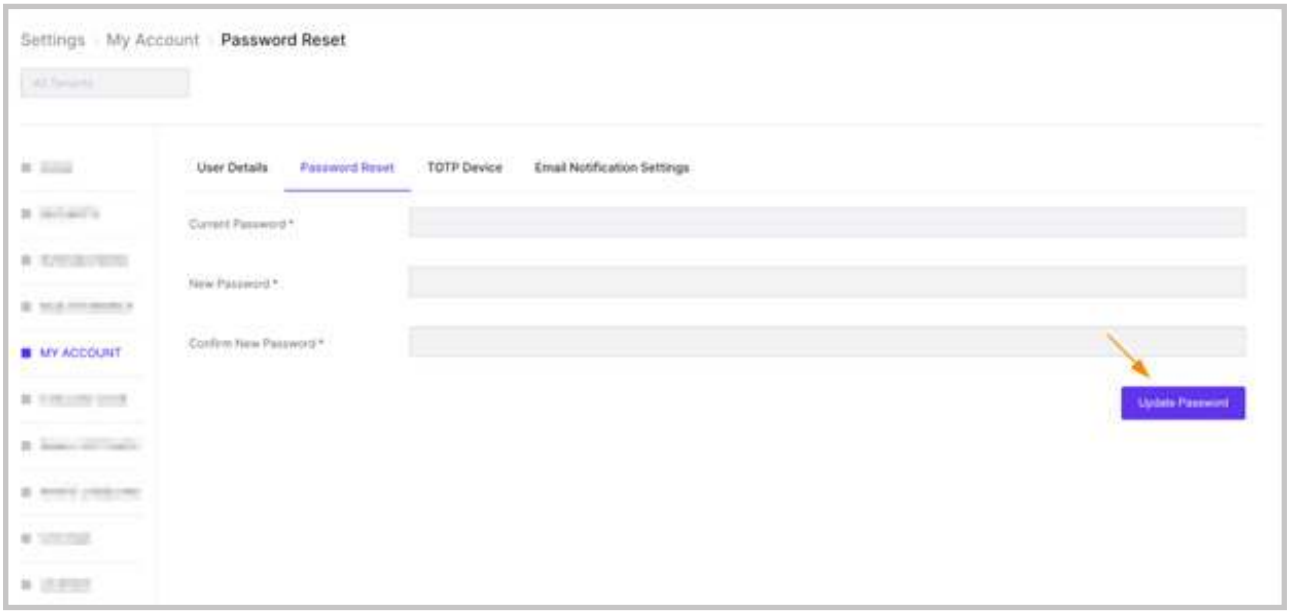
Delete tenant

A tenant can be deleted as shown in the image below.

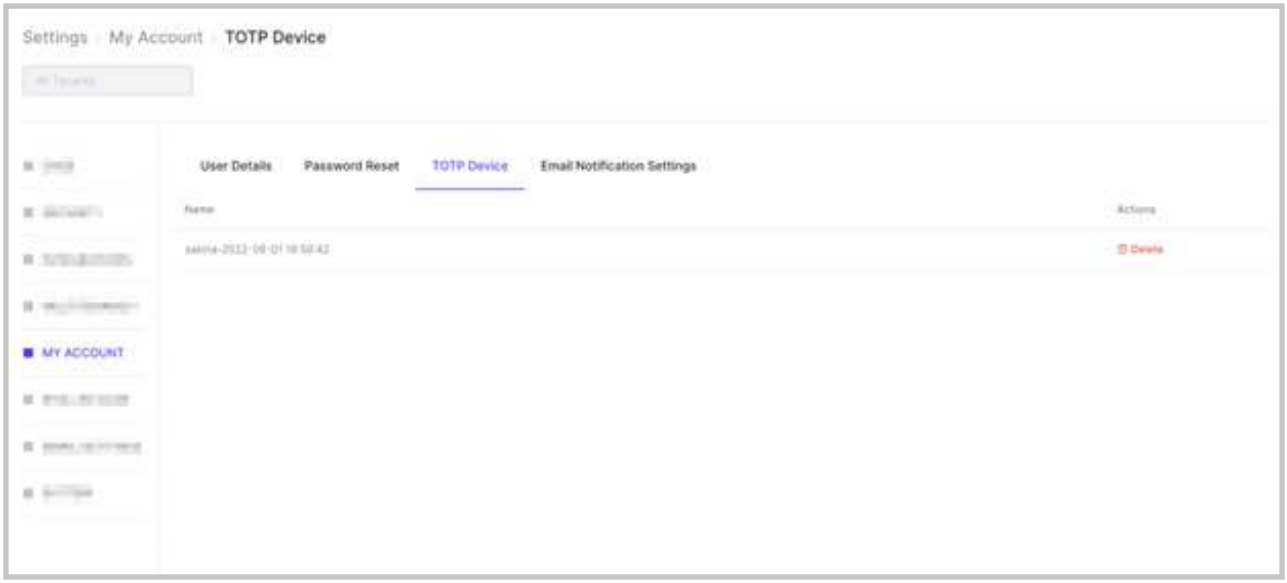
My account

This feature helps in maintaining the user's account. A user can update their user details.

The user can reset the password as shown below. Click on Update Password once done.



If a user account is two factors authenticated, the device token details can be seen under TOTP Device.



The Email Notification Settings provide the user with the option to choose what kind of notification they want to receive.

Stalled Case

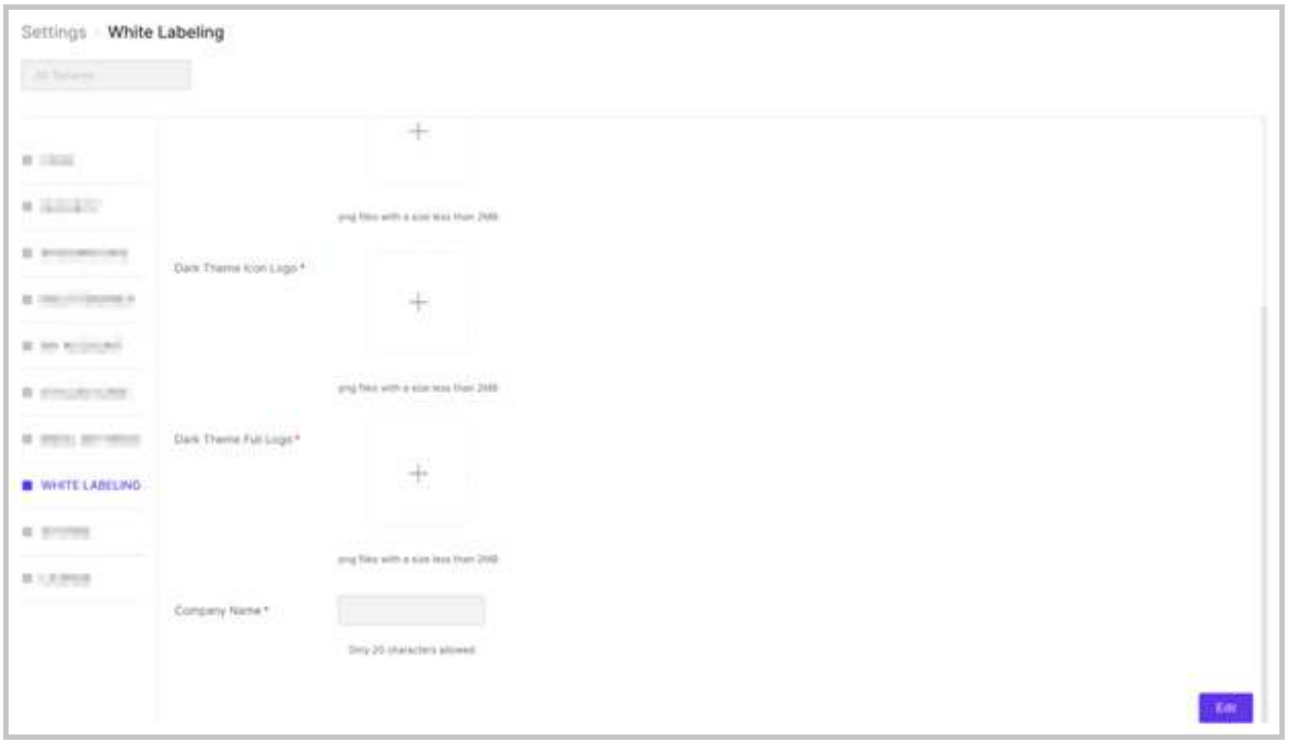
There is a status called Stalled, wherein the status automatically changes to Stalled for a case that is idle and not worked upon for a specified number of days.

Email Settings

The user can set up configurations for email.

The user can edit the email settings as well.

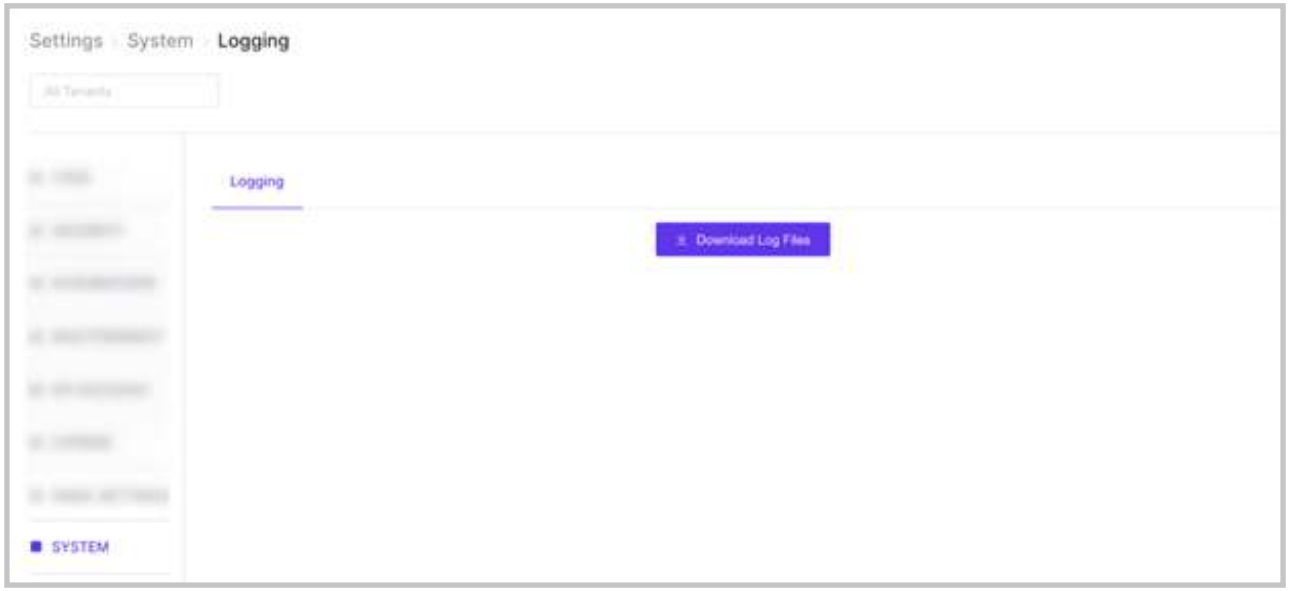
White Labeling



The user can click on Edit to add logos and company name.

System

The user can download log files by clicking on ‘Download Log Files’. The downloaded file is a zip file, which can be extracted to be further analyzed.



License

This gives details about the license pertaining to the product.

The admin can upload the License as well.