CASE SCREENING GUIDE

Replicating escalation rules in Integrity Line

Table of Contents

1. Case Screening Guide – Recreating Convercent Escalation Rules

In Convercent, escalation rules were utilized to supersede any routing in the system if a named party, who would normally have case access, should not be notified of the case. Each rule was set up using conditional logic to ensure that only a narrow group of case managers would be able to access the case based on certain keywords.

For example, you might have a rule that triggered if the CEO was mentioned in the case, and as a result, access to the case would be restricted to only the CECO instead of the compliance manager(s) who would typically triage new cases.

Note- In EQS, Integrity Line offers equivalent functionality via Case Screening, with one difference from Convercent: In Compliance Cockpit, there is a user role called Admin, which grants a user full, complete access to the entire Compliance Cockpit account, including all Integrity Line cases, regardless of Case Screening rules. EQS recommends that you restrict the Admin role to only one or two trusted individuals in the organization. For additional security, you may want to create a special log-in for those who have full Admin permissions.

For example, if one of your case managers is trusted with the Admin role, then they could have one set of credentials for logging into Compliance Cockpit as a case manager, for their day-to-day work, and a separate set of credentials that they could use on occasion to access the full Admin role.

The EQS **Case Screening** feature is used to replicate Convercent escalation rule functionality by identifying and routing reports based on selected keywords. When combined with user access settings and permissions, visibility and access to these cases can be appropriately restricted.

Note - All escalation rules from Convercent will be migrated. However, if your organization has more than 30 escalation rules, you will be unable to create any additional rules. You will be able to edit/delete any existing rules and create new ones if there are less than 30.

2. What is Case Screening?

The Case Screening feature available in Integrity line is used to automatically identify and flag sensitive reports based on specific keywords, enabling restricted access and routing of cases to the appropriate reviewers by defining target folders. It helps ensure that high-risk or confidential issues are handled with the right level of attention and discretion.

Note - This feature routes cases to folders, and it depends on having a corresponding user role that grants access to the appropriate folder. Case Screening does not assign a case manager directly to specific cases.

2.1. How can I use Case Screening to replicate Convercent escalation rules?

Two steps are required to replicate or update your escalation rules from Convercent. The first is to create or update the case screening rules, and the second is to update the roles/permissions for any impacted user roles. Below are more details.

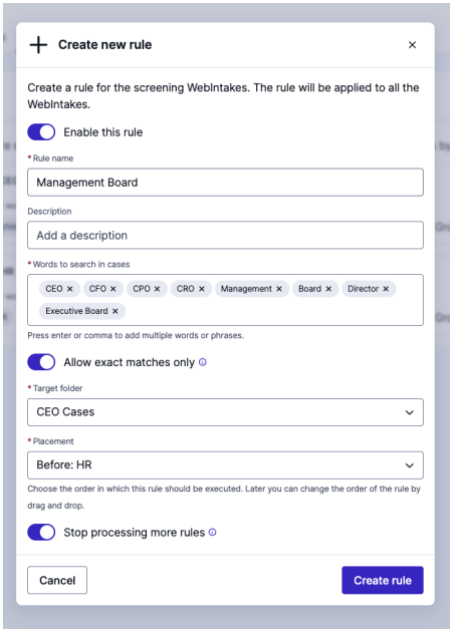
2.1.1. In Integrity Line – Configuration

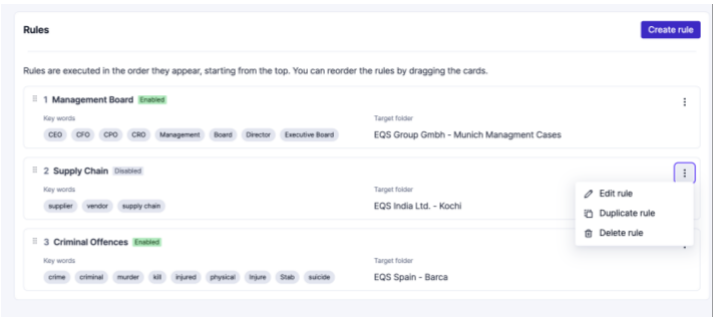
This is where you will set up the rules themselves, with one folder for each rule.

01. If necessary, create a new folder which the screened cases will be routed to.

02. Create a case screening rule for each desired escalation rule – for example, one rule for screening cases related to the Chief Executive Officer, one rule for Board of Directors, etc.

    a. Enter the keywords that will trigger the rule
    b. Toggle on "Allow exact matches only" to avoid screening additional cases that contain a related word.
    c. Select the desired target folder that the cases will be routed to.
    d. Select the placement for this rule. This can also be updated via drag and drop after the rule is created.
    e. Toggle on "Stop processing more rules" so that a case will ONLY be added to the target folder for the first rule whose criteria it meets.





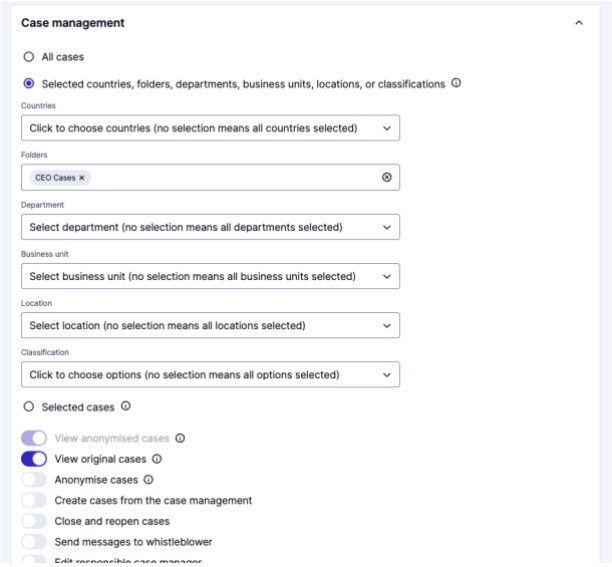
2.1.2. In Data Center – Roles & Permissions:

This is where you will create one custom role per escalation rule. Additionally, you will need to create or update your default Case Manager role to block access to the Case Screening folders.

01. Create a new role or navigate to an existing role that needs to be updated.

02. Under the Integrity Line > Case Management area of permissions, ensure that the radio option "Selected countries, folders, departments, business units, locations, or classifications" is selected.

    a. Update the "Folders" dropdown to limit the user role to allow or deny access to the folder that the case screening rule points to.
    b. Toggle any additional permissions required for the role.



3. Best Practices

- We recommend using "Allow exact matches only"

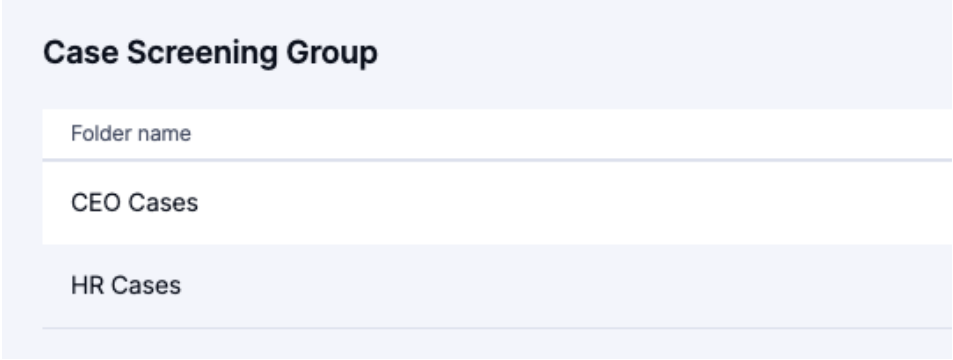
- For example, if this is toggled off, then “fraud” will also match “fraudulent” or “fraudster”
- Please keep in mind that in this case, “HR” will not execute if the reporter typed “H.R.” in their report.

- We recommend using “Stop processing more rules” - without this, multiple rules will execute
- We recommend setting up a folder group for any case screening folders, which ensures an even stricter separation and confidentiality of cases within your organization.
  - For example, the folder group named “Screened Cases” will contain folders that live within the group, appropriately named for each case screening rule.
- We recommend setting up one role for each folder in which screened cases are routed to.
  - For example, one role that allows access only to see CEO cases, one role that allows access only to see HR cases, etc.
  - Roles can be stacked for users, so if one user should have access to multiple screened case folders, they will be assigned each role that is created.
- We recommend setting up one role that does not allow access to any folders in which screened cases are routed to.
  - This role would have access to all cases, except any cases that are screened and routed to folders.

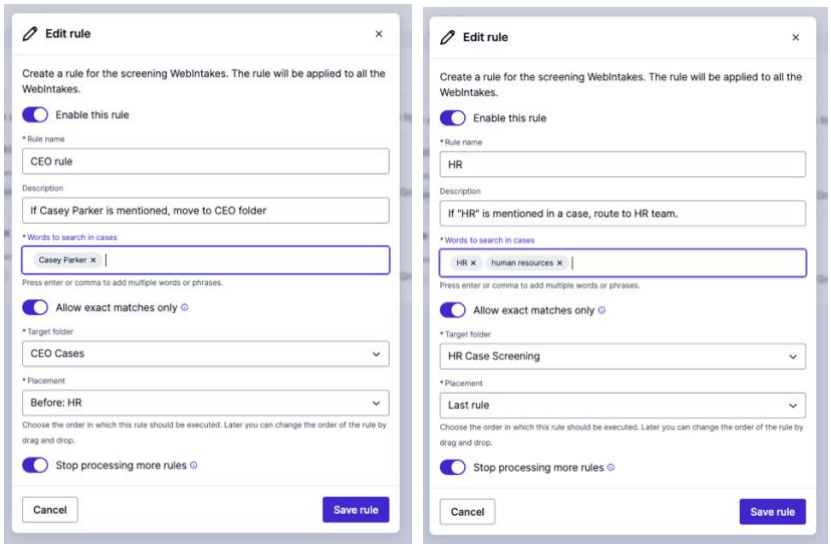
3.1. Example Case Screening Configuration

An organization wants to set up case screening and roles in which any reports that name the CEO are routed to a folder in which only one case manager will have access. They also want to route any HR related cases to a folder where only the HR team has access, and no other case managers.

01. Folders – The organization created the Case Screening Folder Group with the two folders for the rules they are going to create – one for CEO cases and one for HR cases.



02. Case Screening Rules – The organization created two different case screening rules – one for cases naming the CEO and one for HR related cases. The rules include keywords that will trigger the rule, have the target folder selected, and the toggles for exact matches turned on. The rules are also set to stop processing if it has been executed.



03. Roles – The organization has created three unique roles – one for the CEO folder, one for the HR folder, and one for all folders except the case screening folder group.