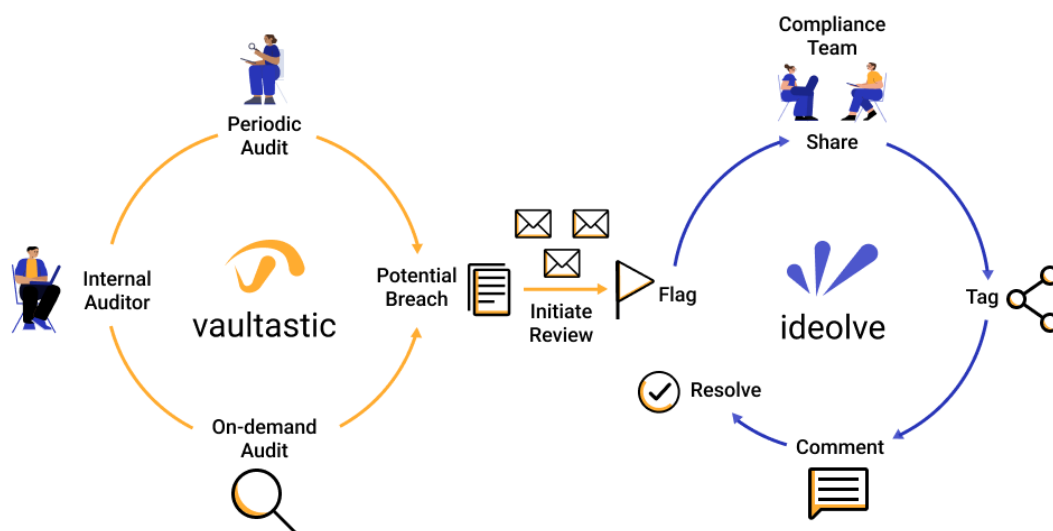# Integration with Vaultastic Active Store

How you can ensure compliance management with Vaultastic

Regular proactive audits of email communication are crucial to mitigating conduct, reputational, and financial risks.

Organizations need to manage the risk related to information leakage and ensure regulatory compliance about supervision and reporting of email communications:

To ensure compliance, organizations often need the help of external experts, auditors, and enforcement agencies to review potential policy violations and decide the course of action.

How can you share critical and possibly classified email information with external people while maintaining privacy and confidentiality?

- The integration of Vaultastic with Ideolve (https://ideolve.mithi.com), Mithi's team collaboration tool, can be of great help here.
- The internal compliance team typically consists of an auditor with access to Vaultastic and who will follow daily, weekly, monthly routines or perform on-demand searches for objectionable emails to share with the other internal members and external auditors.
- The internal and external compliance team members will have shared access to specific workspaces on the Ideolve tool.
- The internal auditor will upload objectionable emails to the individual workspaces on ideolve and share those with the relevant people for deeper analysis and review.
- The team members will post comments and tag each other to collaborate and arrive at actionable steps to

deal with the violation.

- And this entire activity, all comments, and decisions are recorded permanently in Ideolve as an audit trail for future reference.
- This document highlights the two-part process - the first is a one-time process of onboarding the compliance teams on Ideolve and Vaultastic. The second is the creation of proactive routines/SOPs to detect and manage (potential) policy violations.

Preparation to ensure compliance management

Onboarding the internal and external compliance team members on Ideolve

1. The internal auditor to sign up on Ideolve (https://docs.mithi.com/home/how-to-sign-up-to-ideolve) using the business email id.

2. The internal auditor now creates workspaces (https://docs.mithi.com/home/how-to-create-and-manage-workspaces-in-ideolve) for each category of compliance (e.g., "regulatory compliance," "communication policy compliance," "information leakage review") to segregate the reviews and possibly the compliance teams too. This structure is as per the organization's policy.

- The internal auditor now invites relevant internal and external auditors (https://docs.mithi.com/home/how-to-create-and-manage-workspaces-in-ideolve#send-an-invitation%C2%A0to-join-workspaces) and team members to each workspace by adding their email ids. The members will accept the invites and create their Ideolve account to now be a part of the relevant workspace(s).

Onboarding the internal auditor on Vaultastic

1. Log in as the Vaultastic Administrator (https://docs.mithi.com/home/how-to-log-in-to-the-admin-panel).

2. Ensure that you have enabled archiving (https://docs.mithi.com/home/how-to-configure-your-primary-email-server-to-journal-or-forward-live-mail-to-vaultastic) for all or targeted employees.

3. Provide ediscovery access (https://docs.mithi.com/home/how-to-use-the-ediscovery-view-to-quickly-locate-mail-or-do-a-compliance-check) to all vaults or selected ones to the designated internal auditor.
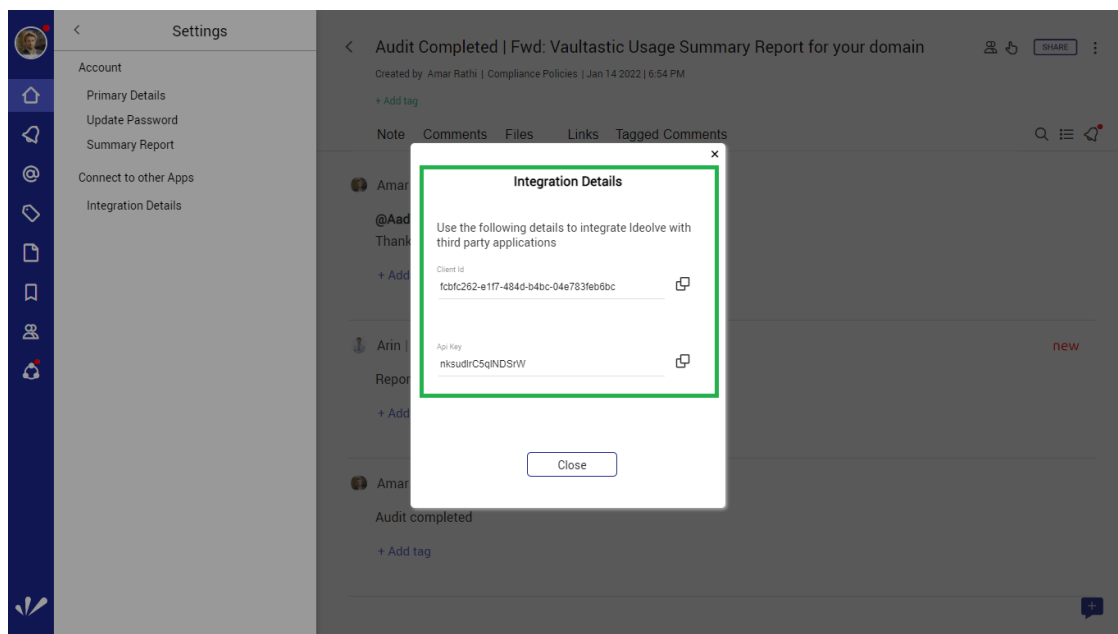
Integrate Ideolve with Vaultastic

1. Login to Ideolve (https://docs.mithi.com/home/how-to-log-in-to-ideolve)
2. The top icon on the Application Bar shows your profile photo. Click on the Profile photo and navigate to the **Settings** page.
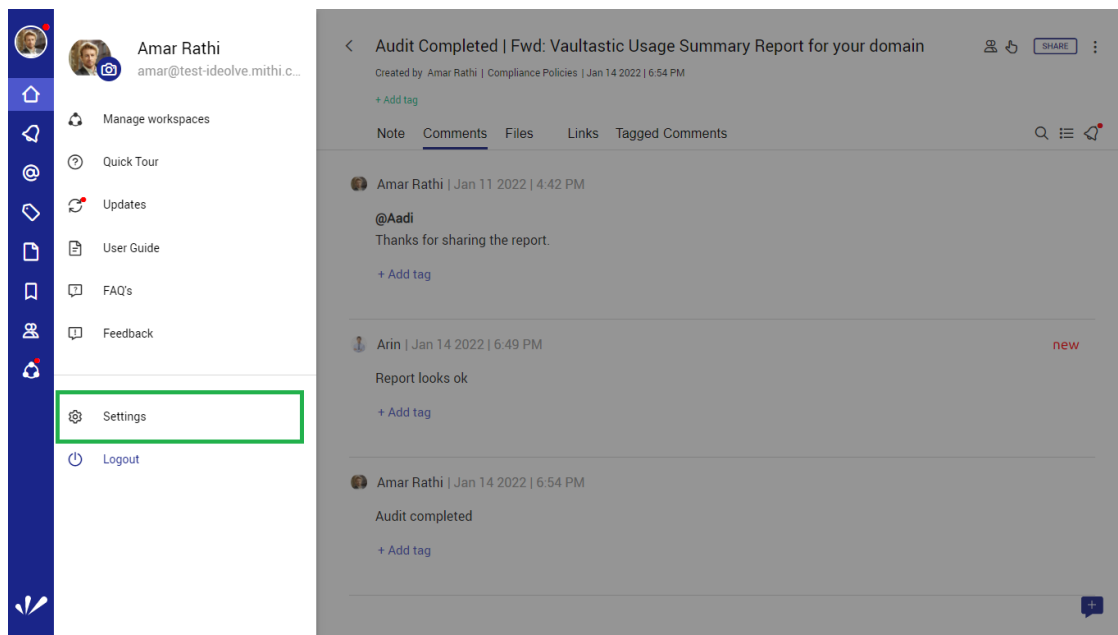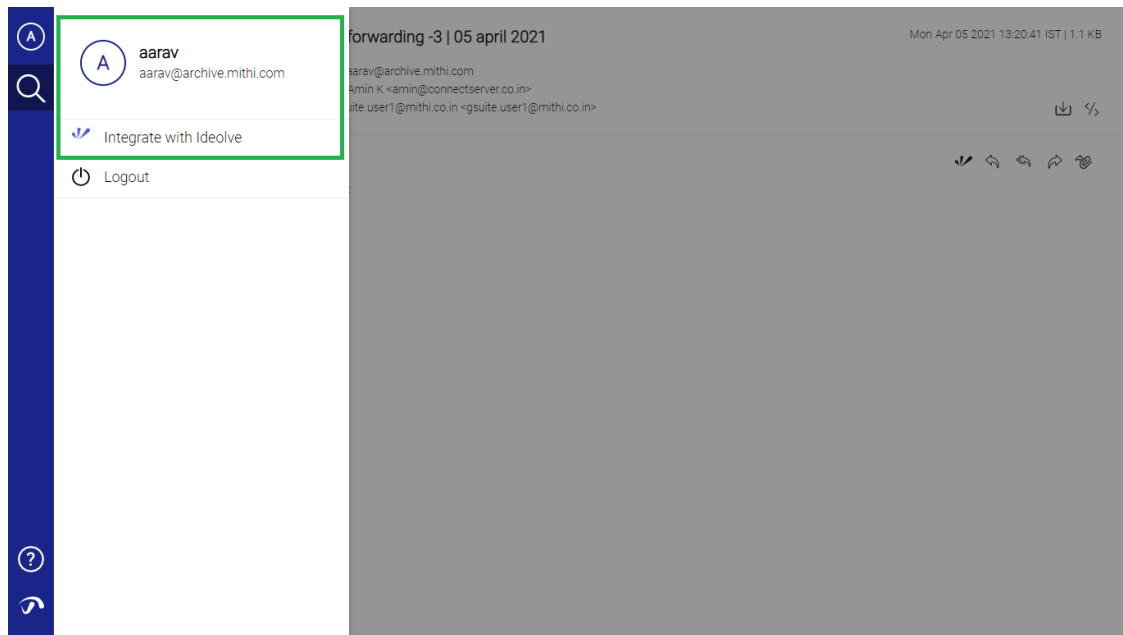
3. Navigate to **Integration Details** under **Connection to Other Apps**.

4. Copy the **Client ID** and the **API Key.**

5. **Login to Vaultastic** (https://docs.mithi.com/home/how-to-log-in-to-the-admin-panel)
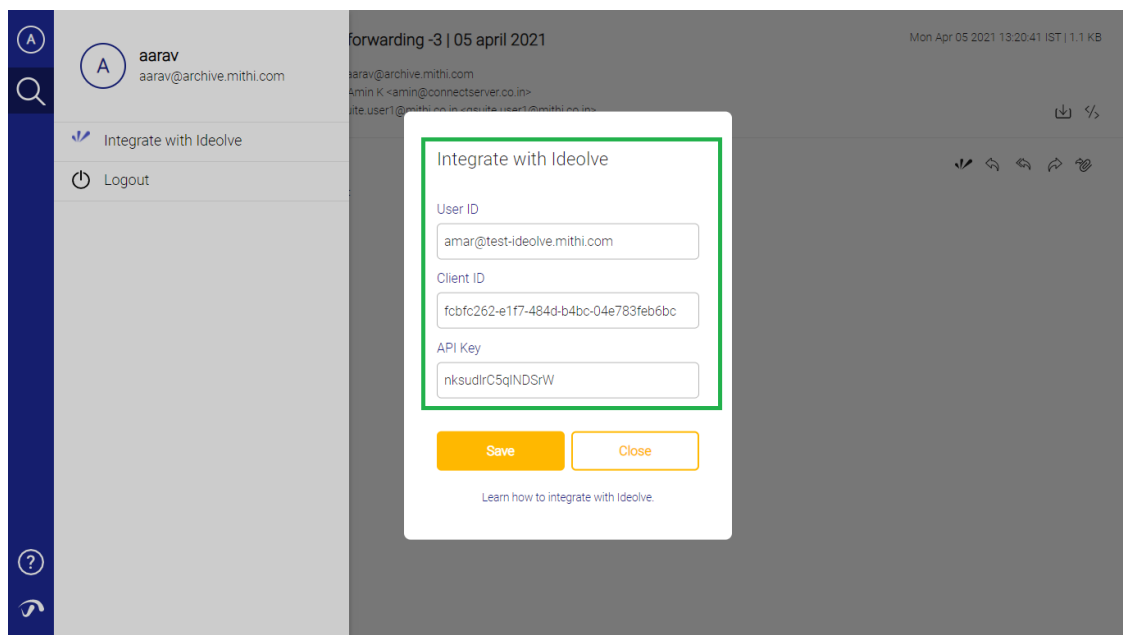
6. Click on the profile initials in the top left corner and select **Integrate with Ideolve**

7. Enter the email-id that you used for signing up on Ideolve in the **User ID** field

8. Enter the **Client ID** and **API key** that you noted in step 4

9. Click **Save**

Routines/SOPs to ensure compliance management

Define and save queries to detect breaches

Define and save searches that look for emails indicating a (potential) compliance violation.

Create the query using mail attributes, keywords, and a date range and give the saved search a relatable name, e.g., "breaches 1-7 Jan 2022", "information leakage," "tone violations," etc.

Scan for breaches on-demand or periodically

1. **Log in to Vaultastic** (https://docs.mithi.com/home/how-to-log-in-to-the-admin-panel) as the internal auditor.

2. Run the appropriate saved search.

3. Review the results and upload all or selected mails to Ideolve. (https://docs.mithi.com/home/compliance-monitoring#uploading-mail-to-ideolve)

4. While uploading, select the appropriate workspace (https://docs.mithi.com/home/ideolve-concepts#workspaces) and share each mail with the relevant auditors who are part of the workspace.

5. Vaultastic flags uploaded emails.

Review notes of the other auditors for flagged email

1. **Log in to Vaultastic** (https://docs.mithi.com/home/how-to-log-in-to-the-admin-panel) **as the internal auditor.**

2. **Run the appropriate saved search.**

3. **The emails earlier uploaded to Ideolve will be flagged.**

4. Click on any of the flagged emails to show the discussion thread for this email in the Ideolve widget.

Review discussions, comments by auditors for all flagged emails together

1. Log in to Ideolve (https://docs.mithi.com/home/how-to-log-in-to-ideolve) as the Internal auditor.

2. Switch to the required workspace (https://docs.mithi.com/home/how-to-create-and-manage-workspaces-in-ideolve#switch-workspace).

3. Search or browse emails and the comments by other auditors.

4. **Tag** (https://docs.mithi.com/home/how-to-add-tags-to-a-note-in-ideolve) or **update the subject** (https://docs.mithi.com/home/how-to-add-tags-to-a-note-in-ideolve) **for all emails whose audit is complete to reflect the completion.**