

Mimecast Incydr Integration Guide

Mimecast Incydr (formerly Code42), an advanced insider threat management and data loss prevention (DLP) platform. Mimecast acquired Code42 in July 2024, integrating its Incydr product into the Mimecast Human Risk Management platform.

Deployment Type

This integration supports **private cloud**, and **vendor cloud** deployments through **port 443**, and **on premises** deployments through **port 636**. If you already know that your environment supports these deployments, continue to the next step. If you are unsure, please check your organization's compatibility before continuing.

Required Information and Setup

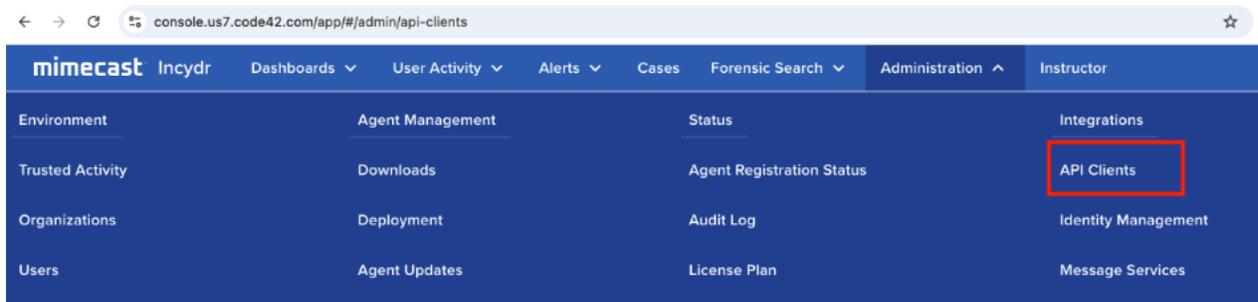
To integrate GreyMatter with Mimecast Incydr, collect the following details:

- URL
 - Default: <https://api.us7.code42.com>
- Client ID
- Client Secret
- Watchlist
 - Prepopulated: RQ_GM_Watchlist

See the instructions below to gather the required information.

Create a New API Client

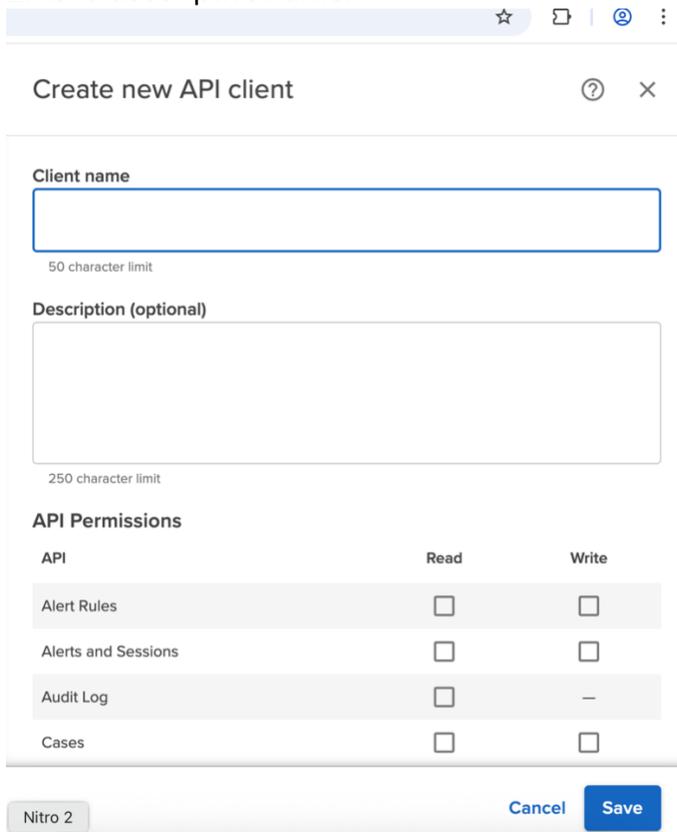
1. Within Mimecast, select **Administration**.
2. Click **Integrations**.
3. Click **API Clients**.



4. Click **Create new API client**.

Mimecast Incydr Integration Guide

5. Enter a descriptive name.



Client name

50 character limit

Description (optional)

250 character limit

API Permissions

API	Read	Write
Alert Rules	<input type="checkbox"/>	<input type="checkbox"/>
Alerts and Sessions	<input type="checkbox"/>	<input type="checkbox"/>
Audit Log	<input type="checkbox"/>	–
Cases	<input type="checkbox"/>	<input type="checkbox"/>

Nitro 2 Cancel Save

6. Add the USERS_WRITE AND USERS_READ permissions .

7. **Save.**

[Learn more in Code42 documentation.](#)

Retrieve Watchlist Name

1. In User Activity, click **Watchlists**.
2. Copy the Watchlist Name for pasting in the GreyMatter Connections Setting page later.

If you don't have a watchlist or would like to use a ReliaQuest-specific watchlist name, create a new watchlist in the Watchlists page named RQ_GM_Watchlist.

Permissions and Functionality

Permissions

[Learn more about Incydr product plan and access levels.](#)

GreyMatter Capability	Action(s)	Required Permission
Respond	Add User to List	USERS_WRITE
	Remove User from List	USERS_WRITE
	Enrich User	USERS_READ

Mimecast Incydr Integration Guide

Respond

Playbook Name	Description	Required Input Variables
Enrich User	Get User details by Username	Username or Email ID Example: johndoe@email.com
Add User to Group	Add User to Watchlist Actor can be any entity, but all users are actors. This user or actor is added to the Watchlist in Integration settings.	Username or Email ID Example: johndoe@email.com Group Name Example: DEPARTED_EMPLOYEES
Remove User from Group	Remove User from Watchlist Actor can be any entity, but all users are actors. This user or actor is removed from the Watchlist in Integration settings.	Username or Email ID Example: johndoe@email.com Group Name Example: DEPARTED_EMPLOYEES

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.