

AQUILA - Setup Integration from Mimecast

Mimecast Integration Guide

Integrate **Mimecast** with your security platform via API to collect email threat data, archive logs, DLP events, and other security-related logs for centralized visibility and incident response.

Credentials & API Access Setup (Mimecast)

Before configuring the integration, prepare your API credentials from the Mimecast Admin Console.

Steps:

1. **Log in** to the Mimecast Administration Console.
2. Navigate to **Administration** → **Account** → **API Applications**.
3. Click **“Register New Application”** and provide a name and description.
4. Once registered, take note of the following credentials:
 - **Application ID**
 - **Application Key**
 - **Access Key**
 - **Secret Key**
5. You may need your **Mimecast Region-specific API URL**:
 - Example: `https://api.mimecast.com`
 - Check with your Mimecast representative for region-specific URLs.

“ **Note:** Some log types may require separate credentials due to rate limits.

Permissions Reference (Mimecast API App)

Ensure the API Application and associated Access Key have the following scopes:

Data Stream	Permission Scope
Archive / Audit Logs	auditevents:read
DLP & SIEM Logs	dlplogs:read , siemlogs:read
Threat Intel Feeds	ti_logs:read
TTP Logs	ttp_logs:read

Integration Configuration (Mimecast)

Data Stream	Required Details
Archive Search Logs	Application ID, App Key, Access Key, Secret Key, URL
Audit Events	Same as above
DLP Logs	Same as above
SIEM Logs	Same as above
Threat Intel Malware (Customer/Grid)	Same as above
TTP Logs (Attachment, URL, Impersonation)	Same as above

Aquila Integration Configuration (Mimecast)

(incomplete)

Revision #2

Created 17 July 2025 23:40:52 by Kent Lauron

Updated 18 July 2025 23:40:12 by Kent Lauron