

AQUILA - Mimecast API v2 Integration

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.

API 2.0 is the current standard - It's been generally available for over a year and is what Mimecast recommends for new integrations

Credentials & API Access Setup (Mimecast API v2)

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

Needed Credentials:

- **API URL**
- **Client ID**
- **Client Secret**

Creating an API 2.0 Application:

To create an API 2.0 Application, follow the steps below:

1. Log in to **Mimecast Administration Console**
2. Navigate to **Integrations | API and Platform Integrations**
3. Locate the following **Mimecast API 2.0** tile and click on **Generate Keys**.



Mimecast API 2.0

Create custom integrations using enhanced and improved APIs.

Generate Keys



4. After reading the **Terms & Conditions**, complete the **I accept** check box to enable the **Next** button to progress onto the next step.
5. Complete the **Application Details** section.

Add Mimecast API 2.0 Application

- ✓ Disclaimer
- 2 Details
- 3 Notifications
- 4 Summary

Fill in your Application Details
We'll generate a key for you.

Application Name *

Category * Select Category

Products * Select products enabled for this app

Application Role * Select Application Role

Description *

- We highly recommend creating a dedicated custom role with **only** the permissions required for the Application to function.
- Select the minimum set of Products the App needs to access to function.

6. Should we need to contact you regarding this API application, please provide details for a **Technical Point of Contact**.

Add Mimecast API 2.0 Application

✓ Disclaimer

✓ Details

3 Notifications

4 Summary

Notification Settings
We'll generate a key for you.

Technical Point of Contact * Security Operations Centre

Email * soc@mycompany.com

“ Mimecast recommends a group rather than an individual contact.

7. Review the Summary information for the API application and click on **Add** if you are happy to proceed with creating the application.

Add Mimecast API 2.0 Application

- ✓ Disclaimer
- ✓ Details
- ✓ Notifications
- 4 Summary

Review your information

Details

Application Name

Threat Management

Category

XDR Integration

Products

Email Security Cloud Gateway, Policy Management, Threat Management, Security Events, Audit Events, User and Group Management, Account Management

Application Role

Basic Administrator

Description

Threat Management app requested by SOC team, for retrieving malware events from Mimecast.

Notifications

Technical Point of Contact

Security Operations Centre

Email

soc@mycompany.com

Edit

Edit

8. The wizard completes and displays a pop-up window including your Client ID and Client Secret key data, where you can copy and save the credentials for the API application.

Credentials for 'Threat Management'

Copy your application credentials to a safe place

⚠

Do not share application credentials.

Client Id

👁📄

Client Secret

👁📄

Close

Base URL (Mimecast API v2)

To transition from your current API 1.0 URLs to API 2.0, we provide three API gateway options tailored to fulfill your performance, compliance, and data residency requirements:

- **Global URL:** The global API URL api.services.mimecast.com which serves traffic from the nearest instance ensuring reduced latency and enhanced performance.

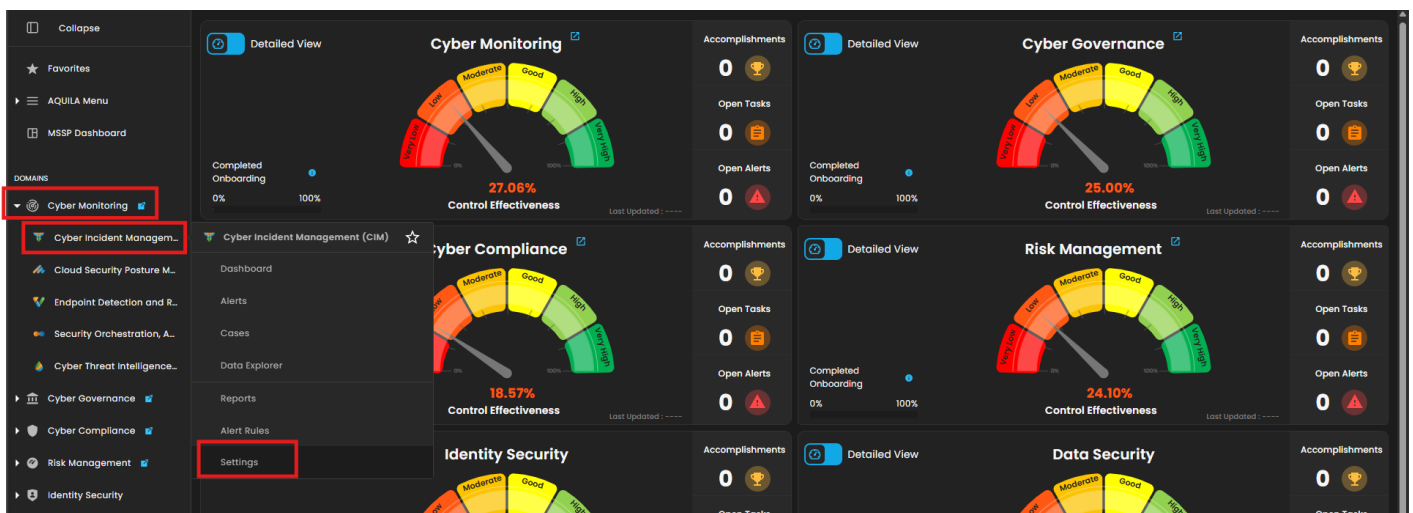
- **UK Instance URL:** For compliance and data residency requirements, customers can choose to process traffic via the UK instance using the regional URL: **uk-api.services.mimecast.com**. This ensures API traffic is only processed within the UK instance of the Apigee Gateway.
- **US Instance URL:** Similarly, customers with compliance or residency requirements in the US can use **us-api.services.mimecast.com** to process API traffic exclusively through the US instance of the Apigee Gateway.

Factor	Global URL	UK Instance URL	US Instance URL
URL Details	api.services.mimecast.com	uk-api.services.mimecast.com	us-api.services.mimecast.com
Availability	☐ Auto failover for high uptime	☒ No failover - requests fail if UK instance is down	☒ No failover - requests fail if US instance is down

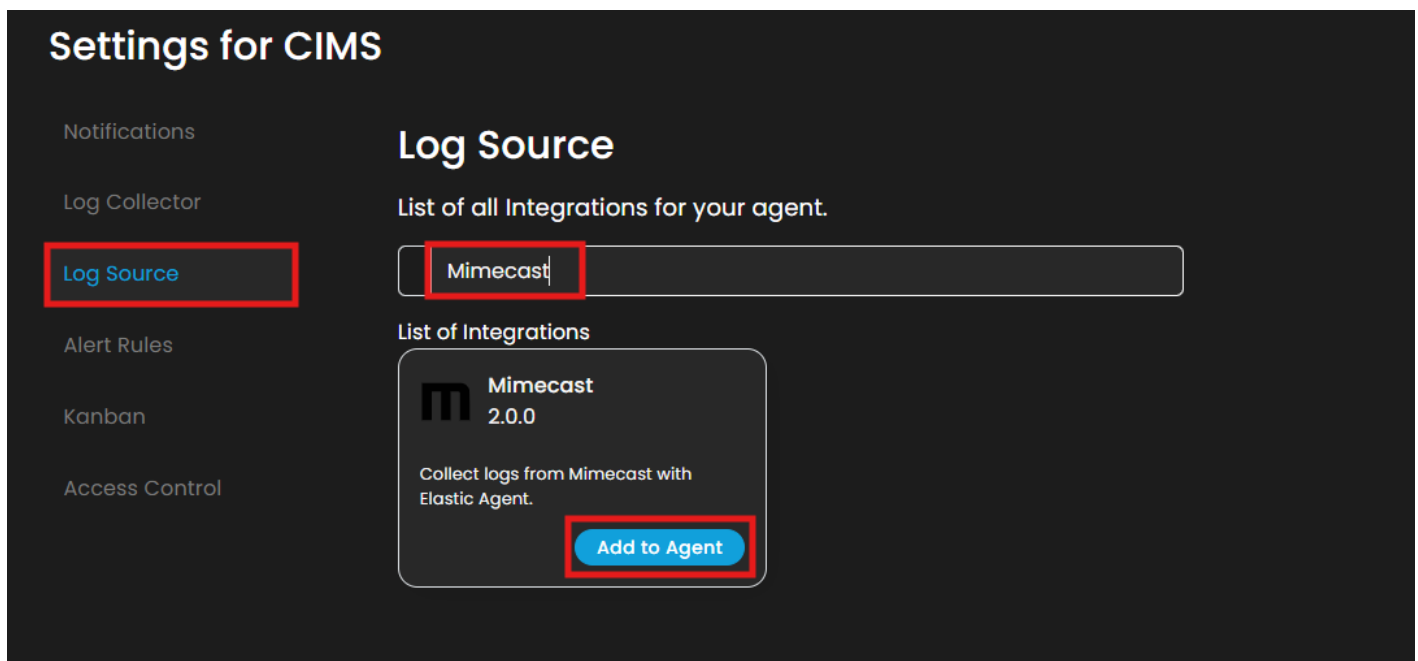
Aquila Integration Configuration

AQUILA – Mimecast Integration

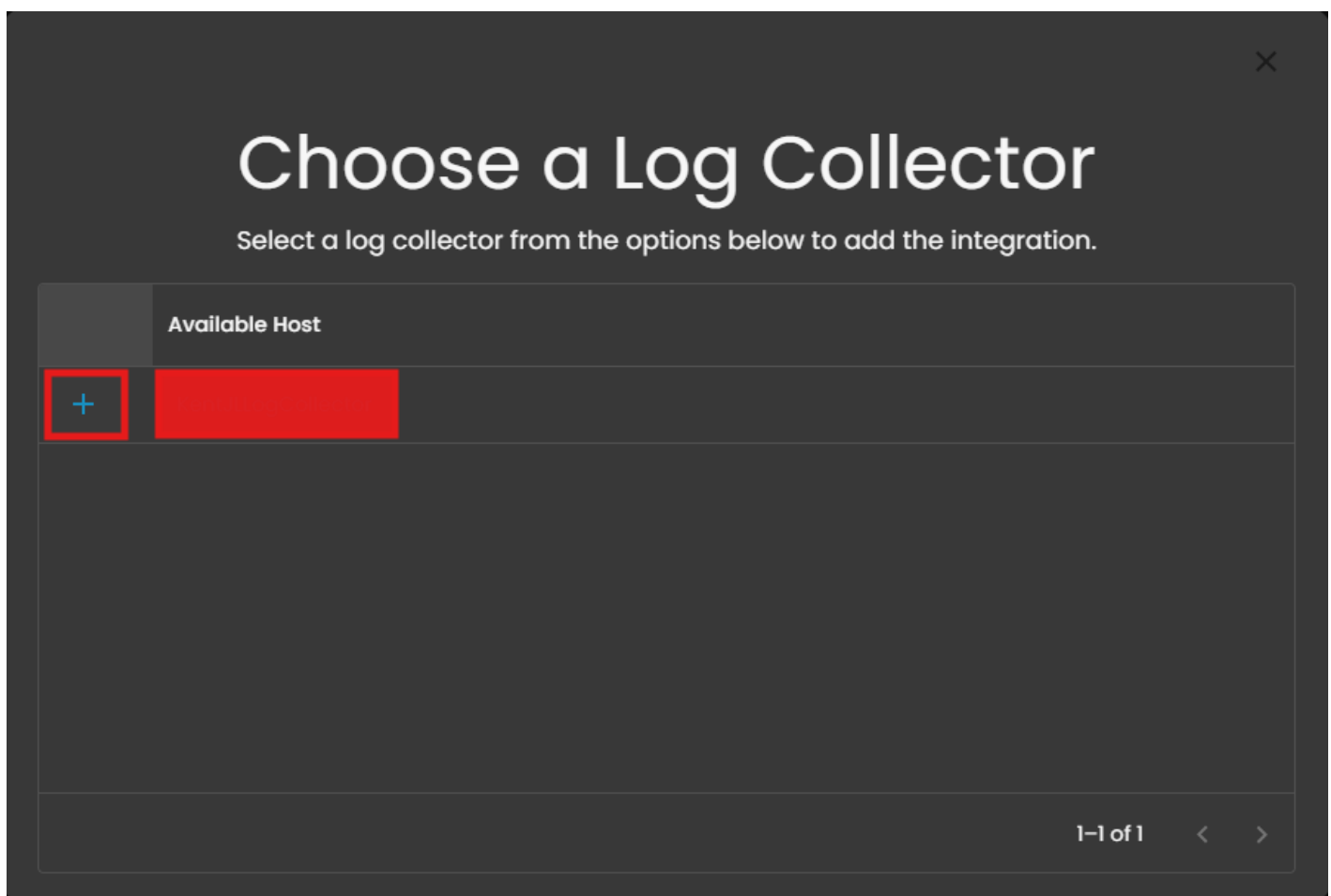
1. Log in to AQUILA click here - [CyTech - AQUILA](#). Choose **Cyber Monitoring -> Cyber Incident Management (CIM) -> Settings**.



2. Navigate through **Log Source -> Search Bar (Search the Source to Add) -> Add to Agent**.



3. Choose your **Log Collector**. (If you not yet installed your **Log Collector** please refer to this link - [Log Collector Installation.](#))



4. In the integration settings follow the instructions given below.

- Click the **drop-down arrow** to display the contents needed for the integration setup.

Integration Settings

Now, please provide the necessary information below.

Chosen Integration: Mimecast

Mimecast	▼
Archive Search Mimecast Logs	▼
Audit Events Mimecast Logs	▼
DLP Mimecast Logs	▼
Mimecast Message Release	▼
SIEM Mimecast Logs	▼



Next

- Upon clicking the drop-down arrow, disable the **v1 API**.

×

Chosen Integration: Mimecast

Mimecast

^

☒ Mimecast v1 API

Collect logs from Mimecast API v1 Endpoints

API URL *

API URL

Application Key for v1 API Endpoints *

Specifies application key for user.

Application ID for v1 API Endpoints *

Set the Application Id.

Access Key for v1 API Endpoints *

Next

- This integration we will use the **v2 API**. Input the required Fields: **Client ID**, **Client Secret** and **API URL (Mimecast API v2 base URL)**.

×

☒ Mimecast v2 API

Collect logs from Mimecast API v2 Endpoints

API URL *

API URL.

Client ID for v2 API Endpoints *

Set Client ID.

Client Secret for v2 API Endpoints *

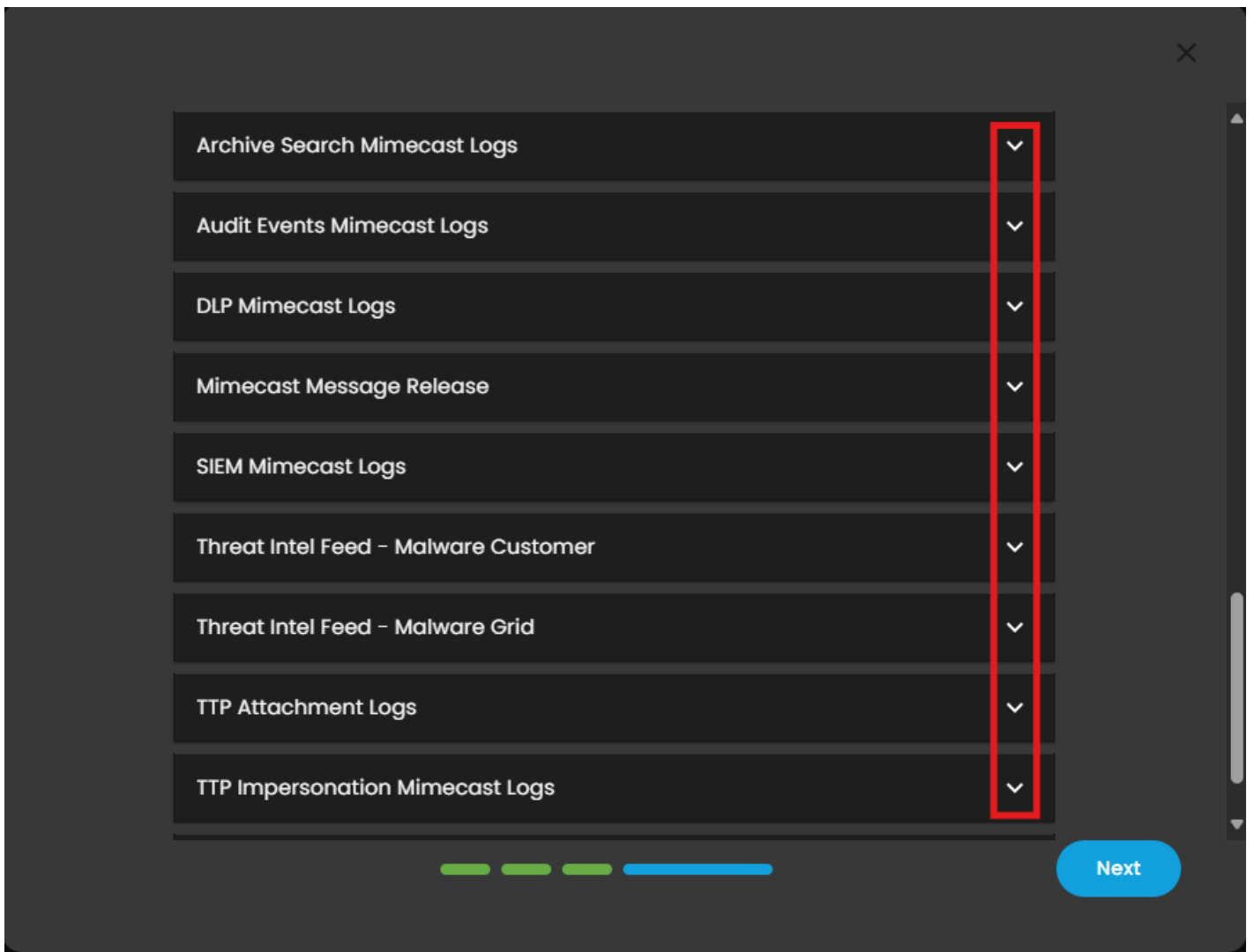
Set Client Secret.

Archive Search Mimecast Logs

▼

Next

- Click the drop-down arrow on all the other fields.



- Click the Tags text field and add the 2 examples.



Archive Search Logs

Collect archive search logs

Interval *

5m

Duration between requests to the API. Supported units for this parameter are h/m/s.

Tags *

Enter Tags

forwarded

mimecast-archive-search-logs

Archive Search Logs

Collect archive search logs

Interval *

5m

Duration between requests to the API. Supported units for this parameter are h/m/s.

Initial Interval *



Next

×

Archive Search Mimecast Logs

^

Archive Search Logs

Collect archive search logs

Interval ^{*}

5m

Duration between requests to the API. Supported units for this parameter are h/m/s.

Tags

forwarded

×

mimecast-archive-search-logs

×

Enter Tags

×

☐ Preserve original event ^{*}

Preserves a raw copy of the original event, added to the field `event.original`

Archive Search Logs

Collect archive search logs

Interval ^{*}

5m

Next

- Finally, click **Next** to install the log source integration.

×

5m

Duration between requests to the API. Supported units for this parameter are h/m/s.

Initial Interval *

24h

Initial interval for the first API call. Defaults to 24 hours. Supported units for this parameter are h/m/s.

Batch Size *

100

Batch size for the response of the Mimecast API.

Tags *

forwarded ×

mimecast-ttp-url ×

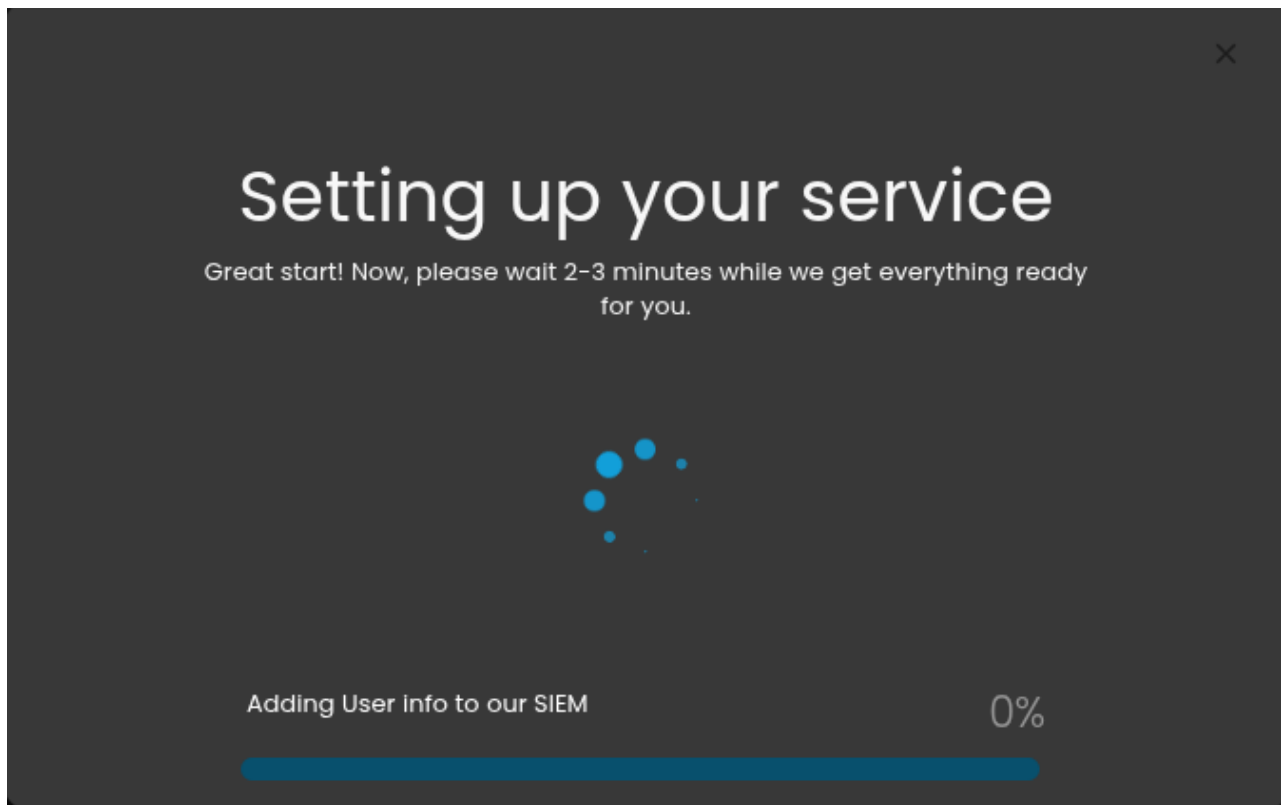
Enter Tags

☐ Preserve original event *

Preserves a raw copy of the original event, added to the field `event.original`

Next

5. Wait for the **Successful** window to display, this will confirm the successful integration.



Reference Links:

[API & Integrations - Managing API 2.0 for Cloud Gateway](#)

[Update Base URL](#)

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #7

Created 17 July 2025 23:40:52

Updated 24 July 2025 23:22:15 by Jeff Saguing