Cisco Secure Email

Secure Email Threat Defense API Guide

May 2023

Table of Contents

Overview

Cisco Secure Email Threat Defense APIs allow partners and customers to programmatically access and consume data in a secure and scalable manner. They can use the Secure Email Threat Defense API to create their own reports and dashboards to better manage their clients. This REST-based API will help users get message information available in the Secure Email Threat Defense UI and filter out the messages based on different parameters in the API requests.

API Features

Using the Secure Email Threat Defense API features is a two-step process:

Step 1: **Authentication**

This API will allow you to use the generated client credentials in the Secure Email Threat Defense Administration page to create a JWT token, which will be used on the search API.

Before we can send a Message Search query to Secure Email Threat Defense, we must first obtain the authorization token that will be used in the Message Search query.

Step 2: **Message Search**

The Secure Email Threat Defense message search API allows you to search Secure Email Threat Defense for message information, within a time period, with using filters to narrow the results.

Responses

Using the API may produce different responses for the HTTP request. Here are the some of the expected results:

Code	Message	Description
200	Success	The request was processed and executed.
400	Bad Request	The request is not formed correctly or there is not enough information to authenticate the request.
401	Unauthorized	Authorization information is either missing, incomplete or incorrect.
404	Not Found	The requested resource does not exist.
429	Too many request	Please wait and retry.
500	Internal Server Error	An unexpected error has occurred. Please retry later or contact support if the issue persists.

Rate Limits

Requests may be throttled when the load on the server is very high. When that happens, please wait a few seconds before retrying. The over all rate limit threshold, and per customer threshold may be adjusted in the future.

Secure Email Threat Defense API Endpoints

The Authorization and Message Search APIs mentioned use a URL that begins with the FQDN of the Secure Email Threat Defense API Servers. There is a European and an American API service and you would use the corresponding service depending on whether your Secure Email Threat Defense instance is in the Americas or EMEA data center.

Americas:

https://api.us.etd.cisco.com/

European:

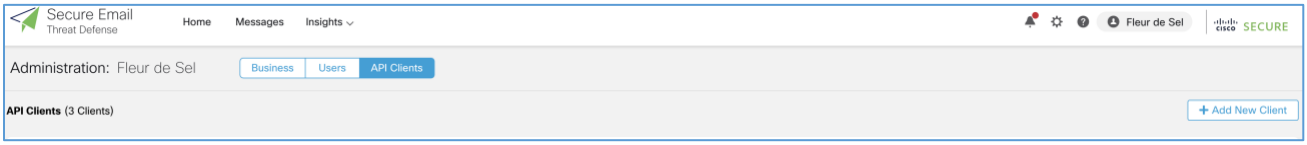
https://api.de.etd.cisco.com/

Authentication API

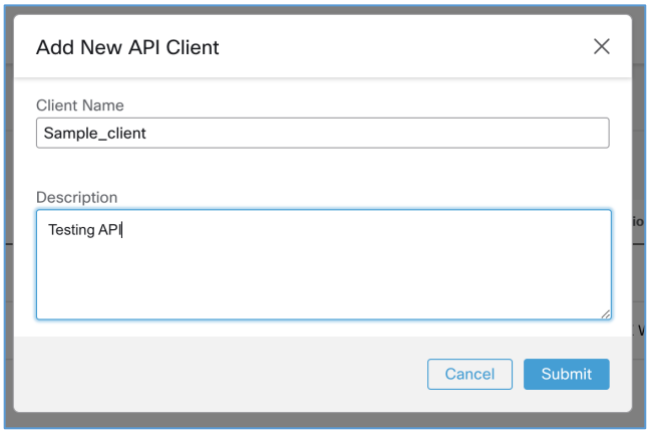
The Message Search API requires an authentication token in each request. The token is obtained through an HTTPS POST to the Secure Email Threat Defense API servers to a specific URL and by passing in a Secure Email Threat Defense Client ID and Client Secret.

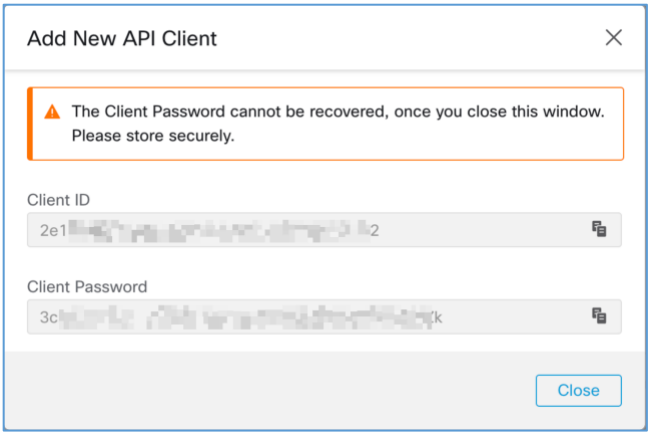
You will need to log in to Secure Email Threat Defense and create your API Client Credentials. Only super-admin and admin users in Secure Email Threat Defense can generate client credentials. To create the credentials, follow the following steps:

1. Log into the Secure Email Threat Defense UI.
2. Navigate to Settings > Administration > API Clients.



3. To generate a client ID and secret, click Add New Client.
4. Input the client name and description (optional), then click Submit. This will generate your Client ID and Password. Note - You must copy and save the Client Password. It cannot be recovered by Cisco.





5. You can also delete client ids from the API clients page in the UI one at a time.

With valid credentials, you can use your region endpoint to get the JWT token using the relative URL /v1/oauth/token.

Available authentication API endpoints are:

Americas API endpoint: https://api.us.etd.cisco.com/v1/oauth/token

Europe API endpoint: https://api.de.etd.cisco.com/v1/oauth/token

Example of an authentication API request using CURL:

curl -X POST \

https://api.us.etd.cisco.com/v1/oauth/token -u <client_id>:<client_secret>

Note: The JWT expiration period is 60 minutes. If the token is expired, or about to expire, user needs to make /token call again to generate new token and to proceed with Message Search API.

Message Search API

By using the previously created JWT, you can use the Message Search API to retrieve message information from Secure Email Threat Defense.

Available Message Search API endpoints are:

Americas API endpoint: https://api.us.etd.cisco.com/v1/messages/search

Europe API endpoint: https://api.de.etd.cisco.com/v1/messages/search

Example of a Message Search API request using CURL:

```
curl -X POST \
https:// api.us.etd.cisco.com/v1/messages/search -H 'authorization: Bearer < Token Here > \
-H 'cache-control: no-cache' \
-H 'content-type: application/json' \
-d '{"timestamp":["2023-04-01T09:34:05.361Z","2023-04-19T17:34:05.361Z"]}'
```

Request Body

The request body acts as the search filters to be used on the search query.

These are the filters currently allowed on the Message Search API:

```
{
  "timestamp": [ "string", "string" ],
  "verdicts": ["spam", "malicious", "phishing", "graymail", "neutral", "bec", "scam"],
  "subject": "string",
  "filename": "string",
  "fileSHA256": "string",
  "directions": ['incoming', 'outgoing', 'internal', 'mixed'],
  "url": "string",
  "pageToken": "string" ,
  “pageSize”: integer,
}
```

Field name	Input Type	Description
1. timestamp	["string", "string"]	• **Timestamp is a mandatory field in the request body.** • It is ISO 8601 formatted date-time string range e.g. ["2023-02-01T12:00:00Z", "2023-02-20T23:59:59Z"]. • The start and end dates are inclusive. • Timestamps should be in the UTC timezone only. • The first timestamp should be smaller than the second.
2. verdicts	["spam", "malicious", "phishing", "graymail", "neutral", "bec", "scam"]	• Search for messages with specific verdicts
3. subject	"string"	• Search emails with subject beginning with input
4. filename	"string"	• Search using filename of attachment. It does an exact match
5. fileSHA256	"string"	• Search using SHA256 hash of attachment file. It does an exact match
6. directions	['incoming', 'outgoing', 'internal', 'mixed']	• Filter emails matching provided directions • It requires a minimum of 1 and maximum 4.
7. url	"string"	• Search emails containing url beginning with input
8. pageToken	"string"	• Use the value present in nextPageToken field in the response object.

Note - The current page limit is 100 messages per request. You can use the nextPage token to navigate if you get more than 100 results on your query

Response Format

The Message Search API results object format is a JSON structure. The fields returned in this object will depend on the message information (convicted or not, direction, without files/URLs, others).

This is the expected response format:


```
{
    "nextPageToken": "timestamp:id of the last document, to be used to request for next page of data",
    "totalSize": 0,
    "data": {
        "messages": [{
            "id": "string",
            "rule": {
                "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
                "type": "allowlist",
                "version": "string"
            },
            "timestamp": "<delivery timestamp>",
            "clientIP": "<sender ip address>",
            "serverIP": "<mail server>",
            "xOriginatingIP": "198.51.100.42",
            "internetMessageId": "<messageID>",
            "toAddresses": [
                "<recipient email address>"
            ],
            "fromAddress": "<header from>",
            "envelopeFrom": "<envelope from>",
            "returnPath": "<return path>",
            "bccAddresses": [
                "user@example.com"
            ],
            "ccAddresses": [
                "user@example.com"
            ],
            "mailboxes": [
                "<recipient mailbox address>"
            ],
            "replyTo": [
                "<reply to address>"
            ],
            "subject": "<message subject>",
            "urls": ["url1", "url2"],
            "attachments": [{
                "filename": "<filename>",
                "SHA256": "<file hash>"
            }],
            "verdict": {
```

```
                "originalVerdict": "<original veridict. Values can be 'spam', 'malicious', 'phishing', 'graymail', 'empty',
'neutral', 'bec','scam'>",
                "userId": "<if the message was manually reclassified, the userID will show up here>",
                "category": "<category of the message>",
                "timestamp": "<timestamp for the detection>",
                "isRetroVerdict": true,
                "ruleId": "string",
                "ruleType": "string",
                "businessRisk": "<sub-category of the message>",
                "techniques": [{
                    "type": "<detection name>",
                    "severity": "<severety level. Values can be 'high', 'medium', 'null'>",
                    "description": "Email content has a bad reputation"
                }]
            },
            "direction": "<message direction. Can be 'incoming', 'outgoing', 'internal'>",
            "action": {
                "folder": "<destination folder. Can be 'junkemail', 'quarantine','deleteditems",
                "type": "<action taken. Can be 'move', 'delete'>",
                "timestamp": "<timestamp of the action>",
                "isAutoRemediated": < remediation occured automatically.Value can be 'true' >
            },
            "domain": "<recipient domain>",
            "senderName": "string",
            "secureEmailGateway": {
                "headerName": "string",
                "originalCip": "198.51.100.42"
            }
        }]
    }
}
```


Backward Compatibility

New request and response fields may be added in future, but breaking changes such as removing of fields will be done in a planned way so customers have time to adjust their api calls.

Troubleshooting

While using the Secure Email Threat Defense APIs we may find some issues or error codes. This section will help you identify those issues so you can easily solve them:

Response code	Response Body	Description
1. 400	Bad Request	You are using an invalid credentials. Please create new client credentials on ETD admin page
2. 401	"Token expired, generate new token to proceed"	Your JWT token has expired. Please create a new one
3. 400	“Invalid date range”	The date-time interval you are using in your query is higher than the 32 days allowed. Please adjust and perform the query again
4. 400	“Unable to deserialize request body”	Please make sure you are using the correct values and format on your request body

Additional Resources

Please leverage the following resources to get more information about Secure Email Threat Defense:

Cisco Secure Email Threat Defense Datasheet

https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/secure-email-threat-defense-ds.html

Cisco Secure Email Threat Defense User Guide

https://www.cisco.com/c/en/us/td/docs/security/email-threat-defense/user-guide/secure-email-threat-defense-user-guide.html

Cisco Secure Email Threat Defense Release Notes

https://www.cisco.com/c/en/us/td/docs/security/email-threat-defense/release-notes/secure-email-threat-defense-release-notes.html

Cisco Secure Email Threat Defense Trial Request

https://cs.co/etd-trial