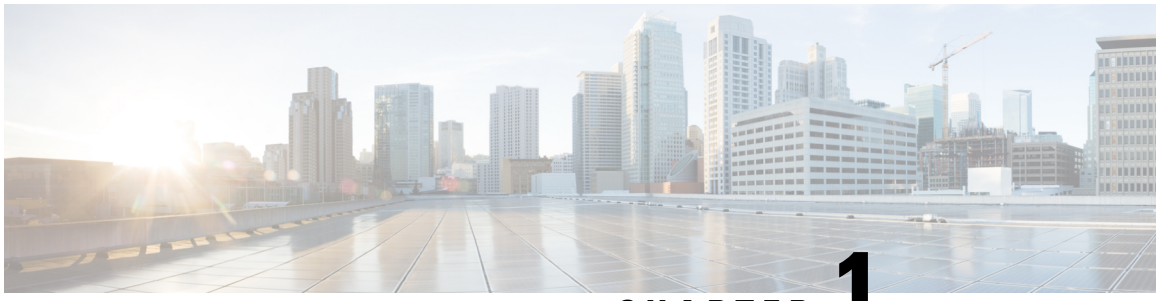
AsyncOS 15.0 API for Cisco Secure Email Gateway - Getting Started Guide - GD (General Deployment)

First Published: 2023-05-04

Last Modified: 2023-08-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview of AsyncOS API for Cisco Secure Email Gateway

The AsyncOS API for Cisco Secure Email Gateway (or AsyncOS API) is a representational state transfer (REST) based set of operations that provide secure and authenticated access to the email gateway reports, report counters, and tracking. You can retrieve the email gateway reporting and tracking data using the API. In this release you can query for configuration information. Posting configuration changes is not supported in this release.

For more information, refer to the Swagger API help. To view the API help, access the new web interface of the email gateway, click the help icon on the top right corner of the page and select **API Help: Swagger**.

This chapter contains the following sections:

Prerequisites for Using AsyncOS API

To use AsyncOS API, you need the knowledge of:

- • HTTP, which is the protocol used for API transactions. Secure communication over TLS.
  - JavaScript Object Notation (JSON), which the API uses to construct resource representations.
  - JSON Web Token (JWT)
- A client or programming library that initiates requests and receives responses from the AsyncOS API using HTTP or HTTPS, for example, cURL. The client or programming library must support JSON to interpret the response from the API.
- Authorization to access the AsyncOS API. See Authorization, on page 5.
- AsyncOS API enabled using web interface or CLI. See Enabling AsyncOS API, on page 2.

Note Version 1.0 APIs are not supported from Cisco Email Security 13.0 release and later. Instead version 2.0 APIs are used.

Enabling AsyncOS API

Before You Begin

Make sure that you are authorized to access the IP Interfaces page on the web interface or the `interfaceconfig` command on CLI. Only administrators, email administrators, cloud administrators, and operators are authorized.

You can also enable the AsyncOS API using the `interfaceconfig` command in CLI.

Step 1 Log in to the web interface.

Step 2 Choose **Network** > **IP Interfaces**.

Step 3 Edit the Management interface.

Note
- You can enable AsyncOS API on any IP interface. However, Cisco recommends that you enable AsyncOS API on the Management interface.
- You must not enable APIs on multiple management interface.

Step 4 Under the AsyncOS API (Monitoring) section, depending on your requirements, select HTTP, HTTPS, or both and the ports to use.

Note AsyncOS API communicates using HTTP / 1.1.

If you have selected HTTPS and you want to use your own certificate for secure communication, see Securely Communicating with AsyncOS API, on page 2.

Note Cisco recommends that you always use HTTPS in the production environment. Use HTTP only for troubleshooting and testing the API.

Step 5 Submit and commit your changes.

Securely Communicating with AsyncOS API

You can communicate with AsyncOS API over secure HTTP using your own certificate.

Note Do not perform this procedure if you are already running the web interface over HTTPS and using your own certificate for secure communication. AsyncOS API uses the same certificate as web interface, for communicating over HTTPS.

Step 1 Set up a certificate using the `certconfig` command in the CLI. For instructions, refer the User Guide or Online Help.

Step 2 Change the HTTPS certificate used by the IP interface to your certificate using the `interfaceconfig` command in CLI. For instructions, refer the User Guide or Online Help.

Step 3 Submit and commit your changes.

AsyncOS API Authentication and Authorization

This section explains about the authentication methods, the user roles which can access APIs, and how to query for APIs accessible to a user.

- Authentication, on page 3
- Authorization, on page 5
- Retrieving APIs Accessible to a User Role, on page 166

Authentication

Submit the email gateway's username and password with all the requests to the API, in the Base64-encoded format or with a JSON Web Token. The user inactivity timeout settings in the email gateway apply to the validity of a JWT. If a request does not include valid credentials in the Authorization header, the API sends a 401 error message. You can use any base64 library to convert your credentials into base64-encoded format.

Note The email gateway allows you to invoke AsyncOS APIs by including access tokens that are retrieved from Identity Providers (IDPs) that support OpenID Connect 1.0. For more details on how to use AsyncOS APIs with external IDPs, see the "System Administration" chapter of the *User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway*.

Authenticating API Queries with JSON Web Token

You can generate a JSON Web Token (JWT) and use it with your API queries.

Note The user inactivity timeout settings in the email gateway applies to the validity of a JWT. The email gateway checks every API query with a JWT, for its time validity. If a JWT is found to be within 5 minutes of time validity, after which it will time out, a new refresh JWT is sent with the response header. You must use this new refresh JWT with API queries, or generate a new one.

Synopsis	`POST /esa/api/v2.0/login`
	Use the syntax below for two factor authentications:
	`POST /esa/api/v2.0/login/two_factor`

Body Parameters	Use Base64 encoded credentials. `{ "data": { "userName":"YWRtaW4=", "passphrase":"aXJvbnBvcnQ=" } }`	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

This example shows a query to log in with Base64 encoded credentials, and generate a JWT.

Sample Request

```
POST /esa/api/v2.0/login
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 95
Connection: keep-alive
{
    "data":
    {
        "userName":"YWRtaW4=",
        "passphrase":"aXJvbnBvcnQ="
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 26 Nov 2018 07:22:47 GMT
Content-type: application/json
Content-Length: 618
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "userName": "admin",
        "is2FactorRedirectRequired": "false",
        "role": "Administrator",
        "email": [],
        "jwtToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwiaXM
         yRmFjdG9yQ2hlY2tSZXF1aXJlZCI6ZmFsc2UsImNvb2tpZSI6IlRucEZOVTFFWTNwTlZFMDlDanRMYVR
         oeENqdFpiV1J6VFVSQk5VMURNWGRpTWxGMVdUSnNlbGt5T0hWWk1qbDBUMnBaZDA5RVFUMEtcbk8xVkh
         PWHBrUnpGb1lteEtNV0p1VW5CaVYxVjJUbmswTUV4cVFUMEtPMVJVUlhkTlJsazNUVlJKZFUxRE5IZE1
         WRWw1VFdwek1FMXFcblNUVlNhazVDVDBWRk1rOUVaM2xTUlVreVRYcGtSazFwTVVSTlZFMHpUbFZXUjA1
```

```
    }
}
```

Authorization

The AsyncOS API is a role based system, the scope of API queries is defined by the role of the user. The email gateway users with the following roles can access the AsyncOS API:

- Administrator
- Operator
- Technician
- Read-Only Operator
- Guest
- URL Filtering Administrator
- Email Administrator
- Help Desk User

Note

- Externally authenticated users can access the API.
- Custom roles, delegated by the administrator can also access the APIs.

AsyncOS API Requests and Responses

AsyncOS API Requests

Requests made to the API have the following characteristics:

- Requests are sent over HTTP or HTTPS
- Each request must contain a valid URI in the following format:

  `http://{appliance}:{port}/esa/api/v2.0/{resource}/{resource_attributes}`

  `https://{appliance}:{port}/esa/api/v2.0/{resource}/{resource_attributes}`

  where:

  - `{appliance}:{port}`

    is the FQDN or the IP address of the email gateway and the TCP port number on which the email gateway is listening.
  - `{resource}`

is the resource you are attempting to access, for example, reports, tracking, quarantine, configuration, or other counters.

- `{resource_attributes}`

  are the supported attributes for a resource, for example, duration, and so on.

- Each request must contain user credentials, or a valid authorization header.
- Each request must be set to accept:

```
application/json
```

- Requests sent over HTTPS (using your own certificate) must contain your CA certificate. For example, in case of cURL, you can specify the CA certificate in the API request as follows:

```
curl --cacert <ca_cert.crt> -u"username:password"
https://<fqdn>:<port>/esa/api/v2.0/{resource}/{resource_attributes}
```

Note API requests are case sensitive and should be entered as shown in this guide.

AsyncOS API Responses

This section explains the key components of the responses, and various HTTP error codes.

- Key Components of Responses, on page 6
- HTTP Response Codes, on page 7

Key Components of Responses

Components		Values	Description
Status Code and Reason		See HTTP Response Codes, on page 7.	HTTP response code and the reason.
Message Header	Content-Type	`application/json`	Indicates the format of the message body.
	Content-Length	n/a	The length of the response body in octets.
	Connection	`close`	Options that are desired for the connection.

Components	Values	Description

Message Body	n/a	The message body is in the format defined by the Content-Type header. The following are the components of the message body:
		1. URI. The URI you specified in the request to the API.
		Example
		`"esa/api/v2.0/config/"`
		2. Counter group and/or counter name
		Example
		`reporting/mail_security_summary`
		3. Query parameters
		Example
		`startDate=2017-01-30T00:00:00.000Z&endDate=2018-01-30T14:00:00.000Z`
		4. Error (Only for Error Events). This component includes three subcomponents—message, code, and explanation.
		Example
		`"error": {"message": "Unexpected attribute - starts_with.","code": "404", "explanation": "404 = Nothing matches the given URI."}`
		If the message body contains empty braces ({}), it means that the API could not find any records matching the query.

HTTP Response Codes

The following is a list of HTTP response codes returned by AsyncOS API:

- 200
- 202
- 300
- 301
- 307
- 400
- 401
- 403
- 404

- 406
- 413
- 414
- 500
- 501
- 503
- 505

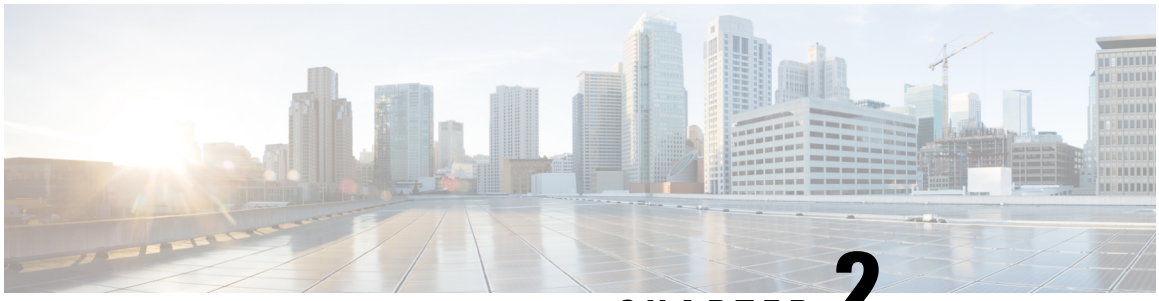
For descriptions of these HTTP response codes, refer the following RFCs:

- RFC1945
- RFC7231

AsyncOS API Capabilities

You can use the AsyncOS API to retrieve information in the following categories:

- APIs for Secure Email, on page 9
- General Purpose APIs, on page 165



CHAPTER 2

APIs for Secure Email

Reporting APIs

Reporting queries can be used to fetch data from reports, for all counters under a specific group, or for a specific counter.

Synopsis	`GET /api/v2.0/reporting/report?resource_attribute` `GET /api/v2.0/reporting/report/counter?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. `startDate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Aggregate report(s) for the specified duration. **Note** The duration attribute supports only 00 as value in the minutes (mm) and seconds (ss) parameters.
	Query Type	• `query_type=graph` Receive data that can be represented as graphs. • `query_type=export` Receive data in the export format.
	Sorting	You should use both these parameters. If you use either, you will not receive data in the response. • `orderBy=<value>` Specify the attribute by which to order the data in the response. For example, `orderBy=total_clean_recipients` • `orderDir=<value>` Specify sort direction. The valid options are: • `asc` Order the results in ascending order. • `desc` Order the results in descending order.
	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.
	Data Retrieval Option	• `top=<value>` Specify the number of records with the highest values to return.
	Filtering	

		Filter parameters restrict the data to be included the response. • `filterValue=<value>` The value to search for. • `filterBy=<value>` Filter the data to be retrieved according to the filter property and value. • `filterOperator=<value>` The valid options are: • `begins_with` Filter the response data based on the value specified. This is not an exact value. • `is` Filter the response data based on the exact value specified.
	Device	• `device_group_name=<value>` Specify the device group name. • `device_type=esa` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter. • `device_name=<value>` Specify the device name.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Examples

Examples for the types of reporting queries are shown below:

• Retrieving All Incoming Messages that Matched a Configured Mail Policy, on page 20
• Retrieving All Outgoing Messages that Matched a Configured Mail Policy, on page 21

Retrieving a Single Value for a Counter

This example shows a query to retrieve the value of a specific counter from a counter group, with the device name and type.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_incoming_traffic_summary/detected_amp?
startDate=2016-09-10T19:00:00.000Z&endDate=2018-09-24T23:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 15:58:29 GMT
Content-type: application/json
Content-Length: 96
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": -1},
    "data": {
        "type": "detected_amp",
        "resultSet": {
            "detected_amp": 11}
    }
}
```

Retrieving Multiple Values for a Counter

This example shows a query to retrieve values of all counters of a counter group, with the device group name and device type.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_incoming_traffic_summary?startDate=2016
-09-10T19:00:00.000Z&endDate=2018-09-24T23:00:00.000Z&device_type=esa
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 17:39:34 GMT
Content-type: application/json
Content-Length: 580
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"meta": {"totalCount": -1}, "data":
{"type":
"mail_incoming_traffic_summary",
"resultSet": [{"verif_decrypt_success":5},
{"detected_virus": 13},
{"verif_decrypt_fail": 5},
{"threat_content_filter": 10},
{"total_graymail_recipients": 9},
{"blocked_invalid_recipient": 2},
{"ims_spam_increment_over_case": 0},
{"blocked_dmarc": 0},
{"blocked_sdr": 0},
{"marketing_mail": 6},
{"detected_amp": 2},
{"bulk_mail": 2},
{"total_recipients": 159},
{"social_mail": 1},
{"detected_spam": 30},
{"total_clean_recipients": 83},
{"malicious_url": 6},
{"total_threat_recipients": 67},
{"blocked_reputation": 10}]}}
```

Retrieving Single Values for Each Counter in a Counter Group

A counter group may have multiple counters. This example shows a query to retrieve single values for each counter in a counter group, with order, device type and top parameters.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_content_filter_incoming/recipients
_matched?startDate=2017-09-10T19:00:00.000Z&endDate=2018-09-24T23:00:00.000Z&device_type
=esa&orderDir=desc&orderBy=recipients_matched&top=2
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 18:17:29 GMT
Content-type: application/json
Content-Length: 153
Connection: close
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "recipients_matched",
        "resultSet": {
            "recipients_matched": [
                {"url_rep_neutral": 16},
                {"url_category": 8}
            ]
        }
    }
}
```

Retrieving Multiple Values for Multiple Counters

This example shows a query to retrieve multiple values for multiple counters, with offset, limit and device type parameters.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_incoming_domain_detail?startDate=2017-09-10T19:00:00.000Z
&endDate=2018-09-24T23:00:00.000Z&device_type=esa&offset=1&limit=2
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 18:25:28 GMT
Content-type: application/json
Content-Length: 1934
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "mail_incoming_domain_detail",
        "resultSet": {
            "conn_tls_total": [
                {"pphosted.com": 0},
                {"vm30bsd0004.ibqa": 5}
            ],
            "conn_tls_opt_success": [
```

```
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 0}
    ],
    "conn_tls_opt_fail": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 0}
    ],
    "blocked_invalid_recipient": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 1}
    ],
    "last_sender_group_name": [
        {"pphosted.com": "UNKNOWNLIST"},
        {"vm30bsd0004.ibqa": "UNKNOWNLIST"}
    ],
    "detected_amp": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 2}
    ],
    "social_mail": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 1}
    ],
    "detected_spam": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 25}
    ],
    "blocked_reputation": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 5}
    ],
    "total_throttled_recipients": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 2}
    ],
    "total_accepted_connections": [
        {"pphosted.com": 2},
        {"vm30bsd0004.ibqa": 119}
    ],...


      ...
    "threat_content_filter": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 5}
    ],
    "marketing_mail": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 5}
    ],
    "blocked_dmarc": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 0}
    ],

    "conn_tls_success": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 5}
    ],
    "total_recipients": [
        {"pphosted.com": 2},
        {"vm30bsd0004.ibqa": 112}
    ],
    "conn_tls_fail": [
```

```
                {"pphosted.com": 0},
                {"vm30bsd0004.ibqa": 0}
            ],
            "total_threat_recipients": [
                {"pphosted.com": 0},
                {"vm30bsd0004.ibqa": 49}
            ]
        }
    }
}
```

Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter

This example shows a query to retrieve multiple values for multiple counters (with multiple values for each counter), with filtering, and query type parameters. The graph attribute retrieves time based counter values of counters.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_incoming_ip_hostname_detail?startDate=
2017-09-10T19:00:00.000Z&endDate=2018-09-24T23:00:00.000Z&device_type=esa&filterBy
=ip_address&filterOperator=begins_with&filterValue=10&query_type=graph
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 18:49:42 GMT
Content-type: application/json
Content-Length: 74110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "mail_incoming_ip_hostname_detail",
        "resultSet": {
            "dns_verified": {
                "10.76.68.103": [
                    {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 2},
                    {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 1},
                    ...

                    ...
                    {"2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 1}
                ],
                "10.76.71.211": [
                    {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 1},
                    {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 3},
```

```
                ...

                ...
                {"2017-11-01T00:00:00.000Z to 2017-11-30T23:59:00.000Z": 1},
                {"2017-12-01T00:00:00.000Z to 2017-12-31T23:59:00.000Z": 0}
            ],

                },
                {
                    "2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 0
                }
            ]
        },
        "last_sender_group": {
            "10.76.68.103": [
                {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 4},
                {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 0},
               }
            ],
            "10.76.71.211": [
                {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 2},
                {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 2},

                }
            ]
        },
        "total_threat_recipients": {
            "10.76.68.103": [
                {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 2},
                {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 20},
...

...
                {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 0},

                }
            ]
        },
        "threat_content_filter": {
            "10.76.68.103": [
                {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 0},
                {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 1},
...

...
                }
            ]
        },
        "total_graymail_recipients": {
            "10.76.68.103": [
                {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 0},
                {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 4},
                ...

                ...

                {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 0},
                {"2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 0}
            ]
        },
        "total_clean_recipients": {
            "10.76.68.103": [
                {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 5},
                {"2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 0}
```

```
                ]
            },
            "sbrs_score": {
                "10.76.68.103": [
                    {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 3},
                    ...

                    ...
                    {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 0},
                    {"2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 0}
                ]
            },
            "blocked_reputation": {
                "10.76.68.103": [
                    {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 0},
                ]
            }
        }
    }
}
```

Retrieving Top Incoming Messages that Matched a Configured Mail Policy

The following example shows a query to retrieve the top incoming messages that matched a configured mail policy in your email gateway.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_policy_incoming/recipients_matched?
device_type=esa&endDate=2021-02-26T14:00:00.000Z&startDate=2020-11-27T18:00:00.000Z&top=10
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Accept: application/json, text/plain, */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 435
Content-Type: application/json; charset=UTF-8
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "recipients_matched",
        "resultSet": {
            "recipients_matched": [
                {
                    "Bypass_Blocklist_Policy": 318172
                },
```

```
                {
                    "Test Mail Policy Marketing2Junk": 177994
                },
                {
                    "DEFAULT": 147011
                },
                {
                    "Allow Marketing Newsletters": 28882
                },
                {
                    "Aggressive Spam Scoring": 18605
                },
                {
                    "Allowed_listEmailAddresses": 15177
                },
                {
                    "ampuser": 9463
                },
                {
                    "Block_Inbound_Mail_Westfield": 9436
                },
                {
                    "Bulk Mail Quarantined": 9365
                },
                {
                    "virususer": 9238
                }
            ]
        }
    }
}
```


Retrieving Top Outgoing Messages that Matched a Configured Mail Policy

The following example shows a query to retrieve the top outgoing messages that matched a configured mail policy in your email gateway.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_policy_outgoing/recipients_matched?
device_type=esa&endDate=2021-02-26T14:00:00.000Z&startDate=2020-11-27T18:00:00.000Z&top=10
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Accept: application/json, text/plain, */*
Host: esa.example.com:6080
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 163
Content-Type: application/json; charset=UTF-8
```

```
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "recipients_matched",
        "resultSet": {
            "recipients_matched": [
                {
                    "Block_Outbound_Traffic": 921281
                },
                {
                    "DEFAULT": 23623
                }
            ]
      }
   }
}
```


Retrieving All Incoming Messages that Matched a Configured Mail Policy

The following example shows a query to retrieve all incoming messages that matched a configured mail policy in your email gateway.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_policy_incoming/recipients_matched?
device_type=esa&endDate=2021-02-26T14:00:00.000Z&limit=25&offset=0&startDate=2020-11-27T18:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Accept: application/json, text/plain, */*
Host: esa.example.com:6080
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 547
Content-Type: application/json; charset=UTF-8
```


```
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "recipients_matched",
        "resultSet": {
            "recipients_matched": [
                {
                    "Bypass_Blocklist_Policy": 318172
                },
                {
                    "Test Mail Policy Marketing2Junk": 177994
```

```
                    },
                    {
                        "DEFAULT": 147011
                    },
                    {
                        "Allow Marketing Newsletters": 28882
                    },
                    {
                        "Aggressive Spam Scoring": 18605
                    },
                    {
                        "Allowed_listEmailAddresses": 15177
                    },
                    {
                        "ampuser": 9463
                    },
                    {
                        "Block_Inbound_Mail_Westfield": 9436
                    },
                    {
                        "Bulk Mail Quarantined": 9365
                    },
                    {
                        "virususer": 9238
                    },
                    {
                        "Allow_Marketing_Filter_Spam": 4651
                    },
                    {
                        "Blocklist Email Addresses": 847
                    },
                    {
                        "second-selva": 12
                    },
                    {
                        "second": 2
                    }
                ]
            }
        }
    }
```


Retrieving All Outgoing Messages that Matched a Configured Mail Policy

The following example shows a query to retrieve all outgoing messages that matched a configured mail policy in your email gateway.

Sample Request

```
GET /esa/api/v2.0/reporting/mail_policy_outgoing/recipients_matched?
device_type=esa&endDate=2021-02-26T14:00:00.000Z&limit=25&offset=0&startDate=2020-11-27T18:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Accept: application/json, text/plain, */*
Host: esa.example.com:6080
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
```

```
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 163
Content-Type: application/json; charset=UTF-8
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "recipients_matched",
        "resultSet": {
            "recipients_matched": [
                {
                    "Block_Outbound_Traffic": 921281
                },
                {
                    "DEFAULT": 23623
                }
            ]
        }
    }
}
```

Tracking APIs

You can search for messages or a group of messages that match criteria that you specify. You can retrieve messages' details, rejected connections ' details, and see the status of a specific message in the email stream. The various API categories for tracking are:

Searching for Messages

You can search for messages that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`GET/esa/api/v2.0/message-tracking/messages?resource_attribute`	
Supported Resource Attributes	See AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway Appliances for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve messages, with the time range, message delivery status, email gateway (which processed the emails), offset and limit parameters.

Sample Request

```
GET /esa/api/v2.0/message-tracking/messages?startDate=2018-01-01T00:00:00.000Z&
endDate=2018-11-20T09:36:00.000Z&ciscoHost=All_Hosts&
searchOption=messages&offset=0&limit=20
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Tue, 20 Nov 2018 09:29:48 GMT
Content-type: application/json
Content-Length: 6693
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "num_bad_records": 7,
        "totalCount": 13
    },
    "data": [
        {
            "attributes": {
                "direction": "incoming",
                "icid": 110,
                "senderGroup": "UNKNOWNLIST",
                "sender": "confikr.qa",
                "replyTo": "N/A",
                "timestamp": "15 Oct 2018 08:33:19 (GMT)",
                "hostName": "esa01",
                "subject": "message is good",
```

```
            "mid": [
                110
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "N/A",
            "recipient": [
                "confikr@cisco.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 103,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                104
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "4201@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 105,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                103
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
```

```
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "4417@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 107,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                102
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "3396@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 106,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                101
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "9985@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
```

```
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 100,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                100
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "1023@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 104,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                99
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "182@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 98,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
```

```
                    "replyTo": "N/A",
                    "timestamp": "15 Oct 2018 08:24:39 (GMT)",
                    "hostName": "esa01",
                    "subject": "message is good",
                    "mid": [
                        98
                    ],
                    "isCompleteData": true,
                    "messageStatus": "Delivered",
                    "mailPolicy": [
                        "DEFAULT"
                    ],
                    "senderIp": "10.8.91.18",
                    "verdictChart": "0",
                    "senderDomain": "example.com",
                    "recipient": [
                        "8668@ironport.com"
                    ],
                    "sbrs": "None",
                    "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
                }
            }
        ]
}
```


Rejected Connections

You can retrieve details of rejected connections with different attributes as explained below.

Synopsis	`GET /api/v2.0/message-tracking/messages?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Aggregate report(s) for the specified duration.
	Search Option	• `searchOption=<value>` This attribute has a single permitted value when querying for rejected connections. For example: `searchOption=rejected_connections`
	Sender IP	• `senderIp=<value>` This is a user defined value. Use the IP address of the server which sends messages. For example: `senderIp=10.76.70.112`
	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve details of rejected connections, with the duration, sender IP address, search option, offset and limit attributes.

Sample Request

```
GET /esa/api/v2.0/message-tracking/messages?startDate=2016-11-16T00:00:00.000Z&endDate=
2018-11-16T14:22:00.000Z&senderIp=10.76.70.112&searchOption=rejected_connections&offset=0&limit=20
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Tue, 20 Nov 2018 11:26:22 GMT
Content-type: application/json
Content-Length: 436
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "num_bad_records": 3,
        "totalCount": 1
    },
    "data": [
        {
            "attributes": {
                "icid": 40,
                "timestamp": "10 Jul 2018 03:19:56 (GMT)",
                "hostName": "Name unresolved",
                "rejected": "(ICID 40) SMTP authentication failed for user fail
                 using AUTH mechanism PLAIN with profile failAuthFailoverExists.",
                "messageStatus": "REJECTED",
                "senderIp": "10.76.70.112",
                "senderGroup": "UNKNOWNLIST",
                "sbrs": "None",
                "serialNumber": "848F69E85EEF-6R50TW1"
            }
        }
    ]
}
```

Message Details

You can retrieve details of messages with different attributes as explained below.

Synopsis	`GET /api/v2.0/message-tracking/details?resource_attribute`	
Supported Resource Attributes	See AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve details of a specific message identified by it's icid, mid and the email gateway serial number.

Sample Request

```
GET /esa/api/v2.0/message-tracking/details?endDate=2018-11-16T12:09:00.000Z&icid
=19214&mid=22125&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-16T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: m680q09.ibqa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 10:28:53 GMT
Content-type: application/json
Content-Length: 5271
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "messages": {
            "direction": "outgoing",
            "smtpAuthId": "",
            "sender": "cf_drop_in@vm30bsd0004.ibqa",
            "midHeader": "<20181116111948.15660.34357@vm30bsd0199.ibqa>",
            "timestamp": "16 Nov 2018 11:19:48 (GMT)",
            "showAMP": true,
            "hostName": "c680q07.ibqa (10.76.71.196)",
            "mid": [
                22125
            ],
            "sendingHostSummary": {
                "reverseDnsHostname": "vm30bsd0199.ibqa (verified)",
                "ipAddress": "10.76.70.111",
                "sbrsScore": "not enabled"
            },
            "summary": [
                {
                    "timestamp": "16 Nov 2018 11:19:48 (GMT)",
                    "description": "ICID 19214 sender_group: RELAYLIST sender_ip:
10.76.70.111, sbrs: not enabled",
                    "lastEvent": false
                },
                {
                    "timestamp": "16 Nov 2018 11:19:48 (GMT)",
                    "description": "Protocol SMTP interface Management  (IP 10.76.71.196)
on incoming connection
                     (ICID 19214) from sender IP 10.76.70.111. Reverse DNS  host
vm30bsd0199.ibqa verified yes.",
                    "lastEvent": false
                },
...

...
                {
                    "timestamp": "16 Nov 2018 11:20:12 (GMT)",
                    "description": "Message 22125 scanned by Advanced Malware Protection
engine. Final verdict
```

```
                     : UNKNOWN","lastEvent": false
                },
                {
                    "timestamp": "16 Nov 2018 11:20:12 (GMT)",
                    "description": "Message 22125 contains attachment
'driver_license_germany.txt' (SHA256 7e3dee4dac
                     8f4af561d1108c4b237e5e139bd8d3ddc8518455d3b5fb7e7a70c3).",
                    "lastEvent": false
                },
                {
                    "timestamp": "16 Nov 2018 11:20:12 (GMT)",
                    "description": "Message 22125 attachment  'driver_license_germany.txt'
 scanned by Advanced Malware
                     Protection engine. File Disposition: Unknown",
                    "lastEvent": false
                },
                {
                    "timestamp": "16 Nov 2018 11:20:12 (GMT)",
                    "description": "Message 22125 Delivery Status: DROPPED",
                    "lastEvent": false
                },
                {
                    "timestamp": "16 Nov 2018 11:20:12 (GMT)",
                    "description": "Message 22125 Verdict chart: 01131212",
                    "lastEvent": true
                }
            ],
            "attachments": [
                "driver_license_germany.txt"
            ],
            "messageSize": "765 (Bytes)",
            "isCompleteData": true,
            "showDLP": true,
            "messageStatus": "Dropped by DLP",
            "showURL": false,
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderGroup": "RELAYLIST",
            "recipient": [
                "7799@vm30bsd0004.ibqa"
            ],
            "showSummaryTimeBox": true,
            "subject": "Testing"
        }
    }
}
```


DLP Details

You can retrieve details of DLP of messages with different attributes as explained below.

Synopsis	`GET /api/v2.0/message-tracking/dlp-details?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Aggregate report(s) for the specified duration.
	Serial Number	• `serialNumber=<value>` Specify the serial number of the email gateway.
	Message ID and Injection Connection ID	You should use both these parameters. If you use either, you will not receive data in the response. • `icid=<value>` Specify the icid of the message. • `mid=<value>` Specify the mid of the message.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the DLP details of a specific message identified by it's icid, mid and serial number.

Sample Request

```
GET /esa/api/v2.0/message-tracking/dlp-details?endDate=2018-11-16T11:25:00.000Z&icid=19213
&mid=22124&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Postman-Token: ab16ff7f-847e-4221-a2a2-01de50a33fea
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 10:38:44 GMT
Content-type: application/json
Content-Length: 820
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
    "data": {
        "messages": {
            "direction": "outgoing",
            "smtpAuthId": "",
            "sender": "cf_drop_in@vm30bsd0004.ibqa",
            "midHeader": "<20181116110108.15629.41969@vm30bsd0199.ibqa>",
            "timestamp": "16 Nov 2018 11:01:08 (GMT)",
            "hostName": "c680q07.ibqa (10.76.71.196)",
            "mid": [
                22124
            ],
            "sendingHostSummary": {},
            "attachments": [
                "driver_license_germany.txt"
            ],
            "messageSize": "765 (Bytes)",
            "dlpDetails": {
                "violationSeverity": "HIGH",
                "dlpMatchedContent": [
                    {
                        "messagePartMatch": [
                            {
                                "classifier": "Driver License Numbers (Germany)",
                                "classifierMatch": [
                                    "driver license number: B072RRE2I51"
                                ]
                            }
                        ],
                        "messagePart": "driver_license_germany.txt"
                    }
                ],
                "mid": "22124",
                "riskFactor": 16,
                "dlpPolicy": "Driver License Numbers (Germany)"
            },
            "showDLPDetails": true,
            "senderGroup": "RELAYLIST",
            "recipient": [
                "6406@vm30bsd0004.ibqa"
            ],
            "subject": "Testing"
        }
    }
}
```


AMP Details

You can retrieve Advanced Malware Protection action details of messages with different attributes as explained below.

Synopsis	`GET /api/v2.0/message-tracking/amp-details?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Aggregate report(s) for the specified duration.
	Serial Number	• `serialNumber=<value>` Specify the serial number of the email gateway.
	Message ID and Injection Connection ID	You should use both these parameters. If you use either, you will not receive data in the response. • `icid=<value>` Specify the icid of the message. • `mid=<value>` Specify the mid of the message.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the Advanced Malware Protection action details of a specific message identified by it's icid, mid and serial number.

Sample Request

```
GET /esa/api/v2.0/message-tracking/amp-details?endDate=2018-11-16T11:25:00.000Z&icid=19213
&mid=22124&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 10:51:08 GMT
Content-type: application/json
Content-Length: 1088
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
```

```
    "data": {
        "messages": {
            "showAMPDetails": true,
            "direction": "outgoing",
            "smtpAuthId": "",
            "sender": "cf_drop_in@vm30bsd0004.ibqa",
            "midHeader": "<20181116110108.15629.41969@vm30bsd0199.ibqa>",
            "timestamp": "16 Nov 2018 11:01:08 (GMT)",
            "hostName": "c680q07.ibqa (10.76.71.196)",
            "mid": [
                22124
            ],
            "sendingHostSummary": {},
            "attachments": [
                "driver_license_germany.txt"
            ],
            "messageSize": "765 (Bytes)",
            "ampDetails": [
                {
                    "timestamp": "16 Nov 2018 11:01:08 (GMT)",
                    "description": "File reputation query initiating. File Name =
driver_license_germany.txt
                     , MID = 22124, File Size = 42 bytes, File Type = text/plain"
                },
                {
                    "timestamp": "16 Nov 2018 11:01:09 (GMT)",
                   "description": "Response received for file reputation query from Cloud.
 File Name = driver
                    _license_germany.txt, MID = 22124, Disposition = FILE UNKNOWN, Malware
 = None, Analysis
                     Score = 0, sha256 =
7e3dee4dac8f4af561d1108c4b237e5e139bd8d3ddc8518455d3b5fb7e7a70c3,
                     upload_action = Recommended to send the file for analysis",
                    "lastEvent": true
                }
            ],
            "senderGroup": "RELAYLIST",
            "recipient": [
                "6406@vm30bsd0004.ibqa"
            ],
            "subject": "Testing"
        }
    }
}
```


URL Details

You can retrieve the URL details of messages with different attributes as explained below.

Synopsis	`GET /api/v2.0/message-tracking/url-details?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Aggregate report(s) for the specified duration.
	Serial Number	• `serialNumber=<value>` Specify the serial number of the email gateway.
	Message ID and Injection Connection ID	You should use both these parameters. If you use either, you will not receive data in the response. • `icid=<value>` Specify the icid of the message. • `mid=<value>` Specify the mid of the message.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the URL details of a specific message identified by it's icid, mid and serial number.

Sample Request

```
GET /esa/api/v2.0/message-tracking/url-details?endDate=2018-11-16T11:25:00.000Z&icid=19124&mid
=21981&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 10:58:21 GMT
Content-type: application/json
Content-Length: 3697
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
```

```
    "data": {
        "messages": {
            "direction": "incoming",
            "smtpAuthId": "",
          "sdrAge": "31 years 11 months 18 days",

            "sender": "cf_quar_in@vm30bsd0004.ibqa",
            "midHeader": "",
            "urlDetails": [
                {
                    "timestamp": "15 Nov 2018 10:29:04 (GMT)",
                  "description": "Message 21981 URL: https://www.google.com/, URL category:
 Search
                     Engines and Portals, Condition: URL Category Rule."
                },
...
...
                {
                    "timestamp": "15 Nov 2018 10:29:04 (GMT)",
                    "description": "Message 21983 rewritten URL
u'http://stage.secure-web.sco.cisco.com/
                     1ytss9mMSYP-JYs4LQ0sT6QALREFaFw/http%3A%2F%2Fdrugstorehost.ru'."
                },
                {
                    "timestamp": "15 Nov 2018 10:29:04 (GMT)",
                    "description": "Message 21983 rewritten URL
u'https://stage.secure-web.sco.cisco.com/

1ymzrg34NKpT-_17H5_rS9dukFQ0FXsvLnYCHc4Eg/https%3A%2F%2Fwww.google.com%2F'."
                }
            ],
            "sdrCategory": "N/A",
            "hostName": "c680q07.ibqa (10.76.71.196)",
            "mid": [
                21981,
                21982,
                21983,
                21984
            ],
            "sendingHostSummary": {},
            "attachments": [],
            "sdrReputation": "neutral",

            "showURLDetails": true,
            "senderGroup": "UNKNOWNLIST",
            "recipient": [
                "4969@vm30bsd0004.ibqa"
            ],
            "subject": "[SUSPICIOUS MESSAGE] [SUSPECTED SPAM] Testing VOF"
        }
    }
}
```


Connection Details

You can retrieve connection details of messages with different attributes as explained below.

Synopsis	`GET /api/v2.0/message-tracking/connection-details?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Aggregate report(s) for the specified duration.
	Serial Number	• `serialNumber=<value>` Specify the serial number of the email gateway.
	Message ID and Injection Connection ID	You should use both these parameters. If you use either, you will not receive data in the response. • `icid=<value>` Specify the icid of the message. • `mid=<value>` Specify the mid of the message.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the connection details of a specific message identified by it's icid, mid and serial number.

Sample Request

```
GET /esa/api/v2.0/message-tracking/connection-details?endDate=2018-11-16T11:25:00.
000Z&icid=19213&mid=22124&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 11:08:56 GMT
Content-type: application/json
Content-Length: 669
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
```

```
    "senderGroup": "RELAYLIST",
    "messages": {
        "summary": [
            {"timestamp": "16 Nov 2018 11:01:08 (GMT)",
               "description": "ICID 19213 sender_group: RELAYLIST sender_ip: 10.76.70.111,

                sbrs: not enabled",
               "lastEvent": false},
            {"timestamp": "16 Nov 2018 11:01:08 (GMT)",
                "description": "Protocol SMTP interface Management  (IP 10.76.71.196) on
                 incoming connection (ICID 19213) from sender IP 10.76.70.111. Reverse DNS
                 host vm30bsd0199.com verified yes.",
                "lastEvent": false},
            {"timestamp": "16 Nov 2018 11:01:08 (GMT)",
                "description": "(ICID 19213) RELAY sender group RELAYLIST match 10.0.0.0/8

                 SBRS not enabled country 10.76.70.111",
                "lastEvent": true}
        ]
    },
    "sbrs": "not enabled"
}
```


Remediation Details

You can retrieve the remediation details of the messages remediated using Mailbox Search and Remediate.

Synopsis	`GET /api/v2.0/message-tracking/remediation-details?resource_attribute`
Supported Resource Attributes	See AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway for more information.
Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection This example shows a query to retrieve the remediation details of the message such as remediation status, batch details, etc.

Sample Request

```
GET esa/api/v2.0/message-tracking/remediation-details?batchID=admin_1590646987
&endDate=2020-05-28T14:24:00.000Z&searchOption=batch_details&startDate=2020-05-26T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: m680q09.ibqa.sgg.cisco.com:6080
accept-encoding: gzip, deflate, br
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 25 May 2020 10:28:53 GMT
Content-type: application/json
Content-Length: 5271
```

```
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
 pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
  {
        "batch_details": {
            "b_init_username": "admin",
            "mor_action": "Delete",
            "b_init_time": 1590646987,
            "batch_name": "Re7",
            "batch_desc": "N/A",
            "b_init_source": "ESA 117"
        },
        "message_details": [
            {
                "delivered_at": 1584574165,
                "mid": "3",
                "from_email": "kr@mar-esa.com",
                "recipient_email": "krs@onpremesa2019.com",
                "mor_status": "Success",
                "msg_read": "0"
            },
            {
                "delivered_at": 1584574165,
                "mid": "3",
                "from_email": "kr@mar-esa.com",
                "recipient_email": "krc@mar-esa.com",
                "mor_status": "Success",
                "msg_read": "0"
            },
            {
                "delivered_at": 1584574165,
                "mid": "3",
                "from_email": "kr@mar-esa.com",
                "recipient_email": "anonpremnew@mar-esa.com",
                "mor_status": "Success",
                "msg_read": "0"
            },
            {
                "delivered_at": 1584574165,
                "mid": "3",
                "from_email": "kr@mar-esa.com",
                "recipient_email": "user5@scale.com",
                "mor_status": "Failed",
                "msg_read": "N/A"
            }
        ]
    }
}
}
```

Retrieving All Incoming Messages that Matched a Configured Mail Policy

You can retrieve all incoming messages that matched a configured mail policy in your email gateway.

Synopsis	`GET esa/api/v2.0/message-tracking/messages?startDate=2021-03-01T18:30:00.000Z&endDate=2021-03-02T12:11:00.000Z&ciscoHost=All_Hosts&mailPolicyName=Default&mailPolicyDirection=inbound&searchOption=messages&offset=0&limit=100`

Supported Resource Attributes	See AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway for more information.
Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection This example shows a query to retrieve all incoming messages that matched a configured mail policy in your email gateway.

Sample Request

```
GET esa/api/v2.0/message-tracking/messages?startDate=2021-03-01T18:30:00.000Z
&endDate=2021-03-02T12:11:00.000Z&ciscoHost=All_Hosts&mailPolicyName=Default
&mailPolicyDirection=inbound&searchOption=messages&offset=0&limit=100
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: application/json, text/plain, */*
Host: esa.cisco.com:6080
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Tue, 02 Mar 2021 12:14:37 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 35014
Connection: keep-alive
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Pragma: no-cache
Server: nginx
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
{
    "meta": {
        "num_bad_records": 0,
        "totalCount": 39
    },
    "data": [
        {
            "attributes": {
                "hostName": "",
                "friendly_from": [
                    "user1@mar-esa.com"
                ],
                "isCompleteData": "N/A",
                "messageStatus": {
                    "2325234": "Delivered"
                },
                "recipientMap": {
                    "2325232": [
```

```
                    "user5@scale.com"
                ],
                "2325234": [
                    "user5@scale.com"
                ]
            },
            "senderIp": "10.10.4.49",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderGroup": "UNKNOWNLIST",
            "subject": "46_2016_smtp_2_5",
            "mid": [
                2325232,
                2325234
            ],
            "senderDomain": "mar-esa.com",
            "finalSubject": {
                "2325234": "46_2016_smtp_2_5"
            },
            "direction": "incoming",
            "icid": 516876,
            "morDetails": {},
            "replyTo": "N/A",
            "timestamp": "02 Mar 2021 17:15:53 (GMT +05:30)",
            "messageID": {
                "2325232": "<76773.751151876-sendEmail@mail.example.com>"
            },
            "verdictChart": {
                "2325234": "11141110"
            },
            "recipient": [
                "user5@scale.com"
            ],
            "sender": "user1@mar-esa.com",
            "serialNumber": "421558305641772925266-ABFF53B75FDE",
            "allIcid": [
                516876
            ],
            "sbrs": "None"
        }
    },
    {
        "attributes": {
            "hostName": "",
            "friendly_from": [
                "user1@mar-esa.com"
            ],
            "isCompleteData": "N/A",
            "messageStatus": {
                "2325233": "Delivered"
            },
            "recipientMap": {
                "2325233": [
                    "user5@scale.com"
                ],
                "2325230": [
                    "user5@scale.com"
                ]
            },
            "senderIp": "10.10.4.49",
            "mailPolicy": [
                "DEFAULT"
            ],
```

```
                    "senderGroup": "UNKNOWNLIST",
                    "subject": "46_2016_smtp_2_4",
                    "mid": [
                        2325230,
                        2325233
                    ],
                    "senderDomain": "mar-esa.com",
                    "finalSubject": {
                        "2325233": "46_2016_smtp_2_4"
                    },
                    "direction": "incoming",
                    "icid": 516875,
                    "morDetails": {},
                    "replyTo": "N/A",
                    "timestamp": "02 Mar 2021 17:15:51 (GMT +05:30)",
                    "messageID": {
                        "2325230": "<564966.601875739-sendEmail@mail.example.com>"
                    },
                    "verdictChart": {
                        "2325233": "11141110"
                    },
                    "recipient": [
                        "user5@scale.com"
                    ],
                    "sender": "user1@mar-esa.com",
                    "serialNumber": "421558305641772925266-ABFF53B75FDE",
                    "allIcid": [
                        516875
                    ],
                    "sbrs": "None"
                }
            },

        ]
}
```


Retrieving All Outgoing Messages that Matched a Configured Mail Policy

You can retrieve all outgoing messages that matched a configured mail policy in your email gateway.

Synopsis	`GET esa/api/v2.0/message-tracking/messages?startDate=2021-03-01T18:30:00.000Z&endDate=2021-03-02T12:11:00.000Z&ciscoHost=All_Hosts&mailPolicyName=Default&mailPolicyDirection=outbound&searchOption=messages&offset=0&limit=100`
Supported Resource Attributes	See AsyncOS 14.0 API - Addendum to the Getting Started guide for Cisco Secure Email Gateway for more information.
Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection This example shows a query to retrieve all outgoing messages that matched a configured mail policy in your email gateway.

Sample Request

```
GET esa/api/v2.0/message-tracking/messages?startDate=2021-03-01T18:30:00.000Z
&endDate=2021-03-02T12:11:00.000Z&ciscoHost=All_Hosts&mailPolicyName=Default
&mailPolicyDirection=outbound&searchOption=messages&offset=0&limit=100
```

```
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: application/json, text/plain, */*
Host: esa.cisco.com:6080
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Tue, 02 Mar 2021 12:14:37 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 1703
Connection: keep-alive
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Pragma: no-cache
Server: nginx
X-Content-Type-Options: nosniff
X-Frame-Options: DENY

{
    "meta": {
        "num_bad_records": 0,
        "totalCount": 2
    },
    "data": [
        {
            "attributes": {
                "hostName": "",
                "friendly_from": [
                    "LaithwaitesWine@fiendofwine.us"
                ],
                "isCompleteData": "N/A",
                "messageStatus": {
                    "2325166": "Delivered"
                },
                "recipientMap": {
                    "2325166": [
                        "testuser2@abc.com"
                    ]
                },
                "senderIp": "10.10.4.46",
                "mailPolicy": [
                    "DEFAULT"
                ],
                "senderGroup": "None",
                "subject": "Top 12 wines for the holidays",
                "mid": [
                    2325166
                ],
                "senderDomain": "testdomain.com",
                "finalSubject": {
                    "2325166": "[SPAM] Top 12 wines for the holidays"
                },
                "direction": "outgoing",
                "icid": 516847,
```

```
            "morDetails": {},
            "replyTo": "N/A",
            "timestamp": "02 Mar 2021 13:14:36 (GMT +05:30)",
            "messageID": {
                "2325166": "<19831342576104719839152803255 6096@makug.fiendofwine.us>"
            },
            "verdictChart": {
                "2325166": "16141113"
            },
            "recipient": [
                "testuser2@abc.com"
            ],
            "sender": "user@testdomain.com",
            "serialNumber": "42155830541772925266-ABFF53B45FDE",
            "allIcid": [
                516847
            ],
            "sbrs": "None"
        }
    },
    {
        "attributes": {
            "hostName": "",
            "mid": [
                2325164
            ],
            "isCompleteData": "N/A",
            "messageStatus": {
                "2325164": "Dropped By Anti-Virus"
            },
            "recipientMap": {
                "2325164": [
                    "testuser1@abc.com"
                ]
            },
            "senderIp": "10.10.4.46",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderGroup": "None",
            "subject": "Shipping confirmation: PIR-54787L-83296",
            "friendly_from": [
                "payment@geiger-sicher.de"
            ],
            "senderDomain": "testdomain.com",
            "direction": "outgoing",
            "icid": 516847,
            "morDetails": {},
            "replyTo": "N/A",
            "timestamp": "02 Mar 2021 13:14:34 (GMT +05:30)",
            "messageID": {
                "2325164": "<9o6bdsq4jgrk@geiger-sicher.de>"
            },
            "verdictChart": {
                "2325164": "11500000"
            },
            "recipient": [
                "testuser1@abc.com"
            ],
            "sender": "user@testdomain.com",
            "serialNumber": "42155830541672825266-ABFF53B45FDE",
            "allIcid": [
                516847
            ],
```

```
                "sbrs": "None"
            }
        }
    ]
}
```


Quarantine

Using API queries for quarantine, you can retrieve all information about messages in quarantine. You can action on the messages by releasing, deleting, and delaying their exit. APIs for quarantine are broadly classified under:

- APIs for Spam Quarantine, on page 46
- APIs for Other Quarantine, on page 73

APIs for Spam Quarantine

You can query for messages in the spam quarantine that match multiple attributes, delete or release messages.

- Searching for Messages, on page 46
- Retrieving Message Details, on page 49
- Releasing Messages, on page 52
- Deleting Messages, on page 51
- Searching for Safelist and Blocklist Entries, on page 53
- Adding, Editing, and Appending Safelist and Blocklist Entries, on page 56
- Deleting Safelist or Blocklist Entries, on page 69

Searching for Messages

You can search for messages in the spam quarantine that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/messages?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. Use this parameter with all API queries. • `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Messages quarantined during this time range.
	Quarantine Type	• `quarantineType=<value>` The accepted value is spam. `quarantineType=spam`
	Sorting	You can specify the value and the direction order the results. • `orderBy=<value>` Valid values are: • `from_address` • `to_address` • `subject` • `orderDir=<value>` Valid values are: • `asc` • `desc`
	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.
	Envelope Recipient	

		• `envelopeRecipientFilterOperator=<value>` The valid values are: • `contains` • `is` • `begins_with` • `ends_with` • `does_not_contain` • `envelopeRecipientFilterValue=<value>` The value to search for. This is a user defined value. For example, `envelopeRecipientFilterValue=user`
	Filtering	Filter parameters restrict the data to be included the response. • `filterOperator=<value>` The value to search for. Valid values are: • `contains` • `is` • `begins_with` • `ends_with` • `does_not_contain` • `filterValue=<value>` The value to search for. This is a user defined value. For example, `filterValue=abc.com`
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve quarantine messages, with the time range, ordering, quarantine type, offset and limit parameters.

Sample Request

```
GET /esa/api/v2.0/quarantine/messages?endDate=2018-11-21T23:59:00.000Z&
limit=25&offset=0&orderBy=date&orderDir=desc&quarantineType=spam&startDate=2018-07-01T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
```

```
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 21 Nov 2018 13:19:37 GMT
Content-type: application/json
Content-Length: 39
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": 1
    },
    "data": [
        {
            "attributes": {
                "envelopeRecipient": [
                    "test@test.com"
                ],
                "toAddress": [
                    "danielyeung@mail.qa"
                ],
                "subject": "[SPAM] Spam",
                "date": "21 Nov 2018 14:31 (GMT)",
                "fromAddress": [
                    "danel"
                ],
                "size": "1.60K"
            },
            "mid": 170
        }
    ]
}
```

Retrieving Message Details

You can retrieve details of a message that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Quarantine Type	• `quarantineType=<value>` The accepted value is spam. `quarantineType=spam`
	Message ID	You must specify the mid of the message to retrieve its details. • `mid=<value>`

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve details of a specific message.

Sample Request

```
GET /esa/api/v2.0/quarantine/messages/details?mid=1755&quarantineType=spam
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 21 Nov 2018 13:43:30 GMT
Content-type: application/json
Content-Length: 6491
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "attributes": {
            "envelopeRecipient": [
                "av_deliver@vm30bsd0004.ibqa"
            ],
            "toAddress": [
                "Surya Allena <sallena@cisco.com>"
            ],
            "attachments": [],
          "messageBody": "Received: from c680q07.ibqa ([10.76.71.196])\r\n  by esa.cisco.com
 with
            ESMTP; 16 Nov 2018 13:58:55 +0000<br />\nIronPort-SDR:
DjDeJA8ZkD90oA9x+n3eGd9Qa/nliZ1dL
          MyxB7dsrdq8oTnn8YSi5amR2qihbeq2eJwvVjskf1\r\n KE7TdyCXSokg==<br />\nX-IronPort-AV:

            E=Sophos;i=\"5.56,240,1539648000\"; \r\n   d=\"scan'\";a=\"22180\"<br
/>\nIronPort-SDR:
            PPj7KDz4Ur8W2ne2fWP/wSOUBwnY3x1XaBz/ryR/98vI6NPraAsA5q7vzUzyaYFpRCWGgfyJaZ\r\n
 4UIJbt91/
            WFccoWcqqO86zz6rYcRASCSM=<br />\nIronPort-PHdr:
=?us-ascii?q?9a23=3Az7tnkBDwN1EwuviG0ROD
            UyQJP3N1i/DPJgcQr6?=\r\n
=?us-ascii?q?AfoPdwSPT7pMbcNUDSrc9gkEXOFd2Cra4c26yO6+jJYi8p2d65",
            "date": "16 Nov 2018 13:58 (GMT)",
```

```
            "fromAddress": [
                "testuser <testuser@cisco.com>"
            ],
            "subject": "[SUSPICIOUS MESSAGE] [SUSPECTED SPAM] Testing VOF"
        },
        "mid": 1755
    }
}
```

Deleting Messages

You can delete messages that match various attribute. The syntax and supported attributes are given below:

Synopsis	`DELETE /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Message ID	You should use this parameter to effect the delete action. • `"mids":[<value>]` Specify the mid of the message.
	Quarantine Type	`"quarantineType":"value"` The valid value is *spam*.

Request Body	`{`
	`"quarantineType":"spam",`
	`"mids":[<mid>]`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to delete messages.

Sample Request

```
DELETE /esa/api/v2.0/quarantine/messages HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 41
Connection: keep-alive

{
"quarantineType":"spam",
"mids":[169]
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
```

```
Date: Thu, 22 Nov 2018 05:48:10 GMT
Content-type: application/json
Content-Length: 47
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delete",
        "totalCount": 1
    }
}
```

Releasing Messages

You can release a message that matches the **mid** attribute. The syntax and supported attributes are given below:

Synopsis	`POST /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Message ID	You should use this parameter to effect the release action. • `"mids":[<value>]` Specify the mid of the message.
	Action	`"action":"value"` The valid value is *release*.
	Quarantine Type	`"quarantineType":"value"` The valid value is *spam*.

Request Body	`{`
	`"action":"release:`
	`"quarantineType":"spam",`
	`"mids":[<mid>]`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to release a specific message with the mid parameter.

Sample Request

```
POST /esa/api/v2.0/quarantine/messages HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
```

```
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 61
Connection: keep-alive

{
"action":"release",
"quarantineType":"spam",
"mids":[184]
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 05:41:10 GMT
Content-type: application/json
Content-Length: 48
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "release",
        "totalCount": 1
    }
}
```

Searching for Safelist and Blocklist Entries

You can retrieve Safelist and Blocklist entries with API queries. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/safelist?resource_attribute` `GET /api/v2.0/quarantine/blocklist?resource_attribute`

Supported Resource Attributes	Action	• `action=<value>` Valid value is *view*.
	Quarantine Type	`quarantineType=<value>` The valid value is *spam*.
	View By	`viewBy=<value>` The valid values are *sender*, and *recipient*.
	Order By	`orderBy=<value>` The valid values are*sender*, and *recipient*.
	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.
	Ordering	`orderDir=<value>` Valid values are: • `asc` • `desc`
	Search	This is only supported for the attribute *orderBy=recipient*. `search=<value>` This is a user defined value.
Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Examples

Viewing Safelist and Blocklist entries by recipient:

This sample request shows an example query to retrieve **safelist** entries by recipient. Use the same query with *blocklist* to retrieve blocklist entries by recipient. An example query is shown below:

```
GET /esa/api/v2.0/quarantine/blocklist?action=view&limit=25&offset=0&orderBy=
recipient&orderDir=desc&quarantineType=spam&search=abc&viewBy=recipient
```

Sample Request

```
GET /esa/api/v2.0/quarantine/safelist?action=view&limit=25&offset=0&orderBy=
recipient&orderDir=desc&quarantineType=spam&search=abc&viewBy=recipient
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 09:08:39 GMT
Content-type: application/json
Content-Length: 126
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": 1
    },
    "data": [
        {
            "senderList": [
                "space.com",
                "xyz.com",
                "abc.com"
            ],
            "recipientAddress": "u1@space.com"
        }
    ]
}
```

Viewing Safelist and Blocklist entries by sender:

This sample request shows an example query to retrieve **blocklist** entries by sender. Use the same query with *safelist* to retrieve blocklist entries by recipient. An example query is shown below:

```
GET /esa/api/v2.0/quarantine/safelist?action=view&limit=25&offset=0&orderBy=
sender&orderDir=desc&quarantineType=spam&viewBy=sender
```

Sample Request

```
GET /esa/api/v2.0/quarantine/blocklist?action=view&limit=25&offset=0&orderBy=
sender&orderDir=desc&quarantineType=spam&viewBy=sender
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Postman-Token: 9b9bc6ef-2290-47ce-a84a-077bb805c57f
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.4.0
Accept: */*
Host: bgl0090-pod.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 09:19:24 GMT
Content-type: application/json
Content-Length: 214
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 09:08:39 GMT
Content-type: application/json
Content-Length: 126
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": 1
    },
    "data": [
        {
            "senderList": [
                "space.com",
                "xyz.com",
                "abc.com"
            ],
            "recipientAddress": "u1@space.com"
        }
    ]
}
```

Adding, Editing, and Appending Safelist and Blocklist Entries

You can add, edit and append Safelist and Blocklist entries. If the record does not exist, the entry is added. If the record exists, the entry is edited. The syntax and supported attributes are given below:

Synopsis	`POST /api/v2.0/quarantine/safelist?resource_attribute` `POST /api/v2.0/quarantine/blocklist?resource_attribute`

Supported Resource Attributes	Action	• `action=<value>` Valid values are: • `add` • `edit` • `append`
	Quarantine Type	`quarantineType=<value>` The valid value is *spam*.
	View By	`viewBy=<value>` The valid values are*sender*, and *recipient*.
	Recipient Addresses	`"recipientAddresses": ["value","value",...]` This is a user defined value. You can enter multiple values.
	Recipient List	`"recipientList": ["value","value",...]` This is a user defined value. You can enter multiple values.
	Sender Addresses	`"senderAddresses": ["value","value",...]` This is a user defined value. You can enter multiple values.
	Sender List	`"senderList": ["value", "value", ...]` This is a user defined value. You can enter multiple values.

Request Body	**Adding a new recipient entry:**
	`{ "action": "add", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }`
	Adding a new sender entry:
	`{ "action": "add", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }`
	Editing a new recipient entry:
	`{ "action": "edit", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }`
	Editing a new sender entry:
	`{ "action": "edit", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }`
	Appending a new recipient entry:
	`{ "action": "append", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }`
	Appending a new sender entry:
	`{ "action": "append", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }`

Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection

Examples

Adding Recipient Safelist Entries

This sample request shows a query to add a safelist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/safelist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 163
Connection: keep-alive

{
"action": "add",
"quarantineType": "spam",
"recipientAddresses": ["user1@acme.com","user2@acme.com"],
"senderList": ["acme.com"],
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:22:23 GMT
Content-type: application/json
Content-Length: 115
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
```

```
        "action": "add",
        "recipientAddresses": [
            "user1@acme.com",
            "user2@acme.com"
        ],
        "senderList": [
            "acme.com"
        ]
    }
}
```

Adding Sender Safelist Entries

This sample request shows a query to add a safelist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/safelist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 155
Connection: keep-alive

{
"action": "add",
"quarantineType": "spam",
"senderAddresses": ["xyz.com","space.com"],
"recipientList": ["user@cronos.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:31:28 GMT
Content-type: application/json
Content-Length: 110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "add",
        "recipientList": [
            "user@cronos.com"
        ],
        "senderAddresses": [
            "xyz.com",
            "space.com"
        ]
    }
}
```

Adding Recipient Blocklist Entries

This sample request shows a query to add a blocklist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/blocklist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Postman-Token: 55570e07-17fb-436e-9132-9f4998c67e7f
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 163
Connection: keep-alive

{
"action": "add",
"quarantineType": "spam",
"recipientAddresses": ["user1@acme.com","user2@acme.com"],
"senderList": ["acme.com"],
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:22:23 GMT
Content-type: application/json
Content-Length: 115
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "add",
        "recipientAddresses": [
            "user1@acme.com",
            "user2@acme.com"
        ],
        "senderList": [
            "acme.com"
        ]
    }
}
```

Adding Sender Blocklist Entries

This sample request shows a query to add a blocklist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/blocklist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
```

```
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 155
Connection: keep-alive

{
"action": "add",
"quarantineType": "spam",
"senderAddresses": ["xyz.com","space.com"],
"recipientList": ["user@cronos.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:31:28 GMT
Content-type: application/json
Content-Length: 110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "add",
        "recipientList": [
            "user@cronos.com"
        ],
        "senderAddresses": [
            "xyz.com",
            "space.com"
        ]
    }
}
```

Editing Recipient Safelist Entries

This sample request shows a query to add a safelist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/safelist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Postman-Token: 55570e07-17fb-436e-9132-9f4998c67e7f
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 163
Connection: keep-alive

{
"action": "edit",
"quarantineType": "spam",
"recipientAddresses": ["user1@acme.com","user2@acme.com"],
"senderList": ["acme.com"],
```

```
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:22:23 GMT
Content-type: application/json
Content-Length: 115
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "edit",
        "recipientAddresses": [
            "user1@acme.com",
            "user2@acme.com"
        ],
        "senderList": [
            "acme.com"
        ]
    }
}
```

Editing Sender Safelist Entries

This sample request shows a query to add a safelist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/safelist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 155
Connection: keep-alive

{
"action": "edit",
"quarantineType": "spam",
"senderAddresses": ["xyz.com","space.com"],
"recipientList": ["user@cronos.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:31:28 GMT
Content-type: application/json
Content-Length: 110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
```

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "edit",
        "recipientList": [
            "user@cronos.com"
        ],
        "senderAddresses": [
            "xyz.com",
            "space.com"
        ]
    }
}
```

Editing Recipient Blocklist Entries

This sample request shows a query to edit a blocklist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/blocklist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Postman-Token: 55570e07-17fb-436e-9132-9f4998c67e7f
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 163
Connection: keep-alive

{
"action": "edit",
"quarantineType": "spam",
"recipientAddresses": ["user1@acme.com","user2@acme.com"],
"senderList": ["acme.com"],
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:22:23 GMT
Content-type: application/json
Content-Length: 115
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "edit",
        "recipientAddresses": [
            "user1@acme.com",
            "user2@acme.com"
        ],
```

```
        "senderList": [
            "acme.com"
        ]
    }
}
```

Editing Sender Blocklist Entries

This sample request shows a query to edit a blocklist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/blocklist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 155
Connection: keep-alive

{
"action": "edit",
"quarantineType": "spam",
"senderAddresses": ["xyz.com","space.com"],
"recipientList": ["user@cronos.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:31:28 GMT
Content-type: application/json
Content-Length: 110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "edit",
        "recipientList": [
            "user@cronos.com"
        ],
        "senderAddresses": [
            "xyz.com",
            "space.com"
        ]
    }
}
```

Appending Recipient Safelist Entries

This sample request shows a query to append a safelist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/safelist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Postman-Token: 55570e07-17fb-436e-9132-9f4998c67e7f
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 163
Connection: keep-alive

{
"action": "append",
"quarantineType": "spam",
"recipientAddresses": ["user1@acme.com","user2@acme.com"],
"senderList": ["acme.com"],
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:22:23 GMT
Content-type: application/json
Content-Length: 115
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "append",
        "recipientAddresses": [
            "user1@acme.com",
            "user2@acme.com"
        ],
        "senderList": [
            "acme.com"
        ]
    }
}
```

Appending Sender Safelist Entries

This sample request shows a query to append a safelist entry.

Sample Request

```
POST /esa/api/v2.0/quarantine/safelist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 155
Connection: keep-alive
```

```
{
"action": "append",
"quarantineType": "spam",
"senderAddresses": ["xyz.com","space.com"],
"recipientList": ["user@cronos.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:31:28 GMT
Content-type: application/json
Content-Length: 110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "append",
        "recipientList": [
            "user@cronos.com"
        ],
        "senderAddresses": [
            "xyz.com",
            "space.com"
        ]
    }
}
```

Appending a Recipient Blocklist Entry

This sample request shows a query to append blocklist entries.

Sample Request

```
POST /esa/api/v2.0/quarantine/blocklist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Postman-Token: 55570e07-17fb-436e-9132-9f4998c67e7f
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 163
Connection: keep-alive

{
"action": "append",
"quarantineType": "spam",
"recipientAddresses": ["user1@acme.com","user2@acme.com"],
"senderList": ["acme.com"],
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:22:23 GMT
Content-type: application/json
Content-Length: 115
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "append",
        "recipientAddresses": [
            "user1@acme.com",
            "user2@acme.com"
        ],
        "senderList": [
            "acme.com"
        ]
    }
}
```

Appending Sender Blocklist Entries

This sample request shows a query to append blocklist entries.

Sample Request

```
POST /esa/api/v2.0/quarantine/blocklist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 155
Connection: keep-alive

{
"action": "append",
"quarantineType": "spam",
"senderAddresses": ["xyz.com","space.com"],
"recipientList": ["user@cronos.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:31:28 GMT
Content-type: application/json
Content-Length: 110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
```

```
    "data": {
        "action": "append",
        "recipientList": [
            "user@cronos.com"
        ],
        "senderAddresses": [
            "xyz.com",
            "space.com"
        ]
    }
}
```

Deleting Safelist or Blocklist Entries

You can run API queries to delete safelist or blocklist entries from either the sender or recipient lists.

Synopsis	`DELETE /api/v2.0/quarantine/safelist?resource_attribute` `DELETE /api/v2.0/quarantine/blocklist?resource_attribute`	
Supported Resource Attributes	Quarantine Type	`quarantineType=<value>` The valid value is *spam*.
	Recipient List	`"recipientList": ["value","value",...]` This is a user defined value. You can enter multiple values.
	Sender List	`"senderList": ["value", "value", ...]` This is a user defined value. You can enter multiple values.
	View By	`"viewBy": "value"` Valid values are *sender*, and *recipient* .

Request Body	**Deleting recipient entries:**
	`{`
	`"quarantineType": "spam",`
	`"recipientList": ["value","value"],`
	`"viewBy": "recipient"`
	`}`
	Deleting sender entries:
	`{`
	`"quarantineType": "spam",`
	`"senderList": ["value"],`
	`"viewBy": "sender"`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

The following APIs are available:

- Deleting Recipient Safelist Entries, on page 70

Deleting Recipient Safelist Entries

This sample request shows a query to delete a safelist entry.

Sample Request

```
DELETE /esa/api/v2.0/quarantine/safelist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 111
Connection: keep-alive

{
"quarantineType": "spam",
"recipientList": ["user@cronos.com","user3@cosco.com"],
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 12:27:40 GMT
Content-type: application/json
Content-Length: 104
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delete",
        "recipientList": [
            "user@cronos.com",
            "user3@cosco.com"
        ],
        "totalCount": 2
    }
}
```

Deleting Sender Safelist Entries

This sample request shows a query to delete a safelist entry.

Sample Request

```
DELETE /esa/api/v2.0/quarantine/safelist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
```

```
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 82
Connection: keep-alive

{
"quarantineType": "spam",
"senderList": ["race.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 12:33:41 GMT
Content-type: application/json
Content-Length: 75
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delete",
        "totalCount": 1,
        "senderList": [
            "race.com"
        ]
    }
}
```

Deleting Recipient Blocklist Entries

This sample request shows a query to delete a blocklist entry.

```
DELETE /esa/api/v2.0/quarantine/blocklist
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 111
Connection: keep-alive

{
"quarantineType": "spam",
"recipientList": ["user@cronos.com","user3@cosco.com"],
"viewBy": "recipient"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 12:27:40 GMT
```

```
Content-type: application/json
Content-Length: 104
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delete",
        "recipientList": [
            "user@cronos.com",
            "user3@cosco.com"
        ],
        "totalCount": 2
    }
}
```

Deleting Sender Blocklist Entries

This sample request shows a query to delete a blocklist entry.

Sample Request

```
DELETE /esa/api/v2.0/quarantine/blocklist HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 82
Connection: keep-alive

{
"quarantineType": "spam",
"senderList": ["race.com"],
"viewBy": "sender"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 12:33:41 GMT
Content-type: application/json
Content-Length: 75
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delete",
        "totalCount": 1,
        "senderList": [
            "race.com"
        ]
```

```
    }
}
```

APIs for Other Quarantine

These queries will have the **quarantineType** resource name as part of the query string.

Quarantine queries support search, sorting, offset, and lazy loading.

Searching for Messages

You can search for messages in the other quarantine that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/messages?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. • `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z`

	Quarantines to Search	This parameter specifies the quarantines to search for.
		• `quarantines=<value, value, ...>`
		Valid values are:
		`Outbreak`
		`Virus`
		`File+Analysis`
		`Unclassified`
		`Policy`
		`<user-defined-quarantine>`

	Subject	• `subjectFilterBy=<value>`
		The valid values are:
		`contains`
		`starts_with`
		`ends_with`
		`matches_exactly`
		`does_not_contain`
		`does_not_start_with`
		`does_not_end_with`
		`does_not_match`
		• `subjectFilterValue=<value>`
		This is a user defined value.

	Originating ESA	`originatingEsaIp=<value>` You can specify the IP address of the ESA in which the message was processed.
	Attachment Details	

		• `attachmentName=<value>`
		This is a user defined value.
		• `attachmentSizeFilterBy=<value>`
		Valid values are:
		`range`
		`less_than`
		`more_than`
		• `attachmentSizeFromValue=<value_in_KB>`
		This is a user defined value. Specify an attachment size in KB. This is applicable when:
		• You choose the *range* attribute for *attachmentSizeFilterBy*
		`attachmentSizeFilterBy=range`
		• You choose the *more_than* attribute for *attachmentSizeFilterBy*
		`attachmentSizeFilterBy=more_than`
		.
		• `attachmentSizeToValue=<value_in_KB>`
		This is a user defined value. Specify an attachment size in KB. This is applicable when:
		• You choose the *range* attribute for *attachmentSizeFilterBy*
		`attachmentSizeFilterBy=range`
		• You choose the *less_than* attribute for *attachmentSizeFilterBy*
		`attachmentSizeFilterBy=less_than`

	Quarantine Type	• `quarantineType=<value>` The accepted value is pvo. `quarantineType=pvo`
	Sorting	

		You can specify the value and the direction order the results.
		• `orderBy=<value>`
		Values are:
		`sender`
		`subject`
		`received`
		`scheduledExit`
		`size`
		• `orderDir=<value>`
		Values are:
		`asc`
		`desc`

	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.

	Envelope Recipient	• `envelopeRecipientFilterBy=<value>`
		The valid values are:
		`contains`
		`starts_with`
		`ends_with`
		`matches_exactly`
		`does_not_contain`
		`does_not_start_with`
		`does_not_end_with`
		`does_not_match`
		• `envelopeRecipientFilterValue=<value>`
		The value to search for. This is a user defined value. For example,
		`envelopeRecipientFilterValue=user`

	Envelope Sender	

		• `envelopeSenderFilterBy=<value>`
		The valid values are:
		`contains`
		`starts_with`
		`ends_with`
		`matches_exactly`
		`does_not_contain`
		`does_not_start_with`
		`does_not_end_with`
		`does_not_match`
		• `envelopeSenderFilterValue=<value>`
		The value to search for. This is a user defined value. For example,
		`envelopeRecipientFilterValue=user`

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve messages in the other Policy, Virus and Outbreak quarantines, with the time range, ordering, quarantine type, offset and limit, originating ESA parameters.

Sample Request

```
GET
/esa/api/v2.0/quarantine/messages?endDate=2018-11-23T00:00:00.000Z&limit=25&offset=0&orderBy=
received&orderDir=desc&quarantineType=pvo&quarantines=Outbreak,Virus,File+Analysis,Unclassified,Policy&startDate
=2017-11-22T00:00:00.000Z&originatingEsaIp=10.8.91.15
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 09:01:11 GMT
Content-type: application/json
Content-Length: 13093
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
```

```
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": 126
    },
    "data": [
        {
            "attributes": {
                "received": "21 Nov 2018 10:10 (GMT)",
                "sender": "usr2@sender.com",
                "subject": "[SUSPICIOUS MESSAGE] Test mail.",
                "esaHostName": "esa01",
                "inQuarantines": "Policy",
                "scheduledExit": "21 Dec 2018 10:10 (GMT)",
                "originatingEsaIp": "10.8.91.15",
                "quarantineForReason": [
                    "Content Filter: 'url'"
                ],
                "esaMid": 379,
                "recipient": [
                    "eriferna@mail.qa.sgg.cisco.com"
                ],
                "quarantineForReasonDict": [
                    {
                        "reason": [
                            "Content Filter: 'url'"
                        ],
                        "quarantineName": "Policy"
                    }
                ],
                "size": "312.69K"
            },
            "mid": 166
        },
        {
            "attributes": {
                "received": "21 Nov 2018 10:10 (GMT)",
                "sender": "usr2@sender.com",
                "subject": "[SUSPICIOUS MESSAGE] Test mail.",
                "esaHostName": "esa01",
                "inQuarantines": "Policy",
                "scheduledExit": "21 Dec 2018 10:10 (GMT)",
                "originatingEsaIp": "10.8.91.15",
                "quarantineForReason": [
                    "Content Filter: 'url'"
                ],
                "esaMid": 369,
                "recipient": [
                    "eriferna@mail.qa.sgg.cisco.com"
                ],
                "quarantineForReasonDict": [
                    {
                        "reason": [
                            "Content Filter: 'url'"
                        ],
                        "quarantineName": "Policy"
                    }
                ],
                "size": "312.69K"
            },
            "mid": 161
        },
```

```
{
    "attributes": {
        "received": "21 Nov 2018 10:09 (GMT)",
        "sender": "usr2@sender.com",
        "subject": "[SUSPICIOUS MESSAGE] Test mail.",
        "esaHostName": "esa01",
        "inQuarantines": "Policy",
        "scheduledExit": "21 Dec 2018 10:09 (GMT)",
        "originatingEsaIp": "10.8.91.15",
        "quarantineForReason": [
            "Content Filter: 'url'"
        ],
        "esaMid": 354,
        "recipient": [
            "eriferna@mail.qa.sgg.cisco.com"
        ],
        "quarantineForReasonDict": [
            {
                "reason": [
                    "Content Filter: 'url'"
                ],
                "quarantineName": "Policy"
            }
        ],
        "size": "312.69K"
    },
    "mid": 153
},
{
    "attributes": {
        "received": "20 Nov 2018 12:42 (GMT)",
        "sender": "test@irontest.com",
        "subject": "[WARNING: ATTACHMENT UNSCANNED]sadsafasd",
        "esaHostName": "esa01",
        "inQuarantines": "Policy",
        "scheduledExit": "20 Dec 2018 12:42 (GMT)",
        "originatingEsaIp": "10.8.91.15",
        "quarantineForReason": [
            "Message is unscannable by AMP - Service Not Available"
        ],
        "esaMid": 254,
        "recipient": [
            "test2@irontest.com"
        ],
        "quarantineForReasonDict": [
            {
                "reason": [
                    "Message is unscannable by AMP - Service Not Available"
                ],
                "quarantineName": "Policy"
            }
        ],
        "size": "330.19K"
    },
    "mid": 143
},
{
    "attributes": {
        "received": "20 Nov 2018 12:41 (GMT)",
        "sender": "test@irontest.com",
        "subject": "[WARNING: ATTACHMENT UNSCANNED]sadsafasd",
        "esaHostName": "esa01",
        "inQuarantines": "Policy",
        "scheduledExit": "20 Dec 2018 12:41 (GMT)",
```

```
                "originatingEsaIp": "10.8.91.15",
                "quarantineForReason": [
                    "Message is unscannable by AMP - Service Not Available"
                ],
                "esaMid": 251,
                "recipient": [
                    "test2@irontest.com"
                ],
                "quarantineForReasonDict": [
                    {
                        "reason": [
                            "Message is unscannable by AMP - Service Not Available"
                        ],
                        "quarantineName": "Policy"
                    }
                ],
                "size": "330.19K"
            },
            "mid": 140
        }
    ]
}
```


Retrieving Message Details

You can retrieve details of a message that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Quarantine Type	• `quarantineType=<value>` The accepted value is pvo. `quarantineType=pvo`
	Message ID	You must specify the mid of the message to retrieve its details. • `mid=<value>`
Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to retrieve details of a specific message.

Sample Request

```
GET /esa/api/v2.0/quarantine/messages/details?mid=166&quarantineType=pvo
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
```

```
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 09:16:27 GMT
Content-type: application/json
Content-Length: 1650
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "attributes": {
            "quarantineDetails": [
                {
                    "received": "21 Nov 2018 10:10 (GMT)",
                    "esaHostName": "esa01",
                    "quarantineName": "Policy",
                    "reason": [
                        "Content Filter: 'url'"
                    ],
                    "scheduledExit": "21 Dec 2018 10:10 (GMT)",
                    "originatingEsaIp": "10.8.91.15"
                }
            ],
            "matchedContents": [],
            "messagePartDetails": [
                {
                    "attachmentId": 1,
                    "attachmentSize": "43",
                    "attachmentName": "[message body]"
                },
                {
                    "attachmentId": 2,
                    "attachmentSize": "307.25K",
                    "attachmentName": "eicar4.pdf"
                }
            ],
            "messageDetails": {
                "recipient": [
                    "eriferna@mail.qa.sgg.cisco.com"
                ],
                "sender": "usr2@sender.com",
                "subject": "[SUSPICIOUS MESSAGE] Test mail."
            },
            "messageBody": "This is a demo mail. http://www.google.com<br>\n",
            "headers": "IronPort-SDR:
4Sh6scwkvc+t4BgD5601B/l5cTAMkUtJtFAY+/Sk6YwaaSxL2TOzEKHwsn+6KxG+kV2Zg
             75sMX<br> DkgdFZYTDPift9VvRsTl0Fz+N6rRgHCB4=<br>X-IPAS-Result:
=?us-ascii?q?A0GSTP/juz9b/+pj4QpOH
             oMagXSCU4gely0HhysBAQEBA?=<br>
=?us-ascii?q?QEBeoIOAQEBPQUEAgEFBQEDAwECAgEBLTEkOCyBFxhDiEefIY8MAQ
             EBAQYBA?=<br>
=?us-ascii?q?QEBAR2PIQEBhH8FiRODF4FVgUqBJ02RGYVLhA55AYEAgTcBAQE?=<br>
             Subject: [SUSPICIOUS MESSAGE] Test mail.<br>Received: from client.cisco.com
             (HELO pod1224-client05.ibwsa) ([10.225.99.234])<br>&amp;nbsp; by pod0090-esa01
             with ESMTP; 21 Nov 2018 07:01:34 +0000<br>Message-ID: &amp;lt;194652.955603914
             -sendEmail@pod1224-client05&amp;gt;<br>From: \"usr2@sender.com\" &amp;lt;usr2@sender
```

```
                .com&gt;<br>To: \"eriferna@mail.qa.sgg.cisco.com\" &lt;testclient@.cisco.com
                &gt;<br>Date: Wed, 21 Nov 2018 10:23:53 +0000<br>X-Mailer: sendEmail-1.55<br
                >MIME-Version: 1.0<br>Content-Type: multipart/mixed; boundary=\"----
                MIME delimiter for sendEmail-936308.539779024\""
            },
            "mid": 166
        }
}
```

Move Messages

You can move messages that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`POST /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Message ID	You should use this parameter to effect the delete action. • `"mids": [<value>]` Specify the mid/s of the message/s.
	Quarantine Type	`"quarantineName": "<value>"` The valid value is *pvo*.

	Destination Quarantine Name	`"destinationQuarantineName": "<value>"`
		The valid values are:
		`Outbreak`
		`Virus`
		`File+Analysis`
		`Unclassified`
		`Policy`
		`<user-defined-quarantine>`

Request Body	`{`
	`"action": "move",`
	`"destinationQuarantineName": "<value>",`
	`"mids": [<value>],`
	`"quarantineName": "<value>",`
	`"quarantineType": "pvo"`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to move a message.

Sample Request

```
POST /esa/api/v2.0/quarantine/messages
HTTP/1.1
```

```
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 138
Connection: keep-alive
{
"action": "move",
"destinationQuarantineName": "Policy",
"mids": [46],
"quarantineName": "Unclassified",
"quarantineType": "pvo"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 11:57:40 GMT
Content-type: application/json
Content-Length: 84
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "move",
        "totalCount": 1,
        "destinationQuarantineName": "Policy"
    }
}
```

Delaying the Exit of a Message from a Quarantine

You can delay the exit of messages from a quarantine. The syntax and supported attributes are given below:

Synopsis	`POST /api/v2.0/quarantine/messages?resource_attribute`

Supported Resource Attributes	Message ID	• `"mids": [value]` Specify the mid of the message.
	Quarantine Type	`"quarantineType": "value"` The valid value is *pvo*.

	Quarantine Name	`"quarantineName": "value"`
		The valid values are:
		`Outbreak`
		`Virus`
		`File+Analysis`
		`Unclassified`
		`Policy`
		`<user-defined-quarantine>`

	Delay	`"delay":"value"` The valid values are *8h*, *24h*, *48h*, or *1w*.

Request Body	`{`
	`"action":"delay",`
	`"delay":"<value>",`
	`"mids": [<value>],`
	`"quarantineName": "<value>",`
	`"quarantineType": "pvo"`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to delay a message's exit.

Sample Request

```
POST /esa/api/v2.0/quarantine/messages HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 107
Connection: keep-alive
{
"action":"delay",
"delay":"1w",
"mids": [46],
"quarantineName": "Policy",
```

```
"quarantineType": "pvo"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 11:59:07 GMT
Content-type: application/json
Content-Length: 71
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delay",
        "totalCount": 1,
        "delayedTime": "1 week"
    }
}
```

Sending a Copy of a Message in Quarantine

You can send a copy of a message in quarantine to an email address. The syntax and supported attributes are given below:

Synopsis	`POST /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Message ID	• `"mids": [value]` Specify the mid of the message.
	Quarantine Type	`"quarantineType": "value"` The valid value is *pvo*.

	Quarantine Name	`"quarantineName": "value"`
		The valid values are:
		`Outbreak`
		`Virus`
		`File+Analysis`
		`Unclassified`
		`Policy`
		`<user-defined-quarantine>`

	Recipients	`"recipients":["value", "value", ...]` This is a user defined value. Enter email address/s of the recipients.

Request Body	{
	"action":"sendCopy",
	"mids": [value],
	"quarantineName": "value",
	"quarantineType": "pvo",
	"recipients":["value"]
	}
	For outbreak, you can add this optional attribute to the message body:
	"sendToCisco":<value>
	The valid value is *true*. An example is shown below:
	{
	"action":"sendCopy",
	"mids": [value],
	"quarantineName": "value",
	"quarantineType": "pvo",
	"recipients":["value"],
	}

Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection

Example

This example shows a query to send a copy of a message in the Unclassified quarantine to an email address.

Sample Request

```
POST /esa/api/v2.0/quarantine/messages HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 136
Connection: keep-alive


{
"action":"sendCopy",
"mids": [46],
"quarantineName": "Unclassified",
"quarantineType": "pvo",
"recipients":["admin@cisco.com"]
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 11:53:52 GMT
Content-type: application/json
Content-Length: 49
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
```

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "sendCopy",
        "totalCount": 1
    }
}
```

Downloading an Attachment

You can download an attachment accompanying a message in a quarantine. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Message ID	• `mid=<value>` Specify the mid of the message.
	Quarantine Type	`quarantineType=<value>` The valid value is *pvo*.
	Attachment ID	`attachmentId=<value>` Specify the attachment ID.
Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to download an attachment.

Sample Request

```
GET /esa/api/v2.0/quarantine/messages/attachment?attachmentId=2&mid=46&quarantineType=pvo
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 12:03:26 GMT
Content-type: application/octet-stream
Content-Disposition: filename="wanacry.exe"
Content-Length: 332511
```

```
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA+AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v
ZGUuDQ0KJAAAAAAAAAAAl+pLDYZv8kGGb/JBhm/yQGofwkGKb/JCilKGQdZv8kA6E95Bg
```

Deleting Messages

You can delete messages that match various attribute. The syntax and supported attributes are given below:

Synopsis	`DELETE /api/v2.0/quarantine/messages?resource_attribute`	
Supported Resource Attributes	Message ID	You should use this parameter to effect the delete action. • `"mids": [<value>]` Specify the mid/s of the message/s.
	Quarantine Type	`"quarantineType": "value"` The valid value is *pvo*.

	Quarantine Name	`"quarantineName": "<value>"`
		The valid values are:
		`Outbreak`
		`Virus`
		`File+Analysis`
		`Unclassified`
		`Policy`
		`<user-defined-quarantine>`

Request Body	`{`
	`"mids": [<mid>],`
	`"quarantineName": "<value>",`
	`"quarantineType": "pvo"`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to delete a specific messages in a specific quarantine.

Sample Request

```
DELETE /esa/api/v2.0/quarantine/messages
HTTP/1.1
```

```
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 41
Connection: keep-alive
{
"mids": [112],
"quarantineName": "Policy",
"quarantineType": "pvo"
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 05:48:10 GMT
Content-type: application/json
Content-Length: 47
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delete",
        "totalCount": 1
    }
}
```

Releasing Messages

You can release messages that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`POST /api/v2.0/quarantine/messages?resource_attribute`

Supported Resource Attributes	Message ID	You should use this parameter to effect the release action. • `"mids": [<value>]` Specify the mid of the message.
	Quarantine Type	`"quarantineType": "pvo"` The valid value is *pvo*.

	Quarantine Name	`"quarantineName": "<value>"`
		The valid values are:
		`Outbreak`
		`Virus`
		`File+Analysis`
		`Unclassified`
		`Policy`
		`<user-defined-quarantine>`

	Action	`"action":"value"` The valid value is *release*.

Request Body	`{`
	`"action":"release",`
	`"mids": [<mid>],`
	`"quarantineName": "<value>",`
	`"quarantineType": "pvo"`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to release a specific message with the mid parameter.

Sample Request

```
POST /esa/api/v2.0/quarantine/messages HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 61
Connection: keep-alive

{
"action":"release",
"mids": [157],
"quarantineName": "Policy",
```

```
"quarantineType":"pvo",
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 05:41:10 GMT
Content-type: application/json
Content-Length: 48
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "release",
        "totalCount": 1
    }
}
```

Viewing the Rule Summary

You can query for the details of messages currently residing in the quarantine. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/rules?resource_attribute`	
Supported Resource Attributes	Quarantine Type	`quarantineType=<value>` The valid value is *pvo*.
Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to retrieve message statistics of messages in quarantine.

Sample Request

```
GET /esa/api/v2.0/quarantine/rules?quarantineType=pvo HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 10:33:46 GMT
```

```
Content-type: application/json
Content-Length: 264
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalAverageMessageSize": "320KB",
        "totalNumberOfMessages": 6
    },
    "data": [
        {
            "attributes": {
                "numberOfMessages": 6,
                "capacity": "0.0%",
                "ruleId": "Malware: Malware",
                "totalSize": "1.9MB",
                "ruleDescription": "N/A",
                "averageMessageSize": "320KB"
            },
            "rid": 1
        }
    ]
}
```

Searching Based on Rule ID

You can search for messages in quarantine that match a specific rule ID. The syntax and supported attributes are given below:

Synopsis	`GET /api/v2.0/quarantine/rules_search?resource_attribute`

Supported Resource Attributes	Quarantine Type	`quarantineType=<value>` The valid value is *pvo*.
	Rule ID	`ruleId=<value>` This is a user defined value.

	Sorting	You can specify the value and the direction order the results.
		• `orderBy=<value>`
		The valid value is:
		`received`
		• `orderDir=<value>`
		Valid values are:
		`asc`
		`desc`

	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.
Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to retrieve messages that match rule parameters.

Sample Request

```
GET /esa/api/v2.0/quarantine/rules_search?limit=25&offset=0&orderBy=
received&orderDir=desc&quarantineType=pvo&ruleId=Malware:+Malware HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 10:35:34 GMT
Content-type: application/json
Content-Length: 3013
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "meta": {
        "totalCount": 6
    },
    "data": [
        {
            "attributes": {
                "received": "22 Nov 2018 10:30 (GMT)",
                "sender": "usr2@sender.com",
                "subject": "[SUSPICIOUS MESSAGE] Test mail.",
                "esaHostName": "esa01",
                "inQuarantines": "Outbreak",
                "scheduledExit": "22 Nov 2018 11:20 (GMT)",
                "originatingEsaIp": "10.8.91.15",
                "quarantineForReason": [
                    "Malware: Malware"
                ],
                "esaMid": 476,
                "recipient": [
                    "eriferna@mail.qa.sgg.cisco.com"
                ],
                "quarantineForReasonDict": [
                    {
                        "reason": [
                            "Malware: Malware"
                        ],
                        "quarantineName": "Outbreak"
                    }
                ],
                "size": "312.98K"
            },
            "mid": 191
        },
        {
            "attributes": {
                "received": "22 Nov 2018 10:30 (GMT)",
                "sender": "usr2@sender.com",
                "subject": "[SUSPICIOUS MESSAGE] Test mail.",
                "esaHostName": "esa01",
                "inQuarantines": "Outbreak",
                "scheduledExit": "22 Nov 2018 11:20 (GMT)",
                "originatingEsaIp": "10.8.91.15",
                "quarantineForReason": [
                    "Malware: Malware"
                ],
                "esaMid": 474,
                "recipient": [
                    "eriferna@mail.qa.sgg.cisco.com"
                ],
                "quarantineForReasonDict": [
                    {
                        "reason": [
```

```
                            "Malware: Malware"
                        ],
                        "quarantineName": "Outbreak"
                    }
                ],
                "size": "312.98K"
            },
            "mid": 190
        },
        {
            "attributes": {
                "received": "22 Nov 2018 10:30 (GMT)",
                "sender": "usr2@sender.com",
                "subject": "[SUSPICIOUS MESSAGE] Test mail.",
                "esaHostName": "esa01",
                "inQuarantines": "Outbreak",
                "scheduledExit": "22 Nov 2018 11:20 (GMT)",
                "originatingEsaIp": "10.8.91.15",
                "quarantineForReason": [
                    "Malware: Malware"
                ],
                "esaMid": 473,
                "recipient": [
                    "eriferna@mail.qa.sgg.cisco.com"
                ],
                "quarantineForReasonDict": [
                    {
                        "reason": [
                            "Malware: Malware"
                        ],
                        "quarantineName": "Outbreak"
                    }
                ],
                "size": "312.98K"
            },
            "mid": 189
        }
    ]
}
```


Releasing Messages from the Rule Summary

You can release messages from the rule summary that match multiple attributes. The syntax and supported attributes are given below:

Synopsis	`POST /api/v2.0/quarantine/rules?resource_attribute`	
Supported Resource Attributes	Rule ID	• `"ruleId": ["value", "value",...]` Specify the rule IDs.
	Quarantine Type	`quarantineType=<value>` The valid value is *pvo*.
	Action	`"action":"value"` The valid value is *release*.

Request Body	{
	"action" : "release",
	"quarantineType": "pvo",
	"ruleId": ["value"]
	}

Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection

Example

This example shows a query to release message.

Sample Request

```
POST /esa/api/v2.0/quarantine/rules
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 89
Connection: keep-alive


{
"action" : "release",
"quarantineType": "pvo",
"ruleId": ["Malware: Malware"]
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 10:39:29 GMT
Content-type: application/json
Content-Length: 48
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken


    "data": {
        "action": "release",
        "totalCount": 3
    }
}
```

Deleting Messages from the Rule Summary

You can delete messages from the rule summary that match specific attributes. The syntax and supported attributes are given below:

Synopsis	`DELETE /api/v2.0/quarantine/rules?resource_attribute`	
Supported Resource Attributes	Rule ID	• `"ruleId": ["value", "value",...]` Specify the rule IDs.
	Quarantine Type	`quarantineType=<value>` The valid value is *pvo*.

Request Body	`{`
	`"quarantineType": "pvo",`
	`"ruleId": ["value"]`
	`}`	

Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

Example

This example shows a query to delete messages from the rule summary.

Sample Request

```
DELETE /esa/api/v2.0/quarantine/rules HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 65
Connection: keep-alive


{
"quarantineType": "pvo",
"ruleId": ["Malware: Malware"]
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 10:41:14 GMT
Content-type: application/json
Content-Length: 47
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "action": "delete",
        "totalCount": 4
```

```
        }
}
```

Configuration APIs

You can use the configuration APIs to perform various operations (such as create, retrieve, update, and delete) in your email gateway. The various API categories for configuration are:

- Authentication APIs, on page 100
- URL Lists APIs, on page 108
- Dictionary APIs, on page 116
- HAT APIs, on page 134

Note For Configuration APIs, the administrator and cloud administrator user roles are only supported.

Note For Configuration APIs:

- If you modify any of the APIs in the cluster mode, the changes apply to all the other machines in the cluster.
- If you modify any of the APIs in the group mode, the changes apply to all the other machines in the group.
- If you modify any of the APIs in the machine mode, the changes only apply to the specified machine.

General Information

The following information is applicable to all Configuration APIs:

- Some special characters might require the equivalent UTF-8 encoded value in the URI of the API request.

  The following table lists a few of the special characters with the equivalent UTF-8 encoded values:

Table 1: UTF-8 (HEX) Values for Special Characters

Character	UTF-8 (HEX) Value
#	%23
%	%25
?	%3f
.	%2e
space	%20

- If you get a generic error on the API client, such as "Parse error: the server returns a malformed request," it is recommended that you switch to a different API client.
- If you need to include a backslash character in the API request, it should be escaped (with an additional backslash).

  For example, if you want to add a new line character - "\n," you must add an additional backslash character as follows -"\\n."

For information on how to troubleshoot Configuration APIs, see section Handling Error Messages of Configuration APIs, on page 173.

Cluster Levels for API Calls - Examples

The cluster mode consists of three levels – cluster, group, and machine. All three levels are supported for all the APIs except Authentication APIs.

Note Only the cluster level is supported by default for Authentication APIs, when you add the email gateway to the cluster.

When the email gateway is in cluster mode, you can use the following parameters:

Level	Key Name	Value for Key Name
cluster	mode	cluster
group	mode	group
	group_name	<name of the group>
machine	mode	machine
	host_name	<hostname of the machine>

Sample Requests

The sample requests to call an API in different levels are explained below:

Note The email gateway must be in cluster mode to use different levels.

- **To call an API in cluster level**

```
GET /esa/api/v2.0/config/dictionaries?device_type=esa&mode=cluster
```

- **To call an API in group level**

```
GET /esa/api/v2.0/config/dictionaries?device_type=esa&mode=group&group_name=<group_name>
```

- **To call an API in machine level**

```
GET /esa/api/v2.0/config/dictionaries?device_type=esa&mode=machine&host_name=<host_name>
```

Authentication APIs

The Configuration APIs must be authenticated by basic authentication (using username and password) or JWT. The Authentication APIs generate JWT and do not disclose the actual username and password on third-party platforms.

Note If you change a user role or password, you must regenerate the client credentials.

The save and load configurations are not supported for client credentials.

Note Authentication APIs do not support external authentication methods (LDAP, RADIUS, and SAML).

The cluster level is applied by default in cluster mode for Authentication APIs.

Perform the following steps to generate JWT:

Step 1 Generate and retrieve client credentials using `client_creds` API.

Step 2 Generate JWT using client credentials with `token` API.

The token generated can be used to authenticate configuration APIs.

Note You can provide basic authentication also to authenticate APIs.

Client Credentials APIs

The `client_creds` API can be used to read existing Client Credentials, generate Client Credentials, or refresh Client Secret for a user.

The various API categories for Client Credentials are:

- Retrieving Client Credentials, on page 100
- Generating Client Credentials, on page 101
- Refreshing Client Secret, on page 102
- Deleting Client Credentials, on page 103

Retrieving Client Credentials

You can retrieve Client Credentials with different attributes as explained below:

Synopsis	[Standalone Machine] `GET /esa/api/v2.0/config/client_creds?device_type=esa` [Cluster Machine] `GET /esa/api/v2.0/config/client_creds?device_type=esa`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve Client Credentials :

Sample Request

```
GET /esa/api/v2.0/config/client_creds?device_type=esa
HTTP/1.1 cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjQk Content-Type: application/json
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:22:20 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 189
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
"data": {
"secret_TOC": "2022-10-18 09:43:13 UTC",
"client_id": "bace0701-15e3-5144-97c5-47487d543032",
"client_secret":
"427c8fd2083c3fd1a5b6d98cfde32ff51080109cd3c775e640785ba252ba888e"
}
}
```

Generating Client Credentials

You can generate Client Credentials with different attributes as explained below:

Synopsis	[Standalone Machine] `POST /esa/api/v2.0/config/client_creds?device_type=esa` [Cluster Machine] `POST /esa/api/v2.0/config/client_creds?device_type=esa`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to generate Client Credentials:

Sample Request

```
POST /esa/api/v2.0/config/client_creds?device_type=esa
HTTP/1.1 cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjQk
Content-Type: application/json
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:22:20 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 189
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
    "data": {
        "message": "Client Credentials for the user have been generated successfully."
    }
}
```

Refreshing Client Secret

You can refresh the Client Secret with different attributes as explained below:

Synopsis	[Standalone Machine] `PUT /esa/api/v2.0/config/client_creds/refresh_client_secret?device_type=esa` [Cluster Machine] `PUT /esa/api/v2.0/config/client_creds/refresh_client_secret?device_type=esa`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to refresh the Client Secret :

Sample Request

```
PUT /esa/api/v2.0/config/client_creds/ refresh_client_secret?device_type=esa
HTTP/1.1 cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjQk
Content-Type: application/json
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:22:20 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 189
Connection: keep-alive Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
 "data": {
  "message": "Client Secret for the user has been refreshed successfully."
 }
}
```

Deleting Client Credentials

You can delete Client Credentials with different attributes as explained below:

Synopsis	[Standalone Machine] `DELETE /esa/api/v2.0/config/client_creds?device_type=esa` [Cluster Machine] `DELETE /esa/api/v2.0/config/client_creds?device_type=esa`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to delete Client Credentials:

Sample Request

```
DELETE /esa/api/v2.0/config/client_creds?device_type=esa
HTTP/1.1 cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjQk
Content-Type: application/json
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:22:20 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 189
Connection: keep-alive Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY
{
    "data": {
        "message": "Client Credentials for the user have been deleted successfully."
    }
}
```

Generating JWT Token

JWT is token that authenticates API when we send it in headers of the API. The client credentials are essential to generate a token. For more information on the steps to generate a token, see Authentication APIs, on page 100.

The token has a set time of expiration. For more information on setting the expiration time of the token, see Configuring the Web UI Session Timeout section of the email gateway user guide associated with this release.

When the JWT expires, you can generate a new JWT using the same `token` API. You can generate JWT token with different attributes as explained below:

Synopsis		[Standalone Machine] `POST esa/api/v2.0/config/token?device_type=esa` [Cluster Machine] `POST esa/api/v2.0/config/token?device_type=esa`
Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Content-Type
Response Headers		Content-Type, Content-Length, Connection
Keys in Request Body (See the Sample Request for key hierarchy)	username	This is a required parameter. Specify the username. All API queries must be accompanied with this parameter.
	client_id	This is a required parameter. Specify the client ID of the user. All API queries must be accompanied with this parameter.
	client_secret	This is a required parameter. Specify the client secret of the user. All API queries must be accompanied with this parameter.

Example

This example shows a query to generate JWT token:

Sample Request

```
POST esa/api/v2.0/config/token?device_type=esa
HTTP/1.1
cache-control: no-cache
Content-Type: application/json
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
 {
    "data": {
        "username": "test_cloud_admin",
        "client_id": "871b3f8d-b2a6-5238-a92b-0c50c82cae78",
       "client_secret": "273a54f51b92ec3cb95d54731442d740e8ef2c84dc834a4dd7d5c33e585dbdf2"

    }
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:23:31 GMT
```

```
Content-Type: application/json; charset=UTF-8
Content-Length: 627
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
    "data": {
        "username": "test_cloud_admin",
        "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6InRlc3RfY2xvdWRfYWRtaW4iLCJzZXNza

W9uRW5kVGltZSI6MTY2NzU4NTAwNSwiaXMyRmFjdG9yQ2hlY2tSZXF1aXJlZCI6ZmFsc2UsInVzZXIiO...",
        "user_role": "Cloud Administrator"
    }
}
```

Using token to authenticate APIs

You can use the token generated using Generating JWT Token API to authenticate other APIs.

Example

This example shows a query to read all URL lists using the generated token.

Sample Request

```
GET /esa/api/v2.0/config/url_lists?device_type=esa
jwtToken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6InRlc3RfY2xvdWRfYWRtaW4iLCJzZXNzaW9uRW5kV
GltZSI6MTY2NzU4NTAwNSwiaXMyRmFjdG9yQ2hlY2tSZXF1aXJlZCI6ZmFsc2UsInVzZXIiOiJOT05FVV...
Content-Type: application/json
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:25:00 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 139
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
jwtToken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNjY5...
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
 "data": {
  "a-aom": {
   "used_by": "",
   "urls_count": 1,
   "urls": [
    "b1a.com"
```

```
   ]
  },
  "a-aom1": {
   "used_by": "",
   "urls_count": 1,
   "urls": [
    "b1a.com"
   ]
  }
 }
}
```

Using Basic Authentication to Authenticate API

You can also use basic authentication to authenticate other APIs.

Example

This example shows a query to retrieve a list of all URL Lists:

Sample Request

```
GET /esa/api/v2.0/config/url_lists?device_type=esa

HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjQk
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:16:18 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 139
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
    "data": {
        "abc": {
            "used_by": "",
            "urls_count": 1,
            "urls": [
                "aaaa.com"
            ]
        },
        "testing": {
            "used_by": "",
            "urls_count": 2,
            "urls": [
                "10.10.10.10",
                "a.com"
            ]
        }
```

```
    }
}
```

URL Lists APIs

You can retrieve specific URL Lists information from your email gateway. The various API categories for URL Lists APIs are:

Retrieving a List of All URL Lists

You can retrieve a list of all URL Lists with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/url_lists?device_type=esa`
		[Cluster Machine]
		`GET /esa/api/v2.0/config/url_lists?device_type=esa&mode=cluster`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve a list of all URL Lists:

Sample Request

```
GET /esa/api/v2.0/config/url_lists?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNj....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:16:18 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 139
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
    "data": {
        "abc": {
            "used_by": "",
            "urls_count": 1,
            "urls": [
                "aaaa.com"
            ]
        },
        "testing": {
            "used_by": "",
            "urls_count": 2,
            "urls": [
                "10.10.10.10",
                "a.com"
            ]
        }
    }
}
```

Retrieving Details for a Specified URL List

You can retrieve details for a specified URL list with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/url_lists/<url_list_name>?device_type=esa`
		[Cluster Machine]
		`GET /esa/api/v2.0/config/url_lists/<url_list_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve details for a specified URL list:

Sample Request

```
GET/esa/api/v2.0/config/url_lists/abc?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNjY5MDEyMTE...
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:08:46 GMT
```

```
Content-Type: application/json; charset=UTF-8
Content-Length: 63
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
    "data": {
        "used_by": "",
        "urls_count": 1,
        "urls": [
            "aaaa.com"
        ]
    }
}
```

Adding URL Lists

You can add URL lists with different attributes as explained below:

Synopsis		[Standalone Machine]
		`POST /esa/api/v2.0/config/url_lists/<url_list_name>?device_type=esa`
		[Cluster Machine]
		`POST /esa/api/v2.0/config/url_lists/<url_list_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.

Request Headers		Host, Accept, Content-Type, JWT token
Response Headers		Content-Type, Content-Length, Connection
Key in Request Body	urls	This is a required parameter. Specify the list of URLs to add to the URL list.

Example

This example shows a query to add a URL list:

Sample Request

```
POST /esa/api/v2.0/config/url_lists/new12?device_type=esa
HTTP/1.1
cache-control: no-cache
Content-Type: application/json
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxN...
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "urls": ["a1.com"]
    }
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:40:05 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 43
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
    "data": {
        "message": "Added Successfully"
    }
}
```

Editing URL Lists

You can edit URL lists with different attributes as explained below:

Synopsis		[Standalone Machine]
		`PUT /esa/api/v2.0/config/url_lists/<url_list_name>?device_type=esa`
		[Cluster Machine]
		`PUT /esa/api/v2.0/config/url_lists/<url_list_name>?device_type=esa&mode=cluster`
		Warning The **PUT** command replaces all contents of an existing URL list.

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, Content-Type, JWT token
Response Headers		Content-Type, Content-Length, Connection
Keys in Request Body(See the Sample Request for key hierarchy)	name	This is an optional parameter. Specify the name of the URL list if it has to be updated.
	urls	This is a required parameter. Specify the list of URLs to update to the URL list.

Example

This example shows a query to edit a URL list:

Sample Request

```
PUT /esa/api/v2.0/config/url_lists/new12?device_type=esa
HTTP/1.1
cache-control: no-cache
Content-Type: application/json
```

```
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNjY5MDEyMTE...
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "name": "new3",
        "urls": ["a123.com"]
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:54:38 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 45
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY
{
    "data": {
        "message": "Updated Successfully"
    }
}
```

Deleting URL Lists

You can delete single or multiple URL lists with different attributes as explained below:

Synopsis	[Standalone Machine]
	`DELETE /esa/api/v2.0/config/url_lists?device_type=esa`
	[Cluster Machine]
	`DELETE /esa/api/v2.0/config/url_lists?device_type=esa&mode=cluster`

Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, Content-Type, JWT token
Response Headers		Content-Type, Content-Length, Connection
Key in Request Body	url_lists	This is a required parameter. Specify the list of URL lists to delete.

Example

This example shows a query to delete single or multiple URL lists:

Sample Request

```
DELETE /esa/api/v2.0/config/url_lists?device_type=esa
HTTP/1.1
cache-control: no-cache
Content-Type: application/json
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNjY5MDEy...
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "url_lists": ["new3", "abc"]
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 10:19:55 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 45
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

{
    "data": {
        "message": "Deleted Successfully"
    }
}
```

Dictionary APIs

You can retrieve dictionary information from your email gateway. The various API categories for dictionaries are:

Retrieving List of All Configured Dictionaries

You can retrieve list of all dictionaries configured in your email gateway with different attributes as explained below:

Synopsis	[Standalone Machine]
	`GET /esa/api/v2.0/config/dictionaries? device_type=esa`
	[Clustered Machine]
	`GET /esa/api/v2.0/config/dictionaries? device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the list of all dictionaries configured in your email gateway:

Sample Request

```
GET/esa/api/v2.0/config/dictionaries?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....

Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
      "data": {
          "NewDict": {
               "ignorecase": 0,
               "words_count": {
                   "term_count": 5,
```

```
                    "smart_identifier_count": 2
                },
                "wholewords": 1,
                "words": [
                    [
                        "À term 1",
                        1
                    ],
                    [
                        "jsu",
                        1
                    ],
                    [
                        "jsu1",
                        1
                    ],
                    [
                        "*credit",
                        2,
                        "prefix"
                     ],
                     [
                        "*aba",
                        1,
                        ""
                     ]
             ],
             "encoding": "utf-8"
        },
        "New-Dict.": {
            "ignorecase": 0,
            "words_count": {
                "term_count": 2,
                "smart_identifier_count": 2
            },
            "wholewords": 1,
            "words": [
            [
                   "*credit",
                   2,
                   "prefix"
            ],
            [
                    "*aba",
                    1,
                    ""
             ],
             [
                    "À term 1",
                    1
             ],
             [
                    "jsu",
                    1
             ]
        ],
        "encoding": "utf-8"
    },
    "NewDictionary": {
        "ignorecase": 0,
        "words_count": {
            "term_count": 2,
            "smart_identifier_count": 2
        },
```

```
        "words": [
            [
                "*credit",
                2,
                "prefix"
             ],
             [
                 "*aba",
                 1,
                 ""
             ],
             [
                 "À term 1",
                 1
              ],
              [
                 "jsu",
                 1
              ]
          ],
          "wholewords": 1,
          "encoding": "utf-8"
},
"New-Dict12": {
    "ignorecase": 0,
    "words_count": {
        "term_count": 2,
        "smart_identifier_count": 2
    },
    "words": [
         [
             "*credit",
             2,
             "prefix"
          ],
          [
             "*aba",
             1,
             ""
          ],
          [
             "À term 1",
             1
          ],
          [
              "\\tjsu",
              1
          ]
      ],
      "wholewords": 1,
      "encoding": "utf-8"
},
"New-Dict1": {
     "ignorecase": 0,
     "words_count": {
         "term_count": 2,
         "smart_identifier_count": 2
     },
     "wholewords": 1,
     "words": [
         [
             "*credit",
             2,
             "prefix"
```

```
            ],
            [
                "*aba",
                1,
                ""
            ],
            [
                "À term 1",
                1
            ],
            [
                "\\\tjsu",
                1
            ]
        ],
        "encoding": "utf-8"
    }
  }
}
```


Retrieving Information of Specific Configured Dictionary

You can retrieve information of a specific dictionary configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token

Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve information of a specific dictionary configured in your email gateway:

Sample Request

```
GET/esa/api/v2.0/config/dictionaries/NewDict?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
       "data": {
           "ignorecase": 0,
           "words_count": {
               "term_count": 5,
               "smart_identifier_count": 2
           },
           "wholewords": 1,
           "words": [
               [
                  "À term 1",
                  1
               ],
               [
                  "jsu",
                  1
               ],
               [
                  "jsu1",
                  1
                ],
                [
                   "*credit",
                   2,
                   "prefix"
                 ],
                 [
                    "*aba",
                    1,
                    ""
                 ]
           ],
           "encoding": "utf-8"
      }
}
```

Adding a New Dictionary

You can add a new dictionary in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`POST /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa`
		[Clustered Machine]
		`POST /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Keys in Request Body (See the Sample Request for the key hierarchy)	ignorecase	This is a required parameter. Indicates if the term that needs to be matched is case-sensitive (represented by "1") or not case-sensitive (represented by "0").
	wholewords	This is a required parameter. Indicates if the words need to be matched completely (represented by "1") or not completely (represented by "0").
	words	This is a required parameter. A list of terms to add to a dictionary. The term can have a weight of (0-10) associated with it. If no weight is given, the default weight is taken as "1." A smart identifier can have an additional parameter - "prefix" associated with it. If no value is mentioned, no prefix is taken as default.
	encoding	This is a required parameter. Denotes the encoding used for the terms. **Note** Only UTF-8 encoding is supported in this release.

Example

This example shows a query to add a new dictionary in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/dictionaries/New-Dict?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "ignorecase": 0,
        "wholewords": 1,
        "words": [
            [
                "*credit",
                2,
                "prefix"
            ],
            ["*aba"],
            ["À term 1"]
        ],
        "encoding": "utf-8"
    }
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
```

```
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
      "data": {
          "message": "Added Successfully"
     }
}
```

Editing an Existing Dictionary

You can edit an existing dictionary configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`PUT: /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa`
		[Clustered Machine]
		`PUT: /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa&mode=cluster`
		Warning The **PUT** command replaces all contents of an existing dictionary entry.

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Keys in Request Body (Refer the Sample Request for the key hierarchy)	name	This is an optional parameter. If you want to modify the name of the dictionary, use the "name" parameter with the value as the new name of the dictionary.
	ignorecase	This is a required parameter. Indicates if the term that needs to be matched is case-sensitive (represented by "1") or not case-sensitive (represented by "0").
	wholewords	This is a required parameter. Indicates if the words need to be matched completely (represented by "1") or not completely (represented by "0").
	words	This is a required parameter. A list of terms to add to a dictionary. The term can have a weight of (0-10) associated with it. If no weight is given, the default weight is taken as "1." A smart identifier can have an additional parameter - "prefix" associated with it. If no value is mentioned, no prefix is taken as default.
	encoding	This is a required parameter. Denotes the encoding used for the terms. **Note** Only UTF-8 encoding is supported in this release.

Example

This example shows a query to edit an existing dictionary configured in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/dictionaries/NewDict?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "ignorecase": 0,
        "wholewords": 1,
        "words": [
            [
                "jsu",
                7
            ],
            [
                "À term 1",
                "",
                3
            ],
            [
                "*ssn",
                2,
```

```
                "prefix"
            ],
            [
                "*credit",
                2,
                "prefix"
            ],
            [
                "eno"
            ]
        ],
        "encoding": "utf-8"
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close ' {
{
    "data": {
     "message": "Updated Successfully"
    }
}
```

Deleting an Existing Dictionary

You can delete an existing dictionary configured in your email gateway with different attributes as explained below:

Synopsis	[Standalone Machine]
	`DELETE /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa`
	[Clustered Machine]
	`DELETE /esa/api/v2.0/config/dictionaries/<dictionary_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to delete an existing dictionary configured in your email gateway:

Sample Request

```
DELETE /esa/api/v2.0/config/dictionaries/NewDictionary?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
     "data": {
        "message": "Deleted Successfully"
    }

}
```

Retrieving List of Words from Specific Dictionary

You can retrieve a list of words from a specific dictionary configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/dictionaries/<dictionary_name> /words?device_type=esa`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/dictionaries/<dictionary_name>/ words?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve a list of words from a specific dictionary configured in your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/dictionaries/NewDict/words?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
         "data": {
              "words_count": {
                  "term_count": 3,
                  "smart_identifier_count": 2
               },
               "words": [
                   [
                       "jsu",
                       7
                    ],
                    [
                        "À term 1",
                        3
                    ],
                    [
                         "*ssn",
                         2,
                         "prefix"
                    ],
                    [
                        "*credit",
                        2,
                        "prefix"
                     ],
                     [
                         "eno",
                         1
                     ]
            ]
    }
}
```

Adding Words to Specific Dictionary

You can add words to a specific dictionary configured in your email gateway with different attributes as explained below:

Synopsis	[Standalone Machine]
	`POST /esa/api/v2.0/config/dictionaries/<dictionary_name>/words?device_type=esa`
	[Clustered Machine]
	`POST /esa/api/v2.0/config/dictionaries/<dictionary_name> /words?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection
Key in Request Body	words	This is a required parameter. A list of terms to add to a dictionary. The term can have a weight of (0-10) associated with it. If no weight is given, the default weight is taken as "1." A smart identifier can have an additional parameter - "prefix" associated with it. If no value is mentioned, no prefix is taken as default.

Example

This example shows a query to add words to a specific dictionary configured in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/dictionaries/NewDict/words?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "words": [
            [
                "tjsu"
```

```
            ],
            [
                "*credit",
                2,
                "prefix"
            ]
        ]
    }
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
     "data": {
         "message": "Added Successfully"
     }
}
```

Modifying Words in Specific Dictionary

You can modify the words in a specific dictionary configured in your email gateway with different attributes as explained below:

Synopsis	[Standalone Machine]
	`PUT /esa/api/v2.0/config/dictionaries /<dictionary_name>/words?device_type=esa`
	[Clustered Machine]
	`PUT /esa/api/v2.0/config/dictionaries /<dictionary_name>/words?device_type=esa&mode=cluster`
	Warning The **PUT** command replaces all contents of specified terms in an existing dictionary.

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection
Key in Request Body	words	This is a required parameter. A list of terms to add to a dictionary. The term can have a weight of (0-10) associated with it. If no weight is given, the default weight is taken as "1." A smart identifier can have an additional parameter - "prefix" associated with it. If no value is mentioned, no prefix is taken as default.

Example

This example shows a query to modify the words in a specific dictionary configured in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/dictionaries/NewDict/words?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "words": [
            [
                "ta da",
```

```
                3
            ],
            [
                "A t",
                9
            ]
        ]
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
      "data": {
          "message": "Updated Successfully"
     }
}
```

Deleting Existing Words from Specific Dictionary

You can delete existing words from a specific dictionary configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`DELETE /esa/api/v2.0/config/dictionaries/<dictionary_name>/words?device_type=esa`
		[Clustered Machine]
		`DELETE /esa/api/v2.0/config/dictionaries/<dictionary_name>/words?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` Specify the mode. This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.

Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection
Key in Request Body	words	This is a required parameter. A list of terms that need to be deleted.

Example

This example shows a query to delete the existing words from a specific dictionary in your email gateway:

Sample Request

```
DELETE /esa/api/v2.0/config/dictionaries/New-words/words?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
 "data": {
        "words": [
            "*credit", "word1", "word2"
        ]
 }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
       "message": "Deleted Successfully"
    }
}
```

HAT APIs

You can retrieve Host Access Table (HAT) information from your email gateway. The various API categories for HAT are:

- Retrieving Configuration Details of All Sender Groups in Listener , on page 135
- Retrieving Configuration Details for Specific Sender Group, on page 139
- Creating Sender Group with Specific Configuration, on page 140
- Editing Existing Configuration Details of Specific Sender Group, on page 144
- Deleting Specific Sender Group, on page 148

Retrieving Configuration Details of All Sender Groups in Listener

You can retrieve configuration details of all sender groups for a specific listener configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/sender_groups/listener /<listener_name>?device_type=esa`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/sender_groups /listener/<listener_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve configuration details of all sender groups for a specific listener configured in your email gateway:

Sample Request

```
GET
/esa/api/v2.0/config/sender_groups/listener/Incoming_mail?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
          "data": {
              "ALL": {
                  "dns_list": [
                      "example.com",
                      ".ex"
                  ],
                  "external_threat_feeds": [
                      "Threat_HAT_another",
                      "Threat_HAT"
                   ],
                   "description": "",
                   "flow_profile": "ACCEPTED",
                   "senders": {
                        "ip_address_list": [
                            {
                                "sender_name": ".cisco.com",
                                "description": ""
                             },
                             {
                                "sender_name": "example_none_d.com",
                                "description": ""
                             }
                      ],
                      "geo_list": [
                          {
                              "sender_name": "India",
                              "description": "Country"
                          }
                      ]
                 },
                 "sbrs": [
                     1,
                     10
                 ],
                 "order": 9,
                 "sbrs_none": true,
                 "dns_host_verification": {
                     "lookup_not_matched": "true",
                     "record_not_exist": "false",
                     "lookup_fail": "false"
                  }
          },
          "CREATE_API": {
```

```
            "dns_list": [
                "example.com",
                ".ex"
            ],
            "external_threat_feeds": [
                "Threat_HAT",
                "Threat_HAT_another"
            ],
            "description": "",
            "flow_profile": "ACCEPTED",
            "senders": {
                 "ip_address_list": [
                     {
                         "sender_name": "10.10.10.",
                         "description": ""
                     },
                     {
                          "sender_name": ".tada",
                          "description": ""
                      }
                 ],
                 "geo_list": [
                     {
                         "sender_name": "India",
                         "description": "My India"
                 }
            ]
       },
       "sbrs": [
           -10,
           10
       ],
       "order": 5,
       "sbrs_none": true,
       "dns_host_verification": {
           "lookup_not_matched": "true",
           "record_not_exist": "false",
           "lookup_fail": "false"
       }
    },
    "SUSPECTLIST": {
        "dns_list": [
            "query.blocked_list.example",
            "example2.com"
        ],
        "external_threat_feeds": [
            "Threat_HAT",
            "Threat_HAT_another"
        ],
        "description": "Suspicious senders are throttled",
        "flow_profile": "THROTTLED",
        "senders": {},
        "sbrs": [
             -3,
             -1
        ],
        "order": 3,
        "sbrs_none": false,
        "dns_host_verification": {
            "lookup_not_matched": "true",
            "record_not_exist": "true",
            "lookup_fail": "true"
         }
     },
```

```
    "BLOCKED_LIST": {
        "dns_list": [],
        "external_threat_feeds": [],
        "description": "Spammers are rejected",
        "flow_profile": "BLOCKED",
        "senders": {},
        "sbrs": [
            -10,
             -3
        ],
        "order": 2,
        "sbrs_none": false,
        "dns_host_verification": {
            "lookup_not_matched": "false",
            "record_not_exist": "false",
            "lookup_fail": "false"
         }
     },
     "UNKNOWNLIST": {
         "dns_list": [],
         "external_threat_feeds": [],
       "description": "Reviewed but undecided, continue normal acceptance", "flow_profile":
"ACCEPTED",
         "senders": {},
         "sbrs": [
             -1,
             10
         ],
         "order": 4,
         "sbrs_none": true,
         "dns_host_verification": {
             "lookup_not_matched": "false",
             "record_not_exist": "false",
             "lookup_fail": "false"
          }
     },
     "ALLOWED_LIST": {
         "dns_list": [],
         "external_threat_feeds": [
             "Threat_HAT"
         ],
         "description": "My trusted senders have no anti-spam scanning or rate limiting",

         "flow_profile": "TRUSTED",
         "senders": {},
         "sbrs": [
             -5,
              1
         ],
         "order": 1,
         "sbrs_none": true,
         "dns_host_verification": {
             "lookup_not_matched": "false",
             "record_not_exist": "false",
             "lookup_fail": "false"
        }
    },
  }
}
```

Retrieving Configuration Details for Specific Sender Group

You can retrieve configuration details for a specific sender group configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/sender_groups/listener/<listener_name>/sender_group/<sender_group_name>?device_type=esa`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/sender_groups/listener/<listener_name>/sender_group/<sender_group_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve configuration details for a specific sender group configured in your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/sender_groups/listener/Incoming_mail/
sender_group/ALL??device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
```

```
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
     "data": {
         "dns_list": [
             "example.com",
             ".ex"
         ],
         "external_threat_feeds": [
             "Threat_HAT_another",
             "Threat_HAT"
         ],
         "description": "",
         "flow_profile": "ACCEPTED",
         "senders": {
             "ip_address_list": [
                 {
                     "sender_name": ".cisco.com",
                     "description": ""
                 },
                 {
                     "sender_name": "example_none_d.com",
                     "description": ""
                 }
  ],
  "geo_list": [
      {
          "sender_name": "India",
          "description": "Country"
      }
   ]
},
"sbrs": [
    1,
    10
],
"order": 9,
"sbrs_none": true,
"dns_host_verification": {
    "lookup_not_matched": "true",
    "record_not_exist": "false",
    "lookup_fail": "false"
     }
  }
}
```

Creating Sender Group with Specific Configuration

You can create a sender group with specific configuration details in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`POST /esa/api/v2.0/config/sender_groups/listener /<listener_name>/sender_group/<sender_group_name>?device_type=esa`
		[Clustered Machine]
		`POST /esa/api/v2.0/config/sender_groups/listener /<listener_name>/sender_group/<sender_group_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Keys in Request Body (See the Sample Request for the key hierarchy)	flow_profile	This is a required parameter. The name of the Mail Flow Policy associated with the sender group.
	order	This is an optional parameter. The index is used to define the position of the sender group. The sender group is moved to the last position in the sender group list by default if you do not provide an index.
	description	This is an optional parameter. The description for the sender group.
	sbrs_none	This is an optional parameter. It includes the SBRS score of "None." The values can be "true" or "false." The value must not be empty.
	senders	The key is an optional parameter. The key contains a dictionary, which can have two lists - `ip_address_list` and `geo_list`.
	ip_address_list	The key is an optional parameter. The key contains data related to IPv4 or IPv6 addresses, host names, and partial host names for the sender group. The key is valid for sender groups in public and private listeners.
	geo_list	The key is an optional parameter. **Note** The key is not a supported parameter for sender groups in private listeners. The key contains data related to the Geolocation of the sender group. The key is valid for sender groups in public listeners.
	sender_name	The key is a required parameter when the `ip_address_list` or `geo_list` key is present in the sender group. The key contains data for a sender in the sender group. The data can be: • IPv4 or IPv6 addresses, hostname, and partial hostname for the `ip_address_list`. • Country name for the `geo_list`.
	description	The key is an optional parameter. The key contains data that describes the sender in the sender group.
	external_threat_feeds	

		This is an optional parameter. The list of External Threat Feed sources (configured in the Mail Policy > External Threat Feed Manager page in the web interface).
	sbrs	This is an optional parameter SenderBase Reputation Score (SBRS) for the sender group. The values can be from -10 to 10. The values are represented in a list format [1,10] for the API input.
	dns_list	This is an optional parameter The DNS lists and the values are represented in a list format.
	dns_host_verification	This is an optional parameter A dictionary that consists of DNS host verification configurations.
	lookup_not_matched	This is an optional parameter The values can be "true" or "false." The value must not be empty. The value - "true " indicates that the - Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).
	record_not_exist	This is an optional parameter. The values can be "true" or "false." The value must not be empty. The value - "true " indicates that the Connecting host PTR record does not exist in DNS.
	lookup_fail	This is an optional parameter The values can be "true" or "false." The value must not be empty. The value - "true " indicates that the Connecting host PTR lookup fails because of temporary DNS failure.

Example

This example shows a query to create a sender group with specific configuration details in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/sender_groups/listener/Incoming_mail/
sender_group/SenderGroupTest?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "dns_list": [
            "example.com",
            ".ex"
```

```
        ],
        "external_threat_feeds": [
            "Thread_HAT_another",
            "Thread_HAT"
        ],
        "description": "",
        "flow_profile": "ACCEPTED",
        "senders": {
            "ip_address_list": [
                {
                    "sender_name": ".cisco.com",
                    "description": "Cisco"
                },
                {
                    "sender_name": "example_none_d.com",
                    "description": ""
                }
            ],
            "geo_list": [
                {
                    "sender_name": "India",
                    "description": ""
                }
            ]
        },
        "sbrs": [
            1,
            10
        ],
        "order": 9,
        "sbrs_none": "true",
        "dns_host_verification": {
            "lookup_not_matched": "true",
            "record_not_exist": "false",
            "lookup_fail": "false"
        }
    }
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
       "message": "Added Successfully"
    }
}
```

Editing Existing Configuration Details of Specific Sender Group

You can edit existing configuration details of a specific sender group configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`PUT /esa/api/v2.0/config/ sender_groups/listener/<listener_name> /sender_group/<sender_group_name>?device_type=esa`
		[Clustered Machine]
		`PUT /esa/api/v2.0/config/ sender_groups/listener/<listener_name> /sender_group/<sender_group_name>?device_type=esa&mode=cluster`
		Warning The **PUT** command replaces all contents of an existing HAT entry.

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Keys in Request Body (See the Sample Request for the key hierarchy)	name	This is an optional parameter. Use this parameter to rename the existing sender group. The value is the new name of the sender group.
	flow_profile	This is a required parameter. The name of the Mail Flow Policy associated with the sender group.
	order	This is an optional parameter. The index is used to define the position of the sender group. The sender group is moved to the last position in the sender group list by default if you do not provide an index.
	description	This is an optional parameter. The description for the sender group.
	sbrs_none	This is an optional parameter. It includes the SBRS score of "None." The values can be "true" or "false." The value must not be empty.
	senders	The key is an optional parameter. The key contains a dictionary, which can have two lists - `ip_address_list` and `geo_list`.
	ip_address_list	The key is an optional parameter. The key contains data related to IPv4 or IPv6 addresses, host names, and partial host names for the sender group. The key is valid for sender groups in public and private listeners.
	geo_list	The key is an optional parameter. **Note** The key is not a valid parameter for sender groups in private listeners. The key contains data related to the Geolocation of the sender group. The key is valid for sender groups in public listeners.
	sender_name	The key is a required parameter when the `ip_address_list` or `geo_list` key is present in the sender group. The key contains data for a sender in the sender group. The data can be: • IPv4 or IPv6 addresses, hostname, and partial hostname for the `ip_address_list`. • Country name for the `geo_list`.
	description	

		The key is an optional parameter. The key contains data that describes the sender in the sender group.
	external_threat_feeds	The key is an optional parameter. The list of External Threat Feed sources (configured in the Mail Policy > External Threat Feed Manager page in the web interface).
	sbrs	The key is an optional parameter. SenderBase Reputation Score (SBRS) for the sender group. The values can be from -10 to 10. The values are represented in a list format [1,10] for the API input.
	dns_list	The key is an optional parameter. The DNS lists and the values are represented in a list format.
	dns_host_verification	The key is an optional parameter. A dictionary that consists of DNS host verification configurations.
	lookup_not_matched	The key is an optional parameter. The values can be "true" or "false." The value must not be empty. The value - "true " indicates that the - Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).
	record_not_exist	The key is an optional parameter. The values can be "true" or "false." The value must not be empty. The value - "true " indicates that the Connecting host PTR record does not exist in DNS.
	lookup_fail	This is an optional parameter. The values can be "true" or "false." The value must not be empty. The value - "true " indicates that the Connecting host PTR lookup fails because of temporary DNS failure.

Example

This example shows a query to edit configuration details of a specific sender group configured in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/
sender_groups/listener/Incoming_mail/sender_group/ALL?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

```
{
    "data": {
        "flow_profile":
"ACCEPTED",
        "sbrs_none": "true",
        "senders": {
             "ip_address_list":
[
                 {

"sender_name": ".cisco.com"
                 }
            ],
            "geo_list": [
                {
"sender_name": "India",
"description": "PUT update"
                 }
         ]
   },

"external_threat_feeds":
["Thread_HAT",
"Thread_HAT_another"],
        "sbrs": [1,10],
        "dns_list":
["example.com", ".ex"],
"dns_host_verification": {
"lookup_not_matched": "true",
"record_not_exist": "false"
        }
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
   "data": {
      "message": "Updated Successfully"
   }
}
```

Deleting Specific Sender Group

You can delete a specific sender group configured in your email gateway with different a ttributes as explained below:

Synopsis	[Standalone Machine]
	`DELETE /esa/api/v2.0/config/sender_groups/listener/<listener_name>/sender_group/<sender_group_name>?device_type=esa`
	[Clustered Machine]
	`DELETE /esa/api/v2.0/config/sender_groups/listener/<listener_name>/sender_group/<sender_group_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query delete a specific sender group configured in your email gateway:

Sample Request

```
DELETE /esa/api/v2.0/config/
sender_groups/listener/Incoming_mail/sender_group/ALLOWED_LIST?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
       "message": "Deleted Successfully"
    }
}
```

Retrieving Information of All Senders of Specific Sender Group

You can retrieve information of all senders of a specific sender group configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/sender_groups/sender_list /<listener_name>/<sender_group_name>?device_type=esa`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/sender_groups/sender_list /<listener_name>/<sender_group_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve information of a ll senders of a specific sender group configured in your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/sender_groups/sender_list/Incoming_mail/ALL?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
        "ip_address_list": [
     {
            "sender_name": ".cisco.com",
            "description": "Cisco"
     },
     {
            "sender_name": "example_none_d.com",
            "description": ""
      }
  ],
  "geo_list": [
      {
          "sender_name": "India",
          "description": "Country"
        }
     ]
  }
}
```

Adding Senders to Existing Sender Group

You can add senders to an existing sender group configured in your email gateway with different attributes as explained below:

Synopsis	[Standalone Machine]
	`POST /esa/api/v2.0/config/sender_groups/sender_list/<listener_name>/<sender_group_name>?device_type=esa`
	[Clustered Machine]
	`POST /esa/api/v2.0/config/ sender_groups/sender_list/<listener_name>/<sender_group_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Keys in Request Body (See the Sample Request for the key hierarchy)	senders	The key is a required parameter. The key contains a dictionary, which can have two lists - `ip_address_list` and `geo_list`.
	ip_address_list	The key is a required parameter. The key contains data related to IPv4 or IPv6 addresses, host names, and partial host names for the sender group. The key is valid for sender groups in public and private listeners.
	geo_list	The key is a required parameter. **Note** The key is not a valid parameter for sender groups in private listeners. The key contains data related to the Geolocation of the sender group. The key is valid for sender groups in public listeners.
	sender_name	The key is a required parameter when the `ip_address_list` or `geo_list` key is present in the sender group. The key contains data for a sender in the sender group. The data can be: • IPv4 or IPv6 addresses, hostname, and partial hostname for the `ip_address_list`. • Country name for the `geo_list`.
	description	The key is not a required parameter. The key contains data describing the sender in the sender group.

Example

This example shows a query to add senders to an existing sender group configured in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/ sender_groups/sender_list/private_list/ALL?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "senders": {
            "ip_address_list": [
             {
                    "sender_name": "sender1.com",
                    "description": "sender 1"
             },
             {
                    "sender_name": "sender2.com",
```

```
                    "description": "sender 2"
                }
            ],
            "geo_list": [
                {
                    "sender_name": "India",
                    "description": "my country"
                },
                {
                    "sender_name": "Iceland",
                    "description": "country"
                }
            ]
        }
    }
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
       "message": "Added Successfully"
    }
}
```

Deleting Specific Senders from Sender Group

You can delete specific senders from a sender group configured in your email gateway with different attributes as explained below:

Synopsis	[Standalone Machine]
	`DELETE /esa/api/v2.0/config/sender_groups/sender_list/<listener_name>/<sender_group_name>?device_type=esa`
	[Clustered Machine]
	`DELETE /esa/api/v2.0/config/sender_groups/sender_list<listener_name>/<sender_group_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` Specify the mode. This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection
Key in Request Body	senders	The key is a required parameter. The key contains the names of the senders to delete.

Example

This example shows a query to delete specific senders from a sender group configured in your email gateway:

Sample Request

```
DELETE /esa/api/v2.0/config/sender_groups/sender_list/Incoming_mail/ALL?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
     "data": {
       "senders": [
            "India",
"sender1.com"
          ]
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
```

```
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
       "message": "Deleted Successfully"
   }
}
```

Updating Order of Sender Groups for Listener

You can update the order of the sender groups for a listener configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`PUT /esa/api/v2.0/config/sender_groups/order /<listener_name>?device_type=esa`
		[Clustered Machine]
		`PUT /esa/api/v2.0/config/sender_groups/order /<listener_name>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Key in Request Body	sender_group_name	The key is the sender group name, and the value is the order in which the sender group is present. **Note** You must provide the order number for all configured sender groups for a specified listener to avoid discrepancies in the order of the sender groups.

Example

This example shows a query to update the order of the sender groups for a listener configured in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/sender_groups/order/myListener?device_type=esa HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "BLOCKED_LIST": 3,
        "ALLOWED_LIST": 1,
        "SUSPECTLIST": 4,
        "UNKNOWNLIST": 2
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
       "message": "Updated Successfully"
   }
}
```

Finding Senders in Sender Groups

You can search for any sender in the sender groups configured in your email gateway.

You can search for any pattern based on the sender name in the following two ways:

- Search in all sender groups across all configured listeners.
- Search in a specific sender group for a specific listener.

Related Topics

- Searching for Senders in All Sender Groups across All Configured Listeners, on page 158
- Searching for Senders in Specific Sender Group for Specific Listener, on page 159

Searching for Senders in All Sender Groups across All Configured Listeners

You can search for senders in all sender groups across all listeners configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/sender_groups/find_in_all_senders/<search text>?device_type=esa`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/sender_groups/find_in_all_senders/<search text>?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to search for senders in all sender groups across all listeners configured in your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/sender_groups/find_in_all_senders/arg/?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8 Content-Length: 777
Connection: close
{
     "data": [
            {
                 "sender_name": "Angola",
                 "listener": "listenercl 10.10.5.206:25",
                 "sender group": "sender_group_cl",
                 "description": "argentina"
             }
       ]
}
```

Searching for Senders in Specific Sender Group for Specific Listener

You can search for senders in a specific sender group for a specific listener configured in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/sender_groups/find_senders/listener/<listener_name>/sender_group/<sender group name>/find/<search-text>/?device_type=esa`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/sender_groups/find_senders/listener/<listener_name>/sender_group/<sender group name>/find/<search text>/?device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.

Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to search for senders in a specific sender group for a specific listener configured in your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/sender_groups/find_senders/listener/
listenercl/sender_group/sender_group_cl/find/arg/?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8 Content-Length: 777
Connection: close
{
   "data": [
          {
               "sender_name": "Angola",
               "description": "argentina"
          }
     ]
}
```

Logging APIs

You can retrieve specific log information from your emal gateway. The various API categories for logging are:

- Retrieving Log Subscription Details from Email Gateway, on page 160
- Retrieving All Log Files for Specific Log Subscription, on page 162
- Retrieving Log Files using URL, on page 163

Retrieving Log Subscription Details from Email Gateway

You can retrieve the details of all log subscriptions configured in your email gateway with different attributes as explained below:

Synopsis	`GET /esa/api/v2.0/config/logs/subscriptions`

Supported Resource Attributes	retrieval Method	This is an optional parameter.
		Available values are:
		`aws_s3_push, scp_push, manual, ftp_push, syslog_push`
		`retrievalMethod=manual`
		You can use this parameter to list the log subscriptions configured with the corresponding retrieval method.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the details of all log subscriptions configured in your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/logs/subscriptions
HTTP/1.1
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 3482
Connection: close

{
    "meta": {
        "totalCount": 43
    },
    "data": [
        {
            "retrievalMethod": "manual",
            "type": "AMP Engine Logs",
            "name": "amp"
        },
        {
            "retrievalMethod": "manual",
            "type": "AMP Archive",
            "name": "amparchive"
        },
        ......................
        ......................
        ......................

        {
            "retrievalMethod": "manual",
            "type": "URL Reputation Client Logs",
```

```
            "name": "url_rep_client"
        }
    ]
}
```

Retrieving All Log Files for Specific Log Subscription

You can retrieve the details of all log files for a specific log subscription with different attributes as explained below:

Note This API is only applicable for log subscriptions configured with the manual log retrieval method in your email gateway. The API lists only the log files that are rolled over. You need to use the `name` attribute of the response obtained from the log subscription name in the Retrieving Log Subscription Details from Email Gateway, on page 160 API.

Synopsis		`GET /esa/api/v2.0/logs/<log_subscription_name>/?resource_attribute`
Supported Resource Attributes	Duration	This is an optional parameter. `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` You can use this parameter to list the log files generated within a specified duration.
	File Hash	This is an optional parameter. `computeHash=True` You can use this parameter only when you need to include the file hash value of the log file in the response. **Note** The default value for this parameter is 'False.'
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the details of all log files modified after a specific timestamp:

Sample Request

```
GET
/esa/api/v2.0/logs/audit_logs/?startDate=2020-08-18T04:47:00.000Z&endDate=2020-08-18T13:55:00.000Z&computeHash=True

HTTP/1.1
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close

{
    "meta": {
        "totalCount": 3
    },
    "data": [
        {
            "modificationDate": 1597742834,
            "downloadUrl": "/esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044745.s",
            "name": "audit_logs.@20200818T044745.s",
           "fileHash": "a1b0afb80e784eed91112111a012bf690d494492acf72bc402a0cebf9edcee45",

            "size": 7216
        },
        {
            "modificationDate": 1597726065,
            "downloadUrl": "/esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044738.s",
            "name": "audit_logs.@20200818T044738.s",
           "fileHash": "868da20790addbf11145d2fc28125a24101ff2424621e634f8a1d570f55220cd",

            "size": 291
        },
        {
            "modificationDate": 1597726058,
            "downloadUrl": "/esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044643.s",
            "name": "audit_logs.@20200818T044643.s",
           "fileHash": "29f78fbdbcf3c4f1a20da6c0b38419e42932cab725653cb92fee87fb5a6cf6e4",

            "size": 1403
        }
    ]
}
```

Retrieving Log Files using URL

You can retrieve the content of the log file using the `downloadUrl` attribute of the response obtained from the Retrieving All Log Files for Specific Log Subscription, on page 162 API.

Note This API is only applicable for log subscriptions configured with the manual log retrieval method in your email gateway.

Note When you use this API to retrieve log files populated frequently (for example, Text Mail logs), it is recommended to configure the rollover parameters in the log subscription appropriately and perform periodic pull of log files of smaller size. If you have configured the file size above the default value in the log subscription, it is recommended to invoke the API for each file sequentially.

Synopsis	`GET /esa/api/v2.0/logs/<log_subscription_name>/<log_file_name>` **Note** You need to use the `downloadUrl` attribute of the response obtained from the Retrieving All Log Files for Specific Log Subscription, on page 162 API.
Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection, Content-Disposition

Example

This example shows a query to retrieve the content of the log file using the `downloadUrl` attribute of the resposne obtained from the Retrieving All Log Files for Specific Log Subscription, on page 162 API:

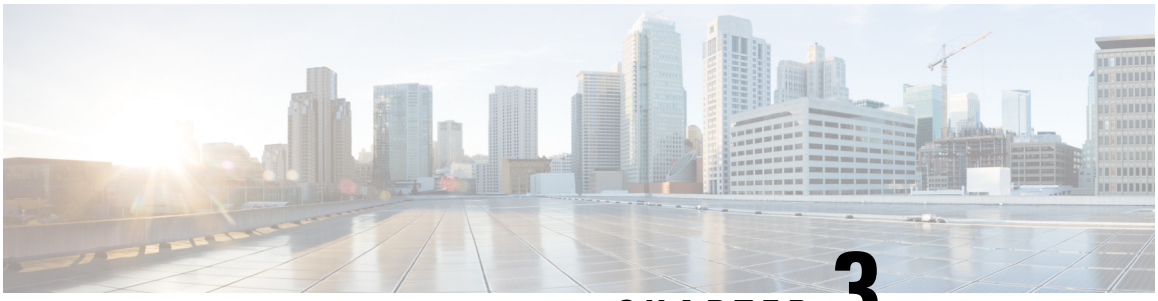
Sample Request

```
GET /esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044738.s
HTTP/1.1
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

The response contains the log file that was requested.

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: text/plain
Content-length: 7216
Connection: close
Content-Disposition:attachment; filename="audit_logs.@20200818T044738.s"
Wed Sep 30 00:38:01 2020 Info: Begin Logfile
Wed Sep 30 00:38:01 2020 Info: Version: 13.7.0-030 SN: 4229CAEC09527FD2570C-F028BAE54A11
Wed Sep 30 00:38:01 2020 Info: Time offset from UTC: 0 seconds
Wed Sep 30 00:38:09 2020 Info: Logfile rolled over
Wed Sep 30 00:38:09 2020 Info: End Logfile
```



CHAPTER 3

General Purpose APIs

General purpose configuration queries will have the **config** resource name as part of the query string. You can only retrieve configuration information (GET), and cannot perform any changes (POST, DELETE) in this release. You can specify the device type to indicate the device from which you need the configuration from the email gateway.

This chapter contains the following sections:

Querying for the System Time

Sample Request

```
GET /esa/api/v2.0/config/system_time?
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Apr 2018 18:06:32 GMT
Content-type: application/json
Content-Length: 121
Connection: close
{
    "data": {
        "continent": [
            "Asia",
            "India",
            "Kolkata"
        ],
        "time": "Thu Apr 12 23:38:05 2018 IST",
        "timezone": "Asia/Kolkata"
```

```
    }
}
```

Retrieving APIs Accessible to a User Role

You can retrieve a list of APIs that are available for a currently logged in user.

Synopsis	`GET /api/v2.0/login/privileges`
Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection

Sample Request

```
GET /esa/api/v2.0/login/privileges
HTTP/1.1
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46SXJvbnBvcnQxMjMk
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Apr 2018 14:17:44 GMT
Content-type: application/json
Content-Length: 4392
Connection: close
{
    "data": [
        "e_message_tracking_messages",
        "e_message_tracking_detail",
        "e_message_tracking_availability",
        "e_message_tracking_verdict",
        "e_message_tracking_dlp_details",
        "e_message_tracking_amp_details",
...
...
        "e_config_macro_file_types",
        "e_config_geo_countries",
        "e_config_tracking_query_timeout",
        "e_config_spam_quarantine_appearance_details",
        "esa_config_users",
        "e_config_euq_authentication_method",
        "e_config_euq_url_details"
    ]
}
```

Health API

You can retrieve information about system health using the health API.

Synopsis	`GET /api/v2.0/health/`
Request Headers	Host, Authorization
Response Headers	Content-Type, Content-Length, Connection

Sample Request

```
GET /esa/api/v2.0/health
HTTP/1.1
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 5782
Connection: close
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "percentage_ram_utilization": 1,
        "messages_in_pvo_quarantines": 0,
        "resource_conservation": 0,
        "messages_in_workqueue": 0,
        "percentage_swap_utilization": 0.0,
        "percentage_queue_utilization": 0.0,
        "percentage_diskio": 0,
        "percentage_cpu_load": 17
    }
}
```

Delivery Status API

You can retrieve information about the mail delivery status using the Delivery Status API.

Synopsis	`GET /api/v2.0/health/delivery_status`
Request Headers	Host, Authorization
Response Headers	Content-Type, Content-Length, Connection

Sample Request

```
GET /esa/api/v2.0/health/delivery_status
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46SXJvbnBvcnRAMzAu
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate, br
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 650
Connection: keep-alive
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "delivery_status",
        "resultSet": [
            {
                "soft_bounces": 0,
                "latest_host_status": "Unknown",
                "hard_bounces": 0,
                "active_recipients": 0,
                "destination_domain": "the.encryption.queue",
                "connections_out": 0,
                "delivered_recipients": 0
            },
            {
                "soft_bounces": 0,
                "latest_host_status": "Unknown",
                "hard_bounces": 0,
                "active_recipients": 0,
                "destination_domain": "the.euq.queue",
                "connections_out": 0,
                "delivered_recipients": 0
            },
            {
                "soft_bounces": 0,
                "latest_host_status": "Unknown",
                "hard_bounces": 0,
                "active_recipients": 0,
                "destination_domain": "the.euq.release.queue",
                "connections_out": 0,
                "delivered_recipients": 0
            }
        ]
    }
}
```

System Status API

You can retrieve information about the overall system status using the System Status API.

Synopsis	`GET /api/v2.0/health/system_status`

Request Headers	Host, Authorization
Response Headers	Content-Type, Content-Length, Connection

Sample Request

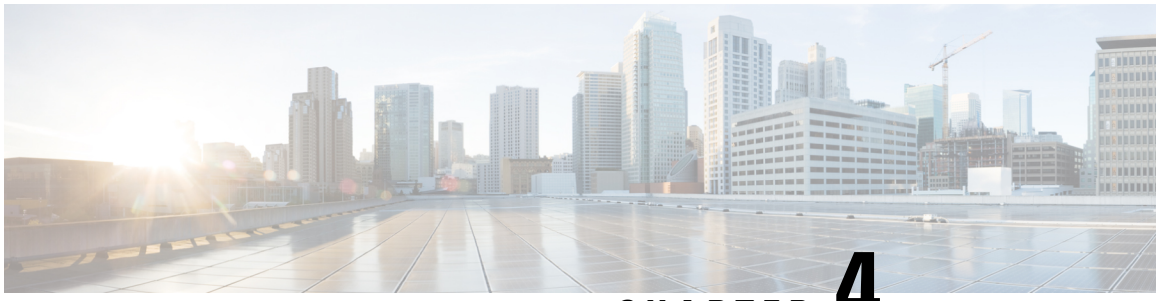
```
GET /esa/api/v2.0/health/system_status
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46SXJvbnBvcnRAMzAu
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate, br
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 4014
Connection: keep-alive
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "system_status",
        "resultSet": {
            "rates": [
                {
                    "total_completed_recipients_rate_five": 0,
                    "delivered_recipients_rate_one": 0,
                    "messages_received_rate_five": 0,
                    "hard_bounced_recipients_rate_one": 0,
                    "hard_bounced_recipients_rate_fifteen": 0,
                    "total_completed_recipients_rate_fifteen": 0,
                    "recipients_received_rate_one": 0,
                    "total_completed_recipients_rate_one": 0,
                    "soft_bounced_events_rate_one": 0,
                    "delivered_recipients_rate_fifteen": 0,
                    "recipients_received_rate_fifteen": 0,
                    "soft_bounced_events_rate_fifteen": 0,
                    "messages_received_rate_one": 0,
                    "soft_bounced_events_rate_five": 0,
                    "messages_received_rate_fifteen": 0,
                    "delivered_recipients_rate_five": 0,
                    "recipients_received_rate_five": 0,
                    "hard_bounced_recipients_rate_five": 0
                }
            ],
            "version_details": [
                {
                    "build_date": "2022-05-12",
                    "operating_system": "14.4.20-008",
                    "install_date": "2022-05-22 19:03:09",
                    "raid_status": "Unknown",
                    "serial_number": "422CBE9B59F1C1EA69CF-34D5DFAB3D39",
                    "model": "C300V"
                }
```

```
],
"gauges": [
    {
        "ram_utilization": "1%",
        "email_security_appliance": "0%",
        "msgs_in_work_queue": 0,
        "disk_io_utilization": "0%",
        "total_active_recipients": 0,
        "current_outgoing_connections": 0,
        "total_queue_utilized": "0.0%",
        "anti_virus": "0%",
        "msgs_in_quarantine": 0,
        "quarantine": "0%",
        "reporting": "0%",
        "space_used_by_quarantine": "0B",
        "unattempted": 0,
        "logging_disk_utilization": "2%",
        "attempted": 0,
        "anti_spam": "0%",
        "logging_disk_available": "356G",
        "current_incoming_connections": 1,
        "total_queue_space_used": "0B",
        "overall_cpu_load": "3%",
        "dest_objects_in_memory": 3
    }
],
"mail_system_status": [
    {
        "up_since": "16d 17h 19m 24s",
        "system_status": "Online",
        "oldest_message": "No Messages",
        "status_as_of": "Sun May 22 19:02:54 2022 GMT"
    }
],
"counters": [
    {
        "dns_reqs_reset": 933,
        "dns_hard_bounces_reset": 0,
        "total_hard_bounces_reset": 0,
        "dropped_messages_uptime": 0,
        "deleted_recipients_uptime": 0,
        "net_reqs_lifetime": 17,
        "dk_signed_lifetime": 0,
        "dropped_messages_reset": 0,
        "messages_received_uptime": 177,
        "expired_hard_bounces_uptime": 0,
        "rejected_recipients_reset": 0,
        "expired_hard_bounces_reset": 0,
        "rejected_recipients_uptime": 0,
        "expired_lifetime": 16,
        "global_unsub_hits_reset": 0,
        "recipients_received_uptime": 177,
        "five_xx_hard_bounces_uptime": 0,
        "cache_misses_reset": 17,
        "filter_hard_bounces_reset": 0,
        "five_xx_hard_bounces_lifetime": 0,
        "other_hard_bounces_reset": 0,
        "dns_hard_bounces_uptime": 0,
        "other_hard_bounces_lifetime": 0,
        "total_hard_bounces_uptime": 0,
        "cache_hits_reset": 933,
        "rejected_recipients_lifetime": 0,
        "dns_reqs_uptime": 933,
        "net_reqs_uptime": 17,
```

```
                        "deleted_recipients_lifetime": 0,
                        "delivered_recipients_uptime": 177,
                        "dns_reqs_lifetime": 933,
                        "exceptions_lifetime": 916,
                        "delivered_recipients_lifetime": 177,
                        "exceptions_reset": 916,
                        "delivered_recipients_reset": 177,
                        "total_completed_recipients_lifetime": 177,
                        "cache_misses_lifetime": 17,
                        "generated_bounce_recipients_uptime": 0,
                        "total_completed_recipients_uptime": 177,
                        "net_reqs_reset": 17,
                        "pending_requests": 0,
                        "global_unsub_hits_uptime": 0,
                        "cache_hits_uptime": 933,
                        "dk_signed_uptime": 0,
                        "other_hard_bounces_uptime": 0,
                        "last_counter_reset_str": "Never",
                        "generated_bounce_recipients_reset": 0,
                        "deleted_recipients_reset": 0,
                        "messages_received_lifetime": 177,
                        "soft_bounced_events_uptime": 0,
                        "recipients_received_reset": 177,
                        "filter_hard_bounces_uptime": 0,
                        "expired_hard_bounces_lifetime": 0,
                        "recipients_received_lifetime": 177,
                        "total_hard_bounces_lifetime": 0,
                        "dk_signed_reset": 0,
                        "filter_hard_bounces_lifetime": 0,
                        "soft_bounced_events_lifetime": 0,
                        "dropped_messages_lifetime": 0,
                        "outstanding_requests": 0,
                        "cache_hits_lifetime": 933,
                        "generated_bounce_recipients_lifetime": 0,
                        "cache_misses_uptime": 17,
                        "soft_bounced_events_reset": 0,
                        "global_unsub_hits_lifetime": 0,
                        "total_completed_recipients_reset": 177,
                        "messages_received_reset": 177,
                        "expired_uptime": 16,
                        "five_xx_hard_bounces_reset": 0,
                        "dns_hard_bounces_lifetime": 0,
                        "expired_reset": 16,
                        "exceptions_uptime": 916
                    }
                ]
            }
        }
}
```



CHAPTER 4

Troubleshooting AsyncOS API

This chapter contains the following sections:

API Logs

Subscribe to the API logs using **System Administration** > **Log Subscriptions**. For instructions, see the email gateway or Online Help.

The following are some of the events that are logged in the API logs:

- API has started or stopped
- Connection to the API failed or closed (after providing response)
- Authentication succeeded or failed
- Request contains errors
- Error while communicating network configuration changes with AsyncOS API

Alerts

Ensure that the email gateway is configured to send you alerts related to AsyncOS API. You will receive alerts when:

Alert Description	Type	Severity
API has restarted due to an error	System	Warning

Handling Error Messages of Configuration APIs

This section lists the following error messages that you might receive when generating the following Configuration APIs ('Authentication,' 'URL lists,' 'Dictionary,' and 'HAT'):

- Error - Unauthorised API calls

- Error - Invalid credentials while generating token
- Error - Token not authenticating API calls
- Error - API calls give an expired token
- Error - API Calls give unsupported operation for mode

Error - Unauthorised API Calls

Following is the error message you may receive for an unauthorized API call:

```
{
      "error": {
      "message": "Unauthorized.",
      "code": "401",
     "explanation": "401 = No permission -- see authorization schemes."
     }
     }
```

Solution: See the Authentication APIs, on page 100section for information about Authentication APIs.

Error - Invalid credentials while Generating Token

Following is the error message you may get when invalid credentials are received when generating the token:

```
{
 "error": {
  "message": "Invalid credentials.",
  "code": "400",
  "explanation": "400 = Bad request syntax or unsupported method."
 }
}
```

Solution: The client credentials might be incorrect. See the Client Credentials APIs, on page 100 for information on how to retrieve the client credentials correctly.

Error - Token not authenticating API Calls

Following is the error message you may receive when the token does not authenticate the API calls:

```
{
 "error": {
  "message": "InvalidTokenError.",
  "code": "401",
  "explanation": "401 = No permission -- see authorization schemes."
 }
}
```

Solution: The token might be incorrect. See the Generating JWT Token , on page 104 section for information on how to generate the token correctly.

Error - API Calls give Expired Token

Following is the error message you may receive when the API calls give an expired token:

```
{
 "error": {
  "message": "ExpiredSignatureError.",
  "code": "401",
  "explanation": "401 = No permission -- see authorization schemes."
 }
}
```

Solution: The token might have expired. You can regenerate a token using the Token API call. For more information, see Generating JWT Token , on page 104.

Error - API Calls give unsupported operation for mode

Following is the error message you may receive when the API calls give unsupported operation for mode:

```
{
    "error": {
        "message": "Unsupported operation for machine mode. Override settings from the UI
for sender_groups to configure through APIs.",
        "code": "404",
        "explanation": "404 = Nothing matches the given URI."
    }

}
```

Solution: You must override settings for the particular feature from the UI. In this example, you must override settings for sender groups from the UI to machine mode, after which API calls for sender groups for machine mode will return a successful response.