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 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 38
- APIs for Other Quarantine, on page 65

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 38
- Retrieving Message Details, on page 41
- Releasing Messages, on page 44
- Deleting Messages, on page 43
- Searching for Safelist and Blocklist Entries, on page 45
- Adding, Editing, and Appending Safelist and Blocklist Entries, on page 48
- Deleting Safelist or Blocklist Entries, on page 61

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 62

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
```

```
    }
}
```

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 90
- Retrieving All Log Files for Specific Log Subscription, on page 91
- Retrieving Log Files using URL, on page 93

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 90 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 91 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 91 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 91 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
```