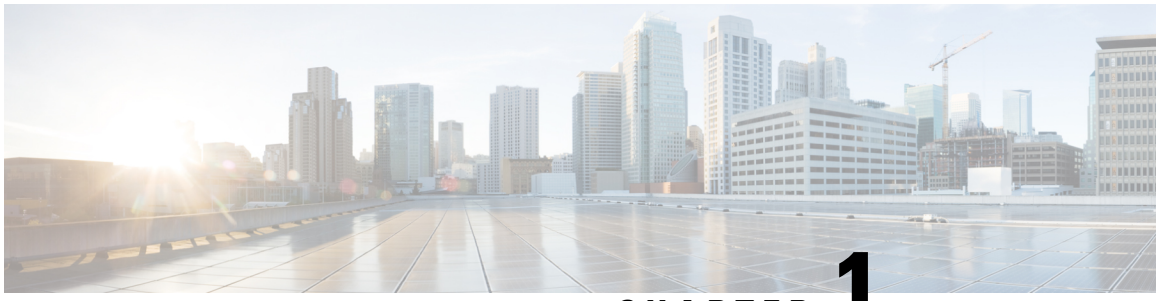
AsyncOS API 13.8.0 for Cisco Security Management Appliances - Getting Started Guide - LD (Limited Deployment)

First Published: 2020-01-06

Last Modified: 2020-10-05

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

CONTENTS



CHAPTER 1

Overview of AsyncOS API for Cisco Security Management Appliances

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

This chapter contains the following sections:

Prerequisites for Using AsyncOS API

To use AsyncOS API, you need:

- A Security Management appliance with AsyncOS 12.0.
- Knowledge of:
  - HTTP, which is the protocol used for API transactions. Secure communication over TLS.
  - JavaScript Object Notation (JSON), which the API uses to construct resource representations.
  - JSON Web Token (JWT)
- A client or programming library that initiates requests and receives responses from the AsyncOS API using HTTP or HTTPS, for example, cURL. The client or programming library must support JSON to interpret the response from the API.
- Authorization to access the AsyncOS API. See Authorization, on page 4.

- AsyncOS API enabled using web interface or CLI. See Enabling AsyncOS API, on page 2.

Enabling AsyncOS API

Before You Begin

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

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

Step 1 Log in to the web interface.

Step 2 [New web interface only] Click the gear icon to load the legacy web interface.

Step 3 Choose **Management Appliance Network** > **IP Interfaces**.

Step 4 Edit the Management interface.

Note You can enable AsyncOS API on any IP interface. However, Cisco recommends that you enable AsyncOS API on the Management interface.

Step 5 Under the AsyncOS API (Monitoring) section, depending on your requirements, select HTTP, HTTPS, or both and the ports to use.

Note AsyncOS API communicates using HTTP / 1.1.

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

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

Step 6 Submit and commit your changes.

Securely Communicating with AsyncOS API

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

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

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

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

Step 3 Submit and commit your changes.

AsyncOS API Authentication and Authorization

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

- Authentication, on page 3
- Authorization, on page 4
- Retrieving APIs Accessible to a User Role, on page 138

Authentication

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

Authenticating API Queries with JSON Web Token

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

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

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

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

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

Sample Request

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

Sample Response

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

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

Authorization

The AsyncOS API is a role based system, the scope of API queries is defined by the role of the user. Cisco Content Security Management appliance users with the following roles can access the AsyncOS API:

- Administrator
- Operator
- Technician
- Read-Only Operator

- Guest
- Web Administrator
- Web Policy Administrator
- URL Filtering Administrator
- Email Administrator
- Help Desk User

Note

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

AsyncOS API Requests and Responses

Note For complete list of APIs, see *AsyncOS API - Addendum to the Getting Started Guide for Cisco Content Security Management Appliances*.

AsyncOS API Requests

Requests made to the API have the following characteristics:

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

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

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

  where:

  - `{appliance}:{port}`

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

    is the resource you are attempting to access, for example, reports, tracking, quarantine, configuration, or other counters.
  - `{resource_attributes}`

    are the supported attributes for a resource, for example, duration, and so on.
- Each request must contain user credentials, or a valid authorization header.
- Each request must be set to accept:

  ```
  application/json
  ```

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

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

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

AsyncOS API Responses

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

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

Key Components of Responses

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

Components	Values	Description

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

HTTP Response Codes

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

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

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

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

- RFC1945
- RFC7231

Comparing API Data with the Web Interface Data

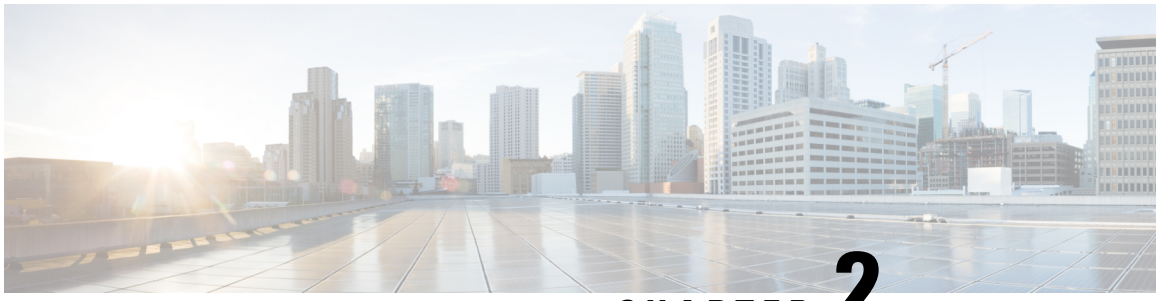
The new web interface uses the AsyncOS APIs to fetch data with the duration attribute specified in the GMT time zone. If you plan to compare the data from your API query with the new web interface data, ensure that your API query has the same time range (in ISO8601 time format) as the new web interface API query.

Related Documentation

In addition to the topics covered in this document, you can find more information about the APIs in the following documents:

Table 1: Related Documentation

Document	Located At:
Addendum to the Getting Started Guide for Cisco Security Management Appliances.	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-programming-reference-guides-list.html
API Help (Swagger UI)	On the new web interface, hover over the help icon, and click **API Help: Swagger**. **Note** The API Help (Swagger UI) also allows you to test the API calls directly from your web browser using the **Try it out** button.



CHAPTER 2

APIs for Email

Monitoring APIs

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, on page 12
- Retrieving Multiple Values for a Counter, on page 12
- Retrieving Single Values for Each Counter in a Counter Group, on page 13
- Retrieving Multiple Values for Multiple Counters, on page 14
- Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter, on page 16

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},
{"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},
                    ]
                }
            }
        }
    }
```

Schedule and Archive APIs

Schedule APIs

Synopsis	`GET /sma/api/v2.0/config/periodic_reports?resource_attribute`
	
	`POST sma/api/v2.0/config/periodic_reports?resource_attribute`
	
	`PUT /sma/api/v2.0/config/periodic_reports/periodic_report_id?resource_attribute`
	
	`DELETE /sma/api/v2.0/config/periodic_reports?resource_attribute`

Supported Resource Attributes	Sorting	You should use both these parameters. If you use either, you will not receive data in the response. • `orderBy=<value>` The valid options are: • `periodic_report_display_name` Order the results based on the display name of the report. • `periodic_report_title` Order the results based on the type of the report. • `periodic_report_type` Order the results based on the type of the report. • `periodic_report_time_range` Order the results based on the time range of the report. • `periodic_report_delivery` Order the results based on the delivery options of the report. • `periodic_report_format` Order the results based on the format of the report. • `periodic_report_schedule_type` Order the results based on the type of the schedule selected for the report. • `periodic_report_tier` Order the results based on the required email gateway. • `periodic_report_next_run_date` Order the results based on the scheduling options of the report. • `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.
	Device	• `device_type=sma` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Examples

The following are some examples for the types of schedule reports queries:

- Retrieving Scheduling Reports, on page 20
- Retrieving the Details of a Schedule Report Entry, on page 21
- Adding a Scheduled Report Entry, on page 23
- Editing a Scheduled Report Entry, on page 24
- Deleting Scheduled Reports, on page 25

Retrieving Scheduling Reports

The following example shows how to retrieve a list of top 25 scheduled report entries sorted based on the a selected scheduling option in descending order.

Sample Request

```
GET /sma/api/v2.0/config/periodic_reports?device_type=sma&
limit=25&offset=0&orderBy=periodic_report_next_run_date&orderDir=desc
HTTP/1.1
cache-control: no-cache
Postman-Token: 0f917f72-82a4-4b6d-93a9-a1fbd3e72b1b
Authorization: Basic YWRtaW46Q2lzY29AMTIzNA==
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: 10.8.159.22:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 12:14:13 GMT
```

```
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 1797
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

{
"data":
{
"periodic_reports": [{"20191120061727_Content Filters_calendar_week": {"periodic_report_type":
 "phoebe",
 "periodic_report_schedule": {"periodic_report_second": 0, "periodic_report_day": "",
"periodic_report_month": "", "periodic_report_minute": 0, "periodic_report_weekday": "",
"periodic_report_year": "", "periodic_report_hour": 0, "periodic_report_schedule_type":
"Daily"},
"periodic_report_options": {"periodic_report_format": "PDF", "periodic_report_time_range":

"Previous 7 calendar days", "periodic_report_lang": "en-us"}, "periodic_report_user_name":
 "admin",
"periodic_report_product_type": "ESA", "periodic_report_type_name": "Content Filters",
"periodic_report_delivery": "Archived Only", "periodic_report_recipients": [],
"periodic_report_tier":
"All Email Appliances", "periodic_report_next_run_date": "21 Nov 2019 00:00 (GMT)",
"periodic_report_title":
"Content Filters"}}, {"20191120060917_Content Filters_calendar_month":
{"periodic_report_type": "phoebe",
"periodic_report_schedule": {"periodic_report_second": 0, "periodic_report_day": "",
"periodic_report_month": "", "periodic_report_minute": 0, "periodic_report_weekday": "",
"periodic_report_year": "", "periodic_report_hour": 0, "periodic_report_schedule_type":
"Daily"},
"periodic_report_options": {"periodic_report_format": "PDF", "periodic_report_time_range":

"Previous 12 calendar months", "periodic_report_lang": "en-us"}, "periodic_report_user_name":
 "admin",
"periodic_report_product_type": "ESA", "periodic_report_type_name": "Content Filters",
"periodic_report_delivery": "Archived Only", "periodic_report_recipients": [],
"periodic_report_tier":
 "All Email Appliances", "periodic_report_next_run_date": "21 Nov 2019 00:00 (GMT)",
"periodic_report_title": "Content Filters"}}], "meta": {"totalCount": 2}
}
}
```

Retrieving the Details of a Schedule Report Entry

The following example shows how to retrieve a list of top 25 archived reports filtered based on the report title and sorted based on the time range of the report generation in descending order.

Sample Request

```
GET /sma/api/v2.0/config/archived_reports?device_type=sma&filterByTitle
=Content+Filters&limit=25&offset=0&orderBy=periodic_report_generated&orderDir=desc
HTTP/1.1
cache-control: no-cache
Postman-Token: 379beccc-d9de-4cd0-a730-69e59385bf90
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
```

```
Host: sma.cisco:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:00:17 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 441
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
{
"data": {
"meta": {
"totalCount": 1
},
"archived_reports": [{"20191120134501_Content Filters_calendar_month.pdf":
{"periodic_report_format":
"PDF", "periodic_report_type_name": "Content Filters", "periodic_report_generated":
"20 Nov 2019 13:45 (GMT)", "periodic_report_time_range": "Previous calendar month",
"periodic_report_tier": "All Email Appliances", "periodic_report_title": "Content Filters",

"periodic_report_product_type": "esa"}}]
}
}
```

Viewing the Details of a Schedule Report Entry

The following example shows how to retrieve a preview PDF document for the scheduled report entry for a particular report type and time range of the report.

Sample Request

```
GET /sma/api/v2.0/config/archived_reports/preview?device_type=
sma&periodic_report_type_name=Outgoing%20Destinations&periodic_report_type=
phoebe&periodic_report_start_date=2017-03-01T15:00:00.000Z&periodic_report_
end_date=2019-07-30T15:00:00.000Z&periodic_report_format=pdf&periodic_report_lang=
en-us&periodic_report_time_range=Custom%20range&periodic_report_rows=
10&periodic_report_sort_columns=%7B%22table%22:%20%22Outgoing%20Destinations
%20Detail%22,%22column%22:%20%22Total%20Processed%22%7D
HTTP/1.1
cache-control: no-cache
Postman-Token: fc05953b-1552-47ab-be49-4cb2be5fc7c0
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: m680q08.ibqa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 Nov 2019 17:38:08 GMT
```

```
Content-type: application/pdf
Content-Disposition: filename="20191121173808_Outgoing Destinations.pdf"
Content-Length: 111240
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

%PDF-1.4
.....
.....
%%EOF
```

Adding a Scheduled Report Entry

The following example shows how to add a scheduled report with report type, report title, device type and other options.

Sample Request

```
POST /sma/api/v2.0/config/periodic_reports?device_type=sma
HTTP/1.1
cache-control: no-cache
Postman-Token: 9bc82e3c-b163-4558-923a-f5c03d40a332
Authorization: Basic YWRtaW46Q2lzY29AMTIzNA==
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: 10.8.159.22:6080
accept-encoding: gzip, deflate
content-length: 509
Connection: keep-alive
{
"data":
{
"periodic_reports":[{"periodic_report_title":"Content
Filters","periodic_report_type":"phoebe",
"periodic_report_type_name":"Content
Filters","periodic_report_options":{"periodic_report_format":
"pdf","periodic_report_lang":"en-us","periodic_report_time_range":"Previous 7 calendar
days"},
"periodic_report_schedule":{"periodic_report_schedule_type":"daily","periodic_report_minute":0,
"periodic_report_hour":0},"periodic_report_tier":"All Email
Appliances","periodic_report_delivery":
"Archived Only"}]
}
}
```

Sample Response

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Wed, 20 Nov 2019 13:17:31 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 49
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

{
"data": "Scheduled Report created Successfully"
}
```

Editing a Scheduled Report Entry

The following example shows how to modify a scheduled report with a schedule report ID.

Sample Request

```
PUT /sma/api/v2.0/config/periodic_reports/20191120133634_
Content%20Filters_calendar_week?device_type=sma
HTTP/1.1
cache-control: no-cache
Postman-Token: 7adc6d87-64bd-40d5-827a-3e5d2ea8406b
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 510
Connection: keep-alive

{
"data":
{
"periodic_reports":[{"periodic_report_title":"Content Filters","periodic_report_type":
"phoebe","periodic_report_type_name":"Content Filters","periodic_report_options":
{"periodic_report_format":"pdf","periodic_report_lang":"en-us","periodic_report_time_range":
"Previous calendar
month"},"periodic_report_schedule":{"periodic_report_schedule_type":"daily",
"periodic_report_minute":45,"periodic_report_hour":13},"periodic_report_tier":
"All Email Appliances","periodic_report_delivery":"Archived Only"}]
}
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 13:44:35 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 49
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

{
"data": "Scheduled Report Updated Successfully"
}
```

Deleting Scheduled Reports

The following example shows how to delete a scheduled report with device type and a schedule report ID.

Sample Request

```
DELETE /sma/api/v2.0/config/periodic_reports?device_type=sma&
id=20191120135041_Advanced+Malware+Protection+File+Analysis_calendar_week
HTTP/1.1
cache-control: no-cache
Postman-Token: 74cf4ad5-ff0f-4173-894e-a0c2a9c3d6d5
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 0
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 13:54:49 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 52
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
{
"data":
{
"message": "1 item deleted successfully"
}
}
```

Archive APIs

Synopsis	`GET /sma/api/v2.0/config/archived_reports?resource_attribute`
	
	`GET sma/api/v2.0/config/archived_reports/archived_report_id?resource_attribute`
	
	`POST /sma/api/v2.0/config/archived_reports?resource_attribute`
	
	`DELETE /sma/api/v2.0/config/archived_reports?resource_attribute`

Supported Resource Attributes	Sorting	You should use both these parameters. If you use either, you will not receive data in the response. • `orderBy=<value>` The valid options are: • `periodic_report_generated` Order the results based on the date and time the report is generated. • `periodic_report_display_name` Order the results based on the display name of the report. • `periodic_report_format` Order the results based on the format of the report. • `periodic_report_title` Order the results based on the type of the report. • `periodic_report_time_range` Order the results based on the time range of the report. • `periodic_report_type` Order the results based on the type of the report. • `periodic_report_tier` Order the results based on the required email gateway. • `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.

	Filtering	Filter parameters restrict the data to be included the response. • `filterByTitle=<value>` Filter the data to be retrieved according to the title of the report and value. • `filterByReportTypeName=<value>` Filter the data to be retrieved according to the type of the report and value. • `filterByTimeRange=<value>` Filter the data to be retrieved according to the time range of the report and value.
	Device	• `device_type=sma` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Examples

The following are some examples for the types of archived reports queries:

- Searching Archived Reports, on page 27
- Retrieving Archived Reports, on page 28
- Retrieving the Details of a Archive Report Entry, on page 29
- Adding an Archive Report Entry, on page 30
- Deleting an Archived Report Entry, on page 31

Searching Archived Reports

The following example shows how to search for a list of top 25 archived reports based on the report title and sorted by the date and time the report is generated, in descending order.

Sample Request

```
GET /sma/api/v2.0/config/archived_reports?device_type=
sma&filterByTitle=content&limit=25&offset=0&orderBy=periodic_
report_generated&orderDir=desc
HTTP/1.1
cache-control: no-cache
Postman-Token: fc26a46d-52f0-410c-ba9a-5a896a8aa691
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
```

```
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:20:37 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 441
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
{
"data":
{
"meta":
{
"totalCount": 1
},
"archived_reports": [{"20191120134501_Content Filters_calendar_month.pdf":
{"periodic_report_format": "PDF", "periodic_report_type_name": "Content Filters",
"periodic_report_generated": "20 Nov 2019 13:45 (GMT)", "periodic_report_time_range":
"Previous calendar month", "periodic_report_tier": "All Email Appliances",
"periodic_report_title": "Content Filters", "periodic_report_product_type": "esa"}}]
}
}
```

Retrieving Archived Reports

The following example shows how to retrieve a list of top 25 archived reports sorted by the time range of the report in descending order.

Sample Request

```
GET /sma/api/v2.0/config/archived_reports?device_type=sma&limit=25
&offset=0&orderBy=periodic_report_generated&orderDir=desc
HTTP/1.1
cache-control: no-cache
Postman-Token: 2adbdec2-ef46-4c7e-abf2-9f06cd52a0d7
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:04:02 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 441
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
{
"data": {
"meta": {
"totalCount": 1
},
"archived_reports": [{"20191120134501_Content Filters_calendar_month.pdf":
{"periodic_report_format":
"PDF", "periodic_report_type_name": "Content Filters", "periodic_report_generated":
"20 Nov 2019 13:45 (GMT)", "periodic_report_time_range": "Previous calendar month",
"periodic_report_tier":
 "All Email Appliances", "periodic_report_title": "Content Filters",
"periodic_report_product_type": "esa"}}]
}
}
```

Retrieving the Details of a Archive Report Entry

The following example shows how to retrieve an archived report entry with device type and an archived report ID.

Sample Request

```
GET /sma/api/v2.0/config/archived_reports/view/20191120134501_Content
%20Filters_calendar_month.pdf?device_type=sma
HTTP/1.1
cache-control: no-cache
Postman-Token: 86b684cc-7721-4fa9-8012-2077d45582a5
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:06:40 GMT
Content-type: application/pdf
Content-Disposition: filename="20191120134501_Content Filters_calendar_month.pdf"
Content-Length: 111141
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

%PDF-1.4
.......
.......
%%EOF
```

Viewing the Details of a Archived Report Entry

The following example shows how to retrieve a preview PDF document for an archived report entry for a particular report type and time range of the report.

Sample Request

```
GET /sma/api/v2.0/config/archived_reports/preview?device_type=sma
&periodic_report_type_name=Outgoing%20Destinations&periodic_report_type=phoebe
&periodic_report_start_date=2017-03-01T15:00:00.000Z&periodic_report_end_date=
2019-07-30T15:00:00.000Z&periodic_report_format=pdf&periodic_report_lang=en-us
&periodic_report_time_range=Custom%20range&periodic_report_rows=10
&periodic_report_sort_columns=%7B%22table%22:%20%22Outgoing%20Destinations
%20Detail%22,%22column%22:%20%22Total%20Processed%22%7D
HTTP/1.1
cache-control: no-cache
Postman-Token: fc05953b-1552-47ab-be49-4cb2be5fc7c0
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: m680q08.ibqa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 Nov 2019 17:38:08 GMT
Content-type: application/pdf
Content-Disposition: filename="20191121173808_Outgoing Destinations.pdf"
Content-Length: 111240
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

%PDF-1.4
.....
.....
%%EOF
```

Adding an Archive Report Entry

The following example shows how to add an archived report with report title, report type, device type and other options.

Sample Request

```
POST /sma/api/v2.0/config/archived_reports?device_type=sma
HTTP/1.1
cache-control: no-cache
Postman-Token: 83c60ea4-e187-41bd-9e13-cacbdf43967a
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 545
Connection: keep-alive
{
```

```
"data":
{
"archived_reports":[{"periodic_report_title":"Connections by Country","periodic_report_type":
"phoebe","periodic_report_type_name":"Connections by Country","periodic_report_options":
{"periodic_report_format":"pdf","periodic_report_lang":"en-us","periodic_report_time_range":
"Previous 7 calendar days","periodic_report_rows":10,"periodic_report_sort_columns":[{"table":
"Total Incoming Mail Connections by Country","column":"Total Connections"}]},
"periodic_report_tier":"All Email Appliances","periodic_report_delivery":"Archived Only"}]
}
}
```


Sample Response

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Wed, 20 Nov 2019 14:11:44 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 46
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
{
"data":
{
"message": "Archived successfully"
}
}
```

Deleting an Archived Report Entry

The following example shows how to delete an archived report with device type and an archived report ID.

Sample Request

```
DELETE /sma/api/v2.0/config/archived_reports?device_type=sma&
id=20191120141701_Connections+by+Country_calendar_week.pdf
HTTP/1.1
cache-control: no-cache
Postman-Token: affe27d3-d8bc-4986-a826-e9a6f449ac80
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 0
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:17:40 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 52
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
{
"data":
{
"message": "1 item deleted successfully"
}
}
```

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, on page 32
- Rejected Connections, on page 37
- Message Details, on page 38
- DLP Details, on page 40
- AMP Details, on page 42
- URL Details, on page 44
- Connection Details, on page 46

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 API - Addendum to the Getting Started Guide for Cisco Content Security Management 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, appliance (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 API - Addendum to the Getting Started Guide for Cisco Content Security Management Appliances 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 appliance' 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 appliance.
	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 appliance.
	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 appliance.
	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 appliance.
	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"
}
```


Quarantine APIs

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 48
- APIs for Other Quarantine, on page 75

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 48
- Retrieving Message Details, on page 51
- Releasing Messages, on page 54
- Deleting Messages, on page 53
- Searching for Safelist and Blocklist Entries, on page 55
- Adding, Editing, and Appending Safelist and Blocklist Entries, on page 58
- Deleting Safelist or Blocklist Entries, on page 71

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

Sample Request

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

Sample Request

```
GET /sma/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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 72

Deleting Recipient Safelist Entries

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

Sample Request

```
DELETE /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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
/sma/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: sma.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 /sma/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: sma.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://bit.ly/2zs6KAq<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 /sma/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: sma.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 /sma/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: sma.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	<pre>{
	"action":"sendCopy",
	"mids": [value],
	"quarantineName": "value",
	"quarantineType": "pvo",
	"recipients":["value"]
	}</pre>
	For outbreak, you can add this optional attribute to the message body:
	<pre>"sendToCisco":<value></pre>
	The valid value is *true*. An example is shown below:
	<pre>{
	"action":"sendCopy",
	"mids": [value],
	"quarantineName": "value",
	"quarantineType": "pvo",
	"recipients":["value"],
	}</pre>

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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.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 /sma/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: sma.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 65
Connection: keep-alive


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

Sample Response

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

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

```
    }
}
```

Configuration APIs

This section contains the following topics:

- Querying for the Service Status
- Querying for File Analysis
- Querying for Reporting Groups
- Querying for Safelist Blocklist
- Querying Spam Settings

Querying for the Service Status

This section contains the following topics:

- Retrieving the Service Status
- Enabling Reporting Status
- Enabling Message Tracking Status
- Updating Spam Quarantine Status
- Enable Safelist or Blocklist Settings
- License Agreement

Retrieving the Service Status

Retrieve the service status of the features.

Synopsis	`GET /sma/api/v2.0/config/centralizedServices/serviceStatus`

This example shows a query to retrieve the service status of a feature.

Sample Request

```
GET /sma/api/v2.0/config/centralizedServices/serviceStatus?device_type=sma& HTTP/1.1
cache-control: no-cache
Postman-Token: 119ae2b6-5f11-4108-a1d9-849672dc66cc
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 13:14:57 GMT
```

```
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 251
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

{"data": {"serviceStatus": {"pvoQuarantine": {"status": "disabled"}, "centralizedReporting":
 {"status": "disabled"}, "safelistBlocklist": {"status": "disabled"}, "centralizedTracking":
 {"status": "disabled"}, "spamQuarantine": {"status": "enabled"}}}}
```

Enabling Reporting Status

Enabling the reporting status for Service Status.

Synopsis	`PUT` `/sma/api/v2.0/config/centralizedServices/serviceStatus/centralizedReporting`

```
{"data":{"serviceStatus":{"centralizedReporting":{"status":"enabled"}}}}
```

This example shows a query to enable the reporting status of a feature.

Sample Request

```
PUT
/sma/api/v2.0/config/centralizedServices/serviceStatus/centralizedReporting?device_type=sma&
 HTTP/1.1
cache-control: no-cache
Postman-Token: 66443747-6962-484e-a5ff-2339bc9c8018
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 72
Connection: keep-alive

{"data":{"serviceStatus":{"centralizedReporting":{"status":"enabled"}}}}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 13:27:21 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
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
```

```
{"data": {"message": "Updated successfully"}}
```

Enabling Message Tracking Status

Synopsis	PUT /sma/api/v2.0/config/centralizedServices/serviceStatus/centralizedTracking

```
{"data":{"serviceStatus":{"centralizedTracking":{"status":"enabled"}}}}
```

This example shows a query to enable the message tracking status of a feature.

Sample Request

```
PUT
/sma/api/v2.0/config/centralizedServices/serviceStatus/centralizedTracking?device_type=sma&
 HTTP/1.1
cache-control: no-cache
Postman-Token: e82ac2ce-cffe-4820-a144-205f59ca6cd6
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 71
Connection: keep-alive

{"data":{"serviceStatus":{"centralizedTracking":{"status":"enabled"}}}}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 13:36:42 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
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

{"data": {"message": "Updated successfully"}}
```

Updating Spam Quarantine Status

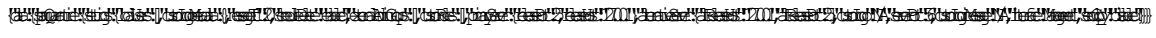
Update Spam Quarantine status with the Schedule Delete after 20 days.

Synopsis	PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings

This example shows a query to update spam quarantine status.

Sample Request

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: a4e76628-cece-4c7b-822a-94fffb6cfe84
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 408
Connection: keep-alive
```



Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 14:07:53 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 56
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

{"data": {"message": "Updated spam quarantine setings"}}
```

Enable Safelist or Blocklist Settings

Enable Safelist or Blocklist settings with the maximum list items per user as 160 and update the frequency for every 3 hours.

Synopsis	PUT /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings {"data":{"safelistBlocklist":{"settings":{"maxUserEntries":160,"updatePeriod":10800}}}}

This example shows a query to enable the safelist or the blocklist settings.

Sample Request

```
PUT /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: 97173889-0246-4c56-bac0-baac336eec26
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 87
```

```
Connection: keep-alive
{"data":{"safelistBlocklist":{"settings":{"maxUserEntries":160,"updatePeriod":10800}}}}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 15:03:29 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
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

{"data": {"message": "Updated successfully"}}
```

License Agreement

This section describes the license agreement for the service status.

Synopsis	`PUT https://10.76.157.163:462/sma/api/v2.0/config/centralizedServices/licenseAgreement?device_type=sma`
Request Body	`{"data": {"licenseAgreement": {"centralizedReporting": "yes", "centralizedTracking": "yes", "spamQuarantine": "yes"}}}`
Response	`{"data": {"message": "Updated successfully"}}`

Synopsis	`PUT https://10.76.157.163:462/sma/api/v2.0/config/centralizedServices/licenseAgreement/centralizedReporting?device_type=sma`
Request Body	`{"data": {"licenseAgreement": {"centralizedReporting": "yes",}}`

Synopsis	`GET https://10.76.157.163:462/sma/api/v2.0/config/centralizedServices/licenseAgreement?device_type=sma`
Request Body	`{"data": {"licenseAgreement": {"centralizedReporting": "yes", "centralizedTracking": "yes", "spamQuarantine": "yes"}}}`

Querying for File Analysis

This section contains the following topics:

Adding a Group (a@cisco.com)

Adding a group (a@cisco.com) to the File Analysis Client ID 06_VLNSMA12345678_422985E30D3CE2CC17BA-1A7EC30F6E9B_M100V_000000

Synopsis	`POST /sma/api/v2.0/config/centralizedServices/fileAnalysis/groupInfo?device_type=sma& HTTP/1.1`

This example shows a query to add a group to the file analysis client ID.

Sample Request

```
POST /sma/api/v2.0/config/centralizedServices/fileAnalysis/groupInfo?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: eabb3018-d0c5-4372-a850-09deb8c89472
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 210
Connection: keep-alive

{"data":{"fileAnalysis":{"groupInfo":[{"server":"https://panacea.threatgrid.com","region":"AMERICAS","groupName":"a@cisco.com","devices":["06_VLNSMA12345678_422985E30D3CE2CC17BA-1A7EC30F6E9B_M100V_000000"]}]}}}
```

Sample Response

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Wed, 27 May 2020 13:24:00 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 32
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

{"data": {"message": "Success"}}
```

Viewing Appliance Grouping for File Analysis Reporting

View Appliance Grouping for File Analysis Reporting.

Synopsis	`GET /sma/api/v2.0/config/centralizedServices/fileAnalysis?device_type`

This example shows a query to view the appliance grouping for file analysis reporting.

Sample Request

```
GET /sma/api/v2.0/config/centralizedServices/fileAnalysis?device_type=sma& HTTP/1.1
cache-control: no-cache
Postman-Token: fdf34da1-3727-42b4-8d62-4cab2ce4a54d
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 27 May 2020 13:33:39 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 306
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

{"data": {"fileAnalysis": {"groupInfo": [{"groupName": "a@cisco.com", "region": "AMERICAS",
 "devices": ["06_VLNSMA12345678_422985E30D3CE2CC17BA-1A7EC30F6E9B_M100V_000000"], "server":
 "https://panacea.threatgrid.com"}], "fileAnalysisId":
"06_VLNSMA12345678_422985E30D3CE2CC17BA-1A7EC30F6E9B_M100V_000000"}}}
```

Querying for Reporting Groups

This section contains the following topics:

Enable Reporting Setting

Enable Reporting setting by adding one or more groups.

Synopsis	POST /sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups

{"data": {"centralizedReporting": {"reportingGroups": [{"Group1": {"appliances": ["420E523A557DB950A34A-0587322DD26C"]}},{"Group2": {"appliances": ["420E523A557DB950A34A-0587322DD26C"]}}]}}}

This example shows a query to enable reporting setting for a feature.

Sample Request

```
POST
/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups?device_type=sma&
 HTTP/1.1
cache-control: no-cache
Postman-Token: 4d0f276b-c246-4f45-bf20-ed7f36b4a14b
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 79
Connection: keep-alive

{"data":{"centralizedReporting":{"reportingGroups":[{"Group 1":{"appliances":[]}}]}}}
```

Sample Response

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Thu, 21 May 2020 16:12:16 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 61
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

{"data": {"message": "Added centralized reporting groups"}}
```

Retrieving the Reporting Groups and Appliances

Retrieve the reporting groups and appliances.

Synopsis	POST /sma/api/v2.0/config/centralizedServices/fileAnalysis/groupInfo?device_type=sma& HTTP/1.1

{"data": {"centralizedReporting": {"reportingGroups": [{
"test 1": {"appliances": ["4229A2096D9E0C1C3A78-A82D93282C7A"
]}},{"test-2": {"appliances": ["4229CAEC09527FD2570C-F028BAE54A11"]}}]}}}

This example shows a query to retrieve the reporting groups and appliances.

Sample Request

```
GET
/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups?device_type=sma&
 HTTP/1.1
cache-control: no-cache
Postman-Token: a1c76d19-24bc-4cfa-b598-da1fcc5b0afc
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 28 May 2020 11:50:00 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 191
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

{"data": {"centralizedReporting": {"reportingGroups": [{"test 1": {"appliances":
["4229A2096D9E0C1C3A78-A82D93282C7A"]}}, {"test-2": {"appliances":
["4229CAEC09527FD2570C-F028BAE54A11"]}}]}}}
```

Reporting Groups and Appliances

By default, offset =0; limit = 25; orderDir=asc; orderBy=group.

Synopsis	GET/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups?device_type=sma

```
{ "data": { "centralizedReporting": { "reportingGroups": [ { "amy": { "appliances": [
"420E6D0465DF4F1107A8-EA6829376651" ] } }, { "beth": { "appliances": [
"420E6D0465DF4F1107A8-EA6829376651" ] } }, }
```

Delete Reporting Groups

To delete one valid reporting group:

Synopsis	https://u32c01p14-vrouter.cisco.com:4599/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups?group=divs30K

Sample Response

```
{
    "data": {
        "message": "Deleted Centralized Reporting groups"
    }
}
```

To delete multiple valid reporting groups:

Synopsis	https://u32c01p14-vrouter.cisco.com:4599/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups?group=divs40K&group=divs50K&group=divs7K

Sample Response

```
{
    "data": {
        "message": "Deleted Centralized Reporting groups"
    }
}
```

Combined All Actions

POST Combined ALL Actions: Add / Edit / Delete groups

Synopsis	POST /sma/api/v2.0/config/centralizedServices/centralizedReporting/allGroups

This example shows a query to combine all actions such as add, edit and to delete groups.

Sample Request

```
POST /sma/api/v2.0/config/centralizedServices/centralizedReporting/allGroups?device_type=sma&
 HTTP/1.1
cache-control: no-cache
Postman-Token: df8d239e-24dd-462e-990f-fd3cba5e0b83
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 277
Connection: keep-alive

{"data":{"centralizedReporting":{"allGroups":[{"test
4":{"appliances":["4229A2096D9E0C1C3A78-A82D93282C7A","4229CAEC09527FD2570C-F028BAE54A11"]}},{"test

1":{"appliances":["4229A2096D9E0C1C3A78-A82D93282C7A"]}},{"test-2":{"appliances":["4229CAEC09527FD2570C-F028BAE54A11"]}}]}}}
```

Sample Response

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Thu, 28 May 2020 17:34:48 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 61
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

{"data": {"message": "Updated centralized reporting groups"}}
```

```
Note: A reporting group can have key parameters, which are 'appliances' and 'newGroup'. The
 'appliances' parameter is mandatory. To edit a group name, use 'newGroup' parameter.
```

Combine All Actions Exceeding 100 Characters

Combined all actions exceeding 100 characters.

Synopsis	https://u32c01p14-vrouter.cisco.com:4599/sma/api/v2.0/config/centralizedServices/centralizedReporting/allGroups

This example shows a query combine all actions that exceeds 100 characters.

Sample Request

```
{
    "data": {
        "centralizedReporting": {
            "allGroups": [
                {
                    "zzz123": {
                        "appliances": [
                            "420E74056157AC99D24A-600741749CD3",
                            "420E6D0465DF4F1107A8-EA6829376651"
                        ]
                    }
                },
                {
"pneumonoultramicroscopicsilicovolcanoconiosispneumonoultrapneumonoultramicroscopicsilicovolcanoconiosispneumonoultrapneumonoultramicroscopicsili":
 {
                        "appliances": [
                            "420E6D0465DF4F1107A8-EA6829376651"
                        ]
                    }
                },
                {
                    "pneumonoultramic": {
                        "appliances": [
                            "420E6D0465DF4F1107A8-EA6829376651"
                        ]
                    }
}
```

Sample Response

```
{

       "error": {

           "message": "Group Name exceeds 100 characters.",

           "code": "404",

           "explanation": "404 = Nothing matches the given URI."

       }

   }
```

Edit Single Reporting Groups

Edit Single Reporting Groups (PUT method).

Synopsis	https://u32c01p14-vrouter.cisco.com:4599/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups

This example shows a query edit single reporting groups.

Sample Request

```
Request:
{
    "data": {
        "centralizedReporting": {
            "reportingGroups": [
                {
                    "divs1K": {
                        "appliances": [
                                "420E6D0465DF4F1107A8-EA6829376651",
                                "420E74056157AC99D24A-600741749CD3"
                        ],
                        "newGroup":"merciii"
                    }
                }
            ]
        }
    }
}
```

Sample Response

```
{
    "data": {
        "message": "Updated successfully"
    }
}
```

Note In PUT method, a reporting group can have key parameters, which are 'appliances' and 'newGroup'. 'appliances' parameter is mandatory. To edit a group name, use 'newGroup' parameter.

Edit Multiple Reporting Groups

Edit Multiple reporting groups with change of group name (PUT).

Synopsis	https://u32c01p14-vrouter.cisco.com:4599/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups

This example shows a query to edit multiple reporting groups.

Sample Request

```
{
    "data": {
        "centralizedReporting": {
            "reportingGroups": [
                {
                    "divs12K": {
                        "appliances": [
                                "420E6D0465DF4F1107A8-EA6829376651",
                                "420E74056157AC99D24A-600741749CD3"
                        ],
                        "newGroup":"merci"
```

```
                    }
                },
                {
                      "divs6K": {
                        "appliances": [
                        ]

                    }
                }
            ]
        }
    }
}
```

Sample Response

```
{
    "data": {
        "message": "Updated successfully"
    }
}
```

Edit Reporting Groups

Edit reporting group with group name that exceeds 100 characters (PUT).

Synopsis	https://u32c01p14-vrouter.cisco.com:4599/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups

This example shows a query to edit reporting group name that exceed 100 characters.

Sample Request

```
{
    "data": {
        "centralizedReporting": {
            "reportingGroups": [
                {
                    "divs1M": {
                        "appliances": [
                                "420E6D0465DF4F1107A8-EA6829376651",
                                "420E74056157AC99D24A-600741749CD3"
                        ],

"newGroup":"pneumonoultramicroscopicsilicovolcanoconiosispneumonoultrpneumonoultramicroscopicsilicovolcanoconiosispneumonoul"

                    }
                },
                {
                    "jo": {
                        "appliances": [
                                "420E6D0465DF4F1107A8-EA6829376651",
                                "420E74056157AC99D24A-600741749CD3"
                        ]
                    }
                }
            ]
        }
    }
}
```

Sample Response

```
{
    "error": {
        "message": "Group Name exceeds 100 characters.",
        "code": "404",
        "explanation": "404 = Nothing matches the given URI."
    }
}
```

Querying for Safelist Blocklist

This section contains the following topics:

Retrieve Safelist Blocklist Settings

Synopsis	GET /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings

```
{"data": {"safelistBlocklist": {"settings": {"maxUserEntries": 100, "updatePeriod": 7200}}}}
```

This example shows a query to retrieve the safelist and blocklist settings.

Sample Request

```
GET /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: e547122f-b5c6-4663-b33f-610405b9fb69
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 17:03:14 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 92
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

{"data": {"safelistBlocklist": {"settings": {"maxUserEntries": 100, "updatePeriod": 7200}}}}
```

Enable Safelist Blocklist Settings

Enable Safelist or Blocklist settings with maximum list items per user as 160 and update the frequency for every 3 hours.

Synopsis	PUT /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings

This example shows a query to enable Safelist or Blocklist settings.

Sample Request

```
PUT /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: 97173889-0246-4c56-bac0-baac336eec26
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 87
Connection: keep-alive
{"data":{"safelistBlocklist":{"settings":{"maxUserEntries":160,"updatePeriod":10800}}}}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 15:03:29 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
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

{"data": {"message": "Updated successfully"}}
```

Retrieve File Transfer Status

Retrieve the File Transfer status of all appliances.

Synopsis	GET /sma/api/v2.0/config/centralizedServices/safelistBlocklist/fileTransferStatus

```
{"data": {"safelistBlocklist": {"fileTransferStatus": {"appliances": []}}}}
```

This example shows a query to retrieve file transfer status.

Sample Request

```
GET
/sma/api/v2.0/config/centralizedServices/safelistBlocklist/fileTransferStatus?device_type=sma&
 HTTP/1.1
cache-control: no-cache
Postman-Token: 1b95101b-8846-4be1-ba3d-3199315f3a1d
Authorization: Basic YWRtaW46Q2lzY29AMTIz
```

```
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 17:07:25 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 75
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

{"data": {"safelistBlocklist": {"fileTransferStatus": {"appliances": []}}}}
```

Synchronize File Transfer Status

Synopsis	GET /sma/api/v2.0/config/centralizedServices/safelistBlocklist/appliancesSyncStatus

```
{"data": {"safelistBlocklist": {"appliancesSyncStatus": {"message": "Safelist/Blocklist
database synchronization started."}}}}
```

This example shows a query to synchronize file transfer status.

Sample Request

```
GET
/sma/api/v2.0/config/centralizedServices/safelistBlocklist/appliancesSyncStatus?device_type=sma&
 HTTP/1.1
cache-control: no-cache
Postman-Token: 51e68356-b83b-404e-ae3a-668f38da04d6
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 29 May 2020 11:51:18 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 126
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

{"data": {"safelistBlocklist": {"appliancesSyncStatus": {"message": "Safelist/Blocklist
database synchronization started."}}}}
```

Querying Spam Settings

This section consists the following topics:

Retrieve Spam Settings with Default Logo

Synopsis	`GET /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings`

```
{"data": {"spamQuarantine": {"settings": {"localUsers": [], "customLogoMetadata": {},
"messageTtl": "N/A", "scheduleDelete": "disabled", "externalAdminGroups": [], "customRoles":
[], "primaryServer": {"releasePort": 25, "releaseHost": "127.0.0.1"}, "alternativeServer":
{"altReleaseHost": "127.0.0.1", "altReleasePort": 25}, "customLogo": "N/A", "serverPort":
57, "customLoginMessage": "N/A", "interface": "Management", "sendCopy": "disabled"}}}}
```

This example shows a query to retrieve spam settings with a default logo.

Sample Request

```
GET /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: 356d3ccf-f90e-40c5-ac17-8704ddcdea40
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 17:47:41 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 446
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
```

{"data": {"spamQuarantine": {"settings": {"localUsers": [], "customLogoMetadata": {},
"messageTtl": "N/A", "scheduleDelete": "disabled", "externalAdminGroups": [], "customRoles":
 [], "primaryServer": {"releasePort": 25, "releaseHost": "127.0.0.1"}, "alternativeServer":
 {"altReleaseHost": "127.0.0.1", "altReleasePort": 25}, "customLogo": "N/A", "serverPort":
 57, "customLoginMessage": "N/A", "interface": "Management", "sendCopy": "disabled"}}}}

Enabling the Scheduled Delete Settings

Enable the scheduled delete settings.

Synopsis	`PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings`

{"data": {"spamQuarantine": {"settings": {"localUsers": [], "customLogoMetadata": {},
"messageTtl": "N/A", "scheduleDelete": "disabled", "externalAdminGroups": [], "customRoles":
 [], "primaryServer": {"releasePort": 25, "releaseHost": "127.0.0.1"}, "alternativeServer":
 {"altReleaseHost": "127.0.0.1", "altReleasePort": 25}, "customLogo": "N/A", "serverPort":
 57, "customLoginMessage": "N/A", "interface": "Management", "sendCopy": "disabled"}}}}

This example shows a query to enable the scheduled delete settings.

Sample Request

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: 63fbf560-70d4-498c-994c-f96d79ef226c
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 408
Connection: keep-alive
```

{"data": {"spamQuarantine": {"settings": {"localUsers": [], "customLogoMetadata": {},
"messageTtl": "N/A", "scheduleDelete": "disabled", "externalAdminGroups": [], "customRoles":
 [], "primaryServer": {"releasePort": 25, "releaseHost": "127.0.0.1"}, "alternativeServer":
 {"altReleaseHost": "127.0.0.1", "altReleasePort": 25}, "customLogo": "N/A", "serverPort":
 57, "customLoginMessage": "N/A", "interface": "Management", "sendCopy": "disabled"}}}}

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 18:04:46 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 56
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

{"data": {"message": "Updated spam quarantine setings"}}
```

Enable Spam Settings

Enable spam settings with schedule delete settings and custom login message “Welcome”.

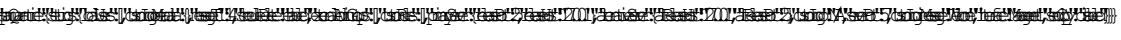
Synopsis	`PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings`

{"data": {"spamQuarantine": {"settings": {"localUsers": [], "customLogoMetadata": {},
"messageTtl": "N/A", "scheduleDelete": "disabled", "externalAdminGroups": [], "customRoles":
 [], "primaryServer": {"releasePort": 25, "releaseHost": "127.0.0.1"}, "alternativeServer":
 {"altReleaseHost": "127.0.0.1", "altReleasePort": 25}, "customLogo": "N/A", "serverPort":
 57, "customLoginMessage": "N/A", "interface": "Management", "sendCopy": "disabled"}}}}

This example shows a query to enable spam settings with schedule delete settings and custom login message.

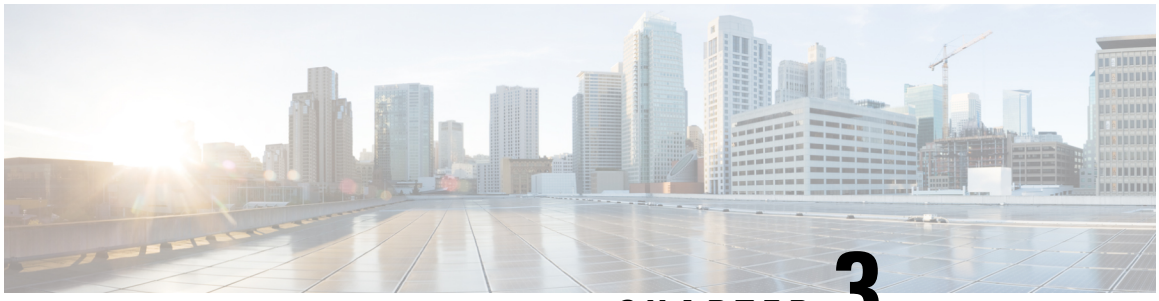
Sample Request

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: d48d5462-98ea-4031-8506-5d6cf91f3393
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 412
Connection: keep-alive
```



Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 18:12:36 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 56
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
{"data": {"message": "Updated spam quarantine setings"}}
```



CHAPTER 3

APIs for Web

Reporting APIs

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

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.
	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_type=wsa` 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, on page 121
- Retrieving Multiple Values for a Counter, on page 122
- Retrieving Single Values for Each Counter in a Counter Group, on page 123
- Retrieving Multiple Values for Multiple Counters, on page 124
- Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter, on page 126

Retrieving a Single Value for a Counter

This example shows a query to retrieve a single value for a counter.

Sample Request

```
GET /sma/api/v2.0/reporting/web_malware_category_malware_name_user_detail/
blocked_malware?startDate=2017-11-14T02:00+00:00&endDate=2018-02-18T01:00+00:00&
filterValue=23&filterBy=na&filterOperator=is&device_type=wsa
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 26 Nov 2018 16:29:33 GMT
Content-type: application/json
Content-Length: 193
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": 4
    },
    "data": {
        "type": "blocked_malware",
        "resultSet": {
            "blocked_malware": [
                {
                    "10.8.93.12": 137511
                },
                {
                    "10.8.93.20": 112554
                },
                {
                    "10.8.93.11": 92839
                },
                {
                    "10.225.98.234": 6
                }
            ]
        }
    }
}
```

Retrieving Multiple Values for a Counter

This example shows a query to retrieve multiple values for a counter, with the order direction and device type parameters.

Sample Request

```
GET /sma/api/v2.0/reporting/web_services_summary?orderBy=transaction_total&
orderDir=desc&startDate=2018-08-16T18:00:00.000Z&endDate=2018-11-15T10:00:00.000Z&device_type=wsa
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
```

```
Accept: */*
Host: 10.8.159.21:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sun, 18 Nov 2018 15:38:52 GMT
Content-type: application/json
Content-Length: 403
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": "web_services_summary",
        "resultSet": [
            {"detected_by_traffic_monitor": 0},
            {"detected_malware_total": 42},
            {"high_risk_transaction_total": 7109},
            {"blocked_by_admin_policy": 0},
            {"detected_by_amp": 0},
            {"allowed_transaction_total": 26369},
            {"transaction_total": 33478},
            {"blocked_or_warned_by_webcat": 29},
            {"blocked_by_wbrs": 7038},
            {"blocked_by_avc": 0}
        ]
    }
}
```

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 the filter, device type, and top parameters.

Sample Request

```
GET /sma/api/v2.0/reporting/web_application_type_detail/bw_not_limited?startDate=
2017-09-10T19:00:00.000Z&endDate=2018-09-24T23:00:00.000Z&device_type=wsa&filterValue=
F&filterOperator=begins_with&filterBy=na&top=2
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.8.159.21:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sun, 18 Nov 2018 15:48:21 GMT
Content-type: application/json
```

```
Content-Length: 138
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": 2
    },
    "data": {
        "type": "bw_not_limited",
        "resultSet": {
            "bw_not_limited": [
                {"File Sharing": 84},
                {"Facebook": 42}
            ]
        }
    }
}
```

Retrieving Multiple Values for Multiple Counters

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

Sample Request

```
GET /sma/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: sma.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 the offset and limit, and query type parameters.

Sample Request

```
GET /sma/api/v2.0/reporting/web_application_name_application_type_detail?startDate
=2017-08-16T18:00:00.000Z&endDate=2018-11-15T15:00:00.000Z&device_type=wsa&query_type=export
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.8.159.21:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sun, 18 Nov 2018 15:55:50 GMT
Content-type: application/json
Content-Length: 1258
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": "web_application_name_application_type_detail",
        "resultSet": {
            "time_intervals": [
                {
                    "end_timestamp": 1538332199,
                    "counter_values": [
                        {
                            "counter_values": [
                                42,
                                25932,
                                0,
                                42,
                                0,
                                42,
```

```
            0
        ],
        "application_type": "File Sharing",
        "counter_key": "4shared"
    },
    {
        "counter_values": [
            2,
            109614,
            0,
            2,
            0,
            2,
            0
        ],
        "application_type": "Media",
        "counter_key": "Dailymotion"
    },
    {
        "counter_values": [
            42,
            20748,
            0,
            42,
            0,
            42,
            0
        ],
        "application_type": "Facebook",
        "counter_key": "Facebook General"
    },
    {
        "counter_values": [
            42,
            20580,
            0,
            42,
            0,
            42,
            0
        ],
        "application_type": "File Sharing",
        "counter_key": "MediaFire"
    },
    {
        "counter_values": [
            229,
            158838,
            0,
            229,
            0,
            229,
            0
        ],
        "application_type": "Social Networking",
        "counter_key": "Twitter"
    },
    {
        "counter_values": [
            1,
            86334,
            0,
            1,
            0,
```

```
                                1,
                                0
                            ],
                            "application_type": "Instant Messaging",
                            "counter_key": "Wechat_web"
                        },
                        {
                            "counter_values": [
                                44,
                                40876,
                                0,
                                44,
                                0,
                                44,
                                0
                            ],
                            "application_type": "Media",
                            "counter_key": "YouTube"
                        }
                    ],
                    "begin_timestamp": 1530383400,
                    "end_time": "2018-09-30T23:59:00.000Z",
                    "begin_time": "2018-07-01T00:00:00.000Z"
                }
            ],
            "counter_names": [
                "bw_not_limited",
                "bandwidth_used",
                "bw_limited",
                "completed_transaction_total",
                "blocked_transaction_total",
                "transaction_total",
                "blocked_by_avc"
            ]
        }
    }
}
```


Tracking APIs

You can use web tracking APIs to search for and get details about individual transactions or patterns of transactions. Web tracking APIs are:

- Proxy Services, on page 128
- Layer 4 Traffic Monitor, on page 131
- SOCKS Proxy, on page 133

Proxy Services

You can retrieve information about web usage for a particular user or for all users using multiple attributes.

Synopsis	`GET /api/v2.0/web-tracking/web_transaction?resource_attribute`
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Cisco Content Security Management Appliances for more information.

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

Example

This example shows a query to retrieve transactions processed by the Proxy Services, with the duration, filtering, offset and limit, ordering, and transactions status parameters.

Sample Request

```
GET /sma/api/v2.0/web-tracking/web_transaction?startDate=2016-09-30T18:00:00.000Z
&endDate=2018-10-31T19:00:00.000Z&filterBy=proxy_services&filterOperator=is&limit=20&offset=0
&device_type=wsa&orderBy=timestamp&orderDir=desc&transactionStatus=all&
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.225.99.234:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 14:43:38 GMT
Content-type: application/json
Content-Length: 26617
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": 20
    },
    "data": [
        {
            "attributes": {
                "webCategory": "Computers and Internet",
                "contentType": "-",
                "pageResources":
"http://update.googleapis.com/service/update2?cup2key=8:128910954&cup2hreq=
                 3a51fa0a72aa94fcba12403f2eb11c4884b27862dd31a779133c03a0e61d334d",
                "applicationBehavior": "-",
                "malwareCategory": "-",
                "fileName": "-",
                "SHA": "-",
                "bandwidth": 0,
                "policyType": "Access",
                "user": "192.168.0.158",
                "srcIP": "192.168.0.158",
                "relatedTransCount": 1,
                "malwareName": "-",
                "applicationName": "-",
```

```
                "policyName": "DefaultGroup",
                "threatType": "Computers and Internet",
                "ampFileVerdict": "-",
                "destinationIP": "-",
                "userType": "[-]",
               "threatReason": "Information about computers and software, such as hardware,
 software, software
                support, information for software engineers, programming and networking,
website design, the web
                and Internet in general, computer science, computer graphics and clipart.
 Freeware and Shareware
                is a separate category.",
                "serialNo": "4229C3B46A609471867D-0720DA1A8A64",
                "wbrsScore": "No Score",
                "decisionSrc": "WEBCAT",
                "url":
"http://update.googleapis.com/service/update2?cup2key=8:128910954&cup2hreq=3a51fa0a72aa94f
                cba12403f2eb11c4884b27862dd31a779133c03a0e61d334d",
                "applicationType": "-",
                "timestamp": 1540275265,
                "transactionStatus": "BLOCK",
                "ampVerdict": "-"
            }
        },
        {
            "attributes": {
                "webCategory": "Business and Industry",
                "contentType": "-",
                "pageResources":
"ftp://www.purple.com/,http://www.purple.com/,http://www.purple.com/",
                "applicationBehavior": "-",
                "malwareCategory": "-",
                "fileName": "-",
                "SHA": "-",
                "bandwidth": 0,
                "policyType": "Access",
                "user": "10.10.5.105",
                "srcIP": "10.10.5.105",
                "relatedTransCount": 3,
                "malwareName": "-",
                "applicationName": "-",
                "policyName": "DefaultGroup",
                "threatType": "Business and Industry",
                "ampFileVerdict": "-",
                "destinationIP": "-",
                "userType": "[-]",
                "threatReason": "Marketing, commerce, corporations, business practices,
workforce, human resources
                , transportation, payroll, security and venture capital, office supplies,
 industrial equipment
                (process equipment), machines and mechanical systems, heating equipment,
cooling equipment,
                materials handling equipment, packaging equipment, manufacturing: solids
handling, metal fabrication
               , construction and building, passenger transportation, commerce, industrial
 design, construction
                , building materials, shipping and freight (freight services, trucking,
freight forwarders,
               truckload carriers, freight and transportation brokers, expedited services,
 load and freight matching
                , track and trace, rail shipping, ocean shipping, road feeder services,
moving and storage).",
                "serialNo": "4229C3B46A609471867D-0720DA1A8A64",
                "wbrsScore": "No Score",
```

```
                "decisionSrc": "WEBCAT",
                "url": "ftp://www.purple.com/",
                "applicationType": "-",
                "timestamp": 1540274946,
                "transactionStatus": "BLOCK",
                "ampVerdict": "-"
            }
        },
...

...
        {
            "attributes": {
                "webCategory": "Business and Industry",
                "contentType": "-",
                "pageResources":
"ftp://www.purple.com/,http://www.purple.com/,http://www.purple.com/",
                "applicationBehavior": "-",
                "malwareCategory": "-",
                "fileName": "-",
                "SHA": "-",
                "bandwidth": 0,
                "policyType": "Access",
                "user": "10.10.5.105",
                "srcIP": "10.10.5.105",
                "relatedTransCount": 3,
                "malwareName": "-",
                "applicationName": "-",
                "policyName": "DefaultGroup",
                "threatType": "Business and Industry",
                "ampFileVerdict": "-",
                "destinationIP": "-",
                "userType": "[-]",
                "threatReason": "Marketing, commerce, corporations, business practices,
workforce, human resources...
                "serialNo": "4229C3B46A609471867D-0720DA1A8A64",
                "wbrsScore": "No Score",
                "decisionSrc": "WEBCAT",
                "url": "ftp://www.purple.com/",
                "applicationType": "-",
                "timestamp": 1540263898,
                "transactionStatus": "BLOCK",
                "ampVerdict": "-"
            }
        }
    ]
}
```


Layer 4 Traffic Monitor

You can retrieve information about connections to malware sites and ports using multiple attributes.

Synopsis	`GET /api/v2.0/web-tracking/web_transaction?resource_attribute`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Cisco Content Security Management Appliances for more information.	
Request Headers		Host, Accept, Authorization

Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve transactions processed by the Layer 4 Traffic Monitor, with the duration, filtering, offset and limit, ordering, and transactions status parameters.

Sample Request

```
GET /sma/api/v2.0/web-tracking/web_transaction?startDate=2016-09-30T18:00:00.000Z
&endDate=2018-10-31T19:00:00.000Z&filterBy=l4tm&filterOperator=is&limit=20&offset=0&device_type
=wsa&orderBy=timestamp&orderDir=desc&transactionStatus=all&
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.225.99.234:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 14:58:11 GMT
Content-type: application/json
Content-Length: 12
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": 20
    },
    "data": [
        {
            "attributes": {
                "l4tmDestDomain": "ticketbooking.com",
                "l4tmUser": "10.10.99.68",
                "timestamp": 1534143578,
                "l4tmPort": 443,
                "serialNo": "42292E04F63C3DE54F13-E5D7466DA42E",
                "l4tmDestIpWithDomain": "103.117.180.6@ticketbooking.com",
                "transactionStatus": "BLOCKED"
            }
        },
        {
            "attributes": {
                "l4tmDestDomain": "ticketbooking.com",
                "l4tmUser": "10.10.99.68",
                "timestamp": 1534143578,
                "l4tmPort": 443,
                "serialNo": "42292E04F63C3DE54F13-E5D7466DA42E",
                "l4tmDestIpWithDomain": "103.117.180.6@ticketbooking.com",
                "transactionStatus": "BLOCKED"
            },
...
```

```
...
        {
            "attributes": {
                "l4tmDestDomain": "ticketbooking.com",
                "l4tmUser": "10.10.99.68",
                "timestamp": 1534143577,
                "l4tmPort": 443,
                "serialNo": "42292E04F63C3DE54F13-E5D7466DA42E",
                "l4tmDestIpWithDomain": "103.117.180.6@ticketbooking.com",
                "transactionStatus": "BLOCKED"
            }
        }
    ]
}
```

SOCKS Proxy

You can retrieve information about transactions processed through the SOCKS proxy, including information about top destinations and users.

Synopsis	`GET /api/v2.0/web-tracking/web_transaction?resource_attribute`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Cisco Content Security Management Appliances for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve transactions processed by the SOCKS Proxy Services, with the duration, filtering, offset and limit, ordering, and transactions status parameters.

Sample Request

```
GET /sma/api/v2.0/web-tracking/web_transaction?startDate=2016-09-30T18:00:00.000Z&
endDate=2018-10-31T19:00:00.000Z&filterBy=socks_proxy&filterOperator=is&limit=20&offset=0&
device_type=wsa&orderBy=timestamp&orderDir=desc&socksTransportProtocol=all&transactionStatus=all&
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.225.99.234:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

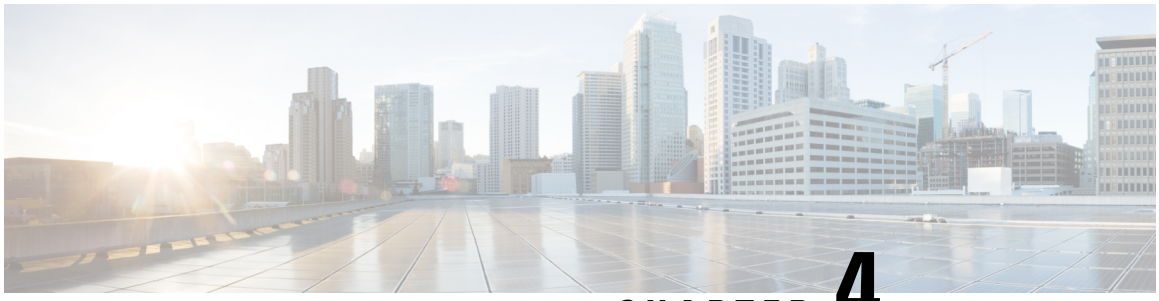
Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 19 Nov 2018 14:53:33 GMT
Content-type: application/json
Content-Length: 6629
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": 20
    },
    "data": [
        {
            "attributes": {
                "socksUser": "10.10.5.106",
                "socksBandwidth": 0,
                "socksUserType": "[-]",
                "timestamp": 1538044948,
                "socksTransportProtocol": "TCP",
                "socksPort": 80,
                "socksSrcIp": "10.10.5.106",
                "socksDestinationIp": "-",
                "socksPolicyName": "DefaultGroup",
                "socksHostName": "concede.fmtlib.net",
                "transactionStatus": "BLOCK"
            }
        },
        {
            "attributes": {
                "socksUser": "10.10.5.106",
                "socksBandwidth": 0,
                "socksUserType": "[-]",
                "timestamp": 1538044948,
                "socksTransportProtocol": "TCP",
                "socksPort": 80,
                "socksSrcIp": "10.10.5.106",
                "socksDestinationIp": "-",
                "socksPolicyName": "DefaultGroup",
                "socksHostName": "erupt.fernetmoretti.com.ar",
                "transactionStatus": "BLOCK"
            }
        },
...

...
        {
            "attributes": {
                "socksUser": "10.10.5.106",
                "socksBandwidth": 0,
                "socksUserType": "[-]",
                "timestamp": 1538044947,
                "socksTransportProtocol": "TCP",
                "socksPort": 80,
                "socksSrcIp": "10.10.5.106",
                "socksDestinationIp": "-",
                "socksPolicyName": "DefaultGroup",
                "socksHostName": "boots.fotopyra.pl",
                "transactionStatus": "BLOCK"
            }
        }
    ]
}
```



CHAPTER 4

General Purpose APIs

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

This chapter contains the following sections:

Querying for the System Time

Sample Request

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

Sample Response

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

```
        "time": "Thu Apr 12 23:38:05 2018 IST",
        "timezone": "Asia/Kolkata"
    }
}
```

Querying for Managed Email Security Appliances' Information

Sample Request

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

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Apr 2018 18:09:07 GMT
Content-type: application/json
Content-Length: 341
Connection: close
{
    "data": {
        "appliances": [
            {
                "123A45B6C678-1CDEFG2": {
                    "host_name": "esa11.1",
                    "ip_address": "10.76.69.29",
                    "product_type": "ESA"
                }
            },
            {
                "123A45B6C678-1CDEFG3": {
                    "host_name": "esa11.0",
                    "ip_address": "10.76.68.224",
                    "product_type": "ESA"
                }
            },
            {
                "123A45B6C678-1CDEFG3": {
                    "host_name": "esa10.0.2",
                    "ip_address": "10.76.71.63",
                    "product_type": "ESA"
                }
            }
        ]
    }
}
```

Querying for the Details of Centralized Services

Sample Request

```
GET /sma/api/v2.0/config/centralized_services?device_type=sma
HTTP/1.1
cache-control: no-cache
```

```
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Accept: */*
Host: sma.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Apr 2018 18:13:50 GMT
Content-type: application/json
Content-Length: 169
Connection: close
{
    "data": {
        "centralized_quarantines": {
            "pvo_quarantine": "Enabled",
            "spam_quarantine": "Enabled"
        },
        "centralized_reporting": "Enabled",
        "centralized_tracking": "Enabled"
    }
}
```

Querying for Reporting Groups' Information

You can query for information about Reporting Groups, that include one or more Email Security appliances.

Sample Request

```
GET /sma/api/v2.0/config/reporting_groups?device_type=sma
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46SXJvbnBvcnQxMjMk
Accept: */*
Host: sma.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Apr 2018 05:41:47 GMT
Content-type: application/json
Content-Length: 397
Connection: close
{
    "data": {
        "reporting_groups": [
            {
                "2_esa_grp": {
                    "appliances": [
                        "123A45B6C678-1CDEFG2",
                        "123A45B6C678-1CDEFG3"
                    ]
                }
            },
            {
                "Emtpy_Group": {
                    "appliances": []
                }
```

```
            },
            {
                "du!@#$%^&*()_+{}=_+{}][:\"';<>?/.,": {
                    "appliances": [
                        "123A45B6C678-1CDEFG4",
                        "123A45B6C678-1CDEFG5"
                    ]
                }
            },
            {
                "Hosted_Group": {
                    "appliances": [
                        "123A45B6C678-1CDEFG6",
                        "123A45B6C678-1CDEFG7"
                    ]
                }
            },
            {
                "1_esa_grp": {
                    "appliances": [
                        "123A45B6C678-1CDEFG8"
                    ]
                }
            }
        ]
    }
}
```

Retrieving APIs Accessible to a User Role

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

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

Sample Request

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

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Apr 2018 14:17:44 GMT
Content-type: application/json
Content-Length: 4392
Connection: close
{
```

```
    "data": [
        "e_message_tracking_messages",
        "e_message_tracking_detail",
        "e_message_tracking_availability",
        "e_message_tracking_verdict",
        "e_message_tracking_dlp_details",
        "e_message_tracking_amp_details",
...
...
        "e_config_macro_file_types",
        "e_config_geo_countries",
        "e_config_tracking_query_timeout",
        "e_config_spam_quarantine_appearance_details",
        "sma_config_users",
        "e_config_euq_authentication_method",
        "e_config_euq_url_details"
    ]
}
```

Retrieving the System Status

Retrieve the system status of the feature.

Synopsis	GET /sma/api/v2.0/config/centralizedServices/systemStatus

This example shows a query to retrieve the system status of a feature.

Sample Request

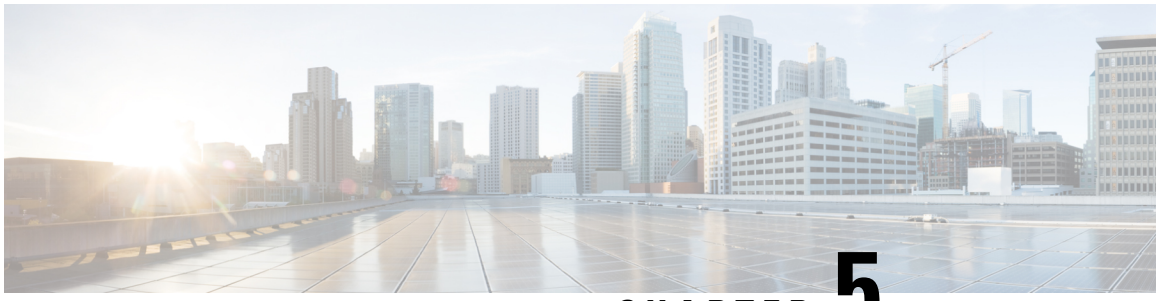
```
GET /sma/api/v2.0/config/centralizedServices/systemStatus?device_type=sma HTTP/1.1
cache-control: no-cache
Postman-Token: 0d768c44-40cd-445d-881e-f13cc0965ff1
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: 10.8.159.21:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 30 Jul 2020 16:37:05 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 788
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

{"data": {"systemStatus": {"diskQuota": {"pvoQuarantine": "0.0", "spamQuarantine": "0.0"},
 "applianceStatus": {"pvoQuarantine": {"activeDevices": 2, "totalDevices": 2},
"centralizedReporting": {"activeDevices": 2, "totalDevices": 2}, "centralizedTracking":
"Service disabled - Centralized Tracking", "spamQuarantine": "Service disabled - Spam
```

Quarantine"}, "licencesStatus": {"pvoQuarantine": {"licences": 2}, "centralizedReporting":
{"licences": 2}, "centralizedTracking": "Service disabled - Centralized Tracking",
"spamQuarantine": "Service disabled - Spam Quarantine"}, "quarantineMessages":
{"pvoQuarantine": 0, "spamQuarantine": 0}, "emailAppliancesStatus": {"activeDevices": 2,
"totalDevices": 2}, "processingQueue": {"centralizedReporting": "0.0", "centralizedTracking":
"0.0"}}}}



CHAPTER 5

Troubleshooting AsyncOS API

This chapter contains the following sections:

API Logs

Subscribe to the API logs using **System Administration** > **Log Subscriptions**. For instructions, see the AsyncOS 11.4 for Cisco Content Security Management Appliances or Online Help.

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

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

Alerts

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

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