



AsyncOS API 13.0 for Cisco Security Management Appliances - Getting Started Guide - LD (Limited Deployment)

First Published: 2019-11-01

Last Modified: 2020-01-06

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Overview of AsyncOS API for Cisco Security Management Appliances 1

- Prerequisites for Using AsyncOS API 1
- Enabling AsyncOS API 2
- Securely Communicating with AsyncOS API 2
- AsyncOS API Authentication and Authorization 3
 - Authentication 3
 - Authenticating API Queries with JSON Web Token 3
 - Authorization 4
- AsyncOS API Requests and Responses 5
 - AsyncOS API Requests 5
 - AsyncOS API Responses 6
 - Key Components of Responses 6
 - HTTP Response Codes 7
- Comparing API Data with the Web Interface Data 8
- Related Documentation 8

CHAPTER 2

APIs for Email 9

- Reporting APIs 9
 - Examples 11
 - Retrieving a Single Value for a Counter 12
 - Retrieving Multiple Values for a Counter 12
 - Retrieving Single Values for Each Counter in a Counter Group 13
 - Retrieving Multiple Values for Multiple Counters 14
 - Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter 16
- Tracking APIs 18
 - Searching for Messages 18

Rejected Connections	23
Message Details	24
DLP Details	27
AMP Details	28
URL Details	30
Connection Details	32
Quarantine APIs	34
APIs for Spam Quarantine	34
Searching for Messages	34
Retrieving Message Details	37
Deleting Messages	39
Releasing Messages	40
Searching for Safelist and Blocklist Entries	41
Adding, Editing, and Appending Safelist and Blocklist Entries	44
Deleting Safelist or Blocklist Entries	57
APIs for Other Quarantine	61
Searching for Messages	61
Retrieving Message Details	68
Move Messages	70
Delaying the Exit of a Message from a Quarantine	71
Sending a Copy of a Message in Quarantine	73
Downloading an Attachment	75
Deleting Messages	76
Releasing Messages	77
Viewing the Rule Summary	79
Searching Based on Rule ID	80
Releasing Messages from the Rule Summary	83
Deleting Messages from the Rule Summary	84

CHAPTER 3**APIs for Web 87**

Reporting APIs	87
Examples	89
Retrieving a Single Value for a Counter	89
Retrieving Multiple Values for a Counter	90

Retrieving Single Values for Each Counter in a Counter Group	91
Retrieving Multiple Values for Multiple Counters	92
Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter	94
Tracking APIs	96
Proxy Services	96
Layer 4 Traffic Monitor	99
SOCKS Proxy	101

CHAPTER 4	General Purpose APIs	103
	Querying for the System Time	103
	Querying for Managed Email Security Appliances' Information	104
	Querying for the Details of Centralized Services	104
	Querying for Reporting Groups' Information	105
	Retrieving APIs Accessible to a User Role	106

CHAPTER 5	Troubleshooting AsyncOS API	109
	API Logs	109
	Alerts	109



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, on page 1](#)
- [Enabling AsyncOS API, on page 2](#)
- [Securely Communicating with AsyncOS API, on page 2](#)
- [AsyncOS API Authentication and Authorization, on page 3](#)
- [AsyncOS API Requests and Responses, on page 5](#)
- [Comparing API Data with the Web Interface Data, on page 8](#)
- [Related Documentation, on page 8](#)

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 106](#)

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. <pre>{ "data": { "userName": "YWRtaW4=", "passphrase": "aXJvbnBvcnQ=" } }</pre>	
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.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoiYmFjdG9yQ2h1Y2tSZXF1aXJlZCI6ZmFsc2UsImNvb2tpZSI6Ii1RucEZOVTFWFTNwTlZFMd1DanRMYVRoeENqdFpiV1J6VFVSQk5VMURNWGRpTWxGMVdUSnNlbGt5T0hWWk1qbDBUMnBaZDA5RVFUMEtcbk8xVkhPWHBrUnpGbl1teEtNV0plVW5CaVYxVjJUbmswTUV4cVFUMEtPMVJVUlhkTlJsaZNUV1JKZFUxRE5I ZE1WRWw1VFdweklFMXFcb1NUV1NhazVDVDBWRk1rOUVaM2xTU1VreVRYcGtSazFwTVVSTlZFMHhUUbFZXUjA1"
  }
}
```

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	<p>The message body is in the format defined by the Content-Type header. The following are the components of the message body:</p> <ol style="list-style-type: none"> 1. URI. The URI you specified in the request to the API. <p>Example</p> <pre>:/api/v2.0/config/</pre> 2. Counter group and/or counter name <p>Example</p> <pre>reporting/mail_security_summary</pre> 3. Query parameters <p>Example</p> <pre>startDate=2017-01-30T00:00:00.000Z&endDate=2018-01-30T14:00:00.000Z</pre> 4. Error (Only for Error Events). This component includes three subcomponents—message, code, and explanation. <p>Example</p> <pre>"error": {"message": "Unexpected attribute - starts_with.", "code": "404", "explanation": "404 = Nothing matches the given URI."}</pre> <p>If the message body contains empty braces ({}), it means that the API could not find any records matching the query.</p>

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)	<p>On the new web interface, hover over the help icon, and click API Help: Swagger.</p> <p>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.</p>



CHAPTER 2

APIs for Email

- [Reporting APIs, on page 9](#)
- [Tracking APIs, on page 18](#)
- [Quarantine APIs, on page 34](#)

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	<code>GET /api/v2.0/reporting/report?resource_attribute</code> <code>GET /api/v2.0/reporting/report/counter?resource_attribute</code>
-----------------	--

Supported Resource Attributes	Duration	<p>This is a required parameter. All API queries should be accompanied with this parameter.</p> <pre>startDate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</pre> <p>Aggregate report(s) for the specified duration.</p> <p>Note The duration attribute supports only 00 as value in the minutes (mm) and seconds (ss) parameters.</p>
	Query Type	<ul style="list-style-type: none"> • <code>query_type=graph</code> Receive data that can be represented as graphs. • <code>query_type=export</code> Receive data in the export format.
	Sorting	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> • <code>orderBy=<value></code> Specify the attribute by which to order the data in the response. For example, <pre>orderBy=total_clean_recipients</pre> • <code>orderDir=<value></code> Specify sort direction. The valid options are: <ul style="list-style-type: none"> • <code>asc</code> Order the results in ascending order. • <code>desc</code> Order the results in descending order.
	Lazy Loading	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> • <code>offset=<value></code> 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. • <code>limit=<value></code> Specify the number of records to retrieve.
	Data Retrieval Option	<ul style="list-style-type: none"> • <code>top=<value></code> Specify the number of records with the highest values to return.
Filtering		

		<p>Filter parameters restrict the data to be included the response.</p> <ul style="list-style-type: none"> • <code>filterValue=<value></code> The value to search for. • <code>filterBy=<value></code> Filter the data to be retrieved according to the filter property and value. • <code>filterOperator=<value></code> The valid options are: <ul style="list-style-type: none"> • <code>begins_with</code> Filter the response data based on the value specified. This is not an exact value. • <code>is</code> Filter the response data based on the exact value specified.
	Device	<ul style="list-style-type: none"> • <code>device_group_name=<value></code> Specify the device group name. • <code>device_type=esa</code> Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter. • <code>device_name=<value></code> 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},
  ]
}
}
}
}
}

```

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 18](#)
- [Rejected Connections, on page 23](#)
- [Message Details, on page 24](#)
- [DLP Details, on page 27](#)
- [AMP Details, on page 28](#)
- [URL Details, on page 30](#)
- [Connection Details, on page 32](#)

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	<p>This is a required parameter. All API queries should be accompanied with this parameter.</p> <p>startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</p> <p>Aggregate report(s) for the specified duration.</p>
	Search Option	<ul style="list-style-type: none"> searchOption=<value> <p>This attribute has a single permitted value when querying for rejected connections. For example:</p> <p>searchOption=rejected_connections</p>
	Sender IP	<ul style="list-style-type: none"> senderIp=<value> <p>This is a user defined value. Use the IP address of the server which sends messages. For example:</p> <p>senderIp=10.76.70.112</p>
	Lazy Loading	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> offset=<value> <p>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.</p> <ul style="list-style-type: none"> limit=<value> <p>Specify the number of records to retrieve.</p>
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
-----------------	---


```

        "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	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> icid=<value> mid=<value> Specify the icid of the message. 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 its 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 YWRtaW46Q21zY28xMjMk
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	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> icid=<value> Specify the icid of the message. <ul style="list-style-type: none"> 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 its 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 YWRtaW46Q21zY28xMjMk
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	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> icid=<value> Specify the icid of the message. <ul style="list-style-type: none"> 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 its 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	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> icid=<value> Specify the icid of the message. <ul style="list-style-type: none"> 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 its 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 34](#)
- [APIs for Other Quarantine, on page 61](#)

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 34](#)
- [Retrieving Message Details, on page 37](#)
- [Releasing Messages, on page 40](#)
- [Deleting Messages, on page 39](#)
- [Searching for Safelist and Blocklist Entries, on page 41](#)
- [Adding, Editing, and Appending Safelist and Blocklist Entries, on page 44](#)
- [Deleting Safelist or Blocklist Entries, on page 57](#)

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	<p>This is a required parameter. Use this parameter with all API queries.</p> <ul style="list-style-type: none"> • <code>startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</code> <p>Messages quarantined during this time range.</p>
	Quarantine Type	<ul style="list-style-type: none"> • <code>quarantineType=<value></code> <p>The accepted value is spam.</p> <p><code>quarantineType=spam</code></p>
	Sorting	<p>You can specify the value and the direction order the results.</p> <ul style="list-style-type: none"> • <code>orderBy=<value></code> <p>Valid values are:</p> <ul style="list-style-type: none"> • <code>from_address</code> • <code>to_address</code> • <code>subject</code> <ul style="list-style-type: none"> • <code>orderDir=<value></code> <p>Valid values are:</p> <ul style="list-style-type: none"> • <code>asc</code> • <code>desc</code>
	Lazy Loading	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> • <code>offset=<value></code> <p>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.</p> <ul style="list-style-type: none"> • <code>limit=<value></code> <p>Specify the number of records to retrieve.</p>
	Envelope Recipient	

		<ul style="list-style-type: none"> • envelopeRecipientFilterOperator=<value> The valid values are: <ul style="list-style-type: none"> • 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	<p>Filter parameters restrict the data to be included the response.</p> <ul style="list-style-type: none"> • filterOperator=<value> The value to search for. Valid values are: <ul style="list-style-type: none"> • 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 YWRtaW46Q2lzMjY28xMjMk
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	<ul style="list-style-type: none"> quarantineType=<value> The accepted value is spam. quarantineType=spam
	Message ID	You must specify the mid of the message to retrieve its details. <ul style="list-style-type: none"> 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
MyxB7dsrdq8oTnn8YSi5amR2qihbeq2eJwvVjskfl\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
    UyQJP3Nli/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. <ul style="list-style-type: none"> "mids": [<value>] Specify the mid of the message.
	Quarantine Type	"quarantineType": "value" The valid value is <i>spam</i> .
Request Body	<pre>{ "quarantineType": "spam", "mids": [<mid>] }</pre>	
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. <ul style="list-style-type: none"> "mids": [<value>] Specify the mid of the message.
	Action	"action": "value" The valid value is <i>release</i> .
	Quarantine Type	"quarantineType": "value" The valid value is <i>spam</i> .
Request Body	<pre> { "action": "release: "quarantineType": "spam", "mids": [<mid>] } </pre>	
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	<ul style="list-style-type: none"> • <code>action=<value></code> <p>Valid value is <i>view</i>.</p>
	Quarantine Type	<code>quarantineType=<value></code> <p>The valid value is <i>spam</i>.</p>
	View By	<code>viewBy=<value></code> <p>The valid values are <i>sender</i>, and <i>recipient</i>.</p>
	Order By	<code>orderBy=<value></code> <p>The valid values are <i>sender</i>, and <i>recipient</i>.</p>
	Lazy Loading	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> • <code>offset=<value></code> <p>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.</p> <ul style="list-style-type: none"> • <code>limit=<value></code> <p>Specify the number of records to retrieve.</p>
	Ordering	<code>orderDir=<value></code> <p>Valid values are:</p> <ul style="list-style-type: none"> • <code>asc</code> • <code>desc</code>
	Search	<p>This is only supported for the attribute <i>orderBy=recipient</i>.</p> <code>search=<value></code> <p>This is a user defined value.</p>
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": "ul@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: bg10090-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": "ul@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	<pre> POST /api/v2.0/quarantine/safelist?resource_attribute POST /api/v2.0/quarantine/blocklist?resource_attribute </pre>
-----------------	---

Supported Resource Attributes	Action	<ul style="list-style-type: none"> • action=<value> <p>Valid values are:</p> <ul style="list-style-type: none"> • add • edit • append
	Quarantine Type	<p>quarantineType=<value></p> <p>The valid value is <i>spam</i>.</p>
	View By	<p>viewBy=<value></p> <p>The valid values are <i>sender</i>, and <i>recipient</i>.</p>
	Recipient Addresses	<p>"recipientAddresses": ["value", "value", ...]</p> <p>This is a user defined value. You can enter multiple values.</p>
	Recipient List	<p>"recipientList": ["value", "value", ...]</p> <p>This is a user defined value. You can enter multiple values.</p>
	Sender Addresses	<p>"senderAddresses": ["value", "value", ...]</p> <p>This is a user defined value. You can enter multiple values.</p>
	Sender List	<p>"senderList": ["value", "value", ...]</p> <p>This is a user defined value. You can enter multiple values.</p>

Request Body	<p>Adding a new recipient entry:</p> <pre>{ "action": "add", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }</pre> <p>Adding a new sender entry:</p> <pre>{ "action": "add", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }</pre> <p>Editing a new recipient entry:</p> <pre>{ "action": "edit", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }</pre> <p>Editing a new sender entry:</p> <pre>{ "action": "edit", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }</pre> <p>Appending a new recipient entry:</p> <pre>{ "action": "append", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }</pre> <p>Appending a new sender entry:</p> <pre>{ "action": "append", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }</pre>
Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection

Examples

- [Adding Recipient Safelist Entries, on page 47](#)
- [Adding Sender Safelist Entries, on page 48](#)
- [Adding Recipient Blocklist Entries, on page 49](#)
- [Adding Sender Blocklist Entries, on page 49](#)
- [Editing Recipient Safelist Entries, on page 50](#)
- [Editing Sender Safelist Entries, on page 51](#)
- [Editing Recipient Blocklist Entries, on page 52](#)
- [Editing Sender Blocklist Entries, on page 53](#)
- [Appending Recipient Safelist Entries, on page 53](#)
- [Appending Sender Safelist Entries, on page 54](#)

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 <i>spam</i> .
	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 <i>sender</i> , and <i>recipient</i> .
Request Body	Deleting recipient entries: <pre> { "quarantineType": "spam", "recipientList": ["value", "value"], "viewBy": "recipient" } </pre> Deleting sender entries: <pre> { "quarantineType": "spam", "senderList": ["value"], "viewBy": "sender" } </pre>	
Request Headers	Host, Accept, Authorization	
Response Headers	Content-Type, Content-Length, Connection	

The following APIs are available:

- [Deleting Recipient Safelist Entries, on page 58](#)

- [Deleting Sender Safelist Entries, on page 58](#)
- [Deleting Recipient Blocklist Entries, on page 59](#)
- [Deleting Sender Blocklist Entries, on page 60](#)

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, on page 61](#)
- [Retrieving Message Details, on page 68](#)
- [Move Messages, on page 70](#)
- [Delaying the Exit of a Message from a Quarantine , on page 71](#)
- [Sending a Copy of a Message in Quarantine, on page 73](#)
- [Downloading an Attachment, on page 75](#)
- [Deleting Messages, on page 76](#)
- [Releasing Messages, on page 77](#)
- [Viewing the Rule Summary, on page 79](#)
- [Searching Based on Rule ID, on page 80](#)
- [Releasing Messages from the Rule Summary, on page 83](#)
- [Deleting Messages from the Rule Summary, on page 84](#)

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	<p>This is a required parameter. All API queries should be accompanied with this parameter.</p> <ul style="list-style-type: none"> startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z
	Quarantines to Search	<p>This parameter specifies the quarantines to search for.</p> <ul style="list-style-type: none"> quarantines=<value, value, ...> <p>Valid values are:</p> <p>Outbreak</p> <p>Virus</p> <p>File+Analysis</p> <p>Unclassified</p> <p>Policy</p> <p><user-defined-quarantine></p>
	Subject	<ul style="list-style-type: none"> subjectFilterBy=<value> <p>The valid values are:</p> <p>contains</p> <p>starts_with</p> <p>ends_with</p> <p>matches_exactly</p> <p>does_not_contain</p> <p>does_not_start_with</p> <p>does_not_end_with</p> <p>does_not_match</p> <ul style="list-style-type: none"> subjectFilterValue=<value> <p>This is a user defined value.</p>
	Originating ESA	<p>originatingEsaIp=<value></p> <p>You can specify the IP address of the ESA in which the message was processed.</p>
	Attachment Details	

		<ul style="list-style-type: none"> • <code>attachmentName=<value></code> This is a user defined value. • <code>attachmentSizeFilterBy=<value></code> Valid values are: <code>range</code> <code>less_than</code> <code>more_than</code> • <code>attachmentSizeFromValue=<value_in_KB></code> This is a user defined value. Specify an attachment size in KB. This is applicable when: <ul style="list-style-type: none"> • You choose the <i>range</i> attribute for <i>attachmentSizeFilterBy</i> <code>attachmentSizeFilterBy=range</code> • You choose the <i>more_than</i> attribute for <i>attachmentSizeFilterBy</i> <code>attachmentSizeFilterBy=more_than</code> • <code>attachmentSizeToValue=<value_in_KB></code> This is a user defined value. Specify an attachment size in KB. This is applicable when: <ul style="list-style-type: none"> • You choose the <i>range</i> attribute for <i>attachmentSizeFilterBy</i> <code>attachmentSizeFilterBy=range</code> • You choose the <i>less_than</i> attribute for <i>attachmentSizeFilterBy</i> <code>attachmentSizeFilterBy=less_than</code>
	<p>Quarantine Type</p>	<ul style="list-style-type: none"> • <code>quarantineType=<value></code> The accepted value is <code>pvo</code>. <code>quarantineType=pvo</code>
	<p>Sorting</p>	

	<p>You can specify the value and the direction order the results.</p> <ul style="list-style-type: none"> • orderBy=<value> <p>Values are:</p> <p>sender</p> <p>subject</p> <p>received</p> <p>scheduledExit</p> <p>size</p> <ul style="list-style-type: none"> • orderDir=<value> <p>Values are:</p> <p>asc</p> <p>desc</p>
Lazy Loading	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> • offset=<value> <p>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.</p> <ul style="list-style-type: none"> • limit=<value> <p>Specify the number of records to retrieve.</p>
Envelope Recipient	<ul style="list-style-type: none"> • envelopeRecipientFilterBy=<value> <p>The valid values are:</p> <p>contains</p> <p>starts_with</p> <p>ends_with</p> <p>matches_exactly</p> <p>does_not_contain</p> <p>does_not_start_with</p> <p>does_not_end_with</p> <p>does_not_match</p> <ul style="list-style-type: none"> • envelopeRecipientFilterValue=<value> <p>The value to search for. This is a user defined value. For example, envelopeRecipientFilterValue=user</p>
Envelope Sender	

		<ul style="list-style-type: none"> • 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": [
          "eriferma@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": [
          "eriferma@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": [
      "eriferma@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	<ul style="list-style-type: none"> quarantineType=<value> The accepted value is pvo. quarantineType=pvo
	Message ID	You must specify the mid of the message to retrieve its details. <ul style="list-style-type: none"> 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/15cTAMkUtJtFAY+/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>&nbsp; by pod0090-esa01
with SMTP; 21 Nov 2018 07:01:34 +0000<br>Message-ID: &lt;194652.955603914
-sendEmail@pod1224-client05&gt;<br>From: \"usr2@sender.com\" &lt;usr2@sender
```

```

.com&gt;<br>To: \"eriferma@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. <ul style="list-style-type: none"> "mids": [<value>] Specify the mid/s of the message/s.
	Quarantine Type	"quarantineName": "<value>" The valid value is <i>pvo</i> .
	Destination Quarantine Name	"destinationQuarantineName": "<value>" The valid values are: Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
Request Body	<pre> { "action": "move", "destinationQuarantineName": "<value>", "mids": [<value>], "quarantineName": "<value>", "quarantineType": "pvo" } </pre>	
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	<ul style="list-style-type: none"> "mids": [value] Specify the mid of the message.
	Quarantine Type	"quarantineType": "value" The valid value is <i>pvo</i> .
	Quarantine Name	"quarantineName": "value" The valid values are: Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
	Delay	"delay": "value" The valid values are <i>8h, 24h, 48h, or 1w</i> .
Request Body	<pre>{ "action": "delay", "delay": "<value>", "mids": [<value>], "quarantineName": "<value>", "quarantineType": "pvo" }</pre>	
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	<ul style="list-style-type: none"> "mids": [value] Specify the mid of the message.
	Quarantine Type	"quarantineType": "value" The valid value is <i>pvo</i> .
	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> <p>For outbreak, you can add this optional attribute to the message body:</p> <pre>"sendToCisco": <value></pre> <p>The valid value is <i>true</i>. An example is shown below:</p> <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	<ul style="list-style-type: none"> • mid=<value> Specify the mid of the message.
	Quarantine Type	quarantineType=<value> The valid value is <i>pvo</i> .
	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//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA+AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSB5dW4gaW4gRE9TIGlv
ZGUuZDQ0KJAAAAAAAAAAl+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. <ul style="list-style-type: none"> "mids": [<value>] Specify the mid/s of the message/s.
	Quarantine Type	"quarantineType": "value" The valid value is <i>pvo</i> .
	Quarantine Name	"quarantineName": "<value>" The valid values are: Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
Request Body	<pre>{ "mids": [<mid>], "quarantineName": "<value>", "quarantineType": "pvo" }</pre>	
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. <ul style="list-style-type: none"> "mids": [<value>] Specify the mid of the message.
	Quarantine Type	"quarantineType": "pvo" The valid value is <i>pvo</i> .
	Quarantine Name	"quarantineName": "<value>" The valid values are: Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
	Action	"action": "value" The valid value is <i>release</i> .
Request Body	<pre>{ "action": "release", "mids": [<mid>], "quarantineName": "<value>", "quarantineType": "pvo" }</pre>	
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 <i>pvo</i> .
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 <i>pvo</i> .
	Rule ID	ruleId=<value> This is a user defined value.
	Sorting	You can specify the value and the direction order the results. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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": [
          "eriferma@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": [
          "eriferma@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	<ul style="list-style-type: none"> "ruleId": ["value", "value", ...] Specify the rule IDs.
	Quarantine Type	quarantineType=<value> The valid value is <i>pvo</i> .
	Action	"action": "value" The valid value is <i>release</i> .

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	<ul style="list-style-type: none"> • "ruleId": ["value", "value", ...] Specify the rule IDs.
	Quarantine Type	quarantineType=<value> The valid value is <i>pvo</i> .
Request Body	<pre>{ "quarantineType": "pvo", "ruleId": ["value"] }</pre>	
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
  }
}
```

```
}  
}
```



CHAPTER 3

APIs for Web

- [Reporting APIs, on page 87](#)
- [Tracking APIs, on page 96](#)

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	<code>GET /api/v2.0/reporting/report?resource_attribute</code> <code>GET /api/v2.0/reporting/report/counter?resource_attribute</code>
-----------------	--

Supported Resource Attributes	Duration	<p>This is a required parameter. All API queries should be accompanied with this parameter.</p> <pre>startDate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</pre> <p>Aggregate report(s) for the specified duration.</p>
	Query Type	<ul style="list-style-type: none"> • <code>query_type=graph</code> Receive data that can be represented as graphs. • <code>query_type=export</code> Receive data in the export format.
	Sorting	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> • <code>orderBy=<value></code> Specify the attribute by which to order the data in the response. For example, <pre>orderBy=total_clean_recipients</pre> • <code>orderDir=<value></code> Specify sort direction. The valid options are: <ul style="list-style-type: none"> • <code>asc</code> Order the results in ascending order. • <code>desc</code> Order the results in descending order.
	Lazy Loading	<p>You should use both these parameters. If you use either, you will not receive data in the response.</p> <ul style="list-style-type: none"> • <code>offset=<value></code> 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. • <code>limit=<value></code> Specify the number of records to retrieve.
	Data Retrieval Option	<ul style="list-style-type: none"> • <code>top=<value></code> Specify the number of records with the highest values to return.
Filtering		

		<p>Filter parameters restrict the data to be included the response.</p> <ul style="list-style-type: none"> • <code>filterValue=<value></code> The value to search for. • <code>filterBy=<value></code> Filter the data to be retrieved according to the filter property and value. • <code>filterOperator=<value></code> The valid options are: <ul style="list-style-type: none"> • <code>begins_with</code> Filter the response data based on the value specified. This is not an exact value. • <code>is</code> Filter the response data based on the exact value specified.
	Device	<ul style="list-style-type: none"> • <code>device_type=wsa</code> Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter. • <code>device_name=<value></code> 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 89](#)
- [Retrieving Multiple Values for a Counter, on page 90](#)
- [Retrieving Single Values for Each Counter in a Counter Group, on page 91](#)
- [Retrieving Multiple Values for Multiple Counters, on page 92](#)
- [Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter, on page 94](#)

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

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 96](#)
- [Layer 4 Traffic Monitor, on page 99](#)
- [SOCKS Proxy, on page 101](#)

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
cbal2403f2eb11c4884b27862dd31a779133c03a0e61d334d",
        "applicationType": "-",
        "timestamp": 1540275265,
        "transactionStatus": "BLOCK",
        "ampVerdict": "-"
    }
},
{
    "attributes": {
        "webCategory": "Business and Industry",
        "contentType": "-",
        "pageResources":
"http://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, on page 103](#)
- [Querying for Managed Email Security Appliances' Information, on page 104](#)
- [Querying for the Details of Centralized Services, on page 104](#)
- [Querying for Reporting Groups' Information, on page 105](#)
- [Retrieving APIs Accessible to a User Role, on page 106](#)

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 YWRtaW46Q21zY28xMjMk
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 YWRtaW46SXXJvbnBvcnQxMjMk
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"
          ]
        }
      },
      {
        "Empty_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"
  ]
}
```




CHAPTER 5

Troubleshooting AsyncOS API

This chapter contains the following sections:

- [API Logs, on page 109](#)
- [Alerts, on page 109](#)

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

