AsyncOS 15.5.1 API for Cisco Secure Email Gateway - Getting Started Guide - GD (General Deployment)

First Published: 2024-04-30

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 NONINFRINGEMENT 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)

© 2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Overview of AsyncOS API for Cisco Secure Email Gateway** 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 5

AsyncOS API Requests and Responses 5

AsyncOS API Requests 5

AsyncOS API Responses 6

Key Components of Responses 6

HTTP Response Codes 7

AsyncOS APIs - Rate Limits 8

AsyncOS API Capabilities 8

CHAPTER 2 **APIs for Secure 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

Retrieving Top Incoming Messages that Matched a Configured Mail Policy 18

Retrieving Top Outgoing Messages that Matched a Configured Mail Policy 19

Retrieving All Incoming Messages that Matched a Configured Mail Policy 20
Retrieving All Outgoing Messages that Matched a Configured Mail Policy 21
Tracking APIs 22
Searching for Messages 22
Rejected Connections 27
Message Details 29
DLP Details 31
AMP Details 33
URL Details 35
Connection Details 37
Remediation Details 39
Retrieving All Incoming Messages that Matched a Configured Mail Policy 40
Retrieving All Outgoing Messages that Matched a Configured Mail Policy 43
Quarantine 46
APIs for Spam Quarantine 46
Searching for Messages 46
Retrieving Message Details 49
Deleting Messages 51
Releasing Messages 52
Searching for Safelist and Blocklist Entries 53
Adding, Editing, and Appending Safelist and Blocklist Entries 56
Deleting Safelist or Blocklist Entries 69
APIs for Other Quarantine 73
Searching for Messages 73
Retrieving Message Details 80
Move Messages 82
Delaying the Exit of a Message from a Quarantine 83
Sending a Copy of a Message in Quarantine 85
Downloading an Attachment 87
Deleting Messages 88
Releasing Messages 89
Viewing the Rule Summary 91
Searching Based on Rule ID 92
Releasing Messages from the Rule Summary 95

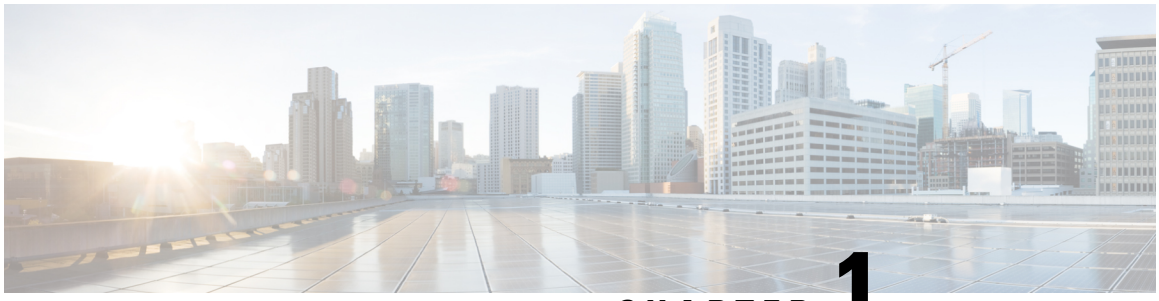
Deleting Messages from the Rule Summary 96
Configuration APIs 98
Cluster Levels for API Calls - Examples 99
Authentication APIs 100
Client Credentials APIs 100
Generating JWT Token 105
URL Lists APIs 108
Retrieving a List of All URL Lists 108
Retrieving Details for a Specified URL List 110
Adding URL Lists 112
Editing URL Lists 113
Deleting URL Lists 115
Dictionary APIs 117
Retrieving List of All Configured Dictionaries 117
Retrieving Information of Specific Configured Dictionary 119
Adding a New Dictionary 121
Editing an Existing Dictionary 123
Deleting an Existing Dictionary 125
Retrieving List of Words from Specific Dictionary 127
Adding Words to Specific Dictionary 128
Modifying Words in Specific Dictionary 130
Deleting Existing Words from Specific Dictionary 132
HAT APIs 133
Retrieving Configuration Details of All Sender Groups in Listener 134
Retrieving Configuration Details for Specific Sender Group 138
Creating Sender Group with Specific Configuration 140
Editing Existing Configuration Details of Specific Sender Group 143
Deleting Specific Sender Group 147
Retrieving Information of All Senders of Specific Sender Group 149
Adding Senders to Existing Sender Group 150
Deleting Specific Senders from Sender Group 153
Updating Order of Sender Groups for Listener 155
Finding Senders in Sender Groups 156
File Hash Lists APIs 159

Retrieving Contents of All File Hash Lists 159
Retrieving Contents of Specific File Hash List 161
Adding File Hash List 163
Adding File Hashes to Specific File Hash List 165
Editing File Hash List 166
RAT APIs 168
Retrieving All Entries for Recipient Access Table 168
Adding New Entry in Recipient Access Table 172
Updating Specific Entry in Recipient Access Table 176
Deleting Specific Entry in Recipient Access Table 178
SMTP Routes APIs 180
Retrieving All SMTP Routes Entries 180
Adding a New SMTP Route Entry 182
Updating a Specific SMTP Routes Entry 186
Deleting a SMTP Route Entry 190
Save and Load Configuration APIs 192
Retrieving Existing Configuration 193
Saving Configuration on Email Gateway 195
Retrieving Configuration by Email 197
Loading Configuration Through Request Body 199
Loading Configuration Using an XML File on the Email Gateway 201
Loading Partial Configuration 203
Address Lists APIs 206
Retrieving All Entries of All Address Lists 206
Retrieving All Entries of Specific Address List 209
Adding New Address List 211
Updating Address List 213
Deleting Address List 215
Incoming Mail Policy Users APIs 216
Retrieving User Entries of an Incoming Mail Policy 216
Adding User Entries to an Incoming Mail Policy 218
Updating User Entries in an Incoming Mail Policy 222
Configuration APIs - Rate Limits 226
Logging APIs 228

Retrieving Log Subscription Details from Email Gateway 228
Retrieving All Log Files for Specific Log Subscription 230
Retrieving Log Files using URL 231

CHAPTER 3 General Purpose APIs 233
Querying for the System Time 233
Retrieving APIs Accessible to a User Role 234
Health API 234
Delivery Status API 235
System Status API 236

CHAPTER 4 Troubleshooting AsyncOS API 241
API Logs 241
Alerts 241
Handling Error Messages of Configuration APIs 241



CHAPTER 1

Overview of AsyncOS API for Cisco Secure Email Gateway

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

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

This chapter contains the following sections:

- Prerequisites for Using AsyncOS API, 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
- AsyncOS APIs - Rate Limits, on page 8
- AsyncOS API Capabilities, on page 8

Prerequisites for Using AsyncOS API

To use AsyncOS API, you need the knowledge of:

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

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

Enabling AsyncOS API

Before You Begin

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

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

Step 1 Log in to the web interface.

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

Step 3 Edit the Management interface.

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

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

Note AsyncOS API communicates using HTTP / 1.1.

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

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

Step 5 Submit and commit your changes.

Securely Communicating with AsyncOS API

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

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

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

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

Step 3 Submit and commit your changes.

AsyncOS API Authentication and Authorization

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

- Authentication, on page 3
- Authorization, on page 5
- Retrieving APIs Accessible to a User Role, on page 234

Authentication

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

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

Authenticating API Queries with JSON Web Token

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

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

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

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

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

Sample Request

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

Sample Response

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

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

```
    }
}
```

Authorization

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

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

Note

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

AsyncOS API Requests and Responses

- AsyncOS API Requests, on page 5
- AsyncOS API Responses, on page 6

AsyncOS API Requests

Requests made to the API have the following characteristics:

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

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

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

  where:

  - `{appliance}:{port}`

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

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

- `{resource_attributes}`

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

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

```
application/json
```

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

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

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

AsyncOS API Responses

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

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

Key Components of Responses

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

Components	Values	Description

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

HTTP Response Codes

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

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

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

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

- RFC1945
- RFC7231

AsyncOS APIs - Rate Limits

The maximum number of concurrent API requests allowed is 45. However, the effective number of requests that can be processed simultaneously (perceived limit) varies depending on the memory consumed by the API requests being processed and the API response time.

For example, if you initiate 45 API requests concurrently and assume that after 20 seconds, 11 of those requests have been successfully processed and completed. Since 11 requests are complete, you can initiate 11 more requests.

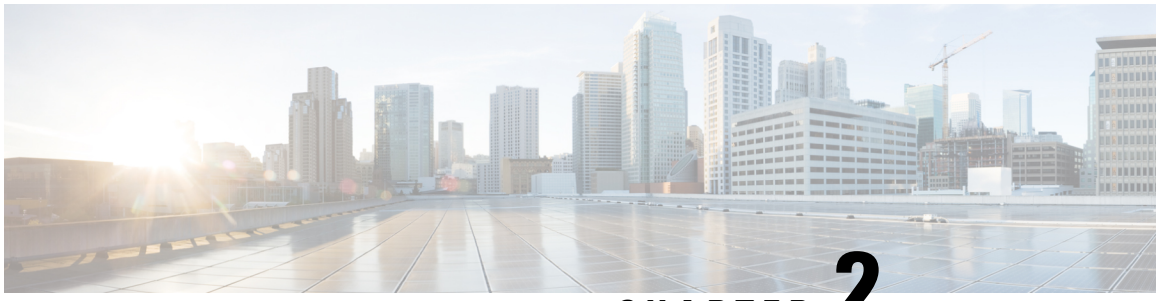
If you exceed this limit, you will receive the `502: Bad Gateway` error response code if the Trailblazer port is used. In case the request is sent directly to the API server port, then the connection is rejected without any response code.

Note The `502: Bad Gateway` error response code will be modified in the upcoming releases.

AsyncOS API Capabilities

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

- APIs for Secure Email, on page 9
- General Purpose APIs, on page 233



CHAPTER 2

APIs for Secure Email

- Reporting APIs, on page 9
- Tracking APIs, on page 22
- Quarantine, on page 46
- Configuration APIs, on page 98
- Logging APIs, on page 228

Reporting APIs

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

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

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

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

Examples

Examples for the types of reporting queries are shown below:

- Retrieving a Single Value for a Counter, on page 12
- Retrieving Multiple Values for a Counter, on page 12
- Retrieving Single Values for Each Counter in a Counter Group, on page 13
- Retrieving Multiple Values for Multiple Counters, on page 14
- Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter, on page 16
- Retrieving Top Incoming Messages that Matched a Configured Mail Policy, on page 18
- Retrieving Top Outgoing Messages that Matched a Configured Mail Policy, on page 19

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

Retrieving a Single Value for a Counter

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

Sample Request

```
GET /sma/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: 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 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 /sma/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: 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 17:39:34 GMT
Content-type: application/json
Content-Length: 580
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

Retrieving Single Values for Each Counter in a Counter Group

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

Sample Request

```
GET /sma/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: 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 18:17:29 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 /sma/api/v2.0/reporting/mail_incoming_domain_detail?startDate=2017-09-10T19:00:00.000Z
&endDate=2018-09-24T23:00:00.000Z&device_type=esa&offset=1&limit=2
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

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

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

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


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

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

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

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

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

Sample Request

```
GET /sma/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: 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 18:49:42 GMT
Content-type: application/json
Content-Length: 74110
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

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

```
                ...

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

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

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

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

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

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

                ...

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

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

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

Retrieving Top Incoming Messages that Matched a Configured Mail Policy

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

Sample Request

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

Sample Response

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

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


Retrieving Top Outgoing Messages that Matched a Configured Mail Policy

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

Sample Request

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

Sample Response

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

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


Retrieving All Incoming Messages that Matched a Configured Mail Policy

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

Sample Request

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

Sample Response

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 547
Content-Type: application/json; charset=UTF-8
{
    "meta": {
        "totalCount": -1
    },
    "data": {
        "type": "recipients_matched",
        "resultSet": {
            "recipients_matched": [
                {
                    "Bypass_Blocklist_Policy": 318172
                },
                {
                    "Test Mail Policy Marketing2Junk": 177994
```

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


Retrieving All Outgoing Messages that Matched a Configured Mail Policy

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

Sample Request

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

Sample Response

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

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

Tracking APIs

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

- Searching for Messages, on page 22
- Rejected Connections, on page 27
- Message Details, on page 29
- DLP Details, on page 31
- AMP Details, on page 33
- URL Details, on page 35
- Connection Details, on page 37
- Remediation Details, on page 39
- Retrieving All Incoming Messages that Matched a Configured Mail Policy, on page 40
- Retrieving All Outgoing Messages that Matched a Configured Mail Policy, on page 43

Searching for Messages

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

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

Example

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

Sample Request

```
GET /sma/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: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

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

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

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

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

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

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


Rejected Connections

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

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

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

Example

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

Sample Request

```
GET /sma/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: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

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

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

Message Details

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

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

Example

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

Sample Request

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

Sample Response

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

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

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

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


DLP Details

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

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

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

Example

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

Sample Request

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

Sample Response

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

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


AMP Details

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

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

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

Example

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

Sample Request

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

Sample Response

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

{
```

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


URL Details

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

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

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

Example

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

Sample Request

```
GET /sma/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: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

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

{
```

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

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

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

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


Connection Details

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

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

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

Example

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

Sample Request

```
GET /sma/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: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

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

{
```

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

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

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


Remediation Details

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

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

Sample Request

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

Sample Response

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

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

Retrieving All Incoming Messages that Matched a Configured Mail Policy

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

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

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

Sample Request

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

Sample Response

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

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

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

        ]
}
```


Retrieving All Outgoing Messages that Matched a Configured Mail Policy

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

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

Sample Request

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

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

Sample Response

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

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

```
            "morDetails": {},
            "replyTo": "N/A",
            "timestamp": "02 Mar 2021 13:14:36 (GMT +05:30)",
            "messageID": {
                "2325166": "<19831342576104719839152803255 6096@makug.fiendofwine.us>"
            },
            "verdictChart": {
                "2325166": "16141113"
            },
            "recipient": [
                "testuser2@abc.com"
            ],
            "sender": "user@testdomain.com",
            "serialNumber": "421558305417729252 66-ABFF53B45FDE",
            "allIcid": [
                516847
            ],
            "sbrs": "None"
        }
    },
    {
        "attributes": {
            "hostName": "",
            "mid": [
                2325164
            ],
            "isCompleteData": "N/A",
            "messageStatus": {
                "2325164": "Dropped By Anti-Virus"
            },
            "recipientMap": {
                "2325164": [
                    "testuser1@abc.com"
                ]
            },
            "senderIp": "10.10.4.46",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderGroup": "None",
            "subject": "Shipping confirmation: PIR-54787L-83296",
            "friendly_from": [
                "payment@geiger-sicher.de"
            ],
            "senderDomain": "testdomain.com",
            "direction": "outgoing",
            "icid": 516847,
            "morDetails": {},
            "replyTo": "N/A",
            "timestamp": "02 Mar 2021 13:14:34 (GMT +05:30)",
            "messageID": {
                "2325164": "<9o6bdsq4jgrk@geiger-sicher.de>"
            },
            "verdictChart": {
                "2325164": "11500000"
            },
            "recipient": [
                "testuser1@abc.com"
            ],
            "sender": "user@testdomain.com",
            "serialNumber": "421558305416728252 66-ABFF53B45FDE",
            "allIcid": [
                516847
            ],
```

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

Quarantine

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

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

APIs for Spam Quarantine

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

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

Searching for Messages

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

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

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

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

Example

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

Sample Request

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

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

Sample Response

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

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

Retrieving Message Details

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

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

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

Example

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

Sample Request

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

Sample Response

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

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

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

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

Deleting Messages

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

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

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

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

Example

This example shows a query to delete messages.

Sample Request

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

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

Sample Response

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

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

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

Releasing Messages

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

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

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

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

Example

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

Sample Request

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

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

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

Sample Response

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

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

Searching for Safelist and Blocklist Entries

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

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

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

Examples

Viewing Safelist and Blocklist entries by recipient:

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

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

Sample Request

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

Sample Response

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

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

Viewing Safelist and Blocklist entries by sender:

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

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

Sample Request

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

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

Sample Response

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

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

Adding, Editing, and Appending Safelist and Blocklist Entries

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

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

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

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

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

Examples

- Adding Recipient Safelist Entries, on page 59
- Adding Sender Safelist Entries, on page 60
- Adding Recipient Blocklist Entries, on page 61
- Adding Sender Blocklist Entries, on page 61
- Editing Recipient Safelist Entries, on page 62
- Editing Sender Safelist Entries, on page 63
- Editing Recipient Blocklist Entries, on page 64
- Editing Sender Blocklist Entries, on page 65
- Appending Recipient Safelist Entries, on page 65
- Appending Sender Safelist Entries, on page 66

Adding Recipient Safelist Entries

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

Sample Request

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

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

Sample Response

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

{
    "data": {
```

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

Adding Sender Safelist Entries

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

Sample Request

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

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

Sample Response

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

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

Adding Recipient Blocklist Entries

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

Sample Request

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

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

Sample Response

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

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

Adding Sender Blocklist Entries

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

Sample Request

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

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

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

Sample Response

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

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

Editing Recipient Safelist Entries

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

Sample Request

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

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

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

Sample Response

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

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

Editing Sender Safelist Entries

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

Sample Request

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

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

Sample Response

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

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

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

Editing Recipient Blocklist Entries

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

Sample Request

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

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

Sample Response

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

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

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

Editing Sender Blocklist Entries

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

Sample Request

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

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

Sample Response

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

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

Appending Recipient Safelist Entries

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

Sample Request

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

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

Sample Response

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

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

Appending Sender Safelist Entries

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

Sample Request

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

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

Sample Response

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

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

Appending a Recipient Blocklist Entry

This sample request shows a query to append blocklist entries.

Sample Request

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

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

Sample Response

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

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

Appending Sender Blocklist Entries

This sample request shows a query to append blocklist entries.

Sample Request

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

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

Sample Response

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

{
```

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

Deleting Safelist or Blocklist Entries

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

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

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

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

The following APIs are available:

- Deleting Recipient Safelist Entries, on page 70

• Deleting Sender Safelist Entries, on page 70
• Deleting Recipient Blocklist Entries, on page 71
• Deleting Sender Blocklist Entries, on page 72

Deleting Recipient Safelist Entries

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

Sample Request

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

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

Sample Response

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

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

Deleting Sender Safelist Entries

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

Sample Request

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

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

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

Sample Response

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

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

Deleting Recipient Blocklist Entries

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

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

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

Sample Response

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

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

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

Deleting Sender Blocklist Entries

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

Sample Request

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

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

Sample Response

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

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

```
    }
}
```

APIs for Other Quarantine

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

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

- Searching for Messages, on page 73
- Retrieving Message Details, on page 80
- Move Messages, on page 82
- Delaying the Exit of a Message from a Quarantine , on page 83
- Sending a Copy of a Message in Quarantine, on page 85
- Downloading an Attachment, on page 87
- Deleting Messages, on page 88
- Releasing Messages, on page 89
- Viewing the Rule Summary, on page 91
- Searching Based on Rule ID, on page 92
- Releasing Messages from the Rule Summary, on page 95
- Deleting Messages from the Rule Summary, on page 96

Searching for Messages

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

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

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

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

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

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

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

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

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

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

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

	Envelope Sender	

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

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

Example

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

Sample Request

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

Sample Response

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

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

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

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

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


Retrieving Message Details

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

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

Example

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

Sample Request

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

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

Sample Response

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

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

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

Move Messages

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

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

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

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

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

Example

This example shows a query to move a message.

Sample Request

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

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

Sample Response

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

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

Delaying the Exit of a Message from a Quarantine

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

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

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

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

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

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

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

Example

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

Sample Request

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

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

Sample Response

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

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

Sending a Copy of a Message in Quarantine

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

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

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

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

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

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

Example

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

Sample Request

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


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

Sample Response

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

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

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

Downloading an Attachment

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

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

Example

This example shows a query to download an attachment.

Sample Request

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

Sample Response

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

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

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

Deleting Messages

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

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

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

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

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

Example

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

Sample Request

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

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

Sample Response

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

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

Releasing Messages

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

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

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

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

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

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

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

Example

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

Sample Request

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

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

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

Sample Response

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

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

Viewing the Rule Summary

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

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

Example

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

Sample Request

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

Sample Response

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

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

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

Searching Based on Rule ID

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

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

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

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

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

Example

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

Sample Request

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

Sample Response

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

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

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


Releasing Messages from the Rule Summary

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

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

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

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

Example

This example shows a query to release message.

Sample Request

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


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

Sample Response

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


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

Deleting Messages from the Rule Summary

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

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

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

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

Example

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

Sample Request

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


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

Sample Response

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

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

```
        }
}
```

Configuration APIs

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

- Authentication APIs, on page 100
- URL Lists APIs, on page 108
- Dictionary APIs, on page 117
- HAT APIs, on page 133
- File Hash Lists APIs, on page 159
- SMTP Routes APIs, on page 180
- RAT APIs, on page 168
- Save and Load Configuration APIs, on page 192
- Address Lists APIs, on page 206
- Incoming Mail Policy Users APIs, on page 216

Note The Save and Load Configuration API is not available in Cisco Cloud Email Security.

Note For all Configuration APIs except Save and Load Configuration API , only the administrator and cloud administrator user roles are supported.

Note For Configuration APIs:

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

General Information

The following information is applicable to all Configuration APIs:

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

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

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

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

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

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

For information on Configuration APIs Rate Limits, see Configuration APIs - Rate Limits , on page 226.

For information on how to troubleshoot Configuration APIs, see section Handling Error Messages of Configuration APIs, on page 241.

Cluster Levels for API Calls - Examples

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

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

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

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

Sample Requests

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

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

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

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

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

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

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

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

Authentication APIs

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

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

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

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

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

Perform the following steps to generate JWT:

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

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

The token generated can be used to authenticate configuration APIs.

Note You can provide basic authentication also to authenticate APIs.

Client Credentials APIs

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

The various API categories for Client Credentials are:

- Retrieving Client Credentials, on page 101

• Generating Client Credentials, on page 102
• Refreshing Client Secret, on page 103
• Deleting Client Credentials, on page 104

Retrieving Client Credentials

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

Synopsis		[Standalone Machine] `GET /esa/api/v2.0/config/client_creds?device_type=esa` [Cluster Machine] `GET /esa/api/v2.0/config/client_creds?device_type=esa`
Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve Client Credentials :

Sample Request

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

Sample Response

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

{
```

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

Generating Client Credentials

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

Synopsis		[Standalone Machine] `POST /esa/api/v2.0/config/client_creds?device_type=esa` [Cluster Machine] `POST /esa/api/v2.0/config/client_creds?device_type=esa`
Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to generate Client Credentials:

Sample Request

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

Sample Response

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

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

Refreshing Client Secret

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

Synopsis		[Standalone Machine] `PUT /esa/api/v2.0/config/client_creds/refresh_client_secret?device_type=esa` [Cluster Machine] `PUT /esa/api/v2.0/config/client_creds/refresh_client_secret?device_type=esa`
Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to refresh the Client Secret :

Sample Request

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

Sample Response

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

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

Deleting Client Credentials

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

Synopsis		[Standalone Machine] `DELETE /esa/api/v2.0/config/client_creds?device_type=esa` [Cluster Machine] `DELETE /esa/api/v2.0/config/client_creds?device_type=esa`
Supported Resource Attributes	Device Type	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization, Content-Type
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to delete Client Credentials:

Sample Request

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

Sample Response

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

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

Generating JWT Token

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

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

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

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

Example

This example shows a query to generate JWT token:

Sample Request

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

```
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
 {
    "data": {
        "username": "test_cloud_admin",
        "client_id": "871b3f8d-b2a6-5238-a92b-0c50c82cae78",
       "client_secret": "273a54f51b92ec3cb95d54731442d740e8ef2c84dc834a4dd7d5c33e585dbdf2"

    }
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:23:31 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 627
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY

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

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

Using token to authenticate APIs

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

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 06:25:00 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 139
Connection: keep-alive
Cache-control: no-store
```

```
Pragma: no-cache
jwtToken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNjY5...
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY
{
    "data": [
        {
            "used_by": "",
            "urls_count": 1,
            "name": "URL1",
            "urls": [
                "aaaaa"
                ]
        },
        {
            "used_by": "",
            "urls_count": 1,
            "name": "url1",
            "urls": [
                "aa"
                ]
        },
        {
            "used_by": "",
            "urls_count": 2,
            "name": "MyURL",
            "urls": [
                "ck.dajk.casnca",
                "acsac.acaca.caaca"
                ]
        }
    ]
}
```

Using Basic Authentication to Authenticate API

You can also use basic authentication to authenticate other APIs.

Example

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

Sample Request

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

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

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:16:18 GMT
Content-Type: application/json; charset=UTF-8
```

```
Content-Length: 139
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY
{
    "data": [
        {
            "used_by": "",
            "urls_count": 1,
            "name": "URL1",
            "urls": [
                "aaaaa"
                ]
        },
        {
            "used_by": "",
            "urls_count": 1,
            "name": "url1",
            "urls": [
            "aa"
                ]
        },
        {
            "used_by": "",
            "urls_count": 2,
            "name": "MyURL",
            "urls": [
            "ck.dajk.casnca",
            "acsac.acaca.caaca"
                ]
        }
    ]
}
```

URL Lists APIs

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

- Retrieving a List of All URL Lists, on page 108
- Retrieving Details for a Specified URL List, on page 110
- Adding URL Lists, on page 112
- Editing URL Lists, on page 113
- Deleting URL Lists, on page 115

Retrieving a List of All URL Lists

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:16:18 GMT
```

```
Content-Type: application/json; charset=UTF-8
Content-Length: 139
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY
{
    "data": [
        {
            "used_by": "",
            "urls_count": 1,
            "name": "URL1",
            "urls": [
                "aaaaa"
            ]
        },
        {
            "used_by": "",
            "urls_count": 1,
            "name": "url1",
            "urls": [
                "aa"
            ]
        },
        {
            "used_by": "",
            "urls_count": 2,
            "name": "MyURL",
            "urls": [
                "ck.dajk.casnca",
                "acsac.acaca.caaca"
            ]
        }
    ]
}
```

Retrieving Details for a Specified URL List

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 21 Nov 2022 09:08:46 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 63
Connection: keep-alive
Cache-control: no-store
Pragma: no-cache
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
```

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Expose-Headers: Content-Disposition, jwtToken
X-Frame-Options: DENY
{
    "data": {
        "used_by": "",
        "urls_count": 2,
        "name": "MyURL",
        "urls": [
            "ck.dajk.casnca",
            "acsac.acaca.caaca"
        ]
    }
}
```

Adding URL Lists

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

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

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

Key in Request Body	urls	This is a required parameter. Specify the list of URLs to add to the URL list.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to add a URL list:

Sample Request

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

Sample Response

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

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

Editing URL Lists

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to edit a URL list:

Sample Request

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

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

Sample Response

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

Deleting URL Lists

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

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

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

Dictionary APIs

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

- Retrieving List of All Configured Dictionaries, on page 117
- Retrieving Information of Specific Configured Dictionary, on page 119
- Adding a New Dictionary, on page 121
- Editing an Existing Dictionary, on page 123
- Deleting an Existing Dictionary, on page 125
- Retrieving List of Words from Specific Dictionary, on page 127
- Adding Words to Specific Dictionary , on page 128
- Modifying Words in Specific Dictionary , on page 130
- Deleting Existing Words from Specific Dictionary, on page 132

Retrieving List of All Configured Dictionaries

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

Sample Response

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

```
            "ignorecase": 1,
            "words": [
                [
                    "Helo, gelo, melo",
                    1
                ],
                [
                    "kelo, &&d23",
                    5
                ]
            ],
            "words_count": {
                "term_count": 2,
                "smart_identifier_count": 0
            },
            "wholewords": 1
        },
        {
            "name": "New-Dict",
            "encoding": "utf-8",
            "ignorecase": 0,
            "words": [
                [
                    "*credit",
                    2,
                    "prefix"
                ],
                [
                    "*aba",
                    1,
                    ""
                ],
                [
                    "À term 1",
                    1
                ],
                [
                    "\\tjsu",
                    1
                ]
            ],
            "words_count": {
                "term_count": 2,
                "smart_identifier_count": 2
            },
            "wholewords": 1
        }
    ]
}
```


Retrieving Information of Specific Configured Dictionary

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
        "name": "MyDict",
        "encoding": "utf-8",
        "ignorecase": 1,
        "words": [
```

```
                [
                    "Helo, gelo, melo",
                    1
                ],
                [
                    "kelo, &&d23",
                    5
                ]
            ],
            "words_count": {
                "term_count": 2,
                "smart_identifier_count": 0
            },
            "wholewords": 1
        }
}
```

Adding a New Dictionary

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

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
```

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

Editing an Existing Dictionary

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

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

Sample Response

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

Deleting an Existing Dictionary

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

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

}
```

Retrieving List of Words from Specific Dictionary

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

```
GET /esa/api/v2.0/config/dictionaries/NewDict/words?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
```

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

Sample Response

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

Adding Words to Specific Dictionary

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

Sample Response

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

Modifying Words in Specific Dictionary

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

Sample Response

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

Deleting Existing Words from Specific Dictionary

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

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

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

HAT APIs

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

- Retrieving Configuration Details of All Sender Groups in Listener , on page 134
- Retrieving Configuration Details for Specific Sender Group, on page 138
- Creating Sender Group with Specific Configuration, on page 140
- Editing Existing Configuration Details of Specific Sender Group, on page 143

• Deleting Specific Sender Group, on page 147
• Retrieving Information of All Senders of Specific Sender Group, on page 149
• Adding Senders to Existing Sender Group, on page 150
• Deleting Specific Senders from Sender Group , on page 153
• Updating Order of Sender Groups for Listener, on page 155
• Finding Senders in Sender Groups, on page 156

Retrieving Configuration Details of All Sender Groups in Listener

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
        "listener_config": {
            "listener_ip": "10.10.60.230:25"
        },
        "sender_groups": [
            {
                "dns_list": [],
                "external_threat_feeds": [],
                "description": "Everyone else",
                "flow_profile": "ACCEPTED",
                "senders": {
                    "ip_address_list": [
                        {
                            "sender_name": "example_none_d.com",
                            "description": "Cisco"
                        }
                    ],
                    "geo_list": [
                        {
                            "sender_name": "American Samoa",
                            "description": "Country"
                        },
                        {
                            "sender_name": "India",
                            "description": "Country"
                        },
                        {
                            "sender_name": "Algeria",
                            "description": "Country"
                        }
                    ]
                },
                "sbrs": [],
                "dns_host_verification": {
                    "lookup_not_matched": "false",
                    "record_not_exist": "false",
                    "lookup_fail": "false"
                },
                "order": 6,
                "sbrs_none": "false",
```

```
        "name": "ALL"
    },
    {
        "dns_list": [],
        "external_threat_feeds": [],
        "description": "",
        "flow_profile": "TRUSTED",
        "senders": {
            "ip_address_list": [
                {
                    "sender_name": ".cisco.com",
                    "description": "Cisco"
                }
            ],
            "geo_list": [
                {
                    "sender_name": "Algeria",
                    "description": "Country"
                }
            ]
        },
        "sbrs": [],
        "dns_host_verification": {
            "lookup_not_matched": "false",
            "record_not_exist": "false",
            "lookup_fail": "true"
        },
        "order": 5,
        "sbrs_none": "false",
        "name": "my_sender_group"
    },
    {
        "dns_list": [],
        "external_threat_feeds": [],
        "description": "Suspicious senders are throttled",
        "flow_profile": "THROTTLED",
        "senders": {
            "ip_address_list": [
                {
                    "sender_name": ".cisco.com",
                    "description": "Cisco"
                }
            ],
            "geo_list": [
                {
                    "sender_name": "Denmark",
                    "description": "aa"
                },
                {
                    "sender_name": "India",
                    "description": "Country"
                }
            ]
        },
        "sbrs": [
            -3.0,
            -1.0
        ],
        "dns_host_verification": {
            "lookup_not_matched": "false",
            "record_not_exist": "false",
            "lookup_fail": "false"
        },
        "order": 3,
```

```
                "sbrs_none": "false",
                "name": "SUSPECTLIST"
            },
            {
                "dns_list": [],
                "external_threat_feeds": [],
                "description": "Spammers are rejected",
                "flow_profile": "BLOCKED",
                "senders": {
                    "geo_list": [
                        {
                            "sender_name": "Austria",
                            "description": "Country"
                        }
                    ]
                },
                "sbrs": [
                    -10.0,
                    -3.0
                ],
                "dns_host_verification": {
                    "lookup_not_matched": "false",
                    "record_not_exist": "false",
                    "lookup_fail": "false"
                },
                "order": 2,
                "sbrs_none": "false",
                "name": "BLOCKED_LIST"
            },
            {
                "dns_list": [],
                "external_threat_feeds": [],
                "description": "Reviewed but undecided, continue normal acceptance",
                "flow_profile": "ACCEPTED",
                "senders": {
                    "geo_list": [
                        {
                            "sender_name": "India",
                            "description": "Country"
                        }
                    ]
                },
                "sbrs": [
                    -1.0,
                    10.0
                ],
                "dns_host_verification": {
                    "lookup_not_matched": "false",
                    "record_not_exist": "false",
                    "lookup_fail": "false"
                },
                "order": 4,
                "sbrs_none": "true",
                "name": "UNKNOWNLIST"
            },
            {
                "dns_list": [],
                "external_threat_feeds": [],
                "description": "My trusted senders have no anti-spam scanning or rate
limiting",
                "flow_profile": "TRUSTED",
                "senders": {},
                "sbrs": [],
                "dns_host_verification": {
```

```
                    "lookup_not_matched": "false",
                    "record_not_exist": "false",
                    "lookup_fail": "false"
                },
                "order": 1,
                "sbrs_none": "false",
                "name": "ALLOWED_LIST"
            }
        ]
    }
}
```

Retrieving Configuration Details for Specific Sender Group

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
        "dns_list": [],
        "external_threat_feeds": [],
        "description": "Everyone else",
        "flow_profile": "ACCEPTED",
        "senders": {
            "ip_address_list": [
                {
                    "sender_name": "example_none_d.com",
                    "description": "Cisco"
                }
            ],
            "geo_list": [
                {
                    "sender_name": "American Samoa",
                    "description": "Country"
                },
                {
                    "sender_name": "India",
                    "description": "Country"
                },
                {
                    "sender_name": "Algeria",
                    "description": "Country"
                }
            ]
        },
        "sbrs": [],
        "dns_host_verification": {
            "lookup_not_matched": "false",
            "record_not_exist": "false",
            "lookup_fail": "false"
        },
        "order": 6,
        "sbrs_none": "false",
        "name": "ALL"
    }
}
```

Creating Sender Group with Specific Configuration

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

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

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

Sample Response

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

Editing Existing Configuration Details of Specific Sender Group

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

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

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

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

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

Sample Response

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

Deleting Specific Sender Group

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

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

Retrieving Information of All Senders of Specific Sender Group

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

Sample Response

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

Adding Senders to Existing Sender Group

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

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

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

Sample Response

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

Deleting Specific Senders from Sender Group

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

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

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

Updating Order of Sender Groups for Listener

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

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

Finding Senders in Sender Groups

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

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

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

Related Topics

- Searching for Senders in All Sender Groups across All Configured Listeners, on page 156
- Searching for Senders in Specific Sender Group for Specific Listener, on page 158

Searching for Senders in All Sender Groups across All Configured Listeners

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
```

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

Searching for Senders in Specific Sender Group for Specific Listener

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

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

Sample Response

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

File Hash Lists APIs

You can retrieve information about file hash lists from your email gateway. The various API categories for file hash lists are:

- Retrieving Contents of All File Hash Lists, on page 159
- Retrieving Contents of Specific File Hash List, on page 161
- Adding File Hash List, on page 163
- Adding File Hashes to Specific File Hash List, on page 165
- Editing File Hash List, on page 166

Retrieving Contents of All File Hash Lists

You can retrieve contents of all file hash lists configured in your email gateway with different attributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve contents of all file hash lists configured in your email gateway:

Sample Request

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

HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
```

```
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": [
        {
            "filehashes_count": 1,
            "filehashes": [
                "2286f6ffea7d0e58dcb3ecfd874041b1"
            ],
            "description": "Changed name",
            "list_type": "md5",
            "name": "fhl_api1"
        },
        {
            "filehashes_count": 2,
            "filehashes": [
                "2286f6ffea7d0e58dcb3ecfd874041b1",
                "25c1e46d60ff28f51bd0d8f80010ea87"
            ],
            "description": "MD5 Type FHL",
            "list_type": "md5",
            "name": "fhlist_md"
        },
        {
            "filehashes_count": 4,
            "filehashes": [
                "2286f6ffea7d0e58dcb3ecfd874041b1",
                "25c1e46d60ff28f51bd0d8f80010ea87",
                "631ef624f4506ea736b518aaf2a800ed7fbde138d6fe1c4b25a3ac8d29fa5026",
                "b2429e8450cebd27be58859c564e1cb7dda9517fecf6d14d4e3f43964bf8c4e1"
            ],
            "description": "All type FHL",
            "list_type": "any",
            "name": "fhlist_all"
        },
        {
            "name": "fhlist_sha",
            "used_by": [
                "Incoming Content Filters"
            ],
            "filehashes_count": 2,
            "filehashes": [
                "631ef624f4506ea736b518aaf2a800ed7fbde138d6fe1c4b25a3ac8d29fa5026",
                "b2429e8450cebd27be58859c564e1cb7dda9517fecf6d14d4e3f43964bf8c4e1"
            ],
            "list_type": "sha256",
            "description": "SHA256 Type FHL"
        }
    ]
}
```

Retrieving Contents of Specific File Hash List

You can retrieve contents of a specific file hash list configured in your email gateway with different attributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve contents of a specific file hash list configured in your email gateway:

Sample Request

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

Sample Response

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

```
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
        "name": "fhlist_sha",
        "used_by": [
            "Incoming Content Filters"
        ],
        "filehashes_count": 2,
        "filehashes": [
            "631ef624f4506ea736b518aaf2a800ed7fbde138d6fe1c4b25a3ac8d29fa5026",
            "b2429e8450cebd27be58859c564e1cb7dda9517fecf6d14d4e3f43964bf8c4e1"
        ],
        "list_type": "sha256",
        "description": "SHA256 type list"
    }
}
```

Adding File Hash List

You can add a file hash list in your email gateway with different attributes as explained below:

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

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

Response Headers		Content-Type, Content-Length, Connection
Keys in Request Body (See the Sample Request for the key hierarchy)	description	The key is an optional parameter. The key contains data that describes the file hash list.
	list_type	The key is a required parameter. The key contains the type of the file hash list. The key must not contain an empty value. The key can have the following values - “md5,” “sha256,” or “any.” **Note** The “any” type of file hash list can have both types of file hashes - “md5” and “sha256.”
	filehashes	The key is a required parameter. The key contains a list of file hashes.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to add a new file hash list in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/file_hash_lists/FHL1?device_type=esa

HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "description": "md5 list from api",
        "list_type": "md5",
        "filehashes": [
            "25c1e46d60ff58f51bd0d8f870010ea67"
        ]
    }
}
```

Sample Response

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

Adding File Hashes to Specific File Hash List

You can add file hashes to a specific file hash list configured in your email gateway with different attributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to add file hashes to a specific file hash list configured in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/file_hash_lists/FHL1/filehashes?device_type=esa

HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "filehashes": [
            "25c1e46d60ff28f51bd0d8f80010ea87",
            "2286f6ffea7d0e58dcb3ecfd874041b1"
        ]
    }
}
```

Sample Response

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

Editing File Hash List

You can edit the contents of an existing file hash list configured in your email gateway with different attributes as explained below:

Synopsis	[Standalone Machine]
	`PUT /esa/api/v2.0/config/file_hash_lists/<file_hash_list_name>?device_type=esa`
	[Clustered Machine]
	`PUT /esa/api/v2.0/config/file_hash_lists/<file_hash_list_name> ?device_type=esa&mode=cluster`
	Warning The **PUT** command replaces all contents of an existing file hash list entry.

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection
Keys in Request Body (Refer the Sample Request for the key hierarchy)	description	The key is an optional parameter. The key contains data that describes the file hash list.
	name	The key is an optional parameter. You can use this parameter to rename the existing file hash list. The value is the new name of the file hash list.
	filehashes	The key is a required parameter. The key contains a list of file hashes.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to edit the contents of an existing file hash list configured in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/file_hash_lists/FHL1?device_type=esa

HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

```
{
    "data": {
        "description": "Changed name",
        "name": "fhl_api3",
        "filehashes": [
            "2286f6ffea7d0e58dcb3ecfd874041b1"
        ]
    }
}
```

Sample Response

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

RAT APIs

You can retrieve Recipient Address Table (RAT) information from your email gateway. The various API categories for RAT are:

- Retrieving All Entries for Recipient Access Table, on page 168
- Adding New Entry in Recipient Access Table, on page 172
- Updating Specific Entry in Recipient Access Table, on page 176
- Deleting Specific Entry in Recipient Access Table, on page 178

Retrieving All Entries for Recipient Access Table

You can retrieve information of all entries of a specific Recipient Access Table (RAT) configured for a listener in your email gateway with different attributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve information of all entries of a specific Recipient Access Table (RAT) configured in your email gateway:

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 13 July 2023 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "meta": {
        "count": 12
    },
```

```
"data": [
    {
        "recipient_address": [
            "test11.com"
        ],
        "recipient_address_count": 1,
        "bypass_receiving_control": "True",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "False",
        "action": "ACCEPT",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 250
        },
        "order": 1
    },
    {
        "recipient_address": [
            "test10.com"
        ],
        "recipient_address_count": 1,
        "bypass_receiving_control": "False",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "False",
        "action": "REJECT",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 550
        },
        "order": 2
    },
    {
        "recipient_address": [
            "test9.com"
        ],
        "recipient_address_count": 1,
        "bypass_receiving_control": "True",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "False",
        "action": "ACCEPT",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 250
        },
        "order": 3
    },
    {
        "recipient_address": [
            "test8.com"
        ],
        "recipient_address_count": 1,
        "bypass_receiving_control": "True",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "False",
        "action": "ACCEPT",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 250
        },
        "order": 4
    },
    {
        "recipient_address": [
            "test7.com"
```

```
        ],
        "recipient_address_count": 1,
        "bypass_receiving_control": "False",
        "bypass_call_ahead": "True",
        "bypass_ldap_accept": "False",
        "action": "ACCEPT",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 250
        },
        "order": 5
    },
    {
        "recipient_address": [
            "test2.com"
        ],
        "recipient_address_count": 1,
        "bypass_receiving_control": "False",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "False",
        "action": "REJECT",
        "custom_smtp_response": {},
        "order": 6
    },
    {
        "recipient_address": [
            "test5.com",
            "test6.com"
        ],
        "recipient_address_count": 2,
        "bypass_receiving_control": "False",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "True",
        "action": "ACCEPT",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 250
        },
        "order": 7
    },
    {
        "recipient_address": [
            "test4.com",
            "test3.com"
        ],
        "recipient_address_count": 2,
        "bypass_receiving_control": "False",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "True",
        "action": "ACCEPT",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 250
        },
        "order": 8
    },
    {
        "recipient_address": [
            "test1.com"
        ],
        "recipient_address_count": 1,
        "bypass_receiving_control": "True",
        "bypass_call_ahead": "False",
        "bypass_ldap_accept": "False",
```

```
            "action": "REJECT",
            "custom_smtp_response": {},
            "order": 9
        },
        {
            "recipient_address": [
                "ALL"
            ],
            "recipient_address_count": 1,
            "bypass_receiving_control": "False",
            "bypass_call_ahead": "False",
            "bypass_ldap_accept": "False",
            "action": "ACCEPT",
            "custom_smtp_response": {},
            "order": 10
        }
    ]
}
```

Note The value of `bypass_call_ahead` may be "N/A" in the response if SMTP Call Ahead is not configured on Secure Email Gateway.

The value of `bypass_ldap_accept` may be "N/A" in the response if LDAP is not configured on Secure Email Gateway.

Adding New Entry in Recipient Access Table

You can add a new entry to an existing Recipient Access Table (RAT) configured for a listener in your email gateway with different attributes as explained below:

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

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

Keys in Request Body (See the Sample Request for the key hierarchy)	order	This is an optional key. It is used to determine the index of the entry. If it is not specified, an entry will be added by default at the end before the 'ALL' entry. It accepts integer values.
	recipient_address	The key is a required parameter. This key contains a list of comma-separated recipient addresses to be added to the entry. They can be full email addresses, domains, partial domains, usernames, or IP addresses.
	action	The key is a required parameter. It is the action to be taken for the recipient addresses. The action can be "accept" or "reject".
	custom_smtp_response	The key is an optional parameter. It is a dictionary that contains two keys: "response_code" and "response_text". The response code is a custom SMTP response code that you provide along with the request. The response text is a custom SMTP response text that you provide along with the request.
	response_code	The key is an optional parameter. The response code is a custom SMTP response code that you provide along with the request.
	response_text	The key is an optional parameter. The response text is a custom SMTP response text that you provide along with the request.
	bypass_receiving_control	The key is an optional parameter. This key specifies that the recipient bypasses throttling control mechanisms enabled on the listener. It accepts "true" or "false". The default value is "false". **Note** It cannot be configured when the "action" is defined as reject.
	bypass_ldap_accept	The key is an optional parameter. This key is used to configure bypassing LDAP acceptance. It accepts "true" or "false". The default value is "false". **Note** It cannot be configured if LDAP is not configured. It cannot be configured when the "action" is defined as reject.
	bypass_call_ahead	

		The key is an optional parameter. This key is used to configure bypassing SMTP call ahead. It accepts “true” or “false”. The default value is “false”. **Note** It cannot be configured if SMTP Call Ahead is not configured. It cannot be configured when the "action" is defined as reject.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to add a new entry to an existing Recipient Access Table (RAT) configured in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/listeners/public_listener/recipients?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
--data '{
    "data":{
        "order": 1,
        "recipient_address": ["test13.com", "::000:1111:1234"],
        "action": "accept",
        "bypass_call_ahead": "False",
        "bypass_receiving_control": "True",
      "bypass_ldap_accept": "True",
        "custom_smtp_response": {
            "response_text": "yolo",
            "response_code": 111
        }
    }
}'
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "meta": {
        "message": "The following addresses have been updated: '[::000:1111:1234]' has been
 updated to '[::17.17.18.52]'."
    },
    "data": {
        "message": "Added Successfully"
    }
}
```

Updating Specific Entry in Recipient Access Table

You can update a specific entry in the Recipient Access Table (RAT) configured for a listener in your email gateway with different attributes as explained below:

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

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

Keys in Request Body (See the Sample Request for the key hierarchy)	order	This is an optional key. It is used to determine the index of the entry. If it is not specified, an entry will be added by default at the end before the 'ALL' entry. It accepts integer values.
	recipient_address	The key is a required parameter. This key contains a list of comma-separated recipient addresses to be added to the entry. They can be full email addresses, domains, partial domains, usernames, or IP addresses.
	action	The key is a required parameter. It is the action to be taken for the recipient addresses. The action can be "accept" or "reject".
	custom_smtp_response	The key is an optional parameter. It is a dictionary that contains two keys: "response_code" and "response_text". The response code is a custom SMTP response code that you provide along with the request. The response text is a custom SMTP response text that you provide along with the request.
	response_code	The key is an optional parameter. The response code is a custom SMTP response code that you provide along with the request.
	response_text	The key is an optional parameter. The response text is a custom SMTP response text that you provide along with the request.
	bypass_receiving_control	The key is an optional parameter. This key specifies that the recipient bypasses throttling control mechanisms enabled on the listener. It accepts "true" or "false". The default value is "false". **Note** It cannot be configured when the "action" is defined as reject.
	bypass_ldap_accept	The key is an optional parameter. This key is used to configure bypassing LDAP acceptance. It accepts "true" or "false". The default value is "false". **Note** It cannot be configured if LDAP is not configured. It cannot be configured when the "action" is defined as reject.
	bypass_call_ahead	

		The key is an optional parameter. This key is used to configure bypassing SMTP call ahead. It accepts “true” or “false”. The default value is “false”. **Note** It cannot be configured if SMTP Call Ahead is not configured. It cannot be configured when the "action" is defined as reject.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to update a specific entry in the Recipient Access Table (RAT) configured in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/listeners/public_listener/recipients?device_type=esa HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
        "recipient_address": "test12.com",
        "recipient_address_new": ["10.10.10.10", "domain1.com", "domain2.com"],
        "order": 2,
        "action": "accept",
        "bypass_ldap_accept": "true",
        "bypass_call_ahead": "true",
        "custom_smtp_response": {}
    }
}
```

Sample Response

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

Deleting Specific Entry in Recipient Access Table

You can delete a specific entry in the Recipient Access Table (RAT) configured for a listener in your email gateway with different a ttributes as explained below:

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

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection
Keys in Request Body (See the Sample Request for thekey hierarchy	recipient_address	This is a required parameter. This key contains any one of the recipient addresses from the entry to be deleted. It can be full email address, domain, partial domain, username, or IP address.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to delete a specific entry in the Recipient Access Table (RAT) configured in your email gateway:

Sample Request

```
DELETE /esa/api/v2.0/config/listeners/public_listener/recipients?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
--data '{
    "data":{
        "recipient_address": "test13.com"
    }
}'
```

Sample Response

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

SMTP Routes APIs

You can retrieve SMTP Route information from your email gateway. The various API categories for SMTP Routes are:

- Retrieving All SMTP Routes Entries, on page 180
- Adding a New SMTP Route Entry, on page 182
- Updating a Specific SMTP Routes Entry, on page 186
- Deleting a SMTP Route Entry, on page 190

Retrieving All SMTP Routes Entries

You can retrieve information of all SMTP Routes in your email gateway with different attributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve information of all SMTP Routes entries configured in your email gateway:

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 28 July 2023 17:54:35 GMT
Content-type: application/json; charset=UTF-8 Content-Length: 777
Connection: close
{
    "data": [
        {
            "receiving_domain": "testingsmtproute.com",
            "destination_hosts": [
                {
```

```
                "priority": 1,
                "destination": "2.2.2.2",
                "port": 1
            },
            {
                "priority": 0,
                "destination": "exchange2.example.com",
                "port": 26
            },
            {
                "priority": 0,
                "destination": "example1.com",
                "port": 25
            },
            {
                "priority": 1,
                "destination": "[::1234:5678:5b7b:438]",
                "port": 1
            },
            {
                "priority": 1,
                "destination": "[2001:db8::7b7b:7b7b]",
                "port": 25
            }
        ]
    }
  ]
}
```

Adding a New SMTP Route Entry

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

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

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

Keys in Request Body (See the Sample Request for the key hierarchy)	receiving_domain	This key is a required parameter. This key contains the value for the receiving domain for this specific entry. The domain can be the special keyword 'ALL' to match all hosts to create a default SMTP route. The domain can also be a partial hostname or a bracketed IP address. The partial hostname may be a regular hostname or a partial hostname starting with a dot. A hostname is a string (combination of two or more labels) that must match the following rules: • A label is a set of characters, numbers and dashes. • The first and last character of a label must be a letter or a number. • The hostname must have at least two labels separated by a period. • The last label cannot be all numbers.
	destination_hosts	This key is a required parameter. This key contains a list of comma-separated destination hosts to be added to this specific entry. Each destination host includes three additional keys for defining that particular destination host: priority, destination, and port.
	priority	This key is a required parameter. This is the priority assigned to a particular destination host. The value must be an integer in the range: 0 to 65535
	port	This key is a required parameter. This is the port assigned to a particular destination host. The value must be an integer in the range: 1 to 65535
	destination	

		This key is a required parameter. This key contains the value of the destination for a particular destination host for this specific entry. The destination may be: • a hostname 'exchange.example.com'or bracketed hostname [exchange.example.com]. • an IPv4 address 192.168.1.1 orbracketed IPv4 address [192.168.1.1]. • an IPv6 address 2001:420:80:1::5 orbracketed IPv6 address [2001:420:80:1::5]. • a special keyword '/dev/null' or 'usedns'. **Note** The keyword 'usedns' may not be used with the "all" default route.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to add a new SMTP Route entry in your email gateway:

Sample Request

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

                "destination_hosts": [
                  {
                      "priority": 1,
                      "destination": "2.2.2.2",
                      "port": 1
                  },
                  {
                     "priority": 0,
                     "destination": "exchange2.example.com",
                     "port": 26
                 },
                 {
                     "priority": 0,
                     "destination": "example1.com",
                     "port": 25
                 },
                 {
                     "priority": 1,
                     "destination": "[::1234:5678:5b7b:438]",
                     "port": 1
                 },
```

```
                {
                    "priority": 1,
                    "destination": "[2001:db8::7b7b:7b7b]",
                    "port": 25
                }
            ]
        }
}
}'
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Fri, 18 Jul 2023 18:15:44 GMT
Content-type: application/json;
charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
        "message": "Added Successfully"
    }
}
```

Updating a Specific SMTP Routes Entry

You can update a specific SMTP Routes entry configured in your email gateway with different attributes as explained below:

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

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

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

Keys in Request Body (See the Sample Request for the key hierarchy)	receiving_domain	This key is a required parameter. This key contains the value for the receiving domain for this specific entry. The domain can be the special keyword 'ALL' to match all hosts to create a default SMTP route. The domain can also be a partial hostname or a bracketed IP address. The partial hostname may be a regular hostname or a partial hostname starting with a dot. A hostname is a string (combination of two or more labels) that must match the following rules: • A label is a set of characters, numbers and dashes. • The first and last character of a label must be a letter or a number. • The hostname must have at least two labels separated by a period. • The last label cannot be all numbers. The “receiving_domain” key can be changed, if required, by entering a new value for “new_receiving_domain”.
	destination_hosts	This key is a required parameter. This key contains a list of comma-separated destination hosts to be added to this specific entry. Each destination host includes three additional keys for defining that particular destination host: priority, destination, and port.
	priority	This key is a required parameter. This is the priority assigned to a particular destination host. The value must be an integer in the range: 0 to 65535
	port	This key is a required parameter. This is the port assigned to a particular destination host. The value must be an integer in the range: 1 to 65535
	destination	

		This key is a required parameter. This key contains the value of the destination for a particular destination host for this specific entry. The destination may be: • a hostname 'exchange.example.com'or bracketed hostname [exchange.example.com]. • an IPv4 address 192.168.1.1 orbracketed IPv4 address [192.168.1.1]. • an IPv6 address 2001:420:80:1::5 orbracketed IPv6 address [2001:420:80:1::5]. • a special keyword '/dev/null' or 'usedns'. **Note** The keyword 'usedns' may not be used with the "all" default route.
	new_receiving_domain	This key is an optional parameter. This key contains the value for the new receiving domain for this specific entry which overrides the previous "receiving_domain". This key cannot take the value "all". No other SMTP Route with this same receiving domain (provided in the “new_receiving_domain” field) should be already present. Otherwise, it returns an error. If the “receiving_domain” key is “all” (default route), then the value for “new_receiving_domain” key is discarded. The domain can be a partial hostname or a bracketed IP address. The partial hostname may be a regular hostnameor a partial hostname starting with a dot. A hostname is a string (combination of two or more labels) that must match the following rules: • A label is a set of characters, numbers and dashes. • The first and last characterof a label must be a letter or a number. • The hostname must have at least 2 labels separated by a period. • The last label cannot be all numbers.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to update a specific SMTP Route entry configured in your email gateway:

Sample Request

```
PUT esa/api/v2.0/config/smtp_routes?device_type=esa
HTTP/1.1
cache-control: no-cache
```

```
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
    "data": {
                "receiving_domain": "testingsmtpput.com",

                "new_receiving_domain": "changedtestingsmtpput.com",

                "destination_hosts": [
                  {
                     "priority": 0,
                     "destination": "exchange3.example.com",
                     "port": 26
                  },
                  {
                     "priority": 0,
                     "destination": "example2.com",
                     "port": 25
                  },
                  {
                     "priority": 1,
                     "destination": "[::1294:5678:5b7b:438]",
                     "port": 1
                  },
                  {
                     "priority": 1,
                     "destination": "[2005:db8::7b7b:7b7b]",
                     "port": 25
                  },
                  {
                     "priority": 1,
                     "destination": "2.2.2.2",
                     "port": 1
                  },
                ]
          }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 18 Jul 2023 18:15:44 GMT
Content-type: application/json;
charset=UTF-8
Content-Length: 777
Connection: close
{
    "data": {
        "message": "Updated Successfully"
    }
}
```

Deleting a SMTP Route Entry

You can delete a SMTP route entry in your email gateway with different attributes as explained below:

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

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration in all three modes: cluster, group, and machine. The group mode must be accompanied with the query parameter `group_name`, which specifies the name of the group. The machine mode must be accompanied with the parameter `host_name`. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection
Keys in Request Body (See the Sample Request for thekey hierarchy	receiving_domain	This is a required parameter. This key contains the SMTP Route entry which you want to delete. If the SMTP Route pertaining to this receiving domain does not exist than an error is thrown.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to delete a specific SMTP Route entry configured in your email gateway:

Sample Request

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

```
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
-- { "data":
        {
        "receiving_domain": "smtpexample1.com"
        }
   }
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 18 Jul 2023 18:15:44 GMT
Content-type: application/json;
charset=UTF-8
Content-Length: 777
Connection: close
{
"data": {
"message": "Deleted Successfully"
}
}
```

Note You cannot delete the default SMTP Route entry. (entry having the "reveiving_domain" value as ‘all’). To delete the destination hosts of default route, use the PUT API with the following request:

```
{
            "data":{
            "receiving_domain":"all",
            "destination_hosts": [     ]
                    }
        }
```

See Updating a Specific SMTP Routes Entry, on page 186 for more information.

Save and Load Configuration APIs

You can save and load configuration information from and to your email gateway.

The various API categories for Save and Load Configuration are:

- Retrieving Existing Configuration, on page 193
- Saving Configuration on Email Gateway, on page 195
- Retrieving Configuration by Email, on page 197
- Loading Configuration Through Request Body, on page 199
- Loading Configuration Using an XML File on the Email Gateway, on page 201
- Loading Partial Configuration , on page 203

Note Only users having the administrator user role can access the Save and Load Configuration APIs.

Note If the configuration contains any Unicode characters, then load the configuration directly from the email gateway to avoid any errors when copying from another system.

Note You may not see any response when loading a configuration in some scenarios. For example, when you update certificates, SSL configuration, or change network settings.

Retrieving Existing Configuration

You can retrieve the existing configuration on your local machine as an XML response and view the entire configuration for the email gateway.

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

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration only in the cluster level. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
	Passphrase	`passphrase_action=encrypt or passphrase_action=mask` Specify the passphrase action. This is an optional paramter. The values for this parameter can be “encrypt” or “mask”. The default value for this parameter is "mask". The value “encrypt” will encrypt the passwords in the configuration. The value “mask” will mask the passwords in the configuration. **Note** Configuration with masked passwords cannot be loaded via the `loadconfig` command.

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve the existing configuration on your local machine as an XML response:

Sample Request

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

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE cluster_config SYSTEM "cluster_config.dtd">
<!--
Product: Cisco C600V Secure Email Gateway Virtual
Model Number: C600V
Version: 14.4.25-051
Serial Number: 420EB8ED5D5006566CD6-0907F84B9594
Number of CPUs: 8
Memory (MB): 8192
Current Time: Tue May 9 04:21:46 2023
Feature "External Threat Feeds": Quantity = 1, Time Remaining = "877 days"
Feature "File Reputation": Quantity = 1, Time Remaining = "877 days"
Feature "IronPort Image Analysis": Quantity = 1, Time Remaining = "877 days"
Feature "Outbreak Filters": Quantity = 1, Time Remaining = "877 days"
Feature "Cloud Administration": Quantity = 1, Time Remaining = "877 days"
Feature "IronPort Anti-Spam": Quantity = 1, Time Remaining = "877 days"
Feature "Sophos": Quantity = 1, Time Remaining = "877 days"
Feature "Graymail Safe Unsubscription": Quantity = 1, Time Remaining = "877 days"
Feature "File Analysis": Quantity = 1, Time Remaining = "877 days"
Feature "Bounce Verification": Quantity = 1, Time Remaining = "877 days"
Feature "Incoming Mail Handling": Quantity = 1, Time Remaining = "878 days"
Feature "Intelligent Multi-Scan": Quantity = 1, Time Remaining = "877 days"
Feature "IronPort Email Encryption": Quantity = 1, Time Remaining = "877 days"
Feature "Data Loss Prevention": Quantity = 1, Time Remaining = "877 days"
Feature "McAfee": Quantity = 1, Time Remaining = "877 days"
-->
<cluster_config>
<cluster>
<config>
<!--
*******************************************************************************
```

```
Network Configuration *
********************************************************************************
-->
<dns>
<local_dns>
<dns_ip priority="0">192.168.0.252</dns_ip>
</local_dns>
<dns_ptr_timeout>20</dns_ptr_timeout>
<dns_hostpref_default>PREFER_V6</dns_hostpref_default>
<dnslist>
<dnslist_negative_ttl>1800</dnslist_negative_ttl>
<dnslist_timeout>3</dnslist_timeout>
</dnslist>
<use_dnssec>0</use_dnssec>
</dns>
<dns_cache_ttl_min>1800</dns_cache_ttl_min>
<dns_interface></dns_interface>
<!--
********************************************************************************
System Configuration *
********************************************************************************
-->

.
.
.
.
.
.
.
.
.
.
.
********************************************************************************

Filebeat Configuration. *
********************************************************************************
-->
<filebeat_config>
<customer_details>
<cd_allocation></cd_allocation>
<cd_data_center></cd_data_center>
<cd_name></cd_name>
</customer_details>
<kafka>
<cert></cert>
<host></host>
<topic></topic>
</kafka>
</filebeat_config>
</config>
</machine>
</cluster_config>
}
```

Saving Configuration on Email Gateway

You can download and save the existing configuration as an XML file on your email gateway.

Synopsis		[Standalone Machine]
		`GET /esa/api/v2.0/config/all/device_type=esa&passphrase_action=encrypt&save_to=appliance`
		[Clustered Machine]
		`GET /esa/api/v2.0/config/all/device_type=esa&passphrase_action=encrypt&save_to=appliance&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration only in the cluster level. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
	Passphrase	`passphrase_action=encrypt or passphrase_action=mask` This is an optional parameter. Specify the passphrase action. The values for this parameter can be “encrypt” or “mask”. The default value for this parameter is "mask". The value “encrypt” will encrypt the passwords in the configuration. The value “mask” will mask the passwords in the configuration. **Note** Configuration with masked passwords cannot be loaded via the `loadconfig` command.
	Save To	`save_to=appliance` This is a required parameter. Specify the parameter to save the configuration on the email gateway.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to save the existing configuration file on your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/all/device_type=esa&passphrase_action=encrypt&save_to=appliance
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
 "data": "Configuration file was saved to esa22008.cs14 as
C600V-420EB8ED5D5006566CD6-0907F84B9594-20230523T042700-14.4.25-070.xml"
}
```

Retrieving Configuration by Email

You can retrieve the existing configuration file by email in any specified email address(es).

Synopsis	[Standalone Machine]
	`GET /esa/api/v2.0/config/all/device_type=esa&passphrase_action=encrypt& &email_to=test%40cisc.com`
	[Clustered Machine]
	`GET /esa/api/v2.0/config/all/device_type=esa&passphrase_action=encrypt& email_to=test%40cisc.com&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration only in the cluster level. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
	Passphrase	`passphrase_action=encrypt or passphrase_action=mask` This is an optional parameter. Specify the passphrase action. The values for this parameter can be “encrypt” or “mask”. The default value of this parameter is "mask". The value “encrypt” will encrypt the passwords in the configuration. The value “mask” will mask the passwords in the configuration. **Note** Configuration with masked passwords cannot be loaded via the `loadconfig` command.

	Email Address	`email_to=test@cisco.com`
		This is a required parameter.
		Specify the email address to which the configuration is to be retrieved.
		To add multiple email addresses, add the parameter for each of the email address separated by commas. For example,
		`email_to=test1@cisco.com,email_to=test2@cisco.com`

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to send the configuration file by email to a specified email address:

Sample Request

```
GET
/esa/api/v2.0/config/all/device_type=esa&passphrase_action=encrypt&email_to=test%40cisco.com
```

```
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
 "data": "Configuration file successfully mailed to: test@cisc.com"
}
```

Loading Configuration Through Request Body

You can modify configuration through load configuration action with the XML information present in the request body.

In case of cluster case scenario, the default action is load for cluster (on the UI) with default topology same as the XML file.

Synopsis	[Standalone Machine]
	`POST /esa/api/v2.0/config/all/device_type=esa`
	[Clustered Machine]
	`POST /esa/api/v2.0/config/all/device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration only in the cluster level. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
	Warnings	`ignore_warnings=no` This is an optional parameter. The values for this parameter can be “yes” or “no”. The default value for this parameter is “no”. The value “no” displays all the warnings in the response and the configuration will not be loaded. The value “yes” ignores the warnings and loads the configuration on the email gateway. **Note** Use the value “yes” for this parameter only after considering all the warnings.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to modify configuration through load configuration action, with XML present in the request body:

Sample Request

```
POST /esa/api/v2.0/config/all/device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
{
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE cluster_config SYSTEM "cluster_config.dtd">

<!--
  Product: Cisco C600V Secure Email Gateway Virtual
  Model Number: C600V
  Version: 14.4.25-070
  Serial Number: 420EB8ED5D5006566CD6-0907F84B9594
  Number of CPUs: 8
  Memory (MB): 8192
  Current Time: Fri Jul  7 05:17:22 2023
-->
<cluster_config>
<cluster>
<config>
<!--
.
.
.
.
.
.
</config>

</machine>
</cluster_config>
}
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
 "meta": {
  "warning": "Following certificates are not FQDN compliant : ['Cisco ESA']."
 },
 "data": {
  "message": "Added Successfully"
 }
}
```

Loading Configuration Using an XML File on the Email Gateway

You can modify configuration information by uploading the XML file directly from the email gateway.

Synopsis	[Standalone Machine]
	`POST /esa/api/v2.0/config/all/device_type=esa source=appliance&file_name=C600V-420EB8ED5D5006566CD6-0907F84B9594-20230619T031259.xml`
	[Clustered Machine]
	`POST /esa/api/v2.0/config/all/device_type=esa&mode=cluster &source=appliance&file_name=C600V-420EB8ED5D5006566CD6-0907F84B9594-20230619T031259.xml`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration only in the cluster level. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
	Source	`source=appliance` This is a required parameter. Specify the source. The value for this parameter can only be “appliance”.
	File Name	`file_name=filename.xml` This is a required parameter. Specify the file name on the email gateway from which the configuration is to be loaded.
	Warnings	`ignore_warnings=no` This is an optional parameter. The values for this parameter can be “yes” or “no”. The default value for this parameter is “no”. The value “no” displays all the warnings in the response and the configuration will not be loaded. The value “yes” ignores the warnings and loads the configuration on the email gateway. **Note** Use the value “yes” for this parameter only after considering all the warnings.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to modify configuration through Load Configuration action, uploading from the local machine:

Sample Request

```
POST /esa/api/v2.0/config/all/device_type=esa&
source=appliance&file_name=C600V-420EB8ED5D5006566CD6-0907F84B9594-20230619T031259.xml'
HTTP/1.1
cache-control: no-cache
jwttoken:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUi....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

Sample Response

```
HTTP/1.1 201 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close{
 "meta": {
  "warning": "Following certificates are not FQDN compliant : ['Cisco ESA']. "
 },
 "data": {
  "message": "Added Successfully"
 }
}
```

Loading Partial Configuration

You can modify the configuration through load configuration action with the required information in the request body.

Note The configuration nodes in the XML request must be properly selected to load the partial configuration successfully.

Synopsis	[Standalone Machine]
	`POST /esa/api/v2.0/config/all/device_type=esa`
	[Clustered Machine]
	`POST /esa/api/v2.0/config/all/device_type=esa&mode=cluster`

Supported Resource Attributes	Device	`device_type=esa` This is a required parameter. Specify the device type. All API queries must be accompanied with this parameter.
	Mode	`mode=cluster` This is a required parameter for all email gateways in cluster mode. **Note** This parameter is not supported for email gateways in standalone mode. Specify the mode. This parameter supports configuration only in the cluster level. For more information on modes, see Cluster Levels for API Calls - Examples, on page 99.
	Warnings	`ignore_warnings=no` This is an optional parameter. The values for this parameter can be “yes” or “no”. The default value for this parameter is “no”. The value “no” displays all the warnings in the response and the configuration will not be loaded. The value “yes” ignores the warnings and loads the configuration on the email gateway. **Note** Use the value “yes” for this parameter only after considering all the warnings.
Request Headers		Host, Accept, JWT token
Response Headers		Content-Type, Content-Length, Connection

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to modify the configuration through load configuration action with the required information present in the request body:

Sample Request

```
POST /esa/api/v2.0/config/all/device_type=esa
HTTP/1.1
cache-control: no-cache
  --header 'Authorization: Basic YWRtaW46Q2lzY28xMyQ=' \
  --header 'Content-Type: application/xml' \
  --data '<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: Cisco C600V Secure Email Gateway Virtual
  Model Number: C600V
  Version: 14.4.25-051
```

```
  Serial Number: 420EB8ED5D5006566CD6-0907F84B9594
  Number of CPUs: 8
  Memory (MB): 8192
  Current Time: Mon Mar 27 18:20:40 2023
  Feature "External Threat Feeds": Quantity = 1, Time Remaining = "920 days"
  Feature "File Reputation": Quantity = 1, Time Remaining = "920 days"
  Feature "IronPort Image Analysis": Quantity = 1, Time Remaining = "920 days"
  Feature "Outbreak Filters": Quantity = 1, Time Remaining = "920 days"
  Feature "Cloud Administration": Quantity = 1, Time Remaining = "920 days"
  Feature "IronPort Anti-Spam": Quantity = 1, Time Remaining = "920 days"
  Feature "Sophos": Quantity = 1, Time Remaining = "920 days"
  Feature "Graymail Safe Unsubscription": Quantity = 1, Time Remaining = "920 days"
  Feature "File Analysis": Quantity = 1, Time Remaining = "920 days"
  Feature "Bounce Verification": Quantity = 1, Time Remaining = "920 days"
  Feature "Incoming Mail Handling": Quantity = 1, Time Remaining = "920 days"
  Feature "Intelligent Multi-Scan": Quantity = 1, Time Remaining = "920 days"
  Feature "IronPort Email Encryption": Quantity = 1, Time Remaining = "920 days"
  Feature "Data Loss Prevention": Quantity = 1, Time Remaining = "920 days"
  Feature "McAfee": Quantity = 1, Time Remaining = "920 days"
-->
<config>

  <users>
    <user>
      <username>admin</username>
      <fullname>Administrator</fullname>
      <group>admin</group>
      <enc_password>MOTMndaeBKZJKX4MLnE0o19LP+s1b9z8Bi2iUhYoUBOm1l5/dXtev1SG8hA2F8t4a1
      CJCjARn8kvX7my5riexIHd4q92DWOFLtv1iYauQiqHcFYhuGzNIO1/XRA5BErs09E=</enc_password>
      <date_range>current_day</date_range>
      <display_rows>10</display_rows>
      <landing_page></landing_page>
      <landing_page_parms></landing_page_parms>
      <language>en-us</language>
      <last_passwd_change>1678777075</last_passwd_change>
      <ignore_pw_expiration>0</ignore_pw_expiration>
      <lock_reason></lock_reason>
      <enable_forced_password_expiration>0</enable_forced_password_expiration>
      <password_expiration_enabled_time_stamp>0</password_expiration_enabled_time_stamp>
      <password_expiration_time>0</password_expiration_time>
      <password_grace_time>0</password_grace_time>
      <delegated_id>None</delegated_id>
    </user>
    <user>
      <username>admin_check</username>
      <fullname>Administrator</fullname>
      <group>admin</group>
     <enc_password>MOTMndaeBKZJKX4MLnE0o19LP+s1b9z8Bi2iUhYoUBOm1l5/dXtev1SG8hA2F8t4a1CJCjARn

      8kvX7my5riexIHd4q92DWOFLtv1iYauQiqHcFYhuGzNIO1/XRA5BErs09E=</enc_password>
      <date_range>current_day</date_range>
      <display_rows>10</display_rows>
      <landing_page></landing_page>
      <landing_page_parms></landing_page_parms>
      <language>en-us</language>
      <last_passwd_change>1678777075</last_passwd_change>
      <ignore_pw_expiration>0</ignore_pw_expiration>
      <lock_reason></lock_reason>
      <enable_forced_password_expiration>0</enable_forced_password_expiration>
      <password_expiration_enabled_time_stamp>0</password_expiration_enabled_time_stamp>
      <password_expiration_time>0</password_expiration_time>
      <password_grace_time>0</password_grace_time>
      <delegated_id>None</delegated_id>
    </user>
```

```
    <user>
      <username>admin_check</username>
      <fullname>Administrator</fullname>
      <group>admin</group>
     <enc_password>MOTMndaeBKZJKX4MLnE0o19LP+s1b9z8Bi2iUhYoUBOm1l5/dXtev1SG8hA2F8t4a1CJCjARn

      8kvX7my5riexIHd4q92DWOFLtv1iYauQiqHcFYhuGzNIO1/XRA5BErs09E=</enc_password>
      <date_range>current_day</date_range>
      <display_rows>10</display_rows>
      <landing_page></landing_page>
      <landing_page_parms></landing_page_parms>
      <language>en-us</language>
      <last_passwd_change>1678777075</last_passwd_change>
      <ignore_pw_expiration>0</ignore_pw_expiration>
      <lock_reason></lock_reason>
      <enable_forced_password_expiration>0</enable_forced_password_expiration>
      <password_expiration_enabled_time_stamp>0</password_expiration_enabled_time_stamp>
      <password_expiration_time>0</password_expiration_time>
      <password_grace_time>0</password_grace_time>
      <delegated_id>None</delegated_id>
    </user>

  </users>


</config>'
```

Sample Response

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

Address Lists APIs

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

- Retrieving All Entries of All Address Lists, on page 206
- Retrieving All Entries of Specific Address List, on page 209
- Adding New Address List, on page 211
- Updating Address List, on page 213
- Deleting Address List, on page 215

Retrieving All Entries of All Address Lists

You can retrieve information of all Address Lists in your email gateway with different attributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve information of all Address Lists in your email gateway:

Sample Request

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

Sample Response

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

```
Date: Thu, 13 July 2023 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "meta": {
        "count": 4
    },
    "data": [
        {
            "description": "IP address list",
            "addresses_count": 1,
            "used_by": {
                "dmarc_verification": "True",
                "mail_flow_policies": [
                    {
                        "listener": "PublicListener",
                        "policy": "MFP_AL_Public"
                    },
                    {
                        "listener": "PrivateListener",
                        "policy": "MFP_AL_Private"
                    }
                ]
            },
            "name": "al_ip",
            "list_type": "ip",
            "addresses": [
                "@[1.2.3.4]"
            ]
        },
        {
            "description": "All type address list",
            "addresses_count": 5,
            "used_by": {
                "mail_flow_policies": [
                    {
                        "listener": "PublicListener",
                        "policy": "MFP_AL_all_full"
                    }
                ]
            },
            "name": "al_all",
            "list_type": "any",
            "addresses": [
                "@.example.com",
                "@example.com",
                "user@",
                "user@example.com",
                "@[1.2.3.4]"
            ]
        },
        {
            "description": "Full email address list",
            "addresses_count": 3,
            "used_by": {
                "incoming_content_filters": [
                    "ICF_AL_Full_FED"
                ],
                "mail_flow_policies": [
                    {
                        "listener": "PublicListener",
                        "policy": "MFP_AL_all_full"
                    }
```

```
                ]
            },
            "name": "al_full",
            "list_type": "email",
            "addresses": [
                "user@example.com2",
                "user@example1.com",
                "user@example.com"
            ]
        },
        {
            "description": "Domain type address list",
            "addresses_count": 2,
            "used_by": {
                "outgoing_content_filters": [
                    "OCF_AL_domain"
                ],
                "incoming_content_filters": [
                    "ICF_AL_domain"
                ]
            },
            "name": "al_domain",
            "list_type": "domain",
            "addresses": [
                "@.example.com",
                "@example.com"
            ]
        }
    ]
}
```


Retrieving All Entries of Specific Address List

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

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve information of a specific Address List in your email gateway:

Sample Request

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

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 13 July 2023 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "meta": {
        "count": 1
    },
```

```
    "data": {
        "description": "This is my address list",
        "addresses_count": 3,
        "used_by": {},
        "name": "MyAddressList",
        "list_type": "any",
        "addresses": [
            "myAddress@example.comm",
            "@example.com",
            "@[1.2.3.4]"
        ]
    }
}
```

Adding New Address List

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

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

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

Keys in Request Body (See the Sample Request for the key hierarchy)	description	This key is an optional parameter. This key contains a description for the newly added Address List.
	list_type	This key is a required parameter. This key defines the type of the Address List. This key must not contain an empty value. It can have the following values - “any,” “domain,” “ip,” or “email”. **Note** If this key value for the Address List is specified as "any," then that Address List can have all other types of addresses ("'domain," "ip," and "email").
	addresses	This key is a required parameter. This key contains a list of comma-separated addresses to be added to the Address List.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

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

Sample Request

```
POST /esa/api/v2.0/config/address_lists/MyAddressList?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNj....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/json
    "data": {
        "description": "This is my address list",
        "list_type": "any",
        "addresses": [
            "myAddress@example.comm",
            "@example.com",
            "@example.com",
            "@[1.2.3.4]",
            "@[ipv6:2001:db8::1234:5678]"
        ]
    }
}'
```

Sample Response

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

```
    }
}
```

Updating Address List

You can update an existing Address List in your email gateway with different attributes as explained below:

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

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

Keys in Request Body (See the Sample Request for the key hierarchy)	name	This key is an optional parameter. This key contains the new name for the Address List. You can use this key to rename the existing Address List.
	description	This key is an optional parameter. This key contains a description for the Address List to be updated.
	addresses	This key is a required parameter. This key contains a list of comma-separated addresses to be updated in the existing Address List.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Note You cannot edit the value of the list_type key using the **PUT** command.

Example

This example shows a query to update an existing Address List in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/address_lists/MyAddressList?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNj....
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/json
{
    "data": {
        "name": "MyAddressList",
        "description": "Tada - new description",
        "addresses": [
            "@alphabeta.com"
        ]
    }
}'
```

Sample Response

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

Deleting Address List

You can delete an existing Address List in your email gateway with different a ttributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to delete an existing Address List in your email gateway:

Sample Request

```
DELETE /esa/api/v2.0/config/address_lists/MyAddressList?device_type=esa
HTTP/1.1
cache-control: no-cache
jwttoken:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwic2Vzc2lvbkVuZFRpbWUiOjE2NjkwN
TUwMTEsImlzMkZhY3RvckNoZWNrUmVxdWlyZWQiOmZhbHNlLCJ1c2VyIjoiTk9ORVVRIiwiZXhwIjoxNj....
Accept: */*
Host: esa.example.com:6080
```

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

Sample Response

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

Incoming Mail Policy Users APIs

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

- Retrieving User Entries of an Incoming Mail Policy, on page 216
- Adding User Entries to an Incoming Mail Policy, on page 218
- Updating User Entries in an Incoming Mail Policy, on page 222

Note Some special characters might require the equivalent UTF-8 encoded value in the URI of the API request. For more information, see Configuration APIs, on page 98.

Retrieving User Entries of an Incoming Mail Policy

You can retrieve information of all users of an Incoming Mail Policy in your email gateway with different attributes as explained below:

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

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

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to retrieve the user information of a specific Incoming Mail Policy in your email gateway:

Sample Request

```
GET /esa/api/v2.0/config/incoming_mail_policies/test/senders_and_recipients?
mode=cluster&device_type=esa'
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMyQ=
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 13 July 2023 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close
{
    "meta": {
        "count": 2
    },
    "data": [
        {
            "sender_config": {
                "sender": {
```

```
                    "domain_entries": [
                        "user@"
                    ]
                }
            },
            "receiver_config": {
                "operation": "and",
                "receiver_not": {
                    "domain_entries": [
                        "hey7@"
                    ]
                },
                "receiver": {
                    "domain_entries": [
                        "user@"
                    ]
                }
            }
        },
        {
            "sender_config": {
                "sender": {
                    "domain_entries": [
                        "user@",
                        "user@example.com"
                    ]
                }
            },
            "receiver_config": {
                "operation": "and",
                "receiver_not": {
                    "domain_entries": [
                        "hey7@"
                    ]
                },
                "receiver": {
                    "domain_entries": [
                        "user@"
                    ]
                }
            }
        }
    ]
}
```

Adding User Entries to an Incoming Mail Policy

You can add users to an Incoming Mail Policy in your email gateway with different attributes as explained below:

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

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

Keys in Request Body (See the Sample Request for the key hirearchy)	sender_config	This key is a required parameter. This key contains the dictionary – either "sender" or "sender_not" which then contains the list of domain_entries.
	sender	This key must be configured if the “sender_not” key is not present. The policy is matched if the message is received from one or more of the specified senders. This key contains the list of domain_entries of the sender. **Note** You cannot add both the “sender” and “sender_not” keys in the same request.
	sender_not	This key must be configured if the “sender” key is not present. The policy is matched if the message received is not from any of the specified senders. This key contains list of domain_entries of the sender_not. **Note** You cannot add both the “sender” and “sender_not” keys in the same request.
	receiver_config	This key is a required parameter. This key contains one entity, “operation”, and also either one or two dictionaries – "receiver" or "receiver_not" based on the operation chosen, which then conatins the list of domain_entries.
	receiver	This key is a required parameter. The policy is matched if the message is sent to the specified recipients. This key contains the list of domain_entries of the receiver.
	receiver_not	This key is an optional parameter. The policy is matched if the message is not sent to any of the specified recipients. This key contains list of domain_entries of the receiver_not. **Note** This key can only be configured with the "and" operation.
	operation	This key is a required parameter. The values can be “and” or “or”. The value must not be empty.
	domain_entries	

		This key is a required parameter. It can have the following list of valid entries: **1.** A domain: user@example.com, User@, @example.com, @.exapmple.com **2.** An IP address enclosed in square brackets: user@[1.2.3.4] or @[1.1.2.3] or user@[ipv6:2001:db8::1] **3.** If there are any special characters, they must be placed before the "@", for example, user!!@example.com **4.** “ANY”: The policy is matched if the message is from or to any sender/receiver. **5.** The domain entry “ANY” is case sensitive and has to be used as is in either receiver_config or sender_config. **6.** The domain entry “ANY” cannot be configured with any other domain entry in sender_config and receiver_config. **7.** The domain entry “ANY” can be configured only with the "or" operation in receiver_config.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Example

This example shows a query to add new users to an Incoming Mail Policy in your email gateway:

Sample Request

```
POST /esa/api/v2.0/config/incoming_mail_policies/test/senders_and_recipients?device_type=esa
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMyQ=
Content-Type: application/json
sid=fMTCqt0NT8ra4lMluc1n
   "data": {
        "sender_config": {
            "sender": {
                "domain_entries": [
                    "user@example.com",
                    "user@"
                ]
            }
        },
        "receiver_config": {
            "operation": "and",
            "receiver": {
                "domain_entries": [
                    "user@"
                ]
            },
            "receiver_not": {
                "domain_entries": [
                    "hey7@"
                ]
            }
        }
}'
```

Sample Response

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

Updating User Entries in an Incoming Mail Policy

You can update or delete existing users of a specific Incoming Mail Policy in your email gateway with different attributes as explained below:

Synopsis		[Standalone Machine]
		`PUT /esa/api/v2.0/config/incoming_mail_policies/<policy_name>/senders_and_recipients?device_type=esa`
		[Clustered Machine]
		`PUT /esa/api/v2.0/config/incoming_mail_policies/<policy_name>/senders_and_recipients?mode=cluster&device_type=esa`
		Note The PUT API request updates all your table entries. Be careful when you make any changes.

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

Response Headers		Content-Type, Content-Length, Connection

Keys in Request Body (See the Sample Request for the key hirearchy)	sender_config	This key is a required parameter. This key contains the dictionary, either "sender" or "sender_not" which then contains the list of domain_entries.
	sender	This key must be configured if the “sender_not” key is not present. The policy is matched if the message is received from one or more of the specified senders. This key contains the list of domain_entries of the sender. **Note** You cannot add both the “sender” and “sender_not” keys in the same request.
	sender_not	This key must be configured if the “sender” key is not present. The policy is matched if the message received is not from any of the specified senders. This key contains list of domain_entries of the sender_not. **Note** You cannot add both the “sender” and “sender_not” keys in the same request.
	receiver_config	This key is a required parameter. This key contains one entity, “operation”, and also either one or two dictionaries – "receiver" or "receiver_not" based on the operation chosen, which then conatins the list of domain_entries.
	receiver	This key is a required parameter. The policy is matched if the message is sent to the specified recipients. This key contains the list of domain_entries of the receiver.
	receiver_not	This key is an optional parameter. The policy is matched if the message is not sent to any of the specified recipients. This key contains list of domain_entries of the receiver_not. **Note** This key can only be configured with the "and" operation.
	operation	This key is a required parameter. The values can be “and” or “or”. The value must not be empty.
	domain_entries	

		This key is a required parameter. It can have the following list of valid entries: **1.** A domain: user@example.com, User@, @example.com, @.exapmple.com **2.** An IP address enclosed in square brackets: user@[1.2.3.4] or @[1.1.2.3] or user@[ipv6:2001:db8::1] **3.** If there are any special characters, they must be placed before the "@", for example, user!!@example.com **4.** “ANY”: The policy is matched if the message is from or to any sender/receiver. **5.** The domain entry “ANY” is case sensitive and has to be used as is in either receiver_config or sender_config. **6.** The domain entry “ANY” cannot be configured with any other domain entry in sender_config and receiver_config. **7.** The domain entry “ANY” can be configured only with the "or" operation in receiver_config.

For information on API Limits, see Configuration APIs - Rate Limits , on page 226.

Note To delete a user entry, exclude the user data (that you want to delete) in the request body.

Example

This example shows a query to update the users of an existing Incoming Mail Policy in your email gateway:

Sample Request

```
PUT /esa/api/v2.0/config/incoming_mail_policies/test/senders_and_recipients?device_type=esa
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMyQ='
Content-Type: application/json
sid=fMTCqt0NT8ra4lMluc1n
{
  "data": [
        {
            "sender_config": {
                "sender": {
                    "domain_entries": [
                        "yyo@[1.11.11.1]"
                    ]
                }
            },
            "receiver_config": {
                "operation": "and",
                "receiver": {
                    "domain_entries": [
                        "heey3311s121@"
                    ]
                },
```

```
                "receiver_not": {
                    "domain_entries": [
                        "hwey7@"
                    ]
                }
            }
        },
        {
            "sender_config": {
                "sender": {
                    "domain_entries": [
                        "yyo@"
                    ]
                }
            },
            "receiver_config": {
                "operation": "and",
                "receiver": {
                    "domain_entries": [
                        "hey3311s121@"
                    ]
                },
                "receiver_not": {
                    "domain_entries": [
                        "hwey7@"
                    ]
                }
            }
        }
    ]'
}
```

Sample Response

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

Configuration APIs - Rate Limits

The following table specifies the rate limits for the Configuration APIs. The limits that are mentioned in this table are for the API calls and are not applicable to the configuration performed through the web interface.

Note The limits specified for adding (POST) and updating (PUT) APIs also apply to retrieving (GET) and deleting (DELETE) APIs.

Note The rate limits for Configuration APIs are tested using the C600V model (16GB Memory, 8 CPU Core), and these limits may vary in the actual production environment based on your system configuration.

Configuration APIs	Rate Limits
URL Lists	The maximum number of URLs allowed for one URL List (each URL with 50 characters) in a single POST request is 19,417. The size of the payload is 1048 KB. The maximum number of URL Lists with maximum URLs allowed is 42.
Dictionary	The maximum number of words allowed for one Dictionary in a single POST request is 74892. The size of the payload is 1048KB. The maximum number of Dictionaries with maximum words allowed is 10. By default, the number of Dictionaries allowed in your email gateway is 100. This limit can be extended to 150 dictionaries using CLI.
Host Access Table (HAT)	The maximum number of senders that can be added in one sender group in a single POST request is 23,036. The size of the payload is 1048 KB. The maximum number of sender groups that can added with the maximum number of senders is 30.
File Hash List	The maximum number of File Hashes that you can add for a particular File Hash List in a single POST request is 15,420. The maximum number of File Hash Lists allowed with each File Hash List having 15k File Hashes is 50-60 File Hash List.
Recipient Address Table (RAT)	The number of recipient addresses in a single recipient address row is limited to 4000. The maximum number of recipient address rows allowed with each recipient address row containing one recipient address is 40118. The maximum number of recipient address rows allowed with each recipient address row containing 4000 recipient addresses is 368.
SMTP Routes	The maximum number of destination hosts that you can add in a single SMTP Route POST request is 100. The maximum number of SMTP Routes that you can add to the database with a single destination host is 40,000.

Save Configuration	The maximum size of the configuration you can receive as an XML response is 95MB. This limit is applicable to Retrieving Existing Configuration, on page 193 API. The maximum size of the configuration file that you can save in your email gateway is 68MB. This limit is applicable to Saving Configuration on Email Gateway, on page 195 API. The recipient mail server can recieve an email with a maximum configuration file size of 22MB. This limit is applicable to Retrieving Configuration by Email, on page 197 API.
Load Configuration	The maximum size of the configuration sent as an XML request is 1MB. This limit is applicable to Loading Configuration Through Request Body, on page 199 and Loading Partial Configuration , on page 203 APIs. The maximum size of the configuration file that is read from your email gateway is 19MB. This limit is applicable to Loading Configuration Using an XML File on the Email Gateway, on page 201 API.
Address Lists	The maximum number of addresses allowed in one Address List in a single POST request is 58,867. The maximum number of Address Lists entries that you can add with each list having three addresses is 62,000.
Incoming Mail Policy Users	The maximum number of user domain entries (email addresses), each user domain entry with 16 characters, that you can add for sender and recipient keys (combined) in a single POST or PUT request is 52,421. The size of the payload is 1048 KB.

Logging APIs

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

- Retrieving Log Subscription Details from Email Gateway, on page 228
- Retrieving All Log Files for Specific Log Subscription, on page 230
- Retrieving Log Files using URL, on page 231

Retrieving Log Subscription Details from Email Gateway

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

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

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

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

Example

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

Sample Request

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

Sample Response

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

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

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

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

Retrieving All Log Files for Specific Log Subscription

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

Note This API is only applicable for log subscriptions configured with the manual log retrieval method in your email gateway. The API lists only the log files that are rolled over. You need to use the `name` attribute of the response obtained from the log subscription name in the Retrieving Log Subscription Details from Email Gateway, on page 228 API.

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

Example

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

Sample Request

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

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

Sample Response

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

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

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

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

            "size": 1403
        }
    ]
}
```

Retrieving Log Files using URL

You can retrieve the content of the log file using the `downloadUrl` attribute of the response obtained from the Retrieving All Log Files for Specific Log Subscription, on page 230 API.

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

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

Synopsis	`GET /esa/api/v2.0/logs/<log_subscription_name>/<log_file_name>` **Note** You need to use the `downloadUrl` attribute of the response obtained from the Retrieving All Log Files for Specific Log Subscription, on page 230 API.
Request Headers	Host, Accept, Authorization
Response Headers	Content-Type, Content-Length, Connection, Content-Disposition

Example

This example shows a query to retrieve the content of the log file using the `downloadUrl` attribute of the resposne obtained from the Retrieving All Log Files for Specific Log Subscription, on page 230 API:

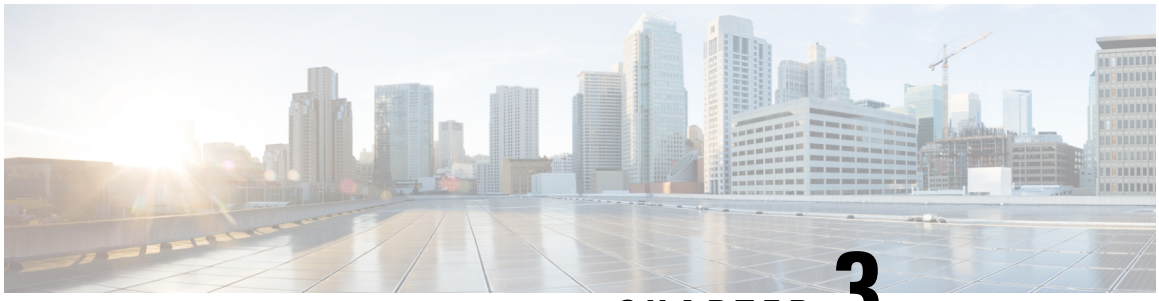
Sample Request

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

Sample Response

The response contains the log file that was requested.

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



CHAPTER 3

General Purpose APIs

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

This chapter contains the following sections:

- Querying for the System Time, on page 233
- Retrieving APIs Accessible to a User Role, on page 234
- Health API, on page 234
- Delivery Status API, on page 235
- System Status API, on page 236

Querying for the System Time

Sample Request

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

Sample Response

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

```
    }
}
```

Retrieving APIs Accessible to a User Role

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

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

Sample Request

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

Sample Response

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

Health API

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

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

Sample Request

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

Sample Response

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

Delivery Status API

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

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

Sample Request

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

Sample Response

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

System Status API

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

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

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

Sample Request

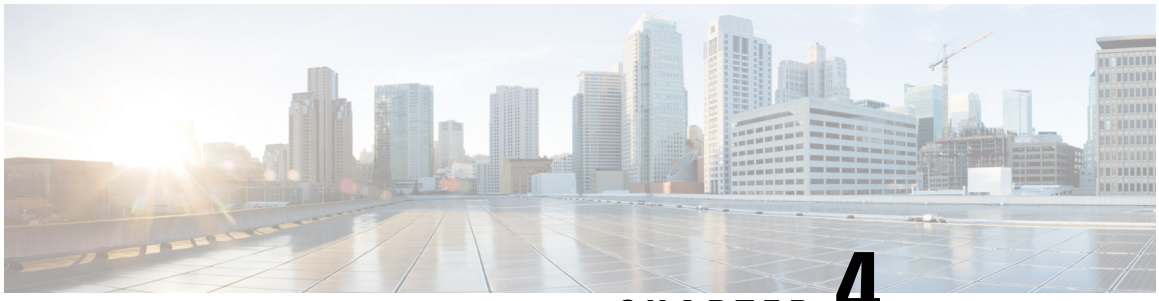
```
GET /esa/api/v2.0/health/system_status
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46SXJvbnBvcnRAMzAu
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate, br
Connection: keep-alive
```

Sample Response

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

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

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



CHAPTER 4

Troubleshooting AsyncOS API

This chapter contains the following sections:

- API Logs, on page 241
- Alerts, on page 241
- Handling Error Messages of Configuration APIs, on page 241

API Logs

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

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

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

Alerts

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

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

Handling Error Messages of Configuration APIs

This section lists the following error messages that you might receive when generating the following Configuration APIs ('Authentication,' 'URL lists,' 'Dictionary,' 'HAT,' 'File Hash Lists,' 'RAT,' 'Save and Load Configuration,' 'Address Lists,' and 'Incoming Mail Policy Users' :

- Error - Unauthorised API calls
- Error - Invalid credentials while generating token
- Error - Token not authenticating API calls
- Error - API calls give an expired token
- Error - API Calls give unsupported operation for mode
- Error - Bad Request Syntax or Unsupported Method
- Error - Request Entity Too Large
- Error - Bad Gateway

Error - Unauthorised API Calls

You may receive the following error message for an unauthorized API call:

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

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

Error - Invalid credentials while Generating Token

You may receive the following error message when invalid credentials are received when generating the token:

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

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

Error - Token not authenticating API Calls

You may receive the following error message when the token does not authenticate the API calls:

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

Solution: The token might be incorrect. See the Generating JWT Token , on page 105 section for information on how to generate the token correctly.

Error - API Calls give Expired Token

You may receive the following error message when the API calls give an expired token:

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

Solution: The token might have expired. You can regenerate a token using the Token API call. For more information, see Generating JWT Token , on page 105.

Error - API Calls give unsupported operation for mode

You may receive the following error message when the API calls give unsupported operation for mode:

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

}
```

Solution: You must override settings for the particular feature from the UI. In this example, you must override settings for sender groups from the UI to machine mode, after which API calls for sender groups for machine mode will return a successful response.

Error - Bad Request Syntax or Unsupported Method

You may receive the following error message when the number of Dictionaries exceeds the upper limit:

```
{"error":
{"message": "Maximum dictionaries count exceeded.",
"code": "400",
"explanation": "400 = Bad request syntax or unsupported method."
}
}
```

You may receive the following error message when the number of destination hosts that you have added in a single SMTP Route POST request exceeds the upper limit.:

```
{"error":
{"message": "Routes must not contain more than 100 destinations",
"code": "400",
"explanation": "400 = Bad request syntax or unsupported method."
}
}
```

You may receive the following error message when the number of SMTP Routes that you have added to the database with a single destination host exceeds the upper limit:

```
{"error":
{"message": "Maximum number of routes allowed is 40,000. Please remove one before trying
to add a new route.",
"code": "400",
"explanation": "400 = Bad request syntax or unsupported method."
}
}
```

Solution: See the Configuration APIs - Rate Limits , on page 226 section for information about the rate limits for Configuration APIs.

Error - Request Entity Too Large

You may receive the following error response when:

- the number of URLs allowed for one URL List (each URL with 50 characters) in a single POST request exceeds the upper limit.
- the number of words in a Dictionary exceeds the upper limit.
- the number of senders that can be added in one sender group in a single POST request exceeds the upper limit.
- the number of File Hashes that you can add for a particular File Hash List exceeds the upper limit.
- the number of user domain entries that you can add for sender and receiver keys in a single IMP Users POST or PUT request exceeds the upper limit.
- the number of user domain entries having 'ANY' that you can add for sender and receiver keys in a single IMP Users POST or PUT request exceeds the upper limit.
- the number of characters allowed for one sender and receiver domain entry in a single IMP Users POST or PUT request exceeds the upper limit.
- the size of the configuration sent or read exceeds the upper limit.
- the number of addresses allowed in one Address List in a single POST request exceeds the upper limit.

```
<html>
<head><title>413 Request Entity Too Large</title></head>
<body bgcolor="white">
<center><h1>413 Request Entity Too Large</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Solution: See the Configuration APIs - Rate Limits , on page 226 section for information about the rate limits for Configuration APIs.

Error - Bad Gateway

You may receive the following error message when:

- the number of URL Lists with maximum URLs exceeds the upper limit.
- the number of sender groups that can added with the maximum number of senders exceeds the upper limit.
- the number of File Hash Lists exceeds the upper limit.
- the number of entries with each entry containing 4000 recipient addresses exceeds the upper limit.
- the size of the configuration that you receive or save exceeds the upper limit.
- the number of Address List entries exceeds the upper limit.

```
{
    "error": {
        "code": "502",
        "explanation": "502 = Bad Gateway"
    }

}
```

Solution: See the Configuration APIs - Rate Limits , on page 226 section for information about the rate limits for Configuration APIs.