



Secure Email 用 API

- [レポート API](#) (1 ページ)
- [トラッキング API](#) (14 ページ)
- [隔離](#) (38 ページ)
- [ロギング API](#) (92 ページ)

レポート API

レポートクエリを使用すると、特定のグループ内のすべてのカウンタまたは特定のカウンタにおいてレポートからデータを取得できます。

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

サポート対象のリソース属性	時間	<p>このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。</p> <p><code>startDate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</code></p> <p>指定した期間の集約レポート。</p> <p>(注) <code>duration</code> 属性は、分 (mm) および秒 (ss) パラメータの値として 00 のみをサポートします。</p>
	クエリのタイプ	<ul style="list-style-type: none"> • <code>query_type=graph</code> グラフとして表現できるデータを受信します。 • <code>query_type=export</code> エクスポート形式のデータを受信します。
	ソート	<p>次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。</p> <ul style="list-style-type: none"> • <code>orderBy=<value></code> 応答内のデータを並べ替える属性を指定します。次の例を参考にしてください。 <code>orderBy=total_clean_recipients</code> • <code>orderDir=<value></code> ソート方向を指定します。 有効なオプションは次のとおりです。 <ul style="list-style-type: none"> • <code>asc</code> 昇順で結果を並べ替えます。 • <code>desc</code> 降順で結果を並べ替えます。
	遅延読み込み	<p>次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。</p> <ul style="list-style-type: none"> • <code>offset=<value></code> オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。 • <code>limit=<value></code> 取得するレコードの数を指定します。

データの取得オプション	<ul style="list-style-type: none"> • top=<value> 最大値を返すレコードの数を指定します。
フィルタリング	<p>フィルタ パラメータは応答に含まれるデータを制限します。</p> <ul style="list-style-type: none"> • filterValue=<value> 検索対象の値。 • filterBy=<value> フィルタプロパティと値に従って取得されるデータをフィルタリングします。 • filterOperator=<value> 有効なオプションは次のとおりです。 <ul style="list-style-type: none"> • begins_with 指定した値に基づいて応答データをフィルタリングします。これは完全一致の値ではありません。 • is 指定した完全一致の値に基づいて応答データをフィルタリングします。
デバイス	<ul style="list-style-type: none"> • device_group_name=<value> デバイス グループ名を指定します。 • device_type=esa デバイスタイプを指定します。このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。 • device_name=<value> デバイス名を指定します。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

例

次に、レポートクエリタイプの例を示します。

- [カウンタの1つの値を取得する \(4 ページ\)](#)

- [カウンタの複数の値を取得する \(5 ページ\)](#)
- [カウンタ グループ内の各カウンタの1つの値を取得する \(5 ページ\)](#)
- [複数のカウンタの複数の値を取得する \(6 ページ\)](#)
- [各カウンタの複数の値を使用して複数のカウンタの複数の値を取得する \(8 ページ\)](#)
- [設定されたメールポリシーに一致する上位受信メッセージを取得する \(10 ページ\)](#)
- [設定されたメールポリシーに一致する上位送信メッセージを取得する \(11 ページ\)](#)
- [設定されたメールポリシーに一致するすべての受信メッセージを取得する \(12 ページ\)](#)
- [設定されたメールポリシーに一致するすべての送信メッセージを取得する \(14 ページ\)](#)

カウンタの1つの値を取得する

次の例では、デバイス名とタイプを使用してカウンタグループから特定のカウンタの値を取得するクエリを示します。

サンプル リクエスト

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

サンプル応答

```
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}
  }
}
```

カウンタの複数の値を取得する

次の例では、デバイス グループとデバイス タイプを使用してカウンタ グループのすべてのカウンタの値を取得するクエリを示します。

サンプル リクエスト

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

サンプル応答

```
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}]}}
```

カウンタ グループ内の各カウンタの1つの値を取得する

カウンタ グループには複数のカウンタが含まれます。次の例では、順序、デバイス タイプ、および上位パラメータを指定して、カウンタ グループ内の各カウンタの1つの値を取得するクエリを示します。

複数のカウンタの複数の値を取得する

サンプル リクエスト

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

サンプル応答

```
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}
      ]
    }
  }
}
```

複数のカウンタの複数の値を取得する

次の例では、オフセット、制限、およびデバイス タイプ パラメータを指定して、複数のカウンタの複数の値を取得するクエリを示します。

サンプル リクエスト

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

サンプル応答

```
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}
      ],
      ...
    }
  },
  ...
}
```

各カウンタの複数の値を使用して複数のカウンタの複数の値を取得する

```

    "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}
    ]
  }
}

```

各カウンタの複数の値を使用して複数のカウンタの複数の値を取得する

次の例では、フィルタリングおよびクエリタイプパラメータを指定して、複数のカウンタの複数の値（各カウンタの複数の値）を取得するクエリを示します。グラフ属性は、カウンタの時間ベースのカウント値を取得します。

サンプルリクエスト

```

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

```

サンプル応答

```

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},

```

設定されたメールポリシーに一致する上位受信メッセージを取得する

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

設定されたメールポリシーに一致する上位受信メッセージを取得する

次の例は、電子メールゲートウェイで設定されたメールポリシーに一致する上位の受信メッセージを取得するクエリを示しています。

サンプル リクエスト

```
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
```

サンプル応答

```
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
        }
      ]
    }
  }
}
```

設定されたメールポリシーに一致する上位送信メッセージを取得する

次の例は、電子メールゲートウェイで設定されたメールポリシーに一致する上位の送信メッセージを取得するクエリを示しています。

サンプル リクエスト

設定されたメールポリシーに一致するすべての受信メッセージを取得する

```
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
```

サンプル応答

```
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
        }
      ]
    }
  }
}
```

設定されたメールポリシーに一致するすべての受信メッセージを取得する

次の例は、電子メールゲートウェイで設定されたメールポリシーに一致するすべての受信メッセージを取得するクエリを示しています。

サンプル リクエスト

```
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
```

サンプル応答

```
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
        }
      ]
    }
  }
}
```

設定されたメールポリシーに一致するすべての送信メッセージを取得する

```
}
}
```

設定されたメールポリシーに一致するすべての送信メッセージを取得する

次の例は、電子メールゲートウェイで設定されたメールポリシーに一致するすべての送信メッセージを取得するクエリを示しています。

サンプル リクエスト

```
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
```

サンプル応答

```
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
        }
      ]
    }
  }
}
```

トラッキング API

ユーザーが指定した基準に一致するメッセージまたはメッセージのグループを検索できます。メッセージの詳細、拒否された接続の詳細を取得し、Eメールストリーム内の特定のメッセー

ジのステータスを確認できます。トラッキング用のさまざまな API カテゴリは次のとおりです。

- [メッセージの検索 \(15 ページ\)](#)
- [拒否された接続 \(20 ページ\)](#)
- [メッセージの詳細 \(21 ページ\)](#)
- [DLP の詳細 \(24 ページ\)](#)
- [AMP の詳細 \(25 ページ\)](#)
- [URL の詳細 \(27 ページ\)](#)
- [接続の詳細 \(29 ページ\)](#)
- [修復の詳細 \(31 ページ\)](#)
- [設定されたメールポリシーに一致するすべての受信メッセージを取得する \(33 ページ\)](#)
- [設定されたメールポリシーに一致するすべての送信メッセージを取得する \(35 ページ\)](#)

メッセージの検索

複数の属性に一致するメッセージを検索することができます。次に、構文とサポート対象の属性を示します。

概要	GET/esa/api/v2.0/message-tracking/messages?resource_attribute	
サポート対象のリソース属性	詳細については、『』 『』 『 AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway Appliances 』を参照してください。	
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次の例では、時間範囲、メッセージ配信ステータス、（電子メールを処理する）電子メールゲートウェイ、オフセット、制限パラメータを指定して、メッセージを取得するクエリを示します。

サンプル リクエスト

```
GET /esa/api/v2.0/message-tracking/messages?startDate=2018-01-01T00:00:00.000Z&
endDate=2018-11-20T09:36:00.000Z&ciscoHost=All_Hosts&
searchOption=messages&offset=0&limit=20
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
```

```
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
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"
      }
    }
  ]
}
```

拒否された接続

次の表からさまざまな属性を持つ拒否された接続の詳細を取得できます。

概要	GET /api/v2.0/message-tracking/messages?resource_attribute	
サポート対象のリソース属性	時間	このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。 startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z 指定した期間の集約レポート。
	検索オプション	<ul style="list-style-type: none"> searchOption=<value> この属性には、拒否された接続をクエリする場合に許可される1つの値が含まれます。次に例を示します。 searchOption=rejected_connections
	送信者 IP	<ul style="list-style-type: none"> senderIp=<value> これはユーザー定義の値です。メッセージを送信するサーバーの IP アドレスを使用します。次に例を示します。 senderIp=10.76.70.112
	遅延読み込み	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> offset=<value> オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。 <ul style="list-style-type: none"> limit=<value> 取得するレコードの数を指定します。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、期間、送信者 IP アドレス、検索オプション、オフセット、制限属性を指定して、拒否された接続の詳細を取得するクエリを示します。

サンプル リクエスト

```
GET /esa/api/v2.0/message-tracking/messages?startDate=2016-11-16T00:00:00.000Z&endDate=2018-11-16T14:22:00.000Z&senderIp=10.76.70.112&searchOption=rejected_connections&offset=0&limit=20
```

```

HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

サンプル応答

```

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"
      }
    }
  ]
}

```

メッセージの詳細

次の表からさまざまな属性を持つメッセージの詳細を取得できます。

概要	GET /api/v2.0/message-tracking/details?resource_attribute
サポート対象のリソース属性	詳細については、『 AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway 』を参照してください。
要求ヘッダー	Host, Accept, Authorization

応答ヘッダー	Content-Type、Content-Length、Connection
--------	--

例

次の例では、`icid`、`mid`、電子メールゲートウェイのシリアル番号で識別される特定のメッセージの詳細を取得するクエリを示します。

サンプル リクエスト

```
GET /esa/api/v2.0/message-tracking/details?endDate=2018-11-16T12:09:00.000Z&icid=19214&mid=22125&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-16T00:00:00.000Z HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: m680q09.ibqa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
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 の詳細

次の表からさまざまな属性を持つメッセージの DLP を取得できます。

概要	GET /api/v2.0/message-tracking/dlp-details?resource_attribute	
サポート対象のリソース属性	時間	このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。 startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z 指定した期間の集約レポート。
	シリアル番号	<ul style="list-style-type: none"> serialNumber=<value> 電子メールゲートウェイのシリアル番号を指定します。
	メッセージ ID とインジェクション接続 ID	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> icid=<value> mid=<value> メッセージの icid を指定します。 メッセージの mid を指定します。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、icid、mid、シリアル番号で識別される特定のメッセージに関する DLP の詳細を取得するクエリを示します。

サンプル リクエスト

```
GET /esa/api/v2.0/message-tracking/dlp-details?endDate=2018-11-16T11:25:00.000Z&icid=19213&mid=22124&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Postman-Token: ab16ff7f-847e-4221-a2a2-01de50a33fea
Authorization: Basic YWRtaW46Q21zY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
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 の詳細

次の表からさまざまな属性を持つメッセージの高度なマルウェア防御の仕組みに関する詳細を取得できます。

概要	GET /api/v2.0/message-tracking/amp-details?resource_attribute	
サポート対象のリソース属性	時間	このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。 startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z 指定した期間の集約レポート。
	シリアル番号	<ul style="list-style-type: none"> • serialNumber=<value> 電子メールゲートウェイのシリアル番号を指定します。
	メッセージ ID とインジェクション接続 ID	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> • icid=<value> メッセージの icid を指定します。 <ul style="list-style-type: none"> • mid=<value> メッセージの mid を指定します。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、icid、mid、シリアル番号で識別される特定のメッセージの高度なマルウェア防御の仕組みに関する詳細を取得するクエリを示します。

サンプル リクエスト

```
GET /esa/api/v2.0/message-tracking/amp-details?endDate=2018-11-16T11:25:00.000Z&icid=19213
&mid=22124&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q21zY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
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 の詳細

次の表からさまざまな属性を持つメッセージの URL に関する詳細を取得できます。

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

サポート対象のリソース属性	時間	このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。 startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z 指定した期間の集約レポート。
	シリアル番号	<ul style="list-style-type: none"> serialNumber=<value> 電子メールゲートウェイのシリアル番号を指定します。
	メッセージ ID とインジェクション接続 ID	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> icid=<value> メッセージの icid を指定します。 mid=<value> メッセージの mid を指定します。
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次の例では、icid、mid、シリアル番号で識別される特定のメッセージの URL に関する詳細を取得するクエリを示します。

サンプル リクエスト

```
GET
/esa/api/v2.0/message-tracking/url-details?endDate=2018-11-16T11:25:00.000Z&icid=19124&mid=21981&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q21zY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
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"
    }
  }
}

```

接続の詳細

次の表からさまざまな属性を持つメッセージの接続に関する詳細を取得できます。

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

サポート対象のリソース属性	時間	このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。 startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z 指定した期間の集約レポート。
	シリアル番号	<ul style="list-style-type: none"> serialNumber=<value> 電子メールゲートウェイのシリアル番号を指定します。
	メッセージ ID とインジェクション接続 ID	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> icid=<value> メッセージの icid を指定します。 mid=<value> メッセージの mid を指定します。
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次の例では、icid、mid、シリアル番号で識別される特定のメッセージの接続に関する詳細を取得するクエリを示します。

サンプルリクエスト

```
GET /esa/api/v2.0/message-tracking/connection-details?endDate=2018-11-16T11:25:00.000Z&icid=19213&mid=22124&serialNumber=64122536256E-FCH1812V1ST&startDate=2018-11-09T00:00:00.000Z
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q21zY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
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"
}

```

修復の詳細

[メールボックスの検索と修復 (Mailbox Search and Remediate)] を使用して修復されたメッセージの修復の詳細を取得できます。

概要	GET /api/v2.0/message-tracking/remediation-details?resource_attribute
サポート対象のリソース属性	詳細については、『』 『』 『 AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway 』を参照してください。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection この例は、修復ステータス、バッチの詳細など、メッセージの修復の詳細を取得するクエリを示しています。

サンプル リクエスト

```

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

```

サンプル応答

```

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": "anonpremnnew@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"
    }
  ]
}

```


設定されたメールポリシーに一致するすべての受信メッセージを取得する

電子メールゲートウェイで設定されたメールポリシーに一致するすべての受信メッセージを取得できます。

概要	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
サポート対象のリソース属性	詳細については、『』、『』『 AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway 』を参照してください。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection 次の例は、電子メールゲートウェイで設定されたメールポリシーに一致するすべての受信メッセージを取得するクエリを示しています。

サンプルリクエスト

```
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
```

サンプル応答

```
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,
```

設定されたメールポリシーに一致するすべての受信メッセージを取得する

```

    "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"
  },
},
]
```

設定されたメールポリシーに一致するすべての送信メッセージを取得する

電子メールゲートウェイで設定されたメールポリシーに一致するすべての送信メッセージを取得できます。

設定されたメールポリシーに一致するすべての送信メッセージを取得する

概要	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
サポート対象のリソース属性	詳細については、『』』』『 AsyncOS 14.0 API - Addendum to the Getting Started guide for Cisco Secure Email Gateway 』を参照してください。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection 次の例は、電子メールゲートウェイで設定されたメールポリシーに一致するすべての送信メッセージを取得するクエリを示しています。

サンプル リクエスト

```
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
```

サンプル応答

```
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": "<198313425761047198391528032556096@makug.fiendofwine.us>"
  },
  },
  "verdictChart": {
    "2325166": "16141113"
  },
  },
  "recipient": [
    "testuser2@abc.com"
  ],
  "sender": "user@testdomain.com",
  "serialNumber": "42155830541772925266-ABFF53B45FDE",
  "allIcid": [
    516847
  ],
  },
  "sbrs": "None"
}
},
{
  "attributes": {
    "hostName": "",
    "mid": [
      2325164
    ],
  },
  "isCompleteData": "N/A",
  "messageStatus": {
    "2325164": "Dropped By Anti-Virus"
  },
  "recipientMap": {
    "2325164": [
      "testuser1@abc.com"
    ]
  },
  },
  "senderIp": "10.10.4.46",
  "mailPolicy": [
    "DEFAULT"
  ],
  },

```

```

        "senderGroup": "None",
        "subject": "Shipping confirmation: PIR-54787L-83296",
        "friendly_from": [
            "payment@geiger-sicher.de"
        ],
        "senderDomain": "testdomain.com",
        "direction": "outgoing",
        "icid": 516847,
        "morDetails": {},
        "replyTo": "N/A",
        "timestamp": "02 Mar 2021 13:14:34 (GMT +05:30)",
        "messageID": {
            "2325164": "<9o6bdsq4jgrk@geiger-sicher.de>"
        },
        "verdictChart": {
            "2325164": "11500000"
        },
        "recipient": [
            "testuser1@abc.com"
        ],
        "sender": "user@testdomain.com",
        "serialNumber": "42155830541672825266-ABFF53B45FDE",
        "allIcid": [
            516847
        ],
        "sbrs": "None"
    }
}
]
}

```

隔離

隔離の API クエリを使用すると、隔離のメッセージに関するすべての情報を取得できます。リリース、削除、および終了の遅延を行うことで、メッセージに対してアクションを実行することができます。隔離の API は次のように広く分類されます。

- [スパム隔離用 API \(38 ページ\)](#)
- [その他の隔離用 API \(66 ページ\)](#)

スパム隔離用 API

複数の属性と一致したり、メッセージを削除またはリリースしたりする、スパム隔離内のメッセージをクエリできます。

- [メッセージの検索 \(39 ページ\)](#)
- [メッセージの詳細の取得 \(42 ページ\)](#)
- [メッセージのリリース \(45 ページ\)](#)
- [メッセージの削除 \(44 ページ\)](#)
- [セーフリスト エントリとブロックリスト エントリの検索 \(46 ページ\)](#)

- [セーフリストとブロックリスト エントリの追加、編集、付加 \(50 ページ\)](#)
- [セーフリストまたはブロックリスト エントリの削除 \(62 ページ\)](#)

メッセージの検索

複数の属性と一致するスパム隔離内のメッセージを検索することができます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/messages?resource_attribute
----	--

サポート対象のリソース属性	時間	<p>このパラメータは必須です。すべての API クエリでこのパラメータを使用します。</p> <ul style="list-style-type: none"> • <code>startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</code> <p>この期間内に隔離されたメッセージ。</p>
	隔離タイプ	<ul style="list-style-type: none"> • <code>quarantineType=<value></code> <p>承認される値は <code>spam</code> です。</p> <p><code>quarantineType=spam</code></p>
	ソート	<p>結果を順序付けする値と方向を指定できます。</p> <ul style="list-style-type: none"> • <code>orderBy=<value></code> <p>有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • <code>from_address</code> • <code>to_address</code> • <code>subject</code> <ul style="list-style-type: none"> • <code>orderDir=<value></code> <p>有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • <code>asc</code> • <code>desc</code>
	遅延読み込み	<p>次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。</p> <ul style="list-style-type: none"> • <code>offset=<value></code> <p>オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。</p> <ul style="list-style-type: none"> • <code>limit=<value></code> <p>取得するレコードの数を指定します。</p>
	エンベロープ受信者	

		<ul style="list-style-type: none"> • envelopeRecipientFilterOperator=<value> 有効な値は次のとおりです。 <ul style="list-style-type: none"> • contains • is • begins_with • ends_with • does_not_contain • envelopeRecipientFilterValue=<value> 検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。 envelopeRecipientFilterValue=user
	フィルタリング	<p>フィルタ パラメータは応答に含まれるデータを制限します。</p> <ul style="list-style-type: none"> • filterOperator=<value> 検索対象の値。有効な値は次のとおりです。 <ul style="list-style-type: none"> • contains • is • begins_with • ends_with • does_not_contain • filterValue=<value> 検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。 filterValue=abc.com
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次の例では、時間範囲、順序、隔離タイプ、オフセット、制限パラメータを指定して、隔離メッセージを取得するクエリを示します。

サンプル リクエスト

```
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

```

サンプル応答

```

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
    }
  ]
}

```

メッセージの詳細の取得

複数の属性と一致するメッセージの詳細を取得することができます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/messages?resource_attribute
----	--

サポート対象のリソース属性	隔離タイプ	<ul style="list-style-type: none"> • quarantineType=<value> 承認される値はspam です。 quarantineType=spam
	メッセージ ID	自身の詳細を取得するメッセージの mid を指定する必要があります。 <ul style="list-style-type: none"> • mid=<value>
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次の例では、特定のメッセージの詳細を取得するクエリを示します。

サンプル リクエスト

```
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
```

サンプル応答

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

{
  "data": {
    "attributes": {
      "envelopeRecipient": [
        "av_deliver@vm30bsd0004.ibqa"
      ],
      "toAddress": [
        "Surya Allena <sallena@cisco.com>"
      ],
      "attachments": [],
      "messageBody": "Received: from c680q07.ibqa ([10.76.71.196])\r\n by
```

```

esa.cisco.com with
    ESMTP; 16 Nov 2018 13:58:55 +0000<br />\nIronPort-SDR:
DjDeJA8ZkD90oA9x+n3eGd9Qa/nliZ1dL
    MyxB7dsrdq8oTnn8YSi5amR2qihbeq2eJwvVjskfl\r\n KE7TdyCXsokg==<br
/>\nX-IronPort-AV:
    E=Sophos;i=\\"5.56,240,1539648000\\"; \r\n    d=\\"scan\\";a=\\"22180\\"<br
/>\nIronPort-SDR:
    PPj7KDz4Ur8W2ne2fWF/wSOUBwnY3x1XaBz/ryR/98vI6NPraAsA5q7vzUzyaYFpRCWGgfyJaZ\r\n
    4UIJbt91/
    WFccoWcqq086zz6rYcRASCSM=<br />\nIronPort-PHdr:
=?us-ascii?q?9a23=3Az7tnkBDwN1EwuviG0ROD
    UyQJP3Nli/DPJgcQr6?=\r\n
=?us-ascii?q?AfoPdwSPT7pMbcNUDSrc9gkEXOFd2Cra4c26y06+jJYi8p2d65",
    "date": "16 Nov 2018 13:58 (GMT)",
    "fromAddress": [
        "testuser <testuser@cisco.com>"
    ],
    "subject": "[SUSPICIOUS MESSAGE] [SUSPECTED SPAM] Testing VOF"
},
"mid": 1755
}
}

```

メッセージの削除

さまざまな属性と一致するメッセージを削除することができます。次に、構文とサポート対象の属性を示します。

概要	DELETE /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	メッセージ ID	<p>削除アクションを有効にするためには、このパラメータを使用する必要があります。</p> <ul style="list-style-type: none"> "mids": [<value>] <p>メッセージの <code>mid</code> を指定します。</p>
	隔離タイプ	<p>"quarantineType": "value"</p> <p>有効な値は <i>spam</i> です。</p>
要求本文	<pre>{ "quarantineType": "spam", "mids": [<mid>] }</pre>	
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、メッセージを削除するクエリを示します。

サンプル リクエスト

```
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]
}
```

サンプル応答

```
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
  }
}
```

メッセージのリリース

mid属性と一致するメッセージをリリースできます。次に、構文とサポート対象の属性を示します。

概要	POST /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	メッセージ ID	リリースアクションを有効にするためには、このパラメータを使用する必要があります。 <ul style="list-style-type: none"> "mids": [<value>] メッセージの mid を指定します。
	操作	"action": "value" 有効な値は <i>release</i> です。
	隔離タイプ	"quarantineType": "value" 有効な値は <i>spam</i> です。

要求本文	{ "action": "release", "quarantineType": "spam", "mids": [<mid>] }
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

例

次の例では、mid パラメータを指定して特定のメッセージをリリースするクエリを示します。

サンプル リクエスト

```
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]
}
```

サンプル 応答

```
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
  }
}
```

セーフリスト エントリとブロックリスト エントリの検索

API クエリを指定してセーフリストとブロックリストのエントリを取得することができます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/safelist?resource_attribute GET /api/v2.0/quarantine/blocklist?resource_attribute	
サポート対象のリソース属性	操作	<ul style="list-style-type: none"> • action=<value> 有効な値はviewです。
	隔離タイプ	quarantineType=<value> 有効な値はspamです。
	表示方法	viewBy=<value> 有効な値はsenderとrecipientです。
	オーダー基準	orderBy=<value> 有効な値はsenderとrecipientです。
	遅延読み込み	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> • offset=<value> オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。 <ul style="list-style-type: none"> • limit=<value> 取得するレコードの数を指定します。
	オーダー	orderDir=<value> 有効な値は次のとおりです。 <ul style="list-style-type: none"> • asc • desc
	検索	これは orderBy=recipient 属性のみでサポートされています。 search=<value> これはユーザー定義の値です。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

受信者別にセーフリストとブロックリストのエントリを表示する。

次の要求例では、セーフリスト エントリを受信者別に取得するクエリを示します。ブロックリストと同じクエリを使用し、ブロックリスト エントリを受信者別に取得します。次に、クエリの例を示します。

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

サンプル リクエスト

```
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
```

サンプル応答

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

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

送信者別にセーフリストとブロックリストのエントリを表示する。

次の要求例では、ブロックリスト エントリを送信者別に取得するクエリを示します。セーフリストと同じクエリを使用し、ブロックリスト エントリを受信者別に取得します。次に、クエリの例を示します。


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

サンプル リクエスト

```
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
```

サンプル 応答

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

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

セーフリストとブロックリスト エントリの追加、編集、付加

セーフリストとブロックリストのエントリを追加、編集、および付加できます。レコードが存在しない場合は、エントリが追加されます。レコードが存在する場合は、エントリを編集します。次に、構文とサポート対象の属性を示します。

概要	POST /api/v2.0/quarantine/safelist?resource_attribute POST /api/v2.0/quarantine/blocklist?resource_attribute	
サポート対象のリソース属性	操作	<ul style="list-style-type: none"> • action=<value> 有効な値は次のとおりです。 <ul style="list-style-type: none"> • add • edit • append
	隔離タイプ	quarantineType=<value> 有効な値は <i>spam</i> です。
	表示方法	viewBy=<value> 有効な値は <i>sender</i> と <i>recipient</i> です。
	受信者アドレス	"recipientAddresses": ["value", "value", ...] これはユーザー定義の値です。複数の値を入力することができます。
	受信者リスト	"recipientList": ["value", "value", ...] これはユーザー定義の値です。複数の値を入力することができます。
	送信者アドレス	"senderAddresses": ["value", "value", ...] これはユーザー定義の値です。複数の値を入力することができます。
	送信者リスト	"senderList": ["value", "value", ...] これはユーザー定義の値です。複数の値を入力することができます。

要求本文	<p>新しい受信者エントリの追加。</p> <pre>{ "action": "add", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }</pre> <p>新しい送信者エントリの追加。</p> <pre>{ "action": "add", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }</pre> <p>新しい受信者エントリの編集。</p> <pre>{ "action": "edit", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }</pre> <p>新しい送信者エントリの編集。</p> <pre>{ "action": "edit", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }</pre> <p>新しい受信者エントリの付加。</p> <pre>{ "action": "append", "quarantineType": "spam", "recipientAddresses": ["value","value"], "senderList": ["value"], "viewBy": "recipient" }</pre> <p>新しい送信者エントリの付加。</p> <pre>{ "action": "append", "quarantineType": "spam", "senderAddresses": ["value","value"], "recipientList": ["value"], "viewBy": "sender" }</pre>
要求ヘッダー	Host、Accept、Authorization

応答ヘッダー	Content-Type、Content-Length、Connection
--------	--

例

- [受信者セーフリスト エントリの追加 \(52 ページ\)](#)
- [送信者セーフリスト エントリの追加 \(53 ページ\)](#)
- [受信者ブロックリスト エントリの追加 \(54 ページ\)](#)
- [送信者ブロックリスト エントリの追加 \(54 ページ\)](#)
- [受信者セーフリスト エントリの編集 \(55 ページ\)](#)
- [送信者セーフリスト エントリの編集 \(56 ページ\)](#)
- [受信者ブロックリスト エントリの編集 \(57 ページ\)](#)
- [送信者ブロックリスト エントリの編集 \(58 ページ\)](#)
- [受信者セーフリスト エントリの付加 \(59 ページ\)](#)
- [送信者セーフリスト エントリの付加 \(59 ページ\)](#)

受信者セーフリスト エントリの追加

次の要求例では、セーフリスト エントリを追加するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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"
    ]
  }
}

```

送信者セーフリスト エントリの追加

次の要求例では、セーフリスト エントリを追加するクエリを示します。

サンプル リクエスト

```

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"
}

```

サンプル応答

```

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"
        ]
    }
}

```

受信者ブロックリスト エントリの追加

次の要求例では、ブロックリスト エントリを追加するクエリを示します。

サンプル リクエスト

```

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"
}

```

サンプル応答

```

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"
    ]
  }
}

```

送信者ブロックリスト エントリの追加

次の要求例では、ブロックリスト エントリを追加するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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"
    ]
  }
}
```

受信者セーフリスト エントリの編集

次の要求例では、セーフリスト エントリを追加するクエリを示します。

サンプル リクエスト

```
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"
}

```

サンプル応答

```

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"
    ]
  }
}

```

送信者セーフリストエントリの編集

次の要求例では、セーフリスト エントリを追加するクエリを示します。

サンプル リクエスト

```

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"
}

```

サンプル応答


```
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"
    ]
  }
}
```

受信者ブロックリスト エントリの編集

次の要求例では、ブロックリスト エントリを編集するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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"
    ]
  }
}

```

送信者ブロックリスト エントリの編集

次の要求例では、ブロックリスト エントリを編集するクエリを示します。

サンプル リクエスト

```

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"
}

```

サンプル応答

```

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"
    ]
  }
}

```

```
}  
}
```

受信者セーフリスト エントリの付加

次の要求例では、セーフリスト エントリを付加するクエリを示します。

サンプル リクエスト

```
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"  
}
```

サンプル応答

```
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"  
    ]  
  }  
}
```

送信者セーフリスト エントリの付加

次の要求例では、セーフリスト エントリを付加するクエリを示します。

サンプル リクエスト

受信者ブロックリスト エントリの付加

```
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"
}
```

サンプル応答

```
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"
    ]
  }
}
```

受信者ブロックリスト エントリの付加

次の要求例では、ブロックリスト エントリを付加するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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"
    ]
  }
}
```

送信者ブロックリスト エントリの付加

次の要求例では、ブロックリスト エントリを付加するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

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

セーフリストまたはブロックリスト エントリの削除

```
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"
    ]
  }
}
```

セーフリストまたはブロックリスト エントリの削除

送信者または受信者のいずれかのリストからセーフリストまたはブロックリストのエントリを削除する API クエリを実行できます。

概要	DELETE /api/v2.0/quarantine/safelist?resource_attribute DELETE /api/v2.0/quarantine/blocklist?resource_attribute	
サポート対象のリソース属性	隔離タイプ	quarantineType=<value> 有効な値は <i>spam</i> です。
	受信者リスト	"recipientList": ["value", "value", ...] これはユーザー定義の値です。複数の値を入力することができます。
	送信者リスト	"senderList": ["value", "value", ...] これはユーザー定義の値です。複数の値を入力することができます。
	表示方法	"viewBy": "value" 有効な値は <i>sender</i> と <i>recipient</i> です。 .

要求本文	<p>受信者エントリの削除。</p> <pre>{ "quarantineType": "spam", "recipientList": ["value", "value"], "viewBy": "recipient" }</pre> <p>送信者エントリの削除。</p> <pre>{ "quarantineType": "spam", "senderList": ["value"], "viewBy": "sender" }</pre>
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

次の API を使用できます。

- [受信者セーフリスト エントリの削除 \(63 ページ\)](#)
- [送信者セーフリスト エントリの削除 \(64 ページ\)](#)
- [受信者ブロックリスト エントリの削除 \(65 ページ\)](#)
- [送信者ブロックリスト エントリの削除 \(65 ページ\)](#)

受信者セーフリスト エントリの削除

次の要求例では、セーフリスト エントリを削除するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

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

送信者セーフリストエントリの削除

```

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
  }
}

```

送信者セーフリストエントリの削除

次の要求例では、セーフリスト エントリを削除するクエリを示します。

サンプル リクエスト

```

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"
}

```

サンプル応答

```

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"
    ]
  }
}

```



```
}  
}
```

受信者ブロックリスト エントリの削除

次の要求例では、ブロックリスト エントリを削除するクエリを示します。

```
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"  
}
```

サンプル応答

```
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  
  }  
}
```

送信者ブロックリスト エントリの削除

次の要求例では、ブロックリスト エントリを削除するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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"
    ]
  }
}
```

その他の隔離用 API

次のクエリには、クエリ文字列の一部として **quarantineType** リソース名が含まれます。

隔離クエリは、検索、ソート、オフセット、および遅延読み込みをサポートします。

- [メッセージの検索 \(67 ページ\)](#)
- [メッセージの詳細の取得 \(74 ページ\)](#)
- [メッセージの移動 \(76 ページ\)](#)
- [隔離からメッセージの終了を遅延する \(77 ページ\)](#)
- [隔離内のメッセージのコピーを送信する \(79 ページ\)](#)
- [添付ファイルのダウンロード \(81 ページ\)](#)
- [メッセージの削除 \(82 ページ\)](#)
- [メッセージのリリース \(83 ページ\)](#)
- [ルール サマリーの表示 \(85 ページ\)](#)
- [ルール ID に基づく検索 \(86 ページ\)](#)
- [ルール サマリーからのメッセージをリリース \(89 ページ\)](#)

- [ルールサマリーからメッセージを削除 \(91 ページ\)](#)

メッセージの検索

複数の属性と一致する他の隔離内のメッセージを検索することができます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/messages?resource_attribute
----	--

サポート対象のリソース属性	時間	このパラメータは必須です。すべての API クエリは、このパラメータと共に使用する必要があります。 <ul style="list-style-type: none"> • startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z
	検索する隔離	このパラメータは検索する隔離を指定します。 <ul style="list-style-type: none"> • quarantines=<value, value, ...> 有効な値は次のとおりです。 Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
	件名	<ul style="list-style-type: none"> • subjectFilterBy=<value> 有効な値は次のとおりです。 contains starts_with ends_with matches_exactly does_not_contain does_not_start_with does_not_end_with does_not_match <ul style="list-style-type: none"> • subjectFilterValue=<value> これはユーザー定義の値です。
	元の ESA	originatingEsaIp=<value> メッセージが処理された ESA の IP アドレスを指定することができます。
	添付の詳細	

	<ul style="list-style-type: none"> • <code>attachmentName=<value></code> これはユーザ一定義の値です。 • <code>attachmentSizeFilterBy=<value></code> 有効な値は次のとおりです。 <code>range</code> <code>less_than</code> <code>more_than</code> • <code>attachmentSizeFromValue=<value_in_KB></code> これはユーザ一定義の値です。添付ファイルのサイズを KB で指定します。これは次の場合に適用可能です。 <ul style="list-style-type: none"> • <code>attachmentSizeFilterBy</code> で <code>range</code> 属性を選択した場合 <code>attachmentSizeFilterBy=range</code> • <code>attachmentSizeFilterBy</code> で <code>more_than</code> 属性を選択した場合 <code>attachmentSizeFilterBy=more_than</code> • <code>attachmentSizeToValue=<value_in_KB></code> これはユーザ一定義の値です。添付ファイルのサイズを KB で指定します。これは次の場合に適用可能です。 <ul style="list-style-type: none"> • <code>attachmentSizeFilterBy</code> で <code>range</code> 属性を選択した場合 <code>attachmentSizeFilterBy=range</code> • <code>attachmentSizeFilterBy</code> で <code>less_than</code> 属性を選択した場合 <code>attachmentSizeFilterBy=less_than</code>
隔離タイプ	<ul style="list-style-type: none"> • <code>quarantineType=<value></code> 承認される値は <code>pvo</code> です。 <code>quarantineType=pvo</code>
ソート	

		<p>結果を順序付けする値と方向を指定できます。</p> <ul style="list-style-type: none"> • orderBy=<value> <p>値は次のとおりです。</p> <pre>sender subject received scheduledExit size</pre> <ul style="list-style-type: none"> • orderDir=<value> <p>値は次のとおりです。</p> <pre>asc desc</pre>
遅延読み込み		<p>次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。</p> <ul style="list-style-type: none"> • offset=<value> <p>オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。</p> <ul style="list-style-type: none"> • limit=<value> <p>取得するレコードの数を指定します。</p>
エンベロープ受信者		<ul style="list-style-type: none"> • envelopeRecipientFilterBy=<value> <p>有効な値は次のとおりです。</p> <pre>contains starts_with ends_with matches_exactly does_not_contain does_not_start_with does_not_end_with does_not_match</pre> <ul style="list-style-type: none"> • envelopeRecipientFilterValue=<value> <p>検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。</p> <pre>envelopeRecipientFilterValue=user</pre>

	エンベ ロープ送 信者	<ul style="list-style-type: none"> • envelopeSenderFilterBy=<value> 有効な値は次のとおりです。 contains starts_with ends_with matches_exactly does_not_contain does_not_start_with does_not_end_with does_not_match • envelopeSenderFilterValue=<value> 検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。 envelopeRecipientFilterValue=user
要求ヘッ ダー		Host、Accept、Authorization
応答ヘッ ダー		Content-Type、Content-Length、Connection

例

次の例では、時間範囲、順序、隔離タイプ、オフセットと制限、元の ESA パラメータを指定して、他のポリシー、ウイルス、アウトブレイク隔離内のメッセージを取得するクエリを示します。

サンプル リクエスト

```
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
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 09:01:11 GMT
Content-type: application/json
Content-Length: 13093
```

```

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

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

```



```
    "size": "312.69K"
  },
  "mid": 161
},
{
  "attributes": {
    "received": "21 Nov 2018 10:09 (GMT)",
    "sender": "usr2@sender.com",
    "subject": "[SUSPICIOUS MESSAGE] Test mail.",
    "esaHostName": "esa01",
    "inQuarantines": "Policy",
    "scheduledExit": "21 Dec 2018 10:09 (GMT)",
    "originatingEsaIp": "10.8.91.15",
    "quarantineForReason": [
      "Content Filter: 'url'"
    ],
    "esaMid": 354,
    "recipient": [
      "eriferma@mail.qa.sgg.cisco.com"
    ],
    "quarantineForReasonDict": [
      {
        "reason": [
          "Content Filter: 'url'"
        ],
        "quarantineName": "Policy"
      }
    ],
    "size": "312.69K"
  },
  "mid": 153
},
{
  "attributes": {
    "received": "20 Nov 2018 12:42 (GMT)",
    "sender": "test@irontest.com",
    "subject": "[WARNING: ATTACHMENT UNSCANNED]sadsafasd",
    "esaHostName": "esa01",
    "inQuarantines": "Policy",
    "scheduledExit": "20 Dec 2018 12:42 (GMT)",
    "originatingEsaIp": "10.8.91.15",
    "quarantineForReason": [
      "Message is unscannable by AMP - Service Not Available"
    ],
    "esaMid": 254,
    "recipient": [
      "test2@irontest.com"
    ],
    "quarantineForReasonDict": [
      {
        "reason": [
          "Message is unscannable by AMP - Service Not Available"
        ],
        "quarantineName": "Policy"
      }
    ],
    "size": "330.19K"
  },
  "mid": 143
},
{
  "attributes": {
    "received": "20 Nov 2018 12:41 (GMT)",
    "sender": "test@irontest.com",
```

```

    "subject": "[WARNING: ATTACHMENT UNSCANNED]sadsafasd",
    "esaHostName": "esa01",
    "inQuarantines": "Policy",
    "scheduledExit": "20 Dec 2018 12:41 (GMT)",
    "originatingEsaIp": "10.8.91.15",
    "quarantineForReason": [
      "Message is unscannable by AMP - Service Not Available"
    ],
    "esaMid": 251,
    "recipient": [
      "test2@irontest.com"
    ],
    "quarantineForReasonDict": [
      {
        "reason": [
          "Message is unscannable by AMP - Service Not Available"
        ],
        "quarantineName": "Policy"
      }
    ],
    "size": "330.19K"
  },
  "mid": 140
}
]
}

```

メッセージの詳細の取得

複数の属性と一致するメッセージの詳細を取得することができます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	隔離タイプ	<ul style="list-style-type: none"> quarantineType=<value> 承認される値は pvo です。 quarantineType=pvo
	メッセージ ID	自身の詳細を取得するメッセージの mid を指定する必要があります。 <ul style="list-style-type: none"> mid=<value>
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、特定のメッセージの詳細を取得するクエリを示します。

サンプル リクエスト

```
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
```

サンプル応答

```
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": [
          "eriferma@mail.qa.sgg.cisco.com"
        ],
        "sender": "usr2@sender.com",
        "subject": "[SUSPICIOUS MESSAGE] Test mail."
      },
      "messageBody": "This is a demo mail. http://bit.ly/2zs6KAq<br>\n",
      "headers": "IronPort-SDR:
4Sh6scwkvc+t4BgD5601B/l5cTAMkUtJtFAY+/Sk6YwaaSxL2TOzEKHwsn+6KxG+kV2Zg
75sMX<br> DkgdFZYTDPIft9VvRsTl0Fz+N6rRgHCB4=<br>X-IPAS-Result:
=?us-ascii?q?A0GSTP/juz9b/+pj4QpOH
oMagXSCU4gely0HhysBAQEBA?=<br>
```

```

=?us-ascii?q?QEBeoIOAQEBPQUEAgEFBQEDAwECAGEBLTEkOCyBFxhDiEefiY8MAQ
EBAQYBA?=<br>
=?us-ascii?q?QEBAR2PIQEBhH8FiRODF4FVgUqBJ02RGYVLhA55AYEAgTcBAQE?=<br>
Subject: [SUSPICIOUS MESSAGE] Test mail.<br>Received: from client.cisco.com

(HELO pod1224-client05.ibwsa) ([10.225.99.234])<br> by pod0090-esa01
with ESMTTP; 21 Nov 2018 07:01:34 +0000<br>Message-ID: <194652.955603914
-sendEmail@pod1224-client05><br>From: \"usr2@sender.com\" <usr2@sender
.com><br>To: \"eriferina@mail.qa.sgg.cisco.com\" <testclient@cisco.com
><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
}
}
}

```

メッセージの移動

複数の属性に一致するメッセージを移動することができます。次に、構文とサポート対象の属性を示します。

概要	POST /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	メッセージ ID	<p>削除アクションを有効にするためには、このパラメータを使用する必要があります。</p> <ul style="list-style-type: none"> • "mids": [<value>] <p>メッセージの mid を指定します。</p>
	隔離タイプ	<p>"quarantineName": "<value>"</p> <p>有効な値は <i>pvo</i> です。</p>
	宛先隔離名	<p>"destinationQuarantineName": "<value>"</p> <p>有効な値は次のとおりです。</p> <p>Outbreak</p> <p>Virus</p> <p>File+Analysis</p> <p>Unclassified</p> <p>Policy</p> <p><user-defined-quarantine></p>
要求本文	<pre>{ "action": "move", "destinationQuarantineName": "<value>", "mids": [<value>], "quarantineName": "<value>", "quarantineType": "pvo" }</pre>	
要求ヘッダー	Host、Accept、Authorization	

応答ヘッダー	Content-Type、Content-Length、Connection
--------	--

例

次の例では、メッセージを移動するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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"
  }
}
```

隔離からメッセージの終了を遅延する

隔離からメッセージの終了を遅延することができます。次に、構文とサポート対象の属性を示します。

概要	POST /api/v2.0/quarantine/messages?resource_attribute
----	---

サポート対象のリソース属性	メッセージ ID	<ul style="list-style-type: none"> "mids": [value] メッセージの mid を指定します。
	隔離タイプ	"quarantineType": "value" 有効な値は <i>pvo</i> です。
	隔離名	"quarantineName": "value" 有効な値は次のとおりです。 Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
	遅延	"delay": "value" 有効な値は、 <i>8h</i> 、 <i>24h</i> 、 <i>48h</i> 、または <i>1w</i> です。
要求本文	<pre>{ "action": "delay", "delay": "<value>", "mids": [<value>], "quarantineName": "<value>", "quarantineType": "pvo" }</pre>	
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、メッセージの終了を遅延するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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"
  }
}
```

隔離内のメッセージのコピーを送信する

Eメールアドレスに隔離内のメッセージのコピーを送信することができます。次に、構文とサポート対象の属性を示します。

概要	POST /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	メッセージ ID	<ul style="list-style-type: none"> "mids": [value] メッセージの mid を指定します。
	隔離タイプ	"quarantineType": "value" 有効な値は <i>pvo</i> です。
	隔離名	"quarantineName": "value" 有効な値は次のとおりです。 Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
	受信者	"recipients":["value", "value", ...] これはユーザー定義の値です。受信者のEメールアドレスを入力します。

要求本文	<pre>{ "action": "sendCopy", "mids": [value], "quarantineName": "value", "quarantineType": "pvo", "recipients": ["value"] }</pre> <p>アウトブレイクの場合、メッセージ本文にこのオプション属性を追加することができます。</p> <p>"sendToCisco": <value></p> <p>有効な値は <i>true</i> です。次に例を示します。</p> <pre>{ "action": "sendCopy", "mids": [value], "quarantineName": "value", "quarantineType": "pvo", "recipients": ["value"], }</pre>
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

例

次の例では、未分類の隔離内のメッセージのコピーを E メール アドレスに送信するクエリを示します。

サンプル リクエスト

```
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"]
}
```

サンプル応答

```
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
  }
}

```

添付ファイルのダウンロード

隔離内のメッセージに付随する添付ファイルをダウンロードできます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	メッセージ ID	<ul style="list-style-type: none"> • mid=<value> メッセージの mid を指定します。
	隔離タイプ	quarantineType=<value> 有効な値は <i>pvo</i> です。
	添付ファイル ID	attachmentId=<value> 添付ファイル ID を指定します。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、添付ファイルをダウンロードするクエリを示します。

サンプル リクエスト

```

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

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 12:03:26 GMT
Content-type: application/octet-stream
Content-Disposition: filename="wanacry.exe"
Content-Length: 332511
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

```

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA+AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIGlv
ZGUuZDQ0KJAAAAAAAAAALpLDYzV8kGGb/JBhm/yQGofwkGKb/JCilKGQdZv8kA6E95Bg

```

メッセージの削除

さまざまな属性と一致するメッセージを削除することができます。次に、構文とサポート対象の属性を示します。

概要	DELETE /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	メッセージ ID	<p>削除アクションを有効にするためには、このパラメータを使用する必要があります。</p> <ul style="list-style-type: none"> "mids": [<value>] <p>メッセージの mid を指定します。</p>
	隔離タイプ	<p>"quarantineType": "value"</p> <p>有効な値は <i>pvo</i> です。</p>
	隔離名	<p>"quarantineName": "<value>"</p> <p>有効な値は次のとおりです。</p> <p>Outbreak</p> <p>Virus</p> <p>File+Analysis</p> <p>Unclassified</p> <p>Policy</p> <p><user-defined-quarantine></p>
要求本文	<pre>{ "mids": [<mid>], "quarantineName": "<value>", "quarantineType": "pvo" }</pre>	
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、特定の隔離内の特定のメッセージを削除するクエリを示します。

サンプル リクエスト

```
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"
}
```

サンプル応答

```
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
  }
}
```

メッセージのリリース

複数の属性に一致するメッセージをリリースすることができます。次に、構文とサポート対象の属性を示します。

概要	POST /api/v2.0/quarantine/messages?resource_attribute
----	---

サポート対象のリソース属性	メッセージ ID	リリースアクションを有効にするためには、このパラメータを使用する必要があります。 • "mids": [<value>] メッセージの mid を指定します。
	隔離タイプ	"quarantineType": "pvo" 有効な値は <i>pvo</i> です。
	隔離名	"quarantineName": "<value>" 有効な値は次のとおりです。 Outbreak Virus File+Analysis Unclassified Policy <user-defined-quarantine>
	操作	"action": "value" 有効な値は <i>release</i> です。
要求本文	<pre>{ "action": "release", "mids": [<mid>], "quarantineName": "<value>", "quarantineType": "pvo" }</pre>	
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、mid パラメータを指定して特定のメッセージをリリースするクエリを示します。

サンプル リクエスト

```
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",
}
```

サンプル応答

```
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
  }
}
```

ルール サマリーの表示

現在隔離内にあるメッセージの詳細をクエリすることができます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/rules?resource_attribute	
サポート対象のリソース属性	隔離タイプ	quarantineType=<value> 有効な値は <i>pvo</i> です。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、隔離内のメッセージのメッセージ統計情報を取得するクエリを示します。

サンプル リクエスト

```
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
```

サンプル応答

```
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
    }
  ]
}
```

ルール ID に基づく検索

特定のルール ID に一致する隔離内のメッセージを検索することができます。次に、構文とサポート対象の属性を示します。

概要	GET /api/v2.0/quarantine/rules_search?resource_attribute
----	--

サポート対象のリソース属性	隔離タイプ	quarantineType=<value> 有効な値は <i>pvo</i> です。
	ルール ID	ruleId=<value> これはユーザー定義の値です。
	ソート	結果を順序付けする値と方向を指定できます。 <ul style="list-style-type: none"> orderBy=<value> 有効な値は次のとおりです。 received orderDir=<value> 有効な値は次のとおりです。 asc desc
	遅延読み込み	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> offset=<value> オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。 limit=<value> 取得するレコードの数を指定します。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、ルールパラメータに一致するメッセージを取得するクエリを示します。

サンプル リクエスト

```
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
```

サンプル応答

```

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

```

```

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

```



```

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

```

ルール サマリーからのメッセージをリリース

複数の属性に一致するルールサマリーからメッセージをリリースすることができます。次に、構文とサポート対象の属性を示します。

概要	POST /api/v2.0/quarantine/rules?resource_attribute	
サポート対象のリソース属性	ルール ID	<ul style="list-style-type: none"> "ruleId": ["value", "value", ...] ルール ID を指定します。
	隔離タイプ	quarantineType=<value> 有効な値は <i>pvo</i> です。
	操作	"action": "value" 有効な値は <i>release</i> です。

要求本文	{ "action" : "release", "quarantineType": "pvo", "ruleId": ["value"] }
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

例

次の例では、メッセージをリリースするクエリを示します。

サンプル リクエスト

```
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"]
}
```

サンプル応答

```
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
  }
}
```

ルール サマリーからメッセージを削除

特定の属性に一致するルールサマリーからメッセージを削除することができます。次に、構文とサポート対象の属性を示します。

概要	DELETE /api/v2.0/quarantine/rules?resource_attribute	
サポート対象のリソース属性	ルール ID	<ul style="list-style-type: none"> "ruleId": ["value", "value", ...] ルール ID を指定します。
	隔離タイプ	quarantineType=<value> 有効な値は <i>pvo</i> です。
要求本文	<pre>{ "quarantineType": "pvo", "ruleId": ["value"] }</pre>	
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

例

次の例では、ルール サマリーからメッセージを削除するクエリを示します。

サンプル リクエスト

```
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"]
}
```

サンプル 応答

```
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
  }
}

```

ロギング API

電子メールゲートウェイから特定のログ情報を取得できます。ロギングの各種APIカテゴリは次のとおりです。

- [電子メールゲートウェイのログサブスクリプション詳細の取得 \(92 ページ\)](#)
- [特定のログサブスクリプションのすべてのログファイルの取得 \(93 ページ\)](#)
- [URL を使用したログファイルの取得 \(95 ページ\)](#)

電子メールゲートウェイのログサブスクリプション詳細の取得

個別の属性を指定して、電子メールゲートウェイに設定されているすべてのログサブスクリプションの詳細を次のように取得できます。

概要		GET /esa/api/v2.0/config/logs/subscriptions
サポート対象のリソース属性	取得方法	<p>これは省略可能なパラメータです。</p> <p>選択可能な値は次のとおりです。</p> <p>aws_s3_push, scp_push, manual, ftp_push, syslog_push</p> <p>retrievalMethod>manual</p> <p>このパラメータを使用して、対応する取得方法で設定されたログサブスクリプションを一覧表示できます。</p>
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次に、電子メールゲートウェイで設定されているすべてのログサブスクリプションの詳細を取得するクエリの例を示します。

サンプル リクエスト

```

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

```

サンプル応答

```

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"
    }
  ]
}

```

特定のログサブスクリプションのすべてのログファイルの取得

次に説明するように、異なる属性を持つ特定のログサブスクリプションのすべてのログファイルの詳細を取得できます。



- (注) この API は、電子メールゲートウェイで手動ログ取得方式を使用して設定されたログサブスクリプションにのみ適用されます。API は、ロールオーバーされたログファイルのみをリストします。[電子メールゲートウェイのログサブスクリプション詳細の取得 \(92 ページ\)](#) API のログサブスクリプション名から取得した応答の `name` 属性を使用する必要があります。

概要	GET /esa/api/v2.0/logs/<log_subscription_name>/?resource_attribute
----	--

サポート対象のリソース属性	時間	これは省略可能なパラメータです。 startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z このパラメータを使用すると、指定した期間内に生成されたログファイルをリストできます。
	ファイルハッシュ	これは省略可能なパラメータです。 computeHash=True このパラメータは、ログファイルのファイルハッシュ値を応答に含める必要がある場合にのみ使用できます。 (注) このパラメータのデフォルト値は False です。
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次に、特定のタイムスタンプの後に変更されたすべてのログファイルの詳細を取得するクエリの例を示します。

サンプル リクエスト

```
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
```

サンプル応答

```
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
    }
  ]
}

```

URL を使用したログファイルの取得

[特定のログサブスクリプションのすべてのログファイルの取得 \(93 ページ\)](#) API から取得した応答の `downloadUrl` 属性を使用して、ログファイルの内容を取得できます。



- (注) この API は、電子メールゲートウェイで手動ログ取得方式を使用して設定されたログサブスクリプションにのみ適用されます。



- (注) この API を使用して頻繁に入力されるログファイル（テキストメールログなど）を取得する場合は、ログサブスクリプションのロールオーバーパラメータを適切に設定し、サイズの小さいログファイルを定期的にプルすることをお勧めします。ログサブスクリプションでファイルサイズをデフォルト値より大きく設定している場合は、各ファイルの API を順番に呼び出すことをお勧めします。

概要	GET /esa/api/v2.0/logs/<log_subscription_name>/<log_file_name> (注) 特定のログサブスクリプションのすべてのログファイルの取得 (93 ページ) API から取得した応答の <code>downloadUrl</code> 属性を使用する必要があります。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection、Content-Disposition

例

次の例は、特定のログサブスクリプションのすべてのログファイルの取得（93 ページ）API から取得した応答の `downloadUrl` 属性を使用して、ログファイルの内容を取得するためのクエリを示しています。

サンプル リクエスト

```
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
```

サンプル応答

応答には、要求されたログファイルが含まれています。

```
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
```