



Eメール用 API

- [モニタリング API \(1 ページ\)](#)
- [トラッキング API \(26 ページ\)](#)
- [隔離 API \(43 ページ\)](#)
- [構成 API \(97 ページ\)](#)

モニタリング API

- [レポート API \(1 ページ\)](#)
- [スケジュールおよびアーカイブ API \(10 ページ\)](#)

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 \(4 ページ\)](#)
- [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 \(8 ページ\)](#)

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},
        {"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。

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
```

複数のカウンタの複数の値を取得する

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}
    ],
    ...

    "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": [
```

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

```

        {"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タ値を取得します。

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},
        {"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},
      ]
    }
  }
}
}

```

スケジュールおよびアーカイブ API

- [スケジュール API \(10 ページ\)](#)
- [アーカイブ API \(19 ページ\)](#)

スケジュール API

概要	GET /sma/api/v2.0/config/periodic_reports?resource_attribute POST sma/api/v2.0/config/periodic_reports?resource_attribute PUT /sma/api/v2.0/config/periodic_reports/periodic_report_id?resource_attribute DELETE /sma/api/v2.0/config/periodic_reports?resource_attribute
----	--

サポート対象のリ ソース属性	ソート
-------------------	-----

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。

- orderBy=<value>

有効なオプションは次のとおりです。

- periodic_report_display_name

レポートの表示名に基づいて結果を並べ替えます。

- periodic_report_title

レポートのタイプに基づいて結果を並べ替えます。

- periodic_report_type

レポートのタイプに基づいて結果を並べ替えます。

- periodic_report_time_range

レポートの時間範囲に基づいて結果を並べ替えます。

- periodic_report_delivery

レポートの配信オプションに基づいて結果を並べ替えます。

- periodic_report_format

レポートの形式に基づいて結果を並べ替えます。

- periodic_report_schedule_type

レポートに選択したスケジュールのタイプに基づいて結果を並べ替えます。

- periodic_report_tier

必要な電子メールゲートウェイに基づいて結果を並べ替えます。

- periodic_report_next_run_date

レポートのスケジュールオプションに基づいて結果を並べ替えます。

- orderDir=<value>

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。

- asc

		<p>昇順で結果を並べ替えます。</p> <ul style="list-style-type: none"> • desc <p>降順で結果を並べ替えます。</p>
	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>
	Device	<ul style="list-style-type: none"> • device_type=sma <p>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。</p>
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次に、スケジュールレポートクエリのタイプの例をいくつか示します。

- [スケジュールレポートの取得 \(13 ページ\)](#)
- [スケジュールレポート エントリの詳細の取得 \(15 ページ\)](#)
- [スケジュールレポート エントリの追加 \(16 ページ\)](#)
- [スケジュールレポート エントリの編集 \(17 ページ\)](#)
- [スケジュール設定されたレポートの削除 \(18 ページ\)](#)

スケジュールレポートの取得

次に、選択したスケジュールオプションに基づいて降順にソートされた上位 25 のスケジュールレポート エントリのリストを取得する例を示します。

サンプル リクエスト

```
GET /sma/api/v2.0/config/periodic_reports?device_type=sma&
limit=25&offset=0&orderBy=periodic_report_next_run_date&orderDir=desc
HTTP/1.1
```

```

cache-control: no-cache
Postman-Token: 0f917f72-82a4-4b6d-93a9-a1fbd3e72b1b
Authorization: Basic YWRtaW46Q21zY29AMTIzNA==
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: 10.8.159.22:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 12:14:13 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 1797
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
    pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "data":
  {
    "periodic_reports": [{"20191120061727_Content Filters_calendar_week":
      {"periodic_report_type": "phoebe",
        "periodic_report_schedule": {"periodic_report_second": 0, "periodic_report_day": "",
          "periodic_report_month": "", "periodic_report_minute": 0, "periodic_report_weekday": "",

"periodic_report_year": "", "periodic_report_hour": 0, "periodic_report_schedule_type":
          "Daily"},
        "periodic_report_options": {"periodic_report_format": "PDF", "periodic_report_time_range":

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

"periodic_report_year": "", "periodic_report_hour": 0, "periodic_report_schedule_type":
            "Daily"},
          "periodic_report_options": {"periodic_report_format": "PDF", "periodic_report_time_range":

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

```

スケジュール レポート エントリの詳細の取得

次の例では、レポートタイトルに基づいてフィルタ処理され、レポート生成の時間範囲に基づいて降順にソートされた上位 25 のアーカイブレポートのリストを取得する方法を示します。

サンプル リクエスト

```
GET /sma/api/v2.0/config/archived_reports?device_type=sma&filterByTitle
=Content+Filters&limit=25&offset=0&orderBy=periodic_report_generated&orderDir=desc
HTTP/1.1
cache-control: no-cache
Postman-Token: 379beccc-d9de-4cd0-a730-69e59385bf90
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:00:17 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 441
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "data": {
    "meta": {
      "totalCount": 1
    },
    "archived_reports": [{"20191120134501_Content Filters_calendar_month.pdf":
{"periodic_report_format":
"PDF", "periodic_report_type_name": "Content Filters", "periodic_report_generated":
"20 Nov 2019 13:45 (GMT)", "periodic_report_time_range": "Previous calendar month",
"periodic_report_tier": "All Email Appliances", "periodic_report_title": "Content Filters",
"periodic_report_product_type": "esa"}}]
  }
}
```

スケジュール レポート エントリの詳細の表示

次の例は、特定のレポートタイプと時間範囲のスケジュール レポート エントリのプレビュー PDF ドキュメントを取得する方法を示しています。

サンプル リクエスト

```
GET /sma/api/v2.0/config/archived_reports/preview?device_type=
sma&periodic_report_type_name=Outgoing%20Destinations&periodic_report_type=
phoebe&periodic_report_start_date=2017-03-01T15:00:00.000Z&periodic_report_
end_date=2019-07-30T15:00:00.000Z&periodic_report_format=pdf&periodic_report_lang=
en-us&periodic_report_time_range=Custom%20range&periodic_report_rows=
```

```

10&periodic_report_sort_columns=%7B%22table%22:%20%22Outgoing%20Destinations
%20Detail%22,%22column%22:%20%22Total%20Processed%22%7D
HTTP/1.1
cache-control: no-cache
Postman-Token: fc05953b-1552-47ab-be49-4cb2be5fc7c0
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: m680q08.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: Thu, 21 Nov 2019 17:38:08 GMT
Content-type: application/pdf
Content-Disposition: filename="20191121173808_Outgoing Destinations.pdf"
Content-Length: 111240
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email,
portal, cache-control, pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

スケジュール レポート エントリの追加

次の例は、レポートタイプ、レポートタイトル、デバイスタイプ、およびその他のオプションを使用して、スケジュールレポートを追加する方法を示しています。

サンプル リクエスト

```

POST /sma/api/v2.0/config/periodic_reports?device_type=sma
HTTP/1.1
cache-control: no-cache
Postman-Token: 9bc82e3c-b163-4558-923a-f5c03d40a332
Authorization: Basic YWRtaW46Q2lzMjY29AMTIzNA==
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: 10.8.159.22:6080
accept-encoding: gzip, deflate
content-length: 509
Connection: keep-alive
{
  "data":
  {
    "periodic_reports":[{"periodic_report_title":"Content
Filters","periodic_report_type":"phoebe",
"periodic_report_type_name":"Content
Filters","periodic_report_options":{"periodic_report_format":
"pdf","periodic_report_lang":"en-us","periodic_report_time_range":"Previous 7 calendar
days"},
"periodic_report_schedule":{"periodic_report_schedule_type":"daily","periodic_report_minute":0,
"periodic_report_hour":0},"periodic_report_tier":"All Email
Appliances","periodic_report_delivery":

```



```
"Archived Only"]}]
}
}
```

サンプル応答

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Wed, 20 Nov 2019 13:17:31 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 49
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

スケジュール レポート エントリの編集

次に、スケジュールレポート ID を使用してスケジュールされたレポートを変更する例を示します。

サンプル リクエスト

```
PUT /sma/api/v2.0/config/periodic_reports/20191120133634_
Content%20Filters_calendar_week?device_type=sma
HTTP/1.1
cache-control: no-cache
Postman-Token: 7adc6d87-64bd-40d5-827a-3e5d2ea8406b
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 510
Connection: keep-alive

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

サンプル応答

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

```

Date: Wed, 20 Nov 2019 13:44:35 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 49
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

スケジュール設定されたレポートの削除

次に、デバイスタイプとスケジュールレポート ID を使用してスケジュールされたレポートを削除する例を示します。

サンプル リクエスト

```

DELETE /sma/api/v2.0/config/periodic_reports?device_type=sma&
id=20191120135041_Advanced+Malware+Protection+File+Analysis_calendar_week
HTTP/1.1
cache-control: no-cache
Postman-Token: 74cf4ad5-ff0f-4173-894e-a0c2a9c3d6d5
Authorization: Basic YWRtaW46Q21zY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 0
Connection: keep-alive

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 13:54:49 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 52
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "data":
  {
    "message": "1 item deleted successfully"
  }
}

```

アーカイブ API

概要	GET /sma/api/v2.0/config/archived_reports?resource_attribute GET sma/api/v2.0/config/archived_reports/archived_report_id?resource_attribute POST /sma/api/v2.0/config/archived_reports?resource_attribute DELETE /sma/api/v2.0/config/archived_reports?resource_attribute
----	---

サポート対象のリソース属性	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> <p>有効なオプションは次のとおりです。</p> <ul style="list-style-type: none"> • <code>periodic_report_generated</code> <p>レポートが生成された日時に基づいて結果を並べ替えます。</p> • <code>periodic_report_display_name</code> <p>レポートの表示名に基づいて結果を並べ替えます。</p> • <code>periodic_report_format</code> <p>レポートの形式に基づいて結果を並べ替えます。</p> • <code>periodic_report_title</code> <p>レポートのタイプに基づいて結果を並べ替えます。</p> • <code>periodic_report_time_range</code> <p>レポートの時間範囲に基づいて結果を並べ替えます。</p> • <code>periodic_report_type</code> <p>レポートのタイプに基づいて結果を並べ替えます。</p> • <code>periodic_report_tier</code> <p>必要な電子メールゲートウェイに基づいて結果を並べ替えます。</p> • <code>orderDir=<value></code> <p>ソート方向を指定します。</p> <p>有効なオプションは次のとおりです。</p> <ul style="list-style-type: none"> • <code>asc</code> <p>昇順で結果を並べ替えます。</p> • <code>desc</code> <p>降順で結果を並べ替えます。</p>
---------------	-----	--

	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>
	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"> • <code>filterByTitle=<value></code> <p>レポートのタイトルと値でデータをフィルタリングします。</p> <ul style="list-style-type: none"> • <code>filterByReportTypeName=<value></code> <p>レポートのタイプと値でデータをフィルタリングします。</p> <ul style="list-style-type: none"> • <code>filterByTimeRange=<value></code> <p>レポートの時間範囲と値でデータをフィルタリングします。</p>
	Device	<ul style="list-style-type: none"> • <code>device_type=sma</code> <p>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。</p>
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

アーカイブレポートクエリのタイプの例を次に示します。

- [アーカイブレポートの検索 \(22 ページ\)](#)
- [アーカイブレポートの取得 \(22 ページ\)](#)
- [アーカイブレポートエントリの詳細の取得 \(23 ページ\)](#)
- [アーカイブレポートエントリの追加 \(25 ページ\)](#)

- [アーカイブレポートエントリの削除 \(25 ページ\)](#)

アーカイブレポートの検索

次に、レポートタイトルに基づいて、レポートが生成された日時で降順にソートされた上位 25 のアーカイブレポートのリストを検索する例を示します。

サンプル リクエスト

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

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:20:37 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 441
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "data":
  {
    "meta":
    {
      "totalCount": 1
    },
    "archived_reports": [{"20191120134501_Content Filters_calendar_month.pdf":
{"periodic_report_format": "PDF", "periodic_report_type_name": "Content Filters",
"periodic_report_generated": "20 Nov 2019 13:45 (GMT)", "periodic_report_time_range":
"Previous calendar month", "periodic_report_tier": "All Email Appliances",
"periodic_report_title": "Content Filters", "periodic_report_product_type": "esa"}}]
  }
}
```

アーカイブレポートの取得

次に、レポートの時間範囲で降順にソートされた上位 25 のアーカイブレポートのリストを取得する例を示します。

サンプル リクエスト

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

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:04:02 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 441
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "data": {
    "meta": {
      "totalCount": 1
    },
    "archived_reports": [{"20191120134501_Content Filters_calendar_month.pdf":
      {"periodic_report_format":
        "PDF", "periodic_report_type_name": "Content Filters", "periodic_report_generated":
        "20 Nov 2019 13:45 (GMT)", "periodic_report_time_range": "Previous calendar month",
        "periodic_report_tier":
        "All Email Appliances", "periodic_report_title": "Content Filters",
        "periodic_report_product_type": "esa"}}]
  }
}
```

アーカイブレポートエントリの詳細の取得

次に、デバイスタイプとアーカイブレポート ID を使用してアーカイブレポートエントリを取得する例を示します。

サンプル リクエスト

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

サンプル応答

アーカイブレポートエントリの詳細の表示

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:06:40 GMT
Content-type: application/pdf
Content-Disposition: filename="20191120134501_Content Filters_calendar_month.pdf"
Content-Length: 111141
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

アーカイブレポートエントリの詳細の表示

次の例は、特定のレポートタイプと時間範囲のアーカイブレポートエントリのプレビューPDFドキュメントを取得する方法を示しています。

サンプル リクエスト

```

GET /sma/api/v2.0/config/archived_reports/preview?device_type=sma
&periodic_report_type_name=Outgoing%20Destinations&periodic_report_type=phoebe
&periodic_report_start_date=2017-03-01T15:00:00.000Z&periodic_report_end_date=
2019-07-30T15:00:00.000Z&periodic_report_format=pdf&periodic_report_lang=en-us
&periodic_report_time_range=Custom%20range&periodic_report_rows=10
&periodic_report_sort_columns=%7B%22table%22:%20%22Outgoing%20Destinations
%20Detail%22,%22column%22:%20%22Total%20Processed%22%7D
HTTP/1.1
cache-control: no-cache
Postman-Token: fc05953b-1552-47ab-be49-4cb2be5fc7c0
Authorization: Basic YWRtaW46Q21zY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: /*/*
Host: m680q08.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: Thu, 21 Nov 2019 17:38:08 GMT
Content-type: application/pdf
Content-Disposition: filename="20191121173808_Outgoing Destinations.pdf"
Content-Length: 111240
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email,
  portal, cache-control, pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```


アーカイブレポートエントリの追加

次の例では、レポートタイトル、レポートタイプ、デバイスタイプ、およびその他のオプションを指定してアーカイブレポートを追加する方法を示します。

サンプル リクエスト

```
POST /sma/api/v2.0/config/archived_reports?device_type=sma
HTTP/1.1
cache-control: no-cache
Postman-Token: 83c60ea4-e187-41bd-9e13-cacbfd43967a
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 545
Connection: keep-alive
{
  "data":
  {
    "archived_reports": [{"periodic_report_title": "Connections by
Country", "periodic_report_type":
"phoebe", "periodic_report_type_name": "Connections by Country", "periodic_report_options":
{"periodic_report_format": "pdf", "periodic_report_lang": "en-us", "periodic_report_time_range":
"Previous 7 calendar
days", "periodic_report_rows": 10, "periodic_report_sort_columns": [{"table":
"Total Incoming Mail Connections by Country", "column": "Total Connections"}]},
"periodic_report_tier": "All Email Appliances", "periodic_report_delivery": "Archived Only"}]
}
}
```

サンプル応答

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Wed, 20 Nov 2019 14:11:44 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 46
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "data":
  {
    "message": "Archived successfully"
  }
}
```

アーカイブレポートエントリの削除

次に、デバイスタイプとアーカイブレポート ID を使用してアーカイブレポートを削除する例を示します。

サンプル リクエスト

```
DELETE /sma/api/v2.0/config/archived_reports?device_type=sma&
id=20191120141701_Connections+by+Country_calendar_week.pdf
HTTP/1.1
cache-control: no-cache
Postman-Token: affe27d3-d8bc-4986-a826-e9a6f449ac80
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: sma.cisco:6080
accept-encoding: gzip, deflate
content-length: 0
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Wed, 20 Nov 2019 14:17:40 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 52
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
    pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "data":
  {
    "message": "1 item deleted successfully"
  }
}
```

トラッキング API

ユーザ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 \(27 ページ\)](#)
- [拒否された接続 \(31 ページ\)](#)
- [メッセージの詳細 \(33 ページ\)](#)
- [DLP の詳細 \(35 ページ\)](#)
- [AMP の詳細 \(37 ページ\)](#)
- [URL の詳細 \(39 ページ\)](#)
- [接続の詳細 \(41 ページ\)](#)

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 API - Addendum to the Getting Started Guide for Cisco Content Security Management 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、アプライアンス（電子メールを処理）、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> <p>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。</p> <pre>searchOption=rejected_connections</pre>
	送信者 IP	<ul style="list-style-type: none"> senderIp=<value> <p>これはユーザ定義の値です。メッセージを送信するサーバの IP アドレスを使用します。次に例を示します。</p> <pre>senderIp=10.76.70.112</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>
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 API - Addendum to the Getting Started Guide for Cisco Content Security Management 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、`icid`、`mid`、アプライアンス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 YWRtaW46Q2lzY28xMjMk
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> アプライアンス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 YWRtaW46Q2lzMjY2xMjMk
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> アプライアンス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> アプライアンス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 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> アプライアンス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"
}
```

隔離 API

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 \(43 ページ\)](#)
- [その他の隔離用 API \(71 ページ\)](#)

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 \(44 ページ\)](#)
- [メッセージの詳細の取得 \(47 ページ\)](#)
- [メッセージのリリース \(50 ページ\)](#)
- [メッセージの削除 \(49 ページ\)](#)
- [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 \(51 ページ\)](#)
- [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 \(55 ページ\)](#)
- [セーフリストまたはブロックリスト エントリの削除 \(67 ページ\)](#)

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"> • startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z <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"> • quarantineType=<value> <p>承認される値はスパムです。</p> <p>quarantineType=spam</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"> • orderBy=<value> <p>有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • from_address • to_address • subject <ul style="list-style-type: none"> • orderBy=<value> <p>有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • asc • desc
	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"> • 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 YWRtaW46Q2lzyY28xMjMk
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> 承認される値はスパムです。 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
      MyxB7dsrdq8oTnn8YSi5amR2qihbeq2eJwvVjskf1\r\n KE7TdyCXsokg==<br
/>\nX-IronPort-AV:
      E=Sophos;i=\\"5.56,240,1539648000\"; \r\n d=\\"scan\";a=\\"22180\"<br
/>\nIronPort-SDR:
      PPj7KDz4Ur8W2ne2fWP/wSOUBwnY3x1XaBz/ryR/98vI6NPraAsA5q7vzUzYaYFpRCWGgfyJaZ\r\n
4UIJbt91/
      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	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。 <ul style="list-style-type: none"> "mids": [<value>] メッセージの <i>mid</i> を指定します。
	隔離タイプ	"quarantineType": "value" 有効な値は <i>spam</i> です。
要求本文	{ "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、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。 • "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> 有効な値はビューです。
	隔離タイプ	quarantineType=<value> 有効な値は <i>spam</i> です。
	表示方法	viewBy=<value> 有効な値は送信者と受信者です。
	オーダー基準	orderBy=<value> 有効な値は送信者と受信者です。
	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 <i>orderBy=recipient</i> 属性のみでサポートされています。 search=<value> これはユーザ定義の値です。
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 /sma/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 /sma/api/v2.0/quarantine/safelist?action=view&limit=25&offset=0&orderBy=recipient&orderDir=desc&quarantineType=spam&search=abc&viewBy=recipient
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

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

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

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> 有効な値は送信者と受信者です。
	受信者アドレス	"recipientAddresses": ["value", "value", ...] これはユーザ定義の値です。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 \(57 ページ\)](#)
- [送信者セーフリスト エントリの追加 \(58 ページ\)](#)
- [受信者ブロックリスト エントリの追加 \(59 ページ\)](#)
- [送信者ブロックリスト エントリの追加 \(59 ページ\)](#)
- [受信者セーフリスト エントリの編集 \(60 ページ\)](#)
- [送信者セーフリスト エントリの編集 \(61 ページ\)](#)
- [受信者ブロックリスト エントリの編集 \(62 ページ\)](#)
- [送信者ブロックリスト エントリの編集 \(63 ページ\)](#)
- [受信者セーフリスト エントリの付加 \(64 ページ\)](#)
- [送信者セーフリスト エントリの付加 \(64 ページ\)](#)

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

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

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

```

```

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

```

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

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

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

```

```

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

```

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

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

```

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

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

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

```
    }
}
```

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

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

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


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

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

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

送信者ブロックリスト エントリの付加

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

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

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"
    ]
  }
}

```

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" 有効な値は送信者と受信者です。 .

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 \(68 ページ\)](#)
- [送信者セーフリストエントリの削除 \(69 ページ\)](#)
- [受信者ブロックリストエントリの削除 \(70 ページ\)](#)
- [送信者ブロックリストエントリの削除 \(70 ページ\)](#)

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

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

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

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

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

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

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

```
content-length: 82
Connection: keep-alive
```

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

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 \(72 ページ\)](#)
- [メッセージの詳細の取得 \(79 ページ\)](#)
- [メッセージの移動 \(81 ページ\)](#)
- [隔離からメッセージの終了を遅延する \(82 ページ\)](#)
- [隔離内のメッセージのコピーを送信する \(84 ページ\)](#)
- [添付ファイルのダウンロード \(86 ページ\)](#)
- [メッセージの削除 \(87 ページ\)](#)
- [メッセージのリリース \(88 ページ\)](#)
- [ルール サマリーの表示 \(90 ページ\)](#)
- [ルール ID に基づく検索 \(91 ページ\)](#)
- [ルール サマリーからのメッセージをリリース \(94 ページ\)](#)

- [ルール サマリーからメッセージを削除 \(96 ページ\)](#)

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	<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> <ul style="list-style-type: none"> • <code>startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</code>
	検索する隔離	<p>このパラメータは検索する隔離を指定します。</p> <ul style="list-style-type: none"> • <code>quarantines=<value, value, ...></code> <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>
	件名	<ul style="list-style-type: none"> • <code>subjectFilterBy=<value></code> <p>有効な値は次のとおりです。</p> <p>contains</p> <p>starts_with</p> <p>ends_with</p> <p>matches_exactly</p> <p>does_not_contain</p> <p>does_not_start_with</p> <p>does_not_end_with</p> <p>does_not_match</p> <ul style="list-style-type: none"> • <code>subjectFilterValue=<value></code> <p>これはユーザ定義の値です。</p>
	元の ESA	<p><code>originatingEsaIp=<value></code></p> <p>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。</p>
	添付の詳細	

	<ul style="list-style-type: none"> • <code>attachmentName=<value></code> これはユーザ定義の値です。 • <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> 値は次のとおりです。 sender subject received scheduledExit size • orderDir=<value> 値は次のとおりです。 asc desc
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> 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。
エンベロープ受信者	<ul style="list-style-type: none"> • envelopeRecipientFilterBy=<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 • envelopeRecipientFilterValue=<value> 検索対象の値。これはユーザ定義の値です。次の例を参考にしてください。 envelopeRecipientFilterValue=user

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

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 /sma/api/v2.0/quarantine/messages/details?mid=166&quarantineType=pvo
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: sma.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

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:
4Sh6scwkvct4BgD5601B/15cTAMkUtJtFAY+/Sk6YwaaSxL2TOzEKHwsn+6KxG+kV2Zg
75sMX<br> DkgdFZYTDpift9VvRsTl0Fz+N6rRgHCB4=<br>X-IPAS-Result:
=?us-ascii?q?A0GSTP/juz9b/+pj4QpOH
oMagXSCU4gely0HhysBAQEBA?=<br>

```



```

=?us-ascii?q?QEBeoIOAQEBPQUEAgEFBQEDAwECAGeBLTEkOCyBFxhDiEefIY8MAQ
EBAQYBA?=<br>
=?us-ascii?q?QEBAR2PIQEBhH8FiRODF4FVgUqBJ02RGYVLhA55AYEAgTcBAQE?=<br>
Subject: [SUSPICIOUS MESSAGE] Test mail.<br>Received: from client.cisco.com

(HELO pod1224-client05.ibwsa) ([10.225.99.234])<br> 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 /sma/api/v2.0/quarantine/messages
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: sma.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 138
Connection: keep-alive
{
  "action": "move",
  "destinationQuarantineName": "Policy",
  "mids": [46],
  "quarantineName": "Unclassified",
  "quarantineType": "pvo"
}
```

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

隔離内のメッセージのコピーを送信する

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

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

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

```

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

TVqQAAMAAAEAAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA+AAAAA4fug4AtAnNlbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIGlv
ZGUuZDQ0KJAAAAAAAAA1pLDYzV8kGGb/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 /sma/api/v2.0/quarantine/messages
HTTP/1.1
Content-Type: application/json
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: sma.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 41
Connection: keep-alive
{
  "mids": [112],
  "quarantineName": "Policy",
  "quarantineType": "pvo"
}
```

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

```
{
```

```
"action": "release",
"mids": [157],
"quarantineName": "Policy",
"quarantineType": "pvo",
}
```

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

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

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

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

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

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

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
  }
}
```

構成 API

ここでは、次の内容について説明します。

- [サービスステータスのクエリ](#)
- [ファイル分析のクエリ](#)
- [レポートグループのクエリ](#)
- [セーフリストブロックリストのクエリ](#)
- [スパム設定のクエリ](#)

サービスステータスのクエリ

ここでは、次の内容について説明します。

- [サービスステータスの取得](#)
- [レポートステータスの有効化](#)
- [メッセージトラッキングステータスの有効化](#)
- [スパム隔離ステータスの更新](#)
- [セーフリストまたはブロックリスト設定の有効化](#)
- [License Agreement](#)

サービスステータスの取得

機能のサービスステータスを取得します。

概要	GET /sma/api/v2.0/config/centralizedServices/serviceStatus
----	--

この例では、機能のサービスステータスを取得するクエリを示します。

サンプル リクエスト

```
GET /sma/api/v2.0/config/centralizedServices/serviceStatus?device_type=sma HTTP/1.1
cache-control: no-cache
Postman-Token: 119ae2b6-5f11-4108-a1d9-849672dc66cc
```

```

Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 13:14:57 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 251
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control, pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

レポートステータスの有効化

サービスステータスのレポートステータスを有効にします。

概要	PUT /sma/api/v2.0/config/centralizedServices/serviceStatus/centralizedReporting
----	--

```

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

```

この例では、機能のレポートステータスを有効にするクエリを示します。

サンプル リクエスト

```

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

```

```

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

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 13:27:21 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

メッセージトラッキングステータスの有効化

概要	PUT /sma/api/v2.0/config/centralizedServices/serviceStatus/centralizedTracking
----	---

```

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

```

この例では、機能のメッセージトラッキングステータスを有効にするクエリを示します。

サンプルリクエスト

```

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

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

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 13:36:42 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

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

スパム隔離ステータスの更新

20日後のスケジュール削除でスパム隔離ステータスを更新します。

概要	PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings
----	--

この例では、スパム隔離ステータスを更新するクエリを示します。

サンプル リクエスト

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: a4e76628-cece-4c7b-822a-94fffb6cfe84
Authorization: Basic YWRtaW46Q21zY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 408
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 14:07:53 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 56
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

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

セーフリストまたはブロックリスト設定の有効化

ユーザあたりの最大リスト項目数を160にして、セーフリストまたはブロックリスト設定を有効にし、3時間ごとの頻度で更新します。

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

この例では、セーフリストまたはブロックリスト設定を有効にするクエリを示します。

サンプル リクエスト

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

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 15:03:29 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

License Agreement

ここでは、サービスステータスのライセンス契約について説明します。

概要	PUT https://10.76.15.164:62/sa/api/v2.0/config/centralizedServices/licenseAgreement?device_type=sma
要求本文	{"data": {"licenseAgreement": {"centralizedReporting": "yes", "centralizedTracking": "yes", "spamQuarantine": "yes"}}}
Response	{"data": {"message": "Updated successfully"}}
概要	PUT https://10.76.15.164:62/sa/api/v2.0/config/centralizedServices/licenseAgreement?centralizedReporting=centralizedReporting
要求本文	{"data": {"licenseAgreement": {"centralizedReporting": "yes",

概要	GET https://10.76.157.16x42/sma/api/v2.0/config/centralizedServices/licenseAgmt?device_type=sma
要求本文	<pre>{"data": {"licenseAgreement": {"centralizedReporting": "yes", "centralizedTracking": "yes", "spamQuarantine": "yes"}}}</pre>

ファイル分析のクエリ

ここでは、次の内容について説明します。

- [グループ \(a@cisco.com\)](#) の追加
- [ファイル分析レポートのアプライアンスグループ化の表示](#)

グループ (a@cisco.com) の追加

グループ (a@cisco.com) のファイル分析クライアント ID
06_VLNSMA12345678_422985E30D3CE2CC17BA-1A7EC30F6E9B_M100V_000000 への追加

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

この例では、ファイル分析クライアント ID にグループを追加するクエリを示します。

サンプルリクエスト

```
POST /sma/api/v2.0/config/centralizedServices/fileAnalysis/groupInfo?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: eabb3018-d0c5-4372-a850-09deb8c89472
Authorization: Basic YWRtaW46Q21zY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 210
Connection: keep-alive

{"id":{"fileAnalysis":{"groupInfo":{"name":"https://aaa.threatgrid.com","key":"AABC","group":"a@cisco.com","sizes":["06_VLNSMA12345678_422985E30D3CE2CC17BA-1A7EC30F6E9B_M100V_000000"]}}}}
```

サンプル応答

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

```

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

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

```

ファイル分析レポートのアプライアンスグループ化の表示

ファイル分析レポートのアプライアンスグループ化を表示します。

概要	GET /sma/api/v2.0/config/centralizedServices/fileAnalysis?device_type
----	---

この例では、ファイル分析レポートのアプライアンスグループ化を表示するクエリを示します。

サンプルリクエスト

```

GET /sma/api/v2.0/config/centralizedServices/fileAnalysis?device_type=sma& HTTP/1.1
cache-control: no-cache
Postman-Token: fdf34da1-3727-42b4-8d62-4cab2ce4a54d
Authorization: Basic YWRtaW46Q2lzY29AMTlz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.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: Wed, 27 May 2020 13:33:39 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 306
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

レポートグループのクエリ

ここでは、次の内容について説明します。

- [レポート設定の有効化](#)

- レポートグループおよびアプライアンスの取得
- レポートグループおよびアプライアンス
- レポートグループの削除
- すべてのアクションの結合
- 100文字を超えるすべてのアクションの結合
- 単一のレポートグループの編集
- 複数のレポートグループの編集
- レポートグループの編集

レポート設定の有効化

1つまたは複数のグループを追加して、レポート設定を有効にします。

概要	POST /sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups
----	---

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

この例では、機能のレポート設定を有効にするクエリを示します。

サンプル リクエスト

```
POST
/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: 4d0f276b-c246-4f45-bf20-ed7f36b4a14b
Authorization: Basic YWRtaW46Q2lzMzY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 79
Connection: keep-alive
```

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

サンプル応答

```
HTTP/1.1 201 Created
Server: API/2.0
Date: Thu, 21 May 2020 16:12:16 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 61
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
```



```

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

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

```

レポートグループおよびアプライアンスの取得

レポートグループおよびアプライアンスを取得します。

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

```

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

```

この例では、レポートグループとアプライアンスを取得するクエリを示します。

サンプルリクエスト

```

GET
/sma/api/v2.0/config/centralizedServices/centralizedReporting/reportingGroups?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: alc76d19-24bc-4cfa-b598-dalfcc5b0afc
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 28 May 2020 11:50:00 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 191
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

レポートグループおよびアプライアンス

デフォルトでは、offset=0、limit=25、orderDir=asc、orderBy=group です。

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

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

レポートグループの削除

1 つの有効なレポートグループを削除する方法は次のとおりです。

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

サンプル応答

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

複数の有効なレポートグループを削除する方法は次のとおりです。

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

サンプル応答

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

すべてのアクションの結合

結合されたすべてのアクション（グループの追加/編集/削除）の POST

概要	POST /sma/api/v2.0/config/centralizedServices/centralizedReporting/allGroups
----	---

この例では、グループの追加、編集、削除などのすべてのアクションを結合するクエリを示します。

サンプル リクエスト

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



```

    }
  },
  {
    "pneumonoultramitic": {
      "appliances": [
        "420E6D0465DF4F1107A8-EA6829376651"
      ]
    }
  }
}

```

サンプル応答

```

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

```

単一のレポートグループの編集

単一のレポートグループを編集します (PUT メソッド)。

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

この例では、単一のレポートグループを編集するクエリを示します。

サンプル リクエスト

```

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

```

サンプル応答

```

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

```

```

    }
  }
}

```



- (注) PUT メソッドでは、レポートグループに「**appliances**」と「**newGroup**」というキーパラメータを設定できます。「**appliances**」パラメータは必須です。グループ名を編集するには、「**newGroup**」パラメータを使用します。

複数のレポートグループの編集

グループ名の変更 (PUT) で複数のレポートグループを編集します。

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

この例では、複数のレポートグループを編集するクエリを示します。

サンプル リクエスト

```

{
  "data": {
    "centralizedReporting": {
      "reportingGroups": [
        {
          "divs12K": {
            "appliances": [
              "420E6D0465DF4F1107A8-EA6829376651",
              "420E74056157AC99D24A-600741749CD3"
            ],
            "newGroup": "merci"
          }
        },
        {
          "divs6K": {
            "appliances": [
            ]
          }
        }
      ]
    }
  }
}

```

サンプル 応答

```

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

```

レポートグループの編集

100 文字を超えるレポートグループ名を編集します (PUT)。

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

この例では、100 文字を超えるレポートグループ名を編集するクエリを示します。

サンプル リクエスト

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

サンプル応答

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

セーフリストブロックリストのクエリ

ここでは、次の内容について説明します。

- [セーフリストブロックリスト設定の取得](#)
- [セーフリストブロックリスト設定の有効化](#)
- [ファイル転送ステータスの取得](#)
- [ファイル転送ステータスの同期](#)

セーフリストブロックリスト設定の取得

概要	GET /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings
----	---

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

この例は、セーフリストおよびブロックリスト設定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 /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: e547122f-b5c6-4663-b33f-610405b9fb69
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 17:03:14 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 92
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

セーフリストブロックリスト設定の有効化

ユーザごとの最大リスト項目数を160にしたセーフリストまたはブロックリスト設定を有効にして、3時間ごとの頻度で更新します。

概要	PUT /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings
----	---

この例では、セーフリストまたはブロックリストの設定を有効にするクエリを示します。

サンプル リクエスト

```
PUT /sma/api/v2.0/config/centralizedServices/safelistBlocklist/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: 97173889-0246-4c56-bac0-baac336eec26
Authorization: Basic YWRtaW46Q2lzY29AMTIz
Content-Type: text/plain
```

```
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 87
Connection: keep-alive
{"data":{"safelistBlocklist":{"settings":{"maxUserEntries":160,"updatePeriod":10800}}}}
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 15:03:29 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 45
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control, pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

ファイル転送ステータスの取得

すべてのアプライアンスのファイル転送ステータスを取得します。

概要	GET /sma/api/v2.0/config/centralizedServices/safelistBlocklist/fileTransferStatus
----	---

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

この例では、ファイル転送ステータスを取得するクエリを示します。

サンプル リクエスト

```
GET
/sma/api/v2.0/config/centralizedServices/safelistBlocklist/fileTransferStatus?device_type=sma&
HTTP/1.1
cache-control: no-cache
Postman-Token: 1b95101b-8846-4be1-ba3d-3199315f3a1d
Authorization: Basic YWRtaW46Q2lzY29AMTIz
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

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



```

Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

ファイル転送ステータスの同期

概要	GET /sma/api/v2.0/config/centralizedServices/safelistBlocklist/appliancesSyncStatus
----	--

```

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

```

この例では、ファイル転送ステータスを同期するクエリを示します。

サンプル リクエスト

```

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

```

サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 29 May 2020 11:51:18 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 126
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

スパム設定のクエリ

ここでは、次の内容について説明します。

- [デフォルトロゴを使用したスパム設定の取得](#)

- スケジュールされた削除設定の有効化
- スпам設定の有効化

デフォルトロゴを使用したスパム設定の取得

概要	GET /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings
----	--

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

この例では、デフォルトロゴを使用してスパム設定を取得するクエリを示します。

サンプル リクエスト

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

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 17:47:41 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 446
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

スケジュールされた削除設定の有効化

スケジュールされた削除設定を有効にします。

概要	PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings
----	--

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma& HTTP/1.1
```

この例は、スケジュールされた削除設定を有効にするクエリを示しています。

サンプル リクエスト

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

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma& HTTP/1.1
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 18:04:46 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 56
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

スパム設定の有効化

スケジュール削除設定とカスタムログインメッセージ「Welcome」を使用してスパム設定を有効にします。

概要	PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings
----	--

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma& HTTP/1.1
```

この例では、スケジュール削除設定とカスタムログインメッセージを使用してスパム設定を有効にするクエリを示します。

サンプル リクエスト

```
PUT /sma/api/v2.0/config/centralizedServices/spamQuarantine/settings?device_type=sma&
HTTP/1.1
cache-control: no-cache
```

```
Postman-Token: d48d5462-98ea-4031-8506-5d6cf91f3393
Authorization: Basic YWRtaW46Q21zY29AMTIz
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 412
Connection: keep-alive
```

```
Content-Length: 412
Content-Type: text/plain
Host: pod1224-sma01.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 412
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 May 2020 18:12:36 GMT
Cache-control: no-store
Pragma: no-cache
Content-type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Length: 56
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
    pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{"data": {"message": "Updated spam quarantine settings"}}
```