



## AsyncOS 14.0 API for Cisco Secure Email Gateway - スタートアップガイド（一般導入）

初版：2021年3月18日

最終更新：2021年7月28日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ [www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/) ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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

© 2021 Cisco Systems, Inc. All rights reserved.



## 目次

---

### 第 1 章

#### Cisco Secure Email Gateway 向け AsyncOS API の概要 1

- AsyncOS API 使用の前提条件 1
- AsyncOS API の有効化 2
- AsyncOS API との安全な通信 3
- AsyncOS API の認証と認可 3
  - 認証 3
    - JSON Web トークンを使用した API クエリの認証 4
  - 認可 5
- AsyncOS API の要求と応答 6
  - AsyncOS API 要求 6
  - AsyncOS API 応答 7
    - 応答の主要なコンポーネント 7
    - HTTP 応答コード 8
- AsyncOS API 機能 9

---

### 第 2 章

#### Secure Email 用 API 11

- レポート API 11
  - 例 13
    - カウンタの 1 つの値を取得する 14
    - カウンタの複数の値を取得する 15
    - 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 15
    - 複数のカウンタの複数の値を取得する 16
    - 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 18
    - 設定されたメールポリシーに一致する上位受信メッセージを取得する 20

設定されたメールポリシーに一致する上位送信メッセージを取得する	21
設定されたメールポリシーに一致するすべての受信メッセージを取得する	22
設定されたメールポリシーに一致するすべての送信メッセージを取得する	24
トラッキング API	24
メッセージの検索	25
拒否された接続	30
メッセージの詳細	31
DLP の詳細	34
AMP の詳細	35
URL の詳細	37
接続の詳細	39
修復の詳細	41
設定されたメールポリシーに一致するすべての受信メッセージを取得する	43
設定されたメールポリシーに一致するすべての送信メッセージを取得する	45
隔離	48
スパム隔離用 API	48
メッセージの検索	49
メッセージの詳細の取得	52
メッセージの削除	54
メッセージのリリース	55
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	56
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	60
セーフリストまたはブロックリスト エントリの削除	72
その他の隔離用 API	76
メッセージの検索	77
メッセージの詳細の取得	84
メッセージの移動	86
隔離からメッセージの終了を遅延する	87
隔離内のメッセージのコピーを送信する	89
添付ファイルのダウンロード	91
メッセージの削除	92

メッセージのリリース	93
ルール サマリーの表示	95
ルール ID に基づく検索	96
ルール サマリーからのメッセージをリリース	99
ルール サマリーからメッセージを削除	101
ロギング API	102
電子メールゲートウェイのログサブスクリプション詳細の取得	102
特定のログサブスクリプションのすべてのログファイルの取得	103
URL を使用したログファイルの取得	105

---

**第 3 章****汎用 API 107**

システム時刻のクエリ	107
管理対象 電子メールゲートウェイの情報のクエリ	108
ユーザー ロールにアクセス可能な API の取得	108
ヘルス API	109

---

**第 4 章****AsyncOS API のトラブルシューティング 111**

API ログ	111
アラート	111





# 第 1 章

## Cisco Secure Email Gateway 向け AsyncOS API の概要

Cisco Secure Email Gateway 向け AsyncOS API（または AsyncOS API）は Representational State Transfer（REST）ベースの一連の操作で、電子メールゲートウェイのレポート、レポートカウンタ、トラッキングへのセキュアで認証済みのアクセスを提供します。APIを使用して、電子メールゲートウェイのレポートおよびトラッキングデータを取得できます。このリリースでは、設定情報をクエリできます。このリリースでは、設定変更の転記はサポートされていません。

詳細については、[Swagger API ヘルプ](#)を参照してください。API ヘルプを表示するには、電子メールゲートウェイの新しい Web インターフェイスにアクセスし、ページの右上隅にあるヘルプアイコンをクリックして、[\[APIヘルプ : Swagger \(API Help: Swagger\)\]](#) を選択します。

この章は、次の項で構成されています。

- [AsyncOS API 使用の前提条件, on page 1](#)
- [AsyncOS API の有効化, on page 2](#)
- [AsyncOS API との安全な通信, on page 3](#)
- [AsyncOS API の認証と認可, on page 3](#)
- [AsyncOS API の要求と応答, on page 6](#)
- [AsyncOS API 機能, on page 9](#)

## AsyncOS API 使用の前提条件

AsyncOS API を使用するには、次の知識が必要です。

- HTTP。API トランザクションに使用されるプロトコル。TLS 経由で保護された通信。
- JavaScript Object Notation（JSON）。API がリソースの表記作成に使用。
- JSON Web トークン（JWT）

- cURL など、HTTP や HTTPS を使用して AsyncOS API に対して要求の開始と応答の受信を行うクライアントまたはプログラミングライブラリ。クライアントまたはプログラミングライブラリは、API からの応答を解釈できるように JSON をサポートする必要があります。
- AsyncOS API へのアクセスの許可。認可, on page 5 を参照してください。
- Web インターフェイスまたは CLI を使用して有効化されている AsyncOS API。AsyncOS API の有効化, on page 2 を参照してください。



**Note** バージョン 1.0 API は、Cisco E メールセキュリティ 13.0 リリース以降ではサポートされていません。その代わりにバージョン 2.0 API が使用されます。

## AsyncOS API の有効化

### はじめる前に

Web インターフェイスの IP インターフェイス ページまたは CLI の `interfaceconfig` コマンドへのアクセスが許可されていることを確認します。許可されているのは、管理者、E メール管理者、クラウド管理者、およびオペレータのみです。

また、CLI で `interfaceconfig` コマンドを使用すると、AsyncOS API を有効にすることもできます。

**ステップ 1** Web インターフェイスにログインします。

**ステップ 2** [ネットワーク (Network) ] > [IP インターフェイス (IP Interfaces) ] を選択します。

**ステップ 3** 管理インターフェイスを編集します。

- Note**
- IP インターフェイスで AsyncOS API を有効にできます。ただし、管理インターフェイスから AsyncOS API を有効にすることをお勧めします。
  - 複数の管理インターフェイスで API を有効することはしないでください。

**ステップ 4** [AsyncOS API (モニタリング) (AsyncOS API (Monitoring))] セクションで、要件に応じて、HTTP、HTTPS、またはその両方、使用するポートを選択します。

**Note** AsyncOS API は HTTP / 1.1 を使用して通信します。

HTTPS を選択して、セキュア通信に独自の証明書を使用する場合は、[AsyncOS API との安全な通信, on page 3](#) を参照してください。

**Note** HTTPS は常に実稼働環境で使用することをお勧めします。API のトラブルシューティングおよびテストには、HTTP のみを使用します。

**ステップ 5** 変更を送信し、保存します。



# AsyncOS API との安全な通信

独自の証明書を使用してセキュア HTTP 経由で AsyncOS API と通信できます。



**Note** HTTPS およびセキュア通信用の独自の証明書を使用して Web インターフェイスをすでに起動している場合は、この手順を実行しないでください。AsyncOS API は、HTTPS 経由で通信するため Web インターフェイスと同じ証明書を使用します。

- ステップ 1** CLI で `certconfig` コマンドを使用して証明書を設定します。手順については、ユーザーガイドまたはオンラインヘルプを参照してください。
- ステップ 2** CLI で `interfaceconfig` コマンドを使用して、IP インターフェイスで使用する HTTPS 証明書を独自の証明書に変更します。手順については、ユーザーガイドまたはオンラインヘルプを参照してください。
- ステップ 3** 変更を送信し、保存します。

## AsyncOS API の認証と認可

このセクションでは、認証方式、API にアクセスできるユーザーロール、ユーザーにアクセス可能な API をクエリする方法について説明します。

- [認証, on page 3](#)
- [認可, on page 5](#)
- [ユーザー ロールにアクセス可能な API の取得, on page 108](#)

## 認証

Base64 エンコード形式または JSON Web トークンによる API へのすべての要求と一緒に、電子メールゲートウェイのユーザー名とパスワードを送信します。電子メールゲートウェイのユーザー非アクティブタイムアウトの設定は、JWT の有効期間に適用されます。要求の認証ヘッダーに有効なクレデンシャルが含まれない場合、API は 401 エラーメッセージを送信します。base64 ライブラリを使用すると、クレデンシャルを base64 エンコード形式に変換できます。



**Note** 電子メールゲートウェイでは、OpenID Connect 1.0 をサポートするアイデンティティプロバイダー (IDP) から取得したアクセストークンを含めることで、AsyncOS API を呼び出すことができます。外部 IDP で AsyncOS API を使用方法の詳細については、『*User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway*』の「System Administration」の章を参照してください。

## JSON Web トークンを使用した API クエリの認証

JSON Web トークン (JWT) を生成すると、API クエリで使用することができます。



- (注) 電子メールゲートウェイのユーザー非アクティブタイムアウトの設定は、JWTの有効期間に適用されます。電子メールゲートウェイは、その有効期間のJWTを含むすべてのAPIクエリをチェックします。JWTの有効期間が5分以内の場合、タイムアウトになると、新しい更新JWTが応答ヘッダーと共に送信されます。APIクエリでこの新しい更新JWTを使用するか、新しいJWTを生成する必要があります。

概要	POST /esa/api/v2.0/login 二要素認証には、次の構文を使用します。 POST /esa/api/v2.0/login/two_factor
本文パラメータ	Base64 エンコード クレデンシアルを使用します。 <pre>{   "data":   {     "userName": "YWRtaW4=",     "passphrase": "aXJvbnBvcnQ="   } }</pre>
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

次の例では、Base64 エンコード クレデンシアルでログインし、JWT を生成するクエリを示します。

### サンプル リクエスト

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

### サンプル応答



# AsyncOS API の要求と応答

- [AsyncOS API 要求, on page 6](#)
- [AsyncOS API 応答, on page 7](#)

## AsyncOS API 要求

API に対する要求には次の特性があります。

- 要求は HTTP または HTTPS 経由で送信されます
- 各要求には、次の形式で有効な URI が含まれている必要があります。

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

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

引数の説明

- {appliance}:{port}

FQDN または電子メールゲートウェイの IP アドレスと、電子メールゲートウェイが待機する TCP ポート番号です。

- {resource}

レポート、トラッキング、隔離、設定、他のカウンタなど、アクセスしようとするリソースです。

- {resource\_attributes}

期間など、リソースでサポートされている属性です。

- 各要求には、ユーザー クレデンシャルまたは有効な認証ヘッダーを含める必要があります。
- 各要求には、承認を設定する必要があります。

```
application/json
```

- HTTPS（独自の証明書を使用）経由で送信された要求には、CA 証明書を含める必要があります。たとえば、cURL の場合、API 要求で CA 証明書を次のように指定することができます。

```
curl --cacert <ca_cert.crt> -u"username:password"
```

```
https://<fqdn>:<port>/esa/api/v2.0/{resource}/{resource_attributes}
```



**Note** API 要求では、大文字と小文字が区別され、このマニュアルで示すように入力する必要があります。

## AsyncOS API 応答

このセクションでは、応答の主要なコンポーネントとさまざまなHTTPエラーコードについて説明します。

- [応答の主要なコンポーネント, on page 7](#)
- [HTTP 応答コード, on page 8](#)

### 応答の主要なコンポーネント

コンポーネント	値	説明	
ステータスコードと理由	<a href="#">HTTP 応答コード, on page 8</a> を参照してください。	HTTP 応答コードと理由。	
メッセージヘッダー	Content-Type	application/json	メッセージ本文の形式を示す。
	Content-Length	適用対象外	オクテットによる応答本文の長さ。
	Connection	close	接続用のオプション。

コンポーネント	値	説明
メッセージ本文	適用対象外	<p>メッセージ本文は Content-Type ヘッダーで定義された形式です。次に、メッセージ本文のコンポーネントを示します。</p> <ol style="list-style-type: none"> <li>URI。API への要求で指定した URI。 例 "/api/v2.0/config/"</li> <li>カウンタ グループやカウンタ名 例 reporting/mail_security_summary</li> <li>クエリ パラメータ 例 startDate=2017-01-30T00:00:00.000Z&amp;endDate=2018-01-30T14:00:00.000Z</li> <li>エラー (エラーイベントのみ)。このコンポーネントは、メッセージ、コード、および説明の 3 つのコンポーネントを示します。 例 "error": {"message": "Unexpected attribute - starts with.", "code": "404", "explanation": "404 = Nothing matches the given URI."}</li> </ol> <p>メッセージ本文に空のカッコ ({} ) が含まれている場合、API がクエリに一致するレコードを見つけられなかったことを表します。</p>

## HTTP 応答コード

次に、AsyncOS API によって返される HTTP 応答コードのリストを示します。

- 200
- 202
- 300
- 301
- 307
- 400

- 401
- 403
- 404
- 406
- 413
- 414
- 500
- 501
- 503
- 505

これらの HTTP 応答コードの詳細については、次の RFC を参照してください。

- RFC1945
- RFC7231

## AsyncOS API 機能

AsyncOS API を使用すると、次のカテゴリの情報を取得できます。

- [Secure Email 用 API, on page 11](#)
- [汎用 API, on page 107](#)







## 第 2 章

# Secure Email 用 API

---

- [レポート API \(11 ページ\)](#)
- [トラッキング API \(24 ページ\)](#)
- [隔離 \(48 ページ\)](#)
- [ロギング API \(102 ページ\)](#)

## 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&amp;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"> <li>• <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。</li> <li>• <code>query_type=export</code> エクスポート形式のデータを受信します。</li> </ul>
	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"> <li>• <code>orderBy=&lt;value&gt;</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></li> <li>• <code>orderDir=&lt;value&gt;</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"> <li>• <code>asc</code> 昇順で結果を並べ替えます。</li> <li>• <code>desc</code> 降順で結果を並べ替えます。</li> </ul> </li> </ul>
	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"> <li>• <code>offset=&lt;value&gt;</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。</li> <li>• <code>limit=&lt;value&gt;</code> 取得するレコードの数を指定します。</li> </ul>

データの取得オプション	<ul style="list-style-type: none"> <li>• top=&lt;value&gt; 最大値を返すレコードの数を指定します。</li> </ul>
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"> <li>• filterValue=&lt;value&gt; 検索対象の値。</li> <li>• filterBy=&lt;value&gt; 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。</li> <li>• filterOperator=&lt;value&gt; 有効なオプションは次のとおりです。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul> </li> </ul>
デバイス	<ul style="list-style-type: none"> <li>• device_group_name=&lt;value&gt; デバイス グループ名を指定します。</li> <li>• 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。</li> <li>• device_name=&lt;value&gt; デバイス名を指定します。</li> </ul>
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 \(14 ページ\)](#)

- [カウンタの複数の値を取得する \(15 ページ\)](#)
- [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 \(15 ページ\)](#)
- [複数のカウンタの複数の値を取得する \(16 ページ\)](#)
- [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 \(18 ページ\)](#)
- [設定されたメールポリシーに一致する上位受信メッセージを取得する \(20 ページ\)](#)
- [設定されたメールポリシーに一致する上位送信メッセージを取得する \(21 ページ\)](#)
- [設定されたメールポリシーに一致するすべての受信メッセージを取得する \(22 ページ\)](#)
- [設定されたメールポリシーに一致するすべての送信メッセージを取得する \(24 ページ\)](#)

## カウンタの1つの値を取得する

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

### サンプル リクエスト

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

### サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 15:58:29 GMT
Content-type: application/json
Content-Length: 96
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "meta": {
    "totalCount": -1},
  "data": {
    "type": "detected_amp",
    "resultSet": {
      "detected_amp": 11}
  }
}
```

## カウンタの複数の値を取得する

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

### サンプル リクエスト

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

### サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 17:39:34 GMT
Content-type: application/json
Content-Length: 580
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

## カウンタ グループ内の各カウンタの1つの値を取得する

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

## 複数のカウンタの複数の値を取得する

### サンプル リクエスト

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

### サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sat, 17 Nov 2018 18:17:29 GMT
Content-type: application/json
Content-Length: 153
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "meta": {
    "totalCount": -1
  },
  "data": {
    "type": "recipients_matched",
    "resultSet": {
      "recipients_matched": [
        {"url_rep_neutral": 16},
        {"url_category": 8}
      ]
    }
  }
}
```

## 複数のカウンタの複数の値を取得する

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

### サンプル リクエスト

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

### サンプル応答

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

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

```
{
  "meta": {
    "totalCount": -1
  },
  "data": {
    "type": "mail_incoming_domain_detail",
    "resultSet": {
      "conn_tls_total": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 5}
      ],
      "conn_tls_opt_success": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 0}
      ],
      "conn_tls_opt_fail": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 0}
      ],
      "blocked_invalid_recipient": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 1}
      ],
      "last_sender_group_name": [
        {"pphosted.com": "UNKNOWNLIST"},
        {"vm30bsd0004.ibqa": "UNKNOWNLIST"}
      ],
      "detected_amp": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 2}
      ],
      "social_mail": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 1}
      ],
      "detected_spam": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 25}
      ],
      "blocked_reputation": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 5}
      ],
      "total_throttled_recipients": [
        {"pphosted.com": 0},
        {"vm30bsd0004.ibqa": 2}
      ],
      "total_accepted_connections": [
        {"pphosted.com": 2},
        {"vm30bsd0004.ibqa": 119}
      ],
      ...
    }
  },
  ...
}
```

各カウンタの複数の値を使用して複数のカウンタの複数の値を取得する

```
        "threat_content_filter": [
          {"pphosted.com": 0},
          {"vm30bsd0004.ibqa": 5}
        ],
        "marketing_mail": [
          {"pphosted.com": 0},
          {"vm30bsd0004.ibqa": 5}
        ],
        "blocked_dmarc": [
          {"pphosted.com": 0},
          {"vm30bsd0004.ibqa": 0}
        ],
        "conn_tls_success": [
          {"pphosted.com": 0},
          {"vm30bsd0004.ibqa": 5}
        ],
        "total_recipients": [
          {"pphosted.com": 2},
          {"vm30bsd0004.ibqa": 112}
        ],
        "conn_tls_fail": [
          {"pphosted.com": 0},
          {"vm30bsd0004.ibqa": 0}
        ],
        "total_threat_recipients": [
          {"pphosted.com": 0},
          {"vm30bsd0004.ibqa": 49}
        ]
      ]
    }
  }
}
```

## 各カウンタの複数の値を使用して複数のカウンタの複数の値を取得する

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

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

## 設定されたメールポリシーに一致する上位受信メッセージを取得する

```

...
        {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 1},
...
    ]
  },
  "total_graymail_recipients": {
    "10.76.68.103": [
      {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 0},
      {"2017-10-01T00:00:00.000Z to 2017-10-31T23:59:00.000Z": 4},
      ...
    ],
    ...
    {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 0},
    {"2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 0}
  ]
},
  "total_clean_recipients": {
    "10.76.68.103": [
      {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 5},
      {"2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 0}
    ]
  },
  "sbrs_score": {
    "10.76.68.103": [
      {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 3},
      ...
    ],
    ...
    {"2018-08-01T00:00:00.000Z to 2018-08-31T23:59:00.000Z": 0},
    {"2018-09-01T00:00:00.000Z to 2018-09-30T23:59:00.000Z": 0}
  ]
},
  "blocked_reputation": {
    "10.76.68.103": [
      {"2017-09-01T00:00:00.000Z to 2017-09-30T23:59:00.000Z": 0},
    ]
  }
}
}
}
}

```

## 設定されたメールポリシーに一致する上位受信メッセージを取得する

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

### サンプル リクエスト

```

GET /esa/api/v2.0/reporting/mail_policy_incoming/recipients_matched?
device_type=esa&endDate=2021-02-26T14:00:00.000Z&startDate=2020-11-27T18:00:00.000Z&top=10
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
Accept: application/json, text/plain, */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
connection: keep-alive

```

### サンプル応答

```

HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 435
Content-Type: application/json; charset=UTF-8
{
  "meta": {
    "totalCount": -1
  },
  "data": {
    "type": "recipients_matched",
    "resultSet": {
      "recipients_matched": [
        {
          "Bypass_Blocklist_Policy": 318172
        },
        {
          "Test Mail Policy Marketing2Junk": 177994
        },
        {
          "DEFAULT": 147011
        },
        {
          "Allow Marketing Newsletters": 28882
        },
        {
          "Aggressive Spam Scoring": 18605
        },
        {
          "Allowed_listEmailAddresses": 15177
        },
        {
          "ampuser": 9463
        },
        {
          "Block_Inbound_Mail_Westfield": 9436
        },
        {
          "Bulk Mail Quarantined": 9365
        },
        {
          "virususer": 9238
        }
      ]
    }
  }
}

```

## 設定されたメールポリシーに一致する上位送信メッセージを取得する

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

### サンプル リクエスト

## 設定されたメールポリシーに一致するすべての受信メッセージを取得する

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

### サンプル応答

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 163
Content-Type: application/json; charset=UTF-8
{
  "meta": {
    "totalCount": -1
  },
  "data": {
    "type": "recipients_matched",
    "resultSet": {
      "recipients_matched": [
        {
          "Block_Outbound_Traffic": 921281
        },
        {
          "DEFAULT": 23623
        }
      ]
    }
  }
}
```

## 設定されたメールポリシーに一致するすべての受信メッセージを取得する

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

### サンプル リクエスト

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

### サンプル応答

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 547
Content-Type: application/json; charset=UTF-8
{
  "meta": {
    "totalCount": -1
  },
  "data": {
    "type": "recipients_matched",
    "resultSet": {
      "recipients_matched": [
        {
          "Bypass_Blocklist_Policy": 318172
        },
        {
          "Test Mail Policy Marketing2Junk": 177994
        },
        {
          "DEFAULT": 147011
        },
        {
          "Allow Marketing Newsletters": 28882
        },
        {
          "Aggressive Spam Scoring": 18605
        },
        {
          "Allowed_listEmailAddresses": 15177
        },
        {
          "ampuser": 9463
        },
        {
          "Block_Inbound_Mail_Westfield": 9436
        },
        {
          "Bulk Mail Quarantined": 9365
        },
        {
          "virususer": 9238
        },
        {
          "Allow_Marketing_Filter_Spam": 4651
        },
        {
          "Blocklist Email Addresses": 847
        },
        {
          "second-selva": 12
        },
        {
          "second": 2
        }
      ]
    }
  }
}
```

設定されたメールポリシーに一致するすべての送信メッセージを取得する

```
}
}
```

## 設定されたメールポリシーに一致するすべての送信メッセージを取得する

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

### サンプル リクエスト

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

### サンプル応答

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Connection: keep-alive
Content-Length: 163
Content-Type: application/json; charset=UTF-8
{
  "meta": {
    "totalCount": -1
  },
  "data": {
    "type": "recipients_matched",
    "resultSet": {
      "recipients_matched": [
        {
          "Block_Outbound_Traffic": 921281
        },
        {
          "DEFAULT": 23623
        }
      ]
    }
  }
}
```

## トラッキング API

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

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

- [メッセージの検索 \(25 ページ\)](#)
- [拒否された接続 \(30 ページ\)](#)
- [メッセージの詳細 \(31 ページ\)](#)
- [DLP の詳細 \(34 ページ\)](#)
- [AMP の詳細 \(35 ページ\)](#)
- [URL の詳細 \(37 ページ\)](#)
- [接続の詳細 \(39 ページ\)](#)
- [修復の詳細 \(41 ページ\)](#)
- [設定されたメールポリシーに一致するすべての受信メッセージを取得する \(43 ページ\)](#)
- [設定されたメールポリシーに一致するすべての送信メッセージを取得する \(45 ページ\)](#)

## 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、『』 『』 『 <a href="#">AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway Appliances</a> 』を参照してください。	
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

### 例

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

### サンプル リクエスト

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

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

### サンプル応答

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

```
{
  "meta": {
    "num_bad_records": 7,
    "totalCount": 13
  },
  "data": [
    {
      "attributes": {
        "direction": "incoming",
        "icid": 110,
        "senderGroup": "UNKNOWNLIST",
        "sender": "confikr.qa",
        "replyTo": "N/A",
        "timestamp": "15 Oct 2018 08:33:19 (GMT)",
        "hostName": "esa01",
        "subject": "message is good",
        "mid": [
          110
        ],
        "isCompleteData": true,
        "messageStatus": "Delivered",
        "mailPolicy": [
          "DEFAULT"
        ],
        "senderIp": "10.8.91.18",
        "verdictChart": "0",
        "senderDomain": "N/A",
        "recipient": [
          "confikr@cisco.com"
        ],
        "sbrs": "None",
        "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
      }
    },
    {
      "attributes": {
        "direction": "incoming",
        "icid": 103,
        "senderGroup": "UNKNOWNLIST",
        "sender": "confikr@example.com",
        "replyTo": "N/A",
        "timestamp": "15 Oct 2018 08:24:39 (GMT)",
        "hostName": "esa01",
        "subject": "message is good",
        "mid": [
```



```

        104
    ],
    "isCompleteData": true,
    "messageStatus": "Delivered",
    "mailPolicy": [
        "DEFAULT"
    ],
    ],
    "senderIp": "10.8.91.18",
    "verdictChart": "0",
    "senderDomain": "example.com",
    "recipient": [
        "4201@ironport.com"
    ],
    ],
    "sbrs": "None",
    "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
}
},
{
    "attributes": {
        "direction": "incoming",
        "icid": 105,
        "senderGroup": "UNKNOWNLIST",
        "sender": "confikr@example.com",
        "replyTo": "N/A",
        "timestamp": "15 Oct 2018 08:24:39 (GMT)",
        "hostName": "esa01",
        "subject": "message is good",
        "mid": [
            103
        ],
    ],
    "isCompleteData": true,
    "messageStatus": "Delivered",
    "mailPolicy": [
        "DEFAULT"
    ],
    ],
    "senderIp": "10.8.91.18",
    "verdictChart": "0",
    "senderDomain": "example.com",
    "recipient": [
        "4417@ironport.com"
    ],
    ],
    "sbrs": "None",
    "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
}
},
{
    "attributes": {
        "direction": "incoming",
        "icid": 107,
        "senderGroup": "UNKNOWNLIST",
        "sender": "confikr@example.com",
        "replyTo": "N/A",
        "timestamp": "15 Oct 2018 08:24:39 (GMT)",
        "hostName": "esa01",
        "subject": "message is good",
        "mid": [
            102
        ],
    ],
    "isCompleteData": true,
    "messageStatus": "Delivered",
    "mailPolicy": [
        "DEFAULT"
    ],
    ],
    "senderIp": "10.8.91.18",

```

```

        "verdictChart": "0",
        "senderDomain": "example.com",
        "recipient": [
            "3396@ironport.com"
        ],
        "sbrs": "None",
        "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 106,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                101
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "9985@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    },
    {
        "attributes": {
            "direction": "incoming",
            "icid": 100,
            "senderGroup": "UNKNOWNLIST",
            "sender": "confikr@example.com",
            "replyTo": "N/A",
            "timestamp": "15 Oct 2018 08:24:39 (GMT)",
            "hostName": "esa01",
            "subject": "message is good",
            "mid": [
                100
            ],
            "isCompleteData": true,
            "messageStatus": "Delivered",
            "mailPolicy": [
                "DEFAULT"
            ],
            "senderIp": "10.8.91.18",
            "verdictChart": "0",
            "senderDomain": "example.com",
            "recipient": [
                "1023@ironport.com"
            ],
            "sbrs": "None",
            "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
        }
    }
}

```

```

    },
    {
      "attributes": {
        "direction": "incoming",
        "icid": 104,
        "senderGroup": "UNKNOWNLIST",
        "sender": "confikr@example.com",
        "replyTo": "N/A",
        "timestamp": "15 Oct 2018 08:24:39 (GMT)",
        "hostName": "esa01",
        "subject": "message is good",
        "mid": [
          99
        ],
        "isCompleteData": true,
        "messageStatus": "Delivered",
        "mailPolicy": [
          "DEFAULT"
        ],
        "senderIp": "10.8.91.18",
        "verdictChart": "0",
        "senderDomain": "example.com",
        "recipient": [
          "182@ironport.com"
        ],
        "sbrs": "None",
        "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
      }
    },
    {
      "attributes": {
        "direction": "incoming",
        "icid": 98,
        "senderGroup": "UNKNOWNLIST",
        "sender": "confikr@example.com",
        "replyTo": "N/A",
        "timestamp": "15 Oct 2018 08:24:39 (GMT)",
        "hostName": "esa01",
        "subject": "message is good",
        "mid": [
          98
        ],
        "isCompleteData": true,
        "messageStatus": "Delivered",
        "mailPolicy": [
          "DEFAULT"
        ],
        "senderIp": "10.8.91.18",
        "verdictChart": "0",
        "senderDomain": "example.com",
        "recipient": [
          "8668@ironport.com"
        ],
        "sbrs": "None",
        "serialNumber": "4229CAEC09527FD2570C-F028BAE54A11"
      }
    }
  ]
}

```

## 拒否された接続

次の表からさまざまな属性を持つ拒否された接続の詳細を取得できます。

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

### 例

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

### サンプル リクエスト

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

```

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

```

### サンプル応答

```

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

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

```

## メッセージの詳細

次の表からさまざまな属性を持つメッセージの詳細を取得できます。

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

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

### 例

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

### サンプル リクエスト

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

### サンプル応答

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

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

```

        "description": "Protocol SMTP interface Management (IP 10.76.71.196)
on incoming connection
        (ICID 19214) from sender IP 10.76.70.111. Reverse DNS host
vm30bsd0199.ibqa verified yes.",
        "lastEvent": false
    },
    ...
    ...
    {
        "timestamp": "16 Nov 2018 11:20:12 (GMT)",
        "description": "Message 22125 scanned by Advanced Malware Protection
engine. Final verdict
        : UNKNOWN", "lastEvent": false
    },
    {
        "timestamp": "16 Nov 2018 11:20:12 (GMT)",
        "description": "Message 22125 contains attachment
'driver_license_germany.txt' (SHA256 7e3dee4dac
8f4af561d1108c4b237e5e139bd8d3ddc8518455d3b5fb7e7a70c3).",
        "lastEvent": false
    },
    {
        "timestamp": "16 Nov 2018 11:20:12 (GMT)",
        "description": "Message 22125 attachment 'driver_license_germany.txt'
scanned by Advanced Malware
Protection engine. File Disposition: Unknown",
        "lastEvent": false
    },
    {
        "timestamp": "16 Nov 2018 11:20:12 (GMT)",
        "description": "Message 22125 Delivery Status: DROPPED",
        "lastEvent": false
    },
    {
        "timestamp": "16 Nov 2018 11:20:12 (GMT)",
        "description": "Message 22125 Verdict chart: 01131212",
        "lastEvent": true
    }
    ],
    "attachments": [
        "driver_license_germany.txt"
    ],
    "messageSize": "765 (Bytes)",
    "isCompleteData": true,
    "showDLP": true,
    "messageStatus": "Dropped by DLP",
    "showURL": false,
    "mailPolicy": [
        "DEFAULT"
    ],
    "senderGroup": "RELAYLIST",
    "recipient": [
        "7799@vm30bsd0004.ibqa"
    ],
    "showSummaryTimeBox": true,
    "subject": "Testing"
    }
}
}

```

## DLP の詳細

次の表からさまざまな属性を持つメッセージの DLP を取得できます。

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

### 例

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

#### サンプル リクエスト

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

#### サンプル応答

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



```

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

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

```

## AMP の詳細

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

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

### 例

次の例では、icid、mid、シリアル番号で識別される特定のメッセージ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"> <li>serialNumber=&lt;value&gt;</li> </ul> 電子メールゲートウェイのシリアル番号を指定します。
	メッセージ ID とインジェクション接続 ID	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> <li>icid=&lt;value&gt;</li> <li>メッセージの icid を指定します。</li> <li>mid=&lt;value&gt;</li> <li>メッセージの mid を指定します。</li> </ul>
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"> <li>serialNumber=&lt;value&gt;</li> </ul> 電子メールゲートウェイのシリアル番号を指定します。
	メッセージ ID とインジェクション接続 ID	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> <li>icid=&lt;value&gt;</li> <li>mid=&lt;value&gt;</li> </ul> メッセージの icid を指定します。  メッセージの mid を指定します。
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

## 例

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

### サンプルリクエスト

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

### サンプル応答

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

```

Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

## 修復の詳細

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

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

### サンプル リクエスト

```

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

```

## サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 25 May 2020 10:28:53 GMT
Content-type: application/json
Content-Length: 5271
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email, portal, cache-control,
  pragma
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "batch_details": {
    "b_init_username": "admin",
    "mor_action": "Delete",
    "b_init_time": 1590646987,
    "batch_name": "Re7",
    "batch_desc": "N/A",
    "b_init_source": "ESA 117"
  },
  "message_details": [
    {
      "delivered_at": 1584574165,
      "mid": "3",
      "from_email": "kr@mar-esa.com",
      "recipient_email": "krs@onpremesa2019.com",
      "mor_status": "Success",
      "msg_read": "0"
    },
    {
      "delivered_at": 1584574165,
      "mid": "3",
      "from_email": "kr@mar-esa.com",
      "recipient_email": "krc@mar-esa.com",
      "mor_status": "Success",
      "msg_read": "0"
    },
    {
      "delivered_at": 1584574165,
      "mid": "3",
      "from_email": "kr@mar-esa.com",
      "recipient_email": "anonpremnnew@mar-esa.com",
      "mor_status": "Success",
      "msg_read": "0"
    },
    {
      "delivered_at": 1584574165,
      "mid": "3",
      "from_email": "kr@mar-esa.com",
      "recipient_email": "user5@scale.com",
      "mor_status": "Failed",
      "msg_read": "N/A"
    }
  ]
}

```



## 設定されたメールポリシーに一致するすべての受信メッセージを取得する

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

概要	GET esa/api/v2.0/message-tracking/messages?startDate=2021-03-01T18:30:00.000Z &endDate=2021-03-02T12:11:00.000Z&ciscoHost=All_Hosts &mailPolicyName=Default&mailPolicyDirection=inbound &searchOption=messages&offset=0&limit=100
サポート対象のリソース属性	詳細については、『』 『』 『 <a href="#">AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Secure Email Gateway</a> 』を参照してください。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection  次の例は、電子メールゲートウェイで設定されたメールポリシーに一致するすべての受信メッセージを取得するクエリを示しています。

### サンプルリクエスト

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

### サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Tue, 02 Mar 2021 12:14:37 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 35014
Connection: keep-alive
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Disposition, jwtToken
Cache-control: no-store
Pragma: no-cache
Server: nginx
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
{
  "meta": {
    "num_bad_records": 0,
```

設定されたメールポリシーに一致するすべての受信メッセージを取得する

```

    "totalCount": 39
  },
  "data": [
    {
      "attributes": {
        "hostName": "",
        "friendly_from": [
          "user1@mar-esa.com"
        ],
        "isCompleteData": "N/A",
        "messageStatus": {
          "2325234": "Delivered"
        },
        "recipientMap": {
          "2325232": [
            "user5@scale.com"
          ],
          "2325234": [
            "user5@scale.com"
          ]
        },
        "senderIp": "10.10.4.49",
        "mailPolicy": [
          "DEFAULT"
        ],
        "senderGroup": "UNKNOWNLIST",
        "subject": "46_2016_smtp_2_5",
        "mid": [
          2325232,
          2325234
        ],
        "senderDomain": "mar-esa.com",
        "finalSubject": {
          "2325234": "46_2016_smtp_2_5"
        },
        "direction": "incoming",
        "icid": 516876,
        "morDetails": {},
        "replyTo": "N/A",
        "timestamp": "02 Mar 2021 17:15:53 (GMT +05:30)",
        "messageID": {
          "2325232": "<76773.751151876-sendEmail@mail.example.com>"
        },
        "verdictChart": {
          "2325234": "11141110"
        },
        "recipient": [
          "user5@scale.com"
        ],
        "sender": "user1@mar-esa.com",
        "serialNumber": "421558305641772925266-ABFF53B75FDE",
        "allIcid": [
          516876
        ],
        "sbrs": "None"
      }
    },
    {
      "attributes": {
        "hostName": "",
        "friendly_from": [
          "user1@mar-esa.com"
        ],
        "isCompleteData": "N/A",

```

```

    "messageStatus": {
      "2325233": "Delivered"
    },
    "recipientMap": {
      "2325233": [
        "user5@scale.com"
      ],
      "2325230": [
        "user5@scale.com"
      ]
    },
    "senderIp": "10.10.4.49",
    "mailPolicy": [
      "DEFAULT"
    ],
    "senderGroup": "UNKNOWNLIST",
    "subject": "46_2016_smtp_2_4",
    "mid": [
      2325230,
      2325233
    ],
    "senderDomain": "mar-esa.com",
    "finalSubject": {
      "2325233": "46_2016_smtp_2_4"
    },
    "direction": "incoming",
    "icid": 516875,
    "morDetails": {},
    "replyTo": "N/A",
    "timestamp": "02 Mar 2021 17:15:51 (GMT +05:30)",
    "messageID": {
      "2325230": "<564966.601875739-sendEmail@mail.example.com>"
    },
    "verdictChart": {
      "2325233": "11141110"
    },
    "recipient": [
      "user5@scale.com"
    ],
    "sender": "user1@mar-esa.com",
    "serialNumber": "421558305641772925266-ABFF53B75FDE",
    "allIcid": [
      516875
    ],
    "sbrs": "None"
  },
},
]
}

```

## 設定されたメールポリシーに一致するすべての送信メッセージを取得する

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

設定されたメールポリシーに一致するすべての送信メッセージを取得する

概要	GET esa/api/v2.0/message-tracking/messages?startDate=2021-03-01T18:30:00.000Z &endDate=2021-03-02T12:11:00.000Z&ciscoHost=All_Hosts&mailPolicyName=Default &mailPolicyDirection=outbound&searchOption=messages&offset=0&limit=100
サポート対象のリソース属性	詳細については、『』 『』 『 <a href="#">AsyncOS 14.0 API - Addendum to the Getting Started guide for Cisco Secure Email Gateway</a> 』を参照してください。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection  次の例は、電子メールゲートウェイで設定されたメールポリシーに一致するすべての送信メッセージを取得するクエリを示しています。

### サンプル リクエスト

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

### サンプル応答

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

{
  "meta": {
    "num_bad_records": 0,
    "totalCount": 2
  },
  "data": [
    {
      "attributes": {
        "hostName": "",
        "friendly_from": [
          "LaithwaitesWine@fiendofwine.us"
        ]
      }
    }
  ]
}
```

```

    "isCompleteData": "N/A",
    "messageStatus": {
      "2325166": "Delivered"
    },
  },
  "recipientMap": {
    "2325166": [
      "testuser2@abc.com"
    ]
  },
  "senderIp": "10.10.4.46",
  "mailPolicy": [
    "DEFAULT"
  ],
  "senderGroup": "None",
  "subject": "Top 12 wines for the holidays",
  "mid": [
    2325166
  ],
  "senderDomain": "testdomain.com",
  "finalSubject": {
    "2325166": "[SPAM] Top 12 wines for the holidays"
  },
  "direction": "outgoing",
  "icid": 516847,
  "morDetails": {},
  "replyTo": "N/A",
  "timestamp": "02 Mar 2021 13:14:36 (GMT +05:30)",
  "messageID": {
    "2325166": "<198313425761047198391528032556096@makug.fiendofwine.us>"
  },
  },
  "verdictChart": {
    "2325166": "16141113"
  },
  },
  "recipient": [
    "testuser2@abc.com"
  ],
  "sender": "user@testdomain.com",
  "serialNumber": "42155830541772925266-ABFF53B45FDE",
  "allIcid": [
    516847
  ],
  "sbrs": "None"
}
},
{
  "attributes": {
    "hostName": "",
    "mid": [
      2325164
    ],
  },
  "isCompleteData": "N/A",
  "messageStatus": {
    "2325164": "Dropped By Anti-Virus"
  },
  "recipientMap": {
    "2325164": [
      "testuser1@abc.com"
    ]
  },
  "senderIp": "10.10.4.46",
  "mailPolicy": [
    "DEFAULT"
  ],
}

```

```

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

```

## 隔離

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

- [スパム隔離用 API \(48 ページ\)](#)
- [その他の隔離用 API \(76 ページ\)](#)

## 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 \(49 ページ\)](#)
- [メッセージの詳細の取得 \(52 ページ\)](#)
- [メッセージのリリース \(55 ページ\)](#)
- [メッセージの削除 \(54 ページ\)](#)
- [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 \(56 ページ\)](#)

- [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 \(60 ページ\)](#)
- [セーフリストまたはブロックリスト エントリの削除 \(72 ページ\)](#)

## 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"> <li>• <code>startdate=YYYY-MM-DDThh:mm:00.000Z&amp;endDate=YYYY-MM-DDThh:mm:00.000Z</code></li> </ul> <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"> <li>• <code>quarantineType=&lt;value&gt;</code></li> </ul> <p>承認される値は <code>spam</code> です。</p> <p><code>quarantineType=spam</code></p>
	ソート	<p>結果を順序付けする値と方向を指定できます。</p> <ul style="list-style-type: none"> <li>• <code>orderBy=&lt;value&gt;</code></li> </ul> <p>有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <code>from_address</code></li> <li>• <code>to_address</code></li> <li>• <code>subject</code></li> </ul> <ul style="list-style-type: none"> <li>• <code>orderDir=&lt;value&gt;</code></li> </ul> <p>有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <code>asc</code></li> <li>• <code>desc</code></li> </ul>
	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"> <li>• <code>offset=&lt;value&gt;</code></li> </ul> <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"> <li>• <code>limit=&lt;value&gt;</code></li> </ul> <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"> <li>• envelopeRecipientFilterOperator=&lt;value&gt; 有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• contains</li> <li>• is</li> <li>• begins_with</li> <li>• ends_with</li> <li>• does_not_contain</li> </ul> </li> <li>• envelopeRecipientFilterValue=&lt;value&gt; 検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。 envelopeRecipientFilterValue=user</li> </ul>
	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"> <li>• filterOperator=&lt;value&gt; 検索対象の値。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• contains</li> <li>• is</li> <li>• begins_with</li> <li>• ends_with</li> <li>• does_not_contain</li> </ul> </li> <li>• filterValue=&lt;value&gt; 検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。 filterValue=abc.com</li> </ul>
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

### 例

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

### サンプル リクエスト

```
GET /esa/api/v2.0/quarantine/messages?endDate=2018-11-21T23:59:00.000Z&
limit=25&offset=0&orderBy=date&orderDir=desc&quarantineType=spam&startDate=2018-07-01T00:00:00.000Z
```

```

HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46Q2lzY28xMjMk
User-Agent: curl/7.54.0
Accept: */*
Host: esa.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

### サンプル応答

```

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

```

```

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

```

## メッセージの詳細の取得

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

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

サポート対象のリソース属性	隔離タイプ	<ul style="list-style-type: none"> <li>• quarantineType=&lt;value&gt; 承認される値はspam です。 quarantineType=spam</li> </ul>
	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"> <li>• mid=&lt;value&gt;</li> </ul>
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
    ESMTTP; 16 Nov 2018 13:58:55 +0000<br />\nIronPort-SDR:
DjDeJA8ZkD90oA9x+n3eGd9Qa/nliz1dL
    MyxB7dsrdq8oTnn8YSi5amR2qihbeq2eJwvVjskfl\r\n KE7TdyCXsokg==<br
/>\nX-IronPort-AV:
    E=Sophos;i=\\"5.56,240,1539648000\\"; \r\n    d=\\"scan\\";a=\\"22180\\"<br
/>\nIronPort-SDR:
    PPj7KDz4Ur8W2ne2fWF/wSOUBwnY3x1XaBz/ryR/98vI6NPraAsA5q7vzUzyaYFpRCWGgfyJaZ\r\n
4UIJbt91/
    WFccoWcqqO86zz6rYcRASCSM=<br />\nIronPort-PHdr:
=?us-ascii?q?9a23=3Az7tnkBDwN1EwuviG0ROD
    UyQJP3Nli/DPJgcQr6?=\r\n
=?us-ascii?q?AfoPdwSPT7pMbcNUDSrc9gkEXOFd2Cra4c26yO6+jJYi8p2d65",
    "date": "16 Nov 2018 13:58 (GMT)",
    "fromAddress": [
        "testuser <testuser@cisco.com>"
    ],
    "subject": "[SUSPICIOUS MESSAGE] [SUSPECTED SPAM] Testing VOF"
},
"mid": 1755
}
}

```

## 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"> <li>"mids": [&lt;value&gt;]</li> </ul> <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>spam</i> です。</p>
要求本文	<pre>{   "quarantineType": "spam",   "mids": [&lt;mid&gt;] }</pre>	
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

### 例

次の例では、メッセージを削除するクエリを示します。

サンプル リクエスト

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

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

### サンプル応答

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

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

## メッセージのリリース

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

概要	POST /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	メッセージ ID	リリースアクションを有効にするためには、このパラメータを使用する必要があります。  • "mids": [<value>]  メッセージの <b>mid</b> 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"> <li>• action=&lt;value&gt;</li> </ul> 有効な値はviewです。
	隔離タイプ	quarantineType=<value> 有効な値はspamです。
	表示方法	viewBy=<value> 有効な値はsenderとrecipientです。
	オーダー基準	orderBy=<value> 有効な値はsenderとrecipientです。
	遅延読み込み	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 <ul style="list-style-type: none"> <li>• offset=&lt;value&gt;</li> </ul> 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"> <li>• limit=&lt;value&gt;</li> </ul> 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"> <li>• asc</li> <li>• desc</li> </ul>
	検索	これは orderBy=recipient 属性のみでサポートされています。 search=<value> これはユーザー定義の値です。
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

## 例

受信者別にセーフリストとブロックリストのエントリを表示する。

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

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

## サンプル リクエスト

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

## サンプル応答

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

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

送信者別にセーフリストとブロックリストのエントリを表示する。

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



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

### サンプル リクエスト

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

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

### サンプル 応答

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

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

## セーフリストとブロックリスト エントリの追加、編集、付加

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

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

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

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

## 例

- [受信者セーフリスト エントリの追加 \(62 ページ\)](#)
- [送信者セーフリスト エントリの追加 \(63 ページ\)](#)
- [受信者ブロックリスト エントリの追加 \(64 ページ\)](#)
- [送信者ブロックリスト エントリの追加 \(64 ページ\)](#)
- [受信者セーフリスト エントリの編集 \(65 ページ\)](#)
- [送信者セーフリスト エントリの編集 \(66 ページ\)](#)
- [受信者ブロックリスト エントリの編集 \(67 ページ\)](#)
- [送信者ブロックリスト エントリの編集 \(68 ページ\)](#)
- [受信者セーフリスト エントリの付加 \(69 ページ\)](#)
- [送信者セーフリスト エントリの付加 \(69 ページ\)](#)

## 受信者セーフリスト エントリの追加

次の要求例では、セーフリスト エントリを追加するクエリを示します。

## サンプル リクエスト

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

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

## サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Fri, 23 Nov 2018 10:22:23 GMT
Content-type: application/json
Content-Length: 115
Connection: close
```

```

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

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

```

## 送信者セーフリスト エントリの追加

次の要求例では、セーフリスト エントリを追加するクエリを示します。

### サンプル リクエスト

```

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

```

```

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

```

### サンプル応答

```

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

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

```

```

        "senderAddresses": [
            "xyz.com",
            "space.com"
        ]
    }
}

```

## 受信者ブロックリスト エントリの追加

次の要求例では、ブロックリスト エントリを追加するクエリを示します。

### サンプル リクエスト

```

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

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

```

### サンプル応答

```

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

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

```

## 送信者ブロックリスト エントリの追加

次の要求例では、ブロックリスト エントリを追加するクエリを示します。

### サンプル リクエスト

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

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

### サンプル応答

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

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

## 受信者セーフリスト エントリの編集

次の要求例では、セーフリスト エントリを追加するクエリを示します。

### サンプル リクエスト

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

```

content-length: 163
Connection: keep-alive

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

```

### サンプル応答

```

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

```

```

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

```

## 送信者セーフリストエントリの編集

次の要求例では、セーフリスト エントリを追加するクエリを示します。

### サンプル リクエスト

```

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

```

```

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

```

### サンプル応答



```

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

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

```

## 受信者ブロックリスト エントリの編集

次の要求例では、ブロックリスト エントリを編集するクエリを示します。

### サンプル リクエスト

```

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

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

```

### サンプル応答

```

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

```

```

Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

## 送信者ブロックリスト エントリの編集

次の要求例では、ブロックリスト エントリを編集するクエリを示します。

### サンプル リクエスト

```

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

```

```

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

```

### サンプル応答

```

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

```

```

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

```

```
    }
}
```

## 受信者セーフリスト エントリの付加

次の要求例では、セーフリスト エントリを付加するクエリを示します。

### サンプル リクエスト

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

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

### サンプル応答

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

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

## 送信者セーフリスト エントリの付加

次の要求例では、セーフリスト エントリを付加するクエリを示します。

### サンプル リクエスト

## 受信者ブロックリスト エントリの付加

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

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

## サンプル応答

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

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

## 受信者ブロックリスト エントリの付加

次の要求例では、ブロックリスト エントリを付加するクエリを示します。

## サンプル リクエスト

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

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

### サンプル応答

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

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

## 送信者ブロックリスト エントリの付加

次の要求例では、ブロックリスト エントリを付加するクエリを示します。

### サンプル リクエスト

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

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

### サンプル応答

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

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

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

## セーフリストまたはブロックリスト エントリの削除

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

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

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

次の API を使用できます。

- [受信者セーフリスト エントリの削除 \(73 ページ\)](#)
- [送信者セーフリスト エントリの削除 \(74 ページ\)](#)
- [受信者ブロックリスト エントリの削除 \(75 ページ\)](#)
- [送信者ブロックリスト エントリの削除 \(75 ページ\)](#)

## 受信者セーフリスト エントリの削除

次の要求例では、セーフリスト エントリを削除するクエリを示します。

### サンプル リクエスト

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

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

### サンプル応答

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

```

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

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

```

## 送信者セーフリストエントリの削除

次の要求例では、セーフリスト エントリを削除するクエリを示します。

### サンプル リクエスト

```

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

```

```

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

```

### サンプル応答

```

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

```

```

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

```



```
    }
}
```

## 受信者ブロックリスト エントリの削除

次の要求例では、ブロックリスト エントリを削除するクエリを示します。

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

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

### サンプル応答

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

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

## 送信者ブロックリスト エントリの削除

次の要求例では、ブロックリスト エントリを削除するクエリを示します。

### サンプル リクエスト

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

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

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

### サンプル応答

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

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

## その他の隔離用 API

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

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

- [メッセージの検索 \(77 ページ\)](#)
- [メッセージの詳細の取得 \(84 ページ\)](#)
- [メッセージの移動 \(86 ページ\)](#)
- [隔離からメッセージの終了を遅延する \(87 ページ\)](#)
- [隔離内のメッセージのコピーを送信する \(89 ページ\)](#)
- [添付ファイルのダウンロード \(91 ページ\)](#)
- [メッセージの削除 \(92 ページ\)](#)
- [メッセージのリリース \(93 ページ\)](#)
- [ルール サマリーの表示 \(95 ページ\)](#)
- [ルール ID に基づく検索 \(96 ページ\)](#)
- [ルール サマリーからのメッセージをリリース \(99 ページ\)](#)

- [ルールサマリーからメッセージを削除 \(101 ページ\)](#)

## メッセージの検索

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

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

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

	<ul style="list-style-type: none"> <li>• <code>attachmentName=&lt;value&gt;</code> これはユーザ一定義の値です。</li> <li>• <code>attachmentSizeFilterBy=&lt;value&gt;</code> 有効な値は次のとおりです。 <code>range</code> <code>less_than</code> <code>more_than</code></li> <li>• <code>attachmentSizeFromValue=&lt;value_in_KB&gt;</code> これはユーザ一定義の値です。添付ファイルのサイズを <b>KB</b> 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"> <li>• <code>attachmentSizeFilterBy</code> で <code>range</code> 属性を選択した場合 <code>attachmentSizeFilterBy=range</code></li> <li>• <code>attachmentSizeFilterBy</code> で <code>more_than</code> 属性を選択した場合 <code>attachmentSizeFilterBy=more_than</code></li> </ul> </li> <li>• <code>attachmentSizeToValue=&lt;value_in_KB&gt;</code> これはユーザ一定義の値です。添付ファイルのサイズを <b>KB</b> 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"> <li>• <code>attachmentSizeFilterBy</code> で <code>range</code> 属性を選択した場合 <code>attachmentSizeFilterBy=range</code></li> <li>• <code>attachmentSizeFilterBy</code> で <code>less_than</code> 属性を選択した場合 <code>attachmentSizeFilterBy=less_than</code></li> </ul> </li> </ul>
隔離タイプ	<ul style="list-style-type: none"> <li>• <code>quarantineType=&lt;value&gt;</code> 承認される値は <code>pvo</code> です。 <code>quarantineType=pvo</code></li> </ul>
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"> <li>• orderBy=&lt;value&gt;</li> </ul> <p>値は次のとおりです。</p> <pre>sender subject received scheduledExit size</pre> <ul style="list-style-type: none"> <li>• orderDir=&lt;value&gt;</li> </ul> <p>値は次のとおりです。</p> <pre>asc desc</pre>
遅延読み込み		<p>次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。</p> <ul style="list-style-type: none"> <li>• offset=&lt;value&gt;</li> </ul> <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"> <li>• limit=&lt;value&gt;</li> </ul> <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"> <li>• envelopeRecipientFilterBy=&lt;value&gt;</li> </ul> <p>有効な値は次のとおりです。</p> <pre>contains starts_with ends_with matches_exactly does_not_contain does_not_start_with does_not_end_with does_not_match</pre> <ul style="list-style-type: none"> <li>• envelopeRecipientFilterValue=&lt;value&gt;</li> </ul> <p>検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。</p> <pre>envelopeRecipientFilterValue=user</pre>

	エンベ ロープ送 信者	<ul style="list-style-type: none"> <li>• envelopeSenderFilterBy=&lt;value&gt; 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</li> <li>• envelopeSenderFilterValue=&lt;value&gt; 検索対象の値。これはユーザー定義の値です。次の例を参考にしてください。 envelopeRecipientFilterValue=user</li> </ul>
要求ヘッ ダー		Host、Accept、Authorization
応答ヘッ ダー		Content-Type、Content-Length、Connection

## 例

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

## サンプル リクエスト

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

## サンプル応答

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

```

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

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

```



```

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

```

```

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

```

## メッセージの詳細の取得

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

概要	GET /api/v2.0/quarantine/messages?resource_attribute	
サポート対象のリソース属性	隔離タイプ	<ul style="list-style-type: none"> <li>quarantineType=&lt;value&gt;</li> </ul> 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"> <li>mid=&lt;value&gt;</li> </ul>
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

### 例

次の例では、特定のメッセージの詳細を取得するクエリを示します。

サンプル リクエスト

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

### サンプル応答

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

{
  "data": {
    "attributes": {
      "quarantineDetails": [
        {
          "received": "21 Nov 2018 10:10 (GMT)",
          "esaHostName": "esa01",
          "quarantineName": "Policy",
          "reason": [
            "Content Filter: 'url'"
          ],
          "scheduledExit": "21 Dec 2018 10:10 (GMT)",
          "originatingEsaIp": "10.8.91.15"
        }
      ],
      "matchedContents": [],
      "messagePartDetails": [
        {
          "attachmentId": 1,
          "attachmentSize": "43",
          "attachmentName": "[message body]"
        },
        {
          "attachmentId": 2,
          "attachmentSize": "307.25K",
          "attachmentName": "eicar4.pdf"
        }
      ],
      "messageDetails": {
        "recipient": [
          "eriferma@mail.qa.sgg.cisco.com"
        ],
        "sender": "usr2@sender.com",
        "subject": "[SUSPICIOUS MESSAGE] Test mail."
      },
      "messageBody": "This is a demo mail. http://bit.ly/2zs6KAq<br>\n",
      "headers": "IronPort-SDR:
4Sh6scwkvctt4BgD5601B/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"> <li>"mids": [&lt;value&gt;]</li> </ul> <p>メッセージの mid を指定します。</p>
	隔離タイプ	<p>"quarantineName": "&lt;value&gt;"</p> <p>有効な値は <i>pvo</i> です。</p>
	宛先隔離名	<p>"destinationQuarantineName": "&lt;value&gt;"</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>&lt;user-defined-quarantine&gt;</p>
要求本文	<pre>{   "action": "move",   "destinationQuarantineName": "&lt;value&gt;",   "mids": [&lt;value&gt;],   "quarantineName": "&lt;value&gt;",   "quarantineType": "pvo" }</pre>	
要求ヘッダー	Host、Accept、Authorization	

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

### 例

次の例では、メッセージを移動するクエリを示します。

### サンプル リクエスト

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

### サンプル応答

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

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

## 隔離からメッセージの終了を遅延する

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

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

サポート対象のリソース属性	メッセージ ID	<ul style="list-style-type: none"> <li>"mids": [value]</li> </ul> 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": "&lt;value&gt;",   "mids": [&lt;value&gt;],   "quarantineName": "&lt;value&gt;",   "quarantineType": "pvo" }</pre>	
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

### 例

次の例では、メッセージの終了を遅延するクエリを示します。

### サンプル リクエスト

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

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

### サンプル応答

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

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

## 隔離内のメッセージのコピーを送信する

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

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

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

## 例

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

### サンプル リクエスト

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

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

### サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 11:53:52 GMT
```



```

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

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

```

## 添付ファイルのダウンロード

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

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

### 例

次の例では、添付ファイルをダウンロードするクエリを示します。

#### サンプル リクエスト

```

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

```

#### サンプル応答

```

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

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

```

## メッセージの削除

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

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

## 例

次の例では、特定の隔離内の特定のメッセージを削除するクエリを示します。

### サンプル リクエスト

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

### サンプル応答

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

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

## メッセージのリリース

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

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

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

### 例

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

### サンプル リクエスト

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

```
{
```

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

### サンプル応答

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

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

## ルール サマリーの表示

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

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

### 例

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

### サンプル リクエスト

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

## サンプル応答

```

HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 22 Nov 2018 10:33:46 GMT
Content-type: application/json
Content-Length: 264
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

## ルール ID に基づく検索

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

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

サポート対象のリソース属性	隔離タイプ	quarantineType=<value> 有効な値は <i>pvo</i> です。
	ルール ID	ruleId=<value> これはユーザー定義の値です。
	ソート	結果を順序付けする値と方向を指定できます。  <ul style="list-style-type: none"> <li>orderBy=&lt;value&gt; 有効な値は次のとおりです。 received</li> <li>orderDir=&lt;value&gt; 有効な値は次のとおりです。 asc desc</li> </ul>
	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"> <li>offset=&lt;value&gt; 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。</li> <li>limit=&lt;value&gt; 取得するレコードの数を指定します。</li> </ul>
要求ヘッダー	Host、Accept、Authorization	
応答ヘッダー	Content-Type、Content-Length、Connection	

## 例

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

### サンプル リクエスト

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

## サンプル応答

```

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

```

```

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

```



```

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

```

## ルール サマリーからのメッセージをリリース

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

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

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

### 例

次の例では、メッセージをリリースするクエリを示します。

#### サンプル リクエスト

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

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

#### サンプル応答

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

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

## ルール サマリーからメッセージを削除

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

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

### 例

次の例では、ルール サマリーからメッセージを削除するクエリを示します。

### サンプル リクエスト

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

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

### サンプル 応答

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

```

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

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

```

## ロギング API

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

- [電子メールゲートウェイのログサブスクリプション詳細の取得 \(102 ページ\)](#)
- [特定のログサブスクリプションのすべてのログファイルの取得 \(103 ページ\)](#)
- [URL を使用したログファイルの取得 \(105 ページ\)](#)

## 電子メールゲートウェイのログサブスクリプション詳細の取得

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

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

### 例

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

### サンプル リクエスト

```

GET /esa/api/v2.0/config/logs/subscriptions
HTTP/1.1

```

```

cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

### サンプル応答

```

HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 3482
Connection: close

```

```

{
  "meta": {
    "totalCount": 43
  },
  "data": [
    {
      "retrievalMethod": "manual",
      "type": "AMP Engine Logs",
      "name": "amp"
    },
    {
      "retrievalMethod": "manual",
      "type": "AMP Archive",
      "name": "amparchive"
    },
    .....
    .....
    .....
    {
      "retrievalMethod": "manual",
      "type": "URL Reputation Client Logs",
      "name": "url_rep_client"
    }
  ]
}

```

## 特定のログサブスクリプションのすべてのログファイルの取得

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



- (注) この API は、電子メールゲートウェイで手動ログ取得方式を使用して設定されたログサブスクリプションにのみ適用されます。API は、ロールオーバーされたログファイルのみをリストします。[電子メールゲートウェイのログサブスクリプション詳細の取得 \(102 ページ\)](#) API のログサブスクリプション名から取得した応答の `name` 属性を使用する必要があります。

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

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

### 例

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

### サンプル リクエスト

```
GET
/esa/api/v2.0/logs/audit_logs/?startDate=2020-08-18T04:47:00.000Z&endDate=2020-08-18T13:55:00.000Z&computeHash=True

HTTP/1.1
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

### サンプル応答

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 777
Connection: close

{
  "meta": {
    "totalCount": 3
  },
  "data": [
    {
      "modificationDate": 1597742834,
      "downloadUrl": "/esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044745.s",
      "name": "audit_logs.@20200818T044745.s",
      "fileHash": "a1b0afb80e784eed91112111a012bf690d494492acf72bc402a0cebf9edcee45",
    }
  ]
}
```

```

        "size": 7216
      },
      {
        "modificationDate": 1597726065,
        "downloadUrl": "/esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044738.s",

        "name": "audit_logs.@20200818T044738.s",
        "fileHash": "868da20790adbf11145d2fc28125a24101ff2424621e634f8a1d570f55220cd",

        "size": 291
      },
      {
        "modificationDate": 1597726058,
        "downloadUrl": "/esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044643.s",

        "name": "audit_logs.@20200818T044643.s",
        "fileHash": "29f78fbdbcf3c4f1a20da6c0b38419e42932cab725653cb92fee87fb5a6cf6e4",

        "size": 1403
      }
    ]
  }
}

```

## URL を使用したログファイルの取得

[特定のログサブスクリプションのすべてのログファイルの取得 \(103 ページ\)](#) API から取得した応答の `downloadUrl` 属性を使用して、ログファイルの内容を取得できます。



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



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

概要	GET /esa/api/v2.0/logs/<log_subscription_name>/<log_file_name>  (注) <a href="#">特定のログサブスクリプションのすべてのログファイルの取得 (103 ページ)</a> API から取得した応答の <code>downloadUrl</code> 属性を使用する必要があります。
要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection、Content-Disposition

## 例

次の例は、特定のログサブスクリプションのすべてのログファイルの取得（103 ページ）API から取得した応答の `downloadUrl` 属性を使用して、ログファイルの内容を取得するためのクエリを示しています。

## サンプル リクエスト

```
GET /esa/api/v2.0/logs/audit_logs/audit_logs.@20200818T044738.s
HTTP/1.1
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

## サンプル応答

応答には、要求されたログファイルが含まれています。

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: text/plain
Content-length: 7216
Connection: close
Content-Disposition:attachment; filename="audit_logs.@20200818T044738.s"
Wed Sep 30 00:38:01 2020 Info: Begin Logfile
Wed Sep 30 00:38:01 2020 Info: Version: 13.7.0-030 SN: 4229CAEC09527FD2570C-F028BAE54A11
Wed Sep 30 00:38:01 2020 Info: Time offset from UTC: 0 seconds
Wed Sep 30 00:38:09 2020 Info: Logfile rolled over
Wed Sep 30 00:38:09 2020 Info: End Logfile
```





## 第 3 章

# 汎用 API

汎用設定のクエリには、クエリ文字列の一部として **config** リソース名が含まれます。取得できるのは設定情報 (GET) のみで、このリリースの変更 (POST、DELETE) を実行することはできません。デバイスタイプを指定して、電子メールゲートウェイからの設定が必要なデバイスを示すことができます。

この章は、次の項で構成されています。

- [システム時刻のクエリ \(107 ページ\)](#)
- [管理対象 電子メールゲートウェイの情報のクエリ \(108 ページ\)](#)
- [ユーザー ロールにアクセス可能な API の取得 \(108 ページ\)](#)
- [ヘルス API \(109 ページ\)](#)

## システム時刻のクエリ

### サンプル リクエスト

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

### サンプル応答

```
HTTP/1.0 200 OK  
Server: API/2.0  
Date: Thu, 12 Apr 2018 18:06:32 GMT  
Content-type: application/json  
Content-Length: 121  
Connection: close  
{  
  "data": {  
    "continent": [  
      "Asia",  
      "India",  
      "Kolkata"  
    ],  
    "time": "Thu Apr 12 23:38:05 2018 IST",
```

```

        "timezone": "Asia/Kolkata"
    }
}

```

## 管理対象 電子メールゲートウェイの情報のクエリ

### サンプル リクエスト

```

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

```

### サンプル応答

```

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

```

## ユーザー ロールにアクセス可能な API の取得

現在ログイン中のユーザーが利用可能な API のリストを取得することができます。

概要	GET /api/v2.0/login/privileges
----	--------------------------------

要求ヘッダー	Host、Accept、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

### サンプル リクエスト

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

### サンプル応答

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Apr 2018 14:17:44 GMT
Content-type: application/json
Content-Length: 4392
Connection: close
{
  "data": [
    "e_message_tracking_messages",
    "e_message_tracking_detail",
    "e_message_tracking_availability",
    "e_message_tracking_verdict",
    "e_message_tracking_dlp_details",
    "e_message_tracking_amp_details",
    ...
    ...
    "e_config_macro_file_types",
    "e_config_geo_countries",
    "e_config_tracking_query_timeout",
    "e_config_spam_quarantine_appearance_details",
    "esa_config_users",
    "e_config_euq_authentication_method",
    "e_config_euq_url_details"
  ]
}
```

## ヘルス API

ヘルス API を使用すると、システムヘルスに関する情報を取得できます。

概要	GET /api/v2.0/health/
要求ヘッダー	Host、Authorization
応答ヘッダー	Content-Type、Content-Length、Connection

### サンプル リクエスト

```
GET /esa/api/v2.0/health
HTTP/1.1
```

```
cache-control: no-cache
Postman-Token: a7eca7b8-0656-43db-b692-812396a86976
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Accept: */*
Host: esa.example.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

### サンプル応答

```
HTTP/1.0 200 OK
Server: API/2.0
Date: Thu, 12 Sept 2019 14:17:44 GMT
Content-type: application/json; charset=UTF-8
Content-Length: 5782
Connection: close
{
  "meta": {
    "totalCount": -1
  },
  "data": {
    "percentage_ram_utilization": 1,
    "messages_in_pvo_quarantines": 0,
    "resource_conservation": 0,
    "messages_in_workqueue": 0,
    "percentage_swap_utilization": 0.0,
    "percentage_queue_utilization": 0.0,
    "percentage_diskio": 0,
    "percentage_cpu_load": 17
  }
}
```



## 第 4 章

# AsyncOS API のトラブルシューティング

この章は、次の項で構成されています。

- [API ログ, on page 111](#)
- [アラート, on page 111](#)

## API ログ

[システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] を使用して API ログに登録します。手順については、電子メールゲートウェイまたはオンラインヘルプを参照してください。

次に、API ログに記録されたイベントの一部を示します。

- API が起動したか、または停止したか
- API への接続に失敗したか、または閉じたか (応答提供後)
- 認証が成功したか、または失敗したか
- 要求に含まれるエラー
- AsyncOS API とのネットワーク設定変更通信中のエラー

## アラート

AsyncOS APIに関連するアラートを送信するように電子メールゲートウェイが設定されていることを確認します。以下の場合にアラートを受信します。

アラートの説明	タイプ	重大度
エラーが原因で API が再起動されました	システム	警告

