Cisco AsyncOS API for Email - 入门指南

版本 1.0
发布日期：2016 年 5 月 20 日

目录

Cisco AsyncOS API for Email 概述

Cisco AsyncOS API for Email（或 AsyncOS API）是基于表述性状态转移 (REST) 的操作集合，允许对邮件安全设备报告和报告计数器进行经过身份验证的安全访问。您可以使用此 API 检索邮件安全设备报告数据。

思科系统公司
www.cisco.com

使用 AsyncOS API 的先决条件

要使用 AsyncOS API，您需要：

- 运行于 Cisco AsyncOS 9.0 for Email 或更高版本的邮件安全设备。
- 了解以下相关知识：
  - HTTP （用于 API 事务的协议）。
  - 通过 TLS 进行的安全通信。
  - JavaScript Object Notation (JSON)， API 用来构建资源表述。
- 使用 HTTP 或 HTTPS 启动请求并从 AsyncOS API 接收响应的客户端或编程库，例如 cURL。该客户端或编程库必须支持 JSON 才能解释来自 API 的响应。
- 访问 AsyncOS API 的授权。请参阅授权 （第 3 页）。
- 使用 Web 界面或 CLI 启用 AsyncOS API。请参阅启用 AsyncOS API （第 2 页）。

启用 AsyncOS API

准备工作

确保您已获得授权，可以访问 Web 界面上的 “IP 接口” (IP Interfaces) 页面或者 CLI 上的 `interfaceconfig` 命令。只有管理员和操作员获得授权，才能访问此页面或命令。

程序

步骤 1 登录 Web 界面。

步骤 2 单击**网络 (Network) > IP 接口 (IP Interfaces)**。

步骤 3 编辑 Management 接口。

注意 您可以在任意 IP 接口上启用 AsyncOS API。但是，思科建议您在 Management 接口上启用 AsyncOS API。

步骤 4 在 “AsyncOS API (监控)” (AsyncOS API [Monitoring]) 部分下,根据您的要求,选择 HTTP 和/或 HTTPS 以及要使用的端口。

注意 AsyncOS API 使用 HTTP/1.0 进行通信。

如果您选择了 HTTPS，并且想要使用自己的证书进行安全通信，请参阅与 AsyncOS API 进行安全通信 （第 3 页）。

注意 Cisco 建议您在生产环境中始终使用 HTTPS。 HTTP 仅用于故障排除和测试 API。

步骤 5 提交并确认更改。

您还可以在 CLI 中使用 `interfaceconfig` 命令启用 AsyncOS API。

与 AsyncOS API 进行安全通信

您可以使用自己的证书通过安全 HTTP 与 AsyncOS API 进行通信。

注意 如果您已经通过 HTTPS 运行 Web 界面并使用自己的证书进行安全通信，请勿执行此程序。AsyncOS API 与 Web 界面使用相同的证书，以便通过 HTTPS 进行通信。

程序

步骤 1 在 Web 界面上使用**网络 (Network) > 证书 (Certificates)** 页面或者在 CLI 中使用 `certconfig` 命令设置证书。有关说明，请参阅《*Cisco AsyncOS for Email 用户指南*》或者联机帮助。

步骤 2 在 Web 界面上使用**网络 (Network) > IP 接口 (IP Interfaces)** 页面或者在 CLI 中使用 `interfaceconfig` 命令将 IP 接口使用的 HTTPS 证书更改为您的证书。有关说明，请参阅《*Cisco AsyncOS for Email 用户指南*》或者联机帮助。

步骤 3 提交并确认更改。

AsyncOS API 身份验证和授权

授权

具有以下角色的邮件安全设备用户可以访问 AsyncOS API：

- 管理员
- 只读操作员
- 操作员
- 访客

注意 集中身份验证系统 （LDAP 或 RADIUS 目录）的用户无权访问 Cisco AsyncOS API for Email。如果 LDAP 或 RADIUS 目录用户尝试访问 API， API 会发送一条 401 错误消息。

身份验证

对于针对 API 的所有请求，API 用户必须提交 base64 编码格式的邮件安全设备用户名和密码。如果请求在 Authorization 标头中不包含有效凭证，则 API 会发送一条 401 错误消息。

您可以使用任意 base64 库将您的凭证转换为 base64 编码格式。下表显示了 base64 编码凭证的示例：

项目	值
用户名	`administrator`
密码	`Password$123`
凭证	`administrator:Password$123`
Base64 编码凭证	`YWRtaW5pc3RyYXRvcjpQYXNzd29yZCQxMjM=`

注意 编码的凭证在标头中必须位于单独一行。

AsyncOS API 请求和响应

AsyncOS API 请求

对 API 执行的请求具有以下特征：

- 请求将通过 HTTP 或 HTTPS 发送
- 每个请求必须包含采用以下格式的有效 URI：
  `https://{appliance}:{port}/api/v1.0/{resource}?{resource_attributes}`，其中：
  - `{appliance}:{port}` 是设备的 FQDN 或 IP 地址以及设备在其上进行侦听的 TCP 端口号。
  - `{resource}` 是您正尝试访问的资源，例如报告或计数器。
  - `{resource_attributes}` 是资源支持的属性，如持续时间、最长时间等。
- 每个请求必须包含采用 base64 编码格式的有效 Authorization 标头。
- 每个请求必须将 Accept 设置为：`application/json`
- 通过 HTTPS 发送的请求 （使用您自己的证书）必须包含您的 CA 证书。例如，如果使用 cURL，您可以在 API 请求中指定 CA 证书，如下所示：

```
curl --cacert <ca_cert.crt> -u "username:password"
https://<fqdn>:<port>/api/v1.0/{resource}?{resource_attributes}
```

注意 API 请求区分大小写，并且应按照本手册所示进行输入。

请求结构

下表列出可与 AsyncOS API 结合使用的请求操作类型。

请求类型	说明
GET	从指定资源请求数据。

下表列出请求的强制性标头：

标头	值	说明
Host	`{appliance}:{port}`	设备的域名或 IP 地址，以及设备在其上进行侦听的 TCP 端口号。
Accept	• `application/json` • `*/*`	向服务器指示此客户端愿意接受的介质类型，包括资源版本。
Authorization	Basic {base64-encoded(username:password)}	识别提交此请求的授权用户。

AsyncOS API 响应

响应的主要组成部分

组成部分		值	说明
状态码和原因		请参阅HTTP 响应代码（第 6 页）。	HTTP 响应代码和原因。
消息标头	Content-Type	• `application/json`	表示消息正文的格式。
	Content-Length	不适用	响应正文的长度 （八位字节）。
	Connection	`close`	连接所需的选项。

消息正文		不适用	消息正文的格式由 Content-Type 标头定义。以下是消息正文的组成部分：
			1. URI。您在请求中为 API 指定的 URI。
			示例
			`"uri":"/api/v1.0/health/"`
			2. 链接或数据。
			– 链接。层次结构中下一级资源的列表。
			示例
			`"links": {"percentage_ram_utilization": "Percentage...}`
			– 数据。 API 基于指定的 URI 提供的报告数据。
			示例
			`"data": {"percentage_diskio": 10}`
			3. （仅针对错误事件）错误。该组成部分包含三个子组成部分：消息、代码和说明。
			示例
			`"error": {"message": "Unexpected attribute - starts_with.", "code": "404", "explanation": "404 = Nothing matches the given URI."}`
			注意 如果消息正文包含空花括号 ({})，则表示 API 找不到任何与查询匹配的记录。

HTTP 响应代码

以下是 AsyncOS API 返回的 HTTP 响应代码列表：

- 200
- 400
- 401
- 404
- 406
- 413
- 414

- 500
- 501
- 505

有关这些 HTTP 响应代码的说明，请参阅以下 RFC：

- RFC1945
- RFC7231

AsyncOS API 功能

您可以使用 AsyncOS API 执行以下操作：

- 检索设备当前的运行状况参数 （第 7 页）
- 检索邮件安全设备统计报告 （第 8 页）
- 访问 Cisco AsyncOS API for Email 联机帮助 （第 12 页）

检索设备当前的运行状况参数

您可以检索设备当前的主要运行状况参数，例如 RAM 利用率、队列利用率、工作队列中的消息等以了解设备的运行状况。

说明	检索邮件安全设备的主要运行状况参数。
摘要	`GET /api/v1.0/health` `GET /api/v1.0/health/{parameter}`
请求头	Host、 Accept、 Authorization
响应头	Content-Type、 Content-Length、 Connection

示例

示例请求

```
GET /api/v1.0/health HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

示例响应

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Wed, 02 Jul 2014 05:07:50 GMT
Content-type: application/json
Content-Length: 246
Connection: close

{
    "data":{
        "percentage_ram_utilization":10,
        "percentage_diskio":20,
```

```
            "resource_conservation":3,
            "messages_in_workqueue":189,
            "messages_in_pvo_quarantines":12,
            "percentage_swap_utilization":2.0,
            "percentage_queue_utilization":5.0,
            "percentage_cpu_load":12
        },
        "uri":"/api/v1.0/health/"
}
```


注意 有关这些运行状况参数的详细信息，请使用以下 URI 访问 API 联机帮助：`https://{appliance}:{port}/api/v1.0/health/help`。请参阅访问 Cisco AsyncOS API for Email 联机帮助 （第 12 页）。

检索邮件安全设备统计报告

您可以从设备中检索各种统计报告，例如传入邮件摘要、病毒类型等。统计报告可分为三种不同类型：

- **简单的报告**。此报告类别会在指定时段内将各种事件计入设备，例如身份验证尝试失败次数、触发的内容过滤器数量等。例如 `mail_authentication_summary` 和 `mail_dlp_outgoing_traffic_summary`。
- **前 N 个报告**。此报告类别会在指定时段内根据某个实体 （IP 地址、域名等）将各种事件计入设备，并列出前 N 个事件，其中 N 是用户指定的值。例如 `mail_content_filter_incoming` 和 `mail_dmarc_incoming_traffic_summary`。
- **基于查询的报告**。此报告类别会在指定时段内根据用户指定的某个实体 （IP 地址、域名等）将各种事件计入设备。例如 `mail_authentication_incoming_domain` 和 `mail_content_filter_outgoing`。

有关每个类别下的报告列表，请参阅统计报告 （第 13 页）。

说明	从邮件安全设备检索各种统计报告。
摘要	`GET /api/v1.0/stats/report?resource_attribute` `GET /api/v1.0/stats/report/counter?resource_attribute`

支持的资源属性	**简单的报告**	• time_range。使用此属性可检索指定时段内的报告。此属性可以设置为以下值： – 1h - 汇总之前一小时的报告 – 1d - 汇总之前一天的报告 – duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD - 汇总指定时段的报告。支持的 TZD 值包括 Z、 +hh:mm 或 -hh:mm。
	前 N 个报告	• time_range。使用此属性可检索指定时段内的报告。此属性可以设置为以下值： – 1h - 汇总之前一小时的报告 – 1d - 汇总之前一天的报告 – duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD - 汇总指定时段的报告。支持的 TZD 值包括 Z、 +hh:mm 或 -hh:mm。 • max=n。使用此属性可限制报告返回的结果数。 n 是您希望报告返回的结果数，可以设置为 1 到 1000 之间的值。
	基于查询的报告	• time_range。使用此属性可检索指定时段内的报告。此属性可以设置为以下值： – 1h - 汇总之前一小时的报告 – 1d - 汇总之前一天的报告 – duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD - 汇总指定时段的报告。支持的 TZD 值包括 Z、 +hh:mm 或 -hh:mm。 • entity=value。使用此属性可基于指定实体 （例如邮箱地址， IP 地址等）检索报告。您可以选择是完全匹配指定文本还是查找以指定文本开头的项目 （例如以 “ex”开头将匹配 “example.com”）。 **注意** 此属性的定义因报告类型而异。有关此属性的允许值，请参阅统计报告 （第 13 页）。 要检索以指定文本开头的项目，您必须将此属性与 starts_with 属性结合使用，例如 entity=us& starts_with=true。 • starts_with=value。使用此属性可检索以指定实体值开头的项目。此属性必须与 entity 属性结合使用，并且 value 必须设置为 true，例如 entity=us&starts_with=true。 • max=n。使用此属性可限制报告返回的结果数。 n 是您希望报告返回的结果数，可以设置为 1 到 1000 之间的值。 **注意** 不能在同一请求中使用 entity 和 max=n 属性。
请求头		Host、 Accept、 Authorization
响应头		Content-Type、 Content-Length、 Connection

注意 利用 AND (&) 运算符来使用多个属性，例如：
https://{appliance}:{port}/api/v1.0/stats/report/counter?attribute1&attribute2。

注意 有关统计报告和计数器的详细信息，请访问 API 联机帮助。请参阅访问 Cisco AsyncOS API for Email 联机帮助 （第 12 页）。

示例

简单的报告类型

以下示例显示如何检索之前一天的汇总传入邮件摘要报告。

示例请求

```
GET /api/v1.0/stats/mail_incoming_traffic_summary?1d HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

示例响应

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Tue, 15 Jul 2014 08:26:46 GMT
Content-type: application/json
Content-Length: 461
Connection: close

{
    "data":{
        "verif_decrypt_success":0,
        "detected_virus":1396438,
        "threat_content_filter":106728,
        "blocked_invalid_recipient":209054,
        "verif_decrypt_fail":0,
        "marketing_mail":0,
        "detected_amp":0,
        "ims_spam_increment_over_case":0,
        "total_recipients":827216461,
        "detected_spam":1265606,
        "total_clean_recipients":1977205,
        "blocked_dmarc":0,
        "malicious_url":14006,
        "total_threat_recipients":825239256,
        "blocked_reputation":822261430
    },
    "uri":"/api/v1.0/stats/mail_incoming_traffic_summary?1d"
}
```

前 N 个报告类型

以下示例显示如何检索指定时段内前五大主题的大量邮件。

示例请求

```
GET
/api/v1.0/stats/mail_subject_stats?duration=2014-04-23T00:00-00:00/2014-10-21T00:00-00:00&
max=5 HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

示例响应

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Tue, 15 Jul 2014 08:26:46 GMT
Content-type: application/json
Content-Length: 182
Connection: close

{
    "data":{
        "num_msgs":{
            "Buying judgments":44584,
            "Additional Income":39691,
            "Why pay more?":46044,
            "Message contains":50460,
            "Off shore":56954
        }
    },

"uri":"/api/v1.0/stats/mail_subject_stats?duration=2014-04-23T00:00-00:00/2014-10-21T00:00
-00:00&max=5"
}
```

基于查询的报告类型

以下示例显示如何检索指定时段内开头为 “2001::6”的 IP 地址的汇总传出发件人报告。

示例请求

```
GET
/api/v1.0/stats/mail_sender_ip_hostname_detail?duration=2014-04-23T00:00-00:00/2014-10-21T
00:00-00:00&entity=2001::63&starts_with=true HTTP/1.0
User-Agent: curl/7.30.0
Host: mail.example.com:8080
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Accept: application/json
```

示例响应

```
HTTP/1.0 200 OK
Server: EmailAPI/1.0
Date: Thu, 04 Sep 2014 09:27:58 GMT
Content-type: application/json
Content-Length: 633
Connection: close

{
    "data":{
        "2001::63":{
```

```
            "detected_virus":2,
            "threat_content_filter":0,
            "total_dlp_incidents":0,
            "total_clean_recipients":4372,
            "total_recipients_processed":4374,
            "detected_spam":0,
            "total_threat_recipients":2
        }
        "2001::6":{
            "detected_virus":2,
            "threat_content_filter":0,
            "total_dlp_incidents":0,
            "total_clean_recipients":1232,
            "total_recipients_processed":1234,
            "detected_spam":0,
            "total_threat_recipients":2
        }
    },
"uri":"/api/v1.0/stats/mail_sender_ip_hostname_detail?duration=2014-04-23T00:00-00:00/2014
-10-21T00:00-00:00&entity=2001::6&starts_with=true"
}
```


访问 Cisco AsyncOS API for Email 联机帮助

AsyncOS API 为所有支持的报告和计数器提供了全面的联机帮助。您可以通过将 `/help` 附加到报告或计数器的 URI 来访问其联机帮助。

下面给出了几个示例：

- `GET /api/v1.0/stats/help` 允许您检索统计报告及其说明的列表。
- `GET /api/v1.0/health/help` 允许您检索设备主要运行状况参数及其说明的列表。
- `GET /api/v1.0/stats/mail_incoming_traffic_summary/help` 允许您检索传入邮件摘要报告的说明、此报告中的计数器及说明以及报告类型说明。
- `GET /api/v1.0/stats/mail_incoming_traffic_summary/detected_virus/help` 允许您检索传入邮件摘要报告中计数器 “`detected_virus`” 的说明。

对 AsyncOS API 进行故障排除

API 日志

使用**系统管理 (System Administration) > 日志订阅 (Log Subscriptions)** 订阅 API 日志。有关说明，请参阅 《*Cisco AsyncOS for Email 用户指南*》或联机帮助。

以下是 API 日志中记录的某些事件。

- API 已启动或停止
- 与 API 的连接失败或关闭 （在提供响应后）
- 身份验证成功或失败

- 请求包含错误
- 与 AsyncOS API 进行网络配置更改通信时出现错误

警报

确保设备配置为向您发送与 AsyncOS API 相关的警报。当出现以下情况时，您将收到警报：

报警说明	类型	严重性
API 由于出现错误而重新启动	系统	警告
使用 Web 界面或 CLI 进行的网络配置或证书更改未传达至 API。请参阅关于网络配置或证书更改的警报未传达至 AsyncOS API （第 13 页）。	系统	严重

关于网络配置或证书更改的警报未传达至 AsyncOS API

问题 您收到严重警报，指出使用 Web 界面或 CLI 进行的网络配置或证书更改未传达至 API。

解决方案 尝试执行以下操作：

- 重新启动设备。
- 如果问题仍然存在，请联系 TAC。

使用 cURL 时证书出错

问题 如果您在某些操作系统（例如 Unix、Ubantu、Mac OS X 等）上使用 HTTPS 和您自己的证书与 API 进行安全通信，则使用 cURL 请求 API 资源时可能会收到证书错误。下面给出了几个示例：

- `curl: (60) SSL certificate problem: Invalid certificate chain`
- `curl: (77) error setting certificate verify locations`

解决方案 请参阅 cURL 相关文档：http://curl.haxx.se/。

AsyncOS API 参考

统计报告

简单的报告

- mail_incoming_malware_threat_file_detail_summary
- mail_incoming_traffic_summary
- mail_outgoing_traffic_summary
- mail_security_summary
- mail_sender_group_summary
- mail_system_capacity

mail_authentication_summary

说明

传入邮件的 SMTP 身份验证统计信息摘要。

Web 界面报告

监控 (Monitor) > 入站 SMTP 身份验证 (Inbound SMTP Authentication) > 已接收的连接 (Received Connections)

计数器	说明
received_conn_cert_success	已使用客户端证书进行身份验证的成功传入连接总数
received_auth	已经接收并通过身份验证的收件人总数
received_total	已经接收的收件人总数
received_conn_auth_success	已使用 SMTP AUTH 命令进行身份验证的成功传入连接总数
received_conn_total	传入连接总数
received_noauth	已经接收的未进行身份验证的收件人总数
received_conn_auth_fail	未能使用 SMTP AUTH 命令进行身份验证的已接收连接总数。
received_conn_noauth	没有进行身份验证尝试的传入连接总数
received_conn_cert_fail	未能通过客户端证书进行身份验证的传入连接总数

mail_dlp_outgoing_traffic_summary

说明

传出邮件中发生的防数据丢失 (DLP) 策略违规事件的摘要。

Web 界面报告

监控 (Monitor) > DLP 事件摘要 (DLP Incident Summary) > 按严重性排列的最前面的事件 (Top Incidents by Severity)

计数器	说明
total_dlp_incidents	DLP 事件总数
dlp_incidents_high	严重性为高的 DLP 事件总数
dlp_incidents_critical	严重性为严重的 DLP 事件总数

计数器	说明
dlp_incidents_medium	严重性为中的 DLP 事件总数
dlp_incidents_low	严重性为低的 DLP 事件总数

mail_incoming_malware_threat_file_detail_summary

说明

高级恶意软件防护 (AMP) 在传入邮件中检测到的恶意软件威胁文件的详细信息。

Web 界面报告

监控 (Monitor) > 高级恶意软件防护 (Advanced Malware Protection) > 排名靠前的传入恶意软件威胁文件 (Top Incoming Malware Threat Files)

计数器	说明
detected_amp_files	AMP 检测到的恶意软件威胁文件的总数

mail_incoming_traffic_summary

说明

设备上的传入邮件活动摘要。

Web 界面报告

监控 (Monitor) > 概述 (Overview) > 传入邮件图 (Incoming Mail Graph)

计数器	说明
verif_decrypt_success	作为 S/MIME 网关验证和解密的一部分成功通过验证或解密的传入邮件 （收件人）总数
detected_virus	被识别为病毒邮件的邮件 （收件人）数量
threat_content_filter	使用删除、退回或隔离操作触发了至少一个内容过滤器的邮件 （收件人）数量
verif_decrypt_fail	未作为 S/MIME 网关验证和解密的一部分通过验证或解密的传入邮件 （收件人）总数
blocked_dmarc	被 DMARC 阻止的邮件 （收件人）总数
marketing_mail	被检测为市场营销邮件的邮件 （收件人）总数
detected_amp	被 AMP 检测为恶意软件的邮件 （收件人）总数
ims_spam_increment_over_case	虽然被 IMS 归类为垃圾邮件，但是本来可以被 IPAS 归类为正常邮件的传入邮件 （收件人）
total_recipients	邮件 （收件人）总数
detected_spam	被识别为垃圾邮件或可疑垃圾邮件的邮件 （收件人）数量。该值是所有已配置反垃圾邮件引擎检测到的垃圾邮件数量之和
total_clean_recipients	正常邮件 （收件人）总数
blocked_invalid_recipient	收件人接受策略拒绝的邮件 （收件人）数量

计数器	说明
malicious_url	被识别为恶意的 URL （收件人）数量
total_threat_recipients	设备检测到的威胁邮件 （收件人）总数
blocked_reputation	由声誉过滤阻止的邮件数量

mail_outgoing_traffic_summary

说明

设备上的传出邮件活动摘要。

Web 界面报告

监控 (Monitor) > 概述 (Overview) > 传出邮件图 (Outgoing Mail Graph)

计数器	说明
detected_virus	被识别为病毒邮件的邮件数量
threat_content_filter	使用删除、退回或隔离操作触发了至少一个内容过滤器的邮件（收件人）数量
total_dlp_incidents	DLP 阻止的邮件 （收件人）总数
total_clean_recipients	正常邮件 （收件人）总数
total_recipients_processed	正常邮件、病毒邮件、垃圾邮件或被过滤器阻止的邮件 （收件人）的总数
total_recipients	邮件 （收件人）总数
detected_spam	被识别为垃圾邮件或可疑垃圾邮件的邮件 （收件人）数量。该值是所有已配置反垃圾邮件引擎检测到的垃圾邮件数量之和
total_hard_bounces	被目标服务器硬退回的邮件 （收件人）总数
malicious_url	被识别为恶意的 URL 数量
total_recipients_delivered	传送的邮件 （收件人）总数

mail_security_summary

说明

传入和传出邮件的传输层安全 (TLS) 摘要。

Web 界面报告

监控 (Monitor) > TLS 连接 (TLS Connections) > 传入 TLS 连接图 (Incoming TLS Connections Graph)

计数器	说明
sent_conn_plain	未加密的传出连接总数
received_unencrypted	传入邮件中的未加密邮件 （收件人）总数
received_total	已经接收的收件人总数
received_conn_tls_success	成功 （需要 TLS）的传入 TLS 连接的总数

计数器	说明
received_conn_total	传入连接总数
sent_total	已经发送的收件人总数
sent_unencrypted	传出邮件中的未加密邮件 （收件人）总数
received_conn_tls_opt_fail	失败 （首选 TLS）的传入 TLS 连接的总数
sent_conn_tls_opt_success	成功 （首选 TLS）的传出 TLS 连接的总数
sent_conn_total	传出连接总数
sent_conn_tls_opt_fail	失败 （首选 TLS）的传出 TLS 连接的总数
received_encrypted_tls	传入邮件中的 TLS 加密邮件 （收件人）总数
sent_conn_tls_fail	失败 （需要 TLS）的传出 TLS 连接的总数
received_conn_tls_opt_success	成功 （首选 TLS）的传入 TLS 连接的总数
received_conn_plain	未加密的传入连接总数
sent_conn_tls_success	成功 （需要 TLS）的传出 TLS 连接的总数
sent_encrypted_tls	传出邮件中的 TLS 加密邮件 （收件人）总数
received_conn_tls_fail	失败 （需要 TLS）的传入 TLS 连接的总数

mail_sender_group_summary

说明

按设备上的所有发件人组的邮件流策略操作列出的连接摘要。

Web 界面报告

监控 (Monitor) > TLS 连接 (TLS Connections) > 传入 TLS 连接图 (Incoming TLS Connections Graph)

计数器	说明
connections_relay	经过中继邮件流策略操作的连接总数
connections_reject	经过拒绝邮件流策略操作的连接总数
connections_accept	经过接受邮件流策略操作的连接总数
connections_tcp_refuse	经过 TCP 拒绝邮件流策略操作的连接总数

mail_system_capacity

说明

设备的系统容量参数摘要。

Web 界面报告

监控 (Monitor) > 系统容量 (System Capacity) > 工作队列 (Work Queue)

计数器	说明
workqueue_average_time_spent	工作队列中花费的平均时间 （以秒为单位）
overall_percent_cpu_usage_for_reporting	报告功能的 CPU 总平均使用率百分比
outgoing_connections	传出连接总数
overall_percent_cpu_usage	CPU 总平均使用率百分比
bytes_in	传入邮件总大小 （字节）
overall_percent_cpu_usage_for_antivirus	防病毒功能的 CPU 总平均使用率百分比
overall_percent_cpu_usage_for_quarantine	隔离区的 CPU 总平均使用率百分比
average_incoming_message_size_in_bytes	传入邮件平均大小 （字节）
overall_percent_cpu_usage_for_antispam	反垃圾邮件功能的 CPU 总平均使用率百分比
average_outgoing_message_size_in_bytes	传出邮件平均大小 （字节）
overall_percent_cpu_usage_for_mail_count	邮件处理功能的 CPU 总平均使用率百分比
workqueue_average_messages	工作队列中的平均邮件数
bytes_out	传出邮件总大小 （字节）
outgoing_messages	传出邮件总数
average_memory_page_swapping	平均内存页面交换
incoming_connections	传入连接总数
incoming_messages	传入邮件总数
workqueue_messages_max	工作队列中的最大邮件数

前 N 个报告

- mail_authentication_incoming_domain_ip
- mail_content_filter_incoming
- mail_dmarc_incoming_traffic_summary
- mail_env_sender_rate_limit
- mail_env_sender_stats
- mail_hvm_msg_filter_stats
- mail_incoming_malware_threat_file_detail
- mail_msg_filter_stats
- mail_sender_group_detail
- mail_subject_stats
- mail_url_category_summary
- mail_url_domain_summary
- mail_url_reputation_summary
- mail_vof_threat_summary
- mail_vof_threats_by_level

- mail_vof_threats_by_threat_type
- mail_vof_threats_by_time_threshold
- mail_vof_threats_by_type
- mail_vof_threats_rewritten_url

mail_authentication_incoming_domain_ip

说明

有关每个域 IP 地址的传入电子邮件身份验证的信息。

Web 界面报告

没有报告

计数器	说明
last_cert_fallback	从域 IP 地址进行身份验证从客户端证书至 SMTP AUTH 命令的最后一次回退接收的连接
last_cert_success	使用客户端证书从域 IP 地址进行身份验证的最后一次成功接收的连接
last_auth_disallow	不允许使用 SMTP AUTH 命令从域 IP 地址进行身份验证的最后一次接收的连接
last_cert_fail	使用客户端证书从域 IP 地址进行身份验证的最后一次失败接收的连接
last_auth_success	使用 SMTP AUTH 命令从域 IP 地址进行身份验证的最后一次成功接收的连接
last_auth_fail	使用 SMTP AUTH 命令从域 IP 地址进行身份验证的最后一次失败接收的连接

mail_content_filter_incoming

说明

传入内容过滤器匹配数详细信息。

Web 界面报告

监控 (Monitor) > 内容过滤器 (Content Filters) > 排名靠前的传入内容过滤器匹配数 (Top Incoming Content Filter Matches)

计数器	说明
recipients_matched	内容过滤器匹配传入收件人总数

mail_dmarc_incoming_traffic_summary

说明

关于传入邮件的 DMARC 验证的信息。

Web 界面报告

监控 (Monitor) > DMARC 验证报告 (DMARC Verification Report) > 按 DMARC 验证失败情况排列的最前面的域 (Top Domains by DMARC Verification Failures)

计数器	说明
dmarc_total_attempted	每个域需要接受 DMARC 验证的邮件 （收件人）总数
dmarc_failed_total	每个域未通过 DMARC 验证的邮件 （收件人）总数
dmarc_failed_rejected	每个域未通过 DMARC 验证并被拒绝的邮件 （收件人）总数
dmarc_failed_none	每个域未通过 DMARC 验证并且未采取任何操作的邮件 （收件人）总数
dmarc_failed_quarantined	每个域未通过 DMARC 验证并被隔离的邮件 （收件人）总数
dmarc_passed	每个域通过 DMARC 验证的邮件 （收件人）总数

mail_env_sender_rate_limit

说明

速率限制策略违反者的详细信息。

Web 界面报告

监控 (Monitor) > 速率限制 (Rate Limits) > 按事件排列的最前面的违反者 (Top Offenders by Incident)

计数器	说明
env_sender_incidents	按信封发件人列出的事件总数
env_sender_rejected_rcpts	按拒绝的收件人列出的事件总数

mail_env_sender_stats

说明

按信封发件人列出的邮件详细信息。

Web 界面报告

监控 (Monitor) > 大量邮件 (High Volume Mail) > 排名靠前的信封发件人 (Top Envelope Senders)

计数器	说明
num_msgs	来自信封发件人的邮件总数

mail_hvm_msg_filter_stats

说明

大量邮件 (HVM) 邮件过滤器 （使用信头重复规则）的统计信息。

Web 界面报告

监控 (Monitor) > 大量邮件 (High Volume Mail) > 按匹配数排列的最前面的邮件过滤器 (Top Message Filters by Number of Matches)

计数器	说明
num_matches	按过滤器列出的匹配邮件总数

mail_incoming_malware_threat_file_detail

说明

高级恶意软件防护 (AMP) 在传入邮件中检测到的恶意软件威胁文件的详细信息。

Web 界面报告

监控 (Monitor) > 高级恶意软件防护 (Advanced Malware Protection) > 排名靠前的传入恶意软件威胁文件 (Top Incoming Malware Threat Files)

计数器	说明
detected_amp_files	AMP 检测到的恶意软件威胁文件的总数

mail_msg_filter_stats

说明

设备上的邮件过滤器匹配数详细信息。

Web 界面报告

监控 (Monitor) > 邮件过滤器 (Message Filters) > 按匹配数排列的排名靠前的邮件过滤器 (Top Message Filters by Number of Matches)

计数器	说明
num_matches	按邮件过滤器列出的匹配邮件 （收件人）总数

mail_sender_group_detail

说明

按发件人组列出的连接详细信息。

Web 界面报告

监控 (Monitor) > 发件人组 (Sender Groups) > 按发件人组列出的连接 (Connections by Sender Group)

计数器	说明
total_connections	按发件人组列出的连接总数

mail_subject_stats

说明

由设备接收的邮件的主题统计信息。

Web 界面报告

监控 (Monitor) > 大量邮件 (High Volume Mail) > 排名靠前的主题 (Top Subjects)

计数器	说明
num_msgs	按主题列出的邮件 （收件人）总数

mail_url_category_summary

说明

有关传入和传出邮件中出现的 URL 类别的信息。

Web 界面报告

监控 (Monitor) > URL 过滤 (URL Filtering) > 传入邮件中排名靠前的 URL 类别 (Top URL Categories in Incoming Messages)

计数器	说明
outgoing_count	传出邮件的 URL 类别分布
incoming_count	传入邮件的 URL 类别分布

mail_url_domain_summary

说明

有关传入和传出垃圾邮件中出现的 URL 域的信息。

Web 界面报告

监控 (Monitor) > URL 过滤 (URL Filtering) > 传入垃圾邮件中排名靠前的 URL (Top URLs in Incoming Spam Messages)

计数器	说明
outgoing_count	按传出垃圾邮件中的域列出的 URL 数量
incoming_count	按传入垃圾邮件中的域列出的 URL 数量

mail_url_reputation_summary

说明

有关传入和传出邮件中出现的恶意和可疑 URL 的信息。

Web 界面报告

监控 (Monitor) > URL 过滤 (URL Filtering) > 包含恶意和可疑 URL 的传入邮件概要 (Summary of Incoming Messages Containing Malicious and Suspicious URLs)

计数器	说明
outgoing_count	传出邮件的 URL 信誉分布
incoming_count	传入邮件的 URL 信誉分布

mail_vof_threat_summary

说明

关于由病毒爆发过滤器检测到的威胁的信息。

Web 界面报告

监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters) > 威胁摘要 (Threat Summary)

计数器	说明
threat_detected	由病毒爆发过滤器检测到的每个威胁类别的威胁数量

mail_vof_threats_by_level

说明

关于由病毒爆发过滤器检测到的威胁的严重性信息。

Web 界面报告

监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters) > 按威胁级别命中邮件 (Hit Messages by Threat Level)

计数器	说明
threat_detected	由病毒爆发过滤器检测到的每个威胁级别的威胁数量

mail_vof_threats_by_threat_type

说明

关于由病毒爆发过滤器检测到的威胁类型的信息。

Web 界面报告

监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters) > 命中传入邮件中的邮件 (Hit Messages from Incoming Messages)

计数器	说明
threat_detected	由病毒爆发过滤器检测到的每个威胁类型的威胁数量

mail_vof_threats_by_time_threshold

说明

关于病毒爆发过滤器 (OF) 隔离区中的邮件的信息。

Web 界面报告

监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters) > 病毒爆发隔离区中驻留的邮件 (Messages resided in Outbreak Quarantine)

计数器	说明
quarantine_message_exit	按隔离区中花费的时间列出的由病毒爆发过滤器隔离的邮件数量

mail_vof_threats_by_type

说明

关于由病毒爆发过滤器检测到的威胁类型的信息。

Web 界面报告

监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters) > 按类型列出的威胁 (Threats by Type)

计数器	说明
threat_detected	由病毒爆发过滤器检测到的每个威胁类型的威胁数量

mail_vof_threats_rewritten_url

说明

关于由病毒爆发过滤器重新写入的 URL 的信息。

Web 界面报告

监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters) > 排名靠前的重新写入的 URL (Top URL's Rewritten)

计数器	说明
rewritten_url	由病毒爆发过滤器重新写入的每个 URL 的 URL 数量

查询特定的报告

- mail_authentication_incoming_domain
- mail_content_filter_outgoing
- mail_destination_domain_detail
- mail_dlp_outgoing_policy_detail
- mail_incoming_domain_detail
- mail_incoming_ip_hostname_detail

- mail_incoming_network_detail
- mail_sender_domain_detail
- mail_sender_ip_hostname_detail
- mail_users_detail
- mail_virus_type_detail

mail_authentication_incoming_domain

说明

按域列出的传入邮件中出现的 SMTP 身份验证统计详细信息。

Web 界面报告

监控 (Monitor) > 入站 SMTP 身份验证 (Inbound SMTP Authentication) > 按域名列出的 SMTP 身份验证详细信息 (SMTP Authentication Details By Domain Name)

实体值

域名

计数器	说明
cert_fallback_success	在域中身份验证从客户端证书退回至 SMTP AUTH 命令的成功传入（已接收）连接总数
cert_fallback_fail	在域中身份验证未能从客户端证书退回至 SMTP AUTH 命令的传入（已接收）连接总数
auth_disallow	不允许在域中使用 SMTP AUTH 命令进行身份验证的传入 （已接收）连接总数
auth_fail	未能在域中使用 SMTP AUTH 命令进行身份验证的传入 （已接收）连接总数
cert_success	在域中已使用客户端证书进行身份验证的成功传入 （已接收）连接总数
noauth	没有进行身份验证尝试的传入 （已接收）连接总数
auth_success	在域中使用 SMTP AUTH 命令进行身份验证的成功传入 （已接收）连接总数
cert_fail	在域中未能使用客户端证书进行身份验证的传入 （已接收）连接总数
总业务销量	已接收连接总数

mail_content_filter_outgoing

说明

传出内容过滤器匹配数详细信息。

Web 界面报告

没有报告

实体值

传出内容过滤器的名称

计数器	说明
recipients_matched	内容过滤器匹配传出收件人总数

mail_destination_domain_detail

说明

发送到目标域的邮件详细信息。

Web 界面报告

监控 (Monitor) > 传出目标 (Outgoing Destinations) > 按威胁邮件总数排列的最前面的目标 (Top Destinations by Total Threat Messages)

实体值

域名

计数器	说明
传送到	发送至目标域的邮件 （收件人）总数
detected_virus	发送至目标域且被识别为病毒邮件的邮件 （收件人）数量
encrypted_tls	使用 TLS 发送的邮件 （收件人）总数
threat_content_filter	发送至目标域且使用删除、退回或隔离操作触发了至少一个内容过滤器的邮件 （收件人）数量
conn_tls_total	使用 TLS 发送的连接总数
conn_tls_opt_fail	按目标域列出的失败 （首选 TLS） TLS 连接的总数
total_clean_recipients	发送至目标域的正常邮件 （收件人）总数
total_recipients_processed	发送至目标域的正常邮件、病毒邮件、垃圾邮件或被过滤器阻止的邮件 （收件人）的总数
conn_tls_opt_success	按目标域列出的成功 （首选 TLS） TLS 连接的总数
conn_plain	非 TLS 连接总数
conn_tls_success	按目标域列出的成功 （TLS 必需） TLS 连接的总数
total_recipients	发送至目标域的邮件 （收件人）总数
conn_tls_fail	按目标域列出的失败 （TLS 必需） TLS 连接的总数
detected_spam	发送至目标域且被识别为垃圾邮件或可疑垃圾邮件 （收件人）数量
conn_last_tls_status	上一 TLS 连接状态
hard_bounces	发送至目标域并被目标服务器硬退回的邮件 （收件人）总数
total_threat_recipients	发送至目标域的威胁邮件 （收件人）总数

mail_dlp_outgoing_policy_detail

说明

传出邮件中发生的防数据丢失 (DLP) 策略违规事件的详细信息。

Web 界面报告

监控 (Monitor) > DLP 事件摘要 (DLP Incident Summary) > 排名靠前的 DLP 策略匹配数 (Top DLP Policy Matches)

实体值

DLP 策略名称

计数器	说明
dlp_action_dropped	已删除的与 DLP 策略匹配的收件人 （邮件）总数
dlp_incidents_high	按策略匹配数列出的严重性为高的 DLP 事件总数
dlp_incidents_critical	按策略匹配数列出的严重性为严重的 DLP 事件总数
dlp_action_encrypted	已发送 （加密）的与 DLP 策略匹配的收件人 （邮件）总数
total_dlp_incidents	DLP 事件总数
dlp_action_delivered	已发送 （清除）的与 DLP 策略匹配的收件人 （邮件）总数
dlp_incidents_medium	按策略匹配数列出的严重性为中的 DLP 事件总数
dlp_incidents_low	按策略匹配数列出的严重性为低的 DLP 事件总数

mail_incoming_domain_detail

说明

用于连接域的传入邮件活动的详细信息。

Web 界面报告

监控 (Monitor) > 传入邮件域 (Incoming Mail Domains) > 排名靠前的 DLP 策略匹配数 (Top DLP Policy Matches)

实体值

域名

计数器	说明
total_throttled_recipients	按域列出的已限制收件人总数
conn_tls_total	按域列出的 TLS 连接总数
detected_virus	每个域被识别为病毒邮件的邮件 （收件人）总数
total_rejected_connections	按域列出的已拒绝连接总数
total_accepted_connections	按域列出的已接受连接总数
threat_content_filter	每个域被内容过滤器阻止的邮件 （收件人）总数
conn_tls_opt_fail	按域列出的失败 （首选 TLS） TLS 连接的总数。
blocked_invalid_recipient	按域列出的无效收件人总数
blocked_dmarc	每个域由于 DMARC 验证被阻止的邮件 （收件人）总数
marketing_mail	每个域被识别为市场营销邮件的邮件 （收件人）总数
conn_plain	按域列出的非 TLS 连接总数

计数器	说明
detected_amp	每个域被高级恶意软件防护识别的邮件 （收件人）总数
conn_tls_success	按域列出的成功 （TLS 必需） TLS 连接的总数
total_recipients	按域列出的尝试收件人总数
conn_tls_fail	按域列出的失败 （TLS 必需） TLS 连接的总数
detected_spam	每个域被识别为垃圾邮件或可疑垃圾邮件的邮件 （收件人）总数
encrypted_tls	通过 TLS 发送的邮件 （收件人）总数
total_clean_recipients	按域列出的正常邮件 （收件人）总数
total_threat_recipients	每个域的威胁邮件 （收件人）总数
blocked_reputation	按域列出的信誉经过滤的收件人总数
conn_tls_opt_success	按域列出的成功 （首选 TLS） TLS 连接的总数

mail_incoming_ip_hostname_detail

说明

用于连接 IP 地址和主机名的传入邮件活动的详细信息。

Web 界面报告

监控 (Monitor) > 传入邮件 IP 地址 (Incoming Mail IP Addresses) > 按威胁邮件总数排列的最前面的发件人 (Top Senders by Total Threat Messages)

实体值

IPv4 或 IPv6 地址

计数器	说明
dns_verified	已验证 IP 的 DNS
detected_virus	按 IP 列出的被识别为病毒邮件的邮件 （收件人）总数
threat_content_filter	使用删除、退回或隔离操作触发了至少一个内容过滤器的邮件总数
blocked_invalid_recipient	按 IP 列出的无效收件人总数
blocked_dmarc	按 IP 列出的由于 DMARC 验证失败被阻止的邮件 （收件人）总数
marketing_mail	按 IP 列出的被检测为市场营销邮件的邮件 （收件人）总数
detected_amp	按 IP 列出的被识别为 AMP 的邮件 （收件人）总数
last_sender_group_name	IP 的发件人组名称
sbrs_score	IP 的 SBRS 得分
total_recipients	按 IP 列出的尝试收件人总数
detected_spam	按 IP 列出的被识别为垃圾邮件或可疑垃圾邮件的邮件 （收件人）总数
total_clean_recipients	按 IP 列出的正常邮件 （收件人）总数
total_threat_recipients	按 IP 列出的垃圾邮件、病毒和威胁过滤器邮件 （收件人）总数
blocked_reputation	按 IP 列出的信誉经过滤的收件人总数

mail_incoming_network_detail

说明

网络所有者的传入邮件活动的详细信息。

Web 界面报告

监控 (Monitor) > 传入邮件网络所有者 (Incoming Mail Network Owners) > 按威胁邮件总数排列的最前面的发件人 (Top Senders by Total Threat Messages)

实体值

网络所有者的名称。

计数器	说明
total_throttled_recipients	网络所有者的已限制连接总数
detected_virus	网络所有者的被识别为病毒邮件的邮件 （收件人）总数
total_threat_recipients	网络所有者的威胁收件人总数
total_accepted_connections	网络所有者的已接受连接总数
threat_content_filter	网络所有者使用删除、退回或隔离操作触发了至少一个内容过滤器的邮件总数
blocked_invalid_recipient	网络所有者的无效收件人总数
blocked_dmarc	网络所有者由于 DMARC 验证失败被阻止的邮件总数
marketing_mail	网络所有者被检测为市场营销邮件的邮件 （收件人）总数
detected_amp	网络所有者被识别为 AMP 的邮件 （收件人）总数
total_recipients	网络所有者的收件人总数
detected_spam	网络所有者被识别为垃圾邮件或可疑垃圾邮件的邮件 （收件人）总数
total_clean_recipients	网络所有者正常邮件 （收件人）的总数
total_rejected_connections	网络所有者被拒绝的连接总数
blocked_reputation	网络所有者信誉经过滤的收件人总数

mail_sender_domain_detail

说明

传出内容过滤器匹配数详细信息。

Web 界面报告

监控 (Monitor) > 传出发件人域 (Outgoing Senders Domains) > 按威胁邮件总数排列的最前面的发件人 (Top Senders by Total Threat Messages)

实体值

域名

计数器	说明
detected_virus	域中被识别为病毒邮件的邮件 （收件人）总数
threat_content_filter	域中被内容过滤器阻止的邮件 （收件人）总数
total_dlp_incidents	域中的 DLP 事件总数
total_clean_recipients	域中正常邮件 （收件人）的总数
total_recipients_processed	域中正常邮件、病毒邮件、垃圾邮件或被过滤器阻止的邮件的总数
detected_spam	域中被识别为垃圾邮件或可疑垃圾邮件的邮件 （收件人）总数
total_threat_recipients	域中的威胁收件人总数

mail_sender_ip_hostname_detail

说明

发送邮件的内部 IP 和主机名详细信息

Web 界面报告

监控 (Monitor) > 传出发件人 IP 地址 (Outgoing Senders IP Addresses) > 威胁邮件总数排名靠前的发件人 (Top Senders by Total Threat Messages)

实体值

IPv4 或 IPv6 地址

计数器	说明
detected_virus	来自某个 IP 地址的被识别为病毒邮件的邮件 （收件人）总数
threat_content_filter	来自某个 IP 地址的被内容过滤器阻止的邮件 （收件人）总数
total_dlp_incidents	来自某个 IP 地址的 DLP 事件总数
total_clean_recipients	来自某个 IP 地址的传出邮件中正常邮件 （收件人）的总数
total_recipients_processed	来自某个 IP 地址的正常邮件或被识别为威胁邮件的邮件 （收件人）的总数
detected_spam	来自某个 IP 地址的被识别为垃圾邮件或可疑垃圾邮件的邮件 （收件人）总数
total_threat_recipients	来自某个 IP 地址的威胁收件人总数

mail_users_detail

说明

由您的内部用户 （按电子邮件地址）通过设备发送和接收的邮件的相关信息。

Web 界面报告

监控 (Monitor) > 内部用户 (Internal Users) > 按正常传入邮件排列的最前面的用户 (Top Users by Clean Incoming Messages)

实体值

内部用户的电子邮件地址

计数器	说明
incoming_detected_amp	被识别为 AMP 的传入邮件 （收件人）
outgoing_detected_content_filter	与内容过滤器匹配的传出邮件 （收件人）
incoming_marketing_mail	传入市场营销邮件 （收件人）
outgoing_detected_spam	被识别为垃圾邮件或可疑垃圾邮件的传出邮件 （收件人）数量该值是所有已配置反垃圾邮件引擎检测到的垃圾邮件数量之和
incoming_threat_content_filter	被内容过滤器阻止的传入邮件 （收件人）
incoming_total_clean_recipients	传入的正常邮件 （收件人）总数
incoming_detected_spam	被识别为垃圾邮件或可疑垃圾邮件的传入邮件 （收件人）数量该值是所有已配置反垃圾邮件引擎检测到的垃圾邮件数量之和
incoming_detected_content_filter	与内容过滤器匹配的传入邮件 （收件人）
incoming_detected_virus	被识别为病毒邮件的传入邮件 （收件人）
outgoing_detected_virus	被识别为病毒邮件的传出邮件 （收件人）
incoming_detected_ims_spam_increment_over_case	虽然被 IMS 归类为垃圾邮件，但是本来可以被 IPAS 归类为正常邮件的传入邮件 （收件人）
outgoing_total_clean_recipients	传出的正常邮件 （收件人）总数
outgoing_threat_content_filter	被内容过滤器阻止的传出邮件 （收件人）
outgoing_detected_ims_spam_increment_over_case	虽然被 IMS 归类为垃圾邮件，但是本来可以被 IPAS 归类为正常邮件的传出邮件 （收件人）

mail_virus_type_detail

说明

被设备识别的排名靠前的传入和传出病毒类型详细信息。

Web 界面报告

监控 (Monitor) > Virus Types (病毒类型) > 检测到的传入病毒类型排行榜 (Top Incoming Virus Types Detected)

实体值

病毒名称

计数器	说明
total_recipients	被前 n 种病毒类型感染的传入和传出邮件 （收件人）总数，其中 n 表示用户指定的值。默认值为前 10 种

计数器	说明
incoming_total_recipients	被前 n 种病毒类型感染的传入邮件 （收件人）总数，其中 n 表示用户指定的值。默认值为前 10 种
outgoing_total_recipients	被前 n 种病毒类型感染的传出邮件 （收件人）总数，其中 n 表示用户指定的值。默认值为前 10 种