AsyncOS 11.0 API - 邮件安全设备入门指南

首次发布日期: 2017 年 05 月 31 日

上次修改日期: --

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

文本部件号:

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的供应商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录

第 1 章

适用于思科邮件安全设备的 AsyncOS API - 入门指南

本章包含以下部分：

适用于思科邮件安全设备的 AsyncOS API 概述

适用于思科邮件安全设备的 AsyncOS API（或 AsyncOS API）是一系列基于具象状态传输 (REST) 的操作，通过它们，您可以对邮件安全设备报告和报告计数器进行安全且经过身份验证的访问。您可以使用此 API 检索邮件安全设备报告数据。

使用 AsyncOS API 的先决条件

要使用 AsyncOS API，您需要：

- 在 AsyncOS 9.0 或更高版本上运行的邮件安全设备。
- 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。

- 客户端或编程库，用来通过 HTTP 或 HTTPS（例如 cURL）发起请求和接收来自 AsyncOS API 的响应。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 启用的 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。

过程

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。

注释 您可以在任意 IP 接口上启用 AsyncOS API。不过，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。

注释 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。

注释 思科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。

接下来的操作

此外，您也可以在 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 进行安全通信。

注释 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 使用与 Web 界面相同的证书通过 HTTPS 进行通信。

过程

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，请参阅用户指南或联机帮助。

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，请参阅用户指南或联机帮助。

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

注释 来自集中身份验证系统（LDAP 或 RADIUS 目录）的用户无权访问适用于思科邮件安全设备的 AsyncOS API。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`
凭据	`administrator:Password$123`
Base64 编码凭证	`YWRtaW5pc3RyYXRvcjpQYXNzd29yZCQxMjM=`

注释 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}`
  为设备的 FQDN 或 IP 地址以及设备正在侦听的 TCP 端口号。

  `{resource}`
  为您尝试访问的资源，例如报告或计数器。

  `{resource_attributes}`
  为受支持的资源属性，例如持续时间、最大值等。

- 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}
```

注释 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

下表列出了可用于 AsyncOS API 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	价值观	描述
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

响应的关键组成部分

组成部分	值	描述
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。

组成部分		值	描述
消息标头	Content-Type	`application/json`	表示消息正文的格式。
	Content-Length	n/a	响应正文的长度（八位字节）。
	Connection	`close`	连接所需的选项。

消息内容		n/a	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."}`
			如果 消息正文包含空的大括号 ({})，则表示 API 找不到 匹配查询的任何记录。

HTTP 响应代码

下面列出了 AsyncOS API 返回的 HTTP 响应代码：

- 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

使用 AsyncOS API 可执行以下操作：

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

请求示例

```
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
```

响应示例

```
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/"
}
```

注释 有关这些运行状况参数的详细信息，请使用以下 URI 访问 API 内联帮助：
`https://{appliance}:{port}/api/v1.0/health/help.`
请参阅访问适用于思科邮件安全设备的 AsyncOS API 内联帮助，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。示例为
  `mail_authentication_summary and 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。示例为
  `mail_content_filter_incoming and 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。示例为
  `mail_authentication_incoming_domain and mail_content_filter_outgoing.`

有关每个类别下的 报告列表，请参阅 AsyncOS API 参考，第 14 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` - 过去一小时的汇总报告 `1d` - 过去一天的汇总报告 `duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD` - 指定时段内的汇总报告。 支持的 TZD 值为 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` - 过去一小时的汇总报告 `1d` - 过去一天的汇总报告 `duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD` - 指定时段的汇总报告。 支持的 TZD 值为 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 为希望报告返回的结果数， 其值可以设置为 1 到 1000。
	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` - 过去一小时的汇总报告 `1d` - 过去一天的汇总报告 `duration=YYYY-MM-DDThh:mmTZD/YYYY-MM-DDThh:mmTZD` - 指定时段内的汇总报告。 支持的 TZD 值为 Z、+hh:mm 或 -hh:mm。

		• `entity=value.` 使用 此属性可基于指定实体（例如邮件地址、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”）。 **注释** 此属性的定义因报告类型而异。有关 此属性允许的值，请参阅 AsyncOS API 参考，第 14 页。 要检索以指定文本开头的项目，必须将此属性与 starts_with 属性一起使用，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 属性一起使用， 值必须设置为 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 为希望报告返回的结果数， 其值可以设置为 1 到 1000。 **注释** 不能在同一请求中同时使用 entity 和 max=n 属性。
请求头		Host、Accept、Authorization
响应头		Content-Type、Content-Length、Connection

注释 使用 AND (&) 运算符可使用多个属性，例如：
`https://{appliance}:{port}/api/v1.0/stats/report/counter?attribute1&attribute2.`

有关统计报告和计数器 的详细信息，请访问 API 内联帮助。请参阅 访问适用于思科邮件安全设备的 AsyncOS API 内联帮助，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。

请求示例

```
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
```

响应示例

```
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
{
  "verif_decrypt_success": 0,
        "detected_virus": 99,
        "total_threat_recipients": 102,
        "threat_content_filter": 0,
        "total_recipients": 102,
        "blocked_invalid_recipient": 0,
        "blocked_dmarc": 0,
        "marketing_mail": 0,
        "ims_spam_increment_over_case": 0,
        "detected_amp": 0,
        "total_graymail_recipients": 0,
        "social_mail": 0,
        "detected_spam": 0,
        "total_clean_recipients": 0,
        "verif_decrypt_fail": 0,
        "malicious_url": 0,
        "bulk_mail": 0,
        "blocked_reputation": 3
    },
    "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。

请求示例

```
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
```

响应示例

```
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以“2001::6”开头的 IP 地址的“传出发件人”汇总报告。

请求示例

```
GET
/api/v1.0/stats/mail_sender_ip_hostname_detail?duration=2014-04-23T00:00-00:00/2014-10-21T00:00-00:00&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
```

响应示例


```
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"
}
```


访问适用于思科邮件安全设备的 AsyncOS API 内联帮助

AsyncOS API 面向支持的所有报告和计数器提供全面的内联帮助。您可以通过将报告或计数器的 URL 附加到以下部分来访问其内联帮助：

```
/help
```

下面是一些 示例：

- `GET /api/v1.0/stats/help`
  允许您检索统计报告列表及它们的说明。
- `GET /api/v1.0/ health /help`
  允许您检索设备的主要运行状况参数列表及它们的说明。
- `GET /api/v1.0/stats/mail_incoming_traffic_summary /help`
  允许您检索传入邮件摘要报告说明、此报告中支持的计数器及其说明以及报告类别。
- `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的计数器 “`detected_virus`” 的说明。

AsyncOS API 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
- 到 API 的连接失败或关闭（在响应后）
- 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：

警报说明	Type	严重性
API 由于出现错误而重新启动	System	Warning
使用 Web 界面或 CLI 进行的网络配置或证书更改未传达至 API。请参阅网络配置或证书更改未传达至 AsyncOS API 的警报，第 14 页。	System	Critical

网络配置或证书更改未传达至 AsyncOS API 的警报

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 时出现证书错误

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 文档：https://curl.haxx.se/。

AsyncOS API 参考

简单的报告类型

支持的简单报告如下：

- `mail_authentication_summary`
- `mail_dlp_outgoing_traffic_summary`
- `mail_incoming_malware_threat_file_detail_summary`
- `mail_incoming_traffic_summary`
- `mail_mailbox_auto_remediation`
- `mail_outgoing_traffic_summary`
- `mail_security_summary`
- `mail_sender_group_summary`
- `mail_system_capacity`

前 N 个报告类型

支持的前 N 个报告如下：

- mail_authentication_incoming_domain_ip
- mail_content_filter_incoming
- mail_dmarc_incoming_traffic_summary
- mail_env_sender_rate_limit
- mail_env_sender_stats
- mail_fed_content_filter_incoming
- mail_hvm_msg_filter_stats
- mail_incoming_hat_connections
- mail_incoming_malware_threat_file_detail
- mail_incoming_web_interaction_track_malicious_users
- mail_incoming_web_interaction_track_urls
- mail_md_attachment_incoming_file_type
- mail_md_attachment_outgoing_file_type
- mail_outgoing_web_interaction_track_malicious_users
- mail_outgoing_web_interaction_track_urls
- 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

特定于查询的报告类型

支持的特定于查询的报告如下：

- mail_authentication_incoming_domain

  实体值：域名，例如 abc.com.

- mail_content_filter_outgoing

  实体值：传出内容过滤器的名称。

- mail_destination_domain_detail

  实体值：域名，例如 abc.com.

- mail_dlp_outgoing_policy_detail

  实体值：DLP 策略的名称。

- mail_incoming_domain_detail

  实体值：域名，例如 abc.com.

- mail_incoming_ip_hostname_detail

  实体值：IPv4 或 IPv6 地址。

- mail_incoming_network_detail

  实体值：网络所有者的名称，例如 Xyz Corporation。

- mail_sender_domain_detail

  实体值：域名，例如 abc.com.

- mail_sender_ip_hostname_detail

  实体值：IPv4 或 IPv6 地址。

- mail_users_detail

  实体值：内部用户的邮件 ID，例如 user@example.com。

- mail_virus_type_detail

  实体值：病毒名称。