Cisco セキュリティ管理アプライアンス向け AsyncOS API の概要

Cisco セキュリティ管理アプライアンス向け AsyncOS API（または AsyncOS API）は Representational State Transfer（REST）ベースの一連の操作で、セキュリティ管理アプライアンス レポート、レポート カウンタ、トラッキング、隔離、設定へのセキュアで認証済みのアクセスを提供します。API を使用すると、セキュリティ管理アプライアンスのレポート、トラッキング、隔離に関するデータ（E メール セキュリティ アプライアンス用）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。

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

AsyncOS API を使用するには、以下が必要です。

- AsyncOS 12.0 を使用するセキュリティ管理アプライアンス。
- 知識：
  - 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 （5 ページ）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 （2 ページ） を参照してください。

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 （新しい Web インターフェイスのみ）歯車アイコン をクリックしてレガシー Web インターフェイスをロードします。

ステップ 3 [管理アプライアンス（Management Appliance）] > [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 4 管理インターフェイスを編集します。

（注） 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。

ステップ 5 [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。

（注） AsyncOS API は HTTP / 1.1 を使用して通信します。

HTTPS を選択して、セキュア通信用に独自の証明書を使用する場合は、AsyncOS API との安全な通信 （3 ページ）を参照してください。

（注） 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 6 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。

（注） 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 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 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 ロール、ユーザにアクセス可能な API をクエリする方法について説明します。

認証

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、セキュリティ管理アプライアンスのユーザ名とパスワードを送信します。アプライアンスのユーザ非アクティブ 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。次の 2 つのいずれかの方法を使用すると、API へのクエリを認証できます。

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） アプライアンスのユーザ非アクティブ タイムアウトの設定は、JWT の有効期間に適用されます。Web セキュリティアプライアンスは、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 /wsa/api/v2.0/login`
	二要素認証には、次の構文を使用します。
	`POST /wsa/api/v2.0/login/two_factor`	

本文パラメータ	Base64 エンコード クレデンシャルを使用します。 `{ "data": { "userName":"YWRtaW4=", "passphrase":"aXJvbnBvcnQ=" } }`	
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 クレデンシャルでログインし、JWT を生成するクエリを示します。

サンプル リクエスト

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

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 26 Nov 2018 07:22:47 GMT
Content-type: application/json
```

```
Content-Length: 618
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": {
        "userName": "admin",
        "is2FactorRedirectRequired": "false",
        "role": "Administrator",
        "email": [],
       "jwtToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwiaXM

        yRmFjdG9yQ2hlY2tSZXF1aXJlZCI6ZmFsc2UsImNvb2tpZSI6IlRucEZOVTFFWTNwTlZFMDlDanRMYVR

        oeENqdFpiV1J6VFVSQk5VMURNWGRpTWxGMVdUSnNlbGt5T0hWWk1qbDBUMnBaZDA5RVFUMEtcbk8xVkh

        PWHBrUnpGb1lteEtNV0p1VW5CaVYxVjJUbmswTUV4cVFUMEtPMVJVUlhkTlJsazNUVlJKZFUxRE5IZE1

        WRWw1VFdwek1FMXFcblNUVlNhazVDVDBWRk1rOUVaM2xTUlVreVRYcGtSazFwTVVSTlZFMHpUbFZXUjA1

    }
}
```

認可

AsyncOS API はロール ベースのシステムで、API クエリの範囲はユーザのロールごとに定義されています。次のロールを使用する Cisco コンテンツ セキュリティ管理アプライアンスのユーザは、AsyncOS API にアクセスすることができます。

- 管理者
- オペレータ
- 専門技術者
- 読み取り専用オペレータ
- ゲスト
- Web Administrator
- Web Policy Administrator
- URL フィルタリング管理者
- メール管理者
- ヘルプ デスク ユーザ

（注）
- 外部認証ユーザは API にアクセスできます。
- また、管理者から委任されたカスタム ロールも API にアクセスできます。

AsyncOS API の要求と応答

（注） API の完全なリストについては、『*AsyncOS API - Addendum to the Getting Started Guide for Cisco Content Security Management Appliances*』を参照してください。

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}/sma/api/v2.0/{resource}/{resource_attributes}
```

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

引数の説明

  - `{appliance}:{port}`

    FQDN またはアプライアンスの IP アドレスと、アプライアンスが待機する 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 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>/sma/api/v2.0/{resource}/{resource_attributes}
```

（注） 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

コンポーネント		値	説明
ステータス コードと理由		HTTP 応答コード （8 ページ）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	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。
		1. URI。API への要求で指定した URI。
		例
		`:"/api/v2.0/config/"`
		2. カウンタ グループやカウンタ名
		例
		`reporting/mail_security_summary`
		3. クエリ パラメータ
		例
		`startDate=2017-01-30T00:00:00.000Z&endDate=2018-01-30T14:00:00.000Z`
		4. 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."}`
		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。

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

API データと Web インターフェイスデータの比較

新しい Web インターフェイスは、AsyncOS API を使用して、GMT タイムゾーンで指定された期間属性を持つデータを取得します。API クエリのデータを新しい Web インターフェイスデータと比較する場合は、API クエリに新しい Web インターフェイス API クエリと同じ時間範囲（ISO8601 時間形式）が設定されていることを確認します。

関連資料

このドキュメントで説明するトピックに加えて、次のドキュメントで API の詳細を確認できます。

表 *1*：関連資料

ドキュメント	場所：
Addendum to the Getting Started Guide for Cisco Security Management Appliances。	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-programming-reference-guides-list.html
API ヘルプ（Swagger UI）	新しい Web インターフェイスで、ヘルプアイコンにカーソルを合わせ、**[APIヘルプ：Swagger（API Help: Swagger）]** をクリックします。 （注） API ヘルプ（Swagger UI）では、[試行する（Try it out）] ボタンを使用して、Web ブラウザから直接 API コールをテストすることもできます。

関連資料