



AsyncOS 16.0 for Cisco Secure Web Appliance-API スタートアップガイド

最終更新：2026 年 9 月 29 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/）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.

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)

© 2026 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

Cisco Secure Web Appliance 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

Web 用 API 11

レポート API 11

API データと Web インターフェイスデータの比較 13

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 16

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 17

スケジュールおよびアーカイブ API	19
スケジュール API	20
例	23
アーカイブ API	28
例	30
トラッキング API	35
プロキシ サービス	35
レイヤ 4 トラフィック モニター	38
SOCKS プロキシ	39
構成 API	41
全体的な帯域幅	42
全体的な帯域幅の詳細の取得	42
全体的な帯域幅の詳細の変更	43
PAC ファイルホスト設定	44
PAC ファイル基本設定の取得	44
PAC ファイルの基本設定の変更	45
PAC ファイルの取得	46
PAC ファイルのリストの取得	48
新しい PAC ファイルの追加	49
既存の PAC ファイルの変更	49
PAC ファイルの削除	50
PAC ファイルとホスト名の関連付けの取得	51
PAC ファイルとホスト名の関連付けの追加	52
既存の PAC ファイルとホスト名の関連付けの変更	53
PAC ファイルとホスト名の関連付けの削除	54
識別プロファイル (Identification Profiles)	54
識別の詳細の取得	55
識別プロファイルの変更	56
識別プロファイルの追加	57
識別プロファイルの削除	58
アクセス ポリシー	59

アクセスポリシーの取得	60
アクセスポリシーの変更	62
アクセス ポリシーの追加	64
アクセスポリシーの削除	65
使用許可コントロール	67
使用許可コントロール	67
ドメイン マップ	68
ドメインマップの詳細の取得	68
ドメインマップの詳細の変更	69
ドメインマップの追加	71
ドメインマップの削除	72
上位プロキシ	73
上位プロキシの詳細の取得	74
上位プロキシ設定の変更	75
上位プロキシの追加	76
上位プロキシの削除	77
上位プロキシサーバーの変更	78
上位プロキシサーバーの追加	79
上位プロキシサーバーの削除	81
HTTPS プロキシ	82
HTTPS プロキシの詳細の取得	82
HTTP プロキシ設定の変更	84
HTTP プロキシの取得：証明書ファイルのダウンロード	85
HTTP プロキシ OCSP 設定の取得	86
HTTP プロキシの変更：OCSP 設定	88
ログサブスクリプション	89
ログサブスクリプションの取得	89
ログサブスクリプションの変更	96
ログサブスクリプションの追加	98
ログサブスクリプションの削除	99
ログサブスクリプションの変更：ロールオーバー	100

取得フィールドリストのログサブスクリプションの取得	101
ログタイプのデフォルト値を取得するためのログサブスクリプションの取得	103
ログサブスクリプション（非匿名化）の追加	104
ヘッダーベース認証	105
ヘッダーベース認証の詳細の取得	105
ヘッダーベース認証の詳細の変更	107
要求ヘッダー書き換えプロファイル	108
要求ヘッダー書き換えの詳細の取得	109
要求ヘッダー書き換えの詳細の変更	110
要求ヘッダー書き換えプロファイルの追加	111
要求ヘッダー書き換えプロファイルの削除	112
スマート ソフトウェア ライセンス	113
スマート ソフトウェア ライセンスの取得	113
スマート ソフトウェア ライセンスの変更	116
スマート ライセンス エージェントのステータスの取得	118
スマート ライセンス エージェントのステータスの変更	119
スマート ソフトウェア ライセンスのステータスの取得	119
スマート ソフトウェア ライセンスのステータスの変更	120
システム セットアップ ウィザード	121
エンドユーザーライセンス契約の詳細の取得	121
システム セットアップ ウィザードの設定の変更	123
復号ポリシー	125
復号ポリシーの取得	125
復号ポリシーの変更	128
復号ポリシーの追加	129
復号ポリシーの削除	132
ルーティングポリシー	133
ルーティングポリシーの取得	133
ルーティングポリシーの変更	134
ルーティングポリシーの追加	135
ルーティングポリシーの削除	136

IP スプーフィングプロファイル	137
IP スプーフィングプロファイルの取得	137
IP スプーフィングプロファイルの変更	138
IP スプーフィングプロファイルの追加	138
IP スプーフィングプロファイルの削除	139
設定ファイル	140
構成ファイルの取得	140
構成ファイルの変更	141
アプライアンス構成ファイルの表示	142
構成ファイルの取得—バックアップ設定	143
構成ファイルの変更—バックアップ設定	143
構成ファイルの変更—リセット	145
認証レلم	146
認証レلم設定の取得	146
認証レلم設定の追加	147
認証レلمシーケンス設定の取得	148
認証レلمシーケンス設定の変更	149
認証レلمシーケンス設定の追加	149
グローバル認証設定の取得	150
グローバル認証設定の変更	151
Umbrella シームレス ID	152
Cisco Umbrella シームレス ID の取得	152
Cisco Umbrella シームレス ID の変更	153
Umbrella シームレス ID の起動テストの実行	154
セキュア DNSSec 設定	155
セキュア DNS 設定の取得	155
セキュア DNS 設定の変更	155
Identity Service Engine	156
Identity Service Engine の設定の取得	157
Identity Service Engine の設定の変更	158
Identity Service Engine の証明書の詳細のアップロード	159

Identity Service Engine の証明書の詳細のダウンロード	159
Identity Service Engine の起動テストの実行	160
マルウェア対策レピュテーション	162
マルウェア対策レピュテーションの詳細の取得	162
マルウェア対策レピュテーションの詳細の変更	169
マルウェア対策分析コンソールの登録	176
マルウェア対策分析コンソールの登録の削除	177
ユーザ通知 (End-User Notification)	178
エンドユーザー通知の詳細の取得	178
エンドユーザー通知の詳細の変更	179

第 3 章

汎用 API 181

SMTP リレーホストの詳細の取得	182
新しい SMTP リレーホストの追加	182
SMTP リレーホストの詳細の変更	183
複数の SMTP リレーホストの削除	184
すべての SMTP リレーホストの削除	185
ユーザー ロールにアクセス可能な API の取得	186
SecureX ファイルの取得	187
SecureX ファイル設定の変更	188
SecureX のユーザー情報詳細の追加	189
認証設定の取得	190
ユーザーエージェントの取得	192
URL カテゴリの取得	193
時間範囲の取得	195
クォータの取得	197
プロキシ設定の取得	198
識別方法の取得	199
ADC の詳細の取得	200
正常性チェック API	203
外部 DLP サーバーの正常性チェック	203

ネットワーク インターフェイスとゲートウェイの正常性チェック 204

NTP サービスの正常性チェック 206

DNS 探索の正常性チェック 207

システム ヘルスのチェック 209

第 4 章

AsyncOS API のトラブルシューティング 213

API ログ 213

アラート 213



第 1 章

Cisco Secure Web Appliance 向け AsyncOS API の概要

Cisco Secure Web Appliance 向け AsyncOS API（または AsyncOS API）は Representational State Transfer（REST）ベースの一連の操作で、Secure Web Appliance 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。この API を使用して、Secure Web Appliance 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。



(注) シスコのコンテンツセキュリティ管理アプライアンスと REST API を使用して、Cisco Secure Web Appliance を設定できます。両方の方法を使用して Cisco Secure Web Appliance を設定すると、以前の方法で行った設定が上書きされます。

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 Token（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。

AsyncOS API の有効化

はじめる前に

CLI で `interfaceconfig` コマンドにアクセスできることを確認します。CLI へのアクセスが許可されるのは管理者、電子メール管理者、クラウド管理者、およびオペレータのみです。

CLI で `interfaceconfig` コマンドを使用すると、AsyncOS API を有効にできます。

Procedure

ステップ 1 CLI にログインして `interfaceconfig` コマンドを実行します。

ステップ 2 編集するインターフェイスを選択します。

ステップ 3 AsyncOS API (モニタリング) HTTP を有効にするための次の質問に回答します。

- Do you want to enable AsyncOS API (monitoring) HTTP on this interface? [Y]> Y を入力します。
- Which port do you want to use for AsyncOS API (monitoring) HTTP? [6080]> デフォルトのポート 6080 か定義するポートを入力します。

ステップ 4 AsyncOS API (モニタリング) HTTPS を有効にするための次の質問に回答します。

- Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [Y]> Y を入力します。
- Which port do you want to use for AsyncOS API (Monitoring) HTTPS? [6443]> デフォルトのポート 6443 か定義するポートを入力します。

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を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。

Procedure

- 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](#)

認証

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。

- Base64 エンコード形式で、API へのすべての要求と一緒に、Secure Web Appliance のユーザー名とパスワードを送信します。
- ヘッダーにトークンキーを含む API 要求で JSON Web トークン (JWT) を使用します。

アプライアンス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。

JSON Web トークンを使用した API クエリの認証

JWT を生成し、API クエリで 사용할 수 있습니다.



- (注) 애플리케이션의 사용자 비활성화 시간 설정은, JWT의 유효기간에 적용됩니다. Secure Web Appliance는, 그 유효기간의 JWT을 포함하는 모든 API 쿼리를 검사합니다. JWT의 유효기간이 5분 이내인 경우, 시간 초과가 되면, 새로운 갱신 JWT이 응답 헤더와 함께 전송됩니다. API 쿼리에서 이 새로운 갱신 JWT을 사용하거나, 새로운 JWT을 생성할 필요가 있습니다.

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。 <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.eyJ1c2VybmFtZSI6ImFkbWluIiwiaXNzIjoiZmFjdG9yQ2hlY2tSZXF1aXJlZCI6ZmFsc2UsImNvb2tpZSI6ImlRucEZOVFFFTWt1ZmFMDlDanRMYVRyRmFjdG9yQ2hlY2tSZXF1aXJlZCI6ZmFsc2UsImNvb2tpZSI6ImlRucEZOVFFFTWt1ZmFMDlDanRMYVRoeENqdFpiV1J6VFVSQk5VMURNWGRpTWxGMVdUSnNlbGt5T0hWWk1qbDBUMnBazDA5RVFUMetcbk8xVkhPWHBrUnpGb1lteEtNV0p1VW5CaVYxVjJUbmswTUV4cVFUMetPMVJVUlhkTlJsazNUV1JKZFUXRE5IZE1WRWw1VfDweklFMXFcblNUV1NhazVDVDBWRk1rOUVaM2xTU1VreVRYcGtSazFwTVVSTlZFMHpbUbFZXUjA1"
  }
}
```

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ー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 Secure Web Appliance のユーザーは、AsyncOS APIにアクセスできます。

- ・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 管理者
- ・Web ポリシー管理者
- ・URL フィルタリング管理者
- ・メール管理者
- ・ヘルプ デスク ユーザー

**Note**

- 外部認証ユーザーは 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。
- 管理者権限を持つユーザーのみが、REST API を使用して設定を変更できます。オペレータや読み取り専用オペレータなどの他のすべてのユーザーは、これらの設定の表示のみが許可されます。

AsyncOS API の要求と応答

**Note**

API の完全なリストについては、『[AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance](#)』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}/wsa/api/v2.0/{resource}/{resource_attributes}
```

```
https://{appliance}:{port}/wsa/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。
- ヘッダーにトークンキーを含む API 要求で以前生成された JSON Web トークン (JWT) を使用します。詳細については、「[JSON Web トークンを使用した API クエリの認証](#)」を参照してください。

- 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>/wsa/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		HTTP 応答コード, on page 8 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。 - URI。API への要求で指定した URI。 例 <code>"/api/v2.0/config/"</code> - カウンタ グループやカウンタ名 例 <code>reporting/mail_security_summary</code> - クエリ パラメータ 例 <code>startDate=2017-01-30T00:00:00.000Z&endDate=2018-01-30T14:00:00.000Z</code> - 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 <pre>"error": { "message": "Unexpected attribute - starts with.", "code": "404", "explanation": "404 = Nothing matches the given URI." }</pre> 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。 Note totalCount は、データセットで返されるデータオブジェクトの数です（UI にテーブル形式で表示される結果の場合）。他のクエリでは、デフォルトで -1 が返されます。

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 応答コードの説明については、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。

- [Web 用 API, on page 11](#)
- [汎用 API, on page 181](#)



第 2 章

Web 用 API

- [レポート API](#) (11 ページ)
- [スケジュールおよびアーカイブ API](#) (19 ページ)
- [トラッキング API](#) (35 ページ)
- [構成 API](#) (41 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レポートまたは特定のレポートにおいてレポート グループ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	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。 <code>startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z</code> 指定した期間の集約レポート。
	クエリのタイプ	• <code>query_type=graph</code> グラフとして表現できるデータを受信します。 • <code>query_type=export</code> エクスポート形式のデータを受信します。
	ソート	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。 • <code>orderBy=<value></code> 応答内のデータを並べ替える属性を指定します。次の例を参考にしてください。 <code>orderBy=total_clean_recipients</code> • <code>orderDir=<value></code> ソート方向を指定します。 有効なオプションは次のとおりです。 • <code>asc</code> 昇順で結果を並べ替えます。 • <code>desc</code> 降順で結果を並べ替えます。
	遅延読み込み	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。 • <code>offset=<value></code> オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。 • <code>limit=<value></code> 取得するレコードの数を指定します。
	データの取得オプション	• <code>top=<value></code> 最大値を返すレコードの数を指定します。

	フィルタリング	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。 • <code>filterValue=<value></code> 検索対象の値。 • <code>filterBy=<value></code> 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。 • <code>filterOperator=<value></code> 有効なオプションは次のとおりです。 • <code>begins_with</code> 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。 • <code>is</code> 指定した完全一致の値に基づいて応答データをフィルタリングします。
	デバイス	• <code>device_type=wsa</code> 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。 • <code>device_name=<value></code> デバイス名を指定します。
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

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。

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 \(16 ページ\)](#)
- [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 \(17 ページ\)](#)

カウンタの1つの値を取得する

次の例では、カウンタの1つの値を取得するクエリを示します。

サンプル リクエスト

```
GET /wsa/api/v2.0/reporting/web_malware_category_malware_name_user_detail/
blocked_malware?startDate=2017-11-14T02:00+00:00&endDate=2018-02-18T01:00+00:00&
filterValue=23&filterBy=na&filterOperator=is&device_type=wsa
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: wsa.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, 26 Nov 2018 16:29:33 GMT
Content-type: application/json
Content-Length: 193
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": 4
  },
  "data": {
    "type": "blocked_malware",
    "resultSet": {
      "blocked_malware": [
        {
          "10.8.93.12": 137511
        },
        {
          "10.8.93.20": 112554
        },
        {
          "10.8.93.11": 92839
        },
        {
          "10.225.98.234": 6
        }
      ]
    }
  }
}
```

```
    ]
  }
}
```

カウンタの複数の値を取得する

次に、順序の方向およびデバイスタイプのパラメータを指定して、カウンタの複数の値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 /wsa/api/v2.0/reporting/web_services_summary?orderBy=transaction_total&
orderDir=desc&startDate=2018-08-16T18:00:00.000Z&endDate=2018-11-15T10:00:00.000Z&device_type=wsa
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.8.159.21:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sun, 18 Nov 2018 15:38:52 GMT
Content-type: application/json
Content-Length: 403
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": "web_services_summary",
    "resultSet": [
      {"detected_by_traffic_monitor": 0},
      {"detected_malware_total": 42},
      {"high_risk_transaction_total": 7109},
      {"blocked_by_admin_policy": 0},
      {"detected_by_amp": 0},
      {"allowed_transaction_total": 26369},
      {"transaction_total": 33478},
      {"blocked_or_warned_by_webcat": 29},
      {"blocked_by_wbrs": 7038},
      {"blocked_by_avc": 0}
    ]
  }
}
```

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。次に、フィルタ、デバイスタイプ、および上位の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の例を示します。

サンプル リクエスト

```
GET /wsa/api/v2.0/reporting/web_application_type_detail/bw_not_limited?startDate=
2017-09-10T19:00:00.000Z&endDate=2018-09-24T23:00:00.000Z&device_type=wsa&filterValue=
F&filterOperator=begins_with&filterBy=na&top=2
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.8.159.21:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sun, 18 Nov 2018 15:48:21 GMT
Content-type: application/json
Content-Length: 138
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": 2
  },
  "data": {
    "type": "bw_not_limited",
    "resultSet": {
      "bw_not_limited": [
        {"File Sharing": 84},
        {"Facebook": 42}
      ]
    }
  }
}
```

複数のカウンタの複数の値を取得する

次に、オフセット、制限、およびデバイスタイプのパラメータなど、複数のカウンタの複数の値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 /wsa/api/v2.0/reporting/web_services_summary?offset=0&limit=20&
startDate=2020-04-10T07:00:00.000Z&endDate=2020-04-11T08:00:00.000Z&device_type=wsa&
HTTP/1.1
cache-control: no-cache
Postman-Token: 692fd2a6-3da7-4bc1-b581-f4b478b5a304
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
```

```
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Sat, 11 Apr 2020 07:42:04 GMT
Content-type: application/json
Content-Length: 387
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"meta": {"totalCount": -1}, "data": {"type": "web_services_summary", "resultSet":
[{"detected_by_traffic_monitor": 0}, {"detected_malware_total": 0},
{"high_risk_transaction_total": 0},
{"blocked_by_admin_policy": 0}, {"detected_by_amp": 0}, {"allowed_transaction_total":
0},
{"transaction_total": 0}, {"blocked_or_warned_by_webcat": 0}, {"blocked_by_wbrs": 0},
{"blocked_by_avc": 0}]}}
```

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

次に、オフセットと制限のパラメータ、およびクエリタイプの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の例を示します。

サンプル リクエスト

```
GET /wsa/api/v2.0/reporting/web_application_name_application_type_detail?startDate
=2017-08-16T18:00:00.000Z&endDate=2018-11-15T15:00:00.000Z&device_type=wsa&query_type=export
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.8.159.21:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Sun, 18 Nov 2018 15:55:50 GMT
Content-type: application/json
Content-Length: 1258
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": "web_application_name_application_type_detail",
```

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

```
"resultSet": {
  "time_intervals": [
    {
      "end_timestamp": 1538332199,
      "counter_values": [
        {
          "counter_values": [
            42,
            25932,
            0,
            42,
            0,
            42,
            0
          ],
          "application_type": "File Sharing",
          "counter_key": "4shared"
        },
        {
          "counter_values": [
            2,
            109614,
            0,
            2,
            0,
            2,
            0
          ],
          "application_type": "Media",
          "counter_key": "Dailymotion"
        },
        {
          "counter_values": [
            42,
            20748,
            0,
            42,
            0,
            42,
            0
          ],
          "application_type": "Facebook",
          "counter_key": "Facebook General"
        },
        {
          "counter_values": [
            42,
            20580,
            0,
            42,
            0,
            42,
            0
          ],
          "application_type": "File Sharing",
          "counter_key": "MediaFire"
        },
        {
          "counter_values": [
            229,
            158838,
            0,
            229,
            0,
            0,
            0
          ],
          "application_type": "File Sharing",
          "counter_key": "MediaFire"
        }
      ]
    }
  ]
}
```

```

        229,
        0
    ],
    "application_type": "Social Networking",
    "counter_key": "Twitter"
},
{
    "counter_values": [
        1,
        86334,
        0,
        1,
        0,
        1,
        0
    ],
    "application_type": "Instant Messaging",
    "counter_key": "Wechat_web"
},
{
    "counter_values": [
        44,
        40876,
        0,
        44,
        0,
        44,
        0
    ],
    "application_type": "Media",
    "counter_key": "YouTube"
}
],
"begin_timestamp": 1530383400,
"end_time": "2018-09-30T23:59:00.000Z",
"begin_time": "2018-07-01T00:00:00.000Z"
}
],
"counter_names": [
    "bw_not_limited",
    "bandwidth_used",
    "bw_limited",
    "completed_transaction_total",
    "blocked_transaction_total",
    "transaction_total",
    "blocked_by_avc"
]
}
}
}

```

スケジュールおよびアーカイブ API

- [スケジュール API \(20 ページ\)](#)
- [アーカイブ API \(28 ページ\)](#)

スケジュール API

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

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

次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。

- orderBy=<value>

有効なオプションは次のとおりです。

- periodic_report_display_name

レポートの表示名に基づいて結果を並べ替えます。

- periodic_report_title

レポートのタイプに基づいて結果を並べ替えます。

- periodic_report_type

レポートのタイプに基づいて結果を並べ替えます。

- periodic_report_time_range

レポートの時間範囲に基づいて結果を並べ替えます。

- periodic_report_delivery

レポートの配信オプションに基づいて結果を並べ替えます。

- periodic_report_format

レポートの形式に基づいて結果を並べ替えます。

- periodic_report_schedule_type

レポートに選択したスケジュールのタイプに基づいて結果を並べ替えます。

- periodic_report_tier

必要な Web ゲートウェイに基づいて結果を並べ替えます。

- periodic_report_next_run_date

レポートのスケジュールオプションに基づいて結果を並べ替えます。

- orderDir=<value>

ソート方向を指定します。

有効なオプションは次のとおりです。

- asc

		昇順で結果を並べ替えます。 • desc 降順で結果を並べ替えます。
	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。 • offset=<value> オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。 • limit=<value> 取得するレコードの数を指定します。
	デバイス	• device_type=wsa 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。
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

次に、スケジュールレポートクエリのタイプの例をいくつか示します。

- [スケジュールレポートの取得 \(23 ページ\)](#)
- [スケジュール レポート エントリの詳細の取得 \(25 ページ\)](#)
- [スケジュール レポート エントリの追加 \(26 ページ\)](#)
- [スケジュール レポート エントリの編集 \(27 ページ\)](#)
- [スケジュール設定されたレポートの削除 \(27 ページ\)](#)

スケジュールレポートの取得

次に、使用可能なすべてのスケジュールレポートエントリのリストを取得する例を示します。

サンプル リクエスト

```
GET /wsa/api/v2.0/config/periodic_reports?device_type=wsa HTTP/1.1
cache-control: no-cache
Postman-Token: 2a8a85d4-50cc-49fd-9ac5-20e07775e1db
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
```

```
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 10:41:02 GMT
Content-type: application/json
Content-Length: 3691
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"data": {"periodic_reports": [{"20200409064843_Web Sites Report_calendar_week":
{"periodic_report_type": "coeus", "periodic_report_schedule": {"periodic_report_second":
0,
"periodic_report_day": "", "periodic_report_month": "", "periodic_report_minute": 0,
"periodic_report_weekday": "", "periodic_report_year": "", "periodic_report_hour": 1,
"periodic_report_schedule_type": "Daily"}, "periodic_report_options":
{"periodic_report_rows": 20,
"periodic_report_charts": {"wsa_web_sites_top_blocked_domains":
"DOMAINS.BLOCKED_TRANSACTION_TOTAL",
"wsa_web_sites_top_domains": "DOMAINS.TRANSACTION_TOTAL"}, "periodic_report_format":
"PDF",
"periodic_report_lang": "en-us", "periodic_report_sort_columns":
{"wsa_web_sites_domains_matched":
"DOMAINS.TRANSACTION_TOTAL"}, "periodic_report_time_range": "Previous calendar month"},

"periodic_report_user_name": "admin", "periodic_report_product_type": "WSA",
"periodic_report_type_name": "Web Sites", "periodic_report_delivery": "Archived Only",
"periodic_report_recipients": [], "periodic_report_tier": "All Web Appliances",
"periodic_report_next_run_date": "11 Apr 2020 01:00 (GMT)", "periodic_report_title":
"Web Sites Report_2 Edit"}},
{"20200402042756_Users_calendar_week": {"periodic_report_type": "coeus",
"periodic_report_schedule":
{"periodic_report_second": 0, "periodic_report_day": "", "periodic_report_month": "",
"periodic_report_minute": 0,
"periodic_report_weekday": "", "periodic_report_year": "", "periodic_report_hour": 1,
"periodic_report_schedule_type": "Daily"}, "periodic_report_options":
{"periodic_report_rows": 10,
"periodic_report_charts": {"wsa_users_top_users_bandwidth_used":
"WEB_USER_DETAIL.BANDWIDTH_USED",
"wsa_users_top_users_blocked_transactions": "WEB_USER_DETAIL.BLOCKED_TRANSACTION_TOTAL"},

"periodic_report_format": "PDF", "periodic_report_lang": "en-us",
"periodic_report_sort_columns":
{"wsa_users_users_table": "WEB_USER_DETAIL.BLOCKED_TRANSACTION_TOTAL"},
"periodic_report_time_range":
"Previous 7 calendar days"}, "periodic_report_user_name": "admin",
"periodic_report_product_type": "WSA",
"periodic_report_type_name": "Users", "periodic_report_delivery": "Emailed Only",
"periodic_report_recipients": ["abc@cic.com"], "periodic_report_tier": "All Web
Appliances",
"periodic_report_next_run_date": "11 Apr 2020 01:00 (GMT)", "periodic_report_title":
"Users"}},
{"20200403094854_Application Visibility_calendar_month": {"periodic_report_type": "coeus",

"periodic_report_schedule": {"periodic_report_second": 0, "periodic_report_day": "",
"periodic_report_month": "", "periodic_report_minute": 0, "periodic_report_weekday": ""},
```

```

"periodic_report_year": "", "periodic_report_hour": 1, "periodic_report_schedule_type":
"Daily"},
"periodic_report_options": {"periodic_report_rows": 10, "periodic_report_charts":
{"wsa_applications_blocked":
"WEB_APPLICATION_NAME_APPLICATION_TYPE_DETAIL.BLOCKED_BY_AVC",
"wsa_applications_top_types":
"WEB_APPLICATION_TYPE_DETAIL.TRANSACTION_TOTAL"}, "periodic_report_format": "PDF",
"periodic_report_lang": "en-us", "periodic_report_sort_columns": {"wsa_applications_total":
"WEB_APPLICATION_NAME_APPLICATION_TYPE_DETAIL.TRANSACTION_TOTAL",
"wsa_applications_types_total":
"WEB_APPLICATION_TYPE_DETAIL.BANDWIDTH_USED"}, "periodic_report_time_range": "Previous
calendar month"},
"periodic_report_user_name": "admin", "periodic_report_product_type": "WSA",
"periodic_report_type_name": "Application Visibility", "periodic_report_delivery":
"Archived Only",
"periodic_report_recipients": [], "periodic_report_tier": "All Web Appliances",
"periodic_report_next_run_date": "11 Apr 2020 01:00 (GMT)", "periodic_report_title":
"Application Visibility"}},
"meta": {"totalCount": 3}}

```

スケジュール レポート エントリの詳細の取得

次の例では、レポート ID を渡すことによって、特定のスケジュールされたレポートの詳細を取得する方法を示します。

サンプル リクエスト

```

GET /wsa/api/v2.0/config/periodic_reports/20200402042756_Users_calendar_week?
device_type=wsa& HTTP/1.1
cache-control: no-cache
Postman-Token: b7038e94-4182-4b35-9aae-73a1a1e35249
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive

```

サンプル 応答

```

HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 10:43:07 GMT
Content-type: application/json
Content-Length: 1130
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"data": {"periodic_reports": {"20200402042756_Users_calendar_week":
{"periodic_report_type":
"coeus", "periodic_report_schedule": {"periodic_report_second": 0, "periodic_report_day":
"",
"periodic_report_month": "", "periodic_report_minute": 0, "periodic_report_weekday": "",
"periodic_report_year": "", "periodic_report_hour": 1, "periodic_report_schedule_type":
"Daily"},
"periodic_report_options": {"periodic_report_rows": 10, "periodic_report_charts":
[{"column":
"Bandwidth Used", "Chart": "Top Users (Right)"}, {"column": "Transactions Blocked",

```

```

"Chart":
"Top Users (Left)"]], "periodic_report_format": "PDF", "periodic_report_lang": "en-us",

"periodic_report_sort_columns": [{"column": "Transactions Blocked", "table": "Users"}],

"periodic_report_time_range": "Previous 7 calendar days", "periodic_report_user_name":
"admin",
"periodic_report_product_type": "WSA", "periodic_report_type_name": "Users",
"periodic_report_delivery": "Emailed Only", "periodic_report_recipients": ["abc@cic.com"],

"periodic_report_tier": "All Web Appliances", "periodic_report_next_run_date": 1586566800,

"periodic_report_title": "Users"}}}}

```

スケジュール レポート エントリの追加

次の例では、レポートタイプ、レポートタイトル、デバイスタイプ、およびその他のオプションを指定してスケジュールレポートを追加する方法を示します。

サンプル リクエスト

```

POST /wsa/api/v2.0/config/periodic_reports?device_type=wsa& HTTP/1.1
cache-control: no-cache
Postman-Token: 32ald150-a8a0-47f2-b9bf-2c7c5b2e8e8a
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 833
Connection: keep-alive

{"data":{"periodic_reports":[{"periodic_report_delivery":"Emailed and Archived",
"periodic_report_options":{"periodic_report_format":"pdf","periodic_report_lang":"en-us",
"periodic_report_rows":10,"periodic_report_sort_columns":[{"table":"Domains
Matched","column":
"Total Transactions"}],"periodic_report_charts":[{"Chart":"Top Domains (Left)","Data to
display":
"Total Transactions"},{"Chart":"Top Domains (Right)","Data to display":"Transactions
Blocked"}]},
"periodic_report_time_range":"Previous 7 calendar days","periodic_report_title":"Web
Sites Report",
"periodic_report_type":"coeus","periodic_report_type_name":"Web Sites",
"periodic_report_user_name":"admin","periodic_report_schedule":{"periodic_report_hour":1,
"periodic_report_minute":0,"periodic_report_schedule_type":"daily"},
"periodic_report_recipients":["abc@test.com"]}]}}

```

サンプル応答

```

HTTP/1.1 201 Created
Date: Thu, 09 Apr 2020 06:50:18 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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

```

スケジュール レポート エントリの編集

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

サンプル リクエスト

```
PUT
/wsa/api/v2.0/config/periodic_reports/20200409064843_Web%20Sites%20Report_calendar_week?
device_type=wsa& HTTP/1.1
cache-control: no-cache
Postman-Token: 2d168727-6e8a-470a-909f-0af9a5dc1e85
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 786
Connection: keep-alive

{"data":{"periodic_reports":[{"periodic_report_delivery":"Archived Only",
"periodic_report_options":{"periodic_report_format":"pdf","periodic_report_lang":"en-us",
"periodic_report_rows":20,"periodic_report_sort_columns":[{"table":"Domains
Matched","column":
"Total Transactions"}]},"periodic_report_charts":[{"Chart":"Top Domains (Left)","Data to
display":
"Total Transactions"}],{"Chart":"Top Domains (Right)","Data to display":"Transactions
Blocked"}]},
"periodic_report_time_range":"Previous calendar month"},"periodic_report_title":
"Web Sites Report_1 Edit","periodic_report_type":"coeus","periodic_report_type_name":
"Web Sites","periodic_report_user_name":"admin","periodic_report_schedule":
{"periodic_report_hour":1,"periodic_report_minute":0,"periodic_report_schedule_type":"daily"}}]}
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Thu, 09 Apr 2020 06:54:19 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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

スケジュール設定されたレポートの削除

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

サンプル リクエスト

```
DELETE /wsa/api/v2.0/config/periodic_reports?id=20200409065018_Web%20Sites
%20Report_calendar_week&device_type=wsa HTTP/1.1
cache-control: no-cache
Postman-Token: 7e09e87c-40c2-410a-a99e-98f73c6e0bf8
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
Accept: */*
```

```
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 0
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Thu, 09 Apr 2020 07:07:05 GMT
Content-type: application/json
Content-Length: 52
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{"data": {"message": "1 item deleted successfully"}}
```

アーカイブ API

概要	GET /wsa/api/v2.0/config/archived_reports?resource_attribute GET wsa/api/v2.0/config/archived_reports/view/archived_report_id?resource_attribute POST /wsa/api/v2.0/config/archived_reports?resource_attribute DELETE /wsa/api/v2.0/config/archived_reports?id=archived_report_id (単一レポートを削除する場合) DELETE /wsa/api/v2.0/config/archived_reports?id=all (すべてのアーカイブレポートを削除する場合)
----	---

サポート対象のリソース属性	ソート	次の両方のパラメータを使用する必要があります。いずれかを使用した場合は、応答でデータを受信できません。 • orderBy=<value> 有効なオプションは次のとおりです。 • periodic_report_generated レポートが生成された日時に基づいて結果を並べ替えます。 • periodic_report_display_name レポートの表示名に基づいて結果を並べ替えます。 • periodic_report_format レポートの形式に基づいて結果を並べ替えます。 • periodic_report_title レポートのタイプに基づいて結果を並べ替えます。 • periodic_report_time_range レポートの時間範囲に基づいて結果を並べ替えます。 • periodic_report_type レポートのタイプに基づいて結果を並べ替えます。 • periodic_report_tier 必要な電子メールゲートウェイに基づいて結果を並べ替えます。 • orderDir=<value> ソート方向を指定します。 有効なオプションは次のとおりです。 • asc 昇順で結果を並べ替えます。 • desc 降順で結果を並べ替えます。
---------------	-----	--

	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。 • <code>offset=<value></code> オフセット値から始まるレコードのサブセットを取得するオフセット値を指定します。オフセットは制限と共に使用し、オフセットから取得するレコードの数を決定します。 • <code>limit=<value></code> 取得するレコードの数を指定します。
	フィルタリング	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。 • <code>filterByTitle=<value></code> レポートのタイトルと値でデータをフィルタリングします。 • <code>filterByReportTypeName=<value></code> レポートのタイプと値でデータをフィルタリングします。 • <code>filterByTimeRange=<value></code> レポートの時間範囲と値でデータをフィルタリングします。
	デバイス	• <code>device_type=wsa</code> 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。
要求ヘッダー		Host、Accept、Authorization
応答ヘッダー		Content-Type、Content-Length、Connection

例

アーカイブレポートクエリのタイプの例を次に示します。

- [アーカイブレポートの検索 \(31 ページ\)](#)
- [アーカイブレポートの取得 \(31 ページ\)](#)
- [アーカイブレポートエントリの詳細の取得 \(33 ページ\)](#)
- [アーカイブレポートエントリの追加 \(33 ページ\)](#)

- [アーカイブレポートエントリの削除 \(34 ページ\)](#)

アーカイブレポートの検索

次に、レポートタイトルに基づいて、レポートが生成された日時に昇順にソートされた上位20のアーカイブレポートのリストを検索する例を示します。

サンプル リクエスト

```
GET /wsa/api/v2.0/config/archived_reports?orderBy=periodic_report_title&
device_type=wsa&filterByTitle=Application&orderDir=asc&offset=0&limit=20 HTTP/1.1
cache-control: no-cache
Postman-Token: elf6fac5-f047-4ab5-9be2-467132a3b29d
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Thu, 09 Apr 2020 07:27:25 GMT
Content-type: application/json
Content-Length: 1262
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"data": {"meta": {"totalCount": 3}, "archived_reports": [{"20200404010011_Application
Visibility_calendar_month.pdf": {"periodic_report_format": "PDF",
"periodic_report_type_name": "Application Visibility", "periodic_report_generated":
"04 Apr 2020 01:00 (GMT)", "periodic_report_time_range": "Previous calendar month",
"periodic_report_tier": "All Web Appliances", "periodic_report_title": "Application
Visibility",
"periodic_report_product_type": "wsa"}}, {"20200409010011_Application
Visibility_calendar_month.pdf":
{"periodic_report_format": "PDF", "periodic_report_type_name": "Application Visibility",
"periodic_report_generated": "09 Apr 2020 01:00 (GMT)", "periodic_report_time_range":
"Previous calendar month", "periodic_report_tier": "All Web Appliances",
"periodic_report_title":
"Application Visibility", "periodic_report_product_type": "wsa"}},
{"20200408010011_Application
Visibility_calendar_month.pdf": {"periodic_report_format": "PDF",
"periodic_report_type_name":
"Application Visibility", "periodic_report_generated": "08 Apr 2020 01:00 (GMT)",
"periodic_report_time_range": "Previous calendar month", "periodic_report_tier":
"All Web Appliances", "periodic_report_title": "Application Visibility",
"periodic_report_product_type": "wsa"}}]}}
```

アーカイブレポートの取得

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

サンプル リクエスト

```
GET /wsa/api/v2.0/config/archived_reports?device_type=wsa&limit=25&
offset=0&orderBy=periodic_report_generated&orderDir=desc HTTP/1.1
cache-control: no-cache
Postman-Token: 9cf1ebad-774d-4e86-af29-fd6d25c446ce
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 10:48:31 GMT
Content-type: application/json
Content-Length: 2792
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"data": {"meta": {"totalCount": 7}, "archived_reports": [{"20200410010016_Application
Visibility_
calendar_month.pdf": {"periodic_report_format": "PDF", "periodic_report_type_name":
"Application Visibility", "periodic_report_generated": "10 Apr 2020 01:00 (GMT)",
"periodic_report_time_range": "Previous calendar month", "periodic_report_tier": "All
Web Appliances",
"periodic_report_title": "Application Visibility", "periodic_report_product_type":
"wsa"}}, {"20200410010009_Web Sites Report_2 Edit_calendar_month.pdf": {"periodic_report_format":
"PDF",
"periodic_report_type_name": "Web Sites", "periodic_report_generated": "10 Apr 2020 01:00
(GMT)",
"periodic_report_time_range": "Previous calendar month", "periodic_report_tier": "All
Web Appliances",
"periodic_report_title": "Web Sites Report_2 Edit", "periodic_report_product_type":
"wsa"}}, {"20200409071005_URL Categories_calendar_week.pdf": {"periodic_report_format": "PDF",
"periodic_report_type_name": "URL Categories", "periodic_report_generated": "09 Apr 2020
07:10 (GMT)",
"periodic_report_time_range": "Previous 7 calendar days", "periodic_report_tier": "All
Web Appliances",
"periodic_report_title": "URL Categories", "periodic_report_product_type": "wsa"}}, {"20200409070946_Web Sites_calendar_week.pdf": {"periodic_report_format": "PDF",
"periodic_report_type_name": "Web Sites", "periodic_report_generated": "09 Apr 2020 07:09
(GMT)",
"periodic_report_time_range": "Previous 7 calendar days", "periodic_report_tier":
"All Web Appliances", "periodic_report_title": "Web Sites", "periodic_report_product_type":
"wsa"}}, {"20200409010011_Application Visibility_calendar_month.pdf": {"periodic_report_format":
"PDF", "periodic_report_type_name": "Application Visibility", "periodic_report_generated":
"09 Apr 2020 01:00 (GMT)", "periodic_report_time_range": "Previous calendar month",
"periodic_report_tier": "All Web Appliances", "periodic_report_title": "Application
Visibility",
"periodic_report_product_type": "wsa"}}, {"20200408010011_Application
Visibility_calendar_month.pdf": {"periodic_report_format": "PDF", "periodic_report_type_name": "Application Visibility",
"periodic_report_generated": "08 Apr 2020 01:00 (GMT)", "periodic_report_time_range":
"Previous calendar month", "periodic_report_tier": "All Web Appliances",
```

```
"periodic_report_title":
"Application Visibility", "periodic_report_product_type": "wsa"}},
{"20200404010011_Application
Visibility_calendar_month.pdf": {"periodic_report_format": "PDF",
"periodic_report_type_name":
"Application Visibility", "periodic_report_generated": "04 Apr 2020 01:00 (GMT)",
"periodic_report_time_range": "Previous calendar month", "periodic_report_tier": "All
Web Appliances",
"periodic_report_title": "Application Visibility",
"periodic_report_product_type": "wsa"}}}]}}
```

アーカイブレポートエントリの詳細の取得

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

サンプル リクエスト

```
GET /wsa/api/v2.0/config/archived_reports/view/20200409070946_Web%20
Sites_calendar_week.pdf?device_type=wsa& HTTP/1.1
cache-control: no-cache
Postman-Token: 986e7426-c8a2-4bbb-9aa5-5b87e9a5ff56
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 10:45:27 GMT
Content-type: application/pdf
Content-Disposition: filename="20200409070946_Web Sites_calendar_week.pdf"
Content-Length: 111175
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

アーカイブレポートエントリの追加

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

サンプル リクエスト

```
POST /wsa/api/v2.0/config/archived_reports?device_type=wsa& HTTP/1.1
cache-control: no-cache
Postman-Token: a144b273-13ff-4f48-bf4c-4232fa5db6f2
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Content-Type: text/plain
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
```

アーカイブレポートエントリの削除

```
accept-encoding: gzip, deflate
content-length: 644
Connection: keep-alive
```

```
{
  "data": {
    "archived_reports": [
      {
        "periodic_report_delivery": "Archived Only",
        "periodic_report_options": {
          "periodic_report_format": "pdf",
          "periodic_report_lang": "en-us",
          "periodic_report_rows": 20,
          "periodic_report_sort_columns": [
            {
              "table": "Users",
              "column": "Transactions Blocked"
            }
          ],
          "periodic_report_charts": [
            {
              "Chart": "Top Users (Left)",
              "Data to display": "Transactions Blocked"
            },
            {
              "Chart": "Top Users (Right)",
              "Data to display": "Bandwidth Used"
            }
          ],
          "periodic_report_time_range": "Previous calendar month",
          "periodic_report_title": "Users Archive Report 2",
          "periodic_report_type": "coeus",
          "periodic_report_type_name": "Users",
          "periodic_report_user_name": "admin"
        }
      ]
    }
  }
}
```

サンプル応答

```
HTTP/1.1 201 Created
Date: Fri, 10 Apr 2020 10:51:41 GMT
Content-type: application/json
Content-Length: 46
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

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

アーカイブレポートエントリの削除

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

サンプル リクエスト

```
DELETE /wsa/api/v2.0/config/archived_reports?id=20200409071005_URL%20
Categories_calendar_week.pdf&device_type=wsa& HTTP/1.1
cache-control: no-cache
Postman-Token: f183a45c-7bcb-40fd-bff1-2940824684b3
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
content-length: 0
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 11:07:27 GMT
Content-type: application/json
Content-Length: 52
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"data": {"message": "1 item deleted successfully"}}
```

トラッキング API

Web トラッキング API を使用すると、個々のトランザクションまたはトランザクションのパターンを検索し、その詳細を取得できます。Web トラッキング API は次のとおりです。

- [プロキシ サービス \(35 ページ\)](#)
- [レイヤ 4 トラフィック モニター \(38 ページ\)](#)
- [SOCKS プロキシ \(39 ページ\)](#)

プロキシ サービス

複数の属性を使用すると、特定のユーザーまたはすべてのユーザーの Web の使用状況に関する情報を取得できます。

概要	GET /api/v2.0/web-tracking/web_transaction?resource_attribute	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、期間、フィルタリング、オフセットと制限、順序、およびトランザクションステータスのパラメータを指定して、プロキシサービスによって処理されるトランザクション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 /wsa/api/v2.0/web-tracking/web_transaction?startDate=2016-09-30T18:00:00.000Z
&endDate=2018-10-31T19:00:00.000Z&filterBy=proxy_services&filterOperator=is&limit=20&offset=0
&device_type=wsa&orderBy=timestamp&orderDir=desc&transactionStatus=all&
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.225.99.234:6080
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 14:43:38 GMT
Content-type: application/json
Content-Length: 26617
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": 20
  },
  "data": [
    {
      "attributes": {
        "webCategory": "Computers and Internet",
        "contentType": "-",
        "pageResources":
"http://update.googleapis.com/service/update2?cup2key=8:128910954&cup2hreq=
3a51fa0a72aa94fcba12403f2eb11c4884b27862dd31a779133c03a0e61d334d",
        "applicationBehavior": "-",
        "malwareCategory": "-",
        "fileName": "-",
        "SHA": "-",
        "bandwidth": 0,
        "policyType": "Access",
        "user": "192.168.0.158",
        "srcIP": "192.168.0.158",
        "relatedTransCount": 1,
        "malwareName": "-",
        "applicationName": "-",
        "policyName": "DefaultGroup",
        "threatType": "Computers and Internet",
        "ampFileVerdict": "-",
        "destinationIP": "-",
        "userType": "[-]",
        "threatReason": "Information about computers and software, such as
hardware, software, software
support, information for software engineers, programming and networking,
website design, the web
and Internet in general, computer science, computer graphics and clipart.
Freeware and Shareware
is a separate category.",
        "serialNo": "4229C3B46A609471867D-0720DA1A8A64",
        "wbrsScore": "No Score",
        "decisionSrc": "WEBCAT",
        "url":
"http://update.googleapis.com/service/update2?cup2key=8:128910954&cup2hreq=3a51fa0a72aa94f
c
ba12403f2eb11c4884b27862dd31a779133c03a0e61d334d",
        "applicationType": "-",
        "timestamp": 1540275265,
        "transactionStatus": "BLOCK",
        "ampVerdict": "-"
      }
    },
    {
      "attributes": {
        "webCategory": "Business and Industry",
        "contentType": "-",
        "pageResources":
"http://www.purple.com/,http://www.purple.com/,http://www.purple.com/",

```

```

        "applicationBehavior": "-",
        "malwareCategory": "-",
        "fileName": "-",
        "SHA": "-",
        "bandwidth": 0,
        "policyType": "Access",
        "user": "10.10.5.105",
        "srcIP": "10.10.5.105",
        "relatedTransCount": 3,
        "malwareName": "-",
        "applicationName": "-",
        "policyName": "DefaultGroup",
        "threatType": "Business and Industry",
        "ampFileVerdict": "-",
        "destinationIP": "-",
        "userType": "[-]",
        "threatReason": "Marketing, commerce, corporations, business practices,
workforce, human resources
        , transportation, payroll, security and venture capital, office supplies,
industrial equipment
        (process equipment), machines and mechanical systems, heating equipment,
cooling equipment,
        materials handling equipment, packaging equipment, manufacturing: solids
handling, metal fabrication
        , construction and building, passenger transportation, commerce,
industrial design, construction
        , building materials, shipping and freight (freight services, trucking,
freight forwarders,
        truckload carriers, freight and transportation brokers, expedited
services, load and freight matching
        , track and trace, rail shipping, ocean shipping, road feeder services,
moving and storage).",
        "serialNo": "4229C3B46A609471867D-0720DA1A8A64",
        "wbrsScore": "No Score",
        "decisionSrc": "WEBCAT",
        "url": "ftp://www.purple.com/",
        "applicationType": "-",
        "timestamp": 1540274946,
        "transactionStatus": "BLOCK",
        "ampVerdict": "-"
    }
},
...
...
{
    "attributes": {
        "webCategory": "Business and Industry",
        "contentType": "-",
        "pageResources":
"ftp://www.purple.com/,http://www.purple.com/,http://www.purple.com/",
        "applicationBehavior": "-",
        "malwareCategory": "-",
        "fileName": "-",
        "SHA": "-",
        "bandwidth": 0,
        "policyType": "Access",
        "user": "10.10.5.105",
        "srcIP": "10.10.5.105",
        "relatedTransCount": 3,
        "malwareName": "-",
        "applicationName": "-",
        "policyName": "DefaultGroup",
        "threatType": "Business and Industry",

```

```

        "ampFileVerdict": "-",
        "destinationIP": "-",
        "userType": "[-]",
        "threatReason": "Marketing, commerce, corporations, business practices,
workforce, human resources...",
        "serialNo": "4229C3B46A609471867D-0720DA1A8A64",
        "wbrsScore": "No Score",
        "decisionSrc": "WEBCAT",
        "url": "ftp://www.purple.com/",
        "applicationType": "-",
        "timestamp": 1540263898,
        "transactionStatus": "BLOCK",
        "ampVerdict": "-"
    }
}
]
}

```

レイヤ 4 トラフィック モニター

複数の属性を使用すると、マルウェアのサイトとポートへの接続に関する情報を取得することができます。

概要	GET /api/v2.0/web-tracking/web_transaction?resource_attribute	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、期間、フィルタリング、オフセットと制限、順序、およびトランザクションステータスのパラメータを指定して、レイヤ 4 トラフィックモニターによって処理されるトランザクション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 /wsa/api/v2.0/web-tracking/web_transaction?startDate=2016-09-30T18:00:00.000Z
&endDate=2018-10-31T19:00:00.000Z&filterBy=l4tm&filterOperator=is&limit=20&offset=0&device_type
=wsa&orderBy=timestamp&orderDir=desc&transactionStatus=all&
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.225.99.234:6080
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 14:58:11 GMT
Content-type: application/json
Content-Length: 12
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": 20
  },
  "data": [
    {
      "attributes": {
        "l4tmDestDomain": "ticketbooking.com",
        "l4tmUser": "10.10.99.68",
        "timestamp": 1534143578,
        "l4tmPort": 443,
        "serialNo": "42292E04F63C3DE54F13-E5D7466DA42E",
        "l4tmDestIpWithDomain": "103.117.180.6@ticketbooking.com",
        "transactionStatus": "BLOCKED"
      }
    },
    {
      "attributes": {
        "l4tmDestDomain": "ticketbooking.com",
        "l4tmUser": "10.10.99.68",
        "timestamp": 1534143578,
        "l4tmPort": 443,
        "serialNo": "42292E04F63C3DE54F13-E5D7466DA42E",
        "l4tmDestIpWithDomain": "103.117.180.6@ticketbooking.com",
        "transactionStatus": "BLOCKED"
      }
    },
    ...
    ...
    {
      "attributes": {
        "l4tmDestDomain": "ticketbooking.com",
        "l4tmUser": "10.10.99.68",
        "timestamp": 1534143577,
        "l4tmPort": 443,
        "serialNo": "42292E04F63C3DE54F13-E5D7466DA42E",
        "l4tmDestIpWithDomain": "103.117.180.6@ticketbooking.com",
        "transactionStatus": "BLOCKED"
      }
    }
  ]
}

```

SOCKS プロキシ

上位宛先とユーザーに関する情報を含む、SOCKS プロキシを通じて処理されるトランザクションに関する情報を取得することができます。

概要	GET /api/v2.0/web-tracking/web_transaction?resource_attribute
----	---

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、期間、フィルタリング、オフセットと制限、順序、およびトランザクションステータスのパラメータを指定して、SOCKS プロキシサービスによって処理されるトランザクション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 /wsa/api/v2.0/web-tracking/web_transaction?startDate=2016-09-30T18:00:00.000Z&
endDate=2018-10-31T19:00:00.000Z&filterBy=socks_proxy&filterOperator=is&limit=20&offset=0&
device_type=wsa&orderBy=timestamp&orderDir=desc&socksTransportProtocol=all&transactionStatus=all&
HTTP/1.1
cache-control: no-cache
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: curl/7.54.0
Accept: */*
Host: 10.225.99.234:6080
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 14:53:33 GMT
Content-type: application/json
Content-Length: 6629
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": 20
  },
  "data": [
    {
      "attributes": {
        "socksUser": "10.10.5.106",
        "socksBandwidth": 0,
        "socksUserType": "[-]",
        "timestamp": 1538044948,
        "socksTransportProtocol": "TCP",
        "socksPort": 80,
        "socksSrcIp": "10.10.5.106",
        "socksDestinationIp": "-",
        "socksPolicyName": "DefaultGroup",
```

```

        "socksHostName": "concede.fmtlib.net",
        "transactionStatus": "BLOCK"
    },
    {
        "attributes": {
            "socksUser": "10.10.5.106",
            "socksBandwidth": 0,
            "socksUserType": "[-]",
            "timestamp": 1538044948,
            "socksTransportProtocol": "TCP",
            "socksPort": 80,
            "socksSrcIp": "10.10.5.106",
            "socksDestinationIp": "-",
            "socksPolicyName": "DefaultGroup",
            "socksHostName": "erupt.fernetmoretti.com.ar",
            "transactionStatus": "BLOCK"
        }
    },
    ...
    ...
    {
        "attributes": {
            "socksUser": "10.10.5.106",
            "socksBandwidth": 0,
            "socksUserType": "[-]",
            "timestamp": 1538044947,
            "socksTransportProtocol": "TCP",
            "socksPort": 80,
            "socksSrcIp": "10.10.5.106",
            "socksDestinationIp": "-",
            "socksPolicyName": "DefaultGroup",
            "socksHostName": "boots.fotopyra.pl",
            "transactionStatus": "BLOCK"
        }
    }
]
}

```

構成 API

構成 API を使用すると、個々のトランザクションまたはトランザクションのパターンを検索し、その詳細を取得できます。構成 API は次のとおりです。

- [全体的な帯域幅](#)
- [PAC ファイル設定](#)
- [識別プロファイル](#)
- [使用許可コントロール \(67 ページ\)](#)
- [アクセス ポリシー \(Access Policies\)](#)
- [ドメイン マップ \(Domain Map\)](#)
- [上位プロキシ](#)

- [HTTPS プロキシ](#)
- [ログ サブスクリプション](#)
- [ヘッダーベース認証](#)
- [要求ヘッダー書き換えプロファイル](#)
- [スマート ソフトウェア ライセンス](#) (113 ページ)
- [システム セットアップ ウィザード](#) (121 ページ)
- [復号ポリシー](#) (125 ページ)
- [ルーティングポリシー](#) (133 ページ)
- [IP スプーフィングプロファイル](#) (137 ページ)
- [設定ファイル](#) (140 ページ)
- [認証レルム](#) (146 ページ)
- [Umbrella シームレス ID](#) (152 ページ)
- [セキュア DNSSec 設定](#) (155 ページ)
- [Identity Service Engine](#) (156 ページ)
- [マルウェア対策レピュテーション](#) (162 ページ)
- [ユーザ通知 \(End-User Notification\)](#) (178 ページ)

全体的な帯域幅

ここでは、次の内容について説明します。

- [全体的な帯域幅の詳細の取得](#)
- [全体的な帯域幅の詳細の変更](#)

全体的な帯域幅の詳細の取得

Secure Web Appliance の全体的な帯域幅に関する情報を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/web_security/overall_bandwidth_limit	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスの全体的な帯域幅設定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 /wsa/api/v3.0/web_security/overall_bandwidth_limit
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 22
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "bandwidth_limit": 0
}
```

全体的な帯域幅の詳細の変更

Secure Web Appliance の全体的な帯域幅制御を変更できます。次に、構文とサポート対象の属性を示します。

概要	PUT wsa/api/v3.0/configure/web_security/overall_bandwidth_limit	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスの全体的な帯域幅設定を変更および設定する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/configure/web_security/overall_bandwidth_limit
```

```

HTTP/1.1
Host: wsa.example.com:6443
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 31

```

```

{
    "bandwidth_limit": 128
}

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:28:32 GMT
Content-type: application/json
Content-Length: 24
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

```

{
    "bandwidth_limit": 128
}

```

PAC ファイルホスト設定

ここでは、次の内容について説明します。

- [PAC ファイル基本設定の取得](#)
- [PAC ファイルの基本設定の変更](#)
- [PAC ファイルの取得](#)
- [PAC ファイルのリストの取得](#)
- [新しい PAC ファイルの追加](#)
- [既存の PAC ファイルの変更](#)
- [PAC ファイルの削除](#)
- [PAC ファイルとホスト名の関連付けの取得](#)
- [PAC ファイルとホスト名の関連付けの追加](#)
- [既存の PAC ファイルとホスト名の関連付けの変更](#)
- [PAC ファイルとホスト名の関連付けの削除](#)

PAC ファイル基本設定の取得

PAC ファイルのホスティングステータス、PAC ファイルの有効期限、およびPAC ファイルの有効期限の制限を取得して設定できます。

概要	GET /wsa/api/v3.0/security_services/pac_basic_setting	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、PAC ファイルのホスティングステータス、PAC ファイルの有効期限ステータス、PAC ファイルサーバーポート、およびPACファイルの有効期限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 /wsa/api/v3.0/security_services/pac_basic_setting HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:33:01 GMT
Content-type: application/json
Content-Length: 135
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "pac_basic_setting": {
    "status": "enable",
    "pac_file_expiry": "enable",
    "pac_server_ports": [
      "3344"
    ],
    "pac_expiration_interval": 1234
  }
}
```

PAC ファイルの基本設定の変更

PAC ファイルホスティングの基本設定を変更できます。

概要	PUT /wsa/api/v3.0/security_services/pac_basic_setting
----	---

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、PAC ファイルのホスティングステータス、PAC ファイルの有効期限ステータス、PAC ファイルサーバーポート、および PAC ファイルの有効期限を変更する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/security_services/pac_basic_setting
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Content-Type: text/plain
Content-Length: 170
{
  "status": "enable",
  "pac_file_expiry": "enable",
  "pac_server_ports": [
    3345
  ],
  "pac_expiration_interval": 1233
}
```

サンプル応答

```
HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 08:12:48 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true

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

PAC ファイルの取得

Secure Web Appliance でホストされている PAC ファイルを取得できます。‘file_name’ パラメータは、Secure Web Appliance から特定のファイルを取得するために使用できます。

概要	GET /wsa/api/v3.0/security_services/pac_file
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Secure Web Appliance でホストされているすべての PAC ファイルのリスト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 /wsa/api/v3.0/security_services/pac_file?file_name=sample_pac_file.pac
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Wed, 13 Jan 2021 09:18:25 GMT
Content-Description: File Transfer
Content-type: application/octet-stream
Content-Disposition: attachment; filename=sample_pac_file.pac
Content-Length: 1195
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
<
function FindProxyForURL(url, host) {

// If the hostname matches, send direct.
    if (dnsDomainIs(host, "intranet.domain.com") ||
        shExpMatch(host, "(*.abcdomain.com|abcdomain.com)"))
        return "DIRECT";

// If the protocol or URL matches, send direct.
    if (url.substring(0, 4)=="ftp:" ||
        shExpMatch(url, "http://abcdomain.com/folder/*"))
        return "DIRECT";

// If the requested website is hosted within the internal network, send direct.
    if (isPlainHostName(host) ||
        shExpMatch(host, "*.local") ||
        isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
        isInNet(dnsResolve(host), "172.16.0.0", "255.240.0.0") ||
        isInNet(dnsResolve(host), "192.168.0.0", "255.255.0.0") ||
        isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
        return "DIRECT";

// If the IP address of the local machine is within a defined
// subnet, send to a specific proxy.
    if (isInNet(myIpAddress(), "10.10.5.0", "255.255.255.0"))
        return "PROXY 1.2.3.4:8080";
```

```
// DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
return "PROXY 4.5.6.7:8080; PROXY 7.8.9.10:8080";
```

PAC ファイルのリストの取得

Secure Web Appliance でホストされているすべての PAC ファイルのリストを取得できます。
 ‘file_name’ パラメータは、Secure Web Appliance から特定のファイルを取得するために使用できます。

概要	GET /wsa/api/v3.0/security_services/pac_file	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Secure Web Appliance でホストされているすべての PAC ファイルのリスト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 /wsa/api/v3.0/security_services/pac_file
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:41:59 GMT
Content-type: application/json
Content-Length: 38
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "pac_files": [
        "sample_pac_file.pac"
    ]
}
```

新しい PAC ファイルの追加

新しい PAC ファイルをアップロードできます。1 つのリクエストで複数のファイルをアップロードできます。

概要	POST /wsa/api/v3.0/security_services/pac_file	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、新しい PAC ファイルを追加する例を示します。

サンプル リクエスト

```
POST /wsa/api/v3.0/security_services/pac_file
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
Content-Length: 1384
Expect: 100-continue
Content-Type: multipart/form-data; boundary=-----6b685d35de1f2379
```

サンプル応答

```
HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 08:52:28 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

既存の PAC ファイルの変更

既存の PAC ファイルを変更できます。



(注) 同じファイル名のファイルが存在する必要があります。

概要	PUT /wsa/api/v3.0/security_services/pac_file
----	--

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、既存の PAC ファイルを変更する方法の例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/security_services/pac_file
HTTP/1.1
Host: wsa.example.com:6443
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Length: 221
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW

----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="";
filename="/C:/Users/Admin/Desktop/sample_pac_file.pac"
Content-Type: <Content-Type header here>

(data)
----WebKitFormBoundary7MA4YWxkTrZu0gW
```

サンプル応答

```
HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 08:55:59 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

PAC ファイルの削除

PAC ファイルを削除できるようになりました。

概要	DELETE /wsa/api/v3.0/security_services/pac_file	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、PAC ファイルを削除する例を示します。

サンプル リクエスト

```
DELETE /wsa/api/v3.0/security_services/pac_file?file_name=sample_pac_file2.pac
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 08:58:39 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

PAC ファイルとホスト名の関連付けの取得

PAC ファイルおよび関連するホスト名を取得できます。

概要	GET /wsa/api/v3.0/security_services/pacfile_host	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、PAC ファイルと関連付けられたホスト名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 /wsa/api/v3.0/security_services/pacfile_host
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 09:00:51 GMT
Content-type: application/json
Content-Length: 160
Connection: close
Access-Control-Allow-Origin: *
```

```

Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "hostname_pac_mapping": {
    "wsa3101": "sample_pac_file.pac",
    "wsa333": "sample_pac_file.pac",
    "wsa3103": "sample_pac_file.pac",
    "wsa332": "sample_pac_file.pac"
  }
}

```

PAC ファイルとホスト名の関連付けの追加

PAC ファイルおよび関連するホスト名を作成できます。

概要	POST /wsa/api/v3.0/security_services/pacfile_host	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、PAC ファイルと関連付けられたホスト名を追加する例を示します。

サンプル リクエスト

```

POST /wsa/api/v3.0/security_services/pacfile_host
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
Content-Type: application/json
Content-Length: 247
{
  "hostname_pac_mapping": [
    {
      "hostname": "wsa1332",
      "pac_filename": "sample_pac_file.pac"
    },
    {
      "hostname": "wsa13101",
      "pac_filename": "sample_pac_file.pac"
    }
  ]
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 09:04:16 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

既存の PAC ファイルとホスト名の関連付けの変更

既存の PAC ファイルおよび関連するホスト名を変更できます。



(注) 与えられたか指定されたホスト名のマッピングが存在する必要があります。

概要	PUT /wsa/api/v3.0/security_services/pacfile_host	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、PAC ファイルをホスト名にマッピングする例を示します。

サンプル リクエスト

```

PUT /wsa/api/v3.0/security_services/pacfile_host
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
Content-Type: application/json
Content-Length: 247
{
  "hostname_pac_mapping": [
    {
      "hostname": "wsa1332",
      "pac_filename": "sample_pac_file.pac"
    },
    {
      "hostname": "wsa13101",
      "pac_filename": "sample_pac_file.pac"
    }
  ]
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 09:06:44 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

PAC ファイルとホスト名の関連付けの削除

既存の PAC ファイルおよび関連するホスト名を削除できます。



(注) 与えられたか指定されたホスト名のマッピングが存在する必要があります。

概要	DELETE /wsa/api/v3.0/security_services/pacfile_host	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、PAC ファイルと関連付けられたホスト名を削除する例を示します。

サンプル リクエスト

```

DELETE /wsa/api/v3.0/security_services/pacfile_host?host_name=wsa1332
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 09:09:18 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

識別プロファイル (Identification Profiles)

ここでは、次の内容について説明します。

- 識別プロファイルの取得
- 識別プロファイルの変更
- 識別プロファイルの追加
- 識別プロファイルの削除

識別の詳細の取得

Secure Web Appliance の識別プロファイルを取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/web_security/identification_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、識別プロファイル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 /wsa/api/v3.0/web_security/identification_profiles
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 14:18:53 GMT
Content-type: application/json
Content-Length: 598
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true

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

{
  "identification_profiles": [
    {
      "status": "enable",
      "description": "Sample ID profile",
      "identification_method": {
```

```

        "auth_scheme": [
            "NTLMSSP"
        ],
        "auth_sequence": "ldaprealm",
        "auth_surrogate_by_proto": {
            "ftp": "ip",
            "http": "ip",
            "https": "ip"
        },
        "prompt_on_sso_failure": "authenticate",
        "use_forward_surrogates": 0,
        "sso_scheme": "sso_none",
        "use_guest_on_auth_failure": 1
    },
    "profile_name": "idsample",
    "members": {
        "protocols": [
            "http",
            "https",
            "ftp"
        ]
    },
    "order": 1
},
{
    "status": "enable",
    "profile_name": "global_identification_profile",
    "description": "Default settings",
    "identification_method": {}
}
]
}

```

識別プロフィールの変更

Secure Web Appliance の識別プロフィールを変更できます。次に、構文とサポート対象の属性を示します。

概要	PUT /wsa/api/v3.0/web_security/identification_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、識別プロフィールを追加する例を示します。

サンプル リクエスト

```

PUT /wsa/api/v3.0/web_security/identification_profiles
HTTP/1.1
Host: wsa.example.com:6443

```

```

User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 275
{
  "identification_profiles": [
    {
      "profile_name": "sample ID",
      "new_profile_name": "sample ID modifiedw"
    },
    {
      "status": "disable",
      "profile_name": "idsample",
      "order": 1
    }
  ]
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 14:28:03 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

識別プロファイルの追加

Secure Web Appliance の識別プロファイルを作成できます。次に、構文とサポート対象の属性を示します。

概要	POST /wsa/api/v3.0/web_security/identification_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、識別プロファイルを変更する例を示します。

サンプル リクエスト

```

POST /wsa/api/v3.0/web_security/identification_profiles
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz

```

```

Content-Type: application/json
Content-Length: 900
{
  "identification_profiles": [
    {
      "status": "enable",
      "description": "Sample description",
      "identification_method": {
        "auth_scheme": [
          "Basic"
        ],
        "auth_sequence": "ldaprealm",
        "auth_surrogate_by_proto": {
          "ftp": "ip",
          "http": "ip",
          "https": "ip"
        },
        "prompt_on_sso_failure": "authenticate",
        "use_forward_surrogates": 1,
        "sso_scheme": "sso_none",
        "use_guest_on_auth_failure": 0
      },
      "profile_name": "sample ID",
      "members": {
        "protocols": [
          "http",
          "https",
          "ftp" ]
      },
      "order": 1
    }
  ]
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 08:12:48 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

識別プロファイルの削除

Secure Web Appliance の識別プロファイルを削除できます。次に、構文とサポート対象の属性を示します。

概要	DELETE /wsa/api/v3.0/web_security/identification_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、識別プロファイルを削除する例を示します。

サンプル リクエスト

```
DELETE
/wsa/api/v3.0/web_security/identification_profiles?profile_names=idsample,%20sample%20ID%20profile

HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
HTTP/1.1 207
Date: Mon, 11 Jan 2021 14:31:21 GMT
Content-type: application/json
Content-Length: 258
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "success_list": [
    {
      "status": 200,
      "message": "success",
      "profile_name": "idsample"
    }
  ],
  "failure_list": [
    {
      "status": 404,
      "message": "profile name 'sample ID profile' doesn't exist",
      "profile_name": "sample ID profile"
    }
  ],
  "success_count": 1,
  "failure_count": 1
}
```

アクセス ポリシー

ここでは、次の内容について説明します。

- [アクセスポリシーの取得](#)
- [アクセスポリシーの変更](#)
- [アクセス ポリシーの追加](#)
- [アクセスポリシーの削除](#)

アクセスポリシーの取得

Secure Web Appliance で設定されたアクセスポリシーのリストを取得できます。

概要	GET /wsa/api/v3.0/web_security/access_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ポリシー名「AP106」のアクセスポリシー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 /wsa/api/v3.0/web_security/access_policies?policy_names=AP106
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTiz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 14:34:52 GMT
Content-type: application/json
Content-Length: 1143
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true

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

```
{
  "access_policies": [
    {
      "policy_expiry": "",
      "policy_status": "enable",
      "policy_name": "AP106",
      "membership": {
        "identification_profiles": [
          {
            "_all_": {
              "auth": "No Authentication"
            }
          }
        ],
        "url_categories": [
          {
            "id_profile": "",
            "value": {
```

```

        "predefined": [
            "Advertisements",
            "Alcohol",
            "Arts",
            "Astrology"
        ]
    }
}
],
},
"objects": {
    "state": "use_global"
},
"protocols_user_agents": {
    "state": "use_global"
},
"http_rewrite_profile": "use_global",
"avc": {
    "state": "use_global"
},
"policy_description": "new test policy",
"policy_order": 1,
"url_filtering": {
    "safe_search": {
        "status": "use_global"
    },
    "content_rating": {
        "status": "use_global"
    },
},
"yt_cats": {
    "use_global": [
        "Film & Animation",
        "Autos & Vehicles",
        "Music",
        "Pets & Animals",
        "Sports",
        "Travel & Events",
        "Gaming",
        "People & Blogs",
        "Comedy",
        "Entertainment",
        "News & Politics",
        "Howto & Style",
        "Education",
        "Science & Technology",
        "Nonprofits & Activism"
    ]
},
"state": "custom",
"exception_referred_embedded_content": {
    "state": "disable"
},
"update_cats_action": "use_global",
"predefined_cats": {
    "use_global": [
        "Advertisements",
        "Alcohol",
        "Arts",
        "Astrology"
    ]
}
},
"amw_reputation": {
    "state": "use_global"
}

```

```

    }
  }
]
}

```

アクセスポリシーの変更

アクセスポリシーとその設定ペイロードのリストを変更できます。

概要	PUT /wsa/api/v3.0/web_security/access_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、アクセスポリシーの変更方法の例を示します。

サンプル リクエスト

```

PUT /wsa/api/v3.0/web_security/access_policies
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Content-Type: application/json
Content-Length: 721
{
  "access_policies": [
    {
      "policy_name": "global policy",
      "protocols_user_agents": {
        "state": "custom",
        "block_protocols": [
          "http",
          "https"
        ]
      }
    },
    {
      "policy_name": "sample AP",
      "protocols_user_agents": {
        "block_protocols": [
          "http"
        ]
      }
    },
    {
      "policy_name": "AP106",
      "protocols_user_agents": {
        "state": "custom",

```

```

        "block_protocols": [
            "https"
        ]
    }
}
]
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 14:28:03 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

次に、アクセスポリシーを変更する方法の別の例を示します。

サンプル リクエスト

```

PUT /wsa/api/v3.0/web_security/access_policies
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 721
{
  "access_policies": [
    {
      "policy_status": "enable",
      "policy_order": 1,
      "policy_name": "ACC25",
      "membership": {
        "identification_profiles": [
          {
            "profile_name": "ID01",
            "auth": "No Authentication"
          }
        ]
      }
    },
    {
      "adc": {
        "applications": {
          "Collaboration": {
            "monitor": {
              "Line": {
                "restrict": [
                  "Block Uploads"
                ]
              }
            }
          },
          "block": [
            "Line2"
          ],
          "default_action": "monitor"
        },
        "Social Networking": {
          "monitor": {
            "LinkedIn": {
              "restrict": [
                "Block Posts/Shares"
              ]
            }
          }
        }
      }
    }
  ]
}

```

サンプル応答

アクセス ポリシーの追加

概要	POST /wsa/api/v3.0/web_security/access_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、アクセスポリシーの作成方法の例を示します。

```
POST /wsa/api/v3.0/web_security/access_policies
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlIz
Content-Type: application/json
Content-Length: 1350
Expect: 100-continue
```

```

{
  "access_policies": [
    {
      "policy_status": "enable",
      "policy_name": "sample AP",
      "policy_order": 1,
      "membership": {
        "identification_profiles": [
          {
            "profile_name": "",
            "auth": "No Authentication"
          }
        ],
        "user_agents": {
          "predefined": [
            "Firefox",
            "Safari",
            "MSIE/10"
          ],
          "custom": [
            "Mozilla/. Gecko/. Firefox/"
          ],
          "is_inverse": 0
        }
      },
      "protocols_user_agents": {
        "state": "custom",
        "allow_connect_ports": [
          "20",
          "21",
          "1-65535"
        ],
        "block_protocols": [
          "ftp",
          "http",
          "https",
          "nativeftp"
        ],
        "block_custom_user_agents": [
          "Mozilla/* Gecko/* Firefox/, Mozilla/4.0 (compatible; MSIE 5.5;)",
          "test"
        ]
      }
    }
  ]
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Mon, 11 Jan 2021 14:28:03 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

アクセスポリシーの削除

ポリシー名を使用してアクセスポリシーを削除できます。

概要	DELETE /wsa/api/v3.0/web_security/access_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、複数のアクセスポリシーを一度に削除する例を示します。

。

サンプル リクエスト

```
DELETE
/wsa/api/v3.0/web_security/access_policies?policy_names=AP105,%20sample%20AP,%20AP110
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
```

サンプル応答

```
HTTP/1.1 207
Date: Mon, 11 Jan 2021 14:44:21 GMT
Content-type: application/json
Content-Length: 289
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
```

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

```
{
  "success_list": [
    {
      "status": 200,
      "message": "success",
      "policy_name": "AP105"
    },
    {
      "status": 200,
      "message": "success",
      "policy_name": "sample AP"
    }
  ],
  "failure_list": [
    {
      "status": 404,
      "message": "policy name does not exist.",
      "policy_name": "AP110"
    }
  ]
}
```

```

    ],
    "success_count": 2,
    "failure_count": 1
  }

```

使用許可コントロール

ここでは、次の内容について説明します。

- [使用許可コントロール \(67 ページ\)](#)

使用許可コントロール

使用許可コントロールAPIは、アプリケーションの可視性制御（AVC）とアプリケーションの検出制御（ADC）を切り替えるために役立ちます。

概要	POST/wsa/api/v3.0/security_services/acceptable_use_control	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Acceptable Use Control API の使用例を示します。

サンプル リクエスト

```

POST/wsa/api/v3.0/security_services/acceptable_use_control
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Content-Type: application/json
Content-Length: 721
{
  "acceptable_use_control": [
    {
      "Cisco Web Usage Controls": "Enable",
      "Application Control": "ADC"
    }
  ]
}

```



- (注)
- Cisco Web Usage Controls の値は、Enable または Disable にする必要があります。
 - Application Control の値は、ADC、AVC、または Disable にする必要があります。

サンプル応答

```
HTTP/1.1 204 No Content
Date: Sat, 11 Feb 2023 02:50:10 GMT
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

ドメインマップ

ここでは、次の内容について説明します。

- [ドメインマップの取得](#)
- [ドメインマップの変更](#)
- [ドメインマップの追加](#)
- [ドメインマップの削除](#)

ドメインマップの詳細の取得

Secure Web Appliance のドメインマップの詳細を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v2.0/configure/web_security/domain_map	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ドメインマップ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 /wsa/api/v2.0/configure/web_security/domain_map
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlZ
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 08:41:26 GMT
Content-type: application/json
Content-Length: 239
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data": [
    {
      "IP_addresses": [
        "10.10.1.1"
      ],
      "domain_name": "example.cisco.com",
      "order": 1
    },
    {
      "domain_name": "sample.cisco.com",
      "IP_addresses": [
        "10.10.2.25"
      ],
      "order": 2
    }
  ],
  "res_message": "Data received successfully.",
  "res_code": 200
}
```

ドメインマップの詳細の変更

ドメインマップの詳細を変更できます。

概要	PUT /wsa/api/v2.0/configure/web_security/domain_map	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ドメインマップの詳細を変更する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v2.0/configure/web_security/domain_map
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Content-Type: application/json
Content-Length: 247
```

```
[
  {
    "new_domain_name": "abcd.com",
    "domain_name": "abc.com",
    "order": 102,
    "IP_addresses": [
      "002:45:32::00:12/24", "2.2.2.1-10"
    ]
  }
]
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 09:03:24 GMT
Content-type: application/json
Content-Length: 204
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data":
  {
    "update_success":
    [
      {
        "order": 4,
        "domain_name":
        "abcd.com",
        "server_list":
        [
          "2:45:32::12/24",
          "2.2.2.1-10"
        ]
      }
    ],
    "update_failure":
    [
    ],
    "res_message":
    "Success: 1,
    Failure: 0",
    "res_code": 200
  }
}
```

ドメインマップの追加

ドメインマップとその設定を作成できます。

概要	POST /wsa/api/v2.0/configure/web_security/domain_map	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ドメインマップを作成する例を示します。

サンプル リクエスト

```
POST /wsa/api/v2.0/configure/web_security/domain_map
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 414
```

```
[
  {
    "domain_name": "abc.com",
    "order": 102,
    "IP_addresses": [
      "002:45:32::00:12/24", "2.2.2.1-10"
    ]
  },
  {
    "domain_name": "xyz.com",
    "order": 102,
    "IP_addresses": [
      "002:55:34::00:12/24", "2.5.5.1-10"
    ]
  }
]
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 08:51:49 GMT
Content-type: application/json
Content-Length: 286
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```

{
  "res_data":
  {
    "add_failure":
    [
    ],
    "add_success":
    [
      {
        "domain_name":
        "abc.com",
        "order": 4,
        "server_list":
        [
          "2:45:32::12/24",
          "2.2.2.1-10"
        ]
      },
      {
        "domain_name": "xyz.com",
        "order": 5,
        "server_list":
        [
          "2:55:34::12/24",
          "2.5.5.1-10"
        ]
      }
    ]
  },
  "res_message":
  "Success: 2,
  Failure: 0",
  "res_code": 201
}

```

ドメインマップの削除

Secure Web Appliance のドメインマップを削除できます。次に、構文とサポート対象の属性を示します。

概要	DELETE /wsa/api/v2.0/configure/web_security/domain_map	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ドメインマップを削除する例を示します。

サンプル リクエスト

```
DELETE /wsa/api/v2.0/configure/web_security/domain_map
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 33

{
  "domain_name": "xyz.com"
}
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 09:10:08 GMT
Content-type: application/json
Content-Length: 103
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition,
jwtToken

{
  "res_data":
  {
    "delete_success":
    [
      "xyz.com"
    ]
  },
  "res_message":
  "Success: 1,
  Failure: 0",
  "res_code": 200
}
```

上位プロキシ

ここでは、次の内容について説明します。

- [上位プロキシの取得](#)
- [アップストリームプロキシの変更](#)
- [上位プロキシの追加](#)
- [上位プロキシの削除](#)
- [プロキシサーバーの上位プロキシの変更](#)
- [プロキシサーバーの上位プロキシの変更](#)
- [プロキシサーバーの上位プロキシの削除](#)

上位プロキシの詳細の取得

Secure Web Appliance の上位プロキシの詳細を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v2.0/configure/ network/upstream_proxy	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、上位プロキシ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 /wsa/api/v2.0/configure/network/upstream_proxy
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 09:17:25 GMT
Content-type: application/json
Content-Length: 253
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data": [
    {
      "used_by_ocsp": true,
      "proxy_servers": [
        {
          "retries": 2,
          "host": "dut058.perf8",
          "port": 3128
        }
      ],
      "load_balancing": "none",
      "failure_handling": "connect",
      "group_name": "Test"
    }
  ],
}
```

```

    "res_message": "Data received successfully.",
    "res_code": 200
}

```

上位プロキシ設定の変更

Secure Web Appliance の上位プロキシ設定を変更できます。

概要	PUT /wsa/api/v2.0/configure/network/upstream_proxy	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、上位プロキシのグループ名、新しいグループ名、障害処理、およびロードバランシングのプロパティを変更する例を示します。

サンプル リクエスト

```

PUT /wsa/api/v2.0/configure/network/upstream_proxy
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 170

```

```

[
  {
    "group_name": "Test11",
    "new_group_name": "Test1",
    "failure_handling": "drop",
    "load_balancing": "none"
  }
]

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 09:35:27 GMT
Content-type: application/json
Content-Length: 187
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"res_data":
{

```

```

    "modify_success":
    [
      {
        "new_group_name": "Test1",
        "failure_handling":
        "drop",
        "load_balancing": "none",
        "group_name": "Test11"
      }
    ],
    "res_message":
    "Success: 1",
    "res_code": 200}

```

上位プロキシの追加

上位プロキシとその設定を作成できます。

概要	POST /wsa/api/v2.0/configure/network/upstream_proxy	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、上位プロキシを作成する例を示します。

サンプル リクエスト

```

POST /wsa/api/v2.0/configure/network/upstream_proxy
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 252

```

```

{
  "group_name": "Test2",
  "failure_handling": "connect",
  "load_balancing": "none",
  "proxy_servers": [
    {
      "host": "www.google.com",
      "retries": 1,
      "port": 22
    }
  ]
}

```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 09:30:52 GMT
Content-type: application/json
Content-Length: 232
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "res_data":
  {
    "add_success":
    [
      {
        "proxy_servers":
        [
          {
            "retries": 1,
            "host":
              "www.google.com",
            "port": 22
          }
        ],
        "load_balancing":
          "none",
        "failure_handling":
          "connect",
        "group_name":
          "Test2"
      }
    ],
    "res_message":
      "Success: 1",
    "Success": 1,
    "res_code": 201
  }
}
```

上位プロキシの削除

Secure Web Appliance の上位プロキシを削除できます。次に、構文とサポート対象の属性を示します。

概要	DELETE /wsa/api/v2.0/configure/network/upstream_proxy	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、上位プロキシを削除する例を示します。

サンプル リクエスト

```
DELETE /wsa/api/v2.0/configure/network/upstream_proxy HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 30
```

```
{
  "proxy_group": "Test1"
}
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 09:39:38 GMT
Content-type: application/json
Content-Length: 160
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data": {
    "delete_success": [
      "Test1"
    ]
  },
  "res_message": "Success: 1",
  "res_code": 200
}
```

上位プロキシサーバーの変更

上位プロキシサーバーの設定を変更できます。

概要	PUT /wsa/api/v2.0/configure/network/upstream_proxy/servers	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、上位プロキシサーバーの名前を変更する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v2.0/configure/network/upstream_proxy/servers
HTTP/1.1
Host: wsas.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 243
```

```
[
  {
    "group_name": "Test3",
    "proxy_servers": [
      {
        "retries": 1,
        "host": "7.7.7.7",
        "new_host": "7.7.8.8",
        "port": 22
      }
    ]
  }
]
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 10:17:00 GMT
Content-type: application/json
Content-Length: 194
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"res_data": {"modify_success": [{"proxy_servers": [{"retries": 1,
"host": "7.7.7.7", "port": 22, "new_host": "7.7.8.8"}], "group_name": "Test3"}]},
"res_message": "Success: 1", "res_code": 200}
```

上位プロキシサーバーの追加

上位プロキシサーバーとその設定を作成できます。

概要	POST /wsa/api/v2.0/configure/network/upstream_proxy/servers	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、上位プロキシサーバーを設定に追加する例を示します。

サンプル リクエスト

```
POST /wsa/api/v2.0/configure/network/upstream_proxy/servers
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Content-Type: application/json
Content-Length: 204
```

```
[
  {
    "group_name": "Test3",
    "proxy_servers": [
      {
        "retries": 1,
        "host": "4.4.4.4",
        "port": 22
      }
    ]
  }
]
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 10:09:43 GMT
Content-type: application/json
Content-Length: 168
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data": {
    "add_success": [
      {
        "proxy_servers": [
          {
            "retries": 1,
            "host": "4.4.4.4",
            "port": 22
          }
        ],
        "group_name": "Test3"
      }
    ]
  },
  "res_message": "Success: 1",
  "res_code": 201
}
```

上位プロキシサーバーの削除

Secure Web Appliance の上位プロキシサーバーの設定を削除できます。次に、構文とサポート対象の属性を示します。

概要	DELETE /wsa/api/v2.0/configure/network/upstream_proxy/servers	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、上位プロキシの設定を削除する例を示します。

。

サンプル リクエスト

```
DELETE /wsa/api/v2.0/configure/network/upstream_proxy/servers
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 204
```

```
[
  {
    "group_name": "Test3",
    "proxy_servers": [
      {
        "retries": 1,
        "host": "7.7.8.8",
        "port": 22
      }
    ]
  }
]
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 10:28:07 GMT
Content-type: application/json
Content-Length: 171
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data":
  {
    "delete_success":
    [
      {
        "proxy_servers":
        [
          {
            "retries": 1,
            "host": "7.7.8.8",
            "port": 22
          }
        ],
        "group_name": "Test3"
      }
    ],
    "res_message":
    "Success: 1",
    "res_code": 200
  }
}
```

HTTPS プロキシ

ここでは、次の内容について説明します。

- [HTTPS プロキシの取得](#)
- [HTTPS プロキシの変更](#)
- [HTTPS プロキシの取得：証明書ファイルのダウンロード](#)
- [HTTPS プロキシの取得：OCSP 設定](#)
- [HTTPS プロキシの変更：OCSP 設定](#)

HTTPS プロキシの詳細の取得

Secure Web Appliance の HTTPS プロキシの詳細を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v2.0/configure/security_services/proxy/https	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、HTTPS プロキシ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 /wsa/api/v2.0/configure/security_services/proxy/https
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 06:31:10 GMT
Content-type: application/json
Content-Length: 659
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
<
* Closing connection 0
* TLSv1.1 (OUT), TLS alert, Client hello (1):
{
  "res_data":
  {
    "uploaded_cert_data": null,
    "decrypt":
    {
      "user_notification": true,
      "user_acknowledgement": true,
      "authentication": true,
      "application_visibility": false
    },
    "current_cert_type":
    "generated",
    "invalid_cert_handling":
    {
      "expired_cert":
      "scan",
      "invalid_leaf_cert":
      "drop",
      "unrecognized_root":
      "drop",
      "invalid_signing_cert":
      "drop",
      "mismatched_hostname":
      "scan",
      "other_error":
      "drop"
    },
    "generated_cert_data":
    {
      "is_x509v3_critical": false,
      "expires": 1768407685,
      "country":
      "US",
      "org_unit":
      "SBG",
```

```

        "common_name": "CISCO",
        "org": "CISCO"
    },
    "https_ports": "443",
    "https_enabled": false
},
"res_message":
"Data received successfully.",
"res_code": 200
}

```

HTTP プロキシ設定の変更

HTTP プロキシ設定を変更できます。

概要	PUT /wsa/api/v2.0/configure/security_services/proxy/https	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、HTTP プロキシ設定を変更する例を示します。

サンプル リクエスト

```

PUT /wsa/api/v2.0/configure/security_services/proxy/https
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Content-Length: 2237
Expect: 100-continue
Content-Type: multipart/form-data; boundary=-----23fc1d072de41043
--form 'https_enabled="true"' \
--form 'https_ports="9443"' \
--form 'authentication="true"' \
--form 'user_acknowledgement="true"' \
--form 'application_visibility="false"' \
--form 'user_notification="false"' \
--form 'expired_cert="drop"' \
--form 'invalid_leaf_cert="drop"' \
--form 'unrecognized_root="drop"' \
--form 'invalid_signing_cert="drop"' \
--form 'mismatched_hostname="drop"' \
--form 'other_error="drop"' \
--form 'current_cert_type="generated"' \
--form 'accept_license="true"' \
--form 'common_name="dut037.perf8"' \
--form 'org="CISCOSBG"' \
--form 'org_unit="CS"' \

```

```
--form 'country="IN"' \
--form 'expires="35"' \
--form 'is_x509v3_critical="true"'
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 07:51:13 GMT
Content-type: application/json
Content-Length: 691
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
<
* Closing connection 0
* TLSv1.1 (OUT), TLS alert, Client hello (1):
{
  "res_data": {
    "expired_cert": "drop",
    "is_x509v3_critical": true,
    "expires": 35,
    "invalid_leaf_cert": "drop",
    "unrecognized_root": "drop",
    "invalid_signing_cert": "drop",
    "user_acknowledgement": true,
    "country": "IN",
    "common_name": "dut037.perf8",
    "org_unit": "CS",
    "mismatched_hostname": "drop",
    "current_cert_type": "generated",
    "user_notification": false,
    "authentication": true,
    "https_ports": "9443",
    "https_enabled": true,
    "org": "CISCOSBG",
    "application_visibility": false,
    "other_error": "drop"
  },
  "res_message": "Data updated successfully.",
  "res_code": 200
}
```

HTTP プロキシの取得：証明書ファイルのダウンロード

Secure Web Appliance の HTTP プロキシダウンロード証明書ファイルを取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v2.0/configure/security_services/proxy/https/download	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』を参照してください。	
要求ヘッダー		Host、Accept、Authorization

例

次に、HTTP プロキシダウンロード証明書ファイルの詳細を取得するクエリの例を示します。

```
GET /wsa/api/v2.0/configure/security_services/proxy/https/download?cert_type=generated
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
```

[illegible]

Secure Web Appliance の HTTP プロキシ OCSP 設定を取得できます。次に、構文とサポート対象の属性を示します。

AsyncOS 16.0 for Cisco Secure Web Appliance-API スタートアップガイド

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、HTTPS プロキシ OCSP 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 /wsa/api/v2.0/configure/security_services/proxy/ocsp
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 08:06:43 GMT
Content-type: application/json
Content-Length: 484
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "res_data": {
    "ocsp_network_error_timeout": 10,
    "ocsp_result_handling": {
      "unknown": "scan",
      "revoked": "drop",
      "error": "scan"
    },
    "ocsp_valid_response_cache_timeout": 3600,
    "ocsp_proxy_group": "",
    "ocsp_enabled": true,
    "ocsp_invalid_response_cache_timeout": 120,
    "ocsp_proxy_group_exempt_list": [],
    "ocsp_clock_skew": 300,
    "ocsp_network_error_cache_timeout": 60,
    "ocsp_use_upstream_proxy": false,
    "ocsp_use_nonce": false
  },
  "res_message": "Data received successfully.",
  "res_code": 200
}
```

HTTP プロキシの変更：OCSP 設定

HTTP プロキシ OCSP 設定を変更できます。

概要	PUT /wsa/api/v2.0/configure/security_services/proxy/ocsp	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、HTTP プロキシ OCSP 設定を変更する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v2.0/configure/security_services/proxy/ocsp
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTiz
Content-Type: application/json
Content-Length: 528
```

```
{
  "ocsp_enabled": true,
  "ocsp_valid_response_cache_timeout": 1200,
  "ocsp_invalid_response_cache_timeout": 120,
  "ocsp_network_error_cache_timeout": 34324,
  "ocsp_clock_skew": 23,
  "ocsp_network_error_timeout": 3,
  "ocsp_result_handling":
    { "unknown": "scan",
      "revoked": "decrypt",
      "error": "scan"
    },
  "ocsp_use_nonce": true,
  "ocsp_use_upstream_proxy": true,
  "ocsp_proxy_group": "Test",
  "ocsp_proxy_group_exempt_list": []
}
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 08:27:32 GMT
Content-type: application/json
Content-Length: 489
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data": {
    "ocsp_enabled": true,
    "ocsp_result_handling": {
      "unknown": "scan",
      "revoked": "decrypt",
      "error": "scan"
    },
    "ocsp_network_error_timeout": 3,
    "ocsp_invalid_response_cache_timeout": 120,
    "ocsp_proxy_group_exempt_list": [],
    "ocsp_valid_response_cache_timeout": 1200,
    "ocsp_clock_skew": 23,
    "ocsp_proxy_group": "Test",
    "ocsp_network_error_cache_timeout": 34324,
    "ocsp_use_upstream_proxy": true,
    "ocsp_use_nonce": true
  },
  "res_message": "Data updated successfully.",
  "res_code": 200
}
```

ログサブスクリプション

ここでは、次の内容について説明します。

- [ログサブスクリプションの取得](#)
- [ログサブスクリプションの変更](#)
- [ログサブスクリプションの追加](#)
- [ログサブスクリプションの削除](#)
- [ログサブスクリプションの変更：ロールオーバー](#)
- [取得フィールドリストのログサブスクリプションの取得](#)
- [ログタイプのデフォルト値を取得するためのログサブスクリプションの取得](#)
- [ログサブスクリプション（非匿名化）の追加](#)

ログサブスクリプションの取得

Secure Web Appliance のログサブスクリプションを取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v2.0/configure/system/log_subscriptions
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ログサブスクリプション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 /wsa/api/v2.0/configure/system/log_subscriptions
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 10:34:48 GMT
Content-type: application/json
Content-Length: 7945
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data": [
    {
      "rollover_interval": "none",
      "log_name": "accesslogs",
      "log_type": "Access Logs",
      "log_file_name": "aclog",
      "enable_deanonymization": true
    },
    {
      "rollover_interval": "none",
      "log_name": "amp_logs",
      "log_type": "AMP Engine Logs",
      "log_file_name": "amp",
      "enable_deanonymization": false
    },
    {
      "rollover_interval": "none",
      "log_name": "archiveinspect_logs",
      "log_type": "ArchiveInspect Logs",
      "log_file_name": "archiveinspect_log",
      "enable_deanonymization": false
    },
    {
      "rollover_interval": "none",
      "log_name": "audit_logs",
      "log_type": "Audit Logs",
      "log_file_name": "audit_log",
      "enable_deanonymization": false
    }
  ],
}
```

```

{
  "rollover_interval": "none",
  "log_name": "authlogs",
  "log_type": "Authentication Framework Logs",
  "log_file_name": "authlog",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "avc_logs",
  "log_type": "AVC Engine Logs",
  "log_file_name": "avc_log",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "bypasslogs",
  "log_type": "Proxy Bypass Logs",
  "log_file_name": "tmon_bypass",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "cli_logs",
  "log_type": "CLI Audit Logs",
  "log_file_name": "cli",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "configdefragd_logs",
  "log_type": "Configuration Logs",
  "log_file_name": "configdefragd_log",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "csid_logs",
  "log_type": "CSI Service Logs",
  "log_file_name": "csid_log",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "dca_logs",
  "log_type": "DCA Engine Logs",
  "log_file_name": "dca_log",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "external_auth_logs",
  "log_type": "External Authentication Logs",
  "log_file_name": "external_auth_logs",
  "enable_deanonymization": false
},
{
  "rollover_interval": "none",
  "log_name": "feedback_logs",
  "log_type": "Feedback Logs",
  "log_file_name": "feedback_log",
  "enable_deanonymization": false
},
{

```

```

        "rollover_interval": "none",
        "log_name": "feedsd_logs",
        "log_type": "Feedsd Logs",
        "log_file_name": "feedsd_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "fips_logs",
        "log_type": "FIPS Logs",
        "log_file_name": "fips_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "ftpd_logs",
        "log_type": "FTP Server Logs",
        "log_file_name": "ftpd",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "gui_logs",
        "log_type": "GUI Logs",
        "log_file_name": "gui",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "haystackd_logs",
        "log_type": "Haystack Logs",
        "log_file_name": "haystackd",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "httpslog",
        "log_type": "HTTPS Logs",
        "log_file_name": "httpslog",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "hybridd_logs",
        "log_type": "Hybrid Service Logs",
        "log_file_name": "hybridd_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "idsdataloss_logs",
        "log_type": "Data Security Logs",
        "log_file_name": "idsdataloss_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "ise_service_log",
        "log_type": "ISE Service Logs",
        "log_file_name": "ise_service_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",

```

```

        "log_name": "logderrorlogs",
        "log_type": "Logging Logs",
        "log_file_name": "logderrlog",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "mcafee_logs",
        "log_type": "McAfee Logs",
        "log_file_name": "mcafee_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "musd_logs",
        "log_type": "AnyConnect Secure Mobility Daemon Logs",
        "log_file_name": "musd_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "ocspd_logs",
        "log_type": "OCSP Logs",
        "log_file_name": "ocspd_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "pacd_logs",
        "log_type": "PAC File Hosting Daemon Logs",
        "log_file_name": "pacd_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "policyinspectord_logs",
        "log_type": "Policy Inspector Logs",
        "log_file_name": "policyinspectord_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "proxylogs",
        "log_type": "Default Proxy Logs",
        "log_file_name": "proxyerrlog",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "reportd_logs",
        "log_type": "Reporting Logs",
        "log_file_name": "reportd",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "reportqueryd_logs",
        "log_type": "Reporting Query Logs",
        "log_file_name": "reportqueryd",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "saas_auth_log",

```

```

        "log_type": "SaaS Auth Logs",
        "log_file_name": "saas_auth_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "shd_logs",
        "log_type": "SHD Logs",
        "log_file_name": "shd",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "sl_usercountd_logs",
        "log_type": "SL Usercount Logs",
        "log_file_name": "sl_usercountd_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "smartlicense",
        "log_type": "Smartlicense Logs",
        "log_file_name": "smartlicense",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "snmp_logs",
        "log_type": "SNMP Logs",
        "log_file_name": "snmp_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "sntpd_logs",
        "log_type": "NTP Logs",
        "log_file_name": "sntpd",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "sophos_logs",
        "log_type": "Sophos Logs",
        "log_file_name": "sophos_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "sse_connectord_logs",
        "log_type": "SSE Connector Daemon Logs",
        "log_file_name": "sse_connectord_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "status",
        "log_type": "Status Logs",
        "log_file_name": "status.log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "system_logs",
        "log_type": "System Logs",

```

```

        "log_file_name": "system",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "trafmon_errlogs",
        "log_type": "Traffic Monitor Error Logs",
        "log_file_name": "tmon_err",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "trafmonlogs",
        "log_type": "Traffic Monitor Logs",
        "log_file_name": "tmon_misc",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "uds_logs",
        "log_type": "UDS Logs",
        "log_file_name": "uds_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "updater_logs",
        "log_type": "Updater Logs",
        "log_file_name": "updater_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "upgrade_logs",
        "log_type": "Upgrade Logs",
        "log_file_name": "upgrade_logs",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "wbnp_logs",
        "log_type": "WBNP Logs",
        "log_file_name": "wbnp_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "webcat_logs",
        "log_type": "Web Categorization Logs",
        "log_file_name": "webcat_log",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "webrootlogs",
        "log_type": "Webroot Logs",
        "log_file_name": "webrootlog",
        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "webtapd_logs",
        "log_type": "Webtapd Logs",
        "log_file_name": "webtapd",

```

```

        "enable_deanonymization": false
    },
    {
        "rollover_interval": "none",
        "log_name": "welcomeack_logs",
        "log_type": "Welcome Page Acknowledgement Logs",
        "log_file_name": "welcomeack_log",
        "enable_deanonymization": false
    }
],
"res_message": "Data received successfully.",
"res_code": 200
}

```

ログサブスクリプションの変更

ログサブスクリプションの基本設定を変更できます。

概要	PUT /wsa/api/v2.0/configure/system/log_subscriptions	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ログサブスクリプションの基本設定を変更する例を示します。

サンプル リクエスト

```

PUT /wsa/api/v2.0/configure/system/log_subscriptions
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 501

```

```

[
  {
    "log_name": "logs_1",
    "new_log_name": "logs_4",
    "log_level": "debug",
    "log_type": "CLI Audit Logs",
    "log_file_name": "cli_file_name",
    "rollover_file_size": 10240,
    "retrieval_method":
    {
      "max_num_files": 10,
      "method": "local"
    },
    "rollover_by_time":

```

```

        {
            "rollover_interval": "custom",
            "rollover_custom_time": 17280
        }
    ]
}

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 12:03:46 GMT
Content-type: application/json
Content-Length: 491
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

```

```

{
    "res_data":
    {
        "update_success":
        [
        ],
        "update_failure": [
        {
            "content":
            {
                "rollover_file_size": 10240,
                "log_name": "logs_1",
                "retrieval_method":
                {
                    "max_num_files": 10,
                    "method": "local"},
                    "new_log_name":
                    "logs_4",
                    "log_level":
                    "debug", "log_type":
                    "CLI Audit Logs",
                    "log_file_name":
                    "cli_file_name",
                    "rollover_by_time":
                    {
                        "rollover_interval":
                        "custom",
                        "rollover_custom_time":
                        17280
                    }
                },
                "error_msg":
                "'log_name':
                'logs_1' does not exist."}
            ],
            "res_message":
            "Success: 0,
            Failure: 1",
            "res_code": 400
        }
    }
}

```

ログサブスクリプションの追加

ログサブスクリプションとその設定を作成できます。

概要	POST /wsa/api/v2.0/configure/system/log_subscriptions	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ログサブスクリプションを作成する例を示します。

サンプル リクエスト

```
POST /wsa/api/v2.0/configure/system/log_subscriptions
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Content-Type: application/json
Content-Length: 527
```

```
[
  {
    "new_log_name": "logs_2",
    "log_level": "debug",
    "log_type": "CLI Audit Logs",
    "log_file_name": "cli_file_name",
    "rollover_file_size": 10240,
    "retrieval_method": {
      "max_num_files": 10,
      "method": "local"
    },
    "rollover_by_time": {
      "rollover_interval": "custom",
      "rollover_custom_time": 17280
    }
  }
]
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 11:16:58 GMT
Content-type: application/json
Content-Length: 481
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "res_data":
  {
    "add_failure":
    [
    ],
    "add_success":
    [
    {
      "rollover_file_size": 10240,
      "log_name":
      "logs_2",
      "retrieval_method":
      {
        "scp_key_method":
        "auto",
        "syslog_protocol":
        "UDP",
        "scp_port": 22,
        "max_num_files": 10,
        "syslog_port": 514,
        "method": "local"
      },
      "log_level":
      "debug",
      "log_type":
      "CLI Audit Logs",
      "log_file_name":
      "cli_file_name",
      "rollover_by_time":
      {
        "rollover_interval":
        "custom",
        "rollover_custom_time": 17280
      }
    }
    ],
    "res_message":
    "Success: 1,
    Failure: 0",
    "res_code": 201
  }
}

```

ログサブスクリプションの削除

Secure Web Appliance のログサブスクリプションを削除できます。次に、構文とサポート対象の属性を示します。

概要	DELETE /wsa/api/v2.0/configure/system/log_subscriptions	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ログサブスクリプションを削除する例を示します。

サンプル リクエスト

```
DELETE /wsa/api/v2.0/configure/system/log_subscriptions
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 54
```

```
{
  "delete_all": false,
  "log_name": "logs_2"
}
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 12:45:26 GMT
Content-type: application/json
Content-Length: 102
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data":
  {
    "delete_success":
    [
      "logs_2"
    ]
  },
  "res_message":
  "Success: 1,
  Failure: 0",
  "res_code": 200
}
```

ログサブスクリプションの変更：ロールオーバー

ログサブスクリプションのロールオーバー設定を変更できます。

概要	PUT /wsa/api/v2.0/configure/system/log_subscriptions/rollover
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ログサブスクリプションのロールオーバー設定を変更する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v2.0/configure/system/log_subscriptions/rollover
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 34
{
  "log_name": "mcafee_logs"
}
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 12:51:41 GMT
Content-type: application/json
Content-Length: 109
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "res_data":
  {
    "rollover_success":
    [
      "mcafee_logs"
    ]
  },
  "res_message":
  "Success: 1,
  Failure: 0",
  "res_code": 200
}
```

取得フィールドリストのログサブスクリプションの取得

Secure Web Appliance の取得フィールドリストのログサブスクリプションを取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v2.0/configure/ system/log_subscriptions/fields
----	--

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、取得フィールドリストのログサブスクリプション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 /wsa/api/v2.0/configure/system/log_subscriptions/fields?fetch=facility_list
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 12:59:40 GMT
Content-type: application/json
Content-Length: 240
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data":
  [
    "auth",
    "authpriv",
    "console",
    "daemon",
    "ftp",
    "local0",
    "local1",
    "local2",
    "local3",
    "local4",
    "local5",
    "local6",
    "local7",
    "mail",
    "ntp",
    "security",
    "user"
  ],
  "res_message":
  "Data received successfully.",
  "res_code": 200
}
```

ログタイプのデフォルト値を取得するためのログサブスクリプションの取得

ログサブスクリプションを取得して、ログタイプのデフォルト値を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v2.0/configure/system/log_subscriptions/defaults	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ログタイプのデフォルト値を取得するためにログサブスクリプション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 /wsa/api/v2.0/configure/system/log_subscriptions/defaults?log_type=Audit%20Logs
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 13:14:45 GMT
Content-type: application/json
Content-Length: 460
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "res_data":
  {
    "fetch_success":
    [
      {
        "log_style":
        "apache",
        "rollover_file_size": 10485760,
        "retrieval_method":
        {
          "scp_key_method":
          "auto",
          "syslog_facility":
          "user",
```

```

        "syslog_protocol":
        "UDP",
        "scp_port": 22,
        "max_num_files": 10,
        "syslog_port": 514,
        "method": "local"
    },
    "log_level":
    "information",
    "log_type":
    "Audit Logs",
    "log_file_name":
    "audit_log",
    "rollover_by_time":
    {
        "rollover_interval":
        "none"
    }
    }
    ],
    },
    "res_message":
    "Success: 1,
    Failure: 0",
    "res_code":
    200
}

```

ログサブスクリプション（非匿名化）の追加

ログサブスクリプション（非匿名化）を追加できます。

概要	POST /wsa/api/v2.0/configure/system/log_subscriptions/deanonymization	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、非匿名化のログサブスクリプションを追加する例を示します。

サンプル リクエスト

```

POST /wsa/api/v2.0/configure/system/log_subscriptions/deanonymization
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Content-Length: 688
Expect: 100-continue
Content-Type: multipart/form-data; boundary=-----7786918e29034048

```

```
--header 'Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz' \
--form 'log_name="accesslogs"' \
--form 'passphrase="Agt@1111"' \
--form 'encrypted_content="encrypted_text"' \
--form 'paste_encrypted_text="\H/6VZtZeUccgwRWM1Ty3MVz8ijfKs/JT2HEEobmKyB0=,
H/6VZtZeUccgwRWM1Ty3MVz8ijfKs/JT2HEEobmKyB0=\'' \
--form 'download_as_file="false"'
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 13:52:10 GMT
Content-type: application/json
Content-Length: 230
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "res_data":
  {
    "deanonymized_list":
    [
      [
        "H/6VZtZeUccgwRWM1Ty3MVz8ijfKs/JT2HEEobmKyB0=",
        "10.10.57.34"
      ],
      [
        "H/6VZtZeUccgwRWM1Ty3MVz8ijfKs/JT2HEEobmKyB0=",
        "10.10.57.34"
      ]
    ],
    "res_message":
    "Data received successfully.",
    "res_code": 201
  }
}
```

ヘッダーベース認証

ここでは、次の内容について説明します。

- [ヘッダーベース認証の取得](#)
- [ヘッダーベース認証の変更](#)

ヘッダーベース認証の詳細の取得

Secure Web Appliance で設定されたヘッダーベース認証の詳細を取得できます。

概要	GET /wsa/api/v3.0/network/xauth_header_setting
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ヘッダーベースの認証の詳細を有効にする例を示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/network/xauth_header_setting
HTTP/1.1
```

サンプル応答

```
Status Code: 200 OK
access-control-allow-credentials: true
access-control-allow-headers: content-type, jwttoken, mid, h, email
access-control-allow-methods: GET, POST, DELETE, PUT, OPTIONS
access-control-allow-origin: *
access-control-expose-headers: Content-Disposition, jwtToken
connection: close
content-length: 329
content-type: application/json
```

```
{
  "xauth_header_setting": {
    {
      "xauth_std_user": {"text_format": "ASCII", "Binary_encoding": "No Encoding"},
      "xauth_std_group": {"text_format": "ASCII", "Binary_encoding": "No Encoding"},
      "xauth_use_group_header": "disable",
      "xauth_header_mode": "standard",
      "xauth_retain_auth_egress": "disable",
      "xauth_header_based_auth": "enable"
    }
  }
}
```

異なるパラメータのヘッダーベース認証の設定

例

次に、ヘッダーベース認証の設定に関連するパラメータのリストを設定する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/network/xauth_header_setting
HTTP/1.1
```

```
{
  "xauth_header_based_auth" : "enable",
  "xauth_use_group_header" : "enable",
  "xauth_retain_auth_egress" : "enable",
  "xauth_header_mode": "standard",
  "xauth_std_user" : {"text_format": "UTF8", "Binary_encoding": "Base64"},
  "xauth_std_group" : {"text_format": "UTF8", "Binary_encoding": "Base64"}
}
```

サンプル応答

```
Status Code: 204 No Content
access-control-allow-credentials: true
access-control-allow-headers: content-type, jwttoken, mid, h, email
access-control-allow-methods: GET, POST, DELETE, PUT, OPTIONS
access-control-allow-origin: *
access-control-expose-headers: Content-Disposition, jwtToken
connection: close
content-length: 3
content-type: application/json
```

ヘッダーベース認証の詳細の変更

ヘッダーベースの認証の詳細を変更できます。

概要	PUT /wsa/api/v3.0/network/xauth_header_setting	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ヘッダーベースの認証設定を変更する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/network/xauth_header_setting
HTTP/1.1
{
  "xauth_header_based_auth": "enable",
  "xauth_use_group_header": "enable",
  "xauth_retain_auth_egress": "enable",
  "xauth_header_mode": "custom",
  "xauth_custom_user": { "name": "user", "text_format": "ASCII", "Binary_encoding": "No Encoding" },
  "xauth_custom_group": { "name": "group", "text_format": "ASCII", "Binary_encoding": "No Encoding" }
}
```

サンプル応答

```
Status Code: 204 No Content
access-control-allow-credentials: true
access-control-allow-headers: content-type, jwttoken, mid, h, email
access-control-allow-methods: GET, POST, DELETE, PUT, OPTIONS
access-control-allow-origin: *
access-control-expose-headers: Content-Disposition, jwtToken
connection: close
content-length: 3
content-type: application/json
```

例

次に、ヘッダーベースの認証の詳細を有効にする例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/network/xauth_header_setting
HTTP/1.1
{
  "xauth_header_based_auth": "enable"
}
```

サンプル応答

```
Status Code: 204 No Content
access-control-allow-credentials: true
access-control-allow-headers: content-type, jwttoken, mid, h, email
access-control-allow-methods: GET, POST, DELETE, PUT, OPTIONS
access-control-allow-origin: *
access-control-expose-headers: Content-Disposition, jwtToken
connection: close
content-length: 3
content-type: application/json
```

例

次に、NTP 認証をディセーブルにする例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/network/xauth_header_setting
HTTP/1.1
{
  "xauth_header_based_auth": "disable"
}
```

サンプル応答

```
Status Code: 204 No Content
access-control-allow-credentials: true
access-control-allow-headers: content-type, jwttoken, mid, h, email
access-control-allow-methods: GET, POST, DELETE, PUT, OPTIONS
access-control-allow-origin: *
access-control-expose-headers: Content-Disposition, jwtToken
connection: close
content-length: 3
content-type: application/json
```

要求ヘッダー書き換えプロファイル

ここでは、次の内容について説明します。

- [要求ヘッダー書き換えの取得](#)
- [要求ヘッダー書き換えの変更](#)
- [要求ヘッダー書き換えの追加](#)
- [要求ヘッダー書き換えの削除](#)

要求ヘッダー書き換えの詳細の取得

Secure Web Appliance で設定された要求ヘッダープロファイルと X-Authenticated ヘッダーのグローバル設定を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/web_security/http_rewrite_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

この例では、要求ヘッダープロファイルと X-Authenticated ヘッダーのグローバル設定を取得するクエリを示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/web_security/http_rewrite_profiles
HTTP/1.1
Host: wsa.example.com:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Wed, 17 Mar 2021 11:38:22 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 533
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true

{
  "global_settings": {
    "delimiter_for_groups": ",",
    "rewrite_format_for_user": "$authMechanism://$domainName/$userName",
    "rewrite_format_for_groups": "$authMechanism://$domainName/$groupName"
  },
  "http_rewrite_profiles": [
    {
      "headers": [
        {
          "header_value": "Username-($ReqMeta[X-Authenticated-User])",
          "text_format": "ASCII",
          "header_name": "X-Authenticated-User",
          "binary_encoding": "No Encoding"
        },
        {
          "header_value": "1.2.3.4",
          "text_format": "ASCII",
          "header_name": "X-Client-IP",

```

```

        "binary_encoding": "No Encoding"
    }
},
"profile_name": "RHR"
}
]
}

```

要求ヘッダー書き換えの詳細の変更

要求ヘッダー書き換えプロファイルと X-Authenticated ヘッダーのグローバル設定を変更できます。

概要	PUT /wsa/api/v3.0/web_security/http_rewrite_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、要求ヘッダーの書き換えの詳細を変更する例を示します。

サンプル リクエスト

```

PUT /wsa/api/v3.0/web_security/http_rewrite_profiles
HTTP/1.1
Host: wsa.example.com:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
Content-Type: text/plain
Content-Length: 1347

```

```

{
  "http_rewrite_profiles": [
    {
      "profile_name": "Profile 4",
      "new_profile_name": "Updated Profile",
      "headers": [
        {
          "header_name": "Header1",
          "header_value": "Value1",
          "text_format": "ASCII",
          "binary_encoding": "No Encoding"
        },
        {
          "header_name": "Header2",
          "header_value": "Value2",
          "text_format": "ASCII",
          "binary_encoding": "Base64"
        },
        {
          "header_name": "Header3",
          "header_value": "val",

```

```

        "text_format": "UTF-8",
        "binary_encoding": "No Encoding"
    },
    {
        "header_name": "Header4",
        "header_value": "val",
        "text_format": "UTF-8",
        "binary_encoding": "Base64"
    }
]
},
"global_settings": {
    "rewrite_format_for_user": "$authMechanism:\\$domainName\\$userName",
    "rewrite_format_for_groups": "$authMechanism:\\$domainName\\$groupName",
    "delimiter_for_groups": ":"
}
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Wed, 17 Mar 2021 11:38:22 GMT
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true

```

要求ヘッダー書き換えプロファイルの追加

要求ヘッダー書き換えプロファイルのリストを作成し、X-Authenticatedヘッダーのグローバル設定を更新できます。

概要	POST /wsa/api/v3.0/web_security/http_rewrite_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、要求ヘッダー書き換えプロファイルを作成し、X-Authenticatedヘッダーのグローバル設定を更新する方法の例を示します。

サンプル リクエスト

```

POST /wsa/api/v3.0/web_security/http_rewrite_profiles
HTTP/1.1
Host: wsa.example.com:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
Content-Type: application/json

```

```

Content-Length: 1295

{
  "http_rewrite_profiles": [
    {
      "profile_name": "Profile 4",
      "headers": [
        {
          "header_name": "Header1",
          "header_value": "Value1",
          "text_format": "ASCII",
          "binary_encoding": "No Encoding"
        },
        {
          "header_name": "Header2",
          "header_value": "Value2",
          "text_format": "ASCII",
          "binary_encoding": "Base64"
        },
        {
          "header_name": "Header3",
          "header_value": "val",
          "text_format": "UTF-8",
          "binary_encoding": "No Encoding"
        },
        {
          "header_name": "Header4",
          "header_value": "val",
          "text_format": "UTF-8",
          "binary_encoding": "Base64"
        }
      ]
    }
  ],
  "global_settings": {
    "rewrite_format_for_user": "$authMechanism:\\$domainName\\$userName",
    "rewrite_format_for_groups": "$authMechanism:\\$domainName\\$groupName",
    "delimiter_for_groups": ":"
  }
}

```

サンプル応答

```

HTTP/1.1 204 No Content
Date: Wed, 17 Mar 2021 11:38:22 GMT
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true

```

要求ヘッダー書き換えプロファイルの削除

profile_name を使用して要求ヘッダー書き換えプロファイルを削除できます。また、alternate_profile_name を使用して、アクセスポリシーで置き換える代替プロファイルを選択できます。次に、構文とサポート対象の属性を示します。

概要	DELETE /wsa/api/v3.0/web_security/http_rewrite_profiles?alternate_profile_name=None&profile_name=RHR
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、要求ヘッダー書き換えプロファイルを削除する例を示します。

サンプル リクエスト

```
DELETE
/wsa/api/v3.0/web_security/http_rewrite_profiles?alternate_profile_name=None&profile_name=RHR

HTTP/1.1
Host: wsa.example.com:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 204 No Content
Date: Wed, 17 Mar 2021 11:38:22 GMT
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
```

スマート ソフトウェア ライセンス

ここでは、次の内容について説明します。

- [スマート ソフトウェア ライセンスの取得 \(113 ページ\)](#)
- [スマート ソフトウェア ライセンスの変更 \(116 ページ\)](#)
- [スマート ライセンス エージェントのステータスの取得 \(118 ページ\)](#)
- [スマート ライセンス エージェントのステータスの変更 \(119 ページ\)](#)
- [スマート ソフトウェア ライセンスのステータスの取得 \(119 ページ\)](#)
- [スマート ソフトウェア ライセンスのステータスの変更 \(120 ページ\)](#)

スマート ソフトウェア ライセンスの取得

ライセンス名と認証ステータスが含まれている、ライセンスの詳細のリストを取得できます。

いずれかのライセンスの認証ステータスが [コンプライアンス違反 (Out of Compliance)] の場合、猶予期間が返されます。

概要	GET wsa/api/v3.0/system_admin/sl_licenses
----	---

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ライセンス名と認証ステータスが含まれている、ライセンスの詳細のリストを取得する方法の例を示します。

サンプルリクエスト 1

```
GET wsa/api/v3.0/system_admin/sl_licenses
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答 1

```
[
  {
    "license_name": "Secure Web Appliance Cisco Web Usage Controls",
    "auth_status": "In Compliance"
  },
  {
    "license_name": "Secure Web Appliance Anti-Virus Webroot",
    "auth_status": "In Compliance"
  },
  {
    "license_name": "Secure Web Appliance L4 Traffic Monitor",
    "auth_status": "In Compliance"
  },
  {
    "license_name": "Secure Web Appliance Cisco AnyConnect SM for AnyConnect",
    "auth_status": "In Compliance"
  },
  {
    "license_name": "Secure Web Appliance Malware Analytics Reputation",
    "auth_status": "Not requested"
  },
  {
    "license_name": "Secure Web Appliance Anti-Virus Sophos",
    "auth_status": "In Compliance"
  },
  {
    "license_name": "Secure Web Appliance Web Reputation Filters",
    "auth_status": "Not requested"
  },
  {
    "license_name": "Secure Web Appliance Malware Analytics",
    "auth_status": "Not requested"
  },
  {
    "license_name": "Secure Web Appliance Anti-Virus McAfee",
    "auth_status": "In Compliance"
  },
]
```

```

    {
      "license_name": "Secure Web Appliance Web Proxy and DVS Engine",
      "auth_status": "In Compliance"
    },
    {
      "license_name": "Secure Web Appliance HTTPS Decryption",
      "auth_status": "In Compliance"
    }
  ]

```

サンプル応答 2

```

[
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Cisco Web Usage Controls",
    "auth_status": "In Compliance"
  },
  {
    "grace_period": "Expired",
    "license_name": "Secure Web Appliance Anti-Virus Webroot",
    "auth_status": "Out Of Compliance"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance L4 Traffic Monitor",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Cisco AnyConnect SM for AnyConnect",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Malware Analytics Reputation",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Anti-Virus Sophos",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Web Reputation Filters",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Malware Analytics",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Anti-Virus McAfee",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",
    "license_name": "Secure Web Appliance Web Proxy and DVS Engine",
    "auth_status": "Not requested"
  },
  {
    "grace_period": "N/A",

```

```

        "license_name": "Secure Web Appliance HTTPS Decryption",
        "auth_status": "Not requested"
    }
]

```

スマートソフトウェアライセンスの変更

ライセンス名と認証ステータスが含まれている、ライセンスの詳細リストを変更できます。

いずれかのライセンスの認証ステータスが [コンプライアンス違反 (Out of Compliance)] の場合、猶予期間が返されます。

概要	PUT wsa/api/v3.0/system_admin/sl_licenses	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ライセンス名と認証ステータスが含まれている、ライセンスの詳細のリストを変更する方法の例を示します。

サンプルリクエスト 1

```

PUT /wsa/api/v3.0/system_admin/sl_licenses
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk

```

Body:

```

{
  "request": ["Secure Web Appliance L4 Traffic Monitor", "Secure Web Appliance Malware Analytics"],
  "release": ["Secure Web Appliance Cisco AnyConnect SM for AnyConnect", "Secure Web Appliance HTTPS Decryption"]
}

```

Sample Response 1: 202 Accepted

```

{
  "message": "The request or release for the licenses is in progress."
}

```

サンプルリクエスト 2

```

PUT /wsa/api/v3.0/system_admin/sl_licenses
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk

```

Body:

```

{
  "request": [],
  "release": ["Secure Web Appliance Malware Analytics", "Secure Web Appliance Malware Analytics"]
}

```

```

}

Sample Response 2: 400
{
  "error": {
    "message": "Invalid request: License name 'Secure Web Appliance Malware Analytics'
is repeated in ['release'].",
    "code": "400",
    "explanation": "400 = Bad request syntax or unsupported method."
  }
}

```

サンプルリクエスト 3

```

PUT /wsa/api/v3.0/system_admin/sl_licenses
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk

```

Body:

```

{
  "request": ["Secure Web Appliance Malware Analytics"],
  "release": ["Secure Web Appliance Malware Analytics"]
}

```

```

Sample Response 3: 400
{
  "error": {
    "message": "Invalid request: License name 'Secure Web Appliance Malware Analytics'
is found in both ['release'] and ['request'].",
    "code": "400",
    "explanation": "400 = Bad request syntax or unsupported method."
  }
}

```

サンプルリクエスト 4

```

PUT /wsa/api/v3.0/system_admin/sl_licenses
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk

```

Body:

```

{
  "request": ["Secure Web Appliance L4 Traffic Monitor", "Secure Web Appliance Malware
Analytics"]
  "release": ["invalid name"]
}

```

```

Sample Response 4: 400
{
  "error": {
    "message": "Invalid request[release][0]. 'invalid name' should be one of these:
['Secure Web Appliance Web Reputation Filters', 'Secure Web Appliance Malware Analytics
Reputation', 'Secure Web Appliance Anti-Virus McAfee', 'Secure Web Appliance Web Proxy
and DVS Engine', 'Secure Web Appliance Cisco Web Usage Controls', 'Secure Web Appliance
Anti-Virus Webroot', 'Secure Web Appliance L4 Traffic Monitor', 'Secure Web Appliance
Cisco AnyConnect SM for AnyConnect', 'Secure Web Appliance Anti-Virus Sophos', 'Secure
Web Appliance Malware Analytics', 'Secure Web Appliance HTTPs Decryption'].",
    "code": "400",
    "explanation": "400 = Bad request syntax or unsupported method."
  }
}

```

サンプルリクエスト 5

```

PUT /wsa/api/v3.0/system_admin/sl_licenses
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk

Body:
{
  "request": ["Secure Web Appliance L4 Traffic Monitor", "Secure Web Appliance Malware Analytics"],
  "release": ["Secure Web Appliance Web Reputation Filters"]
}

Sample Response 5: 400
{
  "error": {
    "message": "Cannot release license 'Secure Web Appliance Web Reputation Filters' as the current authorization status of the license is 'Not requested'.",
    "code": "400",
    "explanation": "400 = Bad request syntax or unsupported method."
  }
}

```

スマート ライセンス エージェントのステータスの取得

ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細を取得できます。

概要	GET wsa/api/v3.0/system_admin/smart_agent_status	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細を取得する方法の例を示します。

サンプル リクエスト

```

GET wsa/api/v3.0/system_admin/smart_agent_status HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz

```

サンプル応答

```

{
  "file_type": "Smart License Agent",
  "version": "3.1.4",
  "new_update": "Failed to fetch manifest",
  "last_update": "Never updated"
}

```

スマート ライセンス エージェントのステータスの変更

ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細を変更できます。

概要	PUT wsa/api/v3.0/system_admin/smart_agent_status	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細を変更する方法の例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/system_admin/smart_agent_status HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 202
```

スマート ソフトウェア ライセンスのステータスの取得

ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細のリストを取得できます。

概要	GET wsa/api/v3.0/system_admin/smart_software_licensing_status HTTP/1.1	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細のリストを取得する方法の例を示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/system_admin/smart_software_licensing_status HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
```

サンプル応答

```
{
  "smart_account_name": "InternalTestDemoAccount9.cisco.com",
  "virtual_account_name": "WSA2",
  "registration_last_renew": "SUCCEEDED on 29 Sep 2021 06:08",
  "last_auth_renewal_attempt_status": "SUCCEEDED on 29 Sep 2021 06:08",
  "transport_url": "https://smartreceiver.cisco.com/licservice/license",
  "transport_mode": "direct",
  "test_interface": "Management",
  "eval_period": "Not In Use",
  "eval_period_remaining": "90 days",
  "smart_lic_status": "AUTHORIZED",
  "authorization_status": "Authorized ( 29 Sep 2021 06:08 ) Authorization Expires on:
( 28 Dec 2021 06:04 )",
  "product_instance_name": "wsa353.cs1",
  "registration_status": "Registered ( 29 Sep 2021 06:08 ) Registration Expires on:
( 29 Sep 2022 06:04 )"
}
```

スマートソフトウェアライセンスのステータスの変更

ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細リストを変更できます。

概要	PUT wsa/api/v3.0/system_admin/smart_software_licensing_status	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ステータスの有効化または無効化や、登録ステータスなどの、シスコ スマート ソフトウェア ライセンスの設定の詳細リストを変更する方法の例を示します。

サンプルリクエスト 1

```
{
  "smart_license_status": "enable"
}
```

サンプルリクエスト 2



```
{ "registration_token":  
"ZfE.....z0A",  
  "action": "register", "test_interface": "Data" } { "action": "deregister" } {  
  "transport_mode": "transport_gateway", "transport_url": "https://www.google.com" } {  
  "action": "renew auth" } { "action": "renew registration" }
```

```
{
  "action": "deregister"
}
```

```
{
  "transport_mode": "transport_gateway",
  "transport_url": "https://www.google.com"
}
```

```
{
  "action": "renew_auth"
}
```

```
{
  "action": "renew_registration"
}
```

- エンドユーザーライセンス契約の詳細の取得 (121 ページ)
- システム セットアップ ウィザードの設定の変更 (123 ページ)

エンドユーザーライセンス契約の詳細を取得できます。



(注) システムセットアップウィザードをセットアップするPUT リクエストを実行する前に、EULA 契約を読む必要があります。

概要	GET wsa/api/v3.0/system_admin/cisco_end_user_license_agreement
----	--

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、エンドユーザーライセンス契約の詳細を取得する方法の例を示します。

サンプルリクエスト 1

```
PUT /wsa/api/v3.0/system_admin/system_setup_wizard
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

```
{
  "cisco_license_agreement": "accept",
  "appliance_mode": "standard",
  "system_settings": {
    "hostname": "dut058.perf8",
    "dns_servers": {
      "dns_choice": "self",
      "user_dns": [
        "192.168.0.252"
      ]
    },
    "ntp_server": {
      "query_interval_time": 23434,
      "sync_up_delay_ms": 500,
      "server_name": "time.sco.cisco.com",
      "server_auth": {
        "status": "enable",
        "key_id": 123,
        "key_val": "MTIzNA==",
        "key_type": "sha1"
      }
    },
    "timezone": {
      "region": "Europe"
    }
  },
  "network_context": {
    "other_proxy": "no"
  },
  "network_interface": {
    "m1": {
      "management_only": "no",
      "ipv4_address_netmask": "10.10.194.68/24",
      "hostname": "dut058.perf8"
    }
  },
  "network_l4tm": {
    "wiring_type": "duplex"
  },
  "network_routes": {
```

```

      "management": {
        "default_gateway": "10.10.194.1"
      }
    },
    "transparent_connection": {
      "redirection_device": "wccp_v2_router",
      "wccp_v2_router": {
        "standard_service_id": {
          "status": "disable"
        }
      }
    },
    "network_admin": {
      "passphrase": "Q21zY28xMjMk",
      "mail_to_addrs": ["sandhgan@cisco.com"],
      "autosupport": "enable",
      "network_participation": {
        "status": "enable",
        "participation_level": "standard"
      }
    },
    "network_security": {
      "global_policy_default_action": "monitor",
      "l4_traffic_monitor": "monitor",
      "cisco_data_security_filtering": "enable"
    }
  }
}

```

サンプル応答 1

204 No-content

サンプルリクエスト 2

```

PUT /wsa/api/v3.0/system_admin/config_backup_server
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q21zY28xMjMk

```

```

{
  "network_admin": {
    "passphrase": "Q21zY28xMjMk",
    "mail_to_addrs": "sandhgan@cisco.com",
  }
}

```

サンプル応答 2

204 No-content

システム セットアップ ウィザードの設定の変更

システム セットアップ ウィザードの設定でオブジェクトを変更できます。

概要	PUT wsa/api/v3.0/system_admin/system_setup_wizard	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、システムセットアップウィザードの設定でオブジェクトを変更する方法の例を示します。

サンプルリクエスト 1

```
PUT /wsa/api/v3.0/system_admin/system_setup_wizard
```

```
Host: dut058.perf8:4431
```

```
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
```

```
{
  "cisco_license_agreement": "accept",
  "appliance_mode": "standard",
  "system_settings": {
    "hostname": "dut058.perf8",
    "dns_servers": {
      "dns_choice": "self",
      "user_dns": [
        "192.168.0.252"
      ]
    },
    "ntp_server": {
      "query_interval_time": 23434,
      "sync_up_delay_ms": 500,
      "server_name": "time.sco.cisco.com",
      "server_auth": {
        "status": "enable",
        "key_id": 123,
        "key_val": "MTIzNA==",
        "key_type": "sha1"
      }
    },
    "timezone": {
      "region": "Europe"
    }
  },
  "network_context": {
    "other_proxy": "no"
  },
  "network_interface": {
    "m1": {
      "management_only": "no",
      "ipv4_address_netmask": "10.10.194.68/24",
      "hostname": "dut058.perf8"
    }
  },
  "network_l4tm": {
    "wiring_type": "duplex"
  },
  "network_routes": {
    "management": {
      "default_gateway": "10.10.194.1"
    }
  },
  "transparent_connection": {
    "redirection_device": "wccp_v2_router",
    "wccp_v2_router": {
      "standard_service_id": {
```

```

        "status": "disable"
    }
}
},
"network_admin": {
    "passphrase": "Q21zY28xMjMk",
    "mail_to_addrs": ["sandhgan@cisco.com"],
    "autosupport": "enable",
    "network_participation": {
        "status": "enable",
        "participation_level": "standard"
    }
},
"network_security": {
    "global_policy_default_action": "monitor",
    "l4_traffic_monitor": "monitor",
    "cisco_data_security_filtering": "enable"
}
}

```

サンプル応答 1

204 No-content

サンプルリクエスト 2

```

PUT /wsa/api/v3.0/system_admin/config_backup_server
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q21zY28xMjMk

```

```

{
    "network_admin": {
        "passphrase": "Q21zY28xMjMk",
        "mail_to_addrs": "sandhgan@cisco.com",
    }
}

```

サンプル応答 2

204 No-content

復号ポリシー

ここでは、次の内容について説明します。

- [復号ポリシーの取得](#) (125 ページ)
- [復号ポリシーの変更](#) (128 ページ)
- [復号ポリシーの追加](#) (129 ページ)
- [復号ポリシーの削除](#) (132 ページ)

復号ポリシーの取得

使用可能な復号ポリシーとその設定を取得できます。

概要	GET wsa/api/v3.0/web_security/decryption_policies
----	---

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、使用可能な復号ポリシーとその設定を取得する方法の例を示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/web_security/decryption_policies?policy_names=DP1 HTTP/1.1
Host: dut058.perf8:6443
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
{
  "decryption_policies": [
    {
      "policy_status": "enable",
      "policy_name": "DP1",
      "policy_description": "",
      "policy_order": 2,
      "policy_expiry": "",
      "membership": {
        "identification_profiles": [
          {
            "global_identification_profile": {
              "auth": "No Authentication"
            }
          }
        ]
      },
      "url_filtering": {
        "custom_cats": {
          "use_global": [
            "GM Global External No Auth Custom URL",
            "Block Netflix",
            "Secure Admin Workstation Allow List",
            "GM Global External Office 365 No Auth",
            "MFG Allow Custom URL",
            "Internet DENY Allow List",
            "Mobile Link GME Ogrinal Custom URL",
            "ESRS Server No Auth GME Orginal Custom URL",
            "CiscoEURservers No Auth GME Oiginal Custom URL"
          ]
        },
        "predefined_cats": {
          "use_global": [
            "Adult",
            "Advertisements",
            "Alcohol",
            "Arts",
            "Astrology",
            "Auctions",

```

"Business and Industry",
"Chat and Instant Messaging",
"Cheating and Plagiarism",
"Child Abuse Content",
"Computer Security",
"Computers and Internet",
"DIY Projects",
"Dating",
"Digital Postcards",
"Dining and Drinking",
"Dynamic and Residential",
"Education",
"Entertainment",
"Extreme",
"Fashion",
"File Transfer Services",
"Filter Avoidance",
"Finance",
"Freeware and Shareware",
"Gambling",
"Games",
"Government and Law",
"Hacking",
"Hate Speech",
"Health and Nutrition",
"Humor",
"Hunting",
"Illegal Activities",
"Illegal Downloads",
"Illegal Drugs",
"Infrastructure and Content Delivery Networks",
"Internet Telephony",
"Job Search",
"Lingerie and Swimsuits",
"Lotteries",
"Military",
"Mobile Phones",
"Nature",
"News",
"Non-governmental Organizations",
"Non-sexual Nudity",
"Online Communities",
"Online Meetings",
"Online Storage and Backup",
"Online Trading",
"Organizational Email",
"Paranormal",
"Parked Domains",
"Peer File Transfer",
"Personal Sites",
"Personal VPN",
"Photo Search and Images",
"Politics",
"Pornography",
"Professional Networking",
"Real Estate",
"Reference",
"Religion",
"SaaS and B2B",
"Safe for Kids",
"Science and Technology",
"Search Engines and Portals",
"Sex Education",
"Shopping",

```

        "Social Networking",
        "Social Science",
        "Society and Culture",
        "Software Updates",
        "Sports and Recreation",
        "Streaming Audio",
        "Streaming Video",
        "Tobacco",
        "Transportation",
        "Travel",
        "Weapons",
        "Web Hosting",
        "Web Page Translation",
        "Web-based Email"
    ],
    },
    "state": "custom",
    "update_cats_action": "use_global",
    "uncategorized_url": "use_global"
},
"web_reputation": {
    "state": "custom",
    "score": {
        "drop": [
            "-10.0",
            "10.0"
        ],
        "decrypt": [],
        "pass_through": []
    },
    "wbrs_no_score_action": "monitor"
},
"default_action": "use_global"
}
]
}

```

復号ポリシーの変更

使用可能な復号ポリシーとその設定を変更できます。

概要	PUT wsa/api/v3.0/web_security/decryption_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、使用可能な復号ポリシーとその設定を変更する方法の例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/web_security/decryption_policies HTTP/1.1
Host: dut058.perf8:6443
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 1151
```

```
{
  "decryption_policies": [
    {
      "policy_status": "enable",
      "policy_name": "DP1",
      "policy_description": "",
      "policy_order": 1,
      "policy_expiry": "12/2/2024 22:00",
      "membership": {
        "identification_profiles": [
          {
            "profile_name": "AllowISEIdentity",
            "auth": "No Authentication"
          }
        ]
      },
      "web_reputation": {
        "state": "custom",
        "score": {
          "drop": [
            "-10.0",
            "5.0"
          ],
          "pass_through": [
            "7.0",
            "10.0"
          ]
        },
        "wbrs_no_score_action": "drop"
      },
      "default_action": "pass_through"
    }
  ]
}
```

サンプル応答

204 (No-content)

復号ポリシーの追加

使用可能な復号ポリシーとその設定を追加できます。

概要	POST wsa/api/v3.0/web_security/decryption_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、使用可能な復号ポリシーとその設定を追加する方法の例を示します。

サンプル リクエスト

```
POST /wsa/api/v3.0/configure/web_security/decryption_policies HTTP/1.1
Host: dut058.perf8:6443
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Content-Type: text/plain
Content-Length: 1518
```

```
{
  "decryption_policies": [
    {
      "policy_status": "enable",
      "policy_name": "DP1",
      "policy_description": "",
      "policy_order": 1,
      "policy_expiry": "12/2/2024 22:00",
      "membership": {
        "identification_profiles": [
          {
            "profile_name": "AllowISEIdentity",
            "auth": "No Authentication"
          }
        ]
      }
    },
    {
      "url_filtering": {
        "custom_cats": {
          "use_global": [
            "GM Global External No Auth Custom URL",
            "Block Netflix",
            "Secure Admin Workstation Allow List",
            "GM Global External Office 365 No Auth",
            "MFG Allow Custom URL",
            "Internet DENY Allow List",
            "Mobile Link GME Ogrinal Custom URL",
            "ESRS Server No Auth GME Orginal Custom URL",
            "CiscoEURservers No Auth GME Oginal Custom URL"
          ]
        }
      },
      "predefined_cats": {
        "use_global": [
          "Adult",
          "Advertisements",
          "Alcohol",
          "Arts",
          "Astrology",
          "Auctions",
          "Business and Industry",
          "Chat and Instant Messaging",
          "Cheating and Plagiarism",
          "Child Abuse Content",
          "Computer Security",
          "Computers and Internet",
          "DIY Projects",
          "Dating",
          "Digital Postcards",
          "Dining and Drinking",
          "Dynamic and Residential",
          "Education",
          "Entertainment",
          "Extreme",

```

```
"Fashion",
"File Transfer Services",
"Filter Avoidance",
"Finance",
"Freeware and Shareware",
"Gambling",
"Games",
"Government and Law",
"Hacking",
"Hate Speech",
"Health and Nutrition",
"Humor",
"Hunting",
"Illegal Activities",
"Illegal Downloads",
"Illegal Drugs",
"Infrastructure and Content Delivery Networks",
"Internet Telephony",
"Job Search",
"Lingerie and Swimsuits",
"Lotteries",
"Military",
"Mobile Phones",
"Nature",
"News",
"Non-governmental Organizations",
"Non-sexual Nudity",
"Online Communities",
"Online Meetings",
"Online Storage and Backup",
"Online Trading",
"Organizational Email",
"Paranormal",
"Parked Domains",
"Peer File Transfer",
"Personal Sites",
"Personal VPN",
"Photo Search and Images",
"Politics",
"Pornography",
"Professional Networking",
"Real Estate",
"Reference",
"Religion",
"SaaS and B2B",
"Safe for Kids",
"Science and Technology",
"Search Engines and Portals",
"Sex Education",
"Shopping",
"Social Networking",
"Social Science",
"Society and Culture",
"Software Updates",
"Sports and Recreation",
"Streaming Audio",
"Streaming Video",
"Tobacco",
"Transportation",
"Travel",
"Weapons",
"Web Hosting",
"Web Page Translation",
"Web-based Email"
```

```

    ],
    "state": "custom",
    "update_cats_action": "use_global",
    "uncategorized_url": "use_global"
  },
  "web_reputation": {
    "state": "custom",
    "score": {
      "drop": [
        "-10.0",
        "10.0"
      ],
      "decrypt": [],
      "pass_through": []
    },
    "wbrs_no_score_action": "monitor"
  },
  "default_action": "use_global"
}
]
}

```

サンプル応答

204 (No-content)

復号ポリシーの削除

使用可能な復号ポリシーとその設定を削除できます。

概要	DELETE wsa/api/v3.0/web_security/decryption_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、使用可能な復号ポリシーとその設定を削除する方法の例を示します。

サンプル リクエスト

```

DELETE /wsa/api/v3.0/web_security/decryption_policies?policy_names=DP1,DP2,DP3 HTTP/1.1
Host: dut058.perf8:6443
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz

```

サンプル応答

```

{
  "success_list": [
    {
      "status": 200,
      "message": "success",
    }
  ]
}

```

```

        "policy_name": "DP1"
      },
      {
        "status": 200,
        "message": "success",
        "policy_name": "DP2"
      }
    ],
    "failure_list": [
      {
        "status": 404,
        "message": "policy name does not exist.",
        "policy_name": "DP3"
      }
    ],
    "success_count": 2,
    "failure_count": 1
  }
}

```

ルーティングポリシー

ここでは、次の内容について説明します。

- [ルーティングポリシーの取得](#) (133 ページ)
- [ルーティングポリシーの変更](#) (134 ページ)
- [ルーティングポリシーの追加](#) (135 ページ)
- [ルーティングポリシーの削除](#) (136 ページ)

ルーティングポリシーの取得

返されるポリシー名の照合によりルーティングポリシーのリストを取得できます。

概要	GET wsa/api/v3.0/web_security/routing_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、返されるポリシー名の照合によりルーティングポリシーのリストを取得する方法の例を示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/web_security/routing_policies?policy_names=RP1 HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW5DaXNjbzEyMyQ=
```

サンプル応答

```
{
  "routing_policies": [
    {
      "policy_description": "test protocol policy",
      "ip_spoofing": "Do not use IP Spoofing",
      "policy_order": 1,
      "policy_status": "enable",
      "policy_name": "RP1",
      "membership": {
        "identification_profiles": [
          {
            "global_identification_profile": {
              "auth": "No Authentication"
            }
          }
        ]
      },
      "routing_destination": {
        "upstream_proxy_group": "use_global"
      }
    }
  ]
}
```

ルーティングポリシーの変更

ルーティングポリシーとその設定ペイロードのリストを変更できます。

概要	PUT wsa/api/v3.0/web_security/routing_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ルーティングポリシーとその設定ペイロードのリストを変更する方法の例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/web_security/routing_policies HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW5DaXNjbzEyMyQ=
Content-Type: application/json
Content-Length: 621
```

```
{
  "routing_policies": [
```

```

    {
      "policy_status": "enable",
      "policy_name": "RP2",
      "policy_description": "test protocol policy",
      "policy_order": 1,
      "membership": {
        "identification_profiles": [
          {
            "profile_name": "ID1",
            "auth": "No Authentication"
          }
        ]
      },
      "ip_spoofing": "IP1",
      "routing_destination": {
        "upstream_proxy_group": "UPProxy1"
      }
    }
  ]
}

```

サンプル応答

204 (No-content)

ルーティングポリシーの追加

ルーティングポリシーとその設定ペイロードのリストを追加できます。

概要	POST wsa/api/v3.0/web_security/routing_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ルーティングポリシーとその設定ペイロードのリストを追加する方法の例を示します。

サンプル リクエスト

```

POST /wsa/api/v3.0/web_security/routing_policies HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW5DaXNjbzEyMyQ=
Content-Type: application/json
Content-Length: 561

```

```

{
  "routing_policies": [
    {
      "policy_status": "enable",
      "policy_name": "RP1",
      "policy_description": "test protocol policy",
      "policy_order": 1,

```

```

    "membership": {
      "identification_profiles": [
        {
          "profile_name": "global_identification_profile",
          "auth": "No Authentication"
        }
      ]
    },
    "ip_spoofing": "Do not use IP Spoofing"
  }
}

```

サンプル応答

204 (No-content)

ルーティングポリシーの削除

削除するポリシー名の照合によりルーティングポリシーのリストを削除できます。

概要	DELETE wsa/api/v3.0/web_security/routing_policies	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、削除するポリシー名の照合によりルーティングポリシーのリストを削除する方法の例を示します。

サンプル リクエスト

```

DELETE /wsa/api/v3.0/web_security/routing_policies?policy_names=RP1 HTTP/1.1
Host: dut058.perf8:6443
Authorization: Basic YWRtaW5DaXNjbzEyMyQ=

```

サンプル応答

```

{
  "success_list": [
    {
      "status": 200,
      "message": "success",
      "policy_name": "RP1"
    }
  ],
  "failure_list": [
    {
      "status": 404,
      "message": "policy name does not exist.",
      "policy_name": "RP2"
    }
  ]
}

```

```

    }
  },
  "success_count": 1,
  "failure_count": 1
}

```

IP スプーフィングプロファイル

ここでは、次の内容について説明します。

- [IP スプーフィングプロファイルの取得](#) (137 ページ)
- [IP スプーフィングプロファイルの変更](#) (138 ページ)
- [IP スプーフィングプロファイルの追加](#) (138 ページ)
- [IP スプーフィングプロファイルの削除](#) (139 ページ)

IP スプーフィングプロファイルの取得

IP スプーフィングプロファイルとその設定ペイロードのリストを取得できます。

概要	GET wsa/api/v3.0/web_security/ip_spoofing_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、IP スプーフィングプロファイルとその設定ペイロードのリストを取得する方法の例を示します。

サンプル リクエスト

```

GET /wsa/api/v3.0/web_security/ip_spoofing_profiles?profile_names=spoof2,spoof3
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk

```

サンプル応答

```

{
  "ip_spoofing_profiles": [
    {
      "profile_name": "spoof3",
      "ip_address": "1.1.1.1"
    },
    {
      "profile_name": "spoof2",
      "ip_address": "2001:420:80:1::15"
    }
  ]
}

```

```

    }
  ]
}

```

IP スプーフィングプロファイルの変更

IP スプーフィングプロファイルとその設定ペイロードのリストを変更できます。

概要	PUT wsa/api/v3.0/web_security/ip_spoofing_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、IP スプーフィングプロファイルとその設定ペイロードのリストを変更する方法の例を示します。

サンプル リクエスト

```

PUT /wsa/api/v3.0/web_security/ip_spoofing_profiles
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk

```

```

{
  "ip_spoofing_profiles": [
    {
      "profile_name": "spoof1"
    },
    {
      "profile_name": "spoof2",
      "new_profile_name": "newspoof2"
    },
    {
      "profile_name": "spoof3",
      "new_profile_name": "newspoof3",
      "ip_address": "2001:420:80:1::15"
    }
  ]
}

```

サンプル応答

```

204 (No-content)

```

IP スプーフィングプロファイルの追加

IP スプーフィングプロファイルとその設定ペイロードのリストを追加できます。

概要	POST wsa/api/v3.0/web_security/ip_spoofing_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、IP スプーフィングプロファイルとその設定ペイロードのリストを追加する方法の例を示します。

サンプル リクエスト

```
POST /wsa/api/v3.0/web_security/ip_spoofing_profiles
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
```

```
{
  "ip_spoofing_profiles": [
    {
      "profile_name": "spoof1",
      "ip_address": "1.1.1.1"
    },
    {
      "profile_name": "spoof2",
      "ip_address": "2001:420:80:1::15"
    }
  ]
}
```

サンプル応答

```
204 (No-content)
```

IP スプーフィングプロファイルの削除

IP スプーフィングプロファイルとその設定ペイロードのリストを削除できます。

概要	DELETE wsa/api/v3.0/web_security/ip_spoofing_profiles	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、IP スプーフィングプロファイルとその設定ペイロードのリストを削除する方法の例を示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/web_security/ip_spoofing_profiles
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
{
  "success_list": [
    {
      "status": 200,
      "message": "success",
      "profile_name": "spoof4"
    }
  ],
  "failure_list": [
    {
      "status": 404,
      "message": "profile_name 'spoof5' doesn't exist",
      "profile_name": "spoof5"
    }
  ],
  "success_count": 1,
  "failure_count": 1
}
```

設定ファイル

ここでは、次の内容について説明します。

- 構成ファイルの取得 (140 ページ)
- 構成ファイルの変更 (141 ページ)
- 構成ファイルの取得—バックアップ設定 (143 ページ)
- 構成ファイルの変更—バックアップ設定 (143 ページ)
- 構成ファイルの変更—リセット (145 ページ)

構成ファイルの取得

Secure Web Appliance で構成ファイルをダウンロード、保存、またはロードできます。

概要	GET wsa/api/v3.0/system_admin/configuration_file
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Secure Web Appliance で構成ファイルをダウンロード、保存、またはロードする方法の例を示します。

サンプル リクエスト

```
curl --location --request GET
'https://wsa308.cs1:4431/wsa/api/v3.0/system_admin/configuration_file?mail_to=xyz123@cisco.com'
--header 'Authorization: Basic YWRtaW46Q2lzY29AMTlz'
```

Sample Response:

```
{
  "message": "config sent to these mails: ['xyz123@cisco.com']"
}
```

構成ファイルの変更

Secure Web Appliance で構成ファイルをダウンロード、保存、またはロードできます。

概要	PUT wsa/api/v3.0/system_admin/configuration_file	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Secure Web Appliance で構成ファイルをダウンロード、保存、またはロードする方法の例を示します。

サンプル リクエスト

```
curl --location --request PUT
'https://wsa308.cs1:4431/wsa/api/v3.0/system_admin/configuration_file' --header
'Authorization: Basic YWRtaW46Q2lzY29AMTlz' --form 'action="save"'
```

サンプル応答

```
{
  "message": "Saved Successfully."
}
```

アプライアンス構成ファイルの表示

Secure Web Appliance に保存されている使用可能な構成ファイルを表示できます。

概要	GET wsa/api/v3.0/system_admin/appliance_config_files	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Secure Web Appliance に保存されている使用可能な構成ファイルを表示する方法の例を示します。

サンプル リクエスト

```
curl --location --request GET
'https://wsa308.cs1:4431/wsa/api/v3.0/system_admin/appliance_config_files' --header
'Authorization: Basic YWRtaW46Q2lzMjY2AMTIZ'
```

サンプル応答

```
{
  "appliance_config_files": [
    "EUN_DEFAULT.tar.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210623T062911-14.5.0-253.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210623T114735-14.5.0-253.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210623T114850-14.5.0-253.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T051947-14.5.0-253.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T052026-14.5.0-253.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T052309-14.5.0-253.xml",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T064846-14.5.0-275.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T091022-14.5.0-275.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T091225-14.5.0-275.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T091249-14.5.0-275.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T091451-14.5.0-275.xml.audit_bkp.gz",
    "S600V-4229463E3D1973742FFF-274CC33B68AB-20210624T091603-14.5.0-275.xml.audit_bkp",
    "config.dtd"
  ]
}
```

構成ファイルの取得—バックアップ設定

設定バックアップサーバーの現在の設定を取得できます。

概要	GET wsa/api/v3.0/system_admin/config_backup_server	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、設定バックアップサーバーの現在の設定を取得する方法の例を示します。

サンプルリクエスト 1

```
GET /wsa/api/v3.0/system_admin/config_backup_server
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答 1

```
{
  "config_backup_status": "disable"
}
```

サンプルリクエスト 2

```
GET /wsa/api/v3.0/system_admin/config_backup_server
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答 2

```
{
  "config_backup_settings": {
    "save_passphrase": false,
    "retrieval_method": "ftp_push",
    "ftp_settings": {
      "directory": "/data/db",
      "username": "sandhgan",
      "ftp_host": "dut058.perf8"
    }
  }
}
```

構成ファイルの変更—バックアップ設定

設定バックアップサーバーの現在の設定を変更できます。

概要	PUT wsa/api/v3.0/system_admin/config_backup_server
----	--

例

サンプルリクエスト 1

```
{
  "config_backup_status": "enable",
  "save_passphrase": false,
  "retrieval_method": "scp_push",
  "scp_settings": {
    "scp_host": "dut058.perf8",
    "directory": "/data",
    "username": "sandhgan",
    "host_key_checking": {
      "status": "enable",
      "key_method": "auto",
      "ssh_key": ""
    }
  }
}
```

```
{
  "SSH Key": "ssh-dss
root@dut058.perf8ssh-rsa
root@dut058.perf8"
}
```

```
{
  "config_backup_status": "enable",
  "save_passphrase": false,
  "retrieval_method": "ftp_push",
  "ftp_settings": {
    "ftp_host": "dut058.perf8",
    "directory": "/data/db",

```

```

        "username": "sandhgan",
        "passphrase": "Q21zY28xMjMk"
    }
}

```

サンプル応答 2

204 No-content

構成ファイルの変更—リセット

設定をリセットすると、ボックスの設定が工場出荷時の設定にリセットされます。構成ファイルが工場出荷時の設定に更新されます。



(注) 設定のリセットは、システムがクラスタメンバーでない場合に管理者のみが実行できます。



注意 設定をリセットすると、アプライアンスが工場出荷時の設定に戻ります（IP アドレスも含む）。以下の操作を実行する前に設定を保存することを強く推奨します。

概要	PUT wsa/api/v3.0/system_admin/configuration_file	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ボックスの設定を工場出荷時の設定にリセットする方法の例を示します。

サンプル リクエスト

```

curl --location --request PUT
'http://wsa301.cs1:6080/wsa/api/v3.0/system_admin/configuration_file' \
--header 'Authorization: Basic YWRtaW46aXJvbnBvcnQ=' \
--form 'action="reset"' \
--form 'reset_network_settings="True"'

```

サンプル応答

```

{
  "message": "All settings have been restored to the factory defaults."
}

```

認証レلم

ここでは、次の内容について説明します。

- [認証レلم設定の取得（146 ページ）](#)
- [認証レلم設定の追加（147 ページ）](#)
- [グローバル認証設定の取得（150 ページ）](#)
- [グローバル認証設定の変更（151 ページ）](#)
- [認証レلمシーケンス設定の追加（149 ページ）](#)
- [認証レلمシーケンス設定の変更（149 ページ）](#)
- [認証レلمシーケンス設定の取得（148 ページ）](#)

認証レلم設定の取得

認証レلم設定を表示および取得できます。

概要	GET wsa/api/v3.0/network/auth_realms	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、認証レلم設定を表示および取得する方法の例を示します。

サンプル リクエスト

```
curl --location --request GET
'https://wsa308.cs1:6443/wsa/api/v3.0/network/auth_realms?realm_names=ad1' --header
'Authorization: Basic YWRtaW46Q2lzY29AMTIz'
```

サンプル応答

```
{
  "auth_realms": [
    {
      "ad_account": {
        "domain_joined": false,
        "trusted_domain_lookup_enabled": true,
        "computer_account": "Computers",
        "ad_domain": "ABCD2121.COM"
      },
      "ad_server": {
```

```

        "interface": "Management",
        "servers": [
            {
                "host": "xyz234.com"
            }
        ],
        "scheme": [
            "Negotiate",
            "NTLMSSP",
            "Basic"
        ],
        "type": "AD",
        "name": "ad1"
    }
}

```

認証レلم設定の追加

認証レلم設定を表示および追加できます。

概要	POST wsa/api/v3.0/network/auth_sequences	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、認証レلم設定を表示および追加する方法の例を示します。

サンプル リクエスト

```

curl --location --request POST
'https://wsa308.csl:6443/wsa/api/v3.0/network/auth_sequences' --header 'Authorization:
Basic YWRtaW46aXJvbnBvcnQ=' --header 'Content-Type: application/json' --data-raw '{
  "auth_sequences": [
    {
      "schemes": {
        "Kerberos": [
          "myADRealm"
        ],
        "Basic": [
          "myRealm",
          "myADRealm"
        ]
      },
      "name": "myAuthSequence2"
    }
  ]
}'

```

サンプル応答

204 No-content

認証レلمシーケンス設定の取得

認証レلمシーケンス設定を表示および変更できます。

概要	GET wsa/api/v3.0/network/auth_sequences	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、認証レلمシーケンス設定を表示および変更する方法の例を示します。

サンプル リクエスト

```
curl --location --request GET 'https://wsa308.cs1:4431/wsa/api/v3.0/network/auth_sequences'
--header 'Authorization: Basic YWRtaW46aXJvbnBvcnQ='
```

サンプル応答

```
{
  "auth_sequences": [
    {
      "schemes": {
        "Kerberos": [
          "myADRealm"
        ],
        "NTLMSSP": [
          "myADRealm"
        ],
        "Basic": [
          "myRealm",
          "myADRealm",
          "myBasicRealm"
        ]
      },
      "name": "All Realms"
    },
    {
      "schemes": {
        "Kerberos": [
          "myADRealm"
        ],
        "Basic": [
          "myRealm",
          "myADRealm"
        ]
      }
    }
  ]
}
```

```

    ],
    },
    "name": "myAuthSequence"
  }
]
}

```

認証レルムシーケンス設定の変更

認証レルムシーケンス設定を表示および変更できます。

概要	PUT wsa/api/v3.0/network/auth_sequences	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、認証シーケンス設定を変更する方法の例を示します。

サンプル リクエスト

```

curl --location --request PUT 'https://wsa308.cs1:6443/wsa/api/v3.0/network/auth_sequences'
--header 'Authorization: Basic YWRtaW46aXJvbnBvcnQ=' --header 'Content-Type:
application/json' --data-raw '{
  "auth_sequences": [
    {
      "schemes": {
        "Basic": [
          "myRealm",
          "myADRealm",
          "myBasicRealm"
        ]
      },
      "name": "myAuthSequence2"
    }
  ]
}'

```

サンプル応答

204 No-content

認証レルムシーケンス設定の追加

認証レルムシーケンス設定を表示および追加できます。

概要	POST wsa/api/v3.0/network/auth_sequences
----	--

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、認証レلمシーケンス設定を表示および追加する方法の例を示します。

サンプル リクエスト

```
curl --location --request POST
'https://wsa308.cs1:6443/wsa/api/v3.0/network/auth_sequences' --header 'Authorization:
Basic YWRtaW46aXJvbnBvcnQ=' --header 'Content-Type: application/json' --data-raw '{
  "auth_sequences": [
    {
      "schemes": {
        "Kerberos": [
          "myADRealm"
        ],
        "Basic": [
          "myRealm",
          "myADRealm"
        ]
      },
      "name": "myAuthSequence2"
    }
  ]
}'
```

サンプル応答

```
204 No-content
```

グローバル認証設定の取得

使用可能なグローバル認証設定の詳細と、認証トークンTTL、クレデンシャルの暗号化、ヘッダーベースの認証などの設定を取得できます。

概要	GET wsa/api/v3.0/network/global_auth_setting	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、グローバル認証設定を取得する方法の例を示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/network/global_auth_setting HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
{
  "global_auth_settings": {
    "failed_auth_handling": "UserSubmitted",
    "re_authentication": "disabled",
    "basic_auth_token_ttl": 3600,
    "action_auth_service_unavailable": "Permit",
    "auth_settings": {
      "ssl_certificate": {
        "country": "IN",
        "basic_constraints": "Critical",
        "org_unit": "WSA",
        "expiry_date": "Jun 16 11:43:16 2041 GMT",
        "common_name": "Cisco",
        "org": "Cisco"
      },
      "header_based_authentication": {
        "xauth_std_user": {
          "text_format": "ASCII",
          "Binary_encoding": "No Encoding"
        },
        "xauth_std_group": {
          "text_format": "ASCII",
          "Binary_encoding": "No Encoding"
        },
        "xauth_use_group_header": "enable",
        "xauth_header_mode": "standard",
        "xauth_retain_auth_egress": "enable",
        "xauth_header_based_auth": "enable"
      },
      "credential_cache_options": {
        "client_ip_idle_timeout": 3600,
        "surrogate_timeout": 3600
      },
      "redirect_hostname": "komal.komal",
      "credential_encryption": 1,
      "Restriction_Timeout": 3601,
      "https_redirect_port": 443
    }
  }
}
```

グローバル認証設定の変更

使用可能なグローバル認証設定の詳細と、認証トークンTTL、クレデンシャルの暗号化、ヘッダーベースの認証などの設定を変更できます。

概要	PUT wsa/api/v3.0/network/global_auth_setting
----	--

サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、グローバル認証設定を変更する方法の例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/web_security/umbrella_seamless_id HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: multipart/form-data
```

サンプル応答

```
204 No-content
```

Umbrella シームレス ID

この項では、次のトピックを扱います。

- [Cisco Umbrella シームレス ID の取得](#) (152 ページ)
- [Cisco Umbrella シームレス ID の変更](#) (153 ページ)

Cisco Umbrella シームレス ID の取得

存在する Cisco Umbrella シームレス ID の詳細と、ホスト、ポート、組織 ID などの設定を取得できます。

概要	GET wsa/api/v3.0/web_security/umbrella_seamless_id	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、存在する Cisco Umbrella シームレス ID の詳細と、ホスト、ポート、組織 ID などの設定を取得する方法の例を示します。

サンプル リクエスト

```
GET /wsa/api/v3.0/web_security/umbrella_seamless_id HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

サンプル応答

```
{
  "cisco_umbrella_seamless_id": {
    "swg_proxy": {
      "host": "54.185.245.81",
      "ports": [
        "80, 443"
      ]
    },
    "org_id": "4709668"
  }
}
```

Cisco Umbrella シームレス ID の変更

存在する Cisco Umbrella シームレス ID の詳細と、ホスト、ポート、組織 ID などの設定を変更できます。

概要	PUT wsa/api/v3.0/web_security/umbrella_seamless_id	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、存在する Cisco Umbrella シームレス ID の詳細と、ホスト、ポート、組織 ID などの設定を変更する方法の例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/web_security/umbrella_seamless_id HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 1151
```

```
{
  "cisco_umbrella_seamless_id": {
    "swg_proxy": {
```

```

        "host": "54.185.245.81",
        "ports": ["80", "443"]
      },
      "org_id": "4709668"
    }
  }
}

```

サンプル応答

204 (No-content)

Umbrella シームレス ID の起動テストの実行

Umbrella シームレス ID の起動テストを実行できます。

概要	GET wsa/api/v3.0/web_security/swg_connectivity_test	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Umbrella シームレス ID の起動テストを実行する方法の例を示します。

サンプル リクエスト

```

GET wsa/api/v3.0/web_security/swg_connectivity_test HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
Query Paramteres: host: wsa353.cs1
Ports: 11

```

サンプル応答

```

{
  "swg_connectivity_test": [
    {
      "host": "wsa353.cs1",
      "port 11": {
        "status": "Failed",
        "message": "Connection to ip and port is refused. Connection to the SWG
Proxy failed. "
      },
      "certificate_validation": {
        "message": "Connect Exception: Error opening publickey fetch server URL.
Certificate validation failed. "
      }
    }
  ]
}

```

セキュア DNSSec 設定

ここでは、次の内容について説明します。

- [セキュア DNS 設定の取得](#) (155 ページ)
- [セキュア DNS 設定の変更](#) (155 ページ)

セキュア DNS 設定の取得

セキュア DNS 設定を有効または無効にすることができます。

概要	GET wsa/api/v2.0/configure/network/dns/dnssec	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、セキュア DNS 設定を有効または無効にする方法の例を示します。

サンプル リクエスト

```
{
  "res_data": {
    "secure_dns": false
  },
  "res_message": "Data received successfully.",
  "res_code": 200
}
```

セキュア DNS 設定の変更

セキュア DNS 設定を有効または無効にすることができます。

概要	PUT wsa/api/v2.0/configure/network/dns/dnssec	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、セキュア DNS 設定を有効または無効にする方法の例を示します。

サンプルリクエスト—セキュア DNS の有効化

```
{
  "secure_dns": true
}
```

サンプル応答—セキュア DNS の有効化

```
{
  "res_data": {
    "update_success": [
      {
        "secure_dns": true
      }
    ]
  },
  "res_message": "Success: 1",
  "res_code": 200
}
```

サンプルリクエスト—セキュア DNS の無効化

```
{
  "secure_dns": false
}
```

サンプル応答—セキュア DNS の無効化

```
{
  "res_data": {
    "update_success": [
      {
        "secure_dns": false
      }
    ]
  },
  "res_message": "Success: 1",
  "res_code": 200
}
```

Identity Service Engine

ここでは、次の内容について説明します。

- [Identity Service Engine の設定の取得](#) (157 ページ)
- [Identity Service Engine の設定の変更](#) (158 ページ)
- [Identity Service Engine の証明書の詳細のアップロード](#) (159 ページ)
- [Identity Service Engine の証明書の詳細のダウンロード](#) (159 ページ)

- [Identity Service Engine の起動テストの実行（160 ページ）](#)

Identity Service Engine の設定の取得

Identity Service Engine の現在の設定を取得できます。

概要	GET wsa/api/v3.0/network/ise	
サポート対象のリソース属性	詳細については、『 <i>AsyncOS 14.5 API - Addendum to the Getting Started Guide for Cisco Secure Web Appliances</i> 』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

次に、Identity Service Engine の設定を取得する方法の例を示します。

サンプルリクエスト 1

```
GET wsa/api/v3.0/network/ise
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
```

サンプル応答 1

```
{
  "ise_service_status": "disable"
}
```

サンプルリクエスト 2

```
GET wsa/api/v3.0/network/ise
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
```

サンプル応答 2

```
{
  "ers_settings": {
    "status": "disable"
  },
  "wa_client_cert": {
    "uploaded": {
      "country": "IN",
      "basic_constraints": "critical",
      "org_unit": "WSA",
      "expiry_date": "Jun 16 11:43:16 2041 GMT",
      "common_name": "Cisco",
      "organization": "Cisco"
    },
    "current_cert": "uploaded"
  },
  "sxp_status": "enable",
  "primary_ise_pxgrid": {
```

```

    "host": "dut058.perf8",
    "certificate": {
      "country": "",
      "basic_constraints": "critical",
      "org_unit": "",
      "expiry_date": "Apr 1 08:15:56 2030 GMT",
      "common_name": "Certificate Services Endpoint Sub CA - ise-server12",
      "organization": ""
    }
  }
}

```

Identity Service Engine の設定の変更

Identity Service Engine の設定を変更できます。

概要	PUT wsa/api/v3.0/network/ise	
サポート対象のリソース属性	詳細については、『 <i>AsyncOS 14.5 API - Addendum to the Getting Started Guide for Cisco Secure Web Appliances</i> 』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

次に、Identity Service Engine の設定を変更する方法の例を示します。

サンプル リクエスト

```

PUT '/wsa/api/v3.0/network/ise' HTTP/1.1
Content-Type: text/plain

{
  "ise_service_status" : "enable",
  "primary_ise_pxgrid": {
    "host": "1.2.3.3"
  },
  "secondary_ise_pxgrid": {
    "host": "1.2.3.9"
  },
  "wa_client_cert": {
    "generated": {
      "expiry_duration": 60,
      "country": "IN",
      "basic_constraints": "not critical",
      "org_unit": "WSA",
      "common_name": "Cisco",
      "organization": "Cisco"
    },
    "current_cert": "generated"
  },
  "sxp_status": "disable",
  "ers_settings": {
    "status": "enable",

```

```

    "username": "qwer-12",
    "password": "YWJjZGVmZW==",
    "secondary_server": "ise-server12.cs1.devit.ciscolabs.com",
    "ers_same_as_ise": false,
    "port": 9061,
    "primary_server": "ise-server12.cs1.devit.ciscolabs.com2"
  }
}

```

サンプル応答

204 (No-content)

Identity Service Engine の証明書の詳細のアップロード

Identity Service Engine の証明書の詳細をアップロードできます。

概要	POST wsa/api/v3.0/network/ise_cert	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Identity Service Engine の証明書の詳細をアップロードする方法の例を示します。

サンプルリクエスト 1

```

POST '/wsa/api/v3.0/network/ise_cert?cert_type=primary_pxgrid' HTTP/1.1
--form 'file=@"/C:/Users/admin/Desktop/rsa-ca.cert.pem"'

```

サンプルリクエスト 2

204 (No-content)

サンプルリクエスト 2

```

POST '/wsa/api/v3.0/network/ise_cert?cert_type=wa_client_uploaded' HTTP/1.1
--form 'file=@"/C:/Users/admin/Desktop/rsa-ca.cert.pem"'
--form 'key=@"/C:/Users/admin/Desktop/rsa-ca.key.pem"'
--form 'key_phrase="aXJvbnBvcnQ="'

```

サンプル応答 2

204 (No-content)

Identity Service Engine の証明書の詳細のダウンロード

Identity Service Engine の証明書の詳細をダウンロードできます。

概要	GET wsa/api/v3.0/network/ise_download_cert
----	--

例

サンプルリクエスト 1

サンプル応答 1

Identity Service Engine の起動テストの実行

概要	GET wsa/api/v3.0/network/ise/start_test	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、Identity Service Engine の現在の設定の起動テストを実行する方法の例を示します。

サンプルリクエスト 1

```
GET wsa/api/v3.0/network/ise/start_test
Host: dut054.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答 1

```
{
  "test_result": "Failure",
  "test_logs": [
    "Checking DNS resolution of ISE pxGrid Node hostname(s) ...",
    "Success: Resolved 'ise-server56.csl.devit.ciscolabs.com' address: 10.10.201.56",
    "Validating WSA client certificate ...",
    "Success: Certificate validation successful",
    "Validating ISE pxGrid Node certificate(s) ...",
    "Success: Certificate validation successful",
    "Checking connection to ISE pxGrid Node(s) ...",
    "Trying primary PxGrid server...",
    "SXP not enabled.",
    "Preparing TLS connection...",
    "",
    "Completed TLS handshake with PxGrid successfully.",
    "",
    "",
    "Trying download SGT from (https://ise-server56.csl.devit.ciscolabs.com:8910)...",
    "",
    "Able to Download 19 SGTs.",
    "",
    "Skipping all SXP related service requests as SXP is not configured.",
    "",
    " ",
    "Trying download user-session from
(https://ise-server56.csl.devit.ciscolabs.com:8910)...",
    "",
    "Failure: Failed to download user-sessions.",
    "Trying connecting to primary ERS service...",
    "",
    "Failure: Unable to communicate with ERS Server.",
    "",
    "Certificate validation error Timeout: connect timed out: 10.10.201.56:9061.",
    "",
    "Failure: Connection to ISE pxGrid Node failed.",
    ""
  ]
}
```

サンプル応答 2

```
Response Code - 400 Bad Request
{
  "error": {
    "message": "ers status is disabled, Unable to initiate ISE test.",
    "code": "400",
    "explanation": "400 = Bad request syntax or unsupported method."
  }
}
```

マルウェア対策レピュテーション

ここでは、次の内容について説明します。

- マルウェア対策レピュテーションの詳細の取得 (162 ページ)
- マルウェア対策レピュテーションの詳細の変更 (169 ページ)
- マルウェア対策分析コンソールの登録 (176 ページ)
- マルウェア対策分析コンソールの登録の削除 (177 ページ)

マルウェア対策レピュテーションの詳細の取得

マルウェア対策スキャンサービス、Web レピュテーションサービス、およびマルウェア分析サービスの設定の詳細が含まれているオブジェクトを取得できます。

概要	GET wsa/api/v3.0/security_services/anti_malware_and_reputation	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、マルウェア対策スキャンサービス、Web レピュテーションサービス、およびマルウェア分析サービスの設定の詳細が含まれているオブジェクトを変更する方法の例を示します。

サンプル リクエスト

```
GET wsa/api/v3.0/security_services/anti_malware_and_reputation HTTP/1.1
Host: dut037.perf8:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTlz
```

サンプル応答

```
{
  "anti_malware_scanning_services": {
    "dvs_max_object_size_mb": 32,
    "webroot": "enable",
    "sophos": "enable",
    "mcafee": "enable",
    "mcafee_heuristic_scanning": "enable",
    "webroot_threat_risk_threshold": 90
  },
  "web_reputation_services": {
    "web_reputaion_filtering": "enable",
    "adaptive_scanning": "enable"
  },
  "malware_analytics_services": {
```

```

"file_analysis": "enable",
"analysis_file_types": {
  "Executables": {
    "selected": [
      "Access.LockFile.14(.ldb)",
      "Application.Reference(.appref-ms)",
      "Piffile(.pif)",
      "Exefile(.exe)"
    ],
    "not_selected": [
      "AWFile(.aw)",
      "VBEFile(.VBE)",
      "WSHFile(.WSH)",
      "Microsoft.PowerShellData.1(.psdl)",
      "LnkFile(.lnk)",
      "Inffile(.inf)",
      "Microsoft.PowerShellScript.1(.ps1)",
      "Word.Wizard.8(.wiz)",
      "JSEFile(.JSE)",
      "Odcfile(.odc)",
      "Htafile(.hta)",
      "VisualStudio.Launcher.suo(.suo)",
      "ShockwaveFlash.ShockwaveFlash(.swf)",
      "Application.Manifest(.application)",
      "Msi.Package(.msi)",
      "FlashPlayer.AudioForFlashPlayer(.f4a)",
      "Diagnostic.Perfmon.Document(.blg)",
      "MSCFile(.msc)",
      "Regfile(.reg)",
      "Microsoft.PowerShellModule.1(.psm)",
      "Textfile(.wtx)",
      "PowerPoint.Wizard.8(.pwz)",
      "JSFile(.js)",
      "FlashPlayer.FlashVideo(.flv)",
      "Oqyfile(.oqy)",
      "OPCFile(.opc)",
      "LEXFile(.lex)",
      "Gmmpfile(.gmmp)",
      "Batfile(.bat)",
      "MSInfoFile(.nfo)",
      "Evtfile(.evt)",
      "Cmdfile(.cmd)",
      "Drvfile(.drv)",
      "VBSFile(.vbs)",
      "WebpnpFile(.webpnp)",
      "Windows.IsoFile(.iso)",
      "Comfile(.com)"
    ]
  },
  "Configuration": {
    "selected": [
      "Hlpfile(.hlp)",
      "Diagnostic.Config(.diagcfg)",
      "Outlook.File.nk2.14(.nk2)",
      "CRTXFile(.crtx)",
      "LibraryFolder(.library-ms)",
      "Inifile(.ini)",
      "VisualStudio.Launcher._vstasln80(. _vstasln80)",
      "CLSID\\{9E56BE60-C50F-11CF-9A2C-00A0C90A90CE}(.mapimail)",
      "Hlwfile(.Hlw)",
      "Aspfile(.cdx)",
      "XEV.GenericApp(.xevgenxml)",
      "VisualStudio.Launcher._sln71(. _sln71)",
      "VisualStudio.Launcher._sln70(. _sln70)",

```

```

"JNLFILE(.jnlp)",
"VisualStudio.Launcher._vjsxsln80(. _vjsxsln80)",
"BrmFile(.printerExport)",
"Group_wab_auto_file(.group)",
"Icmfile(.icm)",
"XTPFILE(.xtp)",
"Vxdfile(.vxd)",
"Outlook.File.hol.14(.hol)",
"Hlsfile(.HlS)",
"Hltfile(.HlT)",
"Jtpfile(.jtp)",
"Hlvfile(.HlV)",
"GCSXFile(.gcsx)",
"Hlhfile(.HlH)",
"Ocxfile(.ocx)",
"AcroExch.SecStore(.secstore)",
"Hlkfile(.HlK)",
"MSGGraph.Chart.8(.gra)",
"RDBFileProperties.1(.sfcache)",
"InfoPath.SolutionManifest.3(.xsf)",
"Scrfile(.scr)",
"Hldfile(.HlD)",
"Wmffile(.wmf)",
"Hlffile(.HlF)",
"MediaCatalogMGC(.mgc)",
"GQSXFile(.gqsx)",
"MediaCenter.MCL(.mcl)",
"Migfile(.mig)",
"InternetShortcut(.URL)",
"Windows.gadget(.gadget)",
"Outlook.File.ics.14(.ics)",
"MediaCenter.C2R(.c2r)",
"OneNote.TableOfContents.12(.onetoc2)",
"Sysfile(.sys)",
"MediaCatalogMML(.mml)",
"JobObject(.job)",
"Emffile(.emf)",
"SavedDsQuery(.qds)",
"VisualStudio.Launcher._vcsxsln80(. _vcsxsln80)",
"CSSFile(.css)",
"VisualStudio.Launcher._sln(. _sln)",
"XTP2FILE(.xtp2)",
"RemoteAssistance.1(.msrcincident)",
"Microsoft.PowerShellXMLData.1(.pslxml)",
"Diagnostic.Perfmon.Config(.perfmoncfg)",
"LpkSetup.1(.mlc)",
"VisualStudio.Launcher._sln80(. _sln80)",
"GrooveLinkFile(.glk)",
"Cplfile(.cpl)",
"RDP.File(.rdp)",
"PDXFileType(.pdx)",
"Microsoft.WindowsCardSpaceBackup(.crds)",
"Cdmpfile(.cdmp)",
"Campfile(.camp)",
"PCBFILE(.pcb)",
"VisualStudio.Launcher._sln60(. _sln60)",
"VisualStudio.Launcher._vbxsln80(. _vbxsln80)",
"VisualStudio.Launcher.sln(.sln)",
"Contact_wab_auto_file(.contact)",
"OfficeListShortcut(.ols)",
"Hlcfiile(.HlC)",
"Wcxfile(.wcx)",
"OneNote.TableOfContents(.onetoc)",
"CABFolder(.cab)",

```

```

"VisualStudio.Launcher._vcppxsl80(.vcppxsl80)",
"MSSppPackageFile(.slupkg-ms)",
"CRLFile(.crl)",
"Ratfile(.rat)"
],
"not_selected": [
"MediaPackageFile(.mpf)",
"Prffile(.prf)",
"GrooveStub(.gfs)",
"SHCmdFile(.scf)"
]
},
"Microsoft Documents": {
"selected": [],
"not_selected": [
"Excel.TemplateMacroEnabled(.xltm)",
"PowerPoint.Addin.8(.ppa)",
"VisualStudio.Launcher._vwdxsl80(.vwdxsl80)",
"Wordhtmlfile(.dohtml)",
"PowerPoint.Template.8(.pot)",
"Excel.OpenDocumentSpreadsheet.12(.ods)",
"Outlook.File.ost.14(.ost)",
"Excelhtmlfile(.xlshtml)",
"PowerPoint.SlideShow.8(.pps)",
"Powerpointhtmlfile(.ppthtml)",
"Excel.Template(.xltx)",
"Powerpointhtmltemplate(.pothtml)",
"Wordxml(.docxml)",
"Publisherhtmlfile(.pubhtml)",
"PowerPoint.SlideShow.12(.ppsx)",
"GrooveFile(.grv)",
"Powerpointmhtmlfile(.pptmhtml)",
"Excel.SheetBinaryMacroEnabled.12(.xlsb)",
"PowerPoint.Template.12(.potx)",
"H1qfile(.H1Q)",
"PowerPoint.Addin.12(.ppam)",
"Dqyfile(.dqy)",
"PowerPoint.TemplateMacroEnabled.12(.potm)",
"Excelhtmltemplate(.xlthtml)",
"VisioViewer.Viewer(.vtx)",
"Excel.CSV(.csv)",
"Excel.Addin(.xla)",
"PowerPoint.Show.12(.pptx)",
"Excel.Sheet.12(.xlsx)",
"Word.Document.12(.docx)",
"Outlook.File.otm.14(.otm)",
"Powerpointxmlfile(.pptxml)",
"Word.Template.12(.dotx)",
"Publisher.Document.14(.pub)",
"Wordhtmltemplate(.dohtml)",
"Excel.SheetMacroEnabled.12(.xlsm)",
"PowerPoint.ShowMacroEnabled.12(.pptm)",
"Wordhtmlfile(.docm)",
"OneNote.Section.1(.one)",
"Word.TemplateMacroEnabled.12(.dotm)",
"PowerPoint.SlideShowMacroEnabled.12(.ppsm)",
"OneNote.Package(.onepkg)",
"Publisherhtmlfile(.pubmhtml)",
"Outlook.File.det.14(.det)",
"Excel.AddInMacroEnabled(.xlam)",
"OfficeTheme.12(.thmx)",
"PowerPoint.Show.8(.ppt)",
"Word.Addin.8(.wll)",
"Outlook.File.oft.14(.oft)",

```

```

        "Word.Document.8(.doc)",
        "Excel.Template.8(.xlt)",
        "Excel.Sheet.8(.xls)",
        "Word.Template.8(.dot)"
    ]
},
"Database": {
    "selected": [
        "Access.MDBFile(.mdb)",
        "Access.Extension.14(.mda)",
        "Access.MDEFile.14(.mde)"
    ],
    "not_selected": [
        "Access.Application.14(.accdb)",
        "Access.ACCDCFile.14(.accdc)",
        "Access.ACCDAExtension.14(.accda)",
        "Access.ACCDEFile.14(.accde)",
        "Access.ACCDRFile.14(.accdr)",
        "Access.Shortcut.Report.1(.mar)",
        "Access.WebApplicationReference.14(.accdw)",
        "Access.ACCDTFile.14(.accdt)",
        "Access.WizardUserDataFile.14(.accdu)",
        "CATFile(.cat)",
        "Access.ACCFTFile.14(.accft)",
        "Access.Workgroup.14(.mdw)",
        "Access.Shortcut.Table.1(.mdt)",
        "Access.Project.14(.adp)",
        "Access.ADEFile.14(.ade)",
        "Access.BlankProjectTemplate.14(.adn)",
        "Access.Shortcut.Query.1(.maq)",
        "Access.Shortcut.StoredProcedure.1(.mas)",
        "Accesshtmlfile(.mdbhtml)",
        "Access.Shortcut.Function.1(.mau)",
        "Access.Shortcut.Table.1(.mat)",
        "Access.Shortcut.DataAccessPage.1(.maw)",
        "Accesssthmltemplate(.wizhtml)",
        "Dbfile(.db)",
        "Microsoft.Jet.OLEDB.4.0(.jod)",
        "Access.Shortcut.Module.1(.mad)",
        "Access.Shortcut.Diagram.1(.mag)",
        "Access.Shortcut.Form.1(.maf)",
        "Access.Shortcut.Macro.1(.mam)",
        "Accesshtmlfile(.mfp)",
        "Odctablefile(.odctablefile)",
        "ACLFile(.acl)",
        "MSDASC(.UDL)",
        "Odcnewfile(.odcnewfile)",
        "Odcdatabasefile(.odcdatabasefile)"
    ]
},
"Miscellaneous": {
    "selected": [],
    "not_selected": [
        "Microsoft.Website(.website)",
        "Dllfile(.rll)",
        "Diagnostic.Cabinet(.diagcab)",
        "IE.AssocFile.PARTIAL(.partial)",
        "CLSID\\{9E56BE61-C50F-11CF-9A2C-00A0C90A90CE}(.desklink)",
        "STLFile(.stl)",
        "Diagnostic.Document(.diagpkg)",
        "Chkfile(.chk)",
        "Pfmfile(.pfm)",
        "Label(.label)",
        "MSDASQL(.dsn)",
    ]
}

```

```

"Windows.CompositeFont(.compositefont)",
"Microsoft.InformationCard(.crd)",
"AcroExch.acrobatsecuritysettings(.acrobatsecuritysettings)",
"PKOFile(.pko)",
"MediaCatalogMMW(.mmw)"
]
},
"Encoded and Encrypted": {
  "selected": [],
  "not_selected": [
    "SPCFile(.spc)",
    "P7RFile(.p7r)",
    "P7SFile(.p7s)",
    "CertificateStoreFile(.sst)",
    "CERFile(.der)",
    "P10File(.p10)",
    "Certificate_wab_auto_file(.p7c)",
    "MSSppLicenseFile(.xrm-ms)",
    "PFXFile(.pfx)",
    "P7MFile(.p7m)"
  ]
},
"Document": {
  "selected": [],
  "not_selected": [
    "Word.RTF.8(.rtf)",
    "Jntfile(.jnt)",
    "AcroExch.XFDFDocAcroExch.XFDFDoc(.xpdf)",
    "InfoPath.Document.3(.infopathxml)",
    "Word.OpenDocumentText.12(.odt)",
    "AcroExch.Plugin(.api)",
    "MSHelp.hxc.2.5(.hxc)",
    "Shtmlfile(.shtml)",
    "MSHelp.hxf.2.5(.hxf)",
    "MSHelp.hxe.2.5(.hxe)",
    "MSHelp.hxd.2.5(.hxd)",
    "MSHelp.hxk.2.5(.hxk)",
    "MSHelp.hxi.2.5(.hxi)",
    "MSHelp.hxh.2.5(.hxh)",
    "Chm.file(.chm)",
    "MSHelp.hxs.2.5(.hxs)",
    "MSHelp.hxr.2.5(.hxr)",
    "MSHelp.hxq.2.5(.hxq)",
    "Htmlfile(.html)",
    "MSHelp.hxw.2.5(.hxw)",
    "MSHelp.hxv.2.5(.hxv)",
    "Windows.XPSReachViewer(.xps)",
    "Xhtmlfile(.xhtml)",
    "Mhtmlfile(.mhtml)",
    "Xmlfile(.xml)",
    "Odccubefile(.odccubefile)",
    "Otffile(.otf)",
    "AcroExch.XDPDoc(.xdp)",
    "AcroExch.FDFDoc(.fdf)",
    "AcroExch.pdfxml(.pdfxml)",
    "Outlook.File.fdm.14(.fdm)",
    "GrooveVCard(.vcg)",
    "GrooveSpaceArchive(.gsa)",
    "AcroExch.Document(.pdf)",
    "Windows.DVD.Maker(.msdvd)"
  ]
},
"Email": {
  "selected": [],

```

```

    "not_selected": [
      "Outlook.File.vcf.14(.vcf)",
      "Outlook.File.eml.14(.eml)",
      "Microsoft.PowerShellConsole.1(.pscl)",
      "Outlook.File ofs.14(.ofs)",
      "Outlook.File.pab.14(.pab)",
      "Outlook.File.msg.14(.msg)"
    ],
  },
  "Archived and compressed": {
    "selected": [
      "GrooveToolArchive(.gta)",
      "GLOXFile(.glox)",
      "7zFile(.7z)"
    ],
    "not_selected": [
      "TarFile(.tar)",
      "ZipFile(.zip)",
      "LzxFile(.lzx)",
      "Microsoft.System.Update.1(.msu)",
      "Jarfile(.jar)",
      "GzFile(.gz)",
      "LzhFile(.lzh)",
      "RarFile(.rar)",
      "VisualStudio.ContentInstaller.vsi(.vsi)",
      "Pbkfile(.pbk)"
    ]
  },
},
"file_reputation_filtering": "enable",
"advanced_settings": {
  "file_analysis_threshold": {
    "score": 95,
    "cloud_service": "enable"
  },
},
"routing_table": "Management",
"file_reputation": {
  "query_timeout": 15,
  "client_id": "a581d63d-4501-4876-8d7c-ff0e1c308372",
  "heart_beat_interval": 900,
  "proxy_settings": {
    "username": "swarchak",
    "port": 80,
    "relax_cert_validation": "enable",
    "server": "testserver.com"
  },
},
"server": {
  "uploaded_cert_details": {
    "subject": "C=IN, O=sbg, OU=in, CN=tesy",
    "expiry_date": "Nov 3 16:07:48 2022 GMT",
    "issuer": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd"
  },
  "cert_authority": "Use Uploaded Certificate Authority",
  "cloud_server": "private",
  "available_servers": [
    "AMERICAS (cloud-sa.amp.cisco.com)",
    "AMERICAS (Legacy) (cloud-sa.amp.sourcefire.com)",
    "EUROPE (cloud-sa.eu.amp.cisco.com)",
    "Private Cloud"
  ],
  "server": "testfilererepserver.com"
},
"cache_expiry_period": {

```

```

    "unknown": 1800,
    "malicious": 172800,
    "clean": 604800
  },
  "file_analysis": {
    "client_id": "02_VLNWSA9294_420743B86D9C2E1D1DDD-B35CFA98811F_S600V_0000000000",
    "proxy_settings": {
      "use_file_reputation_proxy": "disable",
      "username": "swarchak",
      "port": 80,
      "server": "testfileanalysisserver.com"
    },
    "server": {
      "uploaded_cert_details": {
        "subject": "C=IN, O=sbg, OU=in, CN=tesy",
        "expiry_date": "Nov  3 16:07:48 2022 GMT",
        "issuer": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd"
      },
      "cert_authority": "Use Uploaded Certificate Authority",
      "cloud_server": "private",
      "tg_servers": [
        "server3.com",
        "server4.com"
      ],
      "available_servers": [
        "AMERICAS (https://panacea.threatgrid.com)",
        "EUROPE (https://panacea.threatgrid.eu)",
        "Private Cloud"
      ]
    }
  }
}
}
}
}

```

マルウェア対策レピュテーションの詳細の変更

マルウェア対策スキャンサービス、Web レピュテーションサービス、およびマルウェア分析サービスの設定の詳細が含まれているオブジェクトを変更できます。

概要	PUT wsa/api/v3.0/security_services/anti_malware_and_reputation	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、マルウェア対策スキャンサービス、Web レピュテーションサービス、およびマルウェア分析サービスの設定の詳細が含まれているオブジェクトを変更する方法の例を示します。

サンプル リクエスト

```
PUT /wsa/api/v3.0/security_services/anti_malware_and_reputation HTTP/1.1
Host: dut037.perf8:4431
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
Content-Type: multipart/form-data;
boundary=-----591659103622018736729500
Content-Length: 17917
```

```
{
  "malware_analytics_services": {
    "file_analysis": "enable",
    "analysis_file_types": {
      "Executables": {
        "selected": [
          "AWFile(.aw)",
          "VBEFile(.VBE)",
          "WSHFile(.WSH)",
          "Piffile(.pif)",
          "LnkFile(.lnk)",
          "Inffile(.inf)",
          "Exefile(.exe)"
        ],
        "not_selected": [
          "Access.LockFile.14(.ldb)",
          "Application.Reference(.appref-ms)",
          "Drvfile(.drv)",
          "Microsoft.PowerShellData.1(.psdl)",
          "Odcfile(.odc)",
          "Word.Wizard.8(.wiz)",
          "JSEFile(.JSE)",
          "Microsoft.PowerShellScript.1(.ps1)",
          "htafile(.hta)",
          "VisualStudio.Launcher.suo(.suo)",
          "ShockwaveFlash.ShockwaveFlash(.swf)",
          "Application.Manifest(.application)",
          "Msi.Package(.msi)",
          "Diagnostic.Perfmon.Document(.blg)",
          "MSCFile(.msc)",
          "Regfile(.reg)",
          "Microsoft.PowerShellModule.1(.psm)",
          "Textfile(.wtx)",
          "PowerPoint.Wizard.8(.pwz)",
          "JSFile(.js)",
          "Oqyfile(.oqy)",
          "OPCFile(.opc)",
          "LEXFile(.lex)",
          "Gmmpfile(.gmmp)",
          "Batfile(.bat)",
          "MSInfoFile(.nfo)",
          "Comfile(.com)",
          "Cmdfile(.cmd)",
          "VBSFile(.vbs)",
          "FlashPlayer.FlashVideo(.flv)",
          "FlashPlayer.AudioForFlashPlayer(.f4a)",
          "WebpnpFile(.webpnp)",
          "Windows.IsoFile(.iso)",
          "Evtfile(.evt)"
        ]
      }
    },
    "Document": {
      "selected": [],
      "not_selected": [
        "Word.RTF.8(.rtf)",
        "Jntfile(.jnt)"
      ]
    }
  }
}
```

```

"AcroExch.XFDFDocAcroExch.XFDFDoc(.xpdf)",
"InfoPath.Document.3(.infopathxml)",
"Word.OpenDocumentText.12(.odt)",
"AcroExch.Plugin(.api)",
"MSHelp.hxc.2.5(.hxc)",
"Shtmlfile(.shtml)",
"MSHelp.hxf.2.5(.hxf)",
"MSHelp.hxe.2.5(.hxe)",
"MSHelp.hxd.2.5(.hxd)",
"MSHelp.hxk.2.5(.hxk)",
"MSHelp.hxi.2.5(.hxi)",
"MSHelp.hxh.2.5(.hxh)",
"Chm.file(.chm)",
"MSHelp.hxs.2.5(.hxs)",
"MSHelp.hxr.2.5(.hxr)",
"MSHelp.hxq.2.5(.hxq)",
"Htmlfile(.html)",
"MSHelp.hxw.2.5(.hxw)",
"MSHelp.hxv.2.5(.hxv)",
"Windows.XPSReachViewer(.xps)",
"Xhtmlfile(.xhtml)",
"Mhtmlfile(.mhtml)",
"Xmlfile(.xml)",
"Odccubefile(.odccubefile)",
"Otffile(.otf)",
"AcroExch.XDPDoc(.xdp)",
"AcroExch.FDFDoc(.fdf)",
"AcroExch.pdfxml(.pdfxml)",
"Outlook.File.fdm.14(.fdm)",
"GrooveVCard(.vcg)",
"GrooveSpaceArchive(.gsa)",
"AcroExch.Document(.pdf)",
"Windows.DVD.Maker(.msdvd)"
]
},
"Microsoft Documents": {
  "selected": [],
  "not_selected": [
    "Excel.TemplateMacroEnabled(.xltm)",
    "PowerPoint.Addin.8(.ppa)",
    "VisualStudio.Launcher._vwdxsln80(.vwdxsln80)",
    "Wordhtmlfile(.dohtml)",
    "PowerPoint.Template.8(.pot)",
    "Excel.OpenDocumentSpreadsheet.12(.ods)",
    "Outlook.File.ost.14(.ost)",
    "Excelhtmlfile(.xlshtml)",
    "PowerPoint.SlideShow.8(.pps)",
    "Excel.AddInMacroEnabled(.xlam)",
    "Excel.Template(.xltx)",
    "Powerpointhtmltemplate(.pothtml)",
    "Wordxml(.docxml)",
    "Publisherhtmlfile(.pubhtml)",
    "PowerPoint.SlideShow.12(.ppsx)",
    "GrooveFile(.grv)",
    "Powerpointmhtmlfile(.pptmhtml)",
    "OneNote.Section.1(.one)",
    "PowerPoint.Template.12(.potx)",
    "H1qfile(.H1Q)",
    "PowerPoint.Addin.12(.ppam)",
    "Dqyfile(.dqy)",
    "PowerPoint.TemplateMacroEnabled.12(.potm)",
    "Word.Addin.8(.wll)",
    "Excelhtmltemplate(.xlthtml)",
    "VisioViewer.Viewer(.vtx)",

```

```

        "Excel.CSV(.csv)",
        "PowerPoint.Show.12(.pptx)",
        "Excel.Sheet.12(.xlsx)",
        "Word.Document.12(.docx)",
        "Outlook.File.otm.14(.otm)",
        "Powerpointxmlfile(.pptxml)",
        "Word.Template.12(.dotx)",
        "Publisher.Document.14(.pub)",
        "Excel.SheetMacroEnabled.12(.xlsm)",
        "PowerPoint.ShowMacroEnabled.12(.pptm)",
        "Wordhtmlfile(.docm)",
        "Excel.SheetBinaryMacroEnabled.12(.xlsb)",
        "Word.TemplateMacroEnabled.12(.dotm)",
        "PowerPoint.SlideShowMacroEnabled.12(.ppsm)",
        "OneNote.Package(.onepkg)",
        "Wordhtmltemplate(.dohtml)",
        "Outlook.File.det.14(.det)",
        "Excel.Addin(.xla)",
        "OfficeTheme.12(.thmx)",
        "PowerPoint.Show.8(.ppt)",
        "Word.Document.8(.doc)",
        "Powerpointhtmlfile(.phtml)",
        "Outlook.File.oft.14(.oft)",
        "Publisherhtmlfile(.pubhtml)",
        "Excel.Template.8(.xlt)",
        "Excel.Sheet.8(.xls)",
        "Word.Template.8(.dot)"
    ],
    },
    "Database": {
        "selected": [],
        "not_selected": [
            "Access.Application.14(.accdb)",
            "Access.ACDCFile.14(.accdc)",
            "Access.ACCEExtension.14(.accda)",
            "Access.ACCEFile.14(.accde)",
            "Access.MDBFile(.mdb)",
            "Access.Extension.14(.mda)",
            "Access.MDEFile.14(.mde)",
            "Access.ACCEFile.14(.accedr)",
            "Access.Shortcut.Report.1(.mar)",
            "Access.WebApplicationReference.14(.accdw)",
            "Access.ACCEFile.14(.accedt)",
            "Access.WizardUserDataFile.14(.accdu)",
            "ACLFile(.acl)",
            "Access.ACCEFile.14(.accft)",
            "Access.Workgroup.14(.mdw)",
            "Access.Shortcut.Table.1(.mdt)",
            "Access.Project.14(.adp)",
            "Access.ADEFile.14(.ade)",
            "Access.BlankProjectTemplate.14(.adn)",
            "Access.Shortcut.Query.1(.maq)",
            "Access.Shortcut.StoredProcedure.1(.mas)",
            "Accesshtmlfile(.mdbhtml)",
            "Access.Shortcut.Function.1(.mau)",
            "Access.Shortcut.Table.1(.mat)",
            "Access.Shortcut.DataAccessPage.1(.maw)",
            "Accesshtmltemplate(.wizhtml)",
            "Dbfile(.db)",
            "Microsoft.Jet.OLEDB.4.0(.jod)",
            "Access.Shortcut.Module.1(.mad)",
            "Access.Shortcut.Diagram.1(.mag)",
            "Access.Shortcut.Form.1(.maf)",
            "Access.Shortcut.Macro.1(.mam)"
        ]
    }
}

```

```

        "Accesshtmlfile(.mfp)",
        "Odctablefile(.odctablefile)",
        "CATFile(.cat)",
        "Odcdatabasefile(.odcdatabasefile)",
        "Odcnewfile(.odcnewfile)",
        "MSDASC(.UDL)"
    ]
},
"Miscellaneous": {
    "selected": [],
    "not_selected": [
        "Microsoft.Website(.website)",
        "Dllfile(.rll)",
        "Diagnostic.Cabinet(.diagcab)",
        "IE.AssocFile.PARTIAL(.partial)",
        "CLSID\\{9E56BE61-C50F-11CF-9A2C-00A0C90A90CE}(.desklink)",
        "STLFile(.stl)",
        "Diagnostic.Document(.diagpkg)",
        "Chkfile(.chk)",
        "Pfmfile(.pfm)",
        "Label(.label)",
        "MSDASQL(.dsn)",
        "Windows.CompositeFont(.compositefont)",
        "Microsoft.InformationCard(.crd)",
        "AcroExch.acrobatsecuritysettings(.acrobatsecuritysettings)",
        "PKOFile(.pko)",
        "MediaCatalogMMW(.mmw)"
    ]
},
"Encoded and Encrypted": {
    "selected": [],
    "not_selected": [
        "P7MFile(.p7m)",
        "P7RFile(.p7r)",
        "P7SFile(.p7s)",
        "CertificateStoreFile(.sst)",
        "CERFile(.der)",
        "P10File(.p10)",
        "Certificate_wab_auto_file(.p7c)",
        "MSSppLicenseFile(.xrm-ms)",
        "PFXFile(.pfx)",
        "SPCFile(.spc)"
    ]
},
"Configuration": {
    "selected": [],
    "not_selected": [
        "MediaCatalogMGC(.mgc)",
        "Prffile(.prf)",
        "GrooveStub(.gfs)",
        "SHCmdFile(.scf)",
        "Hlpfile(.hlp)",
        "H1cfile(.H1C)",
        "Outlook.File.nk2.14(.nk2)",
        "CRTXFile(.crtx)",
        "LibraryFolder(.library-ms)",
        "Inifile(.ini)",
        "VisualStudio.Launcher._vstasln80(.vstasln80)",
        "MediaCatalogMML(.mml)",
        "CLSID\\{9E56BE60-C50F-11CF-9A2C-00A0C90A90CE}(.mapimail)",
        "GCSXFile(.gcsx)",
        "Aspfile(.cdx)",
        "XEV.GenericApp(.xevgenxml)",
        "VisualStudio.Launcher._sln71(.sln71)",
    ]
}

```

```

"VisualStudio.Launcher._sln70(._sln70)",
"JNLFILE(.jnl)",
"VisualStudio.Launcher._vjsxsl80(._vjsxsl80)",
"Campfile(.camp)",
"BrmFile(.printerExport)",
"Group_wab_auto_file(.group)",
"Icmfile(.icm)",
"XTPFILE(.xtp)",
"Vxdfile(.vxd)",
"Outlook.File.hol.14(.hol)",
"Hlsfile(.HlS)",
"Hltfile(.HlT)",
"Jtpfile(.jtp)",
"Hlvfile(.HlV)",
"Hlwfile(.HlW)",
"Hlhfile(.HlH)",
"Ocxfile(.ocx)",
"AcroExch.SecStore(.secstore)",
"Hlkfile(.HlK)",
"Contact_wab_auto_file(.contact)",
"MSGraph.Chart.8(.gra)",
"RDBFileProperties.1(.sfcache)",
"Scrfile(.scr)",
"Hldfile(.HlD)",
"WmfFile(.wmf)",
"Hlffile(.HlF)",
"CRLFile(.crl)",
"MediaPackageFile(.mpf)",
"GQSXFile(.gqsx)",
"MediaCenter.MCL(.mcl)",
"Migfile(.mig)",
"InternetShortcut(.URL)",
"Windows.gadget(.gadget)",
"OneNote.TableOfContents.12(.onetoc2)",
"Sysfile(.sys)",
"Outlook.File.ics.14(.ics)",
"JobObject(.job)",
"GrooveLinkFile(.glk)",
"SavedDsQuery(.qds)",
"VisualStudio.Launcher._vcsxsl80(._vcsxsl80)",
"VisualStudio.Launcher._sln(._sln)",
"XTP2FILE(.xtp2)",
"RemoteAssistance.1(.msrcincident)",
"Microsoft.PowerShellXMLData.1(.pslxml)",
"Diagnostic.Perfmon.Config(.perfmoncfg)",
"LpkSetup.1(.mlc)",
"VisualStudio.Launcher._sln80(._sln80)",
"Emffile(.emf)",
"Cplfile(.cpl)",
"RDP.File(.rdp)",
"PDXFileType(.pdx)",
"Microsoft.WindowsCardSpaceBackup(.crds)",
"Cdmpfile(.cdmp)",
"MediaCenter.C2R(.c2r)",
"PCBFILE(.pcb)",
"VisualStudio.Launcher._sln60(._sln60)",
"VisualStudio.Launcher._vbxsln80(._vbxsln80)",
"VisualStudio.Launcher.sln(.sln)",
"OfficeListShortcut(.ols)",
"InfoPath.SolutionManifest.3(.xsf)",
"CSSFile(.css)",
"Wcxfile(.wcx)",
"OneNote.TableOfContents(.onetoc)",
"CABFolder(.cab)",

```

```

        "VisualStudio.Launcher._vcppxsln80(._vcppxsln80)",
        "MSSppPackageFile(.slupkg-ms)",
        "Diagnostic.Config(.diagcfg)",
        "Ratfile(.rat)"
    ]
},
"Email": {
    "selected": [],
    "not_selected": [
        "Outlook.File.vcf.14(.vcf)",
        "Outlook.File.eml.14(.eml)",
        "Microsoft.PowerShellConsole.1(.pscl)",
        "Outlook.File ofs.14(.ofs)",
        "Outlook.File.pab.14(.pab)",
        "Outlook.File.msg.14(.msg)"
    ]
},
"Archived and compressed": {
    "selected": [],
    "not_selected": [
        "GrooveToolArchive(.gta)",
        "TarFile(.tar)",
        "ZipFile(.zip)",
        "LzxFile(.lzx)",
        "Microsoft.System.Update.1(.msu)",
        "Jarfile(.jar)",
        "GzFile(.gz)",
        "GLOXFile(.glox)",
        "LzhFile(.lzh)",
        "RarFile(.rar)",
        "VisualStudio.ContentInstaller.vsi(.vsi)",
        "7zFile(.7z)",
        "Pbkfile(.pbk)"
    ]
}
},
"file_reputation_filtering": "enable",
"advanced_settings": {
    "file_analysis_threshold": {
        "score": 95,
        "cloud_service": "enable"
    },
    "routing_table": "Management",
    "file_reputation": {
        "query_timeout": 15,
        "client_id": "ab54d0e2-a978-466c-a37f-e9451d173ac6",
        "heart_beat_interval": 900,
        "proxy_settings": {
            "username": "",
            "port": 80,
            "relax_cert_validation": "disable",
            "server": ""
        },
    },
    "server": {
        "uploaded_cert_details": {
            "subject": "C=IN, O=Cisco, OU=Cisco, CN=Cisco",
            "expiry_date": "Apr 6 13:43:19 2026 GMT",
            "issuer": "C=IN, O=Cisco, OU=Cisco, CN=Cisco"
        },
        "cert_authority": "Use Uploaded Certificate Authority",
        "cloud_server": "private",
        "available_servers": [
            "AMERICAS (cloud-sa.amp.cisco.com)",
            "AMERICAS (Legacy) (cloud-sa.amp.sourcefire.com)",

```

```

        "EUROPE (cloud-sa.eu.amp.cisco.com)",
        "Private Cloud"
    ],
    "server": "testfilerepserver.com"
  }
},
"cache_expiry_period": {
  "unknown": 900,
  "malicious": 86400,
  "clean": 604800
},
"file_analysis": {
  "client_id":
"02_VLNWSA9294_4229DB97298D40B6DB38-2F09FC0ABBD9_S300V_0000000000",
  "proxy_settings": {
    "use_file_reputation_proxy": "disable",
    "username": "testadmin123",
    "port": 635,
    "server": "testdomain.com"
  },
  "server": {
    "uploaded_cert_details": {
      "subject": "C=IN, O=Cisco, OU=Cisco, CN=Cisco",
      "expiry_date": "Apr  6 13:43:19 2026 GMT",
      "issuer": "C=IN, O=Cisco, OU=Cisco, CN=Cisco"
    },
    "cert_authority": "Use Uploaded Certificate Authority",
    "cloud_server": "private",
    "tg_servers": [
      "analysis_server.com"
    ],
    "available_servers": [
      "AMERICAS (https://panacea.threatgrid.com)",
      "EUROPE (https://panacea.threatgrid.eu)",
      "Private Cloud"
    ]
  }
}
}
}
}

```

サンプル応答

Response: 204 (No-content)

マルウェア対策分析コンソールの登録

マルウェア対策分析コンソールのエンドポイント登録ステータスの詳細を含むオブジェクトのリストを取得できます。

概要	GET wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registration	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、マルウェア対策分析コンソールのエンドポイント登録ステータスの詳細を含むオブジェクトのリストを取得する方法の例を示します。

サンプル リクエスト

```
GET wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registration
HTTP/1.1
Host: wsall8.cs14:10118
Authorization: Basic Auth
```

サンプル応答 1—登録前

```
{ "status": "Not registered" }
```

サンプル応答 2—登録後

```
{
  "status": "Registered",
  "device_name": "VLNWSA9294_42292897BFE970627FA5-0E60982C2E26"
}
```

マルウェア対策分析コンソールの登録の削除

マルウェア対策分析コンソールのエンドポイント登録ステータスの詳細を含むオブジェクトのリストを削除できます。

概要	DELETE wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registration	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、マルウェア対策分析コンソールのエンドポイント登録ステータスの詳細を含むオブジェクトのリストを削除する方法の例を示します。

サンプル リクエスト

```
DELETE
wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registration
HTTP/1.1
Host: wsall8.cs14:10118
Authorization: Basic Auth
```

サンプル応答

```
""Successfully deregistered from Malware Analytics for Endpoints.""
```

ユーザ通知 (End-User Notification)

ここでは、次の内容について説明します。

- [エンドユーザー通知の詳細の取得 \(178 ページ\)](#)
- [エンドユーザー通知の詳細の変更 \(179 ページ\)](#)

エンドユーザー通知の詳細の取得

Secure Web Appliance のエンドユーザー通知の設定情報を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/security_services/eun_config	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、エンドユーザー通知の設定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 /wsa/api/v3.0/security_services/eun_config
HTTP/1.1
Host: dut104.perf8:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
{
  "http_https": {
    "general_settings": {
      "logo_image": "CISCO",
      "language": "English"
    },
    "end_user_notification_pages": {
      "notification_type": "Use On-box End User Notification",
      "end_user_feedback": false,
      "contact": "Admin",
      "email_address": "admin@cisco.com",
      "custom_message": "Test*"
    }
  }
}
```

```

    },
    "end_user_url_filtering_warning_page": {
      "custom_message": "##### Warn #####",
      "time_between_warning": 18000
    }
  }
}

```

エンドユーザー通知の詳細の変更

Secure Web Appliance のエンドユーザー通知の設定情報を変更できます。次に、構文とサポート対象の属性を示します。

概要	PUT /wsa/api/v3.0/security_services/eun_config	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、エンドユーザー通知の設定を変更する方法の例を示します。

。

サンプル リクエスト

```

PUT /wsa/api/v3.0/security_services/eun_config
HTTP/1.1
Host: dut104.perf8:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
Content-Type: application/json
Content-Length: 360
{
  "http_https": {
    "general_settings": {
      "language": "English",
      "logo_image": "CISCO"
    },
    "end_user_notification_pages": {
      "end_user_feedback": false,
      "contact": "admin",
      "email_address": "admin@cisco.com",
      "notification_type": "Use On-box End User Notification",
      "custom_message": "This is cm"
    },
    "end_user_url_filtering_warning_page": {
      "custom_message": "",
      "time_between_warning": 3600
    }
  }
}

```

```
}  
}
```

サンプル応答

204 (No-content)



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 **configure** リソース名が含まれます。設定情報の取得（GET）と、設定データの変更（POST、DELETE）を実行できます。

概要	GET /wsa/api/v2.0/configure/system/smtp POST /wsa/api/v2.0/configure/system/smtp PUT /wsa/api/v2.0/configure/system/smtp DELETE /wsa/api/v2.0/configure/system/smtp	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

- [SMTP リレーホストの詳細の取得（182 ページ）](#)
- [新しい SMTP リレーホストの追加（182 ページ）](#)
- [SMTP リレーホストの詳細の変更（183 ページ）](#)
- [複数の SMTP リレーホストの削除（184 ページ）](#)
- [すべての SMTP リレーホストの削除（185 ページ）](#)
- [ユーザー ロールにアクセス可能な API の取得（186 ページ）](#)
- [SecureX ファイルの取得（187 ページ）](#)
- [SecureX ファイル設定の変更（188 ページ）](#)
- [SecureX のユーザー情報詳細の追加（189 ページ）](#)
- [認証設定の取得（190 ページ）](#)
- [ユーザーエージェントの取得（192 ページ）](#)
- [URL カテゴリの取得（193 ページ）](#)
- [時間範囲の取得（195 ページ）](#)
- [クォータの取得（197 ページ）](#)
- [プロキシ設定の取得（198 ページ）](#)

- [識別方法の取得 \(199 ページ\)](#)
- [ADC の詳細の取得 \(200 ページ\)](#)
- [正常性チェック API \(203 ページ\)](#)

SMTP リレーホストの詳細の取得

サンプル リクエスト

```
GET /wsa/api/v2.0/configure/system/smtp
HTTP/1.1
Content-Type: application/json
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.24.1
Accept: */*
Cache-Control: no-cache
Postman-Token: 4dd1c428-a4b7-4df9-94d7-7e29e4e0dd2d
Host: 10.8.159.34:6080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Tue, 12 May 2020 06:10:34 GMT
Content-type: application/json
Content-Length: 129
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"res_data": {"routing_table": "Management", "relay_hosts": []},
"res_message": "Data received successfully.", "res_code": "200"}
```

新しい SMTP リレーホストの追加

サンプル リクエスト

```
POST /wsa/api/v2.0/configure/system/smtp
HTTP/1.1
Content-Type: application/json
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.24.1
Accept: */*
Cache-Control: no-cache
Postman-Token: 30ad35bc-253d-4787-8e18-4cdfa3ff3d1f
Host: 10.8.159.34:6080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 549

{
  "routing_table": "management",
  "relay_hosts": [
    {
```

```

        "host": "191.10.55.255"
      },
      {
        "host": "10.10.55.8",
        "port": "3"
      },
      {
        "host": "google1.com",
        "port": "13"
      },
      {
        "host": "ggtalk.com",
        "port": "11"
      },
      {
        "host": "google.com",
        "port": "35"
      },
      {
        "host": "google.com",
        "port": "37"
      }
    ]
  }
}

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Tue, 12 May 2020 07:08:30 GMT
Content-type: application/json
Content-Length: 215
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"res_data": {"add_failure": [], "add_success": ["10.10.55.8:3", "191.10.55.255:25",
"ggtalk.com:11", "google1.com:13", "google.com:37", "google.com:35"]},
"res_message": "Success:6, Failure: 0.", "res_code": "201"}

```

SMTP リレーホストの詳細の変更

サンプル リクエスト

```

PUT /wsa/api/v2.0/configure/system/smtp
HTTP/1.1
Content-Type: application/json
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.24.1
Accept: */*
Cache-Control: no-cache
Postman-Token: 8c18cbba-8ff3-4993-a5f3-5562fd854fde
Host: 10.8.159.34:6080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 537

{
  "routing_table": "management",
  "relay_hosts": [

```

```

    {
      "old_host": "google.com",
      "old_port": "35",
      "new_host": "google.com",
      "new_port": "37"
    },
    {
      "old_host": "ggtalk.com",
      "old_port": "11",
      "new_host": "10.10.194.12",
      "new_port": "23"
    },
    {
      "old_host": "10.10.194.12",
      "old_port": "28",
      "new_host": "10.10.194.12",
      "new_port": "27"
    }
  ]
}

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Tue, 12 May 2020 07:09:47 GMT
Content-type: application/json
Content-Length: 450
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"res_data": {"update_success": [{"relay_host_old": "ggtalk.com:11",
"relay_host_new": "10.10.194.12:23"}], "update_failure": [{"relay_host_old":
"google.com:35", "relay_host_new": "google.com:37", "err_message":
"Given new host or port is already exist."}, {"relay_host_old":
"10.10.194.12:28", "relay_host_new": "10.10.194.12:27", "err_message":
"Given old host or port is not found."}]}, "res_message": "Success:1,
Failure: 2.", "res_code": "201"}

```

複数の SMTP リレーホストの削除

サンプル リクエスト

```

DELETE /wsa/api/v2.0/configure/system/smtp
HTTP/1.1
Content-Type: application/json
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.24.1
Accept: */*
Cache-Control: no-cache
Postman-Token: 282c385c-1804-4cd7-be25-5b62a923e175
Host: 10.8.159.34:6080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 132

```

```

[
  {
    "host": "10.10.194.12",

```

```

        "port": "23"
      },
      {
        "host": "google.com",
        "port": "37"
      }
    ]
  }
}

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Tue, 12 May 2020 07:14:00 GMT
Content-type: application/json
Content-Length: 150
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"res_data": {"delete_success": ["10.10.194.12:23", "google.com:37"],
"delete_failure": []}, "res_message": "Success:2,
Failure:0", "res_code": "200"}

```

すべての SMTP リレーホストの削除

サンプル リクエスト

```

DELETE /wsa/api/v2.0/configure/system/smtp HTTP/1.1
Content-Type: application/json
Authorization: Basic YWRtaW46aXJvbnBvcnQ=
User-Agent: PostmanRuntime/7.24.1
Accept: */*
Cache-Control: no-cache
Postman-Token: c1514e19-b401-499d-9b29-47ada4f6981e
Host: 10.8.159.34:6080
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 22

{
  "delete_all":true
}

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Tue, 12 May 2020 07:35:12 GMT
Content-type: application/json
Content-Length: 68
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"res_message": "Successfully deleted all hosts", "res_code": "200"}

```

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 /wsa/api/v2.0/login/privileges HTTP/1.1
cache-control: no-cache
Postman-Token: 0cd8d318-e29b-40e0-bdc8-473f09cbd2b2
Authorization: Basic YWRtaW46aXJybnBvcnQ=
User-Agent: PostmanRuntime/7.6.0
Accept: */*
Host: pod1224-wsa04.ibwsa.sgg.cisco.com:6080
accept-encoding: gzip, deflate
Connection: keep-alive
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Sat, 11 Apr 2020 07:35:16 GMT
Content-type: application/json
Content-Length: 2342
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"data": ["w_preferences_preferences", "w_config_user_dashboard", "w_config_cpu_threshold",
"w_config_memory_threshold", "config_detail", "w_reporting_web_webcat_detail",
"w_reporting_web_ytcat_detail", "w_reporting_domains", "w_reporting_web_user_detail",
"w_reporting_web_application_type_detail", "w_reporting_web_malware_category",
"w_reporting_web_user_by_traffic_monitor", "w_reporting_web_amp_detail_by_filename",
"w_reporting_web_wbrs_score_detail",
"w_reporting_web_malware_name_malware_category_detail",
"w_reporting_web_application_name_application_type_detail", "w_reporting_web_port_detail",
"w_reporting_web_host_by_traffic_monitor", "w_reporting_web_amp_summary",
"w_reporting_web_amp_detail_summary", "w_reporting_web_amp_file_analysis_by_filename",
"w_reporting_web_wbrs_threat_type_detail", "w_reporting_users_by_app_type",
"w_reporting_web_socks_destinations", "w_reporting_web_user_application_detail",
"w_reporting_web_socks_users", "w_reporting_users_by_category",
"w_reporting_web_services_summary",
"w_reporting_web_application_type_application_name_detail",
"w_reporting_web_user_webcat_detail",
"w_reporting_web_user_amp_detail",
"w_reporting_web_user_malware_name_malware_category_detail",
"w_reporting_policy_by_user", "w_reporting_web_malware_category_malware_name_detail",
"w_reporting_web_users_by_sha_detail",
"w_reporting_web_malware_category_malware_name_user_detail",
"w_reporting_web_filenames_by_sha", "w_reporting_web_amp_reputation_update",
"w_reporting_users_by_app", "w_reporting_web_application_name_detail",
```

```
"w_reporting_web_application_name_application_behavior_detail",
"w_reporting_web_transaction",
"w_reporting_web_transaction_type", "w_reporting_web_cipher_detail_client",
"w_reporting_web_cipher_detail_server", "w_reporting_web_reporting_system",
"w_percent_cpu_utilized",
"w_percent_ram_utilized", "w_percent_disk_utilized", "w_system_uptime", "w_alerts",
"w_disk_usage",
"w_raid_status", "w_proxy_cpu_usage", "w_proxy_disk_io_util", "w_proxy_status",
"w_high_availability",
"w_proxy_traffic_characteristics", "w_system_cpu_usage", "w_system_memory_usage",
"w_bandwidth",
"w_rps", "w_cpu_usage_by_function", "w_server_connection", "w_client_connection",
"w_bandwidth_count",
"w_rps_count", "w_decryption_count", "w_services", "w_web_tracking_web_transaction",
"ctr_token",
"ctr_client_info"]}]}
```

SecureX ファイルの取得

登録ユーザーの詳細を取得できます。

概要	GET /wsa/api/v2.0/ctr/user_info	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、登録ユーザーのユーザー情報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/wsa/api/v2.0/ctr/user_info
```

```
HTTP/1.1
```

サンプル応答

```
HTTP/1.1
```

```
Response
```

```
HTTP/1.1 200 OK
```

```
Date: Thu, 25 Mar 2021 07:48:19 GMT
```

```
Content-type: application/json
```

```
Content-Length: 92
```

```
Connection: close
```

```
Access-Control-Allow-Origin: *
```

```
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
```


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

例

次に、SecureX の登録ユーザーの詳細を変更する例を示します。

サンプル リクエスト

```
PUT /wsa/api/v2.0/ctr/user_info
```

```
HTTP/1.1
```

サンプル応答

```
HTTP/1.1 200 OK
```

```
Date: Thu, 25 Mar 2021 07:48:19 GMT
Content-type: application/json
Content-Length: 92
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{"data":{"client_id":"Y2xpZW50LWY2NzQzNjdlLTJhOTMtNDI3Yy05MGVmLWJjZmFhMGVhY2RjNA==",
"client_secret":"QmlHbGlpeFlENXNzQWVkb0RlNFprSTdzaDVGaVc5OEJMYVhEWkcydlBtWWJnR3Bud0pVZUF3",
"server":"YXBqYw=="}}
}
```

SecureX のユーザー情報詳細の追加

SecureX のユーザー情報の詳細を追加できます。この操作で SecureX リボンにログインできます。

概要	POST /wsa/api/v2.0/ctr/user_info	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、ユーザー情報を作成する例を示します。

サンプル リクエスト

HTTP/1.1

```
{
  "data": {
    "client_id": "Y2xpZW50LWY2NzQzNjdLTJhOTMtNDI3Yy05MGVmLWJjZmFhMGVhY2RjNA==",
    "client_secret": "MFVTTs05cERieVh0RDF5RGE2dzZvMnlJTWtwNkZleFU2YnJIY1VkcWlwdzZ0MlpNMTVVGWGNn",
    "server": "YXBqYw=="
  }
}
```

サンプル応答

HTTP/1.1 200 OK

```
Date: Thu, 25 Mar 2021 07:32:19 GMT
Content-type: application/json
Content-Length: 32
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
OK
```

認証設定の取得

Secure Web Appliance の現在の認証関連の設定に関する基本情報を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/generic_resources/auth_settings	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスの認証設定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 /wsa/api/v3.0/generic_resources/auth_settings
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 1339
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "header_based_auth": "disable",
  "realms": [
    {
      "schemes": [
        "Basic"
      ],
      "type": "LDAP",
      "name": "AuthLDAP",
      "supportes_tui": false
    },
    {
      "schemes": [
        "Basic"
      ],
      "type": "LDAP",
      "name": "AuthLDAPTUI",
      "supportes_tui": true
    },
    {
      "schemes": [
        "Kerberos",
        "NTLMSSP",
        "Basic",
        "Header"
      ],
      "type": "AD",
      "name": "AuthADTUI",
      "supportes_tui": true
    },
    {
      "schemes": [
        "Kerberos",
        "NTLMSSP",
        "Basic",
        "Header"
      ],
      "type": "AD",
      "name": "AuthAD",
      "supportes_tui": false
    }
  ],
  "sequences": [
    {
      "schemes": [
        "NTLMSSP",
```

```

        "Basic",
        "Header",
        "Kerberos"
    ],
    "name": "All Realms"
  },
  {
    "schemes": [
      "Basic",
      "Header",
      "Kerberos"
    ],
    "name": "myAuthSequence"
  }
]
}

```

ユーザーエージェントの取得

Secure Web Appliance によって認識される、許可されたすべてのユーザーエージェントを取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/generic_resources/user_agents	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスによって認識されるすべてのユーザーエージェント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 /wsa/api/v3.0/generic_resources/user_agents
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 616
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email

```

```
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "user_agents": [
    "Chrome/48",
    "windows_updater",
    "Firefox/40",
    "Firefox/41",
    "Firefox/42",
    "Firefox/43",
    "Chrome/45",
    "Chrome/46",
    "Chrome/47",
    "Chrome",
    "Safari",
    "adobe_updater",
    "MSIE",
    "Safari/5",
    "Safari/4",
    "Safari/7",
    "Safari/6",
    "Opera",
    "Safari/9",
    "Safari/8",
    "MSIE/11",
    "MSIE/10",
    "Firefox",
    "MSIE/9",
    "MSIE/8",
    "Opera/33",
    "Opera/32",
    "Opera/35",
    "Opera/34"
  ]
}
```

URL カテゴリの取得

Cisco Secure Web Appliance によって定義された、許可されたすべての URL カテゴリを取得できます。この API には、いくつかのユーザー定義のカテゴリも含まれています。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/generic_resources/url_categories	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスで設定されているすべての URL カテゴリ（事前定義およびカスタム）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 /wsa/api/v3.0/generic_resources/url_categories
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 2316
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "predefined": [
    "Adult",
    "Advertisements",
    "Alcohol",
    "Arts",
    "Astrology",
    "Auctions",
    "Business and Industry",
    "Chat and Instant Messaging",
    "Cheating and Plagiarism",
    "Child Abuse Content",
    "Computer Security",
    "Computers and Internet",
    "DIY Projects",
    "Dating",
    "Digital Postcards",
    "Dining and Drinking",
    "Dynamic and Residential",
    "Education",
    "Entertainment",
    "Extreme",
    "Fashion",
    "File Transfer Services",
    "Filter Avoidance",
    "Finance",
    "Freeware and Shareware",
    "Gambling",
    "Games",
    "Government and Law",
    "Hacking",
    "Hate Speech",
    "Health and Nutrition",
    "Humor",
    "Hunting",
    "Illegal Activities",
    "Illegal Downloads",
    "Illegal Drugs",
```

```

    "Infrastructure and Content Delivery Networks",
    "Internet Telephony",
    "Job Search",
    "Lingerie and Swimsuits",
    "Lotteries",
    "Military",
    "Mobile Phones",
    "Nature",
    "News",
    "Non-governmental Organizations",
    "Non-sexual Nudity",
    "Online Communities",
    "Online Meetings",
    "Online Storage and Backup",
    "Online Trading",
    "Organizational Email",
    "Paranormal",
    "Parked Domains",
    "Peer File Transfer",
    "Personal Sites",
    "Personal VPN",
    "Photo Search and Images",
    "Politics",
    "Pornography",
    "Professional Networking",
    "Real Estate",
    "Reference",
    "Religion",
    "SaaS and B2B",
    "Safe for Kids",
    "Science and Technology",
    "Search Engines and Portals",
    "Sex Education",
    "Shopping",
    "Social Networking",
    "Social Science",
    "Society and Culture",
    "Software Updates",
    "Sports and Recreation",
    "Streaming Audio",
    "Streaming Video",
    "Tobacco",
    "Transportation",
    "Travel",
    "Weapons",
    "Web Hosting",
    "Web Page Translation",
    "Web-based Email"
  ],
  "custom": [
    "mycategory",
    "mycategoryo365"
  ]
}

```

時間範囲の取得

Secure Web Appliance で設定されている時間範囲のリストを取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/web_security/time_ranges	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスの設定された時間範囲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 /wsa/api/v3.0/web_security/time_ranges
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 971
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken
```

```
{
  "time_ranges": [
    {
      "time_values": [
        {
          "time_of_day": "all_day",
          "valid_days": [
            "Saturday",
            "Friday",
            "Thursday",
            "Monday",
            "Tuesday",
            "Wednesday"
          ]
        }
      ],
      "name": "TestTimeRange",
      "time_zone": "America/Los_Angeles"
    },
    {
      "time_values": [
        {
          "time_of_day": {
```

```

        "to": "18:00",
        "from": "10:00"
      },
      "valid_days": [
        "Monday",
        "Sunday"
      ]
    }
  ],
  "name": "mytimerange",
  "time_zone": "Asia/Shanghai"
}
]
}

```

クォータの取得

Secure Web Appliance で設定されているクォータのリストを取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/web_security/quotas	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスの設定されたクォータ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 /wsa/api/v3.0/web_security/quotas
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzMjY28xMjMk

```

サンプル応答

```

HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 607
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true

```

```

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

{
  "quotas": [
    {
      "reset_time": "0:00",
      "volume_quota": 1073741824,
      "time_quota_secs": 0,
      "name": "myquota2",
      "time_zone": "America/Los_Angeles"
    },
    {
      "volume_quota": 0,
      "time_quota_secs": 54000,
      "name": "myquota",
      "time_range": "mytimerange"
    },
    {
      "reset_time": "0:00",
      "volume_quota": 60129542144,
      "time_quota_secs": 58560,
      "name": "myquota3",
      "time_zone": "America/Los_Angeles"
    }
  ]
}

```

プロキシ設定の取得

Secure Web Appliance のプロキシ（Web プロキシ、SOCKS プロキシなど）関連の設定を取得できます。応答では、特定のタイプのプロキシが有効かどうかを示されます。また、透過や転送などの、プロキシのモードに関する情報も提供されます（Web プロキシにのみ適用されます）。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/generic_resources/proxy_settings	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスのプロキシ（Web プロキシ、SOCKS プロキシなど）関連の設定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 /wsa/api/v3.0/generic_resources/proxy_settings
HTTP/1.1
Host: wsa.example.com:6443

```

```
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 207
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "proxy_settings": {
    "web": {
      "status": "enable",
      "mode": "transparent"
    },
    "socks": "disable",
    "https": "enable",
    "ftp": "enable"
  }
}
```

識別方法の取得

識別プロファイルの作成中に使用できる、許可された識別方法と許可されていない識別方法の情報を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/generic_resources/identification_methods	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスで設定された識別方法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 /wsa/api/v3.0/generic_resources/identification_methods
HTTP/1.1
Host: wsa.example.com:6443
User-Agent: curl/7.55.1
Accept: */*
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

サンプル応答

```
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 08:22:28 GMT
Content-type: application/json
Content-Length: 154
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
  "identification_methods": {
    "tui": "disable",
    "authentication": "enable",
    "asa": "enable",
    "ise": "disable"
  }
}
```

ADC の詳細の取得

バージョン、アプリケーション、カテゴリ、アクティビティの正規表現、アプリケーションドメインなどの ADC の詳細を取得できます。次に、構文とサポート対象の属性を示します。

概要	GET /wsa/api/v3.0/web_security/adc	
サポート対象のリソース属性	詳細については、『 AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance 』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

次に、デバイスで設定された識別方法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 /wsa/api/v3.0/web_security/adc
HTTP/1.1
Content-Type: application/json
Host: localhost:60001
User-Agent: curl/7.74.0
Accept: */*
```

サンプル応答

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Thu, 21 Sep 2023 06:07:18 GMT
```

```

Content-type: application/json
Content-Length: 336888
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, PUT, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken
{
  "adc_version": [
    "Cisco Web Usage Controls - Application Discovery and Control Data: 1693557522
(Fri Sep 01 08:55:20 2023)"
  ],
  "adc_apps": {
    "737280": {
      "possible_action": [
        "block",
        "monitor"
      ],
      "name": "Zucks",
      "cat_name": "Ad Publishing"
    },
    "1": {
      "possible_action": [
        "block",
        "monitor"
      ],
      "name": "1&1 IONOS Web Hosting",
      "cat_name": "Hosting Services"
    },
    "540676": {
      "possible_action": [
        "block",
        "monitor"
      ],
      "name": "Webkinz",
      "cat_name": "Games"
    }
  },
  "adc_categories": {
    "Marketing & Sales": {
      "possible_action": [
        "block",
        "monitor"
      ]
    },
    "Media": {
      "possible_action": [
        "block",
        "monitor"
      ]
    },
    "Travel": {
      "possible_action": [
        "block",
        "monitor"
      ]
    },
    "Human Resources": {
      "possible_action": [
        "block",
        "monitor"
      ]
    }
  },

```

```

    "Service Management": {
      "possible_action": [
        "block",
        "monitor"
      ]
    }
  },
  "adc_activity_regexes": {
    "5000064": [
      "download\\.wettransfer\\.com\/.*"
    ],
    "5000065": [
      "photos\\.smugmug\\.com\/.*\/.*\/.*\/.*\/.*\/D\/.*-D\\..*",
      "photos\\.smugmug\\.com\/.*\/.*\/.*\/.*\/.*\/.*\/.*D\/.*D\\..*",
      "photos\\.smugmug\\.com\/photos\/.*\/.*\/.*\/.*\/.*-D\\..*",
      "photos\\.smugmug\\.com\/photos\/.*\/.*\/.*\/.*D\/.*D\\..*",
      "secure\\.smugmug\\.com\/archive\/.*",
      "photos\\.smugmug\\.com\/Folder\/.*\/.*\/.*\/.*D\/.*-D\\..*",
      "www\\.smugmug\\.com\/api\/.*\/album\/.*!download",
      "api\\.smugmug\\.com\/api\/.*\/album\/.*!download"
    ],
    "5000077": [
      "i\\.instagram\\.com\/upload_igphoto\/.*",
      ".\\.instagram\\.com\/accounts\/web_change_profile_picture",
      "i\\.instagram\\.com\/upload_igvideo\/.*"
    ],
    "5000078": [
      "www\\.linkedin\\.cn\/dms-uploads\/.*\/profile.*uploadedImage\/.*",
      "www\\.linkedin\\.com\/dms-uploads\/.*\/.*"
    ],
    "5000079": [
      "upload\\.twitter\\.com\/i\/media\/upload.*\\.json"
    ]
  },
  "adc_app_domains": {
    "737280": [
      "s.side3.zucks.net",
      "zimg.jp",
      "zucks.co.jp",
      "zucks.net"
    ],
    "540676": [
      "webkinz.com"
    ],
    "438273": [
      "admin.privacy.com",
      "dashboard.privacy.com",
      "privacy.com",
      "privymktg.com"
    ],
    "11": [
      "4sharedapi.com",
      "4shared.com",
      "api.4sharedapi.com",
      "api.4shared.com",
      "e.4shared.com",
      "epomads2.4shared.com",
      "search.4shared.com",
      "static.4shared.com",
      "upload.4shared.com",
      "webdav.4shared.com"
    ],
    "901132": [
      "flowplay.com"
    ]
  }
}

```

```
}
```

正常性チェック API

これらの API は、外部 DLP サーバーの接続、ネットワークインターフェイスとゲートウェイ、NTP サービス、DNS 探索、およびシステムの正常性メトリックの監視とトラブルシューティングに役立ちます。

これらの API でサポートされているリソース属性については、『[AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance](#)』を参照してください。



重要 正常性チェック API は、REST API v3.0 エンドポイントでのみサポートされています。

外部 DLP サーバーの正常性チェック

概要

```
GET /wsa/api/v3.0/diagnostic/health_check/external_dlp_api
```

例

次の例では、設定済みのすべての外部 DLP サーバーをテストします。

サンプル リクエスト

```
GET /wsa/api/v3.0/diagnostic/health_check/external_dlp_api
```

サンプル応答

```
{
  "res_data": {
    "total_servers": 2,
    "results": [
      {
        "message": "Trying connect to host: 10.10.36.163.\r\nIP Address is: 10.10.36.163.\r\nICAP OPTION success! Response Time <0.26> seconds.\r\n\nSuccess: Connection to server was successful.",
        "server_info": {
          "url": "icap://10.10.36.163/dlp",
          "host": "10.10.36.163",
          "port": 1344
        },
        "server_index": 1,
        "return_code": 0
      },
      {
        "message": "Trying connect to host: 10.10.36.163.\r\nIP Address is: 10.10.36.163.\r\nICAP OPTION success! Response Time <0.22> seconds.\r\n\nSuccess: Connection to server was successful.",
        "server_info": {
```

```

        "url": "icap://10.10.36.163/dlp",
        "host": "10.10.36.163",
        "port": 1345
      },
      "server_index": 2,
      "return_code": 0
    }
  ]
},
"res_message": "Data received successfully.",
"res_code": 200
}

```

次の例では、設定済みの最初の外部 DLP サーバーをテストします。

サンプル リクエスト

```
GET /wsa/api/v3.0/diagnostic/health_check/external_dlp_api?index=1
```

サンプル応答

```

{
  "res_data": {
    "message": "Trying connect to host: 10.10.36.163.\r\nIP Address is:
10.10.36.163.\r\nICAP OPTION success! Response Time <0.26> seconds.\r\n\nSuccess:
Connection to server was successful.",
    "server_info": {
      "url": "icap://10.10.36.163/dlp",
      "host": "10.10.36.163",
      "port": 1344
    },
    "server_index": 1,
    "return_code": 0
  },
  "res_message": "Data received successfully.",
  "res_code": 200
}

```

ネットワーク インターフェイスとゲートウェイの正常性チェック

概要

```
GET /wsa/api/v3.0/diagnostic/health_check/network_interface_api
```

例

次の例では、すべてのインターフェイスと特定のインターフェイスをテストします。

サンプルリクエスト

```

GET /wsa/api/v3.0/diagnostic/health_check/network_interface_api
GET /wsa/api/v3.0/diagnostic/health_check/network_interface_api?interface=Management
GET /wsa/api/v3.0/diagnostic/health_check/network_interface_api?interface=P1

```

すべてのインターフェイスのサンプル応答

```

{
  "res_data": {
    "results": [
      {
        "ping_version": "v4",

```

```

    "source_ip": "10.10.194.89",
    "route_name": "defaultrouter",
    "ping_result": {
      "ping_statistics": {
        "packets_transmitted": 3,
        "packets_received": 3,
        "packet_loss": "0.0%",
        "round_trip_times": {"min": 0.313, "avg": 0.355, "max": 0.376, "stddev":
0.03}
      },
      "source_ip": "10.10.194.89",
      "target_ip": "10.10.194.1",
      "connection_result": "Success",
      "return_code": 0,
      "raw_output": "PING 10.10.194.1 (10.10.194.1) from 10.10.194.89: ..."
    },
    "test_status": "completed",
    "interface_name": "Management",
    "gateway": "10.10.194.1"
  },
  {
    "ping_version": "v6",
    "source_ip": "2001:420:5440:2005:710:0:3:59",
    "route_name": "defaultrouter",
    "ping_result": {
      "ping_statistics": {
        "packets_transmitted": 3,
        "packets_received": 3,
        "packet_loss": "0.0%",
        "round_trip_times": {"min": 0.373, "avg": 0.401, "max": 0.423, "stddev":
0.021}
      },
      "source_ip": "2001:420:5440:2005:710:0:3:59",
      "target_ip": "2001:420:5440:2005:710:0:3:1",
      "connection_result": "Success",
      "return_code": 0,
      "raw_output": "PING6(56=40+8+8 bytes) ..."
    },
    "test_status": "completed",
    "interface_name": "Management",
    "gateway": "2001:420:5440:2005:710:0:3:1"
  }
],
[
  {
    "ping_version": "v4",
    "interface_name": "P1",
    "gateway": "10.10.117.129",
    "test_status": "completed",
    "ping_result": {"connection_result": "Success", "return_code": 0, "...": "..."}
  }
],
[
  {"ping_version": "v4", "interface_name": "P2", "test_status": "not_configured"}
]
],
"res_message": "Data received successfully.",
"res_code": 200
}

```

管理インターフェイスのサンプル応答

```
{
  "res_data": {
    "interface": "Management",
    "result": [
      {
        "ping_version": "v4",
        "source_ip": "10.10.194.89",
        "route_name": "defaultrouter",
        "ping_result": {
          "ping_statistics": {
            "packets_transmitted": 3,
            "packets_received": 3,
            "packet_loss": "0.0%",
            "round_trip_times": {"min": 0.313, "avg": 0.355, "max": 0.376, "stddev":
0.03}
          },
          "source_ip": "10.10.194.89",
          "target_ip": "10.10.194.1",
          "connection_result": "Success",
          "return_code": 0,
          "raw_output": "...",
        },
        "test_status": "completed",
        "interface_name": "Management",
        "gateway": "10.10.194.1"
      }
    ]
  },
  "res_message": "Data received successfully.",
  "res_code": 200
}
```

NTP サービスの正常性チェック

概要

GET /wsa/api/v3.0/diagnostic/health_check/ntp_health_check_api

例

サンプル リクエスト

GET /wsa/api/v3.0/diagnostic/health_check/ntp_health_check_api

正常な NTP サービスのサンプル応答

```
{
  "res_data": {
    "results": [
      {
        "service_name": "sntpd",
        "enabled": true,
        "process_running": true,
        "ready": true,
        "process_id": 41625,
        "ignore_flag": false,
        "status": "Healthy",
        "last_started": "Info: sntpd: started PID=41625 on Thu Jan 9 06:23:13 2025",
        "time_const_adjustments": ["No Time change detected"],
        "errors_warnings": ["No Errors"],
        "heimdall_return_code": 0
      }
    ]
  }
}
```

```

    }
  ],
  "res_message": "Data received successfully.",
  "res_code": 200
}

```

異常な NTP サービスのサンプル応答

```

{
  "res_data": {
    "results": [
      {
        "service_name": "sntpd",
        "enabled": true,
        "process_running": false,
        "ready": false,
        "process_id": "N/A",
        "ignore_flag": false,
        "status": "Not Healthy",
        "last_started": "No sntpd started entry found",
        "time_const_adjustments": ["No Time change detected"],
        "errors_warnings": [
          "Warning: sntpd: process not responding",
          "Error: sntpd: failed to bind NTP port"
        ],
        "heimdall_return_code": 1
      }
    ]
  },
  "res_message": "Data received successfully.",
  "res_code": 200
}

```

DNS 探索の正常性チェック

API は、google.com、cisco.com、example.com、および yahoo.com の正引きルックアップを実行します。8.8.8.8 および 1.1.1.1 の逆引きルックアップを実行します。アプライアンスでインターネットのルート DNS サーバーを使用するように設定されている場合、この API はそれらのサーバーもサポートします。

概要

```
GET /wsa/api/v3.0/diagnostic/health_check/dns_lookup_api
```

例

サンプルリクエスト

```

GET /wsa/api/v3.0/diagnostic/health_check/dns_lookup_api
GET /wsa/api/v3.0/diagnostic/health_check/dns_lookup_api?server=primary
GET /wsa/api/v3.0/diagnostic/health_check/dns_lookup_api?server=alternate
GET /wsa/api/v3.0/diagnostic/health_check/dns_lookup_api?server=secondary

```

すべてのサーバーのサンプル応答

```

{
  "res_data": {
    "results": [
      [

```

```

{
  "server_name": "primary",
  "test_type": "forward_lookup",
  "dns_server_ip": "192.168.0.252",
  "test_domain": "google.com",
  "dns_result": {
    "dns_server": "192.168.0.252",
    "test_domain": "google.com",
    "server_info": {"authoritative": false, "server_ip": "192.168.0.252",
"server_responsive": true},
    "resolved_ips": ["172.217.24.174", "142.250.183.142",
"2404:6800:4007:805::200e"],
    "resolution_result": "Success",
    "return_code": 0,
    "response_time_ms": 0.0,
    "raw_output": "Server: 192.168.0.252\nAddress:
192.168.0.252#53\n\nNon-authoritative answer:\nName:\tgoogle.com\nAddress:
172.217.24.174\n..."
  },
  "test_status": "completed"
},
{
  "server_name": "primary",
  "test_type": "reverse_lookup",
  "test_ip": "8.8.8.8",
  "dns_server_ip": "192.168.0.252",
  "dns_result": {
    "dns_server": "192.168.0.252",
    "resolution_result": "Success",
    "return_code": 0,
    "test_ip": "8.8.8.8",
    "resolved_hostname": "dns.google",
    "raw_output": "8.8.8.8.in-addr.arpa\tname = dns.google.\n..."
  },
  "test_status": "completed"
}
],
[
{
  "server_name": "alternate",
  "test_type": "forward_lookup",
  "dns_server_ip": "1.2.3.1",
  "test_domain": "google.com",
  "dns_result": {
    "dns_server": "1.2.3.1",
    "resolution_result": "Failed",
    "return_code": 3,
    "resolved_ips": [],
    "response_time_ms": 0.0,
    "raw_output": ";; communications error to 1.2.3.1#53: timed out\n..."
  },
  "test_status": "completed"
}
],
[
{
  "server_name": "secondary",
  "test_type": "configuration_check",
  "dns_result": {
    "resolution_result": "Not Configured",
    "return_code": 10,
    "error_message": "secondary DNS server not configured"
  },
  "test_status": "not_configured"
}
]

```

```

    }
  ]
},
"res_message": "Data received successfully.",
"res_code": 200
}

```

プライマリサーバーのサンプル応答

```

{
  "res_data": {
    "server": "primary",
    "result": [
      {
        "server_name": "primary",
        "test_type": "forward_lookup",
        "dns_server_ip": "192.168.0.252",
        "test_domain": "google.com",
        "dns_result": {"resolution_result": "Success", "return_code": 0, "resolved_ips":
["172.217.24.174"], "...": "..."},
        "test_status": "completed"
      },
      {
        "server_name": "primary",
        "test_type": "forward_lookup",
        "dns_server_ip": "192.168.0.252",
        "test_domain": "cisco.com",
        "dns_result": {"resolution_result": "Success", "return_code": 0, "...": "..."},
        "test_status": "completed"
      }
    ]
  },
  "res_message": "Data received successfully.",
  "res_code": 200
}

```

システムヘルスのチェック

概要

GET /wsa/api/v3.0/diagnostic/health_check/system_health_check_api

例

サンプルリクエスト

```

GET /wsa/api/v3.0/diagnostic/health_check/system_health_check_api
GET /wsa/api/v3.0/diagnostic/health_check/system_health_check_api?index=0
GET /wsa/api/v3.0/diagnostic/health_check/system_health_check_api?index=0,2,4

```

サンプル応答

```

{
  "res_data": {
    "timestamp": "2026-06-11T16:33:02.083538",
    "total_metrics_collected": 8,
    "total_errors": 0,
    "system_health_metrics": {
      "ram_utilization": {"index": 0, "status": "success", "return_code": 0, "data":
[{"memory_utilization": 11.7}]},
      "disk_utilization": {"index": 1, "status": "success", "return_code": 0, "data":

```

```

[{"disk_utilization": "4.3"}],
  "proxy_cpu_usage": {"index": 2, "status": "success", "return_code": 0, "data":
[{"proxy_cpu_usage": 0.0}]},
  "disk_usage": {"index": 3, "status": "success", "return_code": 0, "data":
[{"used_disk_space": 12123472, "total_disk_space": 281370640}]},
  "raid_status": {
    "index": 4,
    "status": "success",
    "return_code": 0,
    "final_status": "Optimal",
    "status_explanation": "RAID is operating normally.",
    "standard_raid_status": ["Optimal"],
    "direct_raid_status": "Optimal"
  },
  "proxy_bandwidth": {
    "index": 5,
    "status": "success",
    "return_code": 0,
    "data": [
      {"bandwidth_avg_start": 0.0},
      {"bandwidth_max_start": 0.0},
      {"bandwidth_max_hour": 0.0},
      {"bandwidth_avg_minute": 0.0},
      {"bandwidth_avg_hour": 0.0}
    ]
  },
  "proxy_connection_details": {
    "index": 6,
    "status": "success",
    "return_code": 0,
    "data": [
      {"current_total_server_conn": 0},
      {"current_idle_server_conn": 0},
      {"current_total_client_conn": 0},
      {"current_idle_client_conn": 0}
    ]
  },
  "_metadata": {
    "available_metrics": [
      {"index": 0, "name": "ram_utilization", "description": "RAM utilization
percentage"},
      {"index": 1, "name": "disk_utilization", "description": "Disk utilization
percentage"},
      {"index": 2, "name": "proxy_cpu_usage", "description": "Proxy CPU usage
percentage"},
      {"index": 3, "name": "disk_usage", "description": "Disk usage: used and total
space"},
      {"index": 4, "name": "raid_status", "description": "RAID status information"},
      {"index": 5, "name": "proxy_bandwidth", "description": "Proxy bandwidth
statistics"},
      {"index": 6, "name": "proxy_connection_details", "description": "Proxy connection
details"}
    ],
    "total_available_metrics": 7,
    "total_requested_metrics": 7,
    "requested_indices": [0, 1, 2, 3, 4, 5, 6]
  }
},
"res_message": "Data received successfully.",
"res_code": 200
}

```

エラー応答

無効なインデックスを指定すると、HTTP ステータスコード 200 と次の応答が返されます。

```
{
  "error": true,
  "error_message": "Invalid index values: 9. Valid indices are 0-6",
  "error_code": "INVALID_INDEX",
  "valid_indices": [0, 1, 2, 3, 4, 5, 6],
  "available_metrics": ["..."],
  "timestamp": "2026-06-11T16:33:02.083538"
}
```

v2.0 エンドポイントへのリクエストでは、HTTP ステータスコード 404 と次の応答が返されます。

```
{"status": "error", "message": "System Health Check API is available only under v3.0 endpoint."}
```




第 4 章

AsyncOS API のトラブルシューティング

- [API ログ, on page 213](#)
- [アラート, on page 213](#)

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、API ログを有効にして登録します。手順については、『[User Guide for Cisco Secure Web Appliance](#)』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アプライアンス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

翻訳について

このドキュメントは、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。