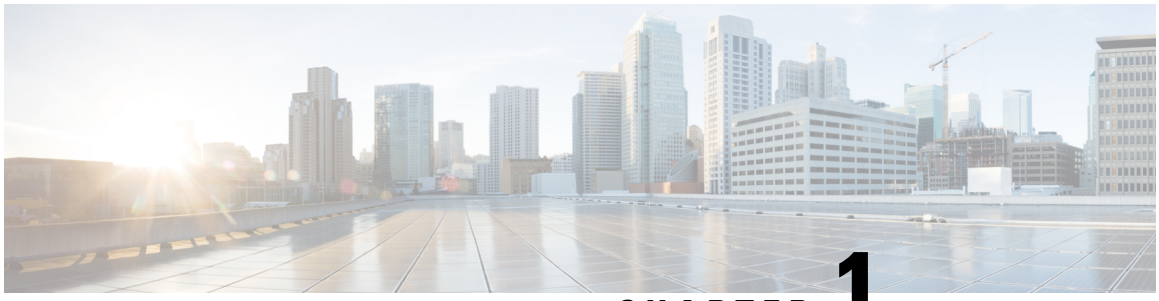
AsyncOS API 14.6 for Cisco Secure Web Appliance with Hybrid SWG–Getting Started Guide

First Published: 2023-05-11

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

CONTENTS



CHAPTER 1

Overview of AsyncOS API for Cisco Secure Web Appliance

The AsyncOS API for Cisco Secure Web Appliance (or AsyncOS API) is a representational state transfer (REST) based set of operations that provide secure and authenticated access to the Secure Web Appliance reports, report counters, and tracking. You can retrieve the Secure Web Appliance reporting and tracking data using the API. In this release you can query for configuration information.

Note You can configure Secure Web Appliance using Cisco Content Security Management appliance and REST APIs. If you use both these methods to configure the Secure Web Appliance, configurations done by the previous method are overwritten.

This chapter contains the following sections:

Prerequisites for Using AsyncOS API

To use AsyncOS API, you must have knowledge of:

- HTTP, which is the protocol used for API transactions. Secure communication over TLS.
- JavaScript Object Notation (JSON), which the API uses to construct resource representations.
- JSON Web Token (JWT).
- A client or programming library that initiates requests and receives responses from the AsyncOS API using HTTP or HTTPS, for example, cURL. The client or programming library must support JSON to interpret the response from the API.
- Authorization to access the AsyncOS API. See Authorization, on page 4.

- AsyncOS API enabled using web interface or CLI. See Enabling AsyncOS API, on page 2.

Enabling AsyncOS API

Before You Begin

Ensure you have access to the `interfaceconfig` command in the CLI. Access to the CLI is restricted only to authorized personnel, who are administrators, email administrators, cloud administrators, and operators.

You can enable the AsyncOS API using the `interfaceconfig` command in the CLI.

Step 1 Log in to the CLI and run the `interfaceconfig` command.

Step 2 Choose the interface that you want to edit.

Step 3 Answer the following questions to enable AsyncOS API (monitoring) HTTP:

- `Do you want to enable AsyncOS API (monitoring) HTTP on this interface? [Y]>` Enter Y.
- `Which port do you want to use for AsyncOS API (monitoring) HTTP?[6080]>` Enter the default port 6080 or the port you want to define.

Step 4 Answer the following questions to enable AsyncOS API (monitoring) HTTPS:

- `Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [Y]>` Enter Y.
- `Which port do you want to use for AsyncOS API (Monitoring) HTTPS?[6443]>` Enter the default port 6443 or the port you want to define.

Note AsyncOS API communicates using HTTP / 1.1.

If you have selected HTTPS and want to use your own certificate for secure communication, see Securely Communicating with AsyncOS API, on page 2.

Note We recommend that you always use HTTPS in the production environment. Use HTTP only for troubleshooting and testing the API.

Step 5 Submit and commit the changes.

Securely Communicating with AsyncOS API

You can communicate with AsyncOS API over secure HTTP using your own certificate.

Note Do not perform this procedure if you are already running the web interface over HTTPS and using your own certificate for secure communication. AsyncOS API uses the same certificate as the web interface for communicating over HTTPS.

Step 1 Set up a certificate using the `certconfig` command in the CLI. For instructions, refer the User Guide or Online Help.

Step 2 Change the HTTPS certificate used by the IP interface to your certificate using the `interfaceconfig` command in CLI. For instructions, refer the User Guide or Online Help.

Step 3 Submit and commit your changes.

AsyncOS API Authentication and Authorization

This section explains the authentication methods, the user roles that can access APIs, and how to query for APIs accessible to a user.

- Authentication, on page 3
- Authorization, on page 4

Authentication

You can authenticate queries to the API using either of the following two methods:

- Submit the Secure Web Appliance's username and password with all the requests to the API, in the Base64-encoded format.
- Use a JSON Web Token (JWT) in an API request with the token key in the header.

The user inactivity timeout settings in the appliance apply to the validity of a JWT. If a request does not include valid credentials in the authorization header, the API sends a 401 error message. You can use any base64 library to convert your credentials into a base64-encoded format.

Authenticating API Queries with JSON Web Token

You can generate a JWT and use it with your API queries.

Note The user inactivity timeout settings in the appliance apply to the validity of a JWT. The Secure Web Appliance checks every API query with a JWT, for its time validity. If a JWT is found to be within 5 minutes of time validity, after which it will time out, a new refresh JWT is sent with the response header. You must use this new refresh JWT with API queries or generate a new one.

Synopsis	`POST /wsa/api/v2.0/login`
	Use the syntax below for two factor authentications:
	`POST /wsa/api/v2.0/login/two_factor`

Body Parameters	Use Base64 encoded credentials.
	`{`
	`"data":`
	`{`
	`"userName":"YWRtaW4=",`
	`"passphrase":"aXJvbnBvcnQ="`
	`}`
	`}`

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

This example shows a query to log in with Base64 encoded credentials, and generate a JWT.

Sample Request

```
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="
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
Server: API/2.0
Date: Mon, 26 Nov 2018 07:22:47 GMT
Content-type: application/json
Content-Length: 618
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: content-type, jwttoken, mid, h, email
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS
Access-Control-Expose-Headers: Content-Disposition, jwtToken

{
    "data": {
        "userName": "admin",
        "is2FactorRedirectRequired": "false",
        "role": "Administrator",
        "email": [],
        "jwtToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyTmFtZSI6ImFkbWluIiwiaXM
         yRmFjdG9yQ2hlY2tSZXF1aXJlZCI6ZmFsc2UsImNvb2tpZSI6IlRucEZOVTFFWTNwTlZFMDlDanRMYVR
         oeENqdFpiV1J6VFVSQk5VMURNWGRpTWxGMVdUSnNlbGt5T0hWWk1qbDBUMnBaZDA5RVFUMEtcbk8xVkh
         PWHBrUnpGb1lteEtNV0p1VW5CaVYxVjJUbmswTUV4cVFUMEtPMVJVUlhkTlJsazNUVlJKZFUxRE5IZE1
         WRWw1VFdwek1FMXFcblNUVlNhazVDVDBWRk1rOUVaM2xTUlVreVRYcGtSazFwTVVSTlZFMHpUbFZXUjA1
    }
}
```

Authorization

The AsyncOS API is a role based system, the scope of API queries is defined by the role of the user. Cisco Secure Web Appliance users with the following roles can access the AsyncOS API:

- Administrator
- Operator
- Technician
- Read-Only Operator
- Guest
- Web Administrator
- Web Policy Administrator
- URL Filtering Administrator
- Email Administrator
- Help Desk User

Note

- Externally authenticated users can access the API.
- Custom roles, delegated by the administrator, can also access the APIs.
- Only users with administrative privileges can use the REST APIs to modify the configurations. All other users like Operator or Read-Only Operator are allowed to only view these configurations.

AsyncOS API Requests and Responses

Note For complete list of APIs, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

AsyncOS API Requests

Requests made to the API have the following characteristics:

- Requests are sent over HTTP or HTTPS.
- Each request must contain a valid URI in the following format:

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

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

  where:

  - `{appliance}:{port}`

    is the FQDN or the IP address of the appliance and the TCP port number on which the appliance is listening.
  - `{resource}`

is the resource you are attempting to access, for example, reports, tracking, quarantine, configuration, or other counters.

- `{resource_attributes}`

  are the supported attributes for a resource, for example, duration, and so on.

- Each request must contain user credentials, or a valid authorization header.
- Use the JSON Web Token (JWT) generated earler in the API request with the token key in the header. For more information, see Authenticating API Queries with JSON Web Token.
- Each request must be set to accept:

  ```
  application/json
  ```

- Requests sent over HTTPS (using your own certificate) must contain your CA certificate. For example, in case of cURL, you can specify the CA certificate in the API request as follows:

  ```
  curl --cacert <ca_cert.crt> -u"username:password"
  https://<fqdn>:<port>/wsa/api/v2.0/{resource}/{resource_attributes}
  ```

Note API requests are case sensitive and should be entered as shown in this guide.

AsyncOS API Responses

This section explains the key components of the responses and various HTTP error codes.

- Key Components of Responses, on page 6
- HTTP Response Codes, on page 7

Key Components of Responses

Components		Values	Description
Status Code and Reason		See HTTP Response Codes, on page 7.	HTTP response code and the reason.
Message Header	Content-Type	`application/json`	Indicates the format of the message body.
	Content-Length	n/a	The length of the response body in octets.
	Connection	`close`	Options that are desired for the connection.

Components	Values	Description

Message Body	n/a	The message body is in the format defined by the Content-Type header. The following are the components of the message body:
		1. URI. The URI you specified in the request to the API.
		Example
		`:"/api/v2.0/config/"`
		2. Counter group and/or counter name
		Example
		`reporting/mail_security_summary`
		3. Query parameters
		Example
		`startDate=2017-01-30T00:00:00.000Z&endDate=2018-01-30T14:00:00.000Z`
		4. Error (Only for Error Events). This component includes three subcomponents—message, code, and explanation.
		Example
		`"error": {"message": "Unexpected attribute - starts_with.","code": "404", "explanation": "404 = Nothing matches the given URI."}`
		If the message body contains empty braces ({}), it means that the API could not find any records matching the query.
		Note **totalCount** is the number of data objects that are returned in a dataset (for results that are displayed as table format in the UI). For other queries, it returns -1 by default.

HTTP Response Codes

These are the list of HTTP response codes returned by AsyncOS API:

- 200
- 202
- 300
- 301
- 307

- 400
- 401
- 403
- 404
- 406
- 413
- 414
- 500
- 501
- 503
- 505

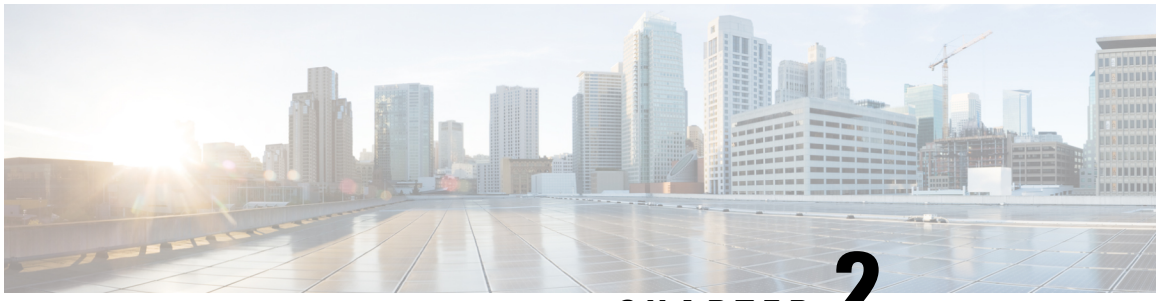
For descriptions of these HTTP response codes, refer to the following RFCs:

- RFC1945
- RFC7231

AsyncOS API Capabilities

You can use the AsyncOS API to retrieve information in the following categories:

- APIs for Web, on page 9
- General Purpose APIs, on page 169



CHAPTER 2

APIs for Web

Reporting APIs

Reporting queries can be used to fetch data from report groups, for all reports under a specific group, or for a specific report.

Synopsis	`GET /api/v2.0/reporting/report?resource_attribute` `GET /api/v2.0/reporting/report/counter?resource_attribute`

Supported Resource Attributes	Duration	This is a required parameter. All API queries should be accompanied with this parameter. `startdate=YYYY-MM-DDThh:mm:00.000Z&endDate=YYYY-MM-DDThh:mm:00.000Z` Aggregate report(s) for the specified duration.
	Query Type	• `query_type=graph` Receive data that can be represented as graphs. • `query_type=export` Receive data in the export format.
	Sorting	You should use both these parameters. If you use either, you will not receive data in the response. • `orderBy=<value>` Specify the attribute by which to order the data in the response. For example, `orderBy=total_clean_recipients` • `orderDir=<value>` Specify sort direction. The valid options are: • `asc` Order the results in ascending order. • `desc` Order the results in descending order.
	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.
	Data Retrieval Option	• `top=<value>` Specify the number of records with the highest values to return.
	Filtering	

		Filter parameters restrict the data to be included the response. • `filterValue=<value>` The value to search for. • `filterBy=<value>` Filter the data to be retrieved according to the filter property and value. • `filterOperator=<value>` The valid options are: • `begins_with` Filter the response data based on the value specified. This is not an exact value. • `is` Filter the response data based on the exact value specified.
	Device	• `device_type=wsa` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter. • `device_name=<value>` Specify the device name.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Comparing API Data with the Web Interface Data

The new web interface uses the AsyncOS APIs to fetch data with the duration attribute specified in the GMT time zone. If you plan to compare the data from your API query with the new web interface data, ensure that your API query has the same time range (in ISO8601 time format) as the new web interface API query.

Examples

Examples of the types of reporting queries are shown below:

• Retrieving a Single Value for a Counter, on page 12
• Retrieving Multiple Values for a Counter, on page 12
• Retrieving Single Values for Each Counter in a Counter Group, on page 13
• Retrieving Multiple Values for Multiple Counters, on page 14
• Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter, on page 15

Retrieving a Single Value for a Counter

This example shows a query to retrieve a single value for a counter.

Sample Request

```
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
```

Sample Response

```
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
                }
            ]
        }
    }
}
```

Retrieving Multiple Values for a Counter

This example shows a query to retrieve multiple values for a counter with the order direction and device type parameters.

Sample Request

```
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
```

Sample Response

```
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}
        ]
    }
}
```

Retrieving Single Values for Each Counter in a Counter Group

A counter group may have multiple counters. This example shows a query to retrieve single values for each counter in a counter group with the filter, device type, and top parameters.

Sample Request

```
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
```

Sample Response

```
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}
            ]
        }
    }
}
```

Retrieving Multiple Values for Multiple Counters

Here is an example of a query that retrieves multiple values for multiple counters, including offset, limit, and device type parameters.

Sample Request

```
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
```

Sample Response

```
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}]}}
```

Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter

This example shows a query to retrieve multiple values for multiple counters with the offset and limit parameters and query type parameters.

Sample Request

```
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
```

Sample Response

```
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",
        "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,
            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"
            ]
        }
    }
}
```


Schedule and Archive APIs

Schedule APIs

Synopsis	`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`

Supported Resource Attributes	Sorting	You should use both these parameters. If you use either, you will not receive data in the response. • `orderBy=<value>` The valid options are: • `periodic_report_display_name` Order the results based on the display name of the report. • `periodic_report_title` Order the results based on the type of the report. • `periodic_report_type` Order the results based on the type of the report. • `periodic_report_time_range` Order the results based on the time range of the report. • `periodic_report_delivery` Order the results based on the delivery options of the report. • `periodic_report_format` Order the results based on the format of the report. • `periodic_report_schedule_type` Order the results based on the type of the schedule selected for the report. • `periodic_report_tier` Order the results based on the required web gateway. • `periodic_report_next_run_date` Order the results based on the scheduling options of the report. • `orderDir=<value>` Specify sort direction. The valid options are: • `asc` Order the results in ascending order. • `desc` Order the results in descending order.

	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.
	Device	• `device_type=wsa` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Examples

The following are some examples for the types of schedule reports queries:

- Retrieving Scheduling Reports, on page 19
- Retrieving the Details of a Schedule Report Entry, on page 21
- Adding a Scheduled Report Entry, on page 21
- Editing a Scheduled Report Entry, on page 22
- Deleting Scheduled Reports, on page 23

Retrieving Scheduling Reports

The following example shows how to retrieve the list of all available scheduled report entries:

Sample Request

```
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
```

Sample Response

```
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}}}
```

Retrieving the Details of a Schedule Report Entry

The following example shows how to retrieve the details of one particular scheduled report by passing the report ID:

Sample Request

```
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
```

Sample Response

```
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"}}}}
```

Adding a Scheduled Report Entry

The following example shows how to add a scheduled report with report type, report title, device type and other options:

Sample Request

```
POST /wsa/api/v2.0/config/periodic_reports?device_type=wsa& HTTP/1.1
cache-control: no-cache
Postman-Token: 32a1d150-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"]}]}}
```

Sample Response

```
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"}
```

Editing a Scheduled Report Entry

The following example shows how to modify a scheduled report with a schedule report ID:

Sample Request

```
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"}}]}}

Sample Response

```
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"}
```

Deleting Scheduled Reports

The following example shows how to delete a scheduled report with device type and a schedule report ID:

Sample Request

```
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
```

Sample Response

```
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"}}
```

Archive APIs

Synopsis	`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`(To delete single report)
	`DELETE /wsa/api/v2.0/config/archived_reports?id=all` (To delete all archived reports)

Supported Resource Attributes	Sorting	You should use both these parameters. If you use either, you will not receive data in the response. • `orderBy=<value>` The valid options are: • `periodic_report_generated` Order the results based on the date and time the report is generated. • `periodic_report_display_name` Order the results based on the display name of the report. • `periodic_report_format` Order the results based on the format of the report. • `periodic_report_title` Order the results based on the type of the report. • `periodic_report_time_range` Order the results based on the time range of the report. • `periodic_report_type` Order the results based on the type of the report. • `periodic_report_tier` Order the results based on the required email gateway. • `orderDir=<value>` Specify sort direction. The valid options are: • `asc` Order the results in ascending order. • `desc` Order the results in descending order.
	Lazy Loading	You should use both these parameters. If you use either, you will not receive data in the response. • `offset=<value>` Specify an offset value to retrieve a subset of records starting with the offset value. Offset works with limit, which determines how many records to retrieve starting from the offset. • `limit=<value>` Specify the number of records to retrieve.

	Filtering	Filter parameters restrict the data to be included the response. • `filterByTitle=<value>` Filter the data to be retrieved according to the title of the report and value. • `filterByReportTypeName=<value>` Filter the data to be retrieved according to the type of the report and value. • `filterByTimeRange=<value>` Filter the data to be retrieved according to the time range of the report and value.
	Device	• `device_type=wsa` Specify the device type. This is a required parameter. All API queries must be accompanied with this parameter.
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Examples

The following are some examples for the types of archived reports queries:

- Searching Archived Reports, on page 26
- Retrieving Archived Reports, on page 27
- Retrieving the Details of a Archive Report Entry, on page 28
- Adding an Archive Report Entry, on page 29
- Deleting an Archived Report Entry, on page 30

Searching Archived Reports

The following example shows how to search for a list of the top 20 archived reports based on the report title and sorted by the date and time the report was generated, in ascending order:

Sample Request

```
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: e1f6fac5-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
```

Sample Response

```
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"}}]}}
```

Retrieving Archived Reports

The following example shows how to retrieve a list of the top 25 archived reports, sorted by the time range of the report in descending order:

Sample Request

```
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
```

Sample Response

```
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"}}]}}
```


Retrieving the Details of a Archive Report Entry

The following example shows how to retrieve an archived report entry with device type and an archived report ID:

Sample Request

```
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
```

Sample Response

```
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
```

Adding an Archive Report Entry

The following example shows how to add an archived report with report title, report type, device type, and other options:

Sample Request

```
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
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"}]}}
```

Sample Response

```
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"}}
```

Deleting an Archived Report Entry

The following example shows how to delete an archived report with device type and an archived report ID:

Sample Request

```
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
```

Sample Response

```
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"}}
```

Tracking APIs

You can use web tracking APIs to search for and get details about individual transactions or patterns of transactions. Web tracking APIs are:

- Proxy Services, on page 30
- Layer 4 Traffic Monitor, on page 33
- SOCKS Proxy, on page 35

Proxy Services

You can retrieve information about web usage for a particular user or for all users using multiple attributes.

Synopsis	`GET /api/v2.0/web-tracking/web_transaction?resource_attribute`
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve transactions processed by the proxy services, with the duration, filtering, offset and limit, ordering, and transactions status parameters:

Sample Request

```
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
```

Sample Response

```
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
                cba12403f2eb11c4884b27862dd31a779133c03a0e61d334d",
                "applicationType": "-",
                "timestamp": 1540275265,
                "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
                , 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": "-"
            }
        }
    ]
}
```


Layer 4 Traffic Monitor

You can retrieve information about connections to malware sites and ports using multiple attributes.

Synopsis	`GET /api/v2.0/web-tracking/web_transaction?resource_attribute`	
Supported Resource Attributes	For more information, seeAsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization

Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve transactions processed by the Layer 4 Traffic Monitor, with the duration, filtering, offset and limit, ordering, and transaction status parameters:

Sample Request

```
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
```

Sample Response

```
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 Proxy

You can retrieve information about transactions processed through the SOCKS proxy, including information about top destinations and users.

Synopsis	`GET /api/v2.0/web-tracking/web_transaction?resource_attribute`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve transactions processed by the SOCKS Proxy Services, with the duration, filtering, offset and limit, ordering, and transaction status parameters:

Sample Request

```
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
```

Sample Response

```
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"
            }
        }
    ]
}
```

Configuration APIs

You can use configuring APIs to search for and get details about individual transactions or patterns of transactions. Configuring APIs are:

- Overall Bandwidth
- PAC File Host Settings
- Identification Profiles
- Access Policies
- Domain Map
- Upstream Proxy
- HTTPS Proxy
- Log Subscriptions
- Header Based Authentication
- Request Header Rewrite Profiles
- Smart Software Licenses, on page 104
- System Setup Wizard, on page 112
- Decryption Policy, on page 115
- Routing Policy, on page 123
- IP Spoofing Profile, on page 127
- Configuration Files, on page 130
- Authentication Realms, on page 135
- Umbrella Seamless ID, on page 141
- Secure DNSSec Settings, on page 144
- Identity Service Engine, on page 145
- Anti-Malware Reputation, on page 151
- End-User Notification, on page 166

Overall Bandwidth

This section contains the following topics:

- Retrieving the Overall Bandwidth Details
- Modifying the Overall Bandwidth Details

Retrieving the Overall Bandwidth Details

You can retrieve information about the overall bandwidth for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/web_security/overall_bandwidth_limit`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the overall bandwidth configuration on the device.

Sample Request

```
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
```

Sample Response

```
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
}
```

Modifying the Overall Bandwidth Details

You can modify the overall bandwidth control for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`PUT wsa/api/v3.0/configure/web_security/overall_bandwidth_limit`	
Supported Resource Attributes	For moreinformation, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization

Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify and set the overall bandwidth configuration on the device.

Sample Request

```
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
}
```

Sample Response

```
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 File Host Settings

This section contains the following topics:

- Deleting a PAC File and the Hostname Association

Retrieving the PAC File Basic Settings

You can retrieve and set the PAC File hosting status, the PAC File expiration, and the PAC File expiration limit.

Synopsis	`GET /wsa/api/v3.0/security_services/pac_basic_setting`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the PAC File hosting status, the PAC File expiration status, PAC file server ports, and the PAC File expiration interval.

Sample Request

```
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
```

Sample Response

```
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
    }
}
```

Modifying the PAC File Basic Settings

You can modify the basic settings for PAC File hosting.

Synopsis	`PUT /wsa/api/v3.0/security_services/pac_basic_setting`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the PAC File hosting status, the PAC File expiration status, PAC file server ports, and the PAC File expiration interval.

Sample Request

```
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
}
```

Sample Response

```
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
```

Retrieving the PAC Files

You can retrieve the PAC files hosted on the Secure Web Appliance. The ‘file_name’ parameter can be used to get a particular file from the Secure Web Appliance.

Synopsis	`GET /wsa/api/v3.0/security_services/pac_file`
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the list of all PAC files hosted on the Secure Web Appliance.

Sample Request

```
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
```

Sample Response

```
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";
```

Retrieving the List of PAC Files

You can retrieve the list of all the PAC files hosted on the Secure Web Appliance. The 'file_name' parameter can be used to get a particular file from the Secure Web Appliance.

Synopsis	`GET /wsa/api/v3.0/security_services/pac_file`	
Supported Resource Attributes	For information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the list of all PAC files hosted on the Secure Web Appliance.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
```

Sample Response

```
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"
                ]
}
```

Adding a New PAC File

You can upload a new PAC file. Multiple files can be uploaded in a single request.

Synopsis	`POST /wsa/api/v3.0/security_services/pac_file`
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add a new PAC file.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
Content-Length: 1384
Expect: 100-continue
Content-Type: multipart/form-data; boundary=------------------------6b685d35de1f2379
```

Sample Response

```
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
```

Modifying the Existing PAC Files

You can modify an existing PAC file.

Note The file with the same file name must exist.

Synopsis	`PUT /wsa/api/v3.0/security_services/pac_file`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify existing PAC files.

Sample Request

```
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
```

Sample Response

```
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
```

Deleting a PAC File

You can now delete a PAC file.

Synopsis	`DELETE /wsa/api/v3.0/security_services/pac_file`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete a PAC file.

Sample Request

```
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
```

Sample Response

```
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
```

Retrieving a PAC File and the Hostname Association

You can retrieve PAC files and their associated hostnames.

Synopsis	`GET /wsa/api/v3.0/security_services/pacfile_host`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve PAC files and the associated hostnames.

Sample Request

```
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
```

Sample Response

```
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"
  }
}
```

Adding a PAC File and the Hostname Association

You can create a PAC file and their associated hostname.

Synopsis	`POST /wsa/api/v3.0/security_services/pacfile_host`

Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add a PAC file and their associated hostname.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
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"
        }
    ]
}
```

Sample Response

```
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
```

Modifying the Existing PAC File and the Hostname Association

You can modify an existing PAC file and the associated hostname.

Note The mapping for the given or provided hostname must exist.

Synopsis	`PUT /wsa/api/v3.0/security_services/pacfile_host`

Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to map the PAC files with the hostnames.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
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"
        }
    ]
}
```

Sample Response

```
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
```

Deleting a PAC File and the Hostname Association

You can delete the existing PAC file and the associated hostname.

Note The mapping for the given or provided hostname must exist.

Synopsis	`DELETE /wsa/api/v3.0/security_services/pacfile_host`

Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete a PAC file and the associated hostname.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
```

Sample Response

```
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
```

Identification Profiles

This section contains the following topics:

- Retrieving the Identification Details
- Modifying the Identification Profiles
- Adding the Identification Profiles
- Deleting the Identification Profile

Retrieving the Identification Details

You can retrieve the identification profiles for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/web_security/identification_profiles`
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the identification profiles.

Sample Request

```
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
```

Sample Response

```
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": {}
        }
    ]
}
```

Modifying the Identification Profiles

You can modify the identification profiles for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`PUT /wsa/api/v3.0/web_security/identification_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add the identification profile.

Sample Request

```
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
        }
    ]
}
```

Sample Response

```
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
```

Adding the Identification Profiles

You can create the identification profiles for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`POST /wsa/api/v3.0/web_security/identification_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the identification profiles.

Sample Request

```
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
        }
    ]
}
```

Sample Response

```
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
```

Deleting the Identification Profile

You can delete an identification profile for the Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v3.0/web_security/identification_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the identification profile.

Sample Request

```
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
```

Sample Response

```
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
}
```


Access Policies

This section contains the following topics:

Retrieving an Access Policy

You can retrieve a list of access policies configured on the Secure Web Appliance.

Synopsis	`GET /wsa/api/v3.0/web_security/access_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve an access policy with the policy name "AP106"

Sample Request

```
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
```

Sample Response

```
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"
      }
    }
  ]
}
```

Modifying an Access Policy

You can modify a list of access policies and their configuration payload.

Synopsis	`PUT /wsa/api/v3.0/web_security/access_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify an access policy.

Sample Request

```
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_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"
                ]
            }
        }
    ]
}
```

Sample Response

```
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
```

Adding an Access Policy

You can create a list of access policies along with their configurations.

Synopsis	`POST /wsa/api/v3.0/web_security/access_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to to create an access policy.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
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"
                ]
            }
        }
    ]
}
```

Sample Response

```
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
```

Deleting an Access Policy

You can delete an access policy using the policy name.

Synopsis	`DELETE /wsa/api/v3.0/web_security/access_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete multiple access policies at once.

.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
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
}
```

Domain Map

This section contains the following topics:

- Retrieving the Domain Map Details
- Modifying the Domain Map Details
- Adding a Domain Map
- Deleting the Domain Map

Retrieving the Domain Map Details

You can retrieve the domain map details for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/web_security/domain_map`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the domain map details.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
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
}
```

Modifying the Domain Map Details

You can modify the domain map details.

Synopsis	`PUT /wsa/api/v2.0/configure/web_security/domain_map`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the domain map details.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
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"
            ]
        }
]
```

Sample Response

```
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
}
```

Adding a Domain Map

You can create a domain map along with their configurations.

Synopsis	`POST /wsa/api/v2.0/configure/web_security/domain_map`
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to create a domain map.

Sample Request

```
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"
            ]
        }
]
```

Sample Response

```
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
}
```

Deleting the Domain Map

You can delete a domain map for the Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v2.0/configure/web_security/domain_map`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the domain map.

Sample Request

```
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"
}
```

Sample Response

```
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
}
```

Upstream Proxy

This section contains the following topics:

- Retrieving the Upstream Proxy Details
- Modifying the Upstream Proxy Settings
- Adding an Upstream Proxy
- Deleting the Upstream Proxy
- Modifying the Upstream Proxy Servers
- Adding an Upstream Proxy Server
- Deleting the Upstream Proxy Servers

Retrieving the Upstream Proxy Details

You can retrieve the upstream proxy details for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/ network/upstream_proxy`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization

Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the upstream proxy details.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
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
}
```

Modifying the Upstream Proxy Settings

You can modify the upstream proxy setting for the Secure Web Appliance.

Synopsis	`PUT /wsa/api/v2.0/configure/network/upstream_proxy`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization

Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the group name, new group name, failure handling, and load balancing properties of the upstream proxy.

Sample Request

```
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"
    }
]
```

Sample Response

```
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}
```

Adding an Upstream Proxy

You can create an upstream proxy along with their configurations.

Synopsis	`POST /wsa/api/v2.0/configure/network/upstream_proxy`

Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to create an upstream proxy.

Sample Request

```
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
        }
    ]
}
```

Sample Response

```
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",
        "res_code": 201
}
```

Deleting the Upstream Proxy

You can delete an upstream proxy for the Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v2.0/configure/network/upstream_proxy`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the upstream proxy.

Sample Request

```
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"
}
```

Sample Response

```
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
}
```

Modifying the Upstream Proxy Servers

You can modify the upstream proxy server settings.

Synopsis	`PUT /wsa/api/v2.0/configure/network/upstream_proxy/servers`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the name of the upstream proxy servers.

Sample Request

```
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
            }
        ]
    }
]
```

Sample Response

```
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}
```

Adding an Upstream Proxy Server

You can create an upstream proxy server along with their configurations.

Synopsis	`POST /wsa/api/v2.0/configure/network/upstream_proxy/servers`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add an upstream proxy server to the configuration.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
Content-Type: application/json
Content-Length: 204

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

Sample Response

```
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
}
```

Deleting the Upstream Proxy Servers

You can delete the configuration for upstream proxy servers for the Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v2.0/configure/network/upstream_proxy/servers`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the configuration for upstream proxy servers.

.

Sample Request

```
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
            }
        ]
    }
]
```

Sample Response

```
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 Proxy

This section contains the following topics:

- Retrieving the HTTPS Proxy Details
- Modifying the HTTP Proxy Settings
- Retrieving the HTTP Proxy—Download Certificate File

- Retrieving the HTTP Proxy OCSP Settings
- Modifying the HTTPS Proxy—OCSP Settings

Retrieving the HTTPS Proxy Details

You can retrieve the HTTPS proxy details for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/security_services/proxy/https`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the HTTPS proxy details.

Sample Request

```
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
```

Sample Response

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


Modifying the HTTP Proxy Settings

You can modify the HTTP Proxy settings.

Synopsis	`PUT /wsa/api/v2.0/configure/security_services/proxy/https`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify HTTP Proxy settings.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
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"'
```

Sample Response

```
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
}
```

Retrieving the HTTP Proxy—Download Certificate File

You can retrieve the HTTP Proxy download certificate file for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/security_services/proxy/https/download`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the HTTP Proxy download certificate file details.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 08:02:21 GMT
Content-Description: File Transfer
Content-type: application/octet-stream
Content-Disposition: attachment; filename=cert.pem
Content-Length: 1346
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
<
-----BEGIN CERTIFICATE-----
MIIDxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx/4zkBgLQZOdJiKWTGYM=
-----END CERTIFICATE-----
```

Retrieving the HTTP Proxy OCSP Settings

You can retrieve the HTTP Proxy OCSP settings for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/security_services/proxy/ocsp`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the HTTP Proxy OCSP settings.

Sample Request

```
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
```

Sample Response

```
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
}
```

Modifying the HTTP Proxy—OCSP Settings

You can modify the HTTP proxy OCSP settings.

Synopsis	`PUT /wsa/api/v2.0/configure/security_services/proxy/ocsp`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the HTTP proxy OCSP settings.

Sample Request

```
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": []
}
```

Sample Response

```
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
}
```

Log Subscriptions

This section contains the following topics:

- Retrieving the Log Subscriptions
- Modifying the Log Subscriptions
- Adding the Log Subscriptions
- Deleting the Log Subscriptions
- Modifying the Log Subscriptions—Rollover
- Retrieving the Log Subscriptions for the Fetch Field Lists
- Retrieving the Log Subscriptions to Fetch Default Values for a Log Type
- Adding the Log Subscriptions—Deanonymization

Retrieving the Log Subscriptions

You can retrieve the log subscriptions for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/system/log_subscriptions`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the log subscriptions.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
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
}
```


Modifying the Log Subscriptions

You can modify the basic settings for log subscriptions.

Synopsis	`PUT /wsa/api/v2.0/configure/system/log_subscriptions`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the basic settings for log subscriptions.

Sample Request

```
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
        }
    }
]
```

Sample Response

```
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
}
```

Adding the Log Subscriptions

You can create log subscriptions along with their configurations.

Synopsis	`POST /wsa/api/v2.0/configure/system/log_subscriptions`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to create log subscriptions.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
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
            }
    }
]
```

Sample Response

```
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
}
```

Deleting the Log Subscriptions

You can delete the log subscriptions for the Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v2.0/configure/system/log_subscriptions`

Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the log subscriptions.

Sample Request

```
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"
}
```

Sample Response

```
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
}
```

Modifying the Log Subscriptions—Rollover

You can modify the log subscriptions rollover settings.

Synopsis	`PUT /wsa/api/v2.0/configure/system/log_subscriptions/rollover`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the log subscriptions rollover settings.

Sample Request

```
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"
}
```

Sample Response

```
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
 }
```

Retrieving the Log Subscriptions for the Fetch Field Lists

You can retrieve the log subscriptions for the fetch field lists for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/ system/log_subscriptions/fields`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the log subscriptions for the fetch field lists.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
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
}
```

Retrieving the Log Subscriptions to Fetch Default Values for a Log Type

You can retrieve the log subscriptions to fetch the default values for a log type. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/system/log_subscriptions/defaults`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the log subscriptions to fetch the default values for a log type.

Sample Request

```
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
```

Sample Response

```
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
}
```


Adding the Log Subscriptions—Deanonymization

You can add the Log Subscriptions—Deanonymization.

Synopsis	`POST /wsa/api/v2.0/configure/system/log_subscriptions/deanonymization`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add the log subscriptions for Deanonymization.

Sample Request

```
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 YWRtaW46SXJvbnBvcnRAMTIz
```

```
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"'
```

Sample Response

```
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
}
```

Header Based Authentication

This section contains the following topics:

- Retrieve the Header Based Authentication Details
- Modifying the Header Based Authentication Details

Retrieve the Header Based Authentication Details

You can retrieve the Header Based Authentication details configured on the Secure Web Appliance.

Synopsis	`GET /wsa/api/v3.0/network/xauth_header_setting`
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to enable the header based authentication details.

Sample Request

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

Sample Response

```
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"
 }
}
```

Configuring Header Based Authentication with Different Parameters

Example

This example shows how to configure a list of parameters related to Header Based Authentication Settings.

Sample Request

```
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"}
}
```

Sample Response

```
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
```

Modifying the Header Based Authentication Details

You can modify the header based authentication details.

Synopsis	`PUT /wsa/api/v3.0/network/xauth_header_setting`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the header based authentication settings

Sample Request

```
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"}
}
```

Sample Response

```
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
```

Example

This example shows how to enable the header based authentication details.

Sample Request

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

Sample Response

```
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
```

Example

This example shows how to disable the header based authentication details.

Sample Request

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

Sample Response

```
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
```

Request Header Rewrite Profiles

This section contains the following topics:

Retrieving the Request Header Rewrite Details

You can retrieve the request Header Profiles and X-Authenticated Header Global Settings configured on the Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/web_security/http_rewrite_profiles`

Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve request header profiles and X-Authenticated Header Global Settings.

Sample Request

```
GET /wsa/api/v3.0/web_security/http_rewrite_profiles
HTTP/1.1
Host: wsa.example.com:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

Sample Response

```
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"
        }
    ]
}
```

Modifying the Request Header Rewrite Details

You can modify the request header rewrite profiles and X-Authenticated Header Global Settings.

Synopsis	`PUT /wsa/api/v3.0/web_security/http_rewrite_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the request header rewrite details.

Sample Request

```
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": ":"
    }
}
```

Sample Response

```
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
```

Adding a Request Header Rewrite Profile

You can create a list of request header rewrite profiles and update X-Authenticated Header Global Settings.

Synopsis	`POST /wsa/api/v3.0/web_security/http_rewrite_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to create request header rewrite profile and update X-Authenticated Header Global Settings.

Sample Request

```
POST /wsa/api/v3.0/web_security/http_rewrite_profiles
HTTP/1.1
Host: wsa.example.com:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
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": ":"
    }
}
```

Sample Response

```
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
```

Deleting the Request Header Rewrite Profile

You can delete request header rewrite profile by using profile_name and select alternate profile to be replaced in access policy using alternate_profile_name. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v3.0/web_security/http_rewrite_profiles?alternate_profile_name=None&profile_name=RHR`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the request header rewrite profile.

Sample Request

```
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
```

Sample Response

```
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
```

Smart Software Licenses

This section contains the following topics:

Retrieving the Smart Software Licenses

You can retrieve the list of license details with license name and authentication status.

The grace period is returned if the authentication status of any of the licenses is "Out Of Compliance."

Synopsis	`GET wsa/api/v3.0/system_admin/sl_licenses`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the list of license details with license name and authentication status.

Sample Request 1

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

Sample Response 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"
    }
]
```


Sample Response 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"
    }
]
```


Modifying the Smart Software Licenses

You can modify the list of license details with the license name and authentication status.

The grace period is returned if the authentication status of any of the licenses is "Out Of Compliance."

Synopsis	`PUT wsa/api/v3.0/system_admin/sl_licenses`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the list of license details with license name and authentication status.

Sample Request 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."
}
```

Sample Request 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."
    }
}
```

Sample Request 3

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

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."
```

```
    }
}
```

Sample Request 4

```
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": ["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."
    }
}
```

Sample Request 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."
    }
}
```

Retrieve the Smart License Agent Status

You can retrieve the details of Cisco Smart Software License configuration such as enable or disable status, registration status, and so on.

Synopsis	`GET wsa/api/v3.0/system_admin/smart_agent_status`

Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the details of Cisco Smart Software License configurations such as enable or disable status, registration status, and so on.

Sample Request

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

Sample Response

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

Modifying the Smart License Agent Status

You can modify the details of Cisco Smart Software License configurations such as enable or disable status, registration status, and so on.

Synopsis	`PUT wsa/api/v3.0/system_admin/smart_agent_status`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the details of Cisco Smart Software License configurations such as enable or disable status, registration status, and so on.

Sample Request

```
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
```

Retrieving the Smart Software Licenses Status

You can retrieve the list of details of Cisco Smart Software License configurations such as enable or disable status, registration status and so on.

Synopsis	`GET wsa/api/v3.0/system_admin/smart_software_licensing_status HTTP/1.1`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the list of details of Cisco Smart Software License configuration such as enable or disable status, registration status and so on.

Sample Request

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

Sample Response

```
{
    "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 )"
}
```

Modifying the Smart Software Licenses Status

You can modify the list of details of Cisco Smart Software License configurations such as enable or disable status, registration status, and so on.

Synopsis	`PUT wsa/api/v3.0/system_admin/smart_software_licensing_status`

Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the list of details of Cisco Smart Software License configurations such as enable or disable status, registration status, and so on.

Sample Request 1

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

Sample Request 2

Note Use your own registeration token.

```
{ "registration_token":
"ZTExxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx%0A",
 "action": "register", "test_interface": "Data" } { "action": "deregister" } {
"transport_mode": "transport_gateway", "transport_url": "https://www.google.com" } { "action":
 "renew_auth" } { "action": "renew_registration" }
```

Sample Request 3

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

Sample Request 4

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

}
```

Sample Request 5

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

Sample Request 6

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

System Setup Wizard

This section contains the following topics:

Retrieving the End User License Agreement Details

You can retrieve the end user license agreement details.

Note You must go through the EULA agreement before performing the PUT request to setup the system setup wizard.

Synopsis	`GET wsa/api/v3.0/system_admin/cisco_end_user_license_agreement`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the end user license agreement details.

Sample Request 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": "Q2lzY28xMjMk",
        "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"
    }
}
```

Sample Response 1

```
204 No-content
```

Sample Request 2

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

{
    "network_admin": {
        "passphrase": "Q2lzY28xMjMk",
        "mail_to_addrs": "sandhgan@cisco.com",
```

```
    }
}
```

Sample Response 2

```
204 No-content
```

Modifying the System Setup Wizard Settings

You can modify the objects with system setup wizard settings.

Synopsis	`PUT wsa/api/v3.0/system_admin/system_setup_wizard`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the objects with system setup wizard settings.

Sample Request 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": "Q2lzY28xMjMk",
        "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"
    }
}
```

Sample Response 1

```
204 No-content
```

Sample Request 2

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

{
    "network_admin": {
        "passphrase": "Q2lzY28xMjMk",
        "mail_to_addrs": "sandhgan@cisco.com",
    }
}
```

Sample Response 2

```
204 No-content
```

Decryption Policy

This section contains the following topics:

Retrieving the Decryption Policy

You can retrieve the decryption policies available and their configuration.

Synopsis	`GET wsa/api/v3.0/web_security/decryption_policies`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the decryption policies available and their configuration.

Sample Request

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

Sample Response

```
{
    "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 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"
        }
    ]
}
```


Modifying the Decryption Policy

You can modify the decryption policies available and their configuration.

Synopsis	`PUT wsa/api/v3.0/web_security/decryption_policies`
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the decryption policies available and their configuration.

Sample Request

```
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"
        }
    ]
}
}
```

Sample Response

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

Adding the Decryption Policy

You can add the decryption policies available and their configuration.

Synopsis	`POST wsa/api/v3.0/web_security/decryption_policies`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add the decryption policies available and their configuration.

Sample Request

```
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"
        }
    ]
}
```

Sample Response

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

Deleting the Decryption Policy

You can delete available decryption policies and their configurations..

Synopsis	`DELETE wsa/api/v3.0/web_security/decryption_policies`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete available decryption policies and their configurations.

Sample Request

```
DELETE /wsa/api/v3.0/web_security/decryption_policies?policy_names=DP1,DP2,DP3 HTTP/1.1
Host: dut058.perf8:6443
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
{
    "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
}
```

Routing Policy

This section contains the following topics:

Retrieving a Routing Policy

You can retrieve the list of routing policies with the matching policy names to be returned.

Synopsis	`GET wsa/api/v3.0/web_security/routing_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the list of routing policies with the matching policy names to be returned.

Sample Request

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

Sample Response

```
{
    "routing_policies": [
        {
            "policy_description": "test protcol 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"
            }
        }
    ]
}
```

Modifying a Routing Policy

You can modify the list of routing policies and their configuration payload.

Synopsis	`PUT wsa/api/v3.0/web_security/routing_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the list of routing policies and their configuration payload.

Sample Request

```
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 protcol policy",
            "policy_order": 1,
            "membership": {
                "identification_profiles": [
                    {
                        "profile_name": "ID1",
                        "auth": "No Authentication"
                    }
                ]
            },
            "ip_spoofing": "IP1",
            "routing_destination":{
                "upstream_proxy_group": "UPProxy1"
            }
        }
    ]
}
```

Sample Response

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

Adding a Routing Policy

You can add the list of routing policies and their configuration payload.

Synopsis	`POST wsa/api/v3.0/web_security/routing_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add the list of routing policies and their configuration payload.

Sample Request

```
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 protcol policy",
            "policy_order": 1,
            "membership": {
                "identification_profiles": [
                    {
                        "profile_name": "global_identification_profile",
                        "auth": "No Authentication"
                    }
                ]
            },
            "ip_spoofing": "Do not use IP Spoofing"
        }
    ]
}
```

Sample Response

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

Deleting a Routing Policy

You can delete the list of routing policies with the matching policy names to be deleted.

Synopsis	`DELETE wsa/api/v3.0/web_security/routing_policies`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the list of routing policies with the matching policy names to be deleted.

Sample Request

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

Sample Response

```
{
    "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 Spoofing Profile

This section contains the following topics:

Retrieving the IP Spoofing Profile

You can retrieve the list of IP spoofing profiles and their configuration payload.

Synopsis	`GET wsa/api/v3.0/web_security/ip_spoofing_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the list of IP spoofing profiles and their configuration payload.

Sample Request

```
GET /wsa/api/v3.0/web_security/ip_spoofing_profiles?profile_names=spoof2,spoof3
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

Sample Response

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

Modifying the IP Spoofing Profile

You can modify the list of IP spoofing profiles and their configuration payload.

Synopsis	`PUT wsa/api/v3.0/web_security/ip_spoofing_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the list of IP spoofing profiles and their configuration payload.

Sample Request

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

{
    "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"
        }
    ]
}
```

Sample Response

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

Adding the IP Spoofing Profile

You can add the list of IP spoofing profiles and their configuration payload.

Synopsis	`POST wsa/api/v3.0/web_security/ip_spoofing_profiles`
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.

Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to add the list of IP spoofing profiles and their configuration payload.

Sample Request

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

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

Sample Response

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

Deleting the IP Spoofing Profile

You can delete the list of IP spoofing profiles and their configuration payload.

Synopsis	`DELETE wsa/api/v3.0/web_security/ip_spoofing_profiles`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the list of IP spoofing profiles and their configuration payload.

Sample Request

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

Sample Response

```
{
    "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
}
```

Configuration Files

This section contains the following topics:

Retrieving the Configuration Files

You can download, save, or load a configuration file on a Secure Web Appliance.

Synopsis	`GET wsa/api/v3.0/system_admin/configuration_file`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to download, save, or load a configuration file on a Secure Web Appliance.

Sample Request

```
curl --location --request GET
'https://wsa308.cs1:4431/wsa/api/v3.0/system_admin/configuration_file?mail_to=xyz123@cisco.com'
 --header 'Authorization: Basic YWRtaW46Q2lzY29AMTIz'

Sample Response:

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

Modifying the Configuration Files

You can download, save, or load a configuration file on a Secure Web Appliance.

Synopsis	`PUT wsa/api/v3.0/system_admin/configuration_file`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to download, save, or load a configuration file on a Secure Web Appliance.

Sample Request

```
curl --location --request PUT
'https://wsa308.cs1:4431/wsa/api/v3.0/system_admin/configuration_file' --header
'Authorization: Basic YWRtaW46Q2lzY29AMTIz' --form 'action="save"'
```

Sample Response

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

Viewing the Appliance Configuration Files

You can view the available configuration files saved on the Secure Web Appliance.

Synopsis	`GET wsa/api/v3.0/system_admin/appliance_config_files`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to view the available configuration files saved on the Secure Web Appliance.

Sample Request

```
curl --location --request GET
'https://wsa308.cs1:4431/wsa/api/v3.0/system_admin/appliance_config_files' --header
'Authorization: Basic YWRtaW46Q2lzY29AMTIz'
```

Sample Response


```
{
    "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"
    ]
}
```


Retrieving the Configuration Files—Backup Settings

You can retrieve the current settings of the configuration backup server.

Synopsis	`GET wsa/api/v3.0/system_admin/config_backup_server`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the current settings of the configuration backup server.

Sample Request 1

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

Sample Response 1

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

Sample Request 2

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

Sample Response 2

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

Modifying the Configuration Files—Backup Settings

You can modify the current settings of the configuration backup server.

Synopsis	`PUT wsa/api/v3.0/system_admin/config_backup_server`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the current settings of the configuration backup server.

Sample Request 1

```
PUT /wsa/api/v3.0/system_admin/config_backup_server
Host: dut058.perf8:4431
```

```
Authorization: Basic YWRtaW46Q2lzY28xMjMk

{
    "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": ""
        }
    }
}
```

Sample Response 1

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

Sample Request 2

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

{
    "config_backup_status": "enable",
    "save_passphrase": false,
    "retrieval_method": "ftp_push",
    "ftp_settings": {
        "ftp_host": "dut058.perf8",
        "directory": "/data/db",
        "username": "sandhgan",
        "passphrase": "Q2lzY28xMjMk"
    }
}
```

Sample Response 2

```
204 No-content
```

Modifying the Configuration Files—Reset

Reset configuration resets the configuration of the box to factory settings. The configuration files are updated to the factory settings.

Note Reset configurations can be performed only by the administrator, provided the system is not a cluster member.

Caution Resetting your configuration reverts your appliance to factory default settings, including the IP address. It is strongly recommended that the configuration is saved before performing these actions.

Synopsis	`PUT wsa/api/v3.0/system_admin/configuration_file`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to reset the configuration of the box to factory settings.

Sample Request

```
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"'
```

Sample Response

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

Authentication Realms

This section contains the following topics:

Retrieving the Authentication Realm Settings

You can view and retrieve the authentication realm settings.

Synopsis	`GET wsa/api/v3.0/network/auth_realms`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to view and retrieve the authentication realm settings.

Sample Request

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

Sample Response

```
{
    "auth_realms": [
        {
            "ad_account": {
                "domain_joined": false,
                "trusted_domain_lookup_enabled": true,
                "computer_acount": "Computers",
                "ad_domain": "ABCD2121.COM"
            },
            "ad_server": {
                "interface": "Management",
                "servers": [
                    {
                        "host": "xyz234.com"
                    }
                ]
            },
            "scheme": [
                "Negotiate",
                "NTLMSSP",
                "Basic"
            ],
            "type": "AD",
            "name": "ad1"
        }
    ]
}
```

Adding the Authentication Realm Settings

You can view and add the authentication realm settings.

Synopsis	`POST wsa/api/v3.0/network/auth_sequences`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to view and add the authentication realm settings.

Sample Request

```
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"
        }
    ]
}'
```

Sample Response

```
204 No-content
```

Retrieving the Authentication Realm Sequence Settings

You can view and change authentication realm sequence settings.

Synopsis	`GET wsa/api/v3.0/network/auth_sequences`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to view and change authentication realm sequence settings.

Sample Request

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

Sample Response


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


Modifying the Authentication Realm Sequence Settings

You can view and modify the authentication realm sequence settings.

Synopsis	`PUT wsa/api/v3.0/network/auth_sequences`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the authentication sequence settings.

Sample Request

```
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"
        }
    ]
}'
```

Sample Response

```
204 No-content
```

Adding the Authentication Realm Sequence Settings

You can view and add the authentication realm sequence settings.

Synopsis	`POST wsa/api/v3.0/network/auth_sequences`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to view and add the authentication realm sequence settings.

Sample Request

```
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"
        }
    ]
}'
```

Sample Response

```
204 No-content
```

Retrieving the Global Authentication Settings

You can retrieve the details of global authentication settings available and configurations such as Authentication Token TTL, Credential Encryption, Header Based Authentication, and so on.

Synopsis	`GET wsa/api/v3.0/network/global_auth_setting`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the global authentication settings.

Sample Request

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

Sample Response

```
{
    "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
        }
    }
}
```


Modifying the Global Authentication Settings

You can modify details of global authentication settings available and configurations such as Authentication Token TTL, Credential Encryption, Header Based Authentication, and so on.

Synopsis	`PUT wsa/api/v3.0/network/global_auth_setting`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the global authentication settings.

Sample Request

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

Sample Response

```
204 No-content
```

Umbrella Seamless ID

The section contains the following topics:

Retrieving the Cisco Umbrella Seamless ID

You can retrieve details of Cisco Umbrella Seamless ID present and configurations such as host, ports, and organization ID.

Synopsis	`GET wsa/api/v3.0/web_security/umbrella_seamless_id`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the details of Cisco Umbrella Seamless ID present and configurations such as host, ports, and organization ID.

Sample Request

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

Sample Response

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

Modifying the Cisco Umbrella Seamless ID

You can modify details of Cisco Umbrella Seamless ID present and configurations such as host, ports, and organization ID.

Synopsis	`PUT wsa/api/v3.0/web_security/umbrella_seamless_id`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the details of Cisco Umbrella Seamless ID present and configurations such as host, ports, and organization ID.

Sample Request

```
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"
    }
}
```

Sample Response

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

Performing Start Test for Umbrella Seamless ID

You can perform the start test for the umbrella seamless ID.

Synopsis	`GET wsa/api/v3.0/web_security/swg_connectivity_test`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to perform the start test for the umbrella seamless ID.

Sample Request

```
GET wsa/api/v3.0/web_security/swg_connectivity_test HTTP/1.1
Host: wsa353.cs1:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
Query Paramteres: host: wsa353.cs1
     Ports: 11
```

Sample Response

```
{
    "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. "
            }
        }
    ]
}
```

Secure DNSSec Settings

This section contains the following topics:

Retrieving the Secure DNS Settings

You can enable or disable the secure DNS settings.

Synopsis	`GET wsa/api/v2.0/configure/network/dns/dnssec`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to enable or disable the secure DNS settings.

Sample Request

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

Modifying the Secure DNS Settings

You can enable or disable the secure DNS settings.

Synopsis	`PUT wsa/api/v2.0/configure/network/dns/dnssec`

Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to enable or disable the secure DNS settings.

Sample Request—Enable Secure DNS

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

Sample Response—Enable Secure DNS

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

Sample Request—Disable Secure DNS

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

Sample Response—Disable Secure DNS

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

Identity Service Engine

This section contains the following topics:

Retrieving the Identity Service Engine Settings

You can retrieve the current settings of the identify service engine.

Synopsis	`GET wsa/api/v3.0/network/ise`	
Supported Resource Attributes	See *AsyncOS 14.5 API - Addendum to the Getting Started Guide for Cisco Secure Web Appliances* for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the identify service engine settings.

Sample Request 1

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

Sample Response 1

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

Sample Request 2

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

Sample Response 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": ""
        }
    }
}
```

Modifying the Identity Service Engine Settings

You can modify the identify service engine settings.

Synopsis	`PUT wsa/api/v3.0/network/ise`	
Supported Resource Attributes	See *AsyncOS 14.5 API - Addendum to the Getting Started Guide for Cisco Secure Web Appliances* for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the identify service engine settings.

Sample Request

```
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"
    }
}
```

Sample Response

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

Uploading the Identity Service Engine Certificate Details

You can upload the identify service engine certificate details.

Synopsis	`POST wsa/api/v3.0/network/ise_cert`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to upload the identify service engine certificate details.

Sample Request 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"'
```

Sample Request 2

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

Sample Request 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="'
```

Sample Response 2

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

Downloading the Identity Service Engine Certificate Details

You can download the identify service engine certificate details.

Synopsis	`GET wsa/api/v3.0/network/ise_download_cert`

Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to download the identify service engine certificate details.

Sample Request 1

```
GET wsa/api/v3.0/network/ise_download_cert?cert_type=csr
Host: dut058.perf8:4431
Authorization: Basic YWRtaW46Q2lzY28xMjMk
```

Sample Response 1

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyzxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxYUvzpUfBmbAZb1ziw=
-----END CERTIFICATE REQUEST-----
```

Performing Start Test for the Identity Service Engine

You can perform the start test for the current settings of the identify service engine.

Synopsis	`GET wsa/api/v3.0/network/ise/start_test`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to perform the start test for the current settings of the identify service engine.

Sample Request 1

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

Sample Response 1

```
{
  "test_result": "Failure",
  "test_logs": [
    "Checking DNS resolution of ISE pxGrid Node hostname(s) ...",
    "Success: Resolved 'ise-server56.cs1.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.cs1.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.cs1.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.",
    ""
  ]
}
```

Sample Response 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."
  }
}
```

Anti-Malware Reputation

This section contains the following topics:

Retrieving Anti-Malware Reputation Details

You can retrieve the objects containing details of anti-malware scanning services, web reputation services, and malware analytics services settings.

Synopsis	`GET wsa/api/v3.0/security_services/anti_malware_and_reputation`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the objects containing details of anti-malware scanning services, web reputation services, and malware analytics services settings..

Sample Request

```
GET wsa/api/v3.0/security_services/anti_malware_and_reputation HTTP/1.1
Host: dut037.perf8:4431
Authorization: Basic YWRtaW46SXJvbnBvcnRAMTIz
```

Sample Response

```
{
 "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(.psd1)",
  "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)",
  "H1wfile(.H1W)",
  "Aspfile(.cdx)",
  "XEV.GenericApp(.xevgenxml)",
  "VisualStudio.Launcher._sln71(._sln71)",
  "VisualStudio.Launcher._sln70(._sln70)",
  "JNLPFILE(.jnlp)",
  "VisualStudio.Launcher._vjsxsln80(._vjsxsln80)",
  "BrmFile(.printerExport)",
```

```
"Group_wab_auto_file(.group)",
"Icmfile(.icm)",
"XTPFILE(.xtp)",
"Vxdfile(.vxd)",
"Outlook.File.hol.14(.hol)",
"H1sfile(.H1S)",
"H1tfile(.H1T)",
"Jtpfile(.jtp)",
"H1vfile(.H1V)",
"GCSXFile(.gcsx)",
"H1hfile(.H1H)",
"Ocxfile(.ocx)",
"AcroExch.SecStore(.secstore)",
"H1kfile(.H1K)",
"MSGraph.Chart.8(.gra)",
"RDBFileProperties.1(.sfcache)",
"InfoPath.SolutionManifest.3(.xsf)",
"Scrfile(.scr)",
"H1dfile(.H1D)",
"Wmffile(.wmf)",
"H1ffile(.H1F)",
"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(.ps1xml)",
"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)",
"H1cfile(.H1C)",
"Wcxfile(.wcx)",
"OneNote.TableOfContents(.onetoc)",
"CABFolder(.cab)",
"VisualStudio.Launcher._vcppxsln80(._vcppxsln80)",
"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._vwdxsln80(._vwdxsln80)",
  "Wordhtmlfile(.dochtml)",
  "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(.dothtml)",
  "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)",
  "Publishermhtmlfile(.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)",
  "Accessthmltemplate(.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(.xfdf)",
  "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(.psc1)",
    "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": "testfilerepserver.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"
    ]
   }
  }
 }
}
```


Modifying the Anti-Malware Reputation Details

You can modify objects that contain details of anti-malware scanning services, web reputation services, and malware analytics services settings.

Synopsis	`PUT wsa/api/v3.0/security_services/anti_malware_and_reputation`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the objects containing details of anti-malware scanning services, web reputation services, and malware analytics services settings.

Sample Request

```
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(.psd1)",
                    "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(.xfdf)",
                    "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(.dochtml)",
            "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(.dothtml)",
            "Outlook.File.det.14(.det)",
            "Excel.Addin(.xla)",
            "OfficeTheme.12(.thmx)",
            "PowerPoint.Show.8(.ppt)",
            "Word.Document.8(.doc)",
            "Powerpointhtmlfile(.ppthtml)",
            "Outlook.File.oft.14(.oft)",
            "Publishermhtmlfile(.pubmhtml)",
            "Excel.Template.8(.xlt)",
            "Excel.Sheet.8(.xls)",
            "Word.Template.8(.dot)"
        ]
    },
    "Database": {
        "selected": [],
        "not_selected": [
            "Access.Application.14(.accdb)",
            "Access.ACCDCFile.14(.accdc)",
            "Access.ACCDAExtension.14(.accda)",
            "Access.ACCDEFile.14(.accde)",
            "Access.MDBFile(.mdb)",
            "Access.Extension.14(.mda)",
            "Access.MDEFile.14(.mde)",
            "Access.ACCDRFile.14(.accdr)",
            "Access.Shortcut.Report.1(.mar)",
            "Access.WebApplicationReference.14(.accdw)",
            "Access.ACCDTFile.14(.accdt)",
            "Access.WizardUserDataFile.14(.accdu)",
            "ACLFile(.acl)",
            "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)",
            "Accessthmltemplate(.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)",
            "JNLPFILE(.jnlp)",
            "VisualStudio.Launcher._vjsxsln80(._vjsxsln80)",
            "Campfile(.camp)",
            "BrmFile(.printerExport)",
            "Group_wab_auto_file(.group)",
```

```
            "Icmfile(.icm)",
            "XTPFILE(.xtp)",
            "Vxdfile(.vxd)",
            "Outlook.File.hol.14(.hol)",
            "H1sfile(.H1S)",
            "H1tfile(.H1T)",
            "Jtpfile(.jtp)",
            "H1vfile(.H1V)",
            "H1wfile(.H1W)",
            "H1hfile(.H1H)",
            "Ocxfile(.ocx)",
            "AcroExch.SecStore(.secstore)",
            "H1kfile(.H1K)",
            "Contact_wab_auto_file(.contact)",
            "MSGraph.Chart.8(.gra)",
            "RDBFileProperties.1(.sfcache)",
            "Scrfile(.scr)",
            "H1dfile(.H1D)",
            "Wmffile(.wmf)",
            "H1ffile(.H1F)",
            "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._vcsxsln80(._vcsxsln80)",
            "VisualStudio.Launcher._sln(._sln)",
            "XTP2FILE(.xtp2)",
            "RemoteAssistance.1(.msrcincident)",
            "Microsoft.PowerShellXMLData.1(.ps1xml)",
            "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(.psc1)",
                "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"
                    ]
                }
            }
        }
    }
```


Sample Response

```
Response: 204 (No-content)
```

Registering the Anti-Malware Analytics Console

You can retrieve a list of objects containing details of malware analytics console endpoints registration status.

Synopsis	`GET wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registration`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to retrieve the list of objects containing details of malware analytics console endpoints registration status.

Sample Request

```
GET wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registration HTTP/1.1
Host: wsa118.cs14:10118
Authorization: Basic Auth
```

Sample Response 1—Before Registration

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

Sample Response 2—After Registration

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

Deleting the Anti-Malware Analytics Console Registeration

You can delete the list of objects containing details of malware analytics console endpoints registration status.

Synopsis	`DELETE wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registration`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to delete the list of objects containing details of malware analytics console endpoints registration status.

Sample Request

```
DELETE wsa/api/v3.0/security_services/malware_analytics_endpoints_console_registrationHTTP/1.1
Host: wsa118.cs14:10118
Authorization: Basic Auth
```

Sample Response

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

End-User Notification

This section contains the following topics:

Retrieving the End-User Notification Details

You can retrieve End-User Notification configuration information for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/security_services/eun_config`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the End-User Notification configuration.

Sample Request

```
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
```

Sample Response

```
{
    "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
        }
    }
}
```

Modifying End-User Notification Details

You can modify the End-User Notification configuration information for Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`PUT /wsa/api/v3.0/security_services/eun_config`

Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify an End-User Notification configuration.

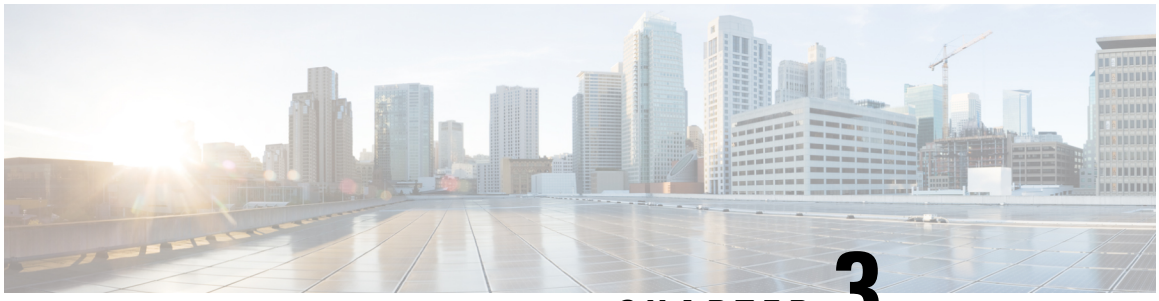
.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
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
    }
  }
}
```

Sample Response

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



CHAPTER 3

General Purpose APIs

General purpose configuration queries have the **configure** resource name as part of the query string. You can retrieve configuration information (GET), and perform any changes (POST, DELETE) in the configuration data.

Synopsis	`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`	

Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Retrieving SMTP Relay Host Details

Sample Request

```
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
```

Sample Response

```
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"}
```

Adding New SMTP Relay Hosts

Sample Request

```
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"
        }
    ]
}
```

Sample Response

```
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"}
```

Modifying SMTP Relay Host Details

Sample Request

```
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"
        }
    ]
}
```

Sample Response

```
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"}
```

Deleting Multiple SMTP Relay Hosts

Sample Request

```
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"
    }
]
```

Sample Response

```
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"}
```

Deleting All SMTP Relay Hosts

Sample Request

```
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
}
```

Sample Response

```
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"}
```

Retrieving APIs Accessible to a User Role

You can retrieve a list of APIs that are available for a currently logged in user.

Synopsis	`GET /api/v2.0/login/privileges`
Request Headers	Host, Accept, Authorization

Response Headers	Content-Type, Content-Length, Connection

Sample Request

```
GET /wsa/api/v2.0/login/privileges HTTP/1.1
cache-control: no-cache
Postman-Token: 0cd8d318-e29b-40e0-bdc8-473f09cbd2b2
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
```

Sample Response

```
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_availbility",
"w_proxy_traffic_charateristics", "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"]}
```

Retrieving the SecureX Files

You can retrieve the details of the registered user.

Synopsis	`GET /wsa/api/v2.0/ctr/user_info`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve the user information of the registered user.

Sample Request

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

HTTP/1.1
```

Sample Response

```
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


{
    "client_id": "client-4c50a1ca-34ad-47c8-a37b-9b16153db578",
    "server": "apjc"
}
```

Sample Request for Token Request

```
GET/wsa/api/v2.0/ctr/token

HTTP/1.1
```

Sample Response for Token Request

```
HTTP/1.1 200 OK
Date: Thu, 25 Mar 2021 07:51:19 GMT
Content-type: application/json
Content-Length: 87
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
{
"access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.
eyJodHRwczpcL1wvc2NoZW1hcy5jaXNjby5jb21cL2lyb2hcL2lkZW50aXR5XC9jbGFpbXNcL3VzZXJcL2VtYWls
IjoiYWhhcmluYXQrYXBqY0BjaXNjby5jb20iLCJodHRwczpcL1wvc2NoZW1hcy5jaXNjby5jb21cL2lyb2hcL2lk
ZW50aXR5XC9jbGFpbXNcL3VzZXJcL3Njb3BlcyI6WyJpcm9oLWFkbWluI
iwiaW50ZWdyYXRpb24iLCJwcml2YXRlLWludGVsIiwiYWRtaW4iLCJwcm9maWxlIiwiaW5zcGVjdCIsImlyb2gt
YXV0aCIsInNzZSIsInVzZXJzIiwiY2lzY28iLCJjYXNlYm9vayIsIm9yYml
0YWwiLCJlbnJpY2giLCJvYXV0aCIsImdsb2JhbC1pbnRlbCIsImNvbGxlY3QiLCJyZXNwb25zZSIsInVpLXNldH
RpbmdzIl0sImh0dHBzOlwvXC9zY2hlbWFzLmNpc2NvLmNvbVwvaXJvaFwvaWRlbnRpdHl
cL2NsYWltc1wvdXNlclwvbmljayI6IkFkaGl0aHlhIEhhIiwiZW1haWwiOiJhaGFyaW5hdCthc
GpjQGNpc2NvLmNvbSIsInN1YiI6ImRiNGFiYTc0LWRiZWYtNGMxMC1iZDE4LTgzNjQ1NGJiZjU2MyIsImlzcyI6IklS
 T0ggQXV0aCIsImh0dHBzOlwvXC9zY2hlbWFzLmNpc2NvLmNvbVwvaXJvaFwvaWRlbnRpdHlcL2NsYWltc1wvc2NvcGVzI
jpbImVucmljaDpyZWFkIiwicmVzcG9uc2UiXSwiZXhwIjoxNTYzNzg4NjU5LCJodHRwczpcL1
hcy5jaXNjby5jb21cL2lyb2hcL2lkZW50aXR5XC9jbGFpbXNcL29hdXRoXC9jbGllbnRcL2lkIjoiY2xpZW50LTRjNTBhMWNhL
TM0YWQtNDdjOC1hMzdiLTliMTYxNTNkYjU3OCIsImh0dHBzOlwvXC9zY2hlbWFzLmNpc2NvLm
NvbVwvaXJvaFwvaWRlbnRpdHlcL2NsYWltc1wvdmVyc2lvbiI6InYxLjIwLjAtOTNjMTkyOGIzMmEwZWRiNDk1ZTUiL
CJpYXQiOjE1NjM3ODgwNTksImh0dHBzOlwvXC9zY2hlbWFzLmNpc2NvLmNvbVwvaXJvaFwvaWRlbnRpd
HlcL2NsYWltc1wvb2F1dGhcL2tpbmQiOiJhY2Nlc3MtdG9rZW4ifQ.SfSzvuAJbwf4gz72KPT2HEYB8D_1g8Xlk8E0O8q9Hrlre
EMl6M9nyFY3YPJueaE6J30mw258Pg8ISoG2b1mN4O5N1hnHe-0zIEmOZbYWfp9puz-0FMfQJ
ysXZ1mRJkxwxWaMJ4c0rPGaPPEuw
ER2Qi6Ql8Xg9FZgp9-s5mEebeWFRbvLW9Zly1h7mjICoNF9n1y1bU8QZt0g549kIj-s047lf2qatkeoRWxinLPGtIeGl9M1s
Cvqya1sGgpGf-hFBB2KvU4JZ-c94vIYdMOHeeh7QtMIpJhy
isClanrq7ke6NJlQHyi2WYifcnRnhe5BVl6MiVE89xq3CmkNBYxG5g",
"token_type": "bearer", "expires_in": 600, "scope": "enrich:read response"
}
```

Modifying the SecureX File Settings

You can modify the registered user details.

Synopsis	`PUT /wsa/api/v2.0/ctr/user_info`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the registered user details for SecureX.

Sample Request

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

HTTP/1.1
```

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

{"data":{"client_id":"Y2xpZW50LWY2NzQzNjdlLTJhOTMtNDI3Yy05MGVmLWJjZmFhMGVkY2RjNA==",

"client_secret":"QmlHbGlpeFlENXNxQWVkb0R1NFprSTdzaDVGaVc5OEJMYVhEWkcydlBtWWJnR3Bud0pVZUF3",

"server":"YXBqYw=="}

}
```

Adding the User Information Details for SecureX

You can add the user information details for SecureX. This operation allows you to login to the SecureX ribbon.

Synopsis	`POST /wsa/api/v2.0/ctr/user_info`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to create the user information.

Sample Request

```
HTTP/1.1


{"data":{"client_id":"Y2xpZW50LWY2NzQzNjdlLTJhOTMtNDI3Yy05MGVmLWJjZmFhMGVkY2RjNA==",

"client_secret":"MFVTTS05cERieVh0RDF5RGE2dzZvMnlJTWtwNkZ1eFU2YnJIY1VkcW1wdzZ0M1pNMTVVWGNn",

"server":"YXBqYw=="}
```

```
}
```

Sample Response

```
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
```

Retrieving Auth Settings

You can retrieve the basic information about current authentication related configurations in Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/generic_resources/auth_settings`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve authentication settings configuration on the device.

Sample Request

```
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
```

Sample Response

```
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"
        }
    ]
}
```

Retrieving User Agents

You can retrieve all allowed user agents recognized by Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/generic_resources/user_agents`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve all user agents recognized by the device.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
```

Sample Response

```
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"
        ]
}
```

Retrieving URL Categories

You can retrieve all allowed URL categories that are defined by Secure Web Appliance. This API also contains some user defined categories. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/generic_resources/url_categories`	
Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve all URL categories (predefined and custom) configured on the device.

Sample Request

```
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
```

Sample Response

```
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"
        ]
}
```

Retrieving Time Ranges

You can retrieve list of time ranges that are configured in Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/web_security/time_ranges`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve configured time ranges on the device.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
```

Sample Response

```
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"
        }
    ]
}
```

Retrieving Quotas

You can retrieve list of quotas that are configured in Secure Web Appliance. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/web_security/quotas`

Supported Resource Attributes	For more information, see AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve configured quotas on the device.

Sample Request

```
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 YWRtaW46Q2lzY28xMjMk
```

Sample Response

```
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"
        }
    ]
}
```

Retrieving Proxy Settings

You can retrieve proxy (web proxy, socks proxy, and so on) related configurations in Secure Web Appliance. The response indicates whether a particular type of proxy is enabled or not. It also provides information about the mode of the proxy, like transparent or forward (only applicable in web proxy). The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/generic_resources/proxy_settings`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to retrieve proxy (web proxy, socks proxy etc.) related configurations on the device.

Sample Request

```
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
```

Sample Response

```
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"
    }
}
```

Retrieving Identification Methods

You can retrieve allowed and not allowed identification methods information which can be used while creating identification profiles. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/generic_resources/identification_methods`	
Supported Resource Attributes	See AsyncOS API - Addendum to the Getting Started Guide for Secure Web Appliance for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows a query to get identification methods configured on the device.

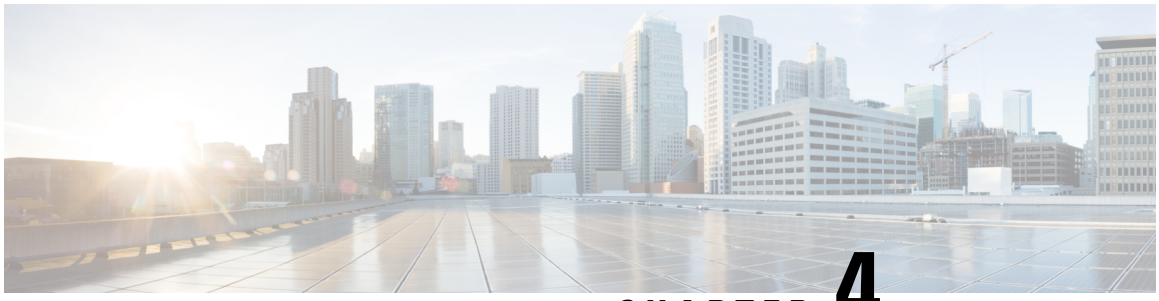
Sample Request

```
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
```

Sample Response

```
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"
    }
}
```



CHAPTER 4

Troubleshooting AsyncOS API

API Logs

Enable and subscribe to the API logs using **System Administration** > **Log Subscriptions**. For instructions, see the User Guide for Cisco Secure Web Appliance.

Some of the events logged in the API logs are as follows:

- API has started or stopped
- Connection to the API failed or closed (after providing response)
- Authentication succeeded or failed
- Request contains errors
- Error while communicating network configuration changes with AsyncOS API

Alerts

Ensure that the appliance is configured to send you alerts related to AsyncOS API. You will receive alerts when:

Alert Description	Type	Severity
API has restarted due to an error	System	Warning