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 for the types of reporting queries are shown below:

• Retrieving a Single Value for a Counter, on page 4
• Retrieving Multiple Values for a Counter, on page 4
• Retrieving Single Values for Each Counter in a Counter Group, on page 5
• Retrieving Multiple Values for Multiple Counters, on page 6
• Retrieving Multiple Values for Multiple Counters, with Multiple Values for Each Counter, on page 7

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

This example shows a query to retrieve multiple values for multiple counters, with the offset and 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, 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 11
- Retrieving the Details of a Schedule Report Entry, on page 13
- Adding a Scheduled Report Entry, on page 13
- Editing a Scheduled Report Entry, on page 14
- Deleting Scheduled Reports, on page 15

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 18
- Retrieving Archived Reports, on page 19
- Retrieving the Details of a Archive Report Entry, on page 20
- Adding an Archive Report Entry, on page 21
- Deleting an Archived Report Entry, on page 22

Searching Archived Reports

The following example shows how to search for a list of top 20 archived reports based on the report title and sorted by the date and time the report is 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 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 22
- Layer 4 Traffic Monitor, on page 25
- SOCKS Proxy, on page 27

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 12.5 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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	See *AsyncOS 12.5 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 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=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	See *AsyncOS 12.5 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 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=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

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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v3.0/web_security/overall_bandwidth_limit`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`PUT /wsa/api/v3.0/configure/web_security/overall_bandwidth_limit`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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:

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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliance. The 'file_name' parameter can be used to get a particular file from the Web Security Appliance.

Synopsis	`GET /wsa/api/v3.0/security_services/pac_file`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security 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 Web Security Appliance. The ‘file_name’ parameter can be used to get a particular file from the Web Security Appliance.

Synopsis	`GET /wsa/api/v3.0/security_services/pac_file`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security 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.

Note Multiple files can be uploaded in a single request.

Synopsis	`POST /wsa/api/v3.0/security_services/pac_file`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* for more information.	
Request Headers		Host, Accept, Authorization
Response Headers		Content-Type, Content-Length, Connection

Example

This example shows how to modify the 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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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

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

Synopsis	`GET /wsa/api/v3.0/web_security/identification_profiles`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`PUT /wsa/api/v3.0/web_security/identification_profiles`

Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`POST /wsa/api/v3.0/web_security/identification_profiles`
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v3.0/web_security/identification_profiles`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliance.

Synopsis	`GET /wsa/api/v3.0/web_security/access_policies`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/web_security/domain_map`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/ network/upstream_proxy`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances.

Synopsis	`PUT /wsa/api/v2.0/configure/network/upstream_proxy`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v2.0/configure/network/upstream_proxy`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/security_services/proxy/https`

Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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-----
MIIDtTCCAp2gAwIBAgIJALizeKzqUcKrMA0GCSqGSIb3DQEBCwUAMEQxCzAJBgNV
BAYTAklOMREwDwYDVQQKEwhDSVNDT1NCRzELMAkGA1UECxMCQ1MxFTATBgNVBAMT
DGR1dDAzNy5wZXJmODAeFw0yMTAxMTkwNzUxNTdaFw0yMzEyMTkwNzUxNTdaMEQx
CzAJBgNVBAYTAklOMREwDwYDVQQKEwhDSVNDT1NCRzELMAkGA1UECxMCQ1MxFTAT
BgNVBAMTDGR1dDAzNy5wZXJmODCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBALaopARbEuWowXwDshJL6jc35s92Wb/aScnBF6w0TNS0C63BKfsmSyWUF2JP
HgoiX6ioPgNNWcJA0z2nKQngFei6SvESl7s8nbBzNBRNiUo9NtP00fkUIJ+FmzYL
utfSB+Etr2E16j8OedQjjMYWGxFUKBMirpEcqlz2aBcCcvzW80ABfGdzcv43p0+R
PPxdV722Wr0sH0zaPf+NZwC1cHlKmIITIHBApJEmHBYYjraY0ulBEN9kkEjtCdS7
djLdYIbRmxSJqNyPrQmjo/oA6aeHC+0jPkffCK2JDnc3buFvg23SD/L2JseMsz4x
iGz3NALZldHDyjPyhW+ZW/AK63sCAwEAAaOBqTCBpjAdBgNVHQ4EFgQUpyD8ZGWJ
I/HtEidCHNQOt1WY62YwdAYDVR0jBG0wa4AUpyD8ZGWJI/HtEidCHNQOt1WY62ah
SKRGMEQxCzAJBgNVBAYTAklOMREwDwYDVQQKEwhDSVNDT1NCRzELMAkGA1UECxMC
Q1MxFTATBgNVBAMTDGR1dDAzNy5wZXJmOIIJALizeKzqUcKrMA8GA1UdEwEB/wQF
MAMBAf8wDQYJKoZIhvcNAQELBQADggEBAJJw9cO3zxGykZieVW9RgnkHkUp0sq7D
EZE5Lajb1ntQB/vfBp8zfxfSRPl+dyAahH5Mb5H+9XigNr2hEDsTZ7jwbnczfPQD
HuJ6V3OExb12CZZ4ex/OKlxonPWWB+1jiG3RqML9jUZg2cccDSPxHv76+DrrEJnH
P+M2f7QrrLwuTlDQ3X/SrPefrGJ3de1dydQvxjh4mTjMudhKgfmj4ps/UWGTV6xW
dc4MvWorajRPhkznuelwGlt5xrVebv3/hdJPKxuNrBYyXR6SY1U9VjK2HByiS9tO
Ot+EaRqbvgMRKheCVBgffXWxWgZWQ/TsOVVj/4zkBgLQZOdJiKWTGYM=
-----END CERTIFICATE-----
```

Retrieving the HTTP Proxy OCSP Settings

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

Synopsis	`GET /wsa/api/v2.0/configure/security_services/proxy/ocsp`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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

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

Synopsis	`GET /wsa/api/v2.0/configure/system/log_subscriptions`
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliance. The syntax and supported attributes are as follows:

Synopsis	`DELETE /wsa/api/v2.0/configure/system/log_subscriptions`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliances. The syntax and supported attributes are as follows:

Synopsis	`GET /wsa/api/v2.0/configure/ system/log_subscriptions/fields`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security Appliance.

Synopsis	`GET /wsa/api/v3.0/network/xauth_header_setting`	
Supported Resource Attributes	See *AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 Web Security 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances* 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
```