AlgoSec Security Management Suite

Software Version: A30.10

API Guide

View our most recent updates in our online ASMS Tech Docs.

Document Release Date: 4 May, 2020 | **Software Release Date**: April 2020

Legal Notices

Proprietary & Confidential Information

Contents

ASMS API reference

AlgoSec Security Management Suite offers access to many features via web services, which are APIs that can be accessed and executed over the network. Web service APIs enable you to perform remote operations in ASMS without using the product interface directly.

Web service APIs are supported via REST for AFA, FireFlow, and AppViz, and via SOAP for AFA and FireFlow. In general, REST services are more advanced and are recommended for use over SOAP.

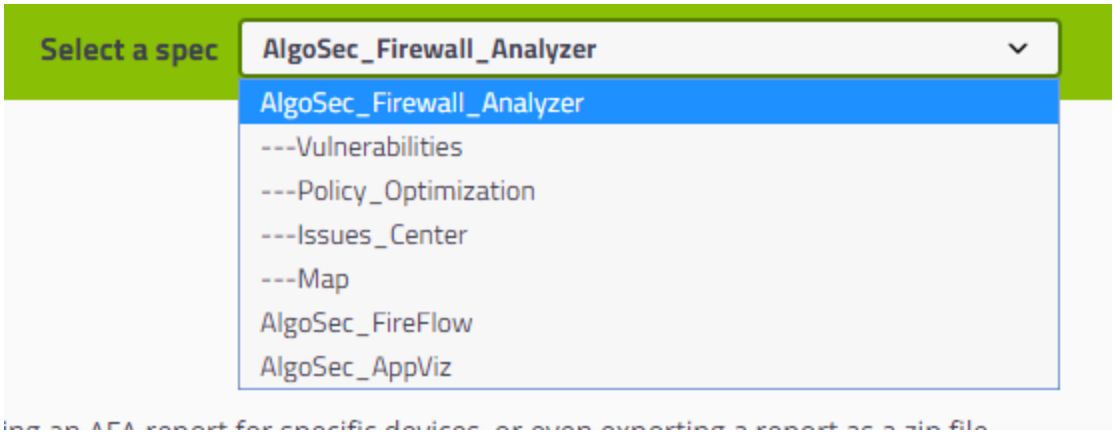
ASMS Swagger documentation

ASMS provides a set of Swagger API documentation, available from inside ASMS.

Swagger enables you to execute API request calls and access lists of request parameters. Access the ASMS Swagger API documentation using one of the following methods:

From inside ASMS	From AFA, FireFlow, or AppViz, do the following: 1. In the toolbar, click your username and click **API Documentation**. 2. Click the links to access Swagger documentation for REST APIs.
Directly from your browser	Log in to ASMS, and navigate to **https://<ASMS IP address>/algosec/swagger/swagger-ui.html**.

In Swagger, select the spec for the APIs you want to view from the drop-down at the top-right.



ASMS API Tech Docs reference

Both REST and SOAP APIs are also documented in the Tech Docs. For details, see:

- AFA REST web services
- AFA SOAP web services
- FireFlow REST web services
- FireFlow SOAP web services
- AppViz REST web services

Device names in the ASMS APIs

ASMS API parameter names and descriptions use the following terms to refer to devices managed by ASMS:

• **display name** • **entity name**	The device's name, as displayed in the UI, both at the bottom level of the device tree, and in other ASMS pages and reports. This name is not necessarily unique, and is therefore not recommended for use via API.

• **tree name** • **treeName** • **name** • **unique name** • **database name** • **canonized name**	A name for the device that includes an aggregated string of the device's name and the name of any parent or grandparent devices. This name is not displayed in the ASMS UI, and must be returned from the database by API. Since this name includes the tree hierarchy, it's used as the unique system device.

AFA REST web services

This section describes the AlgoSec Firewall Analyzer REST web services APIs.

Note: To view vulnerability data in AFA device reports, you must either have vulnerability scanners configured in AppViz, or import your vulnerability data manually.

For more details, see the AppViz User Guide and Import vulnerability data.

Base URL

There are two types of base URLs and corresponding authentication method:

- The base URL for most requests is:

  ```
  https:://<algosec_server>/afa/api/v1
  ```

  where **<algosec_server>** is the AFA server URL.

  Authentication is through a cookie session. For example:

  ```
  curl --cookie "PHPSESSID=g4mgnv4cno9ivt7rclmhmejj27" https://
  <IP:Port>/afa/api/v1/security_zones/get_profiles_list
  ```

- The base URL for the remaining requests is:

  ```
  https://<algosec_server>/fa/server
  ```

  where **<algosec_server>** is the AFA server URL.

  Authentication is through a URL parameter. For example:

  ```
  curl -H "Accept:application/json" -k " https://192.168.3.76/fa/server/
  rules/read?session=c69bcc3e6832149642b32e6f269c82c0&entity=admin
  ```

Note: For each request, the documentation specifies the base URL and authentication method.

Swagger

The AlgoSec Firewall Analyzer RESTful API includes Swagger support, enabling you to execute simplified API request calls and access full lists of request parameters.

To access Swagger API documentation:

1. In the toolbar, click your username and click **API Documentation**.
2. From the dropdown at the top-right, select one of the following options:

AlgoSec_Firewall_Analyzer	Controls most central AFA API requests, such as object or device requests
Vulnerabilities	Controls AFA API requests related to vulnerabilites.
Policy_Optimization	Controls AFA APIs related to network rules.
Issues_Center	Controls AFA APIs related to the ASMS Issues Center
Map	Control AFA APIs related to the ASMS network map.

AFA REST API reference

The following table lists the REST APIs supported for AFA. For more details, see EntitiesResponse type and AFA search rule fields.

Feature	APIs
Login and logout	Log in to ASMS Log out of ASMS
Analysis and reports	Start an analysis Retrieve an analysis status Retrieve a baseline compliance report Running the Query Troubleshooting Tool

Feature	APIs
Object data	Retrieve network objects Retrieve service objects Retrieve interfaces Identify missing routers Merge routers Get details for a specified device Add/Edit a device Delete a device Get a list of devices Get data on managed devices
Risks	Retrieve a risk profile list
Rule data	Retrieve rules Retrieve risky rules Rules hit count
Security zones	Retrieve security zones Assign zone types to interfaces
User data	Retrieve user data Retrieve role data
Issues Center	Manage AFA issues
Relocating devices	Relocate devices between nodes Check device relocation progress Cancel device relocation
Traffic Simulation	Traffic simulation query

Login and logout APIs

The AFA REST API supports the following APIs for logging in and out of ASMS:

Log in to ASMS

The AFA REST API uses sessions to avoid re-authenticating with every request. You obtain a session ID with the `login` request, which is used in all other REST API requests.

Resource Name: `/fa/server/connection/login`

Request Method: POST

Request:

Element	Type	Description
`username`*Mandatory*	String	AlgoSec Security Management Suite username.
`password`*Mandatory*	String	AlgoSec Security Management Suite password.
`domain`*Optional*	String	Domain name. Relevant only when domains are enabled. Default: **0**

Response:

Element	Type	Description
`SessionID`	String	Session ID you will use in all your requests.
`status`	String	One of the following: ■ `true`. Indicates login succeeded. ■ `false`. Indicates login failed.
`message`*Only is returned when the request fails.*	String	An error message.

Request example

```
curl -H "Accept: application/json" -k --data "username=ned&password=
algosec" 'https://192.168.3.198/fa/server/connection/login'
```

Response example

```
{"SessionID":"0b4bd2cff378f66bc55eeadb89537cde"} HTTP Code=200 OK
{"message": "incorrect user/password combination"} HTTP Code=401
Unauthorized
```

Log out of ASMS

The `logout` request terminates the session, invalidating the session ID for any additional requests.

Resource Name: `/fa/server/connection/logout`

Request Method: POST

Request:

Element	Type	Description
`session`	String	Session ID returned in `login` request.

Response:

Element	Type	Description
`SessionID` *Only is returned when the request succeeds.*	String	Session ID.
`status`	String	One of the following: ■ `true`. Indicates logout succeeded. ■ `false`. Indicates logout failed.
`message` *Only is returned when the request fails.*	String	An error message.

Request example

```
curl -k --data "session=061e25b659d75ac22255133feb628cc2"
'https://192.168.3.198/fa/server/connection/logout'
```

Response example

```
{"SessionID": "5f779cceb9c6936926cea98178ec5a61",   "status": true}
```

Analysis and report APIs

The AFA REST API supports the following APIs for managing analysis and AFA reports:

- Start an analysis
- Retrieve an analysis status
- Retrieve a baseline compliance report
- Running the Query Troubleshooting Tool

Start an analysis

The `start_analysis` request initiates an analysis on a device, group, or matrix.

The input will be the active session ID and the name of the device, group, or matrix. The output will include a status and message which indicates success or failure.

Resource Name: `/fa/server/analysis/start`

Request Method: POST

Request URL Parameters:

Element	Type	Description
`session`*Mandatory*	String	Session ID returned in `login` request.
`entity`*Mandatory*	String	The display name of the device, group, or matrix.

`entityType`*Mandatory*	String	One of the following:
		`device`
		`group`
		`matrix`

Response:

Element	Type	Description
`status`	String	One of the following: ■ `true`. Indicates the request succeeded. ■ `false`. Indicates the request failed.
`message`	String	An message which indicates success or a reason for failure.

Request example

```
curl -k " -H "Accept:application/json" 'https://10.20.1.242/fa/server/
analysis/start?session=d42b992578b5f3ef07358a29797bd442&entityType=
device&entity=Humus'
```

Response example

```
{   "status": true,   "message": "success"}
```

Retrieve an analysis status

AFA's REST API enables you to retrieve the status of a specific analysis, or the statuses of all analyses currently running.

Get all current analysis statuses

The **status** request retrieves the statuses of all analysis processes currently running in AFA.

This request has no parameters, but only responds with data about current analyses if an analysis is actually running. If no analysis is running, the response returns null.

Resource Name:

```
/api/v1/analyzeTask/status
```

Request Method: GET

Response:

If one or more analysis processes are currently running in AFA, the response will include the following data for each analysis:

reportID	The name of the report currently being generated
deviceName	The name of the device on which the analysis is running
status	The current analysis status. One of the following: • COLLECTING_DATA • QUEUED • INIT • RUNNING
updatedDate	The date and time the analysis status was last updated, in Unix epoch time format.

Note: If no analysis is currently running in AFA, the response is empty.

Request example

```
curl -X GET "https://<AFA server IP>/afa/api/v1/analyzeTask/status" -H
"accept: */*"
```

Response example

```
[
{
"reportId": "afa-5276",
"deviceName": "Poppy",
"status": "INIT",
"updatedDate": 1581515387753
},
{
"reportId": "afa-5289",
"deviceName": "Rose",
"status": "INIT",
```

```
"updatedDate": 1581515392769
},
{
"reportId": "afa-5291",
"deviceName": "Daffodil",
"status": "INIT",
"updatedDate": 1581515399219
},
{
"reportId": "afa-5288",
"deviceName": "Buttercup",
"status": "INIT",
"updatedDate": 1581515390297
},
{
"reportId": "afa-5290",
"deviceName": "Lily",
"status": "INIT",
"updatedDate": 1581515394252
}
]
```


Get status of a specific analysis

The **get_analysis_status** request retrieves the current status of an analysis.

The input will be the active session ID and the device, group or matrix display name. The output will indicate the status of the analysis.

Resource Name:

```
/fa/server/analysis/status
```

Request Method: GET

Request URL Parameters:

Element	Type	Description
session Mandatory	String	Session ID returned in login request.
entity Mandatory	String	The display name of the device, group, or matrix.
entityType Optional	String	One of the following: • **device** (default) • **group** • **matrix**

Response:

Element	Type	Description
reportStatus	String	The status of the analysis. One of the following: ■ **FAILED** ■ **COMPLETED** ■ **RUNNING**
status	String	One of the following: ■ **true**. Indicates the request succeeded. ■ **false**. Indicates the request failed.
message Returned only if the request fails.	String	An error message.

Request example

```
curl -H "Accept:application/json" -k 'https://<AFA server IP address>/
fa/server/analysis/status?entity=fw1&entityType=device&session=
f87381213f579c424370e9c21c709e40'
```

Response example

```
{   "status": true,   "reportStatus": "FAILED"}
```

Retrieve a baseline compliance report

The `baseline_compliance` request retrieves the baseline compliance report for a device.

The input will be the active session ID and the device name. The output will be the Baseline Compliance Report in JSON format.

Resource Name: `/afa/api/v1/baseline_compliance`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`device` *Mandatory*	String	The name of the device: • Currently, baseline compliance reports are only supported for devices which are of type firewall, and not groups or matrices. In the '`device_data`' DB table, the devices are '`type`' = 0. • Device 'name' is `device_data` from the DB table, not '`display_name`'.

Response:

Element	Type	Description
`device`	String	Name of the device.
`version`	String	Version of the device.
`policy`	String	Policy on the device.
`date`	String	Date of report in YYYY-MM-DD format.
`profile`	String	Name of baseline profile.
`baseline_compliance_score`	Integer	Baseline compliance score.

Element	Type	Description
passed_requirement_count	Integer	Number of successful requirements.
failed_requirement_count	Integer	Number of failed requirements.
requirements	List of BaselineRequirementResult type objects	A list of baseline requirement result objects.

Request example:

```
curl -i -H "Accept:application/json" -k "https://127.0.0.1:7443/
afa/api/v1/baseline_compliance?session=
8ikhlni6c46dvbdcton4aqmcj2&device=10_132_20_1_root"
```

Response example:

```
{
"device" : "root (62.219.117.1)",
"version" : "Fortinet FortiGate Fortigate-50B v4.0,build0689,140731 (MR3
Patch 18)",
"policy" : "10_132_20_1_root.fortigate",
"date" : "2019-03-14",
"profile" : "FortiGateProfile",
"baseline_compliance_score" : 55,
"passed_requirement_count" : 8,
"failed_requirement_count" : 6,
"requirements" : [ {
"name" : "Device details",
"status" : "UNKNOWN",
"id" : 1,
"tests" : [ {
"command" : "Get System Status",
```

```
"criterion" : "Manual Review",
"item" : "System time:\\s(.*)",
"comments" : "Found: Thu Mar 14 12:00:27 2019",
"status" : "UNKNOWN",
"id" : 1
}, {
"command" : "Get System Status",
"criterion" : "Manual Review",
"item" : "IPS-DB:\\s*(.*)",
"comments" : "Found: 3.00295(2013-01-30 19:23)",
"status" : "UNKNOWN",
"id" : 2
}, {
"command" : "Get System Status",
"criterion" : "Manual Review",
"item" : "Serial-Number:\\s*(.*)",
"comments" : "Found: FGT50B3G11605125",
"status" : "UNKNOWN",
"id" : 3
}, {
.
.
}, {
"command" : "Get System Status",
"criterion" : "Manual Review",
"item" : "Virtual domains status:\\s*(.*)",
"comments" : "Found: 9 in NAT mode, 1 in TP mode",
"status" : "UNKNOWN",
"id" : 14
```

```
} ]
.
.
}, {
"name" : "Time out Settings",
"status" : "PASSED",
"id" : 17,
"tests" : [ {
"command" : "Global Configuration",
"criterion" : "Required Regexp",
"item" : "set admintimeout\\s(.*)",
"comments" : "Found: 480",
"status" : "PASSED",
"id" : 1
} ]
} ]
}
```


Retrieve a baseline compliance report

The `baseline_compliance` request retrieves the baseline compliance report for a device.

The input will be the active session ID and the device name. The output will be the Baseline Compliance Report in JSON format.

Resource Name: `/afa/api/v1/baseline_compliance`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`device` *Mandatory*	String	The name of the device: • Currently, baseline compliance reports are only supported for devices which are of type firewall, and not groups or matrices. In the '`device_data`' DB table, the devices are '`type`' = 0. • Device 'name' is `device_data` from the DB table, not '`display_name`'.

Response:

Element	Type	Description
`device`	String	Name of the device.
`version`	String	Version of the device.
`policy`	String	Policy on the device.
`date`	String	Date of report in YYYY-MM-DD format.
`profile`	String	Name of baseline profile.
`baseline_compliance_score`	Integer	Baseline compliance score.
`passed_requirement_count`	Integer	Number of successful requirements.
`failed_requirement_count`	Integer	Number of failed requirements.
`requirements`	List of BaselineRequirementResult type objects	A list of baseline requirement result objects.

Request example:

```
curl -i -H "Accept:application/json" -k "https://127.0.0.1:7443/
afa/api/v1/baseline_compliance?session=
8ikhlni6c46dvbdcton4aqmcj2&device=10_132_20_1_root"
```

Response example:


```
{
"device" : "root (62.219.117.1)",
"version" : "Fortinet FortiGate Fortigate-50B v4.0,build0689,140731 (MR3
Patch 18)",
"policy" : "10_132_20_1_root.fortigate",
"date" : "2019-03-14",
"profile" : "FortiGateProfile",
"baseline_compliance_score" : 55,
"passed_requirement_count" : 8,
"failed_requirement_count" : 6,
"requirements" : [ {
"name" : "Device details",
"status" : "UNKNOWN",
"id" : 1,
"tests" : [ {
"command" : "Get System Status",
"criterion" : "Manual Review",
"item" : "System time:\\s(.*)",
"comments" : "Found: Thu Mar 14 12:00:27 2019",
"status" : "UNKNOWN",
"id" : 1
}, {
"command" : "Get System Status",
"criterion" : "Manual Review",
"item" : "IPS-DB:\\s*(.*)",
"comments" : "Found: 3.00295(2013-01-30 19:23)",
"status" : "UNKNOWN",
"id" : 2
```

```
}, {
"command" : "Get System Status",
"criterion" : "Manual Review",
"item" : "Serial-Number:\\s*(.*)",
"comments" : "Found: FGT50B3G11605125",
"status" : "UNKNOWN",
"id" : 3
}, {
.
.
}, {
"command" : "Get System Status",
"criterion" : "Manual Review",
"item" : "Virtual domains status:\\s*(.*)",
"comments" : "Found: 9 in NAT mode, 1 in TP mode",
"status" : "UNKNOWN",
"id" : 14
} ]
.
.
}, {
"name" : "Time out Settings",
"status" : "PASSED",
"id" : 17,
"tests" : [ {
"command" : "Global Configuration",
"criterion" : "Required Regexp",
"item" : "set admintimeout\\s(.*)",
"comments" : "Found: 480",
```

```
"status" : "PASSED",
"id" : 1
} ]
} ]
}
```

Running the Query Troubleshooting Tool

The `troubleshoot` method helps to determine why a group traffic simulation query produced an inaccurate traffic path.

The input is the ID of the query ran in the online wizard and a list of the expected devices on the query path. The output is a response message with the found paths, detected devices, problem scenario, recommended resolution steps, the device causing the inconsistency, and information about expected and unexpected devices.

Note: The Query Troubleshooting Tool is available only to admin users.

Resource Name: `ms-mapDiagnostics/v1/api/queryTroubleshootin/troubleshoot`

Request Method: POST

Authentication: Cookie with session ID.

Request Body Parameters:

A JSON object with the following properties:

Element	Type	Description
`queryID` *Mandatory*	String	Query ID received from the troubleshooting wizard.
`expectedQueryPath` *Mandatory*	List of `ExpectedQueryDevice` (see ExpectedQueryDevice type)	List containing details for expected query path: device display name and IP address.

Response:

Element	Type	Description
`foundPaths`	Map	All paths found for the query. Object consists of key/value pairs of the path number and its path. The path is a list of QueryNetworkObject (see QueryNetworkObject Type).
`detectedDevices`	List of `QueryTroubleshootingPathItem` (see QueryTroubleshootingPathItem Type)	A list of the detected devices with identifying properties.
`scenario`	`QueryTroublshootingScenario` (see QueryTroubleshootingScenario Type)	Object containing the scenario which caused the problem and recommended steps for its resolution.
`inconsistencyCauseDevice`	`QueryTroubleshootingInconsistencyCause` (see QueryTroubleshootingInconsistencyCause Type)	Object containing data for the device causing inconsistency.
`expectedDevice`	`ExpectedQueryDevice (see` ExpectedDevice type `)`	Object containing identifying properties for expected device.
`firstUnexpectedDevice`	`QueryTroubleshootingPathItem` (see QueryTroubleshootingPathItem Type)	Object containing properties for first unexpected device.

Request example:

```
{
    "queryId":"ALL_FIREWALLS_query-1534764120587",
        "expectedQueryPath": [{
            "displayName": "Pecan_PaloAlto",
            "ip": "10.176.46.197"
            }, {
            "displayName": "Poppy_juniper",
            "ip": "192.168.6.6"
            }, {
            "displayName": "Violet_Fortinet",
            "ip": "10.42.65.100"
            }]
}
```

Response example:

```
{
   "foundPaths":{
      "1":[
         {
            "mapId":"Subnet__489",
            "id":489,
            "type":"SUBNET",
            "locationOnPath":1,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__40",
            "id":40,
            "type":"DEVICE",
            "locationOnPath":2,
            "displayName":"Pecan_PaloAlto",
            "ip":{
               "id":0,
               "minIp":179318469,
               "maxIp":179318469,
               "display":"10.176.46.197",
               "displayRange":"10.176.46.197",
               "optimalDisplay":[
                  "10.176.46.197"
               ],
               "singleIP":true,
               "cidr":true,
```

```
            "any":false
         },
         "empty":false
      },
      {
         "mapId":"Subnet__11",
         "id":11,
         "type":"SUBNET",
         "locationOnPath":3,
         "displayName":null,
         "ip":null,
         "empty":false
      },
      {
         "mapId":"Device__252",
         "id":252,
         "type":"DEVICE",
         "locationOnPath":5,
         "displayName":"Poppy_juniper",
         "ip":{
            "id":0,
            "minIp":3232237062,
            "maxIp":3232237062,
            "display":"192.168.6.6",
            "displayRange":"192.168.6.6",
            "optimalDisplay":[
               "192.168.6.6"
            ],
            "singleIP":true,
            "cidr":true,
            "any":false
         },
         "empty":false
      },
      {
         "mapId":"Subnet__9",
         "id":9,
         "type":"SUBNET",
         "locationOnPath":8,
         "displayName":null,
         "ip":null,
         "empty":false
      },
      {
```

```
            "mapId":"Device__8",
            "id":8,
            "type":"DEVICE",
            "locationOnPath":9,
            "displayName":"Rose_checkpoint",
            "ip":{
               "id":0,
               "minIp":173150740,
               "maxIp":173150740,
               "display":"10.82.18.20",
               "displayRange":"10.82.18.20",
               "optimalDisplay":[
                  "10.82.18.20"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__404",
            "id":404,
            "type":"SUBNET",
            "locationOnPath":11,
            "displayName":null,
            "ip":null,
            "empty":false
         }
      ]
   },
   "detectedDevices":[
      {
         "mapId":"Device__40",
         "ip":"10.176.46.197",
         "displayName":"Pecan_PaloAlto"
      },
      {
         "mapId":"Device__252",
         "ip":"192.168.6.6",
         "displayName":"Poppy_juniper"
      }
   ],
   "scenario":{
```

```
      "name":"REACHED_WRONG_DEVICE",
      "message":"There might be an issue with device",
      "recommendedSteps":[
         {
            "text":"Collect logs",
            "action":"support"
         },
         {
            "text":"Open a support case on Algosec Portal",
            "action":"portal"
         }
      ]
   },
   "inconsistencyCauseDevice":{
      "ip":"192.168.6.6",
      "dnsName":"192.168.6.6",
      "snmpName":null
   },
   "expectedDevice":{
      "displayName":"Violet_Fortinet",
      "ip":"10.42.65.100"
   },
   "firstUnexpectedDevice":{
      "mapId":"Device__8",
      "ip":"10.82.18.20",
      "displayName":"Rose_checkpoint"
   }
{
   "foundPaths":{
      "1":[
         {
            "mapId":"Subnet__489",
            "id":489,
            "type":"SUBNET",
            "locationOnPath":1,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__40",
            "id":40,
            "type":"DEVICE",
            "locationOnPath":2,
```

```
            "displayName":"Pecan_PaloAlto",
            "ip":{
               "id":0,
               "minIp":179318469,
               "maxIp":179318469,
               "display":"10.176.46.197",
               "displayRange":"10.176.46.197",
               "optimalDisplay":[
                  "10.176.46.197"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__11",
            "id":11,
            "type":"SUBNET",
            "locationOnPath":3,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__252",
            "id":252,
            "type":"DEVICE",
            "locationOnPath":5,
            "displayName":"Poppy_juniper",
            "ip":{
               "id":0,
               "minIp":3232237062,
               "maxIp":3232237062,
               "display":"192.168.6.6",
               "displayRange":"192.168.6.6",
               "optimalDisplay":[
                  "192.168.6.6"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
```

```
            "empty":false
         },
         {
            "mapId":"Subnet__9",
            "id":9,
            "type":"SUBNET",
            "locationOnPath":8,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__8",
            "id":8,
            "type":"DEVICE",
            "locationOnPath":9,
            "displayName":"Rose_checkpoint",
            "ip":{
               "id":0,
               "minIp":173150740,
               "maxIp":173150740,
               "display":"10.82.18.20",
               "displayRange":"10.82.18.20",
               "optimalDisplay":[
                  "10.82.18.20"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__404",
            "id":404,
            "type":"SUBNET",
            "locationOnPath":11,
            "displayName":null,
            "ip":null,
            "empty":false
         }
      ]
   },
   "detectedDevices":[
```

```
      {
         "mapId":"Device__40",
         "ip":"10.176.46.197",
         "displayName":"Pecan_PaloAlto"
      },
      {
         "mapId":"Device__252",
         "ip":"192.168.6.6",
         "displayName":"Poppy_juniper"
      }
   ],
   "scenario":{
      "name":"REACHED_WRONG_DEVICE",
      "message":"There might be an issue with device",
      "recommendedSteps":[
         {
            "text":"Collect logs",
            "action":"support"
         },
         {
            "text":"Open a support case on Algosec Portal",
            "action":"portal"
         }
      ]
   },
   "inconsistencyCauseDevice":{
      "ip":"192.168.6.6",
      "dnsName":"192.168.6.6",
      "snmpName":null
   },
   "expectedDevice":{
      "displayName":"Violet_Fortinet",
      "ip":"10.42.65.100"
   },
   "firstUnexpectedDevice":{
      "mapId":"Device__8",
      "ip":"10.82.18.20",
      "displayName":"Rose_checkpoint"
   }
{
   "foundPaths":{
      "1":[
         {
            "mapId":"Subnet__489",
```

```
            "id":489,
            "type":"SUBNET",
            "locationOnPath":1,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__40",
            "id":40,
            "type":"DEVICE",
            "locationOnPath":2,
            "displayName":"Pecan_PaloAlto",
            "ip":{
               "id":0,
               "minIp":179318469,
               "maxIp":179318469,
               "display":"10.176.46.197",
               "displayRange":"10.176.46.197",
               "optimalDisplay":[
                  "10.176.46.197"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__11",
            "id":11,
            "type":"SUBNET",
            "locationOnPath":3,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__252",
            "id":252,
            "type":"DEVICE",
            "locationOnPath":5,
            "displayName":"Poppy_juniper",
            "ip":{
```

```
            "id":0,
            "minIp":3232237062,
            "maxIp":3232237062,
            "display":"192.168.6.6",
            "displayRange":"192.168.6.6",
            "optimalDisplay":[
               "192.168.6.6"
            ],
            "singleIP":true,
            "cidr":true,
            "any":false
         },
         "empty":false
      },
      {
         "mapId":"Subnet__9",
         "id":9,
         "type":"SUBNET",
         "locationOnPath":8,
         "displayName":null,
         "ip":null,
         "empty":false
      },
      {
         "mapId":"Device__8",
         "id":8,
         "type":"DEVICE",
         "locationOnPath":9,
         "displayName":"Rose_checkpoint",
         "ip":{
            "id":0,
            "minIp":173150740,
            "maxIp":173150740,
            "display":"10.82.18.20",
            "displayRange":"10.82.18.20",
            "optimalDisplay":[
               "10.82.18.20"
            ],
            "singleIP":true,
            "cidr":true,
            "any":false
         },
         "empty":false
      },
```

```
         {
            "mapId":"Subnet__404",
            "id":404,
            "type":"SUBNET",
            "locationOnPath":11,
            "displayName":null,
            "ip":null,
            "empty":false
         }
      ]
   },
   "detectedDevices":[
      {
         "mapId":"Device__40",
         "ip":"10.176.46.197",
         "displayName":"Pecan_PaloAlto"
      },
      {
         "mapId":"Device__252",
         "ip":"192.168.6.6",
         "displayName":"Poppy_juniper"
      }
   ],
   "scenario":{
      "name":"REACHED_WRONG_DEVICE",
      "message":"There might be an issue with device",
      "recommendedSteps":[
         {
            "text":"Collect logs",
            "action":"support"
         },
         {
            "text":"Open a support case on Algosec Portal",
            "action":"portal"
         }
      ]
   },
   "inconsistencyCauseDevice":{
      "ip":"192.168.6.6",
      "dnsName":"192.168.6.6",
      "snmpName":null
   },
   "expectedDevice":{
      "displayName":"Violet_Fortinet",
```

```
      "ip":"10.42.65.100"
   },
   "firstUnexpectedDevice":{
      "mapId":"Device__8",
      "ip":"10.82.18.20",
      "displayName":"Rose_checkpoint"
   }
{
   "foundPaths":{
      "1":[
         {
            "mapId":"Subnet__489",
            "id":489,
            "type":"SUBNET",
            "locationOnPath":1,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__40",
            "id":40,
            "type":"DEVICE",
            "locationOnPath":2,
            "displayName":"Pecan_PaloAlto",
            "ip":{
               "id":0,
               "minIp":179318469,
               "maxIp":179318469,
               "display":"10.176.46.197",
               "displayRange":"10.176.46.197",
               "optimalDisplay":[
                  "10.176.46.197"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__11",
            "id":11,
            "type":"SUBNET",
```

```
            "locationOnPath":3,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__252",
            "id":252,
            "type":"DEVICE",
            "locationOnPath":5,
            "displayName":"Poppy_juniper",
            "ip":{
               "id":0,
               "minIp":3232237062,
               "maxIp":3232237062,
               "display":"192.168.6.6",
               "displayRange":"192.168.6.6",
               "optimalDisplay":[
                  "192.168.6.6"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__9",
            "id":9,
            "type":"SUBNET",
            "locationOnPath":8,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__8",
            "id":8,
            "type":"DEVICE",
            "locationOnPath":9,
            "displayName":"Rose_checkpoint",
            "ip":{
               "id":0,
               "minIp":173150740,
```

```
                "maxIp":173150740,
                "display":"10.82.18.20",
                "displayRange":"10.82.18.20",
                "optimalDisplay":[
                   "10.82.18.20"
                ],
                "singleIP":true,
                "cidr":true,
                "any":false
             },
             "empty":false
          },
          {
             "mapId":"Subnet__404",
             "id":404,
             "type":"SUBNET",
             "locationOnPath":11,
             "displayName":null,
             "ip":null,
             "empty":false
          }
       ]
    },
    "detectedDevices":[
       {
          "mapId":"Device__40",
          "ip":"10.176.46.197",
          "displayName":"Pecan_PaloAlto"
       },
       {
          "mapId":"Device__252",
          "ip":"192.168.6.6",
          "displayName":"Poppy_juniper"
       }
    ],
    "scenario":{
       "name":"REACHED_WRONG_DEVICE",
       "message":"There might be an issue with device",
       "recommendedSteps":[
          {
             "text":"Collect logs",
             "action":"support"
          },
          {
```

```
            "text":"Open a support case on Algosec Portal",
            "action":"portal"
         }
      ]
   },
   "inconsistencyCauseDevice":{
      "ip":"192.168.6.6",
      "dnsName":"192.168.6.6",
      "snmpName":null
   },
   "expectedDevice":{
      "displayName":"Violet_Fortinet",
      "ip":"10.42.65.100"
   },
   "firstUnexpectedDevice":{
      "mapId":"Device__8",
      "ip":"10.82.18.20",
      "displayName":"Rose_checkpoint"
   }
{
   "foundPaths":{
      "1":[
         {
            "mapId":"Subnet__489",
            "id":489,
            "type":"SUBNET",
            "locationOnPath":1,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__40",
            "id":40,
            "type":"DEVICE",
            "locationOnPath":2,
            "displayName":"Pecan_PaloAlto",
            "ip":{
               "id":0,
               "minIp":179318469,
               "maxIp":179318469,
               "display":"10.176.46.197",
               "displayRange":"10.176.46.197",
               "optimalDisplay":[
```

```
                "10.176.46.197"
             ],
             "singleIP":true,
             "cidr":true,
             "any":false
          },
          "empty":false
       },
       {
          "mapId":"Subnet__11",
          "id":11,
          "type":"SUBNET",
          "locationOnPath":3,
          "displayName":null,
          "ip":null,
          "empty":false
       },
       {
          "mapId":"Device__252",
          "id":252,
          "type":"DEVICE",
          "locationOnPath":5,
          "displayName":"Poppy_juniper",
          "ip":{
             "id":0,
             "minIp":3232237062,
             "maxIp":3232237062,
             "display":"192.168.6.6",
             "displayRange":"192.168.6.6",
             "optimalDisplay":[
                "192.168.6.6"
             ],
             "singleIP":true,
             "cidr":true,
             "any":false
          },
          "empty":false
       },
       {
          "mapId":"Subnet__9",
          "id":9,
          "type":"SUBNET",
          "locationOnPath":8,
          "displayName":null,
```

```
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__8",
            "id":8,
            "type":"DEVICE",
            "locationOnPath":9,
            "displayName":"Rose_checkpoint",
            "ip":{
               "id":0,
               "minIp":173150740,
               "maxIp":173150740,
               "display":"10.82.18.20",
               "displayRange":"10.82.18.20",
               "optimalDisplay":[
                  "10.82.18.20"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__404",
            "id":404,
            "type":"SUBNET",
            "locationOnPath":11,
            "displayName":null,
            "ip":null,
            "empty":false
         }
      ]
   },
   "detectedDevices":[
      {
         "mapId":"Device__40",
         "ip":"10.176.46.197",
         "displayName":"Pecan_PaloAlto"
      },
      {
         "mapId":"Device__252",
         "ip":"192.168.6.6",
```

```
            "displayName":"Poppy_juniper"
         }
      ],
      "scenario":{
         "name":"REACHED_WRONG_DEVICE",
         "message":"There might be an issue with device",
         "recommendedSteps":[
            {
               "text":"Collect logs",
               "action":"support"
            },
            {
               "text":"Open a support case on Algosec Portal",
               "action":"portal"
            }
         ]
      },
      "inconsistencyCauseDevice":{
         "ip":"192.168.6.6",
         "dnsName":"192.168.6.6",
         "snmpName":null
      },
      "expectedDevice":{
         "displayName":"Violet_Fortinet",
         "ip":"10.42.65.100"
      },
      "firstUnexpectedDevice":{
         "mapId":"Device__8",
         "ip":"10.82.18.20",
         "displayName":"Rose_checkpoint"
      }
   {
      "foundPaths":{
         "1":[
            {
               "mapId":"Subnet__489",
               "id":489,
               "type":"SUBNET",
               "locationOnPath":1,
               "displayName":null,
               "ip":null,
               "empty":false
            },
            {
```

```
            "mapId":"Device__40",
            "id":40,
            "type":"DEVICE",
            "locationOnPath":2,
            "displayName":"Pecan_PaloAlto",
            "ip":{
               "id":0,
               "minIp":179318469,
               "maxIp":179318469,
               "display":"10.176.46.197",
               "displayRange":"10.176.46.197",
               "optimalDisplay":[
                  "10.176.46.197"
               ],
               "singleIP":true,
               "cidr":true,
               "any":false
            },
            "empty":false
         },
         {
            "mapId":"Subnet__11",
            "id":11,
            "type":"SUBNET",
            "locationOnPath":3,
            "displayName":null,
            "ip":null,
            "empty":false
         },
         {
            "mapId":"Device__252",
            "id":252,
            "type":"DEVICE",
            "locationOnPath":5,
            "displayName":"Poppy_juniper",
            "ip":{
               "id":0,
               "minIp":3232237062,
               "maxIp":3232237062,
               "display":"192.168.6.6",
               "displayRange":"192.168.6.6",
               "optimalDisplay":[
                  "192.168.6.6"
               ],
```

```
            "singleIP":true,
            "cidr":true,
            "any":false
         },
         "empty":false
      },
      {
         "mapId":"Subnet__9",
         "id":9,
         "type":"SUBNET",
         "locationOnPath":8,
         "displayName":null,
         "ip":null,
         "empty":false
      },
      {
         "mapId":"Device__8",
         "id":8,
         "type":"DEVICE",
         "locationOnPath":9,
         "displayName":"Rose_checkpoint",
         "ip":{
            "id":0,
            "minIp":173150740,
            "maxIp":173150740,
            "display":"10.82.18.20",
            "displayRange":"10.82.18.20",
            "optimalDisplay":[
               "10.82.18.20"
            ],
            "singleIP":true,
            "cidr":true,
            "any":false
         },
         "empty":false
      },
      {
         "mapId":"Subnet__404",
         "id":404,
         "type":"SUBNET",
         "locationOnPath":11,
         "displayName":null,
         "ip":null,
         "empty":false
```

```
            }
         ]
      },
      "detectedDevices":[
         {
            "mapId":"Device__40",
            "ip":"10.176.46.197",
            "displayName":"Pecan_PaloAlto"
         },
         {
            "mapId":"Device__252",
            "ip":"192.168.6.6",
            "displayName":"Poppy_juniper"
         }
      ],
      "scenario":{
         "name":"REACHED_WRONG_DEVICE",
         "message":"There might be an issue with device",
         "recommendedSteps":[
            {
               "text":"Collect logs",
               "action":"support"
            },
            {
               "text":"Open a support case on Algosec Portal",
               "action":"portal"
            }
         ]
      },
      "inconsistencyCauseDevice":{
         "ip":"192.168.6.6",
         "dnsName":"192.168.6.6",
         "snmpName":null
      },
      "expectedDevice":{
         "displayName":"Violet_Fortinet",
         "ip":"10.42.65.100"
      },
      "firstUnexpectedDevice":{
         "mapId":"Device__8",
         "ip":"10.82.18.20",
         "displayName":"Rose_checkpoint"
      }
```

Acknowledge an issue

The `acknowledge` request marks active issues in the AFA issues center as acknowledged. Issues marked as acknowledged will appear in the list of acknowledged issues and will no longer appear in the list of active issues.

Resource Name: `/ms-watchdog/v1/api/issues-center/issues/acknowledge`

Request Method: POST

Authentication: Cookie with session ID.

Request Body: Any array of issue IDs. To retrieve the issue IDs, see Manage AFA issues.

Response:

Element	Type	Description
`newStatus`	String	The new status of the issues: **ACKNOWLEDGED**.
`updatedIssues`	Array	An array of issue IDs.
`successful`	Boolean	Whether the request was successful.

Request example

```
#/ms-watchdog/v1/api/issues-center/issues/acknowledge
[2,4]
```

Response example

```
{
        "newStatus":"ACKNOWLEDGED",
        "updatedIssues":[
                2,
                4
        ],
        "successful":true
}
```

Object and device data APIs

The AFA REST API supports the following APIs for managing network objects and devices:

Object management	Retrieve network objects Retrieve service objects
Device management	Retrieve interfaces Identify missing routers Merge routers Get details for a specified device Add/Edit a device View device parameter templates Delete a device Get a list of devices Get data on managed devices

Retrieve network objects

The `get_network_objects` request retrieves all the network objects of a device or a group of devices, along with the IP addresses contained in each object.

The input will be the active session ID and the name of a device or a device group. The output will be a list of all the network objects of all the devices of the selected group, along with the content of each object.

Resource Name: `/fa/server/network_objects/read`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`session` *Mandatory*	String	Session ID returned in `login` request.
`entity` *Mandatory*	String	The display name of the device, group, or matrix.

Element	Type	Description

`entityType` *Optional*	String	One of the following:
		■ `device` (default)
		`group`
		`matrix`

`size` *Optional*	Integer	Number of results per page. The default value is 200000000.
`page` *Optional*	Integer	Page number to return. The default value is 1 (the first page). **Note:** This element requires a definition for `size`. Defining this element without `size` will cause the return to be empty.

Response:

Element	Type	Description
`totalPages`	Integer	The total number of pages. By default, all of the results are on one page.
`totalElements`	Integer	The total number of network objects for the `entity`.
`currPageNumber`	Integer	The page number returned. By default, the first page (1).
`currPageElements`	Integer	The number of network objects whose information has been returned.
`entitiesResponses`	List of `entitiesResponse` objects.	A list of network object information. See entitiesResponse Type (see EntitiesResponse type).

Element	Type	Description
`status`	String	One of the following: ■ `true`. Indicates the request succeeded. ■ `false`. Indicates the request failed.
`message` *Only is returned when the request fails.*	String	An error message.

Request example

```
curl -H "Accept:application/json" -k  "https://192.168.3.76/fa/server/
network_objects/read?session=b24d684a54595483db7def6a84129dc2
&entity=admin&size=2&page=2
```

Response example


```
{   "totalPages": 30,
"totalElements": 59,
"currPageNumber": 2,
"currPageElements": 2,
"entitiesReponses": [   {
"name": "admin",
"devices": ["admin"],
"values":       [
{
"name": "Einat_test_ipv6_6",
"ipaddresses": ["1111:2222:3333:4444:5555:6666:7777:8888"],
"ipType": "IPv6"
},
{
"name": "name_2",
"ipaddresses": ["2001::ffd3:0:57ab"],
"ipType": "IPv6"
```

```
}
]
}],
"status": true
}
```

Retrieve service objects

The `get_service_objects` request retrieves all the service objects of a device or a group of devices, along with the protocol and ports contained in each object.

The input will be the active session ID and the name of a device or a device group. The output will be a list of all the service objects of all the devices of the selected group, along with the content of each object.

Resource Name: `/fa/server/network_services/read`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`session` *Mandatory*	String	Session ID returned in `login` request.
`entity` *Mandatory*	String	The display name of the device, group, or matrix.

`entityType` *Optional*	String	One of the following:
		■ `device` (default)
		`group`
		`matrix`

`size` *Optional*	Integer	Number of results per page. The default value is 200000000.

Element	Type	Description
`page` *Optional*	Integer	Page number to return. The default value is 1 (the first page). **Note:** This element requires a definition for `size`. Defining this element without `size` will cause the return to be empty.

Response:

Element	Type	Description
`totalPages`	Integer	The total number of pages. By default, all of the results are on one page.
`totalElements`	Integer	The total number of network objects for the `entity`.
`currPageNumber`	Integer	The page number returned. By default, the first page (1).
`currPageElements`	Integer	The number of network objects whose information has been returned.
`entitiesResponses`	List of `entitiesResponse` objects.	A list of network object information. See entitiesResponse Type (see EntitiesResponse type).
`status`	String	One of the following: ■ `true`. Indicates the request succeeded. ■ `false`. Indicates the request failed.
`message`*Only is returned when the request fails.*	String	An error message.

Request example

```
curl -H "Accept:application/json" -k  https://192.168.3.76/fa/server/
network_services/read?session=b24d684a54595483db7def6a84129dc2&entity
```

```
=Alessia&size=2&page=3
```

Response example

```
{
"totalPages": 1428,
"totalElements": 2856,
"currPageNumber": 3,
"currPageElements": 2,
"entitiesReponses": [   {
"name": "Alessia",
"devices": ["Alessia"],
"values":       [
{
"id": 506605,
"name": "Pinterest",
"serviceDefinitions": ["tcp/443/*"]
},
{
"id": 506644,
"name": "IRTP",
"serviceDefinitions": ["28/*/*"]
}
]
}],
"status": true
}
```

Retrieve containing objects

The `get_containing_objects` request retrieves a list of containing objects for a specified object.

Request Method: GET

Request URL Parameters:

Element	Type	Description
SessionID Mandatory	String	Session ID returned in `login` request.
ObjectName Mandatory	String	The name of the object for which you want a list of containing objects.

Response:

Element	Type	Description
ContainingObjectName	String	The names of the objects that contain the specified object.

Search for object by IP

The `search_object_by_ip` request performs a search in AFA for all objects that match the details provided in the request.

Request Method: GET

Request URL Parameters:

Element	Type	Description
sessionID Mandatory	String	Session ID returned in `login` request.
First Mandatory	String	The first IP address in the range to search for.
Last Mandatory	String	The last IP address in the range to search for.
MatchType Mandatory	String	The type of object to search for. Possible values: • **exact** • **containing** • **contained** • **overlap**

Response:

Element	Type	Description
EntityID	String	A string containing the search results.

Retrieve parent device

The `get_parent_device` request retrieves the parent object of a specified device.

Request Method: GET

Request URL Parameters:

Element	Type	Description
SessionID mandatory	String	Session ID returned in the **login** request
DeviceID mandatory	String	The ID of the device you want to return the parent for.

Response:

Element	Type	Description
DeviceID	String	The ID of the device that is the parent of the device specified in the request.

Retrieve interfaces

The `get_interfaces` request retrieves the interfaces of a device or a group/matrix of devices, along with their IP addresses.

The input will be the active session ID and the name of a device, group, or matrix. The output will be a list of all the interfaces of all the devices in the selected group and their IP addresses.

Note: This request requires permission for All_Firewalls.

Resource Name: `/fa/server/interfaces/read`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`session`*Mandatory*	String	Session ID returned in `login` request.
`entity`*Mandatory*	String	The display name of the device, group, or matrix.

`entityType`*Optional*	String	One of the following:
		■ `device` (default)
		`group`
		`matrix`

Note: The `page` and `size` elements are not supported for the `get_interfaces` request.

Response:

Element	Type	Description
`name`	String	The entity name.
`type`	String	The entity type.
`interfaces`	A list of `interface` objects.	A list of interface information. See Interface Type (see Interface Type).
`status`	String	One of the following: ■ `true`. Indicates the request succeeded. ■ `false`. Indicates the request failed.
`message`*Only is returned when the request fails.*	String	An error message.

Request example

```
curl -H "Content-Type: application/json" -k 'https://127.0.0.1/fa/server/
interfaces/read?session=1cb3ec62e5db893f960130070d54900a&entityType=firewall&entity=Imma
```

Response example


```
{
"0":    {
"name": Immacolata",
"type":"DEVICE",
"interfaces":[
{"hwName":"eth5",
"ip":"10.60.32.0\/30",
"id":"293",
"zoneType":"INTERNAL",
"ipsBehindInterface":"10.60.32.0 - 10.60.32.3,26.26.26.0 - 26.26.26.255"},
{"hwName":"eth0",
"ip":"10.20.0.0\/16",
"id":"295",
"zoneType":"INTERNAL",
"ipsBehindInterface":"0.0.0.0 - 10.10.2.255,10.10.4.0 -
10.20.32.0,10.20.32.2 - 10.30.31.255,10.30.32.4 - 10.40.2.255,10.40.4.0 -
10.50.2.255,10.50.4.0 - 10.60.31.255,10.60.32.4 - 10.110.2.255,10.110.4.0
- 10.120.2.255,10.120.4.0 - 20.20.19.255,20.20.21.0 -
26.26.25.255,26.26.27.0 - 255.255.255.255"},
]
},
"status": true
}
```


Identify missing routers

The following requests allow you to identify routers in the AFA graphic network map that should be defined as devices in AFA.

Run the Map Completeness tool

The `execute` method runs the map completeness tool. This tool searches for routers missing from the AFA graphic network map.

The input will be the network's SNMP key, internal networks, external networks, and the maximum number of queries the tool should run. The output is a status message. To retrieve the results, Retrieve missing routers results.

Note: The `execute` method may take several minutes to complete, depending on the number of queries.

Resource Name: `/ms-mapDiagnostics/v1/api/mapCompleteness/execute*/`

Request Method: POST

Authentication: Cookie with session ID.

Request Body Parameters:

Element	Type	Description
`maxQueries` *Optional*	Integer	The maximum number of paths to query. By default, the maximum number of queries is 400.
`snmpKey` *Optional*	String	The network's SNMP key. This is used to retrieve the names of the routers. If the DNS lookup fails and the SNMP key is not provided, the results will only provide the router's IP address.
`internalNetworks` *Optional*	A list of subnets (CIDR format).	All of the network's internal subnets. In order to determine the default values for your environment, seeRetrieve Map Completeness default values.
`externalNetworks` *Optional*	A list of subnets (CIDR format).	All of the external subnets that should be reachable from each of the network's internal subnets. In order to determine the default values for your environment, see Retrieve Map Completeness default values.

Response:

Element	Type	Description
`status`	String	A message which indicates success or a reason for failure.

Request Body Example

```
{   "maxQueries": 400,  "snmpKey": "alkfaklfjk34mk4h3j4nj3k4hy2n54j",
"internalNetworks": ["10.0.0.0/8","192.168.0.0/16","172.16.0.0/12"],
"externalNetworks": ["8.8.8.8"] }
```

Response example

```
{   "status": success,}
```

Retrieve missing routers results

The `missingStubRouters` request provides the results of the `execute` request: a list of routers missing from the graphic network map.

The input will be the page number you want to retrieve. You can optionally filter the result that you want to retrieve by providing the name of a router, the name of the closest device, or a relevant subnet. The output is a list of routers.

Note: You must wait for the `execute` request to complete before retrieving the missing routers with the `missingStubRouters` request.

Resource Name: `ms-mapDiagnostics/v1/api/mapCompleteness/missingStubRouters`

Request Method: GET

Authentication: Cookie with session ID.

Request URL Parameters:

Element	Type	Description
`form`	String	A URL encoded JSON object with the following properties.

Properties:

Element	Type	Description
`pageNumber` *Mandatory*	Integer	The page number for the page of results to return in the response.

Element	Type	Description
`byStubName` *Optional*	String	The name of router to return in the response.
`byClosestDeviceName` *Optional*	String	The name of the closest device to the routers to return in the results.
`byNetwork` *Optional*	String	A subnet (in CIDR format) that is relevant to the routers to return in the results.

Response:

Element	Type	Description
`totalStubs`	Integer	The number of routers returned in the response.
`pageNumber`	Integer	The page number of the results returned in the response.
`stubs`	A list of `stub` objects.	A list of routers. See Stub Type (see Stub Type).
`score`	Integer	The map completeness score for the current graphic network map.

Request Body Example

```
{"pageNumber" : 1,"byStubName" : "10.110.15","byClosetDeviceName":
"10.110.151.1","byNetwork":"10.110.15"}
```

Response example

```
{
"totalStubs":1,
"pageNumber":1,
"stubs":[
{
"id":123,
"name":"10.110.151.10",
"stubs":[
{
```

```
"id":123,
"ip":{
"id":10,
"minIp":175019786,
"maxIp":175019786,
"display":"10.110.151.10",
"displayRange":"10.110.151.10",
"optimalDisplay":[
"10.110.151.10"
],
"singleIP":true,
"cidr":true,
"any":false
},
"closestDevices":[
{
"id":176,
"brand":"junos",
"name":"10.20.151.1"
}
]
}
],
"missingInPaths":42
}
],
"score":18
}
```


Retrieve the last run configuration

The `lastExecution` request provides the parameters that were used the last time the map completeness tool was executed.

Resource Name: `ms-mapDiagnostics/v1/api/mapCompleteness/lastExecution*/`

Request Method: GET

Authentication: Cookie with session ID.

Response:

Element	Type	Description
`score`	Integer	The map completeness score for the current graphic network map.
`executionTime`	Integer	The timestamp for the last execution.
`queries`	Integer	The number of queries that were run.
`snmpKey`	String	The network's SNMP key.
`internalNetworks`	A list of `ip` objects	The internal subnets that were used for the execution.
`externalNetworks`	A list of `ip` objects	The external subnets that were used for the execution.
`status`	String	The status of the last execution.
`progress`	Boolean	The last execution's progress.

Response example

```
{
"score": 43,
"executionTime": 1524471616454,
"queries": 400,
"snmpKey": "askjdaksdjask",
"internalNetworks": [
{
"id": 5,
"minIp": 3232235777,
"maxIp": 3232235777,
"display": "192.168.1.1",
```

```
"displayRange": "192.168.1.1",
"optimalDisplay": [
"192.168.1.1"
],
"singleIP": true,
"cidr": true,
"any": false
},
{
"id": 2,
"minIp": 167772160,
"maxIp": 184549375,
"display": "10.0.0.0/8",
"displayRange": "10.0.0.0-10.255.255.255",
"optimalDisplay": [
"10.0.0.0/8"
],
"singleIP": false,
"cidr": true,
"any": false
}
],
"externalNetworks": [
{
"id": 1,
"minIp": 134744072,
"maxIp": 134744072,
"display": "8.8.8.8",
"displayRange": "8.8.8.8",
"optimalDisplay": [
"8.8.8.8"
],
```

```
"singleIP": true,
"cidr": true,
"any": false
}
],
"status": "Done",
"progress": 1
}
```

Stop a Map Completeness job

The `abort` request stops an execution that is in progress.

Resource Name: `ms-mapDiagnostics/v1/api/mapCompleteness/abort*/`

Request Method: POST

Authentication: Cookie with session ID.

Response:

Element	Type	Description
`status`	String	A message which indicates success or a reason for failure.

Retrieve Map Completeness default values

The `defaultValues` request provides the default values of the map completeness tool parameters for the specific AFA environment.

By default, the maximum number of paths that will be simulated (queries that will be run) is 400. The default external networks used in the calculation is 8.8.8.8. If a custom risk profile spreadsheet is being used in AFA, the networks in the spreadsheet are used as the default internal networks. If no such spreadsheet is being used, RFC 1918 is used to provide the default internal networks.

Resource Name: `ms-mapDiagnostics/v1/api/mapCompleteness/defaultValues*/`

Request Method: GET

Authentication: Cookie with session ID.

Response:

Element	Type	Description
`score`	Integer	The map completeness score for the current graphic network map.
`executionTime`	Integer	The timestamp for the execution.
`executionTimeofLastSucceccfulJob`	Integer	The timestamp for the last execution.
`queries`	Integer	The default number of queries.
`snmpKey`	String	The network's SNMP key.
`internalNetworks`	A list of `ip` objects	The default internal subnets for the environment.
`externalNetworks`	A list of `ip` objects	The default external subnets for the environment.
`status`	String	The status of the last execution.
`progress`	Boolean	The last execution's progress.

Response example


```
{
"score":18,
"executionTime":1528141226870,
"executionTimeOfLastSuccessfulJob":1528141226826,
"queries":400,
"snmpKey":null,
"internalNetworks":[
{
"id":4,
"minIp":3232235520,
```

```
"maxIp":3232301055,
"display":"192.168.0.0/16",
"displayRange":"192.168.0.0-192.168.255.255",
"optimalDisplay":[
"192.168.0.0/16"
],
"singleIP":false,
"cidr":true,
"any":false
},
{
"id":2,
"minIp":167772160,
"maxIp":184549375,
"display":"10.0.0.0/8",
"displayRange":"10.0.0.0-10.255.255.255",
"optimalDisplay":[
"10.0.0.0/8"
],
"singleIP":false,
"cidr":true,
"any":false
},
{
"id":23,
"minIp":2896166912,
"maxIp":2897215487,
"display":"172.160.0.0/12",
"displayRange":"172.160.0.0-172.175.255.255",
"optimalDisplay":[
"172.160.0.0/12"
],
```

```
"singleIP":false,
"cidr":true,
"any":false
}
],
"externalNetworks":[
{
"id":1,
"minIp":134744072,
"maxIp":134744072,
"display":"8.8.8.8",
"displayRange":"8.8.8.8",
"optimalDisplay":[
"8.8.8.8"
],
"singleIP":true,
"cidr":true,
"any":false
}
],
"status":"Done",
"progress":1.0
}
```


Merge routers

Base URL

The base URL for all requests is:

```
https://<MACHINE-ADDRESS>/ms-mapDiagnostics/v1/api/mergeRouters
```

where `MACHINE-ADDRESS` is the AFA server IP.

Retrieve merged routers

Retrieves a list of merged routers with the status "MERGED" *only*. Merged routers with the status "OUTDATED_MERGED" are excluded.

Resource URL: `/mergeRouters/list`

Resource Method: GET

Authentication: Cookie with session ID.

Response:

Element	Type	Description
mergedRouters	Array of MergedRoutersData (see MergedRoutersData type)	A list of merged routers with status "MERGED" only.

Response example:

```
[
   {
      "id":35,
      "name":"router1",
      "status":"MERGED",
      "domainId":0,
      "routersToMerge":[   //List of the the stubs that "router1" contains.
         {
            "id":11,
            "minIp":3628449016,
            "maxIp":3628449016,
            "display":"216.69.188.248",
            "displayRange":"216.69.188.248",
            "optimalDisplay":[
               "216.69.188.248"
            ],
            "singleIP":true,
            "cidr":true,
            "any":false
         },
         {
            "id":10,
            "minIp":175019786,
            "maxIp":175019786,
            "display":"10.110.151.10",
```

```
            "displayRange":"10.110.151.10",
            "optimalDisplay":[
               "10.110.151.10"
            ],
            "singleIP":true,
            "cidr":true,
            "any":false
         }
      ],
      "creationTime":1528194887856
   }
]
```


Retrieve merged router statuses

Retrieve the status of the current or the last running process of merged stubs. This request is usually used for an asynchronous process.

Resource URL: `/mergeRouters/status`

Resource Method: GET

Authentication: Cookie with session ID.

Response:

Element	Type	Description
MergeRouterJobStatus	String	Status of current or last run process of merged routers: ■ RUNNING - Router is in a merge process. ■ MERGED - Router is merged. ■ UNMERGED - Unmerged router. ■ ERROR - Merge process failed. ■ OUTDATED_MERGED - Router merged before or after the last execution. A list of the status for merged routers.

Merge routers

Merges routers:

- Stub routers into a merged router.
- Merges merged routers into another merged router.
- Adds stub routers and/or merged routers into a merged router.

Routers that are merged with the API are stored in the DB table '`merge_router_job`' and can only be unmerged using the `/unmerge` API.

Resource URL: `/mergeRouters/merge`

Resource Method: POST

Authentication: Cookie with session ID.

Request Body Formats:For stub routers:

Parameter	Type	Description
`forms`	Array of StubsToMerge (see StubsToMerge Type)	List of name for new merged router and IPs of stub routers to add.
`async`	Boolean	Whether to run the merge process in the background.

To merge merged routers:

Parameter	Type	Description
`forms`	Array of MergedRoutersToMerge (see MergedRoutersToMerge Type)	List of name of merged router with list of merged routers to add.
`async`	Boolean	Whether to run the merge process in the background.

To add stub routers and/or merged routers to a merged router.:

Parameter	Type	Description
`async`	Boolean	Whether to run the merge process in the background.
`forms`	MixedMergedRouters (see MixedMergedRouters Type)	List of the name of the merged router and the stub and/or mergers routers to add.

Response:

Element	Type	Description
`Status`	String	Status of merge.

Request examples:

```
// Merge stub routers
{
  "forms": [
            {
                "name":"mergedRouter1",
                "routerIps":["10.20.1.8/8","192.168.1.1"]
              }
        ],
  "async":true //when true, the merge process will run in the background.
}

// Merge merged routers
{
   "forms":[
      {
         "name":"mergedRouter3",
         "mergedRoutersNames":[
            "mergedRouter1",
            "mergedRouter2"
         ]
      }
   ],
  "async":true
}

// Merge merged routers
{
   "forms":[
      {
         "name":"mergedRouter3",
         "mergedRoutersNames":[
            "mergedRouter1",
            "mergedRouter2"
         ]
      }
   ],
```

```
  "async":true
}
// Add stub routers and/or merged routers to a merged router
{
   "async":true,
   "forms":[
      {
         "name":"mergedRouter3",
         "routerIps":[
            "64.202.161.240"
         ],
         "mergedRoutersNames":[
            "mergedRouter1"
         ]
      }
   ]
}
```

Unmerge routers

Unmerges a merged router. Only routers merged by the API and stored in the `merged_router_job` table can be unmerged with the API.

Resource URL: `/mergeRouters/unmerge`

Resource Method: POST

Authentication: Cookie with session ID.

Request Body:

Parameter	Type	Description
`name`	String	Name of router to unmerge.

Response:

Element	Type	Description
`status`	String	Status of unmerge.

Request example:

```
{
"name:"router1"
}
```

Get details for a specified device

Get detailed information such as name, brand name, domain ID for the device specified.

Resource Name: `/api/v1/devices/{firewallName}`

Request Method: GET

Request URL Parameters:

Element	Type	Description
firewallName *Mandatory*	String	Name of the device for which you want to get detailed information.
displayName	Boolean	**True** - you can use device display name as the firewall name. **False** (default) - you must use the device-name as the firewall name.

Response:

Code	Description
200	OK. Returns the requested data as specified in JSON format.
400	Bad request
401	Unauthorized

Request example

```
curl -X GET "https://1.1.1.1/afa/api/v1/devices/Iris_Cisco?displayName=true" -H "accept
```

Add/Edit a device

Adds a device to AFA, or edits the device configuration for a device already managed by AFA.

Resource details

Resource Name: `/api/v1/devices/`

Request Methods:

- **POST** - adds a device
- **PUT** - edits a device

Request URL Parameters:

Parameter	Required	Type	Description
body	Mandatory	String	Data in JSON format that specifies the values for all parameters applicable to the brand of the added or edited device. For more details, see Request parameters by brand.
addChildren	Optional	Boolean	**True** - managed devices are automatically added. (Default) **False** - managed devices are not added unless specifiably explicitly.
testMode	Optional	Boolean	**True** - used as a test run without actually adding or editing the device specified. Returns all parameters that would have been sent by the request. **False** (default) - performs the actual request.

Response:

Code	Description
200	Operation completed successfully

Code	Description
400	Bad request, with one of the following error messages: • **ALREADY_EXISTS**. Specified device not found in AFA. • **SCHEME_ERROR**. Failed to load the device schema. • **Validation Error**. API values are not valid according to the device schema. • **Not Found**. Relevant when editing a device configuration, if the specified device is not found in AFA.
401	Unauthorized
403	Non-admin user

Request example - edit device

```
curl --location --request PUT 'https://docker:7443/afa/api/v1/devices/'
\
--header 'Content-Type: application/json' \
--header 'Accept: */*' \
--header 'Cookie: PHPSESSID=r9psihhnjebng2oovhv268odh1' \
--data-raw '{
    "display_name": "myUpdatedNSC",
    "name": "fw_10_20_13_1",
    "host_name": "10.20.13.1",
    "user_name": "admin",
    "passwd": "algosec",
    "collector": "Central Manager",
    "baseline_profile": "JuniperNetscreenProfile",
    "vrouters": "yes",
    "con": "SSH",
    "ssh_port": "",
    "log_collection_mode": "extensive",
    "collect_log": "yes",
    "collect_log_from": "nsm",
    "log_host_name": "10.0.0.2",
    "log_user_name": "root",
    "log_passwd": "algosec",
    "collect_log_from_adt": "nsm",
    "log_host_name_adt": "10.0.0.1",
    "log_user_name_adt": "root",
    "log_passwd_adt": "algosec",
```

```
    "additional_fw_ids": "1.1.1.1:2.2.2.2:ServerName",
    "log_collection_frequency": "20",
    "active_change": "yes",
    "monitoring": "no",
    "set_user_permissions": "no",
    "password_fields": "passwd:log_passwd:log_passwd_adt",
    "FW_TYPE": "FW_NSC"
  }'
```

Response example - edit device

```
{
  "httpStatus": "200",
  "message": "Successfully modified \"myUpdatedNSC\"",
  "LogData": "",
  "fw_name": "fw_10_20_13_1",
  "syslog_restart_needed": false,
  "not_supported_audit_from_clm": false,
  "set_user_permissions": false
}
```

Request parameters by brand

The following tables list the parameters valid for each brand recognized by AFA. In the tables, click each parameter name to jump to more details.

Amazon Web Services (AWS) EC2

Required	Parameter
Mandatory	• aws_access_key_id • aws_secret_access_key • aws_specific_region • brand • host_name • name (mandatory only when editing)
Optional	• active_change • aws_assume_role • aws_resource_name • monitoring

Azure

Required	Parameter
Mandatory	• azure_client_id • azure_client_key • azure_subscription_id • azure_tenant_id • brand • host_name • name
Optional	• monitoring • route_collection

Checkpoint Provider 1

For managed devices parameters, see Checkpoint Provider 1 managed device parameters.

Required	Parameter
Mandatory	• CKP_R80_or_higher • CMA • CMA_HOST • FW_TYPE • MS_passwd • name • SelectedCMA

Required	Parameter
Optional	• active_change • Allow_Auto_Implementation • **arrFW** - Array of managed devices. For a list of parameters for managed devices, see Checkpoint Provider 1 managed device parameters. • Add/Edit a device • collector • communication • display_name • log_collection_frequency • monitoring • MS_epasswd • MS_host_name • MS_os • MS_user_name • ssh_port

Checkpoint Provider 1 managed device parameters

Required	Parameter
Mandatory	• arrFWs/FW_NAME • arrFWs/LOGSERVER

Required	Parameter
Optional	• arrFWs/do_log_analysis • arrFWs/FW_baseline_profile • arrFWs/FW_display_name • arrFWs/FW_epasswd • arrFWs/FW_host_name • arrFWs/FW_os • arrFWs/FW_passwd • arrFWs/FW_user_name • arrFWs/IS_ENABLED • arrFWs/log_collection_mode • arrFWs/RM_NAME

Checkpoint Smart Center

For managed devices parameters, see Checkpoint Smart Center managed devices parameters.

Required	Parameter
Mandatory	• CKP_R80_or_higher • FW_TYPE • MS_epasswd • MS_host_name • MS_passwd • MS_user_name

Required	Parameter
Optional	• active_change • Allow_Auto_Implementation • **arrFW** - array of managed devices. For a list of parameters for managed devices, see Checkpoint Smart Center managed devices parameters. • collector • communication • display_name • log_collection_frequency • monitoring • MS_os • ssh_port

Checkpoint Smart Center managed devices parameters

Required	Parameter
Mandatory	• arrFWs/FW_display_name • arrFWs/FW_NAME • arrFWs/LOGSERVER
Optional	• arrFWs/do_log_analysis • arrFWs/FW_baseline_profile • arrFWs/FW_epasswd • arrFWs/FW_host_name • arrFWs/FW_os • arrFWs/FW_passwd • arrFWs/FW_user_name • arrFWs/IS_ENABLED • arrFWs/log_collection_mode • arrFWs/RM_NAME

Cisco Application Centric Infrastructure (ACI)

Required	Parameter
Mandatory	• brand • host_name • name • passwd • user_name
Optional	• active_change • collector • display_name • monitoring • route_collection • static_urt_filename

Cisco ASA

Required	Parameter
Mandatory	• epasswd • FW_TYPE • name • passwd • user_name

Required	Parameter
Optional	• additional_fw_ids • baseline_profile • collect_log • collect_log_from • collector • con • display_name • GenerateACL • host_name • log_collection_frequency • log_collection_mode • log_host_name • log_passwd • log_user_name • monitoring • number_of_allowed_encryption_keys • route_collection • rules_view • ssh_port • static_urt_filename

Cisco Firepower

For managed devices parameters, see Cisco Firepower managed device parameters.

Required	Parameter
Mandatory	• brand • fetched_devices - array of managed devices. For a list of parameters for managed devices, see Cisco Firepower managed device parameters. • name • passwd • selected_devices • user_name
Optional	• active_change • collector • display_name • host_name • monitoring

Cisco Firepower managed device parameters

Required	Parameter
Mandatory	• fetched_devices/device_UID • fetched_devices/host_name • fetched_device-host-name • fetched_devices/FW_host_name * • fetched_devices/FW_passwd * • fetched_devices/FW_user_name *
Optional	• fetched_devices/device_domain • fetched_devices/display_name • fetched_devices/FW_baseline_profile • fetched_devices/log_collection_mode • fetched_devices/name • fetched_devices/RM_NAME

Note: Starred parameters are technically listed as optional. However, adding a Firepower device without it's childrens' credentials will cause analysis to fail.

Cisco Identity Services Engine (ISE)

Required	Parameter
Mandatory	• brand • host_name • name • passwd • user_name
Optional	• collector • display_name • monitoring

Cisco IOS

Required	Parameter
Mandatory	• enable_user_name • epasswd • FW_TYPE • host_name • name • passwd • user_name

Required	Parameter
Optional	• Auto_Tree_Update_Enabled • baseline_profile • collector • con • display_name • full_analysis • monitoring • number_of_allowed_encryption_keys • route_collection • separate_vrfs • ssh_port • static_urt_filename

Cisco Nexus Router

Required	Parameter
Mandatory	• brand • collector • host_name • name • passwd • user_name

Required	Parameter
Optional	• Auto_Tree_Update_Enabled • baseline_profile • con • display_name • full_analysis • monitoring • number_of_allowed_encryption_keys • route_collection • separate_vrfs • ssh_port • static_urt_filename

Device from file

Required	Parameter
Mandatory	• existingFile • FW_TYPE • name
Optional	• display_name • fileSource • monitoring • route_collection • static_urt_filename

F5 BIG

Required	Parameter
Mandatory	• brand • host_name • name • passwd • user_name
Optional	• additional_fw_ids • baseline_profile • collect_log • collect_log_from • collector • display_name • log_collection_frequency • log_collection_mode • log_host_name • log_passwd • log_user_name • monitoring • route_collection • static_urt_filename

Fortinet Fortigate

Required	Parameter
Mandatory	• brand • host_name • name • passwd • user_name

Required	Parameter
Optional	• additional_fw_ids • baseline_profile • collect_log • collect_log_from • collector • con • display_name • log_collection_frequency • log_collection_mode • log_host_name • log_passwd • log_user_name • monitoring • number_of_allowed_encryption_keys • route_collection • ssh_port • static_urt_filename

Fortinet Fortimanager

For managed devices parameters, see Fortinet Fortimanager managed devices parameters.

Required	Parameter
Mandatory	• brand • display_name • host_name • name • passwd • user_name

Required	Parameter
Optional	• **arrFW** - array of managed devices. For a list of parameters for managed devices, see Fortinet Fortimanager managed devices parameters. • collect_log • collect_log_from • collector • con • log_collection_frequency • log_collection_mode • log_host_name • log_passwd • log_user_name • monitoring • rest_port

Fortinet Fortimanager managed devices parameters

Required	Parameter
Mandatory	• arrFWs/FWName • arrFWs/FWParent
Optional	• arrFWs/FW_baseline_profile • arrFWs/FW_display_name • arrFWs/FW_host_name • arrFWs/FW_passwd • arrFWs/FW_user_name • arrFWs/FWDefined • arrFWs/FWLogAnalysis • arrFWs/FWLogCollectMode • arrFWs/FWOrigName

Juniper Netscreen

Required	Parameter
Mandatory	• FW_TYPE • host_name • name • passwd • user_name
Optional	• active_change • additional_fw_ids • baseline_profile • collect_log • collect_log_from • collect_log_from_adt • collector • con • display_name • log_collection_frequency • log_collection_mode • log_host_name • log_host_name_adt • log_passwd • log_passwd_adt • log_user_name • log_user_name_adt • monitoring • ssh_port • vrouters

Juniper Space

For managed devices parameters, see Juniper Space managed devices parameters.

Required	Parameter
Mandatory	• brand • fetched_devices - array of managed devices. For a list of parameters for managed devices, see Juniper Space managed devices parameters. • name • passwd • selected_devices • syslog-server-identifier • user_name
Optional	• active_change • additional_fw_ids • collect_log • collect_log_from • collector • display_name • host_name • log_collection_frequency • log_host_name • log_passwd • log_user_name • monitoring

Juniper Space managed devices parameters

Required	Parameter
Mandatory	• fetched_devices/device_domain • fetched_devices/device_id • fetched_devices/device_UID • fetched_devices/display_name • fetched_devices/FW_host_name • fetched_devices/syslogIdentifiers

Required	Parameter
Optional	• fetched_devices/FW_baseline_profile • fetched_devices/FW_epasswd • fetched_devices/FW_os • fetched_devices/FW_passwd • fetched_devices/FW_user_name

Juniper SRX

Required	Parameter
Mandatory	• brand • host_name • name • passwd • user_name
Optional	• additional_fw_ids • baseline_profile • collect_log • collect_log_from • collector • con • display_name • log_collection_frequency • log_collection_mode • log_host_name • log_passwd • log_user_name • monitoring • number_of_allowed_encryption_keys • route_collection • static_urt_filename • vrouters

Palo Alto firewall

Required	Parameter
Mandatory	• brand • host_name • name • passwd • user_name
Optional	• additional_fw_ids • baseline_profile • collect_log • collect_log_from • collector • con • display_name • log_collection_frequency • log_collection_mode • log_host_name • log_passwd • log_user_name • monitoring • number_of_allowed_encryption_keys • route_collection • static_urt_filename

Palo Alto Panorama

For managed devices parameters, see Palo Alto Panorama managed devices parameters.

Required	Parameter
Mandatory	• brand • device_UID • log_host_name • original_name • passwd • selected_devices • user_name
Optional	• active_change • additional_fw_ids • collect_log • collect_log_from • collector • fetched_devices - array of managed devices. For a list of parameters for managed devices, see Palo Alto Panorama managed devices parameters. • host_name • log_collection_frequency • log_passwd • log_user_name • secondary_host_ip

Palo Alto Panorama managed devices parameters

Required	Parameter
Mandatory	• fetched_devices/device_group • fetched_devices/device_UID • fetched_devices/display_name • fetched_devices/FW_host_name • fetched_devices/host_name

Required	Parameter
Optional	• fetched_devices/FW_baseline_profile • fetched_devices/FW_epasswd • fetched_devices/FW_os • fetched_devices/FW_passwd • fetched_devices/FW_user_name

VMWare NSX

Required	Parameter
Mandatory	• brand • host_name • name • passwd • user_name
Optional	• active_change • collector • con • display_name • learning_mode • monitoring • route_collection • separate_vrfs

Device parameter details

The following tables lists all the parameters used by **/api/v1/devices/** GET, POST and PUT methods. All of the listed values are formatted as Strings, unless otherwise indicated.

Note: By default, parameter values for child objects are automatically imported into your REST API call. This functionality is controlled by the addChildren parameter.

Parameter	Description
active_change	Licenses ActiveChange capabilities for the domain. Possible values: • **yes** • **no** (default)
additional_fw_ids	Additional device identifiers. AFA can use multiple IP addresses or hostnames to identify this device when parsing logs, in addition to the default host.
Allow_Auto_ Implementation	Possible values: • **yes** • **no** (default)
arrFWs/do_log_analysis	Configures whether to perform log analysis on child devices in the array.
arrFWs/FW_baseline_ profile	The default baseline profile for the child device in the array.
arrFWs/FW_display_name	Display name of the child device in the array.
arrFWs/FW_epasswd	Password used for advanced mode for the child device in the array. Relevant for Cisco routers only.
arrFWs/FW_host_name	Host name of the child device in the array.
arrFWs/FW_NAME	Name of the child device in the array.
arrFWs/FW_os	Operating system of the child device in the array.
arrFWs/FW_passwd	Password to access the child device in the array.
arrFWs/FW_user_name	Username to access the child device in the array.

Parameter	Description
arrFWs/FWDefined	Determines whether the child device in the array is defined. Possible values: • **yes** • **no**
arrFWs/FWLogAnalysis	Determines whether log analysis is enabled for the child device in the array. Possible values: • **yes** • **no**
arrFWs/FWLogCollectMode	The log collection mode defined for the child device in the array. Possible values: • **none** • **standard** • **extensive**
arrFWs/FWName	The unique AFA name for the child device in the array.
arrFWs/FWOrigName	The original named as defined in the child device in the array.
arrFWs/FWParent	The name of the child device's parent in the array.
arrFWs/IS_ENABLED	Determines whether the child device in the array is enabled. Possible values: • **yes** • **no**

Parameter	Description
arrFWs/log_collection_mode	Mode of log collection. Possible values: • **none** • **standard** • **extensive**
arrFWs/LOGSERVER	The name of the log server for the child device in the array.
arrFWs/RM_NAME	The name of the ASMS system node that collects data for the child device in the array. Default value: **Central Manager**
Auto_Tree_Update_Enabled	Allows monitor to auto update the device tree if new VRFs are found on monitor
aws_access_key_id	AWS access key ID.
aws_assume_role	Set of temporary security credentials you can use to access AWS resources that you might not normally have access to
aws_resource_name	Amazon Resource Name (ARN).
aws_secret_access_key	AWS secret access key.
aws_specific_region	AWS region.
azure_client_id	Azure app client ID (Application ID).
azure_client_key	Client secret key.
azure_subscription_id	GUID that identifies your subscription.
azure_tenant_id	GUID that identifies the Azure Active Directory instance.
baseline_profile	The default baseline profile for the device.

Parameter	Description
brand	Device brand, for devices that don't have a specific FW_TYPE parameter value. Possible values: • **aws** - Amazon Web Services (AWS) EC2. • **azure** - Azure. • **pv1** - Checkpoint Provider 1. • **cma** - Checkpoint Smart Center. • **ciscoaci** - Cisco Application Centric Infrastructure (ACI). • **pix** - Cisco ASA. • **firepower** - Cisco Firepower. • **ciscoise** - Cisco Identity Services Engine (ISE). • **ios** - Cisco IOS. • **nexus** - Cisco Nexus Router. • **file** - Device from file. • **f5bigip_afm** - F5 BIG-IP LTM and AFM. • **fortigate** - Fortinet Fortigate. • **fortimanager** - Fortinet Fortimanager. • **nsc** - Juniper Netscreen. • **space_security_director** - Juniper Space. • **junos** - Juniper SRX. • **paloalto** - Palo Alto firewall. • **panorama** - Palo Alto Panorama. • **nsx** - VMWare NSX.
CKP_R80_or_higher	Relevant for Checkpoint Provider 1 and SmartCenter. Possible values: • **1** - device will be connected to CKP Manager R80 or higher. • **0** - device will not be connected to CKP Manager R80 or higher.

Parameter	Description
CMA	Comma-separated list of the Check Point Smart Center names.
CMA_HOST	Comma-separated list of the Check Point Smart Center IP addresses.
collect_log	Enable log collection. Possible values: • **yes** • **no**
collect_log_from	Log server type for traffic logs. Possible values: • (blank) - no log collection. • **syslog** - syslog NG Server. • **nsm** - Juniper NSM - relevant only for NetScreen devices.
collect_log_from_adt	Log server type for audit logs. Possible values: • (blank) - no log collection. • **syslog** - syslog NG Server. • **nsm** - Juniper NSM - relevant only for NetScreen devices.
collector	Name of the ASMS system node that collects data from the device. Possible values: • **Central Manager** (Default) • **<name of the collector>**
communication	Relevant for all SSH Direct devices. Possible values: **cpstat**

Parameter	Description
con	Type of connection. Possible values for most relevant brands: • **SSH** (Default) • **telnet** For Cisco ASA, additional possible values include: • **SSH(3des)** • **SSH(des)** For Fortigate Fortimanager, possible values include only: • **ssh** • **rest**
device_UID	The device's unique ID.*
display_name	Display name of the device.
enable_user_name	Username used for advanced mode. Relevant for Cisco routers only.
epasswd	Password used for advanced mode. Relevant for Cisco routers only.
existingFile	Relevant for **Device From File**. Enables an existing file in the Algosec file system to be specified as the data source. File must be located in **/home/afa/algosec/fwfiles**
fetched_devices	The device's children, in a comma-separated list of the **fetched_device** objects.*
fetched_devices/device_domain	The ID of the fetched device's domain.* Value: **0**, unless you have Provider Edition enabled. For more details, see ASMS Provider Edition documentation.

Parameter	Description
fetched_devices/device_group	The ID of the fetched device's group.*
fetched_devices/device_id	The fetched device's ID.*
fetched_devices/device_UID	The fetched device's unique ID.*
fetched_devices/display_name	The fetched device's display name.*
fetched_devices/FW_baseline_profile	The name of the baseline profile associated with the fetched devices.
fetched_devices/FW_epasswd	Password used for advanced mode for the fetched device. Relevant for Cisco routers only.
fetched_devices/FW_host_name	The host name of a fetched device.
fetched_devices/FW_NAME	The fetched device's name.
fetched_devices/FW_os	The fetched device's operating system.
fetched_devices/FW_passwd	The password used to access the fetched device.
fetched_devices/FW_user_name	The username used to access the fetched device.
fetched_devices/host_name	The host name of the fetched device, as defined in the device itself.*
fetched_devices/log_collection_mode	Mode of log collection for the fetched device.* Possible values: • **none** • **standard** • **extensive**

Parameter	Description
fetched_devices/name	The fetched device's unique name, as defined in AFA.*
fetched_devices/original_name	The original name for the fetched device, as defined in the device itself.*
fetched_devices/RM_NAME	The ASMS system node that collects data from the fetched device. Default value: **Central Manager**
fetched_devices/serial_num	The fetched device's serial number.*
fetched_devices/syslogIdentifiers	Comma-separated list of the fetched device's syslog servers.*
fileSource	Enables a file to be uploaded to add or edit a device from a file. **Possible value:** Absolute path to the file you want to upload, including the file name. These files are stored in the **/home/afa/algosec/fwfiles/** directory. For example: **/home/afa/algosec/fwfiles/myCiscoASA.zip**
full_analysis	Enable policy analysis. Possible values: • **no** - default and recommended value for routers with no ACLs. • **yes**

Parameter	Description
FW_TYPE	Device type, for devices that don't have a brand parameter. Possible values: • **CMA** - Check Point Smart Center • **FW_FILE** - Device from file • **FW_IOS** - Cisco IOS routers • **FW_NSC** - Juniper Netscreen • **FW_NSM** - Juniper NSM • **FW_PIX** - Cisco ASA • **PV1** - Check Point Multi-Domain Security Management **Note:** All other devices do not need a specific value for this parameter. Set the brand parameter value instead.
GenerateACL	Determines whether FireFlow can generate CLI recommendations and push them to the device via ActiveChange. Possible values: • **yes** • **no** (Default)
host_name	Host name of the device. **Note:** For cloud devices, use the name defined for the device in AFA.

Parameter	Description
learning_mode	Determines whether Learning Mode is enabled. Possible values: • **yes.** Learning Mode is enabled. • **no** (Default) **Note:** Learning Mode marks all traffic from the firewall as blocked, without actually blocking traffic. This enables you to better understand that traffic that flows through the firewall, enabling you to optimize your rules to support your business needs.
log_collection_frequency	Sets how often the log is collected. Value in minutes. Default = **60**
log_collection_mode	Mode of log collection for the child device. Possible values: • **none** • **standard** • **extensive** **Note:** For Cisco firewalls, if only hit-counters are required (and no traffic logs), set to 'none'.
log_host_name	Host name of the traffic log server.
log_host_name_adt	Host name of the ADT Syslog server. Required for configuring a Syslog-NG server for the first time. Default: **localhost**
log_passwd	Password to connect to the traffic log server.
log_passwd_adt	Password to connect to the audit log server.
log_user_name	Username to connect to the traffic log server.

Parameter	Description
log_user_name_adt	Username to connect to the audit log server.
monitoring	Sets if the device is monitored. Possible values: • **yes** • **no** (default)
MS_epasswd	Password used for advanced mode for the device.
MS_host_name	Host name of the device.
MS_os	Operating system of the device.
MS_passwd	Password to access the device.
MS_user_name	Username to access the device.
name	Tree name of the device. Relevant only for device edit (PUT). **Note:** This is not the name displayed in the tree. Get this name using another API. For details, see Get details for a specified device or Get a list of devices.
number_of_allowed_encryption_keys	Relevant for all SSH Direct devices. Controls how many SSH keys are stored for the device to avoid known_host issues. Possible values: • **unlimited** - default • **1** • **2**
original_name	The device's original name, as defined in the device itself.
passwd	Password of user.

Parameter	Description
rest_port	The device's REST connection port number.
route_collection	The device's routing information collection method. Possible values: • **automatic** (Default) • **static** **Note:** If you have manually edited the device's routing table, use the **static** value together with filename of the static URT file. Use this parameter together with the static_urt_filename parameter.
rules_view	Determines the type of rules view used in ASMS. Possible values: • **CLI** • **ASDM**. Use together with the Intelligent Policy Tuner and to display unused objects within rules. **Note:** ASDM is supported even if you manage the Cisco firewall from the command line.
secondary_host_ip	Allows allocation of a secondary IP for the management platform. If the primary IP is not accessible after several attempts, the secondary IP is accessed.

Parameter	Description

selected_devices	Key and value list of child devices you want to add to AFA.
	Use a list of a device names with empty key values.
	For example:
	`"selected_devices": {`
	`"Lion_New": {},`
	`"vSRX-Neptune": {},`
	`"vSRX-Uranus": {}`
	`}`
	Note: If you are working with a management devices, you must add the child devices even if you are making no changes to those children. Children that are not listed in this value will not be added to AFA.

fetched_device-host-name	The fetched device's host name. Use the APIs listed in Get data on managed devices to get these values.
SelectedCMA	List of Smart Centers that are managed by MDLM.
separate_vrfs	Determines whether VRF separation is enabled. Relevant for Cisco routers only. Possible values: • **yes** (default and recommended) • **no**
ssh_port	The port used to connect via SSH.
static_urt_filename	The name of the file that contains static routing data. Use this parameter together with the route_collection parameter.

Parameter	Description
syslog-server-identifier	The ID of the device's syslog server.
user_name	Name of user used to access the device.
vrouters	Determines whether to display virtual routers in the device tree and network map for the device.

View device parameter templates

Gets the brand parameters template for the specified device.

Use this request as a utility to view the relevant parameters per brand before adding or editing device using the **/api/v1/devices/** request. For more details, see Add/Edit a device.

Resource Name: `/api/v1/devices/examples/<brandName>`

Request Method:

GET

Request URL Parameters:

Parameter	Required	Type	Description
brandName	Mandatory	String	Brand name of the required device as follows: **aws**, **azure**, **ciscoaci**, **ciscoise**, **ios**, **nexus**, **cma**, **pv1**, **f5bigip_afm**, **file**, **firepower**, **fortigate**, **fortimanager**, **junos**, **nsc**, **space_security_director**, **nsx**, **paloalto**, **panorama**
requiredOnly	Optional	Boolean	**True** - Returns only mandatory parameters **False** - Returns both mandatory and optional parameters

Response:

Code	Description
200	OK. Returns the requested data as specified in JSON format.

Code	Description
400	Bad request
401	Unauthorized

Request example

```
curl --location --request GET 'https://docker:7443/afa/api/v1/devices/e
xamples/nsc' \
--header 'Content-Type: application/json' \
--header 'Accept: */*' \
--header 'Cookie: PHPSESSID=r9psihhnjebng2oovhv268odh1'
```

Response example

```
{
"collect_log_from": "nsm",
"ssh_port": "",
"con": "SSH",
"FW_TYPE": "FW_NSC",
"log_passwd": "<syslog-server-password>",
"user_name": "<user-name>",
"log_collection_mode": "extensive",
"active_change": "yes",
"log_user_name": "<syslog-server-user-name>",
"log_host_name": "<syslog-server-host-name>",
"monitoring": "no",
"display_name": "<display-name>",
"log_user_name_adt": "<auditing-server-user-name>",
"collector": "Central Manager",
"log_passwd_adt": "<auditing-server-password>",
"collect_log": "yes",
"passwd": "<password>",
"vrouters": "yes",
"baseline_profile": "JuniperNetscreenProfile",
"name": "<unique name set by AFA, relevant only for 'EDIT'>",
"log_host_name_adt": "<auditing-server-host-name>",
"collect_log_from_adt": "nsm",
"host_name": "<host-name>",
"log_collection_frequency": "60",
"additional_fw_ids": ""
}
```

Delete a device

Deletes the specified device from AFA.

Resource Name: `/api/v1/devices/{firewallName}`

Request Method: DELETE

Request URL Parameters:

Element	Type	Description
`device-name` *Mandatory*	String	Name of the device you want to delete. **Note:** This is not the name displayed in the tree. Get this name using another API. For details, see Get details for a specified device or Get a list of devices.

Response:

Code	Description
200	Operation completed successfully
400	Bad request. This response may include the following error message: **Not Found**. Relevant when editing a device configuration, if the specified device is not found in AFA.
401	Unauthorized
403	Non-admin user

Request example

```
curl --location --request DELETE 'https://1.1.1.1/afa/api/v1/devices/10_20_13_1' \
--header 'Content-Type: application/json' \
--header 'Accept: */*' \
--header 'Cookie: PHPSESSID=7qdbj3us6488i7hvfh2fb817f1'
```

Response example

```
{
```

```
 "httpStatus": "200",
  "message": "Successfully deleted the device: fw_10_20_13_1",
  "LogData": "",
  "fw_name": "",
  "syslog_restart_needed": false,
  "not_supported_audit_from_clm": false,
  "set_user_permissions": false
}
```

Get a list of devices

Gets a list of all devices that the user has permissions to view.

Resource Name: `/api/v1/devices/`

Request Method: GET

Request URL Parameters:

Element	Type	Description
getBylevel	String	• **no** (default) - returns all elements as a flat list • **yes** - returns all elements ordered by level

Response:

Code	Description
200	OK. Returns the requested data as specified in JSON format.
400	Bad request
401	Unauthorized

Request example

```
curl -X GET "https://1.1.1.1/afa/api/v1/devices/?getBylevel=yes"
-H "accept: */*"
```

Get data on managed devices

Gets information on devices managed by the specified management device.

Note: For example, you may want to use these APIs to get values for parameters when adding new management devices to AFA, or editing management device configurations. For more details, see Add/Edit a device.

Resource Name:

Brand	URL
Cisco Firepower, Palo Alto Panorama, Juniper Space	`/api/v1/devices/managedDevices/genericDevices`
Fortinet Fortimanager	`/api/v1/devices/managedDevices/fortimanager`
Checkpoint Smart Center	`/api/v1/devices/managedDevices/cma`
Checkpoint Provider 1	`/api/v1/devices/managedDevices/pv1`
Checkpoint Provider 1/Checkpoint Smart Center	`/api/v1/devices/managedDevices/pv1/cma`

Request Method: POST

Request URL Parameters:

Brand	Element	Type	Description
Cisco Firepower, Palo Alto Panorama, Juniper Space	body	String	JSON that specifies the management device that manages the devices for which you want to get details.

Brand	Element	Type	Description
Fortinet Fortimanager, **Checkpoint Smart Center, Checkpoint Smart Center, Checkpoint Provider 1**	body	String	A map of devices in the following syntax: **map<String, Object>**

Response:

Brand	Description
Cisco Firepower, Palo Alto Panorama, Juniper Space	JSON that specifies the management device that manages the devices for which you want to get details.
Fortinet Fortimanager, **Checkpoint Smart Center, Checkpoint Smart Center, Checkpoint Provider 1**	A map of devices in the following syntax: **map<String, Object>**

.

Code	Description
200	OK
400	Bad request
401	Unauthorized
403	Non-admin user

Request example

```
curl --location --request POST 'https://docker:7443/afa/api/v1/
firewallData/managedDevices/fortimanager' \
```

```
--header 'Content-Type: application/json' \
--header 'Accept: */*' \
--header 'Cookie: PHPSESSID=r9psihhnjebng2oovhv268odh1' \
--data-raw '{
        "brand": "fortimanager",
        "host_name": "10.20.138.1",
        "user_name": "admin",
        "passwd": "algosec1"
      }'
```

Response example


```
[
  {
    "FWOrigName": "root",
    "FWParent": "FG100D3G16803186-TEST_DontChange",
    "FWName": "FG100D3G16803186_TEST_DontChange_root"
  },
  {
    "FWOrigName": "Da_VDOM1",
    "FWParent": "FG100D3G16803186-TEST_DontChange",
    "FWName": "Da_VDOM1"
  },
  {
    "FWOrigName": "Da_vDOM2",
    "FWParent": "FG100D3G16803186-TEST_DontChange",
    "FWName": "Da_vDOM2"
  },
  {
    "FWOrigName": "root",
    "FWParent": "Sarid-1",
    "FWName": "root"
  },
  {
    "FWOrigName": "VDOM",
    "FWParent": "Sarid-1",
    "FWName": "VDOM"
  },
  {
    "FWOrigName": "newVDOM-5",
    "FWParent": "Sarid-1",
    "FWName": "newVDOM-5"
  },
```

```
  {
    "FWOrigName": "root",
    "FWParent": "Ott_Dam_HA",
    "FWName": "Ott_Dam_HA_root"
  },
  {
    "FWOrigName": "vDOM1_HA",
    "FWParent": "Ott_Dam_HA",
    "FWName": "vDOM1_HA"
  },
  {
    "FWOrigName": "vDOM2_HA",
    "FWParent": "Ott_Dam_HA",
    "FWName": "vDOM2_HA"
  },
  {
    "FWOrigName": "V_ICS_PCI",
    "FWParent": "Ott_Dam_HA",
    "FWName": "V_ICS_PCI"
  },
  {
    "FWOrigName": "V_ICS_SADCO",
    "FWParent": "Ott_Dam_HA",
    "FWName": "V_ICS_SADCO"
  }
]
```


Risk APIs

The AFA REST API supports the following APIs for managing risk data:

- Retrieve a risk profile list
- Import risks from XML
- Import risks from spreadsheet

Retrieve a risk profile list

Use the sessionID to retrieve a list of risk profile Excel files for the session user. Pass the name of an Excel file in get_zones to retrieve the list of the security zones in each risk profile. If you have the name of the risk profile Excel file, it is not necessary to execute this API.

Resource Name: `/afa/api/v1/security_zones/get_profiles_list`

Request Method: GET

Authentication: Cookie with session ID

Header Requirements:

Element	Type	Description
`sessionID` *Mandatory*	String	Session ID returned in Login request.

Response:

Element	Type	Description
`data`	Array of String	List of risk profile Excel file names for use in get_zones request.
`status`	String	One of the following: • true - Request succeeded. • false - Request failed.
`message`	String	An error message returned when request fails.

Request example

```
curl --cookie "PHPSESSID=g4mgnv4cno9ivt7rclmhmejj27" https://
<IP:Port>/afa/api/v1/security_zones/get_profiles_list
```

Response example

```
[ "spreadsheet_2.xlsx", "1.xlsx" ]
```

Import risks from XML

The `import_risks_from_xml` request imports risks to a custom risk profile from an XML file.

Request Method: PUT

Request URL Parameters:

Element	Type	Description
SessionID Mandatory	String	Session ID returned in `login` request.
RiskProfileName Mandatory	String	Name of the risk profile you are importing risks to.
EncodedFileData Mandatory	String	Path to an XML file, 64-encoded

Response:

Element	Type	Description
RetVal	Integer	One of the following: • 0 = Failed • 1 = Succeeded
RetMessage	String	Message to indicate the success of the API call.

Import risks from spreadsheet

The `import_risks_from_spreadsheet` request imports risks to a custom risk profile from a spreadsheet file.

Request Method: PUT

Request URL Parameters:

Element	Type	Description
SessionID Mandatory	String	Session ID returned in `login` request.
RiskProfileName Mandatory	String	Name of the risk profile you are importing risks to.

Element	Type	Description
EncodedFileData Mandatory	String	Path to a spreadsheet file, 64-encoded
InheritStandard Mandatory	Integer	Determines whether the new risk profile should inherit from the standard profile. • 0 = No • 1 = Yes

Response:

Element	Type	Description
RetVal	Integer	One of the following: • 0 = Failed • 1 = Succeeded
RetMessage	String	Message to indicate the success of the API call.

Rule data APIs

The AFA REST API supports the following APIs for managing rule data:

- Retrieve rules
- Retrieve risky rules
- Rules hit count

Retrieve rules

The `get_rules` request retrieves all the rules in a device's or group's policy.

The input will be the active session ID and the name of the device, group, or matrix. The output will be a list of all the rules of all the policies that apply to each device, including the value of each rule field.

Resource Name: `/fa/server/rules/read`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`session`*Mandatory*	String	Session ID returned in `login` request.
`entity`*Mandatory*	String	The display name of the device, group, or matrix.

`entityType`*Optional*	String	One of the following:
		■ `device` (default)
		`group`
		`matrix`

Note: The `page` and `size` elements are not supported for the `get_rules` request.

Response:

Element	Type	Description
`name`	String	The name of the entity.
`type`	String	The entity type.
`rules`	A list of `rule` objects.	A list of rules, including the values for each rule's fields. The fields for each rule vary by device brand .
`status`	String	One of the following: ■ `true`. Indicates the request succeeded. ■ `false`. Indicates the request failed.
`message`*Only is returned when the request fails.*	String	An error message.

Request example

```
curl -H "Accept:application/json" -k "https://192.168.3.76/fa/server/
rules/read?session=c69bcc3e6832149642b32e6f269c82c0&entity=admin
```

Response example

```
{
```

```
"0":    {
"name": "admin",
"type": "DEVICE",
"rules":       [
{
"ruleNum": "CSM_IPV6_FW_ACL_MGT(2)",
"ruleId": "0x3e40f580",
"deviceID": 468,
"source": ["TammarsIPv6"],
"isNegateSource": false,
"destination": ["ALONOBJ"],
"isNegateDestination": false,
"service": ["102"],
"isNegateService": false,
"action": "permit",
"enable": "enabled",
"log": "",
"comments": [""],
"time": [""],
"cli": ["ipv6 access-list CSM_IPV6_FW_ACL_MGT permit object-group 102
object-group TammarsIPv6 object-group ALONOBJ"]
},
{
"ruleNum":"CSM_IPV6_FW_ACL_MGT(6)",
"ruleId": "0x108b3f0b",
"deviceID": 468,
"source": ["fdf8:c07d:9849:25b1:1000:2000:3000:4001"],
"isNegateSource": false,
"destination": ["any"],
"isNegateDestination": false,
"service": ["tcp/588"],
"isNegateService": false,
```

```
"action": "permit",
"enable": "enabled",
"log": "informational",
"comments": ["FireFlow #6161 Einats comment"],
"time": [""],
"cli": ["ipv6 access-list CSM_IPV6_FW_ACL_MGT permit tcp host fdf8:c07d:
9849:25b1:1000:2000:3000:4001 any eq 588 log"]
},
{
"ruleNum": "Int-30_access_in_1(16)",
"ruleId": "0xf15f1e42",
"deviceID": 468,
"source": ["10.30.9.147"],
"isNegateSource": false,
"destination": ["10.110.9.158"],
"isNegateDestination": false,
"service": ["tcp/16992"],
"isNegateService": false,
"action": "permit",
"enable": "enabled",
"log": "informational",
"comments": ["6988 AsherAdded"],
"time": [""],
"cli": ["access-list Int-30_access_in_1 extended permit tcp host
10.30.9.147 host 10.110.9.158 eq 16992 log"]
}
]
},
"status": true
}
```


Retrieve risky rules

The `riskyRules_get` request retrieves all the risky rules in a device's or group's policy.

The input will be the active session ID and the name of the device, group, or matrix. The output will be a list of all risky rules of all the policies that apply to each device, including the risk severity of each rule.

Resource Name: `/fa/server/risks/riskyRules`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`session`*Mandatory*	String	Session ID returned in `login` request.
`entity`*Mandatory*	String	The display name of the device, group, or matrix.

`entityType`*Mandatory*	String	One of the following:
		■ `device` (default)
		`group`
		`matrix`

`responseType`*Optional*	String	Format of response data.One of the following: ■ `json` (default) `csv`

Note: The `page` and `size` elements are not supported for the `riskyRules_get` request.

Response:

Element	Type	Description
`riskyRules`	Array of RiskyRules (see RiskyRules)	The risky rules data, sorted by severity.
`status`	String	One of the following: ■ `true`. Indicates the request succeeded. ■ `false`. Indicates the request failed.

Element	Type	Description
`message` *Only returned when the request fails.*	String	One of the following error messages: ■ Device not found Not found "Unknown firewall '<firewall name>' http status 400 ■ Unauthorized Unauthorized. You are not permitted to perform this operation http status 401 ■ There is no report for the device Backend error: There is no completed report for the firewall <firewall name> http status 500 ■ There is no rules for the firewall in DB Backend error: Failed to get rules for the firewall <firewall name> http status 500 ■ There is no risky rules data Backend error: Failed to find risky rules data in report <report name> http status 500

Request examples

```
curl -k 'https://127.0.0.1/fa/server/risks/riskyRules?session=
1d61d46c3093b0f31bb76054dfc3271b&entity=Dev-GW-R71Test1curl -k
'https://127.0.0.1/fa/server/risks/riskyRules?session=
1d61d46c3093b0f31bb76054dfc3271b&entity=Dev-GW-R71Test1
```

Response example of RiskyRules in JSON Format

```
{
"riskyRules":[
{
"device":"Nachos",
"ruleId":"2B1EA29F-3ED3-4FAC-BA7C-FC27F1A6305F",
```

```
"ruleNum":"1",
"source":["n10_20_0_0"],
"destination":["Any"],
"service":["Any"],
"action":"accept",
"documentation":{"documentation":""},
"risks":[{"code":"R01","severity":"MEDIUM","title":"\"From somewhere to
Any allow Any service\" rules"}],
"totalBySeverity":{"LOW":0,"HIGH":0,"MEDIUM":1,"SUSP_HIGH":0},
"trafficCount":"0"},
 …
],
"status":true
}
```


Example of RiskyRules in CSV Format


```
{ "riskyRules":"Device,Rule,Id,Source,Destination,Application,Service,
Action,Comment,Traffic count,Documentation,High Risks,Suspected High
Risks,Meduim Risks,Low Risks\n Nachos,1,2B1EA29F-3ED3-4FAC-BA7C-
FC27F1A6305F,[n10_20_0_0],[Any],N\/A,[Any],accept,N\/A,0,,0,0,1,0\n
Nachos,2,6A5BBC4B-D8AA-4533-A01F-89A08F3E310D,[n192_168_0_0],[Any],
N\/A,[Any],accept,N\/A,0,,0,0,1,0\n", "status":true }
```


Rules hit count

Count the number of times a specific rule or rules were triggered on a specific device.

Resource Name: `/api/v1/rules/hit-count`

Request Method: POST

Request URL Header:

Element	Type	Description
Cookie *Mandatory*	String	Cookie obtained from the connect method.

Request URL Parameters:

Element	Type	Description
invertSorting *Optional*	Boolean	If true, sorts the rules with the least hits first. Default = **False**

Request body parameters

Element	Type	Description
deviceTreeName *Mandatory*	String	Tree name of the device.
ruleIds *Optional*	String	The Rule IDs for which to collect hit counts. If more than one Rule ID, separate with commas. For example: **[ruleid1, ruleid2, ruleid3]**
startTime **endTime** *Mandatory, when **latestReport** is set to **false**, or left blank*	Integer (Epoch/Unix Timestamp)	Count the number of hits that occurred between **startTime** and **endTime**.
latestReport *Mandatory, when **startTime** and **endTime** are left blank*	Boolean	If true, uses the **startTime** and **endTime** defined in the latest report.
pageSize *Optional*	Integer	The number of rows to display per page in the output JSON file. **Tip:** By default, rules with zero hits are not shown in the results, although the user is notified that these rules exist. To include rules with zero hit counts in the response, increase the **pageSize** parameter in the API enough to fit all the rules onto a single page.
page *Optional*	Integer	The page to display in the output JSON file.

Response:

Code	Description
200	OK. The response includes a set of JSON code based on the data included in the request.
400	Request is invalid
403	Unauthorized
404	Device not found
500	Policy Optimization failed

Example request

The following example sorts the rules included in the response by least hit counts to most.

```
curl  -X POST -H "Content-Type: application/json"
"http://<server>:<port>/ms-policy-optimizations/api/v1/rules/hit-count?
invertSorting=true"
--cookie "PHPSESSID=<sessionID>"  -d '{
"deviceTreeName": "MyDevice",
"ruleIds":[],
"startTime": 1,
"endTime": 1774667654000,
}'
```

Example response

The following is a truncated response showing a few rules on the device, and the number of times each rule was used.

Note: We've formatted the following example to make it easier to read. Real responses for the hit-count API are formatted as a single line.

```
{
"status":"OK",
```

```
"data":
{
 "deviceTreeName":"MyDevice",
 "ruleIds":
 {"content":
  [
   {"ruleId":"from_dmz_to_untrust_name_119","count":11937},
   {"ruleId":"from_untrust_to_dmz_name_153","count":10371},
   {"ruleId":"from_untrust_to_dmz_name_166","count":8942},
   {"ruleId":"from_dmz_to_untrust_name_154","count":6513},
   ....
   ....
   {"ruleId":"from_untrust_to_dmz_name_150","count":73}],"number":0,
"size":900,"totalElements":35,"pageable":
   {"sort":
    {"sorted":false,"unsorted":true,"empty":true},
    "pageNumber":0,"pageSize":900,"offset":0,"paged":true,"unpaged":false
     },
    "last":true,"totalPages":1,"sort":
    {"sorted":false,"unsorted":true,"empty":true},
    "first":true,"numberOfElements":35,"empty":false
    },
   "startTime":1,"endTime":1974667654000},"additionalInfo":{}
 }
```


Security zone APIs

The AFA REST API supports the following APIs for managing security zones:

- Retrieve security zones
- Assign zone types to interfaces

Retrieve security zones

The `get_zones` method retrieves a list of the Security Zone names and IP ranges for each zone listed in the **Networks** tab of the passed risk profile Excel spreadsheet. If the spreadsheet name is known, it is not necessary to call `get_profiles_list`.

Related screens in ASMS are the Security Zones section in **AppViz > Administration > Customization** and the Risk Profiles section in **Firewall Analyzer> Administration > Compliance > Risk Profiles**.

Resource Name: `/afa/api/v1/security_zones/<risk_profile_excel_filename>/get_zones`

Request Method: GET

Authentication: Cookie with session ID

Header Requirements:

Element	Type	Description
`sessionID` *Mandatory*	String	Session ID returned in `Login` request.

Response:

Element	Type	Description
`data`	Array of SecurityZoneObject	List of security zones, each with the list of IP address ranges for the zone.
`status`	String	One of the following: • true - Request succeeded. • false - Request failed.
`message`	String	An error message returned when the request fails.

Request example

```
curl --cookie "PHPSESSID=g4mgnv4cno9ivt7rclmhmejj27" https://<IP:Port>/afa/api/v1/security_zones/my_file_name.xlsx/get_zones
```

where `my_file_name.xlsx` is an item from the Retrieve a risk profile list response.

Response example

```
[ {
"name" : "Net1",
"addresses" : [ "10.21.0.2/24", "10.25.3.2/24" ]
}, {
```

```
"name" : "Net2",
"addresses" : [ "10.50.64.2/20" ]
}, {
"name" : "Net3",
"addresses" : [ "10.3.64.2/24" ]
}, {
"name" : "PartnerNet",
"addresses" : [ "10.120.46.2/28" ]
}, {
"name" : "PCIzone",
"addresses" : [ "10.176.50.2-10.176.60.255" ]
} ]
```

Assign zone types to interfaces

The `update_interfaces` request assigns a zone type to each of a device's interfaces.

The input will be the active session ID, the name of the device, and the zone type for each interface. The output will include a status and message which indicates success or failure.

Note: This request requires permission for All_Firewalls and the Topology action.

Resource Name: `/fa/server/interfaces/update`

Request Method: POST

Request URL Parameters:

Element	Type	Description
`session`*Mandatory*	String	Session ID returned in `login` request.
`firewall`*Mandatory*	String	The display name of the device.
`interfaceZoneTypes` *Mandatory*	Map	A map of device interfaces and the zone types to assign to each.

Response:

Element	Type	Description
`status`	String	One of the following: ■ `true`. Indicates the request succeeded. ■ `false`. Indicates the request failed.
`message`	String	A message which indicates success or a reason for failure.

Request example

```
curl -H "Content-Type: application/json" -X POST -d '{"firewall":"Borscht",
 "interfaceZoneTypes":{"eth0":"DMZ", "eth2":"INTERNAL"}}' -k
'https://127.0.0.1/fa/server/interfaces/update?session=
7d4fe1fc0c8f1c0c6ac2f01a8f915973'
```

Response example

```
{   "status": true,   "message": "success"}
```

User data APIs

The AFA REST API supports the following APIs for managing users and licenses:

- Retrieve license
- Retrieve user data
- Retrieve role data

Retrieve license

The `get_license` request retrieves details about the current ASMS license installed.

Request Method: GET

Response:

Element	Type	Description
Modules	String	The ASMS product modules included in the license.

Element	Type	Description
Expires	String	The date the license expires
Issued_on	String	The date the license was issued.

Retrieve user data

The `users` request retrieves AFA users data.

Resource Name: `/afa/api/v1/users`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`domain` *Optional*	String	Domain ID. Relevant only when domains are enabled. Default: **0**

Response:

Code	Description
200	OK and returns data in JSON format.
401	Unauthorized domain
403	Non-admin user

Request example

```
curl -X GET "https://10.20.7.94/afa/api/v1/users" -H "accept:
application/json"

curl -k 'https://127.0.0.1/afa/api/v1/users?session=
1d61d46c3093b0f31bb76054dfc3271b
```

Response example

```
{
```

```
  "UserName":”<user name>”,
  "FullName":”<full user name>”,
  "Email":”email”,
  "Roles":[<list of roles of the user>],
  "AuthenticationType":”< authentication type : local, ldap, etc >”,
  "LandingPage":”<landing page name>”,
  "Administrator":”<is administrator : yes or no>”,
  "FireflowAdmin":”<is administrator : yes or no>”,
  "EnableAnalysisFromFile":”<permitted to run analysis from file :
yes or no>”,
  "EnableGlobalCustomization":”<permitted for global configuration : yes or no>”,
  "AuthorizedDevices":[
      {
       "ID":”<device name>”,
       “DisplayName”:”<display name>”,
       "Profile":”<authorization profile : standard, read only, etc>”,
       "Notification":”<notification : yes, no>”
                                                  }
                                              ],
     “Domain”:”<domain ID>”
}
```

Retrieve role data

The `roles` request retrieves AFA roles data.

The input will be the active session ID.

Resource Name: `/afa/api/v1/users/Roles`

Request Method: GET

Parameters:

Element	Type	Description
`session`*Mandatory*	String	Session ID returned in `login` request.
`domain`*Optional*	String	Domain ID for a multi-domain environment Relevant only when domains are enabled. Default: **0**

Response:

Code	Description
200	OK and returns data in JSON format.
401	Unauthorized domain
403	Non-admin user

Request example

```
curl -k 'https://127.0.0.1/afa/api/v1/users/Roles?session=
1d61d46c3093b0f31bb76054dfc3271b
```

Response example{

```
{
     "RolesName":”<user name>”,
     "RoleDescription ":”<roles description>”,
     "LadpDN":”<LDAP group corresponding to the current role>”,
     "LandingPage":”<landing page name>”,
     "FireflowAdmin":”<is administrator : yes or no>”,
     "EnableAnalysisFromFile":”<permitted to run analysis from file :
yes or no>”,
     "EnableGlobalCustomization":”<permitted for global configuration :
yes or no>”,
     "AuthorizedDevices":[
          {
          "ID":”<device name>”,
          “DisplayName”:”<display name>”,
          "Profile":”<authorization profile : standard, read only, etc>”,
          "Notification":”<notification : yes, no>”
                                                  }
                                          ],
     “Domain”:”<domain ID>”
}
```

Manage AFA issues

Use the following request methods to manage issues in the AFA issues center.

Note: All of the API requests for managing issues can only be run by administrators.

In a distributed architecture environment, they can only be run on the central manager / master appliance.

Retrieve unresolved issues

The `get_issues` request retrieves all the unresolved issues in the AFA issues center. This includes both acknowledged and active issues.

Resource Name: `/ms-watchdog/v1/api/issues-center/issues`

Request Method: POST

Authentication: Cookie with session ID.

Request URL Parameters:

Element	Type	Description
`size` *Optional*	Integer	Number of results per page. The default value is 10.
`page` *Optional*	Integer	Page number to return. The default value is 0 (the first page). **Note:** This element requires a definition for `size`. Defining this element without `size` will cause the return to be empty.
`sortColumn` *Optional*	String	The column / issue attribute to sort by. One of the elements of the `issueAttributes`, `issue`, or `device` objects. See IssueAttributes type.
`sortDirection` *Optional*	String	The sort direction. One of the following: • `DESC` (Default) • `ASC`

Request Body:

(*Optional*) A map of column names and values.

The response will only include issues which match the specified value(s) for the specified columns.

The column name can be any of the elements of the `issueAttributes`, `issue`, or `device` objects. See IssueAttributes type.

Response:

Element	Type	Description
`content`	Array	An array of `issueAttributes` objects. See IssueAttributes type.
Various elements that describe the paging of the issues.		See the spring framework for more information.

Request example

```
https://<ASMS_Server>/ms-watchdog/v1/api/issues-center/issues?size=13
&page=0&sortColumn=lastFailure&sortDirection=DESC

{"nodeType":"MASTER","issue.type":"System"}
```

Response example


```
{
 "content":[
  {
   "id":1,
   "status":"OPEN",
   "lastFailure":"2019-05-01T14:33:40.369",
   "lastSuccess":null,
   "count":15,
   "nodeType":"MASTER",
   "nodeName":"10.20.15.82",
   "issue":{
    "type":"System",
    "failureType":"Disk space",
    "description":"Low free disk space on /data",
    "remediation":"- Configure/change the backup configuration for a
smaller retention size\n- Delete temporary files.",
    "kbLink":""
    },
```

```
     "device":null
    },
    {
     "id":357,
     "status":"ACKNOWLEDGED",
     "lastFailure":"2019-04-24T08:26:45.264",
   "lastSuccess":"2019-04-21T10:18:19.033",
   "count":818,
   "nodeType":"MASTER",
   "nodeName":"10.20.15.82",
   "issue":{
   "type":"System",
   "failureType":"Disk space",
   "description":"Low free disk space",
   "remediation":"- Configure/change the backup configuration for a
smaller retention size\n- Delete temporary files",
   "kbLink":""
    },
    "device":null
     },
     {
     "id":133,
     "status":"ACKNOWLEDGED",
     "lastFailure":"2019-04-24T08:26:45.06",
     "lastSuccess":null,
     "count":1893,
     "nodeType":"MASTER",
     "nodeName":"10.20.15.82",
     "issue":{
      "type":"System",
      "failureType":"DFS",
      "description":"Synchronization error",
      "remediation":"Synchronization error on node",
      "kbLink":""
      },
      "device":null
      },
],
"pageable":"INSTANCE",
"last":true,
"totalPages":1,
"totalElements":6,
"sort":{
```

```
        "sorted":false,
        "unsorted":true,
        "empty":true
},
"first":true,
"numberOfElements":6,
"size":0,
"number":0,
"empty":false
}
```

Acknowledge an issue

The `acknowledge` request marks active issues in the AFA issues center as acknowledged. Issues marked as acknowledged will appear in the list of acknowledged issues and will no longer appear in the list of active issues.

Resource Name: `/ms-watchdog/v1/api/issues-center/issues/acknowledge`

Request Method: POST

Authentication: Cookie with session ID.

Request Body: Any array of issue IDs. To retrieve the issue IDs, see Retrieve unresolved issues.

Response:

Element	Type	Description
`newStatus`	String	The new status of the issues: **ACKNOWLEDGED**.
`updatedIssues`	Array	An array of issue IDs.
`successful`	Boolean	Whether the request was successful.

Request example

```
#/ms-watchdog/v1/api/issues-center/issues/acknowledge
[2,4]
```

Response example

```
{
        "newStatus":"ACKNOWLEDGED",
        "updatedIssues":[
                2,
                4
        ],
        "successful":true
}
```

Activate an issue

The `activate` request marks acknowledged issues in the AFA issues center as active. Issues marked as active will appear in the list of active issues and will no longer appear in the list of acknowledged issues.

Resource Name: `/ms-watchdog/v1/api/issues-center/issues/activate`

Request Method: POST

Authentication: Cookie with session ID.

Request Body: Any array of issue IDs. To retrieve the issue IDs, see Retrieve unresolved issues.

Response:

Element	Type	Description
`newStatus`	String	The new status of the issues: **OPEN**.
`updatedIssues`	Array	An array of issue IDs.
`successful`	Boolean	Whether the request was successful.

Request example

```
#/ms-watchdog/v1/api/issues-center/issues/activate
[2,4]
```

Response example

```
{
```

```
        "newStatus":"OPEN",
        "updatedIssues":[
                2,
                4
        ],
        "successful":true
}
```

Device relocation APIs

The AFA REST API supports the following APIs for device relocation:

- Relocate devices between nodes
- Check device relocation progress
- Cancel device relocation
- Enable processes after relocation

Relocate devices between nodes

Relocates devices between nodes in distributed architectures.

Note: Before relocating devices, disable monitoring and analysis for those devices in AFA.

Resource Name: `/api/v1/device/relocation`

Request Method: POST

Request URL Parameters:

Element	Type	Description
relocationTimeFrameInMinutes *Optional*	Integer	Time limit, in minutes, after which you want the relocation process to time-out if not completed. **0** = Unlimited. **Note:** Devices are fully relocated as soon as they pass a connectivity check. If a configured time limit is reached, and not all devices have been relocated, any subsequent devices are left on the source nodes. Devices that were relocated remain on the new, target, node, and are not reverted.
runDeviceAction *Optional*	String	One of the following: • **Enabled**. Monitoring, analysis, and syslog messages are enabled for all relocated devices • **Disabled**. Monitoring, analysis, and syslog messages are disabled for all relocated devices. This helps to reduce CPU load. • **NO_ACTION**. Retains current configuration for each setting.
sourceNode *Mandatory*	String	Name of the current device node, as listed on the **Architecture** tab of the AFA **Administration** area.
targetNode *Mandatory*	String	Name of the node you want to relocate your devices to. Check the names of the nodes listed on the **Architecture** tab of the AFA **Administration** area.

Element	Type	Description
treeNames *Mandatory when the source is an ASMS Central Manager.*	String	One of the following: • **For relocating from a Central Manager**, the name of the device group you want to relocate. • **For relocating from a Remote Agent**, the name of the device group you want to relocate. This group must include only Remote Agent devices. For example, you may have created a group of devices before starting your relocation process. If the source is a Remote Agent, and this value is empty, all devices on the source Remote Agent are relocated. **Note:** This parameter is defined as the device name listed in the **firewall_data.xml** file. This name may be different than the one listed in the device tree.

Response:

Code	Description
200	Operation completed successfully
400	Bad request
401	Unauthorized
423	Device relocation is already running

Request example

```
curl -X POST --cookie "PHPSESSID=24l2tk7p8skuk4bbv20krqe7s7" -d '{
"treeNames":["10_20_26_1"], "sourceNode":"RA1", "targetNode":"RA2" }'
--header "Content-Type: application/json" 0:8080/afa/api/v1/device/
```

```
relocation
```

Response example

```
{
"bd98c84e-f88c-42b4-899c-9a7584a75951"
}
```

Check device relocation progress

Checks the progress of the currently running device relocation process.

Resource Name: `/api/v1/device/relocation`

Request Method: GET

Request URL Parameters:

Element	Type	Description
uuid *Mandatory*	String	The UUID of the currently running relocation process.

Response:

Code	Description
200	Operation completed successfully
400	Bad request
401	Unauthorized

Request example

```
curl -X GET --cookie "PHPSESSID=24l2tk7p8skuk4bbv20krqe7s7" --header "Content-Type: appl
0:8080/afa/api/v1/device/relocation?uuid=bd98c84e-f88c-42b4-899c-9a7584a75951
```

Response example

```
{
  "uuid": " bd98c84e-f88c-42b4-899c-9a7584a75951",
```

```
  "taskName": "device-relocation",
  "startTaskTime": 1582540248574,
  "endTaskTime": 1582540255994,
  "taskState": "COMPLETE",
  "result": {
    "successes": [
      "10_20_26_1"
    ]
  }
}
```

Cancel device relocation

Stops the currently running device relocation process.

Resource Name: `/api/v1/device/relocation`

Request Method: DELETE

Request URL Parameters:

Element	Type	Description
uuid *Mandatory*	String	The UUID of the currently running relocation process.

Response:

Code	Description
200	Operation completed successfully
400	Bad request
401	Unauthorized

Request example

```
curl -X DELETE --cookie "PHPSESSID=24l2tk7p8skuk4bbv20krqe7s7"
--header "Content-Type: application/json"
0:8080/afa/api/v1/device/relocation?uuid=bd98c84e-f88c-42b4-
899c-9a7584a75951
```

Enable processes after relocation

By default, after relocating devices from a Remote Agent to a Central Manager, or between Remote Agents, some processes may be disabled on the Remote Agent, including monitoring, scheduled analysis, and syslog messaging. This topic describes APIs that enable you to enable these services again on a device after relocation.

Enable processes for a specific device

Enables monitoring, scheduled analysis, and syslog messaging on a specific device after relocation from a Remote Agent

Resource Name: `/api/v1/device/relocation/enableDevices`

Request Method: PUT

Request URL Parameters:

Element	Type	Description
treeNames *Mandatory*	String	One or more **treeNames** of devices on which you want to enable processes. Separate multiple values with commas.

Response:

Code	Description
200	Operation completed successfully
400	Bad request
401	Unauthorized

Request example

```
curl -X PUT "https://10.20.7.20/afa/api/v1/device/relocation/enableDevices" -H  "accept
```

Enable processes for all devices on a Remote Agent

Enables monitoring, scheduled analysis, and syslog messaging on all devices managed by a specific Remote Agent, after relocating from a different Remote Agent.

Resource Name:

`/api/v1/device/relocation/enableDevicesOnRemoteAgent`

Request Method: PUT

Request URL Parameters:

Element	Type	Description
node *Mandatory*	String	Name of the node on which you want to enable processes, as listed on the **Architecture** tab of the AFA**Administration** area.

Response:

Code	Description
200	Operation completed successfully
400	Bad request
401	Unauthorized

Request example:

```
curl -X PUT "https://10.20.7.20/afa/api/v1/device/relocation/enableDevicesOnRemoteAgent
```

Traffic simulation query

Performs a batch traffic simulation query on a single device or groups of devices.

Required permissions

To perform this request, you must have access to all the firewalls that are relevant for your query results path. Queries will fail if the query goes through a non-permitted device.

Users with permissions to view an entire group can run queries on the group. If you do not have permission to view a group of devices, or the **ALL_FIREWALLS** group, we recommend that you perform single-device queries on the devices you have permissions to view.

Resource Name: `/api/v1/query/`

Request Method: POST

Request URL Parameters:

Element	Type	Description
`QueryInput` *Mandatory*	List of `QueryRequestData` objects	Lists one or more queries to perform. See **QueryRequestData Type** table below.
`QueryTarget` *Mandatory*	String	Name of a device or group the query will run on. If empty, the query runs on the entire network and all permitted devices for the user.

QueryRequestData Type:

Element	Type	Description
`Source` *Mandatory*	List of strings	Source(s) for the query. Multiple values are separated by commas (,).
`Destination` *Mandatory*	List of strings	Destination(s) for the query. Multiple values are separated by commas (,).
`Service` *Mandatory*	List of strings	Service(s) for the query. Multiple values are separated by commas (,).
`User` *Optional*	List of strings	User(s) who created the rule. Multiple values are separated by commas (,).
`Application` *Optional*	List of strings	Application(s) for the rule. Multiple values are separated by commas (,).

Response:

A queryResponse JSON that includes a list of `QueryData` objects:

Element	Type	Description
`QueryDescription` *Mandatory*	String	Description of query.
`QueryHTMLPath` *Mandatory*	String	URL to the results in the UI.
`FIPResult` *Mandatory*	String	One of the following: • **Unreachable** • **SameZone** • **Routed** • **PartiallyRouted** • **NotExecuted** • **Unknown**
`QueryResult` *Mandatory*	String	One of the following: • **allowed** • **blocked** • **partially allowed** • **not routed**
`QueryItem` *Mandatory*	`QueryValueResults`	List of query value results. See **QueryValueResults** type below.

QueryValueResults:

Element	Type	Description
`Device` *Mandatory*	List of `DeviceResult` objects	List of device results. See **DeviceResult** type below.

DeviceResult:

Element	Type	Description
`IsAllowed` *Mandatory*	String	Status information and the number of rules that support it. For example: Allowed (x1), Blocked (x4), Partially allowed (x4).
`DeviceName` *Mandatory*	String	Display name of the device.
`Rules` *Mandatory*	List of QueryRules objects	List of rules. See **QueryRules** type below.

QueryRules:

Element	Type	Description
`Rule` *Optional*	String	Internal AlgoSec Rule ID. To retrieve the rule ID, call one of the rule APIs, such as `get_rules_by_device` or `search_rules`.
`Service` *Optional*	String	List of services.
`Source` *Optional*	String	List of sources.
`Source_Nat` *Optional*	String	List of NAT sources.
`Destination` *Optional*	String	List of destinations.
`Destination_Nat` *Optional*	String	List of NAT destinations.
`Install` *Optional*	String	List of installs.

Element	Type	Description
`Action` *Optional*	String	Action.
`ACL` *Optional*	String	ACL

Request example

```
curl -X POST "https://1.1.1.1/afa/api/v1/query" -H "accept: */*"
-H "Content-Type: application/json"
-d "{ \"queryInput\": [ { \"application\": [ \"string\" ],
\"businessApplicationsData\": [ { \"businessApplicationFlowId\": 0,
\"businessApplicationId\": 0, \"businessApplicationName\":
\"string\" } ], \"defaultValue\": [ \"string\" ],
\"destination\": [ \"string\" ], \"service\": [ \"string\" ],
\"source\": [ \"string\" ], \"user\": [ \"string\" ] } ],
\"queryTarget\": \"string\"}"
```

Response example

```
{
  "queryResult": [
    {
      "fipResult": "string",
      "queryDescription": "string",
      "queryHTMLPath": "string",
      "queryItem": [
        {
          "deviceName": "string",
          "displayName": "string",
          "isAllowed": "string"
        }
      ]
    }
  ],
  "queryUIResult": "string"
}
```

AFA data types

The following is a reference of AFA data types used in the AFA REST API:

- Action type
- AddObjectsToGroup type
- BaselineRequirementResult type
- BaselineRequirementTestResult type
- Create type
- Delete type
- EntitiesResponse type
- ExpectedDevice type
- ExpectedQueryDevice type
- Fields type
- FirstUnexpectedDevice type
- IssueAttributes type
- MergedRoutersData type
- MergedRoutersToMerge Type
- MessageDetails type
- MixedMergedRouters Type
- NatDetails type
- Interface Type
- Network Type
- ObjectChangeRequestDetails Type
- QueryNetworkObject Type
- QueryTroubleshootingInconsistencyCause Type
- QueryTroubleshootingPathItem Type
- QueryTroubleshootingScenario Type
- RemoveObjectsFromGroup type

- RiskyRules
- Stub Type
- SecurityZoneObject Type
- StubsToMerge Type
- TrafficChangeRequest type
- TrafficFieldDetails type
- TrafficItemDetails type
- TrafficLineDetails type
- Value Type

Action type

Element	Type	Description
`action`	String	One of the following: • create • delete • addObjectsToGroup • removeObjectsFromGroup • replaceContent
`devices`	Array of String	List of device ids. Example: "fw_ny_dc_01","fw_kmtc_02"
`lineOrder`	Integer	When executing multiple actions, the sequence number this action should be listed as. Example: 0,1,2,3...
`name`	String	The Display name of the Object being modified.

Element	Type	Description
`isGroup`	String	Whether the object is able to hold multiple values within it. Non-group objects may not be transformed into group objects, and group objects may not become non-group objects(though they may contain only 1 value). One of the following:: • True • False Example of a non-group object: host_1.1.1.1 Example of group object: ntp_servers
`objectContainers`	Array of Integer	List of object containers IDs.
`type`	String	The type of object. One of the following: • network • service
`values`	Array of String	List of values being added, removed, or placed. Example for Service Object: ["tcp/23","udp/53"] Example for Network Object: ["1.1.1.1","192.168.0.1/24"]

➔ See also:

- AFA data types

AddObjectsToGroup type

Element	Type	Description
`devices`	Array of String	List of devices.
`lineOrder`	Integer	Line order number.
`name`	String	Name of group.

`objectContainers`	Array of Integer	List of object container IDs.
`type`	String	One of the following: • network • service
`values`	Array of String	List of values.

➔ See also:

- AFA data types

BaselineRequirementResult type

Element	Type	Description
`id`	Integer	Requirement ID.
`name`	String	Requirement name.
`status`	`ComplianceCriteriaStatusEnum`	Status calculated from all the 'tests' results for this requirement. One of the following: • PASSED - If there is a PASSED test result for this requirement and all other test results are either PASSED or UNKNOWN. • FAILED - If there is a FAILED test result for this requirement. • UNKNOWN - If all test results for this requirement are UNKNOWN.
`tests`	Set of BaselineRequirementTestResult type objects	A set of baseline requirement test result objects.

➔ See also:

- AFA data types

BaselineRequirementTestResult type

Element	Type	Description
`id`	Integer	Requirement test ID.
`command`	String	Command of the requirement test.
`item`	String	Criterion of the requirement test.
`comments`	String	Comments of the requirement test, extra information from the result.
`status`	`ComplianceCriteriaStatusEnum`	Status of the requirement test. One of the following: • PASSED • FAILED • UNKNOWN

➔ See also:

- AFA data types

Create type

Element	Type	Description
`devices`	Array of String	List of devices.
`lineOrder`	Integer	Line order number.
`name`	String	
`objectContainers`	Array of Integer	List of object containers IDs.
`type`	String	One of the following: • network • service
`group`	Boolean	Whether device belongs to a group.

`isGroup`	Boolean	Whether this is a group.
`values`	Array of String	List of values.

➔ See also:

- AFA data types

Delete type

Element	Type	Description
devices	Array of String	List of devices to delete.
lineOrder	Integer	
name	String	
objectContainers	Array of Integer	List of object containers.
type	String	One of the following: • network • service

➔ See also:

- AFA data types

EntitiesResponse type

Element	Type	Description
`name`	String	The entity name.
`devices`	A list of strings.	A list of the display names of the devices. **Note:** This will be a list with only one item when the `entityType` is a single device.
`values`	A list of `values` objects.	A list of object information. See Value Type (see Value Type).

➔ See also:

- AFA data types

ExpectedDevice type

Element	Type	Description
`displayName`	String	Display name of expected device.
`ip`	String	IP address of expected device.

➔ See also:

- AFA data types

ExpectedQueryDevice type

Element	Type	Description
`displayName`*Mandatory*	String	Display name of device.
`ip`*Mandatory*	String	IP address of device.

➔ See also:

- AFA data types

Fields type

Element	Type	Description
`key`	String	Name of field.
`values`	Array of String	Values for field.

➔ See also:

- AFA data types

FirstUnexpectedDevice type

Element	Type	Description
`map`	String	ID of map with first unexpected device.
`ip`	String	IP address of first unexpected device.
`displayName`	String	Display name of first unexpected device.

➔ See also:

- AFA data types

IssueAttributes type

Element	Type	Description
`id`	Integer	The issue's unique ID.
`status`	String	The issue's status. One of the following: • **OPEN**. The issue is active. • **ACKNOWLEDGED**. The issue is acknowledged.
`lastFailure`	String	The date / time (UTC) of the last failure of the process.
`lastSuccess`	String	The date / time (UTC) of the last successful completion of the process. Null when the process has never succeeded.
`count`	Integer	The number or times the process failed.
`nodeType`	String	The effected server / appliance's role. One of the following: • **STANDALONE**. The ASMS server (Central Manager) in a single server environment. • **MASTER**. The Central Manager appliance in a distributed architecture. • **SLAVE**. A Load Unit appliance in a load distribution environment. • **REMOTE_MANAGER**. A Remote Agent appliance in a geographic distribution environment.

Element	Type	Description
`nodeName`	String	The name of the appliance.

Element	Type	Description
`issue`	Object	The details of the event. **`type`** The type of issue. One of the following: • **System** • **Device** **`failureType`** The type of failure. One of the following: • **Monitor** • **Analysis** • **Backup** • **Log Collection** • **Disk space** • **NAS Disk space** • **CPU** • **Memory** • **File descriptors** • **Audit logs** • **NAS** • **Cyber Ark** • **DFS** • **HA/DR** • **System Maintenance** • **Software Upgrade** **`description`** Description of the issue. **`remediation`** Information to solve the problem. **`kbLink`** A link to an AlgoPedia article which may help solve the problem.

Element	Type	Description
`device`	Object	The details of the relevant device. Null when the issue type is **System**. • `treeName`. The device's internal name. • `displayName`. The device's name in the Web Interface. • `brand`. The device's brand. • `workingFolder`. The device's working folder.

➔ See also:

- AFA data types

MergedRoutersData type

Parameter	Type	Description
`id`	Integer	ID of the merged router.
`name`	String	Name of the merged router.
`status`	String	Status of merged router: "MERGED".
`domain Id`	Integer	ID of the domain. Relevant only when domains are enabled. Default: **0**
`routersToMerge`	Array of IPData (see Network Type)	List of IPs for routers to merge.
`creationTime`	Integer	Date in system format.

➔ See also:

- AFA data types

MergedRoutersToMerge Type

Element	Type	Description
`name`	String	Name of the merged router.
`mergedRouterNames`	Array of String	List of names of merged routers to merge.

➔ See also:

- AFA data types

MessageDetails type

Element	Type	Description
`code`	String	Message code.
`message`	String	Message text.

➔ See also:

- AFA data types

MixedMergedRouters Type

Element	Type	Description
`name`	String	Name of merged router.
`routerIps`	Array of String	List of stub router IPs to add to merged router.
`mergedRoutersNames`	Array of String	List of merged routers to add to merged router (`name`).

➔ See also:

- AFA data types

NatDetails type

Element	Type	Description
destination	Array of String	List of destinations.
port	Array of String	List of ports.
source	Array of String	List of sources.
type	String	One of the following: • Static • Dynamic • None

➔ See also:

- AFA data types

Interface Type

Element	Type	Description
`hwName`	String	The interface's name.
`ip`	String	The interface's IP address.
`id`	String	The interface's ID.
`zoneType`	String	The zone's types.
`ipsBehindInterface`	A list of strings	The IP addresses behind the interface.

➔ See also:

- AFA data types

Network Type

Element	Type	Description
`id`	Integer	ID of IP detail.

Element	Type	Description
minIp	Integer	Minimum IP address.
maxIP	Integer	Maximum IP address.
display	String	IP display address.
displayRange	String	Range of IP display address.
optimalDisplay	List of String	List of IP addresses for optimal display.
singleIP	Boolean	Whether there is a single IP address.
cidr	Boolean	Whether IP is a CIDR address.
any	Boolean	Whether the IP is any type of address.

➔ See also:

- AFA data types

ObjectChangeRequestDetails Type

Element	Type	Description
attachments	Array of String	List of attachments.
cc	Array of String	CCs for Change Request.
description	String	Change Request description.
devices	Array of String	List of devices.
domain	String	Name of domain.
due	String	Date change is due.
expire	String	Date Change Request expires.
externalId	String	External ID.
owner	String	Name of owner.

Element	Type	Description
`priority`	String	Priority.
`referredBy`	Array of String	List of referrals.
`refersTo`	Array of String	List of refers to.
`requestedActions` *Mandatory*	Array of Action type	List of requested actions.
`requestor`	String	Name of requestor.
`subject`	String	Subject of request.
`template` *Mandatory*	String	Name of request template.
`customFields` *Mandatory*	Array of Fields type	List of custom field name and values.
`objectContainers` *Mandatory*	Array of Integer	List of object containers IDs.
`objectContainerLevel`	String	The device/management level on which to change the object. One of the following: ■ `highest`. To change the object at the highest level/management. **Note:** For Check Point devices, choosing highest will change the object on the CMA, not the PV1. ■ `lowest`. To change the object on the lowest level/individual device. ■ `automatic`. The level on which to change the object is determined based on an algorithm. [Default]

➔ See also:

- AFA data types

QueryNetworkObject Type

Element	Type	Description
`mapId`	String	Object ID in the AFA network map.
`id`	Integer	Object ID.
`type`	String	Type of the query network object. ■ SUBNET ■ DEVICE
`locationOnPath`	Integer	Position of the object on the map.
`displayName`	String	Display name, if any.
`ip`	Network (see Network Type)	IP details.
`empty`	Boolean	Whether the object is empty.

➔ See also:

- AFA data types

QueryTroubleshootingInconsistencyCause Type

Element	Type	Description
`ip`	String	IP address.
`dnsName`	String	DNS name.
`snmpName`	String	SNMP name, if any.

➔ See also:

- AFA data types

QueryTroubleshootingPathItem Type

Element	Type	Description
`mapId`	String	Device ID in the AFA network map.
`ip`	String	IP address of device.
`displayName`	String	Display name of device.

➔ See also:

- AFA data types

QueryTroubleshootingScenario Type

Element	Type	Description
`name`	String	Name of scenario. For example, "Reached_Wrong_Device".
`message`	String	Scenario message.
`recommendedSteps`	List of `RecommendedStep`	List of recommended steps to take: • `text` - String - Step to take, such as "Collect logs". • `action`- String - Target of step, such as "support", "portal".

➔ See also:

- AFA data types

RemoveObjectsFromGroup type

Element	Type	Description
devices	Array of String	List of devices.
lineOrder	Integer	Sequence
name	String	Name.

Element	Type	Description
objectContainters	Array of Integer	List of object container IDs.
type	String	One of the following: • network • service
values	Array of String	List of values.

➔ See also:

- AFA data types

RiskyRules

JSON Format

Element	Type	Description
device	String	Device name.
ruleid	String	ID of rule.
ruleNum	String	Rule number or name.
source	Array of String	List of names of hosts.
destination	Array of String	List of names of host.
application	Array of String	List of names of applications.
service	Array of String	List of names of services.
action	String	Rule action.
documentation	A Documentation Object	Each field in the object is the name of a documentation field and each field's value is the value of the documentation field.

Element	Type	Description
risks	Array of Risk Objects	Each risk object has the following fields: • risk code : String • severity : String • title : String
totalBySeverity	List of RuleSeverity	List of risk severity levels and the total number of rules at each level: • HIGH : Integer • SUSP_HIGH : Integer (Suspected high risks) • MEDIUM : Integer • LOW : Integer
trafficCount	Integer	Count of traffic meeting rule.

CSV Format

Element	Type	Description
Device	String	Device name.
Rule	String	Name of rule.
Id	String	ID of rule.
Source	String	Source.
Destination	String	Destination.
Application	String	Name of application.
Service	String	Name of service.
Action	String	Rule action.
Comment	String	Comment
Traffic count	String	Count of traffic meeting rule.
Documentation	String	Name of documentation fields.
High Risks	Integer	Number of rules at high risk level.

Element	Type	Description
Suspected High Risks	Integer	Number of rules at suspected high risk level.
Medium Risks	Integer	Number of rules at medium risk level.
Low Risks	Integer	Number of rules at low risk level.

➔ See also:

- AFA data types

Stub Type

Element	Type	Description
`id`	String	The router's ID.
`ip`	An `ip` object.	The router's IP address(es).
`closestDevices`	A list of `device` objects.	A list of devices that are defined in AFA that are closest to the router.
`missingInPaths`	Integer	The number of paths that are incomplete because the router is not defined in AFA.

➔ See also:

- AFA data types

SecurityZoneObject Type

Element	Type	Description
name	String	Name of network Security Zone.
addresses	Array of String	List of IP address ranges for the zone. For example: [10.21.0.2/24", "10.25.3.2/24"]

➔ See also:

- AFA data types

StubsToMerge Type

Element	Type	Description
`name`	String	Name of the merged router.
`routerIps`	Array of String	List of IPs to merge.

➔ See also:

- AFA data types

TrafficChangeRequest type

Element	Type	Description
template *Mandatory*	String	Name of template.
traffic *Mandatory*	Array of TrafficLineDetails	Traffic details.
fields *Mandatory*	Array of Fields type	Ticket fields.

➔ See also:

- AFA data types

TrafficFieldDetails type

Element	Type	Description
items	Array of TrafficItemDetails type	Traffic items.

➔ See also:

- AFA data types

TrafficItemDetails type

Element	Type	Description
customFields	Array of Fields type	List of custom fields.
name	String	

➔ See also:

- AFA data types

TrafficLineDetails type

Element	Type	Description
action	String	Action.
source	TrafficFieldDetails type	
destination	TrafficFieldDetails	
service	TrafficFieldDetails type	
application	TrafficFieldDetails type	
user	TrafficFieldDetails type	
customFields	Array of Fields type	
natDetails	NatDetails type	

➔ See also:

- AFA data types

Value Type

There is a value object type for network objects, and a value object type for service objects.

Value Type for Network Objects

Element	Type	Description
`name`	String	The network object name.
`ipaddresses`	A list of strings	A list of IP addresses contained in the object.

`ipType`	String	One of the following:
		`IPv6`
		`IPv4`

Value Type for Service Objects

Element	Type	Description
`id`	String	The id of the service object.
`name`	String	The name of the service object.
`serviceDefinitions`	A list of strings	A list of the services contained in each object (protocol and port).

➔ See also:

- AFA data types

AFA SOAP web services

AFA offers a SOAP API which allows you to integrate AFA functionality into external applications.

The AFA WSDL file

The AFA Web service's WSDL file is available at:

```
https://<algosec_server>/AFA/php/ws.php?wsdl
```

where <algosec_server> is the AFA/FireFlow server URL.

AFA SOAP method reference

The standard SOAP request envelope header for AFA is:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:afa="https://www.algosec.com/afa-ws">
<soapenv:Header/>
```

Note: The *entity name* is the display name for the device/group/matrix. The *entity ID* (tree name) is an internal representation of the device/group/matrix, usually the display name without non-alphanumeric characters or spaces.

The AFA SOAP interface supports the following methods:

AFA SOAP methods	Description
connect	Starting a Session **Note:** All other methods require a session ID which is obtained with the `connect` method.
is_session_alive	Verifying a Session is Active
disconnect	Ending a Session
get_configuration	Getting the Configuration
get_entity_name	Retrieving an Entity Name

AFA SOAP methods	Description
get_entity_id	Retrieving an Entity ID
create_device	Creating a Device
create_device_group	Creating a Device Group
add_device_to_group	Adding a Device to a Group
get_devices_list	Retrieving a List of all Devices
get_groups_list	Retrieving a List of all Groups
get_group_content	Retrieving a List of Devices Contained in a Group
device_changes_over_time_report	Device Changes Over Time
set_scheduler_job	Creating and Updating a Scheduler Job
delete_scheduler_job	Deleting a Scheduler Job
start_analysis	Starting an Analysis
query	Run traffic simulation queries
get_all_hostgroups	Retrieving a List of all Network Object Information
get_hostgroups_by_device	Retrieving a Device's Network Object Information
get_hostgroup_by_name_and_device	Retrieving a Network Object's Information
get_all_services	Retrieving a List of all Service Object Information
get_services_by_device	Retrieving a Device's Service Object Information
get_service_by_name_and_device	Retrieving a Service Object's Information
get_rules_by_device	Retrieving a List of a Device's Rules
search_rule	Searching for Rules
get_rule_documentation	Retrieving a Rule's Documentation

AFA SOAP methods	Description
edit_rule_documentation	Editing a Rule's Documentation
get_unused_rules	Retrieving a List of Unused Rules
risks_summary	Retrieving Risk Information for a Device
get_device_statistics	Retrieving Statistics for a Device
get_nat_discovery	Retrieving NAT Values for a Device or Group
get_report_pdf	Retrieving PDF of Report Page
set_configuration	Setting Configuration Parameters
importing_risks_from_spreadsheet	Import Risks from Spreadsheet
importing_risks_from_XML	Import Risks from XML File
create_role	Creating a New Role
delete_role	Deleting a Role
update_role	Updating a Role
create_user	Creating a New User
delete_user	Deleting a User
update_user	Updating a User
get_containing_objects	Retrieve containing objects
get_license	Retrieve license
get_parent_device	Retrieve parent device
search_object_by_IP	Search for object by IP

If the method's operation is successful, the method response returns data items or an indication of success. If the method's operation was not successful, the response

indicates that a SOAP fault has been thrown. For more details, see SOAP faults and SOAP fault list.

SOAP faults

The returned SOAP fault name is **connectError**.

The following are some of the possible additional SOAP faults:

- The user does not have the necessary permissions.
- The device is a group.

The following example is for a fault thrown when the user does not have permissions on the firewall.

```
<SOAP-ENV:Body>
   <SOAP-ENV:Fault>
      <faultcode>ns1:AFA-WS</faultcode>
      <faultstring>[710]  [device [fw3] is not in the list of permitted
devices]</faultstring>
      <faultactor>AFA Web Service</faultactor>
      <detail>
         <ns1:ErrorDetails>
            <code>710</code>
            <description>[710]  [device [fw3] is not in the list of
permitted
devices]</description>
         </ns1:ErrorDetails>
      </detail>
   </SOAP-ENV:Fault>
</SOAP-ENV:Body>
```

Managing the Session

The following methods control a Web Service session.

Starting a Session

The AFA SOAP API uses sessions to avoid re-authenticating with every request. You obtain a session key with the `connect` method. This session key is used in all other SOAP API requests.

Request Type: `ConnectRequest`

Element	Type	Description
`UserName` *Mandatory*	String	AFA username.
`Password` *Mandatory*	String	AFA password.
`Domain` *Optional*	String	Domain name. Relevant only when domains are enabled. Default: **0**
`ImpersonateUser` *Optional*	Sting	Username of the user you want to impersonate. The option to impersonate a user is only available for administrator users. The `UserName` and `Password` must be administrator credentials.

Response Type: `ConnectResponse`

Element	Type	Description
`SessionID` *Mandatory*	String	On success, returns the session ID. On failure, throws a standard SOAP fault.

Request example:

```
<ConnectRequest>
    <UserName>admin</UserName>
    <Password>admin_password</Password>
</ConnectRequest>
```

Response example:

```
<ConnectResponse>
    <SessionID>8cea15d11c4aa8eb338ce5c4a91e69ea</SessionID>
</ConnectResponse>
```

Verifying a Session is Active

To verify that your session has not timed out, use the `is_session_alive` method.

Request Type: `IsSessionAliveRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID received in `connect` request.

Response Type: `IsSessionAliveResponse`

Element	Type	Description
`IsSessionAliveResponse`	Integer	If the session is active, 1; otherwise, 0.

Request example:

```
<IsSessionAliveRequest>
    <SessionID>107220f9f300f936cf743ee29bea9d38</SessionID>
</IsSessionAliveRequest>
```

Response example:

```
<IsSessionAliveResponse>1</IsSessionAliveResponse>
```

Ending a Session

When a session is completed, you must terminate your session using the `disconnect` method.

Request Type: `DisconnectRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID received in `connect` request.

Response Type: `DisconnectResponse`

Element	Type	Description
`DisconnectResponse`	Integer	If the session was terminated successfully, 1; otherwise, 0.

Request example:

```
<DisconnectRequest>
    <SessionID>8cea15d11c4aa8eb338ce5c4a91e69ea</SessionID>
</DisconnectRequest>
```

Response example:

```
<DisconnectResponse>1</DisconnectResponse>
```

Getting the Configuration

The `get_configuration` method returns all the configuration parameters and their values. This includes the parameters in the following locations:

- **/home/afa/.fa/config**
- **/home/afa/.fa/machine_config**

Request Type: **`GetConfigurationRequest`**

Element	Type	Description
SessionID *Mandatory*	String	AFA session ID.

Response Type: **`GetConfigurationResponse`**

Element	Type	Description
`parameter`	List of KeyValue objects	List of key/value pairs for the configuration parameters. See KeyValue (see KeyValue type) type.

Request example:

```
<GetConfigurationRequest>
    <SessionID>107220f9f300f936cf743ee29bea9d38D</SessionID>
</GetConfigurationRequest>
```

Response example:

```
<GetConfigurationResponse>
```

```
    <parameter>
        <key>KEY1</key>
        <value>VAL1</value>
    </parameter>
    <parameter>
        <key>KEY2</key>
        <value>VAL2</value>
    </parameter>
    <parameter>
        <key>KEY2</key>
        <value>VAL2</value>
    </parameter>
    <parameter>
        <key>KEY1</key>
        <value>VAL1</value>
    </parameter>
    <!-- ... -->
    <parameter>
        <key>KEYN</key>
        <value>VALN</value>
    </parameter>
</GetConfigurationResponse>
```

Retrieving Device, Group, or Matrix Names and IDs

The following methods retrieve device, group, and matrix identification information.

Retrieving an Entity Name

The `get_entity_name` method returns the display name of a given group, device, or matrix entity ID.

Request Type: **`GetEntityNameRequest`**

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from the `connect` method.

Element	Type	Description
`EntityType` *Mandatory*	AfaNonEmptyString	Entity type. One of the following: ■ device ■ group ■ matrix
`EntityID` *Mandatory*	AfaNonEmptyString	Entity's tree name.

Response Type: **`GetEntityNameResponse`**

Element	Type	Description
`GetEntityNameResponse`	AfaNonEmptyString	On success, returns the entity's name. On failure, throws a SOAP Fault.

Retrieving an Entity ID

The `get_entity_id` method retrieves the entity ID of a given group, device, or matrix entity name.

Request Type: **`GetEntityIDRequest`**

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from `Connect` method.
`EntityType` *Mandatory*	AfaNonEmptyString	Entity type. One of the following: ■ device ■ group ■ matrix
`EntityName` *Mandatory*	AfaNonEmptyString	Entity's display name.

Response Type: **`GetEntityIDResponse`**

Element	Type	Description
`GetEntityIDResponse`	AfaNonEmptyString	On success, returns the entity's ID (tree name). On failure, throws a SOAP Fault.

Managing Devices and Groups

The following methods create and retrieve data for devices and device groups.

Creating a Device

The `create_device` method creates a device.

Request Type: `CreateDeviceRequest`

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from `connect` method.
`DeviceDetails` *Mandatory*	`NewDevice`	Details of device. See New Device Type (see NewDevice type).

Response Type: `CreateDeviceResponse`

Element	Type	Description
`Result`	AfaNonEmptyString	Result of method.

Request example:

```
<CreateDeviceRequest>
    <SessionID>d89d0cc1f0f9737133a0c53a31598c20</SessionID>
    <DeviceDetails>
        <Brand>ios</Brand>
        <HostName>Foo</HostName>
        <UserName>Bob</UserName>
        <Password>408KWl%8</Password>
        <ConnectionType>regular</ConnectionType>
    </DeviceDetails>
</:CreateDeviceRequest>
```

Response example:

```
<CreateDeviceResponse>
    <Result>1</Result>
</CreateDeviceResponse>
```

Creating a Device Group

The `create_device_group` method creates a device group in AFA from a list of devices.

Note: The group display name cannot contain non-alphanumeric characters or spaces. The tree name will be the same as the group display name.

Request Type: **`CreateDeviceGroupRequest`**

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from `Connect` method.
`GroupName` *Mandatory*	AfaNonEmptyString	The group display name. The group's display name will also be the group ID (tree name) for the device group. The group ID is created automatically.
`DeviceID` *Mandatory*	List of AfaNonEmptyString	List of device IDs included in the device group. Each deviceID must be unique.

Response Type: **`CreateDeviceGroupResponse`**

Element	Type	Description
`CreateDeviceGroupResponse`	AfaNonEmptyString	On success, returns the device group ID. On failure, throws a SOAP fault.

Request example:

```
<CreateDeviceGroupRequest>
    <SessionID>d67d8cc0f8f7525022a8c52a20486c18</SessionID>
    <GroupName>Foo</GroupName>
```

```
    <!--1 or more repetitions:-->
    <DeviceID>10_132_16_1</DeviceID>
</CreateDeviceGroupRequest>
```

Response example:

```
<CreateDeviceGroupResponse>Bar4</CreateDeviceGroupResponse>
```

Adding a Device to a Group

The `add_device_to_group` method adds a new device to an existing device group.

Request Type: `AddDeviceToGroupRequest`

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from `Connect` method.
`GroupID` *Mandatory*	AfaNonEmptyString	Device group ID (tree name) to which the new device is added.
`DeviceID` *Mandatory*	AfaNonEmptyString	Tree name (entity ID) of the device.

Response Type: `AddDeviceToGroupResponse`

Element	Type	Description
`AddeviceToGroupResponse`	AfaNonEmptyBoolean	On success, returns the device group ID. On failure, throws a SOAP fault.

Request example:

```
<AddDeviceToGroupRequest>
    <SessionID>d67d8cc0f8f7525022a8c52a20486c18</SessionID>
    <GroupID>Foo</GroupID>
    <DeviceID>m_10_132_31_1</DeviceID>
</AddDeviceToGroupRequest>
```

Response example:

```
<AddDeviceToGroupResponse>1</AddDeviceToGroupResponse>
```

Retrieving a List of all Devices

The `get_devices_list` method retrieves the list of all devices defined in AFA. For non-administrators, only the devices which the user has permission to view are returned.

Request Type: `GetDevicesListRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	SessionID obtained from `Connect` method.

Response Type: `GetDevicesListResponse`

Element	Type	Description
`Device`	List of `DeviceDataResult` objects	On success, returns a list of devices. See DeviceDataResult Type (see DeviceDataResult type). On failure, throws a SOAP fault.

Request example:

```
<GetDevicesListRequest>
    <SessionID>d67d8cc0f8f7525022a8c52a20486c18</SessionID>
</GetDevicesListRequest>
```

Response example:

```
<GetDevicesListResponse>
    <Device>
        <Brand>Cisco ASA</Brand>
        <EntityName>10.132.16.1</EntityName>
        <EntityID>10_132_16_1</EntityID>
        <IP>10.131.16.1</IP>
    </Device>
    <Device>
        <Brand>Check Point</Brand>
        <EntityName>Alon_Cluster</EntityName>
        <EntityID>m_10_132_31_1</EntityID>
```

```
        <IP>10.132.44.20</IP>
        <Policy>yaara_01.W</Policy>
    </Device>
    <Device>
        <Brand>Check Point</Brand>
        <EntityName>Dev_gw-R71</EntityName>
        <EntityID>Dev_gw_R71</EntityID>
        <IP>10.132.37.1</IP>
        <Policy>yaara_01.W</Policy>
    </Device>
</GetDevicesListResponse>
```

Retrieving a List of all Groups

The `get_groups_list` method retrieves a list of all groups defined in AFA. For non-administrators, only the groups which the user has permission to view are returned.

Request Type: **`GetGroupsListRequest`**

Element	Type	Description
`SessionID`*Mandatory*	String	SessionID obtained from `Connect` method.

Response Type: **`GetGroupsListResponse`**

Element	Type	Description
`Groups` *Mandatory*	`Groups`	List containing `GroupsID`. See Groups Type (see Groups type).

Request example:

```
<GetGroupsListRequest>
    <SessionID>74180e54d6023281d9bfcffd4e65f268</SessionID>
</afa:GetGroupsListRequest>
```

Response example:

```
<GetGroupsListResponse>
    <Groups>
        <GroupsID>Bar</GroupsID>
        <GroupsID>Bar3</GroupsID>
```

```
        <GroupsID>Foo</GroupsID>
    </Groups>
</GetGroupsListResponse>
```

Retrieving a List of Devices Contained in a Group

The `get_group_content` method retrieves a list of devices contained in a group.

Request Type: `GetGroupContentRequest`

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from `Connect` method.
`GroupID` *Mandatory*	String	Device group ID (tree name) of the group.

Response Type: `GetGroupContentResponse`

Element	Type	Description
`Device` *Mandatory*	List of `DeviceDataResult` objects	List of device data results. See DeviceDataResult Type (see DeviceDataResult type).

Request example:

```
<GetGroupContentRequest>
    <SessionID>74180e54d6023281d9bfcffd4e65f268</SessionID>
    <GroupID>Foo</GroupID>
</GetGroupContentRequest>
```

Response example:

```
<GetGroupContentResponse>
    <Device>
        <Brand>Cisco ASA</Brand>
        <DeviceName>10.132.16.1</DeviceName>
        <DeviceID>10_132_16_1</DeviceID>
    </Device>
    <Device>
        <Brand>Check Point</Brand>
        <DeviceName>Alon_Cluster</DeviceName>
        <DeviceID>Alon_Cluster</DeviceID>
```

```
    </Device>
    <Device>
        <Brand>Check Point</Brand>
        <DeviceName>fw3</DeviceName>
        <DeviceID>fw3</DeviceID>
    </Device>
    <Device>
        <Brand>Check Point</Brand>
        <DeviceName>Log_server_external</DeviceName>
        <DeviceID>Log_server_external</DeviceID>
    </Device>
</GetGroupContentResponse>
```

Device Changes Over Time

This enables you to generate a report for monitored changes in devices/groups over time, without logging into the AFA UI. This is mainly for 3rd party applications to store reports, send reports to other users, etc.

Request Type: **`device_changes_over_time_report`**

The web service input is:

Element	Type	Description
`SessionID` *Mandatory*	String	The Session ID.
`EntityID` *Mandatory*	String	Device or Group name.
`StartDate, EndDate`	String	Date ranges, using the format (yyyy-mm-dd).
Mandatory		
`IsLinkReturnType` *Mandatory*	String	Whether the output is linked to a pdf file (1) or pdf content encoded as a 64-based string (0).

Response Type:

The output is the PDF export of the report generated by AFA (as if the report was generated from the UI and exported) or the file is encoded in 64-bit format.

Request example:

```
<afa:ChangeOverTimeReportRequest>
          <SessionID>?</SessionID>
          <StartDate>?</StartDate>
          <EndDate>?</EndDate>
          <EntityID>?</EntityID>
          <IsLinkReturnType>?</IsLinkReturnType>
       </afa:ChangeOverTimeReportRequest>
```

Response example:

```
<ns1:ChangeOverTimeReportResponse>
          <Output>Link url </Output>
      </ns1:ChangeOverTimeReportResponse>
```

Deleting a device

The `delete_device` method deletes a device.

Request Type: `DeleteDeviceRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	SessionID obtained from `connect` method.
`DeviceID`*Mandatory*	String	Device ID.

Response Type: `DeleteDeviceResponse`

Element	Type	Description
`Result`	AfaNonEmptyString	Result of method.

Request example:

```
<DeleteDeviceRequest>
    <SessionID>d89d0cc1f0f9737133a0c53a31598c20</SessionID>
    <DeviceID>10_132_16_1</DeviceID>
</:DeleteDeviceRequest>
```

Response example:

```
<DeleteDeviceResponse>
    <Result>1</Result>
</DeleteDeviceResponse>
```

Create a domain via API

The `create_domain` method creates a new domain.

Request Type: **`CreateDomainRequest`**

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from `Connect` method.
`DomainName` *Mandatory*	AfaNonEmptyString	AFA domain name.
`Description` *Optional*	String	Description for the AFA domain.
`TemplateDomainSettings` *Optional*	`TemplateDomainSettingsType`	Specifies the template for the domain. See TemplateDomainSettings Type (see TemplateDomainSettings type).
`LicenseFirewallsQuota` *Optional*	Integer	Number of firewalls licensed in the domain. Minimum value is 0.
`LicenseRoutersQuota` *Optional*	Integer	Number of routers licensed in the domain. Minimum value is 0.
`LicenseExpirationDate` *Mandatory*	Date	Sets expiration date for domain. Date format is `YYYY-MM-DD`, `f`or example: 2014-10-23.

Element	Type	Description
`LicenseModule`*Optional*	List of AfaNonEmptyString	List specifying the modules licensed in the domain as defined below: ■ Risk: Licenses the risk and compliance capabilities for the domain. ■ Optimization: Licenses the policy optimization capabilities for the domain. ■ ActiveChange: Licenses ActiveChange capabilities for the domain. All global licenses that are licensed for the Provider Edition environment will automatically be licensed in the new domain. Global licenses include: ■ Core (Core AlgoSec capabilities) ■ FireFlow ■ AppViz

Response Type: `CreateDomainResponse`

Element	Type	Description
`CreateDomainResponse`	AfaBoolean	On success, returns 1. On failure, throws a SOAP fault, such as 0 - WS_ERR_OPERATION_FAILED.

Managing Analyses

The following methods manage AFA device, group, and matrix analyses.

Creating and Updating a Scheduler Job

The `set_scheduler_job` method creates a new, or updates a pre-existing scheduler job.

Request Type: `SetSchedulerJobRequest`

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from the `connect` method.
`JobName` *Mandatory*	AfaNonEmptyString	Name of the job to create or update.

`EntityType` *Mandatory*	AfaNonEmptyString	Entity the job is scheduled for. One of the following:
		`device`
		`group`
		`matrix`

`EntityID` *Mandatory*	AfaNonEmptyString	Tree name of the group/device/matrix.
`BaseAnalysisOnExistingReports` *Optional*	AfaBoolean	If True, aggregates all existing reports for the device/group/matrix. [Default] If False, generates new reports for each device/group/matrix.

Element	Type	Description
`Recurrence`*Mandatory*	String	Specifies how often the job is run. Options are: `daily` ■ `weekly`: Specify the day (s) to run the job in the `Weekday` parameter. ■ `upon_policy_inst`: Runs the job when the policy is installed. The entity type must be a single device.

`Weekday`*Optional*	List of AfaNonEmptyString	List of weekdays to schedule:
		`Monday`
		`Tuesday`
		`Wednesday`
		`Thursday`
		`Friday`
		`Saturday`
		`Sunday`

`Hour`*Optional*	Integer	Specifies the hour of day the job is run. Valid values are from `0` to `23`.
`Minute`*Optional*	Integer	Specifies the minute the job is run. Valid values are from `0` to `59`.

Response Type: `SetSchedulerJobResponse`

Element	Type	Description
`SetSchedulerJobResponse`	AfaBoolean	On success, returns 1. On failure, throws a SOAP fault, such as 0 - WS_ERR_OPERATION_FAILED.

Deleting a Scheduler Job

The `delete_scheduler_job` method deletes a Scheduler Job.

Request Type: `DeleteSchedulerJobRequest`

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from the `connect` method.
`JobName` *Mandatory*	AfaNonEmptyString	Name of the job to delete.

Response Type: `DeleteSchedulerJobResponse`

Element	Type	Description
`DeleteSchedulerJobResponse`	AfaBoolean	On success, returns 1. On failure, throws a SOAP fault, such as 0 - WS_ERR_OPERATION_FAILED.

Starting an Analysis

The `start_analysis` method begins a new analysis of a device, group, or matrix.

In order to run the `start_analysis` method, your must log in with permissions to start analysis.

Request Type: `StartAnalysisRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	SessionID obtained from the `Connect` method.

`EntityType`*Mandatory*	AfaNonEmptyString	Entity the job is scheduled for. One of the following:
		`device`
		`group`
		`matrix`

`EntityID`*Mandatory*	AfaNonEmptyString	Tree name of the group/device/matrix.
`RiskProfile`*Optional*	AfaNonEmptyString	Risk Profile name. When empty, the standard Risk Profile is used. **Note**: Although optional, we recommend you select a Risk Profile each time you perform an analysis.
`AvoidEmailNotification` *Optional*	AfaBoolean	If True, avoids sending out notifications and updates via email. [Default] If False, sends notifications and updates via email.

Element	Type	Description
`BaseAnalysisOnExistingReports` *Optional*	AfaBoolean	If True, aggregates all existing reports for the device/group/matrix. [Default] If False, generates a new report for the device/group/matrix. Analysis for a specific log date range or a What-if analysis is not available through the Web Service. To specify log dates or a What-if analysis, use the AFA Web Interface.

Response Type: `StartAnalysisResponse`

Element	Type	Description
`StartAnalysisResponse`	AfaBoolean	On success, returns 1. On failure, throws a SOAP fault, such as 0 - WS_ERR_OPERATION_FAILED.

Run traffic simulation queries

The **query** method performs a batch traffic simulation query on groups.

Tip: This request may take a long time to run. You may want to raise the value of the timeout configuration in your SOAPUI client.

Required permissions

To perform this request, you must have access to all the firewalls that are relevant for your query results path. Queries will fail if the query goes through a non-permitted device.

Users with permissions to view an entire group can run queries on the group. If you do not have permission to view a group of devices, or the **ALL_FIREWALLS** group, we recommend that you perform single-device queries on the devices you have permissions to view.

Request Type: QueryRequest

Element	Type	Description
SessionID *Mandatory*	String	Session ID obtained from the connect method.
QueryInput *Mandatory*	List of **QueryRequestData** objects	Describes one or more queries to perform. For details, see QueryRequestData type .
QueryTarget *Optional*	String	Name of a device or a group the query should run on. If empty, the query will run on the entire network and all permitted devices for the user.

Response Type: QueryResponse

Element	Type	Description
QueryResult	List of **QueryData** objects	Contains a **QueryResult** for each query. The **QueryResult** contains all query results and details. For details, see QueryData type .

Retrieving Network and Service Objects

The following methods retrieve information about network and service objects.

Retrieving a List of all Network Object Information

The `get_all_hostgroups` method retrieves a list of all network object information for every device defined in AFA.

Request Type: `GetAllHostGroupsRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.

Response Type: `GetAllHostGroupsResponse`

Element	Type	Description
HostGroup	List of `HostGroup` objects	List of host group information. See HostGroup Type (see HostGroup type).

Request example:

```
<GetAllHostGroupsRequest>
    <SessionID>tbuumksnrvj8mqslos2gfhrdl2</SessionID>
</GetAllHostGroupsRequest>
```

Response example:

```
<GetAllHostGroupsResponse>
    <HostGroup>
        <EntityID>m_10_132_31_1</EntityID>
        <Name>gg_10.131.32.11-13-43</Name>
        <CanonizedName>gg_10.131.32.11-13-43</CanonizedName>
        <IP>
            <xsd:string>10.131.32.11-10.131.32.13</xsd:string>
            <xsd:string>10.131.32.15</xsd:string>
            <xsd:string>10.131.32.43</xsd:string>
         </IP>
         <ClassName>network_object_group</ClassName>
         <Members>
            <xsd:string>a_10.131.32.43</xsd:string>
            <xsd:string>a_10.131.32.15</xsd:string>
            <xsd:string>aa_10.131.32.12-13</xsd:string>
            <xsd:string>aa_10.131.32.11</xsd:string>
         </Members>
    </HostGroup>
    <HostGroup>
        <EntityID>m_10_132_31_1</EntityID>
        <Name>a_10.131.23.14</Name>
        <CanonizedName>a_10.131.23.14</CanonizedName>
        <IP>
            <xsd:string>10.131.23.14</xsd:string>
```

```
        </IP>
        <ClassName>host_plain</ClassName>
        <Members>
            <xsd:string/>
        </Members>
    </HostGroup>
</GetAllHostGroupsResponse>
```

Retrieving a Device's Network Object Information

The `get_hostgroups_by_device` method retrieves a list of a device's network object information.

Request Type: `GetHostGroupsRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
`EntityID`*Mandatory*	String	Entity ID of the device.

Response Type: `GetHostGroupsResponse`

Element	Type	Description
HostGroup	List of `HostGroup` objects	List of host groups. See HostGroupType (see HostGroup type).

Request example:

```
<GetHostGroupsRequest>
    <SessionID>tbuumksnrvj8mqslos2gfhrdl2</SessionID>
    <EntityID>m_10_132_31_1</EntityID>
</GetHostGroupsRequest>
```

Response example:

```
<GetHostGroupsResponse>
    <HostGroup>
        <EntityID>m_10_132_31_1</EntityID>
        <Name>gg_10.131.32.11-13-43</OriginalName>
        <CanonizedName>gg_10.131.32.11-13-43</CanonizedName>
```

```
        <IP>
            <xsd:string>10.131.32.11-10.131.32.13</xsd:string>
            <xsd:string>10.131.32.15</xsd:string>
            <xsd:string>10.131.32.43</xsd:string>
        </IP>
        <ClassName>network_object_group</ClassName>
        <Members>
            <xsd:string>a_10.131.32.43</xsd:string>
            <xsd:string>a_10.131.32.15</xsd:string>
            <xsd:string>aa_10.131.32.12-13</xsd:string>
            <xsd:string>aa_10.131.32.11</xsd:string>
        </Members>
    </HostGroup>
    <HostGroup>
        <EntityID>m_10_132_31_1</EntityID>
        <Name>a_10.131.23.14</OriginalName>
        <CanonizedName>a_10.131.23.14</CanonizedName>
        <IP>
            <xsd:string>10.131.23.14</xsd:string>
        </IP>
        <ClassName>host_plain</ClassName>
        <Members>
            <xsd:string/>
        </Members>
    </HostGroup>
</GetHostGroupsResponse>
```

Retrieving a Network Object's Information

The `get_hostgroup_by_name_and_device` method retrieves information about a a specific network object, given its name and the device it is defined on.

Request Type: **`GetHostGroupNameDeviceRequest`**

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
`EntityID`*Mandatory*	String	Entity ID of the device.
`HostGroupName`*Mandatory*	String	Original name of the host group.

Response Type: **`GetHostGroupNameDeviceResponse`**

Element	Type	Description
`HostGroup` *Mandatory*	A `HostGroup` object	Host group information. See HostGroup Type (see HostGroup type).

Request example:

```
<GetHostGroupNameDeviceRequest>
    <SessionID>tbuumksnrvj8mqslos2gfhrdl2</SessionID>
    <EntityID>m_10_132_31_1</EntityID>
    <HostGroupName>EW1662d11345</HostGroupName>
</GetHostGroupNameDeviceRequest>
```

Response example:

```
<GetHostGroupNameDeviceResponse>
    <HostGroup>
        <EntityID>m_10_132_31_1</EntityID>
        <HostGroupName>EW1662d11345</HostGroupName>
        <CanonizedName>EW1662d11345</CanonizedName>
        <IP>
            <xsd:string>10.131.32.35</xsd:string>
        </IP>
        <ClassName>host_plain</ClassName>
        <Members>
            <xsd:string/>
        </Members>
    </HostGroup>
</GetHostGroupNameDeviceResponse>
```

Retrieving a List of all Service Object Information

The `get_all_services` method retrieves a list of all service object information for every device defined in AFA.

Request Type: **`GetAllServicesRequest`**

Element	Type	Description
`SessionID` *Mandatory*	String	Session ID obtained from the `connect` method.

Response Type: **`GetAllServicesResponse`**

Element	Type	Description
`Service`	List of `ServiceInfo` objects	Service information. See ServiceInfo Type (see ServiceInfo type).

Request example:

```
<GetAllServicesRequest>
    <SessionID>c25uvd7g58qv0a1r1ht65ep1j0</SessionID>
</GetAllServicesRequest>
```

Response example:

```
<GetAllServicesResponse>
    <Service>
        <EntityID>Alon_Cluster</EntityID>
        <Name>microsoft_rpc_http</Name>
        <Ports>
            <Port>TCP/593</Port>
        </Ports>
    </Service>
    <Service>
        <EntityID>Alon_Cluster</EntityID>
        <Name>Microsoft_services</Name>
        <Ports>
            <Port>UDP/138</Port>
            <Port>UDP/137</Port>
        </Ports>
    </Service>
    <Service>
        <EntityID>Alon_Cluster</EntityID>
        <Name>Microsoft_services</Name>
        <Ports>
            <Port>TCP/139</Port>
            <Port>TCP/445</Port>
            <Port>TCP/135</Port>
            <Port>TCP/593</Port>
        </Ports>
    </Service>
</GetAllServicesResponse>
```

Retrieving a Device's Service Object Information

The `get_services_by_device` method retrieves a list of a device's service object information.

Request Type: `GetServicesDeviceRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
`DeviceID`*Mandatory*	String	Tree name of the device.

Response Type: `GetServicesDeviceResponse`

Element	Type	Description
Service	List of `ServiceInfo` objects	List of service information. See ServiceInfo Type (see ServiceInfo type).

Request example:

```
<GetServicesDeviceRequest>
    <SessionID>c25uvd7g58qv0a1r1ht65ep1j0</SessionID>
    <DeviceID>10_132_20_1_root</DeviceID>
</GetServicesDeviceRequest>
```

Response example:

```
<GetServicesDeviceResponse>
    <Service>
        <DeviceID>10_132_20_1_root</DeviceID>
        <Name>AFS3</Name>
        <Ports>
            <Port>UDP/7000-7009</Port>
        </Ports>
    </Service>
    <Service>
        <DeviceID>10_132_20_1_root</DeviceID>
        <Name>AH</Name>
        <Ports>
            <Port>51/0-65535</Port>
        </Ports>
```

```
    </Service>
    <Service>
        <DeviceID>10_132_20_1_root</DeviceID>
        <Name>Algosec_Client_IM_ports_allowed</Name>
        <Ports>
            <Port>TCP/1863</Port>
            <Port>TCP/5190</Port>
            <Port>TCP/5222</Port>
        </Ports>
    </Service>
</GetServicesDeviceResponse>
```

Retrieving a Service Object's Information

The `get_service_by_name_and_device` method retrieves information about a a specific service object, given its name and the device it is defined on.

Request Type: **`GetServiceNameDeviceRequest`**

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
`DeviceID`*Mandatory*	String	Tree name of the device.
`Name`*Mandatory*	String	Name of the service.

Response Type: **`GetServiceNameDeviceResponse`**

Element	Type	Description
Service	List of `ServiceInfo` objects	List of service information. See ServiceInfo Type (see ServiceInfo type).

Request example:

```
<GetServicesNameDeviceRequest>
    <SessionID>c25uvd7g58qv0a1r1ht65ep1j0</SessionID>
    <DeviceID>10_132_20_1_root</DeviceID>
    <Name>AFS3</Name>
</GetServicesNameDeviceRequest>
```

Response example:

```
<ns1:GetServiceNameDeviceResponse>
    <Service>
        <DeviceID>10_132_20_1_root</DeviceID>
        <Name>AFS3</Name>
        <Ports>
            <Port>TCP/7000-7009</Port>
        </Ports>
    </Service>
    <Service>
        <DeviceID>10_132_20_1_root</DeviceID>
        <Name>AFS3</Name>
        <Ports>
            <Port>UDP/7000-7009</Port>
        </Ports>
    </Service>
</GetServiceNameDeviceResponse>
```

Managing Rules

The following methods search, retrieve, and edit rules.

Retrieving a List of a Device's Rules

The **get_rules_by_device** method retrieves a list of rules for a device.

Note: The list of parameters in the rules element depends on the device.

Request Type: GetRulesByDeviceRequest

Element	Type	Description
SessionID Mandatory	String	SessionID returned by connect method.
DeviceID Mandatory	String	Tree name of the device.

Response Type: GetRulesByDeviceResponse

Element	Type	Description
Rules	Rules	Returned rules for device. For details, see Rules type . **Note:** The response includes **RuleID**, which is a request parameter in **get_rule_documentation**. For details, see Retrieving a Rule's Documentation.

Request example 1:

```
<GetRulesByDeviceRequest>
    <SessionID>djiid120v5kge1quf01s6p5r11</SessionID>
    <DeviceID>10_132_16_1</DeviceID>
</GetRulesByDeviceRequest>
```

Response example 1:

```
<GetRulesByDeviceResponse>
    <Rules>
        <Rule>
            <RuleID>acl(247)</RuleID>
            <Name>dmz_access_in(1)</Name>
            <Source>10.134.191.1</Source>
            <Destination>any</Destination>
            <Action>permit</Action>
            <Enable>disabled</Enable>
            <Service>icmp/echo</Service>
            <ACL>dmz_access_in</ACL>
            <Interface>dmz</Interface>
            <LineNum>247</LineNum>
            <Internal_Name>dmz_access_in(2)</Internal_Name>
            <UID>oBr68ezuOqr3BLIsq1AwXw</UID>
            <Line>access-list dmz_access_in extended permit icmp host
10.134.191.1 any echo inactive</Line>
        </Rule>
        <Rule>
            <RuleID>acl(249)</RuleID>
            <Name>dmz_access_in(2)</Name>
            <Source>192.168.3.80</Source>
            <Destination>any</Destination>
            <Action>permit</Action>
            <Enable>disabled</Enable>
```

```
            <Service>tcp/talk</Service>
            <ACL>dmz_access_in</ACL>
            <Interface>dmz</Interface>
            <LineNum>249</LineNum>
            <Internal_Name>dmz_access_in(4)</Internal_Name>
            <UID>RzHkFIr5kdsZ+gWbfDtc+Q</UID>
            <Line>access-list dmz_access_in extended permit tcp host
192.168.3.80 any eq talk inactive</Line>
        </Rule>
        <Rule>
            <RuleID>acl(251)</RuleID>
            <Name>dmz_access_in(3)</Name>
            <Source>any</Source>
            <Destination>192.168.3.184</Destination>
            <Action>permit</Action>
            <Enable>disabled</Enable>
            <Service>tcp/http</Service>
            <ACL>dmz_access_in</ACL>
            <Interface>dmz</Interface>
            <LineNum>251</LineNum>
            <Internal_Name>dmz_access_in(6)</Internal_Name>
            <UID>0ef41BscLmJC37JSv8EWfQ</UID>
            <Line>access-list dmz_access_in extended permit tcp any host
192.168.3.184 eq www inactive</Line>
        </Rule>
    </Rules>
</GetRulesByDeviceResponse>
```

Request example 2:

```
<GetRulesByDeviceRequest>
    <SessionID>djiid120v5kge1quf01s6p5r11</SessionID>
    <DeviceID>p_10_132_30_1</DeviceID>
</GetRulesByDeviceRequest>
```

Response example 2:

```
<ns1:GetRulesByDeviceResponse>
    <Rules>
        <Rule>
            <RuleNum>1</RuleNum>
            <RuleID>086D5DE5-D0F0-4EDA-BF1F-B345F7E73725</RuleID>
```

```
            <Source>afa-amichai</Source>
            <Destination>Any</Destination>
            <Services>Any</Services>
            <Action>accept</Action>
            <Enable>disabled</Enable>
            <Track>None</Track>
            <Time>Any</Time>
            <Install>Any</Install>
            <Global>before</Global>
            <Comments>comment 3</Comments>
        </Rule>
        <Rule>
            <RuleNum>2</RuleNum>
            <RuleID>DB9519FB-2FC4-430A-BD9E-0D4D68552641</RuleID>
            <Name>allow amichai's ssh</Name>
            <Source>amichai-pc</Source>
            <Destination>LocalMachine</Destination>
            <Services>gssh_version_2</Services>
            <Action>accept</Action>
            <Enable>disabled</Enable>
            <Track>None</Track>
            <Time>Any</Time>
            <Install>Any</Install>
            <Global>before</Global>
            <Comments>for log collection</Comments>
        </Rule>
        <Rule>
            <RuleNum>18</RuleNum>
            <RuleID>6343F5EE-29B2-42E1-B4B2-F4C3D634A881</RuleID>
            <Source>Any</Source>
            <Destination>Any</Destination>
            <Services>Any</Services>
            <Action>drop</Action>
            <Enable>enabled</Enable>
            <Track>None</Track>
            <Time>Any</Time>
            <Install>Any</Install>
            <Global>after</Global>
        </Rule>
    </Rules>
</GetRulesByDeviceResponse>
```

Searching for Rules

The **search_rule** method searches for rules.

Request Type: SearchRuleRequest

Element	Type	Description
SessionID Mandatory	String	Session ID obtained from the **connect** method.
EntityID Optional	String	ID of the entity to search. If not provided, search is for all devices.
EntityType Optional	String	Entity type to search for. If not provided, search is for all devices. Possible values include: • **device** • **group** • **matrix**
SearchFor Mandatory	SearchParam	Criteria to search for. For details, see SearchParam type.

Response Type: SearchRuleResponse

Element	Type	Description
Rules Mandatory	List of Rule objects	Returned rules. For details, see Rules type . **Note:** The response includes RuleID, which is a request parameter in **get_rule_documentation**. For details, see Retrieving a Rule's Documentation.

Request example 1:

```
<SearchRuleRequest>
    <SessionID>366a6ae034ce7a4357f6f66fad629018</SessionID>
    <EntityID>10_132_16_1</EntityID>
    <!--1 or more repetitions:-->
    <SearchFor>
```

```
        <Search>10.134</Search>
    </SearchFor>
</SearchRuleRequest>
```

Response example 1:

```
<SearchRuleResponse>
    <Rules>
        <Rule>
            <RuleID>acl(247)</RuleID>
            <Name>dmz_access_in(1)</Name>
            <Source>10.134.191.1</Source>
            <Destination>any</Destination>
            <Action>permit</Action>
            <Enable>disabled</Enable>
            <Service>Array</Service>
            <ACL>dmz_access_in</ACL>
            <Interface>dmz</Interface>
            <LineNum>247</LineNum>
            <Internal_Name>dmz_access_in(2)</Internal_Name>
            <UID>oBr68ezuOqr3BLIsq1AwXw</UID>
            <Line>access-list dmz_access_in extended permit icmp host
10.134.191.1 any echo inactive</Line>
        </Rule>
        <Rule>
            <RuleID>acl(285)</RuleID>
            <Name>inside_access_in(8)</Name>
            <Source>dmz-network/24</Source>
            <Destination>10.134.14.0/24</Destination>
            <Action>permit</Action>
            <Enable>enabled</Enable>
            <Service>Array</Service>
            <Comment>amichai's rule</Comment>
            <ACL>inside_access_in</ACL>
            <Interface>inside</Interface>
            <LineNum>285</LineNum>
            <Internal_Name>inside_access_in(11)</Internal_Name>
            <UID>0xf5cb4128</UID>
            <Line>access-list inside_access_in extended permit tcp
10.136.16.0 255.255.255.0 10.134.14.0 255.255.255.0 eq aol log</Line>
        </Rule>
    </Rules>
</SearchRuleResponse>
```

Request example 2:

```
<SearchRuleRequest>
    <SessionID>366a6ae034ce7a4357f6f66fad629018</SessionID>
    <EntityID>10_132_16_1</EntityID>
    <!--1 or more repetitions:-->
    <SearchFor>
         <Search>10.132</Search>
         <Field>Destination</Field>
    </SearchFor>
</SearchRuleRequest>
```

Response example 2:

```
<SearchRuleResponse>
    <Rules>
        <Rule>
            <RuleID>acl(247)</RuleID>
            <Name>dmz_access_in(1)</Name>
            <Source>10.134.191.1</Source>
            <Destination>any</Destination>
            <Action>permit</Action>
            <Enable>disabled</Enable>
            <Service>Array</Service>
            <ACL>dmz_access_in</ACL>
            <Interface>dmz</Interface>
            <LineNum>247</LineNum>
            <Internal_Name>dmz_access_in(2)</Internal_Name>
            <UID>oBr68ezuOqr3BLIsq1AwXw</UID>
            <Line>access-list dmz_access_in extended permit icmp host
10.134.191.1 any echo inactive</Line>
        </Rule>
        <Rule>
            <RuleID>acl(285)</RuleID>
            <Name>inside_access_in(8)</Name>
            <Source>dmz-network/24</Source>
            <Destination>10.134.14.0/24</Destination>
            <Action>permit</Action>
            <Enable>enabled</Enable>
            <Service>Array</Service>
            <Comment>amichai's rule</Comment>
            <ACL>inside_access_in</ACL>
            <Interface>inside</Interface>
```

```
            <LineNum>285</LineNum>
            <Internal_Name>inside_access_in(11)</Internal_Name>
            <UID>0xf5cb4128</UID>
            <Line>access-list inside_access_in extended permit tcp
10.136.16.0 255.255.255.0 10.134.14.0 255.255.255.0 eq aol log</Line>
            </Rule>
         </Rules>
</SearchRuleResponse>
```

Retrieving a Rule's Documentation

The **get_rule_documentation** method retrieves data from a specified column.

Request Type: GetRuleDocumentationRequest

Element	Type	Description
SessionID Mandatory	String	SessionID obtained from the **connect** method.
DeviceID Mandatory	String	Tree name of the device.
RuleUid Mandatory	String	Internal AlgoSec Rule ID. To retrieve the rule ID, call one of the rule APIs, such as **get_rules_by_device** or **search_rule**. For details, see Retrieving a List of a Device's Rules or Searching for Rules.
DocumentationColumn Mandatory	String	The name of the column from which you want to retrieve data. **Note:** By default, AFA adds a field called **Documentation** to each device policy. For information on adding other columns, see Customizing Device Policy Documentation Fields.

Response Type: GetRuleDocumentationResponse

Element	Type	Description
GetRuleDocumentationResponse	String	The content in the specified column.

Editing a Rule's Documentation

The edit_rule_documentation method edits data in a specified column.

Request Type: EditRuleDocumentationRequest

Element	Type	Description
SessionID Mandatory	String	SessionID obtained from the **connect** method.
DeviceID Mandatory	String	Tree name of the device.
RuleUid Mandatory	String	Rule ID. To get the rule ID, call one of the rule APIs, such as **get_rules_by_device**. For details, see Retrieving a List of a Device's Rules.
DocumentationColumn Mandatory	String	Name of the column you want to edit. **Note:** By default, AFA adds a field called **Documentation** to each device policy. For information on adding other columns, see Customizing Device Policy Documentation Fields.
DocumentationData Mandatory	String	Content to put in the specified column. Existing data will be overwritten.

Response Type: EditRuleDocumentationResponse

Element	Type	Description
EditRuleDocumentationResponse	Integer	On success, returns **1**. On failure, returns **0**.

Retrieving a List of Unused Rules

The **get_unused_rules** method retrieves the list of unused rules detected in the last successful report of a device or a group of devices.

Request Type: GetRulesByDeviceRequest

Element	Type	Description
SessionID Mandatory	String	SessionID returned by **connect** method.
EntityID Mandatory	String	Tree name of the device.
EntityType Mandatory	String	Device, group, or matrix.

Response Type: GetRulesByDeviceResponse

Element	Type	Description
Rules	Rules	Returns unused rules of the given EntityID based on its last report.

Request example 1:

```
<GetUnusedRulesRequest>
    <SessionID>49a6ce6f7341b340edefae630b8b25a1</SessionID>
    <EntityID>Humus</EntityID>

    <EntityType>Device</EntityType>
</GetUnusedRulesRequest>
```

Response example 1:

```
<GetUnusedRulesResponse>
    <Rules>
        <Rule>
            <DeviceID>Humus</DeviceID>
            <Report>afa-754</Report>
            <Analyzed_On>2016-05-29 14:29:22</Analyzed_On>
            <RuleID>2FBCB893-1F26-2343-BOAE-BD1371D27C2A</RuleID>
            <RuleNum>33</RuleNum>
            <Source>a_10.10.18.95</Source>

            <Destination>ip=10.30.18.95</Destination>
            <Service>udp-16994</Service>
            <Action>accept</Action>
            <Enable>enabled</Enable>
            <Time>Any</Time>
```

```
            <Section_Header>Default rule</Section_Header>
            <Global>middle</Global>
            <Log>Log</Log>
            <Comment>4180</Comment>
            <Install>Humus</Install>
            <LastUse>N/A<LastUse>
        <Rule>
     <Rules>
</GetUnusedRulesResponse>
```

Request example 2:

```
<GetUnusedRulesRequest>
    <SessionID>e4a1edb6f40ff69cbe021123077b</SessionID>
    <EntityID>Humus</EntityID>
    <EntityType>Device</EntityType>
</GetUnusedRulesRequest>
```

Response example 2:

```
<Fault>
    <faultcode>ns1:AFA-WS</faultcode>
    <faultstring>[505] [You are not permitted to perform this operation.]
    <faultactor>AFA Web Service</faultactor>
    <detail>
       <ns1:ErrorDetails>
          <code>505</code>
          <description>[505] [You are not permitted to perform this
operation.]
       </ns1:ErrorDetails>
    </detail>
<Fault>
```

Request example 3:

```
<GetUnusedRulesRequest>
    <SessionID>1a3cfbf7e4f82f309d9893dc2b6fb932</SessionID>
    <EntityID>Humus</EntityID>
    <EntityType>Device</EntityType>
</GetUnusedRulesRequest>
```

Response example 3:

```
<GetUnusedRulesResponse>
   <Rules/>
</GetUnusedRulesResponse>
```

Retrieving Data for a Device or Group

The following methods retrieve device or group information.

Retrieving Risk Information for a Device

The `risks_summary` method retrieves risk statistics for a device. It does not support retrieving group or matrix risk statistics.

Request Type: `RisksSummaryRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	SessionID obtained from the `connect` method.
`DeviceID`*Mandatory*	String	Tree name of the device.

Response Type: `RisksSummaryResponse`

Element	Type	Description
`Date`	String	The date and time the web service was activated. The format is `YYYY-MM-DD HH:MM:SS`.
`High`	String	High risk.

Element	Type	Description
`Suspected_high`	String	Suspected high risk.
`Medium`	String	Medium risk.
`Low`	String	Low risk.
`Security_Rating`	String	Security rating.

Request example:

```
<RisksSummaryRequest>
    <SessionID>a78cc74a80b70efe253f44daad620fb7</SessionID>
    <DeviceID>p_10_132_30_1</DeviceID>
</RisksSummaryRequest>
```

Response example:

```
<RisksSummaryResponse>
    <Date>2013-05-20 15:42:44</Date>
    <High>0</High>
    <Suspected_high>0</Suspected_high>
    <Medium>3</Medium>
    <Low>1</Low>
    <Security_Rating>97</Security_Rating>
</RisksSummaryResponse>
```

Retrieving Statistics for a Device

The `get_device_statistics` method retrieves statistics for a device.

For a list of possible statistics for a device, see StatsData Type (see StatsData type).

Request Type: `GetDeviceStatisticsRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	SessionID obtained from the `connect` method.
`DeviceID`*Mandatory*	String	Tree name of the device for which to retrieve statistics.

Response Type: `GetDeviceStatisticsResponse`

Element	Type	Description
`Statistics`	List of `StatsData` objects	List of statistical data. See StatsData Type (see StatsData type).

Request example:

```
<GetDeviceStatisticsRequest>
    <SessionID>a78cc74a80b70efe253f44daad620fb7</SessionID>
    <DeviceID>p_10_132_30_1</DeviceID>
</GetDeviceStatisticsRequest>
```

Response example:

```
<GetDeviceStatisticsResponse>
    <Statistics>
        <StatType>simple_count</StatType>
        <StatName>unused_rules</StatName>
        <StatValue/>
    </Statistics>
    <Statistics>
        <StatType>compliance_undef</StatType>
        <StatName>PCI</StatName>
        <StatValue>17</StatValue>
    </Statistics>
    <Statistics>
        <StatType>risk_level</StatType>
        <StatName>highest</StatName>
        <StatValue>1</StatValue>
    </Statistics>
</GetDeviceStatisticsResponse>
```

Retrieving NAT Values for a Device or Group

The `get_nat_discovery` method receives an IP address as an input and retrieves all the potential translations to and/or from it performed by the selected device or device group.

Request Type: `GetNatDiscoveryRequest`

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from the `connect` method.
`EntityName` *Optional*	String	Tree name of the device or group for which to retrieve NAT values. Default is all the devices (`ALL_FIREWALLS`).
`IPAddress` *Optional*	String	IP address of device/group. Default is all definitions.
`PreNat` *Optional*	Integer	To retrieve addresses this IP is translated to 1; otherwise, 0. Default is 1.
`PostNat` *Optional*	Integer	To retrieve addresses that are translated to this IP address, 1; otherwise, 0. Default is 1.
`Source` *Optional*	Integer	To retrieve source address translations, 1; otherwise, 0. Default is 1.
`Destination` *Optional*	Integer	To retrieve destination address translation, 1; otherwise, 0. Default is 1.

Response Type: `GetNatDiscoveryResponse`

Element	Type	Description
`SourceNat/ DestinationNat`	List of `NatResult` objects	List of source and/or destination NatResult information. See NatResult Type (see NatResult type).

Request example:

```
<GetNatDiscoveryRequest>
    <SessionID>d5b1c34a1696a06321523e588b82cdd0</SessionID>
    <EntityName>rose</EntityName>

    <!--1 or more repetitions:-->

    <IpAddress>16.47.59.14</IpAddress>

    <PreNat>1</PreNat>

    <PostNat>1</PostNat>

    <Source>1</Source>
```

```
    <Destination>1</Destination>
</GetNatDiscoveryRequest>
```

Response example:

```
<GetNatDiscoveryResponse>
    <SourceNat>
        <NatResult>
            <DeviceName>rose</DeviceName>
            <PreNat>10.1.20.3</PreNat>
            <PostNat>16.47.59.14</PostNat>
            <Type>Static</Type>
        </NatResult/>
    </SourceNat>
    <DestinationNat>
        <NatResult>
            <DeviceName>rose</DeviceName>
            <PreNat>16.47.59.14</PreNat>
            <PostNat>10.1.20.3</PostNat>
            <Type>Static</Type>
        </NatResult/>
    </DestinationNat>
</GetNatDiscoveryResponse>
```

Retrieving PDF of Report Page

The `get_report_pdf` method retrieves a PDF copy of a report page for a device or group.

Request Type: **`GetReportPdfRequest`**

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from the `connect` method.

Element	Type	Description
`EntityID` *Mandatory*	String	Tree name of the device/group.
`EntityType` *Mandatory*	String	Entity type. One of the following: ■ device ■ group ■ matrix
`ReportPage` *Mandatory*	String	Name of report page. See the list of report page names below. **Note:** Not all devices contain all these pages. To confirm which pages a device's report contains, open a sample report in the AFA Web Interface **Note:** Each report page must be requested individually.

Report Page Names
• home • policy • policy.rules • policy.hostgroups • changes • risks • risky-rules • custom-report • vpn • baseline-compliance • regulatory-compliance • regulatory-compliance.pci • regulatory-compliance.nist_800-53 • regulatory-compliance.glba • regulatory-compliance.iso27001 • regulatory-compliance.nerc5 • regulatory-compliance.basel • regulatory-compliance.sox • regulatory-compliance.nist_800-41 • regulatory-compliance.dsd • regulatory-compliance.hipaa • regulatory-compliance.trm • optimize-policy • optimize-policy.unused-rules • optimize-policy.covered-rules • optimize-policy.special-case-rules • optimize-policy.consolidate-rules • optimize-policy.disabled-rules • optimize-policy.time-inactive-rules • optimize-policy.rules-without-logging • optimize-policy.rules-with-empty-comments • optimize-policy.rules-with-non-compliant-comments

Report Page Names
• optimize-policy.rules-with-a-time-clause • optimize-policy.unattached-objects • optimize-policy.unattached-user-groups • optimize-policy.unattached-users • optimize-policy.unused-global-objects • optimize-policy.unused-nat-rules • optimize-policy.empty-objects • optimize-policy.expired-users • optimize-policy.expiring-rules • optimize-policy.no-traffic-nat-rules • optimize-policy.duplicate-objects • optimize-policy.duplicate-services • optimize-policy.unused-objects-within-rules • optimize-policy.unattached-acls • optimize-policy.unattached-global-objects • optimize-policy.rule-ordering • optimize-policy.least-used-rules • optimize-policy.most-used-rules • optimize-policy.all-rules-usage • optimize-policy.all-rules-ips-usage • optimize-policy.unrouted-rules • optimize-policy.unrouted-objects-within-rules • optimize-policy.policy-refinement

Response Type: `GetReportPdfResponse`

Element	Type	Description
`RetVal`	Integer	If the report was retrieved successfully, 1; otherwise, 0.
`RetMessage`	String	Detailed return message / error message if errors occur during operation.
`EncodedReportPdf`	String	64-base encoded pdf file.

Request example:

```
<afa:GetReportPdfRequest>
    <SessionID>a9108d658a2743cb890e9f6010ed2108</SessionID>
    <EntityID>10_20_104_1</EntityID>
    <EntityType>firewall</EntityType>
    <ReportPage>home</ReportPage>
</afa:GetReportPdfRequest>
```

Response example:

```
<ns1:GetReportPdfResponse>
    <RetVal>1</RetVal>
    <RetMessage>Success</RetMessage>
    <EncodedReportPdf>The base 64 encoded PDF content</EncodedReportPdf>
</ns1:GetReportPdfResponse>
```

Setting Configuration Parameters

The `set_configuration` method sets configuration attribute values, avoiding manual configuration of the .fa/config file.

The configuration attributes are saved as follows:

- The attribute is set in the AFA default configuration file (~/.fa/config).

Request Type: **`SetConfigurationRequest`**

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from the `connect` method.
`AttributeName` *Mandatory*	AfaNonEmptyString	Attribute name.
`AttributeValue` *Mandatory*	AfaNonEmptyString	Attribute value.

Response Type: **`SetConfigurationResponse`**

Element	Type	Description
`SetConfigurationResponse`	AfaBoolean	On success, returns 1. On failure, throws a SOAP fault.

Importing Risks

The following services upload risks to AFA.

Import Risks from Spreadsheet

Request Type: `ImportingRisksfromSpreadsheetRequest`

This web service operation will receive the following parameters:

Element	Type	Description
`SessionID` *Mandatory*	String	Allows the consequent calls of various web services, without performing full AFA login each time.
`RiskProfileName` *Mandatory*	String	The name of the risk profile in which to save the risks.
`ImportedFileType` *Mandatory*	String	The extention of the imported spreadsheet. It can be only xlsx/xls.
`EncodedFileData` *Mandatory*	String	The contents of the imported spreadsheet file, encoded in base64.
`InheritStandard` *Optional*	Integer	Considered only for a new risk profile (that does not exist). 1 - to inherit from the standard, 0 (or unset) - not inherited from the standard.

Response Type: `ImportingRisksfromSpreadsheetResponse`

1. RetVal - integer - 1- for success 0- for failure.
2. RetMessage - string - a detailed return/error message, if errors came up during the operation.

Request example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:afa="https://www.algosec.com/afa-ws">
   <soapenv:Header/>
   <soapenv:Body>
      <afa:ImportRisksFromSpreadsheetRequest>
         <SessionID>2931306bb7e1ab756b0caf5ecf9a4d36</SessionID>
         <RiskProfileName>Risks12</RiskProfileName>
         <ImportedFileType>xls</ImportedFileType>
   <!--Below is a partial text example of encoded64bit xls file:-->
         <EncodedFileData>UEsDBBQABgAIAAAAIQB8bJgWaQEAAKAFAAATAAgC
W0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIooAAC
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
....</EncodedFileData>
         <!--Optional:-->
         <InheritStandard>0</InheritStandard>
      </afa:ImportRisksFromSpreadsheetRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Response example:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:ns1="https://www.algosec.com/afa-ws">
   <SOAP-ENV:Body>
      <ns1:ImportRisksFromSpreadsheetResponse>
         <RetVal>0</RetVal>
         <RetMessage>Failed to import risks:
Traffic sheet not found
Networks sheet not found
Services sheet not found</RetMessage>
      </ns1:ImportRisksFromSpreadsheetResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Import Risks from XML File

Notes:

The web service caller requires AFA administration privileges.

The definition of new services or hostgroups for risks is not supported.

Request Type: `ImportingRisksFromXMLRequest`

This web service operation will receive the following parameters:

Element	Type	Description
`SessionID` *Mandatory*	String	SessionID obtained from Connect method.
`RiskProfileName` *Mandatory*	String	The name of the risk profile in which to save the risks.
`EncodedFileData` *Mandatory*	String	The contents of the imported risk profile XML file, encoded in base64.

Response Type: `ImportingRisksFromXMLResponse`

1. RetVal - integer - 1- for success 0- for failure.
2. RetMessage - string - a detailed return/error message, if errors came up during the operation.

The Import Risks from Spreadsheet should work the same via web services as it does via the AFA GUI.

Request example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:afa="https://www.algosec.com/afa-ws">
   <soapenv:Header/>
   <soapenv:Body>
      <afa:ImportRisksFromXMLRequest>
         <SessionID>6b7f0760750a63ba97abefe1dfccac6f</SessionID>
         <RiskProfileName>XMLRisk3</RiskProfileName>
         <EncodedFileData>PD94bWwgd...M+Cg==</EncodedFileData>
            </afa:ImportRisksFromXMLRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Response example:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:ns1="https://www.algosec.com/afa-ws">
   <SOAP-ENV:Body>
      <ns1:ImportRisksFromXMLResponse>
```

```
         <RetVal>0</RetVal>
         <RetMessage>Failed to import risks:
Traffic sheet not found
Networks sheet not found
Services sheet not found</RetMessage>
      </ns1:ImportRisksFromXMLResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Managing Users and Roles

The following methods create, delete, and update users and roles.

Creating a New Role

The `create_role` method creates a new role.

Request Type: **`CreateRoleRequest`**

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
RoleName *Mandatory*	String	The name of the role.
RoleDescription *Mandatory*	String	The description of the role.
LdapDN *Optional*	String	The LDAP group that should automatically inherit this role.
Administrator *Optional*	String	Whether the role should have administrator permissions. If set to **yes**, the **AuthorizedDevices** element is automatically set to **ALL_FIREWALLS**.

Element	Type	Description
LandingPage *Optional*	String	The product that appears upon logging in. One of the following: ■ afa ■ aff ■ abf ■ automatic
FireflowAdmin *Optional*	String	Whether the role should have FireFlow administrator permissions.
EnableAnalysisFromFile *Optional*	String	Whether the role can perform analyses from configuration files.
EnableGlobalTrustTraffic *Optional*	String	Whether the role can view and edit trusted traffic settings.
AuthorizedDevices *Mandatory*	A list of `Device` objects	A list of devices the role has permission to view. See Device Type (see Device type). **Note:** If the **Administrator** element is set to **yes**, this value is automatically set to **ALL_FIREWALLS** to allow permissions to all devices.

Response Type: `CreateRoleResponse`

Element	Type	Description
Result	String	A message describing whether the role was created successfully.

Deleting a Role

The `delete_role` method deletes one or more roles.

Request Type: `DeleteRoleRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
RoleName *Mandatory*	A list of strings	The names for the role(s).

Response Type: `DeleteRoleResponse`

Element	Type	Description
Result	String	A message describing whether the role was deleted successfully.

Updating a Role

The `update_role` method edits a role.

Request Type: `UpdateRoleRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
RoleName *Mandatory*	String	The name for the role.
RoleDescription *Mandatory*	String	The description of the role.
LdapDN *Optional*	String	The LDAP group that should automatically inherit this role.
Administrator *Optional*	String	Whether the role should have administrator permissions. If set to **yes**, the **AuthorizedDevices** element is automatically set to **ALL_FIREWALLS**.

Element	Type	Description
LandingPage *Optional*	String	The product which appears upon logging in. One of the following: ■ afa ■ aff ■ abf ■ automatic
FireflowAdmin *Optional*	String	Whether the role should have FireFlow administrator permissions.
EnableAnalysisFromFile *Optional*	String	Whether the role can perform analyses from configuration files.
EnableGlobalTrustTraffic *Optional*	String	Whether the role can view and edit trusted traffic settings.
AuthorizedDevices *Mandatory*	A list of `Device` objects	A list of devices the role has permission to view. See Device Type (see Device type). **Note:** If the **Administrator** element is set to **yes**, this value is automatically set to **ALL_FIREWALLS** to allow permissions to all devices.

Response Type: `UpdateRoleResponse`

Element	Type	Description
Result	String	A message describing whether the role was updated successfully.

Creating a New User

The `create_user` method creates a new user.

Request Type: `CreateUserRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.

Element	Type	Description
`UserName`*Mandatory*	String	The user's username.
`Password`*Mandatory*	String	The user's password.
`FullName`*Mandatory*	String	The user's full name.
`Email`*Mandatory*	String	The user's email address.
`Role`*Optional*	A list of strings	The roles to assign to the user.
`AuthenticationType` *Mandatory*	String	How the user should be authenticated. One of the following: ■ local ■ radius ■ ldap
`Administrator`*Optional*	String	Whether the user should have administrator permissions. If set to **yes**, the **AuthorizedDevices** element is automatically set to **ALL_FIREWALLS**.
LandingPage *Optional*	String	The product which appears upon logging in. One of the following: ■ afa ■ aff ■ abf ■ automatic
FireflowAdmin *Optional*	String	Whether the user should have FireFlow administrator permissions.
EnableAnalysisFromFile *Optional*	String	Whether the user can perform analyses from configuration files.
EnableGlobalTrustTraffic *Optional*	String	Whether the user can view and edit trusted traffic settings.

Element	Type	Description
AuthorizedDevices *Mandatory*	A list of `Device` objects	A list of devices the user has permission to view. See Device Type (see Device type). **Note:** If the **Administrator** element is set to **yes**, this value is automatically set to **ALL_FIREWALLS** to allow permissions to all devices.

Response Type: `CreateUserResponse`

Element	Type	Description
Result	String	A message describing whether the user was created successfully.

Deleting a User

The `delete_user` method deletes one or more users.

Request Type: `DeleteUserRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
UserName *Mandatory*	A list of strings	The names for the user(s).

Response Type: `DeleteUserResponse`

Element	Type	Description
Result	String	A message describing whether the user was deleted successfully.

Updating a User

The `update_user` method edits a user.

Request Type: `UpdateUserRequest`

Element	Type	Description
`SessionID`*Mandatory*	String	Session ID obtained from the `connect` method.
`UserName`*Mandatory*	String	The user's username.
`Password`*Mandatory*	String	The user's password.
`FullName`*Mandatory*	String	The user's full name.
`Email`*Mandatory*	String	The user's email address.
`Role`*Optional*	A list of strings	The roles to assign to the user.
`AuthenticationType` *Mandatory*	String	How the user should be authenticated. One of the following: ■ local ■ radius ■ ldap
`Administrator`*Optional*	String	Whether the user should have administrator permissions. If set to **yes**, the **AuthorizedDevices** element is automatically set to **ALL_FIREWALLS**.
LandingPage *Optional*	String	The product which appears upon logging in. One of the following: ■ afa ■ aff ■ abf ■ automatic
FireflowAdmin *Optional*	String	Whether the user should have FireFlow administrator permissions.
EnableAnalysisFromFile *Optional*	String	Whether the user can perform analyses from configuration files.
EnableGlobalTrustTraffic *Optional*	String	Whether the user can view and edit trusted traffic settings.

Element	Type	Description
AuthorizedDevices *Mandatory*	A list of `Device` objects	A list of devices the user has permission to view. See Device Type (see Device type). **Note:** If the **Administrator** element is set to **yes**, this value is automatically set to **ALL_FIREWALLS** to allow permissions to all devices.

Response Type: `UpdateUserResponse`

Element	Type	Description
Result	String	A message describing whether the user was updated successfully.

AFA SOAP data types

Each statistic is represented by a type and name combination.

Available Statistics

Statistics Type (StatType)	Supported data for the type (StatName)
simple_count	■ security_rating ■ rules ■ optimization_items ■ objects ■ interfaces ■ unused_rules ■ covered_rules ■ special_case_rules ■ rule_consolidation_opportunities ■ disabled_rules ■ time_inactive_rules ■ rules_without_logging ■ unattached_objects ■ unused_objects ■ unused_objects_within_rules ■ IPT_tightening_opportunities ■ baseline_compliance_failures ■ policy_installations ■ rules_without_comment ■ duplicate_objects ■ current_rule_order_RMPP ■ top_ten_optimization_RMPP
risks_per_risk_level	■ high ■ suspected_high ■ medium ■ low

Statistics Type (StatType)	Supported data for the type (StatName)
risk_with_risk_level	■ high ■ suspected_high ■ medium ■ low
rule_changes	■ added ■ deleted ■ modified
risk_level	highest
compliance_pass	PCI
compliance_fail	PCI
compliance_undef	PCI
compliance_color	The name of the regulatory compliance report.
compliance_score	The name of the regulatory compliance report.
service_changes	■ added ■ modified ■ deleted
hostgroup_changes	■ added ■ modified ■ deleted
topology_changes	■ added ■ modified ■ deleted
total_changes	The sum of all changes last found for the device, across all ASMS functionality.

AFA SOAP data type reference

Device type

Element	Type	Description
`ID` *Mandatory*	String	The device ID.
`Profile` *Optional*	String	The permission profile: ■ standard ■ read only ■ none
`Notification` *Optional*	String	Whether the role will receive notifications for the device.

➔ **See also**:

- AFA SOAP data types

DeviceDataResult type

The following table describes the elements in the `DeviceDataResult` type object.

Note: All elements are *optional*.

Element	Type	Description
`Brand`	String	Device brand. Possible values: ■ asa- Cisco firewalls ■ ios - Cisco routers ■ nsc - Juniper NetScreen ■ junos - Juniper SRX ■ fortigate - Fortinet FortiGate
`Name`	String	Display name of the Device.
`ID`	String	Tree name of the device.
`IP`	String	IP address of the device
`DomainName`	String	Domain name of the device. Relevant only when domains are enabled. Default: **0**

➔ See also:

- AFA SOAP data types

Groups type

The following table describes the elements in the `Groups` type object:

Element	Type	Description
`GroupsID`*Optional*	String	Tree name of the group.

➔ See also:

- AFA SOAP data types

HostGroup type

The following table describes the elements in the `HostGroup` type object:

Element	Type	Description
`EntityID`*Mandatory*	String	Entity ID of the container.
`Name`*Mandatory*	String	Original name of host group.
`CanonizedName`*Mandatory*	String	Canonized name.
`IP`*Mandatory*	ArrayOfstring	Array of IP addresses.
`ClassName`*Mandatory*	String	Name of class.
`Members`*Mandatory*	ArrayOfstring	Array of members.

➔ See also:

- AFA SOAP data types

KeyValue type

The following table describes the elements in the `KeyValue` type object:

Element	Type	Description
key	String	Parameter name.
value	String	Parameter value.

➔ See also:

- AFA SOAP data types

NatResult type

The following table describes the elements in the `NatResult` type object.

Note: All elements are *optional*.

Element	Type	Description
`DeviceName/GroupName`	String	Display name of the Device/Group.
`PreNat`	String	Pre-NAT value of source/destination.
`PostNat`	String	Post-NAT value of source/destination.
`Type`	String	Static or dynamic.

➔ See also:

- AFA SOAP data types

NewDevice type

The following table describes the elements in the `NewDevice` type object:

Element	Type	Description
`Brand`*Mandatory*	String	Device brand. Values include: • **fortigate**. Fortinet FortiGate • **ios**. Cisco IOS routers • **junos**. SRX • **nexus.** Cisco Nexus routers • **nsc**. Juniper NetScreen • **paloalto**. Palo Alto • **asa**. Cisco firewalls
`DisplayName`*Optional*	String	Display name of the device.
`Name`*Optional*	String	Tree name of the device.
`HostName`*Mandatory*	String	Host name of the device.
`UserName`*Mandatory*	String	Name of user.
`Password`*Mandatory*	String	Password of user.

Element	Type	Description
`ConnectionType` *Mandatory*	String	Type of connection. Possible values: ■ SSH ■ telnet
`FW_TYPE` *Mandatory*	String	Device type. Possible values: ■ FW_GEN - Cisco Nexus routers, Juniper SRX, Fortinet FortiGate, and Palo Alto ■ FW_IOS - Cisco IOS routers ■ FW_NSC - Juniper Netscreen ■ FW_ASA - Cisco firewalls
`RulesView` *Optional*	String	View of rules. Relevant only for Cisco firewalls. Possible values: ■ ASDM ■ CLI
`Monitoring` *Optional*	String	Monitoring. Possible values: ■ yes ■ no
`Collector` *Optional*	String	If Geographical Distribution is not enabled, enter 'Central Manager'. If it is enabled, enter the name of the collector.

Element	Type	Description
`LogCollectionMode` *Optional*	String	Mode of log collection. Possible values: ■ none ■ standard ■ extensive For Cisco firewalls, if only hit-counters are required (and no traffic logs), set to 'none'.
`LogCollectionFrequency` *Optional*	String	Value in minutes. Default is 60.
`CollectLog`*Optional*	String	Enable log collection. Possible values: ■ yes ■ no
`CollectLogFrom`*Optional*	String	Log server type for traffic logs. Possible values: ■ [blank] - No log collection ■ syslog - Syslog NG Server ■ nsm - Juniper NSM - Relevant only for NetScreen devices
`CollectLogFromAdt` *Optional*	String	Log server type for audit logs. Possible values: ■ [blank] - No log collection ■ syslog - Syslog NG Server ■ nsm - Juniper NSM - Relevant only for NetScreen devices
`LogHostName`*Optional*	String	Host name of the traffic log server.

Element	Type	Description
`LogUserName` *Optional*	String	Username to connect to the traffic log server.
`LogHostNameAdt` *Optional*	String	Host name of the audit log server.
`LogUserNameAdt` *Optional*	String	Username to connect to the audit log server.
`LogPassword` *Optional*	String	Password to connect to the traffic log server.
`LogPasswordAdt` *Optional*	String	Password to connect to the audit log server.
`AdditionalFwIDs` *Optional*	String	Additional device identifiers.
`FirewallUsers` *Optional*	String	Users to have permissions to this device.
`SeparateVrfs` *Optional*	String	Enable VRF separation. Relevant for Cisco routers only. Default and recommended value is 'yes'.
`FullAnalysis` *Optional*	String	Enable policy analysis. Relevant for Cisco routers only. Default and recommended value for routers with no ACLs is 'no'.
`SshPort` *Optional*	String	The port used to connect via SSH.
`BaselineProfile` *Optional*	String	The baseline profile you want the new device to use by default.
`EnableUserName` *Optional*	String	Username used for advanced mode. Relevant for Cisco routers only.
`EnablePassword` *Optional*	String	Password used for advanced mode. Relevant for Cisco routers only.

Note:

Support for the Forcepoint brands (Sidewinder, StoneGate) and Hillstone was deprecated in ASMS version A30.00.

If you had defined these devices in an earlier version of ASMS, these devices are still available to you, with all the existing capabilities, but you cannot add new ones after upgrading.

We recommend backing up device data before or after upgrading and then removing these devices from AFA. Make sure to download any report zip files for the device before deleting.

For more details, see the relevant AlgoPedia KB article.

➔ See also:

- AFA SOAP data types

QueryData type

The following table describes the elements in the `QueryData` type object:

Element	Type	Description
`QueryDescription` *Mandatory*	String	Description of query.
`QueryHTMLPath` *Mandatory*	String	URL to the results in the UI.
`FIPResult` *Mandatory*	String	One of the following: ■ Unreachable ■ SameZone ■ Routed ■ PartiallyRouted ■ NotExecuted ■ Unknown

Element	Type	Description
`QueryResult` *Mandatory*	String	One of the following: ■ allowed ■ blocked ■ partially allowed ■ not routed
`QueryItem` *Mandatory*	`QueryValueResults`	List of query value results. See QueryValueResults type below.

QueryValueResults Type

The following table describes the elements in the `QueryValueResults` type object:

Element	Type	Description
`Device` *Mandatory*	List of `DeviceResult` objects	List of device results. See DeviceResult type below.

DeviceResult Type

The following table describes the elements in the `DeviceResult` type object:

Element	Type	Description
`IsAllowed` *Mandatory*	String	Status information and the number of rules that support it. For example: Allowed (x1), Blocked (x4), Partially allowed (x4).
`DeviceName` *Mandatory*	String	Display name of the device.
`Rules` *Mandatory*	List of `QueryRules` objects	List of rules. See QueryRules type below.

QueryRules Type

The following table describes the elements in the `QueryRules` type object.

Note: All elements are *optional*.

Element	Type	Description
`Rule`	String	Internal AlgoSec Rule ID. To retrieve the rule ID, call one of the rule APIs, such as get_rules_by_device (see Retrieving a List of a Device's Rules) or search_rules (see Searching for Rules).
`Service`	String	List of services.
`Source`	String	List of sources.
`Source_Nat`	String	List of NAT sources.
`Destination`	String	List of destinations.
`Destination_Nat`	String	List of NAT destinations.
`Install`	String	List of installs.
`Action`	String	Action.
`ACL`	String	ACL.

➔ See also:

- AFA SOAP data types

QueryRequestData type

The following table describes the elements in the `QueryRequestData` type object:

Element	Type	Description
`Source` *Mandatory*	List of String	Source(s) for the query. Multiple values are separated by commas (,).
`Destination` *Mandatory*	List of String	Destination(s) for the query. Multiple values are separated by commas (,).

Element	Type	Description
`Service` *Mandatory*	List of String	Service(s) for the query. Multiple values are separated by commas (,).
`User` *Optional*	List of String	User(s) who created the rule. Multiple values are separated by commas (,).
`Application` *Optional*	List of String	Application(s) for the rule. Multiple values are separated by commas (,).

➔ See also:

- AFA SOAP data types

Rules type

The following table describes the elements in the `Rules` type object:

Element	Type	Description
`Rule` *Mandatory*	`Rule`	Rule information. See Rule Type below.

Rule Type

The following table describes the elements in the `Rule` type object:

Note: All elements are *optional*.

Element	Type	Description
`DeviceID`	String	ID of device.
`Document`	String	Document.
`RuleID`	String	AlgoSec internal rule ID.
`RuleNum`	Integer	Number of rule.
`Name`	String	Name of rule.
`Source`	String	List of sources.

Element	Type	Description
Destination	String	List of destinations.
Services	String	List of services.
Action	String	Action.
Enable	String	Enable.
Track	String	Track.
Time	String	Time.
Install	String	Install.
VPN	String	VPN.
Section_Header	String	Section header.
Global	String	Global.
Service	String	Service.
Log	String	Log.
From	String	From.
To	String	To.
Schedule	String	Schedule.
Comment	String	Comment.
Comments	String	Comments.
ACL	String	Access Control List
Interface	String	Interface.
LineNum	String	Line number.
Internal_Name	String	Internal name.
UID	String	UID.
Line	String	Line.

Element	Type	Description
`Layer_Name`	String	Name of the layer. Only relevant for Check Point R80.
`Layer_Type`	String	Type of Layer. Only relevant for Check Point R80.

➔ **See also**:

- AFA SOAP data types

SearchParam type

The following table describes the elements in the `SearchParam` type object:

Element	Type	Description
`Search` *Mandatory*	String	Search string.
`Field` *Optional*	String	Search field. If no device is selected, search is run on all devices. If no device field is selected, search is run on all fields for device type. For more details, see AFA search rule fields.

Note:

Support for the Forcepoint brands (Sidewinder, StoneGate) and Hillstone was deprecated in ASMS version A30.00.

If you had defined these devices in an earlier version of ASMS, these devices are still available to you, with all the existing capabilities, but you cannot add new ones after upgrading.

We recommend backing up device data before or after upgrading and then removing these devices from AFA. Make sure to download any report zip files for the device before deleting.

For more details, see the relevant AlgoPedia KB article.

➔ See also:

- AFA SOAP data types

ServiceInfo type

The following table describes the elements in the `ServiceInfo` type object:

Element	Type	Description
`DeviceID` *Mandatory*	String	Tree name of the device.
`Name` *Mandatory*	String	Display name of the device.
`Ports` *Mandatory*	`Ports`	Device ports. See Ports Type below.

Ports Type

The following table describes the elements in the `Ports` type object:

Element	Type	Description
`Port` *Mandatory*	List of Strings	List of device ports.

➔ See also:

- AFA SOAP data types

StatsData type

The following table describes the elements in the `StatsData` type object:

Element	Type	Description
`StatType` *Mandatory*	String	Type of statistic. See Available Statistics (see Each statistic is represented by a type and name combination.) for details.

Element	Type	Description
`StatName` *Mandatory*	String	Name of the statistic. See Available Statistics (see Each statistic is represented by a type and name combination.) for details.
`StatValue` *Mandatory*	String	Value of the statistic.

➔ See also:

- AFA SOAP data types

TemplateDomainSettings type

The following table describes the elements in the `TemplateDomainSettingsType` object:

Element	Type	Description
`TemplateDomainName` *Mandatory*	AfaNonEmptyString	Name of the template domain. AFA copies relevant information from the specified template domain.

Element	Type	Description
`CopyRiskProfiles` *Mandatory*	AfaBoolean	If True, AFA should copy risk profiles and their connected files from the template domain to the new domain: ■ Risk Profiles in the risk_profiles folder ■ User defined services saved in the user_def.srv file ■ User defined host groups saved in the algosec_hostgroups.out file ■ Zone risks saved in the zones_advisor.xml file The following Zone types configuration parameters are also copied: ■ Zones_Types_Letters ■ Zones_Types_Names ■ Zones_Types_Same_As ■ Zones_Types_Colors ■ Zones_Types_Hosts
`CopyRoles` *Mandatory*	AfaBoolean	If True, AFA should copy roles defined in the template domain to the new domain. When true the *users_info.xml* file in the template domain is copied to the *users_info.xml* file in the new domain. Any roles associated with the `ALL_FIREWALLS` group in the template domain are copied to the `ALL_FIREWALLS` group in the new domain. `CopyRoles` only copies roles and not user information to the new domain.

➔ See also:

- AFA SOAP data types

SOAP fault list

Code	Text	Constant
0	Invalid Device ID	
	Invalid Column Name There are no permissions for this user to update rule documentation.	
		_WS_ERR__NONE
	System Error	_WS_ERR__SYSTEM
	Invalid User	_WS_ERR__INVALID_ USER
	Incorrect Password	_WS_ERR__ PASSWORD_ INCORRECT
	Not connected	_WS_ERR__NOT_ CONNECTED
	Not implemented	_WS_ERR__NOT_ IMPLEMENTED
	Operation failed	_WS_ERR__ OPERATION_FAILED
500		
501	Session ID expired or does not exist	_WS_ERR__INVALID_ TOKEN
505	You are not permitted to perform this operation	_WS_ERR__NOT_ PERMITTED
710		
721	Attribute name and value cannot be empty	
729		
731	Group name cannot be empty	

Code	Text	Constant
732	Group must consist of at least one device	
733	Group $sGroupName already exists	
734	Group with ID $sGroupTreeName already exists	
735	Group '$sGroupName' could not be created - '$member' was not found	
741	Group ID cannot be empty	
742	Group ID cannot contains spaces or special characters	
743	Group ID cannot be empty	
744	Group with ID '$sGroupTreeName' was not found	
745	Device with ID '$sDeviceTreeName' was not found	
749		
751	Scheduler job name cannot be empty	
752	Scheduler job recurrence cannot be empty	
753	Hour must be between 0 and 23	
754	Minutes must be between 0 and 55 in 5 minute increments	
756	Job name cannot contains special characters	
791	Entity type must be device, group or matrix	
792	Entity (device/group/matrix) ID cannot be empty	
793	Entity ID cannot contain spaces or special characters	
794	'ucfirst($sEntityType)' with ID '$sEntityTreeName' was not found	

SOAP API examples

This section contains examples for using the SOAP API in the following languages: PERL, PHP, and Python.

PERL example

```
#!/usr/bin/perl -w
use Data::Dumper;
#use SOAP::Lite ( +trace => all, maptype => {} );
use SOAP::Lite;
#$ENV{PERL_LWP_SSL_VERIFY_HOSTNAME} = 0;
my $soap = SOAP::Lite->proxy('https://localhost/AFA/php/ws.php?wsdl');
# Do not verify the SSL key
$soap->transport->ssl_opts(
verify_hostname => 0,
SSL_verify_mode => 0x00
);
#
# Login to AFA Web Service
#
sub ConnectAFA
{
my $sUserName = shift; # User name
my $sPassword = shift; # Password
my $sDomain   = shift; # Domain name or empty for non domain envirnment
$sDomain  = (!defined $sDomain) ? '' : $sDomain;
my $method = SOAP::Data->name('ConnectRequest')->attr({xmlns =>
'https://www.algosec.com/afa-ws'});
my @params = (
SOAP::Data->name(UserName => $sUserName),
SOAP::Data->name(Password => $sPassword),
SOAP::Data->name(Domain   => $sDomain)
);
```

```
my $sSessionID = $soap->call($method => @params)->result;
}
#
# Executing query request
#
sub ExecQuery
{
my $sSessionID   = shift;
my $sQueryTarget = shift;
$sQueryTarget    = (!defined $sQueryTarget) ? '' : $sQueryTarget;
my $method = SOAP::Data->name('QueryRequest')->attr({xmlns =>
'https://www.algosec.com/afa-ws'});
my $QueryInput   =  SOAP::Data->name('QueryRequest')->attr({xmlns =>
'https://www.algosec.com/afa-ws'});
my @params = (
SOAP::Data->name(SessionID   => $sSessionID),
SOAP::Data->name(QueryInput  => \SOAP::Data->value(
SOAP::Data->name(Source       => '*'),
SOAP::Data->name(Destination  => '*'),
SOAP::Data->name(Service      => '80'),
SOAP::Data->name(Service      => '443')
)
),
SOAP::Data->name(QueryTarget => $sQueryTarget)
);
return $soap->call($method => @params);
}
#
# Disconnect from AFA Web Service (terminate session)
#
sub DisconnectAFA
{
my $sSessionID   = shift;
```

```
my $method = SOAP::Data->name('DisconnectRequest')->attr({xmlns =>
'https://www.algosec.com/afa-ws'});
my @params = (
SOAP::Data->name(SessionID => $sSessionID),
);
return $soap->call($method => @params)->valueof('//DisconnectResponse');
}
my $sSessionID = ConnectAFA('admin', 'algosec', '');
print "\n";
print "Session ID: '" . $sSessionID ."'";
print "\n";
my $QueryResult = ExecQuery($sSessionID, 'afa-276');
foreach my $Result ($QueryResult->valueof('//QueryResult/')) {
print Dumper($Result);
}
print "\n";
my $Disconnect = DisconnectAFA($sSessionID);
print "Disconnect: ";
print $Disconnect;
print "\n";
```

PHP example

```
<?php
ini_set("soap.wsdl_cache_enabled", "0"); // disabling WSDL cache for
development
$sHost = '10.135.1.45'; // AFA host
$sWSDLlocavion = 'https://'.$sHost.'/AFA/php/ws.php?wsdl';
$client = new SoapClient($sWSDLlocavion);
$src = '192.168.1.100';
$dst = '10.228.16.10';
$srv = 'tcp/22';
try {
```

```
$client->__setLocation($sWSDLlocavion);
$return = $client->connect(array('UserName'=>'admin','Password'=>'algosec',
'Domain'=>''));
echo "Response of the 'connect' method: \n";
print_r($return);
echo "\n";
flush();
if (isset($return->SessionID)) {
$sSessionID = $return->SessionID;
echo 'Submitting query request...' . "\n";
flush();
$query = array('Source'=>$src, 'Destination'=>$dst, 'Service'=>$srv);
$QueryResult = $client->query(array('SessionID'=>$sSessionID,
'QueryInput'=>$query));
echo "Response of the 'query' method: \n";
flush();
print_r($QueryResult);
echo "\n";
$QueryHTMLlink = $QueryResult->QueryUIResult;
echo 'Query HTML link: ' . $QueryHTMLlink."\n";
flush();
$return = $client->disconnect(array('SessionID'=>$sSessionID));
echo "Response of the 'disconnect' method (terminating session): \n";
print_r($return);
echo "\n";
}
}
catch (Exception $objException) {
echo 'Error: '.$objException->getMessage ();
echo 'Error: '.$objException->faultstring;
echo '<xmp>';
print_r($objException);
echo '</xmp>';
```

```
}
?>
```

Python example

```
#!/usr/bin/python
from SOAPpy import SOAPProxy
def ConnectAFA(params):
# username/password
username = params['UserName']
password = params['Password']
domain   = params['Domain']
proxy = 'https://'+sHost+'/AFA/php/ws.php?wsdl'
namespace = 'https://www.algosec.com/afa-ws'
server = SOAPProxy(proxy, namespace)
if (DebugMode):
# uncomment these for debugging output
server.config.dumpHeadersIn = 1
server.config.dumpHeadersOut = 1
server.config.dumpSOAPOut = 1
server.config.dumpSOAPIn = 1
response = server.ConnectRequest(UserName=username, Password=password,
Domain=domain)
return response
def SendQueryRequest(params):
# username/password
SessionID = params['SessionID']
QueryInput = params['QueryInput']
proxy = 'https://'+sHost+'/AFA/php/ws.php?wsdl'
namespace = 'https://www.algosec.com/afa-ws'
server = SOAPProxy(proxy, namespace)
if (DebugMode):
# uncomment these for debugging output
```

```
server.config.dumpHeadersIn = 1
server.config.dumpHeadersOut = 1
server.config.dumpSOAPOut = 1
server.config.dumpSOAPIn = 1
response = server.QueryRequest(SessionID=SessionID, QueryInput=QueryInput)
return response
def DisconnectAFA(params):
# username/password
SessionID = params['SessionID']
proxy = 'https://'+sHost+'/AFA/php/ws.php?wsdl'
namespace = 'https://www.algosec.com/afa-ws'
server = SOAPProxy(proxy, namespace)
if (DebugMode):
# uncomment these for debugging output
server.config.dumpHeadersIn = 1
server.config.dumpHeadersOut = 1
server.config.dumpSOAPOut = 1
server.config.dumpSOAPIn = 1
response = server.DisconnectRequest(SessionID=SessionID)
return response
sHost = '192.168.3.82'
#DebugMode = True
DebugMode = False
print "\n" + "Submitting connect request:" + "\n"
values = {'UserName': 'admin', 'Password': 'algosec', 'Domain': ''}
afa_connect = ConnectAFA(values)
SessionID = afa_connect
print "Returned Session ID: "+repr(SessionID)
print "\n" + "Submitting query request:" + "\n"
QueryParams = {'SessionID': SessionID,'QueryInput': {'Source':
 '192.168.1.100', 'Destination': '10.228.16.10', 'Service': 'tcp/22'}}
QueryResult = SendQueryRequest(QueryParams)
```

```
print QueryResult
print "\n" + "Submitting disconnect request:" + "\n"
DisconnectParams = {'SessionID': SessionID}
DisconnectResult = DisconnectAFA(DisconnectParams)
print DisconnectResult
```

AFA search rule fields

The following are lists of possible search field values based on the devices searched.

Note:

Support for the Forcepoint brands (Sidewinder, StoneGate) and Hillstone was deprecated in ASMS version A30.00.

If you had defined these devices in an earlier version of ASMS, these devices are still available to you, with all the existing capabilities, but you cannot add new ones after upgrading.

We recommend backing up device data before or after upgrading and then removing these devices from AFA. Make sure to download any report zip files for the device before deleting.

For more details, see the relevant AlgoPedia KB article.

No device selected

If no device is selected, the search is run on all devices.

- [EMPTY] - all fields
- SOURCE
- DESTINATION
- SOURCE_DESTINATION (Source or Destination)
- SERVICE
- ACTION
- FROM (from zone)
- TO (to zone)
- USER

- APPLICATION
- NAME
- COMMENT
- LOG
- TIME
- ENABLE
- DOCUMENTATION

Symantec Blue Coat Devices

- [EMPTY] - all fields
- RULE (rule number)
- SOURCE
- DESTINATION
- SOURCE_DESTINATION (source or destination)
- SERVICE
- Service
- TIME
- ACTION
- TRACK
- COMMENTS

Check Point Devices

- [EMPTY] - all fields
- ACTION
- COMMENTS
- DESTINATION
- ENABLE

- INSTALL (installed on)
- NAME (rule name)
- RULENUM (rule number)
- SERVICES
- SOURCE
- SOURCE_DESTINATION (Source or Destination)
- TIME
- TRACK
- VPN

Cisco Firewalls

- [EMPTY] – all fields
- ENABLE
- SOURCE
- DESTINATION
- SOURCE_DESTINATION (source or destination)
- SERVICE
- ACTION
- LOG
- TIME
- COMMENTS

Cisco Routers

- [EMPTY] – all fields
- NAME (rule id)
- LINE (text in the configuration line)

Forcepoint (McAfee) Sidewinder Devices

- [EMPTY] – all fields
- NAME (rule name)
- ENABLE
- ACTION
- SERVICE
- FROM (source burb)
- SOURCE
- TO (destination burb)
- DESTINATION
- SOURCE_DESTINATION (source or destination)
- COMMENT (description)
- APPLICATION DEFENSE
- AUTHENTICATION
- DESCRIPTION
- PORTS
- IPS SIGNATURE GROUP
- IPS RESPONSE
- TRUSTEDSOURCE
- SOURCE NAT
- DESTINATION REDIRECT

Fortinet FortiGate and FortiManager Devices

- [EMPTY] – all fields
- RULE (rule ID)
- FROM

- TO
- SOURCE
- DESTINATION
- SOURCE_DESTINATION (source or destination)
- SERVICE
- ACTION
- COMMENT
- LOG
- SCHEDULE

Juniper Space and SRX Devices

- [EMPTY] – all fields
- RULE (rule name)
- FROM (from zone)
- TO (to zone)
- SOURCE
- DESTINATION
- SOURCE_DESTINATION (source or destination)
- SERVICE (Application)
- ACTION
- LOG
- TIME

Juniper NSM and NetScreen Devices

- [EMPTY] – all fields
- RULE (rule ID)
- NAME (rule name)

- FROM ZONE
- TO ZONE
- SOURCE
- DESTINATION
- SOURCE_DESTINATION (source or destination)
- SERVICE
- ACTION
- SOURCENAT (source NAT)
- DESTINATIONNAT (destination NAT)
- TIMECLAUSE
- ENABLE
- TRACK

Palo Alto Devices

- [EMPTY] – all fields
- NAME
- TAG
- FROM (from zone)
- SOURCE
- USER
- HIP PROFILE
- TO (to zone)
- DESTINATION
- SOURCE_DESTINATION (source or destination)
- APPLICATION
- SERVICE

- ACTION
- PROFILE
- OPTIONS
- COMMENT

FireFlow REST web services

This section describes the FireFlow REST web services APIs.

Base URL

The base URL for all REST requests is the following:

```
https://<algosec_server>/FireFlow/api
```

where `<algosec_server>` is the AFA/FireFlow server URL.

Note: Every request must be in JSON format. Each request must include the `content-type` header with the value `application/json`.

Swagger

The FireFlow RESTful API includes Swagger support, enabling you to execute simplified API request calls and access full lists of request parameters.

To access Swagger API documentation:

1. In the toolbar, click your username and click **API Documentation**.
2. From the dropdown at the top-right, click **AlgoSec_FireFlow**.

FireFlow REST API reference

FireFlow supports the following REST APIs:

- Authenticating
- Run an advanced search
- Check if session is alive
- Create a traffic change request
- Create a device object change request
- Create a rule removal change request
- Update a traffic change request's custom fields

- Get permitted request templates
- Get details for a specified change request

For more details, see FireFlow data types.

Authenticating

The FireFlow REST API uses cookie-based authentication. The authentication request returns a `sessionId` that you use to manually create a cookie. The cookie is required for all other API requests.

Resource Name: `/FireFlow/api/authentication/authenticate`

Request Method: POST

Request Body:

Element	Type	Description
`username`*Mandatory*	String	AlgoSec Security Management Suite username.
`password`*Mandatory*	String	AlgoSec Security Management Suite password.
`domain`*Optional*	String	Domain name. Relevant only when domains are enabled. Default: **null**

Response Body:

Element	Type	Description

`status`	String	One of the following:
		`Success`
		`Failure`

`messages`	List of strings	The `code` and `message`. See below.

`code`	String	One of the following:
		`success`
		`authentication.failure`

Element	Type	Description

`message`	String	One of the following:
		`Success`
		`Authentication Failed`

`data`	List of strings	In the case of a success, the `sessionId`, `faSessionId`, and `phpSessionId`. In case of failure, the value is null.

Example Request:

```
{"username":"admin","password":"algosec","domain":null}
```

Example Response (Success):

```
{
"status": "Success",
"messages": [
{
"code": "success",
"message": "Success"
}
],
"data": {
"sessionId": "adaa420aaf8fc37bfae506ecd742ab75",
"faSessionId": "a5326bb7a200d3984de6a2533af5b351",
"phpSessionId": "PHPSESSID=n1rgrme4mi5m9cj51jfp4rbc07; path=/; secure;
HttpOnly"
}
}
```

Example Response (Failure):

```
{
"status": "Failure",
```

```
"messages": [
{
"code": " authentication.failure",
"message": "Authentication Failed"
}
],
"data": null
}
```

Run an advanced search

The `savedsearch` method allows you to run an advanced search that is currently saved in FireFlow by specifying the name of the search.

Resource Name: `/FireFlow/api/savedsearch`

Request Method: `GET`

Header Requirements:

Parameter	Key	Type	Value
`Cookie`	`FireFlow_Session`	String	The `sessionId` retrieved in the authentication request.

Request Query Parameters:

Parameter	Type	Description
`savedSearchName`	String	The name of the saved search you want to run. **Note:** There is no requirement to name saved searches uniquely. If more than one saved search with the specified name exists, the first one will be returned.

Response:

Element	Type	Description

`status`	String	One of the following:
		`Success`
		`Failure`

`messages`	Object containing the `code` and the `message`.	Strings that indicate whether the request succeeded or failed.
`data`	Object containing the `savedSearchResults` and the `resultsCount`.	See below.
`savedSearchResults`	A list of `changeRequestId`	The change request IDs returned for the search.
`resultsCount`	Integer	The number of search results.

Example Request:

```
https://192.168.11.40/FireFlow/api/savedsearch?savedSearchName=Show-results
```

Example Response:

```
{
"status": "Success",
"messages": [
{
"code": "success",
"message": "Success"
}
],
"data": {
"savedSearchResults": [
{
"changeRequestId": 1
```

```
},
{
"changeRequestId": 3
},
{
"changeRequestId": 4
},
{
"changeRequestId": 5
},
{
"changeRequestId": 6
}
],
"resultsCount": 5
}
}
```


Check if session is alive

Check if a session is alive by entering a cookie.

Note: This API is read-only from swagger.

Resource Name: `/FireFlow/api/session`

Request Method: GET

Request Body:

Element	Type	Description
`sessionID`	String	ID of session to check.

Response Body:

Element	Type	Description
`message`	MessageDetails type	Response message.
`valid`	Boolean	• true • false

Response example:

```
{
"message": {
"code": "string",
"message": "string"
},
"valid": true
}
```

Create a traffic change request

The FireFlow REST API creates a Traffic Change Request.

FireFlow validates the API to ensure that mandatory elements are in place, such as permissions, template, date formats, that any specified device exists in AFA, and so on.

Resource Name: `/FireFlow/api/change-requests/traffic`

Request Method: POST

Request Body:

Element	Type	Description
`trafficChangeRequestDetails`	TrafficChangeRequest type	Object body containing details for creation of traffic change request.

Storing firewall suffix in host or service groups

If you are using the **StoreFirewallSuffixInHostGroup** and

StoreFirewallSuffixInServiceGroup configuration, the address format in source and destination fields must be as follows:

Firewall suffixes	This definition is translated from the fireall as follows: **<object_name>:fw:<firewall treeName>** For example: **host-1:fw:My_GW1**
Group suffixes	This definition is translated from the one of the group members, as follows: **<object_name>:grp:<firewall treeName>** For example: **grp-1:grp:My_GW1**

Source with firewall suffix example:

```
{
"source": {
"items": [{
"address": "host-1:fw:My_GW1"
}
]
}
```

Device names and rule IDs

If you are defining the device, you must enter the device database name, not the name displayed in the AFA device tree. Rule IDs must also be defined as the internal AFA IDs.

Retrieve both device database names and internal rule IDs using the following API:

https://<server_IP>/fa/server/rules/read?session=<FA_session_Id>&entity=<AFA_UI_display_name>

Any error messages that include the device name include the name displayed in AFA.

Attachment field details

The attachment field accepts single or multiple values, and expects the following syntax:

'filename=<filename>:content=<encoded file content to base64 string>'

Additionally:

- Filenames must be valid Linux filenames, including valid characters only, no more than 255 characters, and not an empty string.
- Files must also have valid extensions, and not be of any file types listed in the **RestrictedFileExtensionsInAttachment** configuration.
- File content should be encoded to base 64.
- Before encoding, the file content should not exceed the maximum size configured in the **MaxAttachmentSize** configuration parameter.

Request example

```
{
 "template": "Basic Change Traffic Request",
  "fields": [
  {
   "key": "subject",
   "values": [
    "Traffic_Ticket_Via_REST_API"
    ]
   },
   {
    "key": "Change Request Description",
    "values": [
     "add here the change request description"
    ]
   },
   {
    "name": "devices",
    "values": [
     "CKP1",
     "Cisco2"
    ]
   }
  ],
  "traffic": [{
   "source": {
```

```
    "items": [{
     "name": "1.1.1.0/24"
    },
    {
     "name": "host_object"
    }
   ]
  },
  "destination": {
   "items": [{
    "name": "2.2.2.2-2.2.2.150",
     "fields": [{
      "key": "CFPTI",
       "values": [
        "destination1"
       ]
     }]
   }]
  },
  "service": {
   "items": [{
    "name": "https"
    },
    {
     "name": "service_object"
     }
    ]
   },
   "user": {
    "items": [{
    "name": "user1"
   }]
  },
  "application": {
   "items": [{
   "name": "any"
   }]
  },
  "action": "Allow",
  "natDetails": {
   "source": ["9.9.9.9"],
   "destination": ["8.8.8.8"],
   "port": ["tcp/8080"],
```

```
    "type": "Static"
   },
   "fields": [{
    "key": "Requested Source Group Name",
    "values": [
    "sourceGroup100"
    ]
  }]
 }]
 }
```

Response: Response type

Create a device object change request

This REST calls supports opening object change requests, including those where objects from multiple devices are being changed.

FireFlow validates the API to ensure that mandatory elements are in place, such as permissions, template, date formats, that any specified device exists in AFA, and so on.

Note: The change request that is created from this request cannot be edited in the Web Interface.

Resource Name: `/FireFlow/api/request/object`

Request Method: `POST`

Header Requirements:

Parameter	Key	Type	Value
`Cookie`	`FireFlow_Session`	String	The `sessionId` retrieved in the authentication request.

Request Query Parameters:

Element	Type	Description

Mandatory basic change request fields:
`template`
Additional, optional basic change request fields, such as:
`description`
`due`
`expire`
`externalId`
`owner`
`priority`
`refersTo`
`referredBy`
`requestor`
`subject`
	String	The change request's value for the field.
		Note: Element syntax in this API may differ slightly from the traffic change request API, even if it refers to the same data.
		For example, the **externalID** in this API is the same as the **CMS ticket id** in the traffic ticket API, and **referredBy** in this API is the same as **ReferredBy** in traffic ticket APIs.

`customFields` *Optional*	A `customFields` object	See customFields type.

Element	Type	Description
`requestedActions: devices` *Mandatory*	List of strings	The list of devices for which the object change request will be created. This element is mandatory only if you do not use the **objectContainers** element. **Note:** If you are defining the device, you must enter the device database name, not the name displayed in the AFA device tree. Retrieve device database names using the following API: **https://<server_IP>/fa/server/rules/read?session=<FA_session_Id>&entity=<AFA_UI_display_name>** Any error messages that include the device name include the name displayed in AFA.
`requestedActions: action`	String	One of the following: • create • delete • addObjectsToGroup • removeObjectsFromGroup • replaceContent
`requestedActions: name`	String	The Display name of the Object being modified.

Element	Type	Description
`requestedActions: isGroup`	String	Whether the object is able to hold multiple values within it. Non-group objects may not be transformed into group objects, and group objects may not become non-group objects(though they may contain only 1 value). One of the following:: • True • False Example of a non-group object: host_1.1.1.1 Example of group object: ntp_servers
`requestedActions: type`	String	The type of object. One of the following: • network • service
`requestedActions: values`	Array of String	List of values being added, removed, or placed. Example for Service Object: ["tcp/23","udp/53"] Example for Network Object: ["1.1.1.1","192.168.0.1/24"]

Element	Type	Description
`objectContainerLevel`	String	The device/management level on which to change the object. One of the following: • **highest**. To change the object at the highest level/management. **Note:** For Check Point devices, choosing highest will change the object on the CMA, not the PV1. • **lowest**. To change the object on the lowest level/individual device. • **automatic**. (Default) The level on which to change the object is determined based on an algorithm.

Response:

Element	Type	Description
`status`	String	One of the following: • Success • Failure
`messages`	Object containing the `code` and the `message`.	Strings that indicate success or failure. In case of failure, contains a list of strings that detail why the change request was not created.
`data`	A `changeRequestId` object or a list of strings	One of the following: • In case of success, the change request ID and a redirect URL • In case of failure, null. **Note:** Change request creation may not have been completed even though the ID is supplied.

Create object request example

```
{
   "template":"135: Object Change Multi Device Request",
   "subject":"Create object request",
   "due":"2019-10-10",
   "owner":"admin",
   "priority":"5",
   "customFields":[
      {
         "key":"cf1",
         "values":[
            "cf value1",
            "cf value2"
         ]
      },
      {
         "key":"cf2",
         "values":[
            "cf2 value1",
            "cf2 value2"
         ]
      }
   ],
   "devices":[
      "FW_101",
      "FW_102"
   ],
   "requestedActions":[
      {
         "action":"create",
         "name":"networkObject1",
         "type":"network",
         "isGroup":"false",
         "values":[
            "1.1.1.1"
         ]
      },
      {
         "action":"create",
         "name":"serviceObject1",
         "type":"service",
         "isGroup":"false",
```

```
         "values":[
            "tcp/12"
         ]
      }
   ],
   "objectContainerLevel":"Automatic"
}
```

Add objects to group request example

```
{
 "template": "135: Object Change Multi Device Request",
 "subject": "Modify object request",
 "description": "adding objects to GR_Network_Devices",
 "externalId": "123a",
 "devices": ["FW_101", "FW_102"],

 "requestedActions": [
  {
   "action": "addObjectsToGroup",
   "name": "GR_Network_Devices",
   "type": "network",
   "isGroup": true,
   "values": ["Net_10.163.40.232_31", "HK_Cyberark_10.133.21.217"]
  }]
 "objectContainerLevel": "Automatic"
}
```

Multiple actions request example: replace content, remove objects from group, and delete

```
{

 "template": "135: Object Change Multi Device Request",
 "subject": "several actions",
 "devices": ["FW_101"],
 "requestedActions": [
```

```
  {
   "action": "replaceContent",
   "name": "object2",
   "type": "network",
   "isGroup": false,
   "values": ["10.20.160.111-10.20.160.125"]
  },

  {
   "action": "removeObjectsFromGroup",
   "name": "GP_Captical",
   "type": "network",
   "isGroup": true,
   "values": ["Net_211.72.241.0", "Net_61.219.22.0"]
  },

  {
   "action": "delete",
   "name": "Net_203.69.50.0",
   "type": "network",
   "isGroup": false
  }
 ],
 "objectContainerLevel": "Automatic"
}
```

(success)

```
{
 "status": "Success",
 "messages": [   {
 "code": "success",
 "message": "Success"
}],
"data":    {
 "changeRequestId": 4341,
 "redirectUrl":
"https://10.45.10.26/FireFlow/Ticket/Display.html?id=4341"
 }
}
```

(object not found failure)

```
{
 "status": "Failure",
 "messages": [{
   "code": "OBJECT_NOT_FOUND",
   "message": "On action: addObjectsToGroup the object: GR_Network_
Devices doesnt exist on devices: [FW_101] ([FW_102])."
  },
  {
   "code": "OBJECT_NOT_FOUND",
   "message": "On action: removeObjectsFromGroup the object: GP_Captical
doesnt exist on devices: [FW_101] ([FW_102])."
  },
  {
   "code": "OBJECT_NOT_FOUND",
   "message": "On action: delete the object: Net_203.69.50.0 doesnt exist
on devices: [FW_101] ([FW_102])."
  }
 ],
 "data": null
}              Response example
```

(create failure)

```
{
 "status": "Failure",
  "messages": [   {
   "code": "CREATE_ZONE_BASED_DEVICE_NOT_SUPPORT_GLOBAL_OBJECTS",
   "message": "Device 10_20_152_1 does not support global objects
(requested action line 1)."
  }],
  "data": null
}
```

Create a rule removal change request

The `ruleRemovalChangeRequest` creates a FireFlow change request to remove or disable a device rule, using the rule removal workflow.

FireFlow validates the API to ensure that mandatory elements are in place, such as permissions, template, date formats, and that any specified device exists in AFA.

Resource name: `/FireFlow/api/change-requests/rule-removal`

Request method: `POST`

Header requirements:

Parameter	Key	Type	Value
`Cookie`	`FireFlow_Session`	String	The `sessionId` retrieved in the authentication request.

Request query parameters:

Element		Type	Description
`template`		String	The name of the change request template to use.
`fields`			Array
	`name`	String	The name of a field in the Change Request. For example, enter **Owner** to set the value of the **Owner** field in the Change Request. FireFlow validates the API for mandatory elements, such **Note:** Each **devices** element can contain one device only, which must be a device from the lowest level in the AFA device tree. For more details, see: • Create a rule removal change request • Attachment field details • Date formats
	`values`	String	The value of the named field. For example, if you are defining the **Owner** field, enter a username or email address.
`requestActions`			Array

Element		Type	Description
	`action`	Array	Determines the action to take. One of the following: • **remove**. Removes the rule completely. • **disable**. Disables the rule but does not remove it. • **automatic**. Determines the rule action based on whether the device supports disabling rules. If the device supports disabling rules, the action is translated consistently as **disable**. However, if the device does not support disabling rules, the action is translated as **remove**. Each request supports one action only, even if it covers multiple rules. You cannot mix remove and disable actions for different rules.
	`ruleId`	String	The ID of the rule to remove or disable.

Date formats

The following date formats are supported:

- **DD-MM-YYYY**, when **DateDayBeforeMonth** =1
- **MM-DD-YYYY**, when **DateDayBeforeMonth**=0

Device names and rule IDs

If you are defining the device, you must enter the device database name, not the name displayed in the AFA device tree. Rule IDs must also be defined as the internal AFA IDs.

Retrieve both device database names and internal rule IDs using the following API:

https://<server_IP>/fa/server/rules/read?session=<FA_session_Id>&entity=<AFA_UI_display_name>

Any error messages that include the device name include the name displayed in AFA.

Attachment field details

The attachment field accepts single or multiple values, and expects the following syntax: **'filename=<filename>:content=<encoded file content to base64 string>'**

Additionally:

- Filenames must be valid Linux filenames, including valid characters only, no more than 255 characters, and not an empty string.
- Files must also have valid extensions, and not be of any file types listed in the **RestrictedFileExtensionsInAttachment** configuration.
- File content should be encoded to base 64.
- Before encoding, the file content should not exceed the maximum size configured in the **MaxAttachmentSize** configuration parameter.

Response:

Element		Type	Description
`status`		String	One of the following: • `Success` • `Failure`
`messages`			Array
	`code`	String	A string that indicates the response code.
	`message`	String	Further details about the response, if needed.
`data`			Array
	`changeRequestID`	String	The ID of the new Change Request created.
	`redirectURL`	String	A link to the new Change Request in FireFlow.

Rule removal request example:

```
{
"template": "140: Rule Removal Request",
  "fields":
```

```
    [    {
     "name":"subject",
     "values":[
     "subject1111"
    ]
    },
    {
    "name":"Owner",
    "values":[
     "sam@mycorp.com"
    ]
    },
    {
     "name": "devices",
     "values": ["<device ID>"]
    }
    ],
    "requestActions":
    [
    {
     "action": "remove",
     "ruleId": "<ruleID>"
    }
 ]}
}
```

Rule removal request example (multiple rules)

```
{
"template": "140: Rule Removal Request",
"fields":
[
{
"key": "subject",
"values": ["test55"]
},
{
"key": "devices",
"values": ["Orit_GW2"]
```

```
}
],
"requestActions":
[
{
"action": "remove",
"ruleId": "BC100ABA-446E-493B-9707-604C2A493676"
},
{
"action": "remove",
"ruleId": "88784DAF-C0A9-4B06-AE94-E8199A802EAC"
}
]
}
```

Rule removal response example (success)

```
{
 "status": "Success",
 "messages": [   {
  "code": "success",
  "message": "Success"
 }],
 "data":    {
  "changeRequestId": 3157,
  "redirectUrl":"https://<IP>/FireFlow/Ticket/Display.html?id=3157"
 }
}
```

Rule removal response example (failure)

```
{
 "status": "Failure",
 "messages": [   {
  "code": "DEVICES_NOT_FOUND",
  "message": "Cannot find devices: <device ID>."
 }],
```

```
 "data": null
}
```

Update a traffic change request's custom fields

The FireFlow REST API updates a Traffic Change Request's Custom Fields.

FireFlow validates the API to ensure that mandatory elements are in place, such as permissions, template, date formats, that any specified device exists in AFA, and so on.

Resource Name: `FireFlow/api/change-requests/traffic/{id}/fields`

Request Method: PUT

Request Path:

Element	Type	Description
`changeRequestID` *Mandatory*	Integer	ID of the Change Request.

Request Body:

A list of **key:value** fields where the key is the field name and the value is an array of update values.

For details, see Fields type.

Response: Response type

Request example

```
[
{
"key": "string",
"values": [
"string"
]
}
]
```

Get permitted request templates

The `templates` method gets a list of permitted change request templates.

Resource Name: `/FireFlow/api/templates`

Request Method: `GET`

Request Parameters: None

Response:

Element	Type	Description
`data`	Array of Objects	• description: String • enabled: Boolean • id: Integer • name: String • type: String - One of the AFF Change Request template types.
`messages`	Array of MessageDetails type	• code: String • message: String
`status`	String	One of the following: • Success • Failure

Response example

```
{
 "status": "Success",
 "messages": [
 {
  "code": "success",
  "message": "Success"
 }
],
"data": [
 {
  "id": 142,
```

```
  "name": "110: Multi-Approval Request",
  "description": "Create a traffic change request which requires multiple
approvals",
  "type": "Traffic Change",
  "enabled": true
  },
  {
   "id": 598,
   "name": "115: Automatic Traffic Change Request",
   "description": "Create a traffic change request that progresses
automatically",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 141,
   "name": "120: Generic request",
   "description": "Create a generic change request",
   "type": "Generic Change",
   "enabled": true
  },
  {
   "id": 219,
   "name": "130: Object Change Request",
   "description": "Create an object change request
   (add/remove/edit network and service objects)",
   "type": "Object Change",
   "enabled": true
  },
  {
   "id": 599,
   "name": "135: Object Change Multi Device Request",
   "description": "Create an object change request on multiple devices
   (add/remove/edit network and service objects)",
   "type": "Object Change Multi Device",
   "enabled": true
  },
  {
   "id": 307,
   "name": "140: Rule Removal Request",
   "description": "Create a change request for removing a device rule",
   "type": "Rule Removal",
   "enabled": true
```

```
  },
  {
   "id": 556,
   "name": "145: Rule Modification Request",
   "description": "Create change request for editing a device rule",
   "type": "Rule Modification",
   "enabled": true
  },
  {
   "id": 356,
   "name": "150: Parallel-Approval Request",
   "description": "Create a traffic change request which requires
parallel approvals",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 431,
   "name": "160: Web Filter-Change Request (Blue Coat)",
   "description": "Create a web-filter change request",
   "type": "Web Filter Change",
   "enabled": true
  },
  {
   "id": 566,
   "name": "170: Traffic Change Request (IPv6)",
   "description": "Create a request for IPv6 traffic change in Cisco
devices",
   "type": "Traffic Change IPv6",
   "enabled": true
  },
  {
   "id": 596,
   "name": "180: Traffic Change Request (Multicast)",
   "description": "Create a request for Multicast traffic change in Cisco
devices",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 597,
   "name": "190: Verbatim Rule Addition",
   "description": "Create a traffic change request for bulk rules
```

```
addition exactly as specified",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 601,
   "name": "BBB",
   "description": "",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 607,
   "name": "Duplicate Test",
   "description": "Create a basic change traffic request",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 550,
   "name": "Duplicate2",
   "description": "Create a basic change traffic request",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 608,
   "name": "Duplicate3",
   "description": "Create a basic change traffic request",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 609,
   "name": "Duplicate4",
   "description": "Create a basic change traffic request",
   "type": "Traffic Change",
   "enabled": true
  },
  {
   "id": 603,
   "name": "No Workflow",
   "description": "",
```

```
    "type": "Traffic Change",
    "enabled": true
   },
   {
    "id": 604,
    "name": "Test upgrade",
    "description": "Create a basic change traffic request",
    "type": "Traffic Change",
    "enabled": true
   },
   {
    "id": 600,
    "name": "aaa",
    "description": "",
    "type": "Traffic Change",
    "enabled": true
   }
  ]
 }
```


Get details for a specified change request

Returns full details about a specified change request, including custom fields configured for the template.

The data included in the response depends on whether the requested change request is a parent or child. We recommend first performing the API on a parent change request, and getting a full list of child requests. The list of child IDs is found in the **subChangeRequests** field in the response.

Perform the API again on each child request to get more details about those children.

For examples, see Sample response - parent change request and Example response - child change requests.

Resource Name: `/api/v1/getticket`

Request Method: GET

Request URL Parameters:

Element	Type	Description
`id` *Mandatory*	Integer	The ID of the change request you want to return data for.

Response:

Code	Description
200	Operation completed successfully
500	Failed to complete operation. The response includes an error message indicating the failure.

Sample request

```
https://12.34.5.67/FireFlow/api/change-requests/traffic/4595
```

Sample response - parent change request

In the following example, the **subChangeRequests** value shows that this change request has three child requests, with the IDs of **24**, **25**, and **26**.

```
{
"status": "Success",
"messages": [
 {
  "code": "success",
  "message": "Success"
 }
],
"data": {
 "id": 20,
 "subChangeRequests": [
  24,
  25,
  26
```

```
],
"fields": [
{
 "name": "Risk Level",
 "values": [
  "No Risk"
 ]
},
{
 "name": "Owner",
 "values": [
  "admin<admin@algosec.com>"
 ]
},
{
 "name": "Creator",
 "values": [
  "admin<admin@algosec.com>"
 ]
},
{
 "name": "Ticket Template Name",
 "values": [
  "Basic Change Traffic Request"
 ]
},
{
"name": "LastUpdated",
"values": [
 "2020-02-07 13:14:19"
 ]
},
```

```
{
 "name": "Requestor",
 "values": [
  "admin<admin@algosec.com>"
 ]
},
{
 "name": "Form Type",
 "values": [
 "Traffic Change"
 ]
},
{
 "name": "Risks Number",
 "values": [
  "0"
 ]
},
{
 "name": "Initial Plan status",
 "values": [
  "Result OK"
 ]
},
{
 "name": "Workflow",
 "values": [
  "Basic"
 ]
},
{
 "name": "status",
```

```
  "values": [
   "implement"
  ]
 }
],
"originalTraffic": [
 {
  "source": {
  "items": [
  {
  "value": "99.99.99.55",
  "fields": []
  }
 ]
},
 "destination": {
 "items": [
  {
  "value": "10.50.152.55",
  "fields": []
  }
 ]
},
 "service": {
 "items": [
 {
  "value": "tcp/22",
  "fields": []
  }
 ]
},
 "application": {
```

```
 "items": [
  {
  "value": "any",
  "fields": []
 }
]
 },
  "user": {
  "items": [
 {
  "value": "any",
  "fields": []
  }
 ]
},
 "fields": [],
 "natDetails": null,
 "action": "Drop"
 },
 {
  "source": {
  "items": [
 {
  "value": "any",
  "fields": []
 }
 ]
 },
  "destination": {
  "items": [
  {
   "value": "any",
```

```
    "fields": []
   }
  ]
 },
  "service": {
  "items": [
  {
   "value": "tcp/22",
   "fields": []
   }
  ]
  },
   "application": {
   "items": [
  {
   "value": "any",
   "fields": []
   }
  ]
 },
  "user": {
  "items": [
  {
   "value": "any",
   "fields": []
   }
  ]
 },
  "fields": [],
  "natDetails": null,
  "action": "Allow"
  }
```

```
],
"plannedTraffic": [
 {
  "source": {
  "items": [
 {
  "value": "99.99.99.55",
  "fields": []
  }
 ]
},
 "destination": {
 "items": [
 {
  "value": "10.50.152.55",
  "fields": []
 },
{
  "value": "10.50.152.56",
  "fields": []
  }
 ]
},
  "service": {
  "items": [
  {
   "value": "tcp/22",
   "fields": []
  }
 ]
},
  "application": {
```

```
  "items": [
  {
   "value": "any",
   "fields": []
  }
 ]
},
  "user": {
  "items": [
  {
   "value": "any",
   "fields": []
  }
 ]
},
 "fields": [],
 "natDetails": null,
 "action": "Drop"
  },
 {
  "source": {
  "items": [
  {
   "value": "any",
   "fields": []
  }
 ]
},
 "destination": {
 "items": [
  {
  "value": "any",
```

```
  "fields": []
  }
 ]
},
 "service": {
 "items": [
 {
  "value": "tcp/22",
  "fields": []
 }
]
},
 "application": {
 "items": [
  {
  "value": "any",
  "fields": []
  }
]
 },
  "user": {
  "items": [
  {
   "value": "any",
   "fields": []
   }
  ]
   },
    "fields": [],
    "natDetails": null,
    "action": "Allow"
   }
```

```
  ]
 }
}
```

Example response - child change requests

In the following example, the **subChangeRequests** value is null because this is a child request with no further children.

```
{
"status": "Success",
"messages": [
{
"code": "success",
"message": "Success"
}
],
"data": {
"id": 24,
"subChangeRequests": null,
"fields": [
 {
  "name": "Owner",
  "values": [
   "admin<admin@algosec.com>"
  ]
 },
 {
  "name": "Creator",
  "values": [
   "admin<admin@algosec.com>"
  ]
 },
```

```
{
 "name": "Devices",
 "values": [
  "10_20_150_3_puma_algosec_com_root_default"
 ]
},
{
 "name": "Ticket Template Name",
 "values": [
  "Basic Change Traffic Request"
 ]
},
{
 "name": "LastUpdated",
 "values": [
  "2020-02-07 14:00:13"
 ]
},
{
 "name": "Workflow",
 "values": [
  "Basic"
 ]
},
{
 "name": "status",
 "values": [
  "implement"
 ]
},
{
 "name": "Requestor",
```

```
  "values": [
   "admin<admin@algosec.com>"
  ]
 },
 {
  "name": "Form Type",
  "values": [
   "Traffic Change"
  ]
 }
 ],
"plannedTraffic": [
 {
  "source": {
  "items": [
{
"value": "any",
"fields": []
   }
  ]
 },
 "destination": {
  "items": [
  {
   "value": "any",
   "fields": []
  }
 ]
},
 "service": {
  "items": [
 {
```

```
  "value": "tcp/22",
  "fields": []
  }
 ]
},
"application": {
 "items": [
 {
  "value": "Any",
  "fields": []
  }
 ]
},
 "user": {
 "items": [
 {
  "value": "Any",
  "fields": []
  }
 ]
},
  "fields": [],
  "natDetails": null,
  "action": "Allow"
   }
  ]
 }
}
```


FireFlow data types

The following is a reference of FireFlow data types used in the FireFlow REST API:

- customFields type
- actionInformation type
- AddObjectsToGroup type
- Create type
- Delete type
- Fields type
- MessageDetails type
- NatDetails type
- ObjectChangeRequestDetails type
- RemoveObjectsFromGroup type
- Response type
- TrafficChangeRequest type
- TrafficFieldDetails type
- TrafficItemDetails type
- TrafficLineDetails type

customFields type

Element	Type	Description
`key`	String	The custom field's key.
`values`	A list of stings	A list of values for the custom field. Even if there is only one value, this must be in a list.

➔ See also:

- FireFlow data types

actionInformation type

Element	Type	Description
`action`	String	One of the following: • addObjectsToGroup • removeObjectsFromGroup • create • delete • replaceContent
`name`	String	The name of the object.
`type`	String	One of the following: • network • service
`isGroup` **Note:** This element is not required when adding or removing objects from a group.	String	One of the following: • `true`. If the object is a group. • `false`. If the object is not a group.
`content` **Note:** This element is not required when deleting an object.	list of strings	List of the object's content.

➔ See also:

- FireFlow data types

AddObjectsToGroup type

Element	Type	Description
`devices`	Array of String	List of devices.
`lineOrder`	Integer	Line order number.
`name`	String	Name of group.

objectContainers	Array of Integer	List of object container IDs.
type	String	One of the following: • network • service
values	Array of String	List of values.

➔ See also:

- AFA data types

Create type

Element	Type	Description
devices	Array of String	List of devices.
lineOrder	Integer	Line order number.
name	String	
objectContainers	Array of Integer	List of object containers IDs.
type	String	One of the following: • network • service
group	Boolean	Whether device belongs to a group.
isGroup	Boolean	Whether this is a group.
values	Array of String	List of values.

➔ See also:

- AFA data types

Delete type

Element	Type	Description

devices	Array of String	List of devices to delete.
lineOrder	Integer	
name	String	
objectContainers	Array of Integer	List of object containers.
type	String	One of the following: • network • service

➔ See also:

- AFA data types

Fields type

Element	Type	Description
`key`	String	Name of field.
`values`	Array of String	Values for field.

➔ See also:

- AFA data types

MessageDetails type

Element	Type	Description
`code`	String	Message code.
`message`	String	Message text.

➔ See also:

- AFA data types

NatDetails type

Element	Type	Description
destination	Array of String	List of destinations.
port	Array of String	List of ports.
source	Array of String	List of sources.
type	String	One of the following: • Static • Dynamic • None

➔ See also:

- AFA data types

ObjectChangeRequestDetails type

Element	Type	Description
`attachments`	Array of String	List of attachments.
`cc`	Array of String	List of CCs.
`description`	String	Change Request description.
`device`	Array of String	List of devices. For example: ["VR-ls-Quality-Assurance-default"]
`domain`	String	Domain.
`due`	String	Due date.
`expire`	String	Expiration date.
`externalId`	String	External ID.
`owner`	String	Owner.
`priority`	String	Priority of Change Request.

Element	Type	Description
`referredBy`	Array of String	List of referred bys.
`refersTo`	Array of String	List of refer tos.
`requestedActions` *Mandatory*	Array of Action type	List of requested actions.
`requestor`	String	Requestor.
`subject`	String	Subject for Change Request. For example: "Multi Object Change Request"
`template` *Mandatory*	String	Name of template to use. For example: "135: Object Change Multi Device Request".
`customFields` *Mandatory*	Array ofFields type	List of custom fields and values.
`objectContainers` *Mandatory*	Array of Integer	List of object container IDs.
`objectContainerLevel`	String	Object container level: • Lowest • Highest • Automatic

➔ See also:

- FireFlow data types

RemoveObjectsFromGroup type

Element	Type	Description
devices	Array of String	List of devices.

Element	Type	Description
lineOrder	Integer	Sequence
name	String	Name.
objectContainters	Array of Integer	List of object container IDs.
type	String	One of the following: • network • service
values	Array of String	List of values.

➔ See also:

- AFA data types

Response type

Element	Type	Description
`data`	String	Depending on API, a unique response object or array of objects.
`message`	Array of MessageDetails type	List of response messages.
`status`	String	One of the following: • Success • Failure

➔ See also:

- FireFlow data types

TrafficChangeRequest type

Element	Type	Description
template *Mandatory*	String	Name of template.
traffic *Mandatory*	Array of TrafficLineDetails	Traffic details.
fields *Mandatory*	Array of Fields type	Ticket fields.

➔ See also:

- AFA data types

TrafficFieldDetails type

Element	Type	Description
items	Array of TrafficItemDetails type	Traffic items.

➔ See also:

- AFA data types

TrafficItemDetails type

Element	Type	Description
customFields	Array of Fields type	List of custom fields.
name	String	

➔ See also:

- AFA data types

TrafficLineDetails type

Element	Type	Description
action	String	Action.
source	TrafficFieldDetails type	
destination	TrafficFieldDetails	
service	TrafficFieldDetails type	
application	TrafficFieldDetails type	
user	TrafficFieldDetails type	
customFields	Array of Fields type	
natDetails	NatDetails type	

➔ See also:

- AFA data types

FireFlow SOAP web services

This section describes the FireFlow SOAP web services API.

The FireFlow WSDL file

The FireFlow Web service's WSDL file is available at `https://<algosec_server>/WebServices/FireFlow.wsdl` where `<algosec_server>` is the AFA/FireFlow server URL.

Web services API reference

FireFlow offers SOAP Web Services. This API allows you to integrate FireFlow functionality into external applications.

The standard SOAP request envelope header for FireFlow is:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ff="https://www.algosec.com/ff-ws">   <soapenv:Header/>
```

Note: All methods require a session key which is obtained with the `authenticate` method. Web Services API can use LDAP or Radius authentication, or Single Sign On (SSO).

The AFF SOAP interface supports the following methods:

- `authenticate` - See Starting a Session (see Starting a Session).
- `isSessionAlive` - See Verifying a Session is Active (see Verifying a Session is Active).
- `createTicket` - See Creating a Change Request (see Creating a Change Request).
- `getTicket` - See Retrieving a Change Request (see Retrieving a Change Request).
- `getFields` - See Retrieving Information From a Change Request (see Retrieving Information from a Change Request).

- `addObjectCustomField` - See Adding Values to a Custom Field in an Object (see Adding Values to a Custom Field in an Object).
- `deleteObjectCustomField` - See Deleting All Values for a Custom Field in an Object (see Deleting All Values for a Custom Field in an Object).
- `updateObjectCustomField` - See Updating a Custom Field in an Object (see Updating a Custom Field in an Object).

If the method's operation is successful, the method response returns data items or an indication of success. If the method's operation was not successful, the response indicates that a SOAP fault has been thrown. See Faults (see Faults) for a list of likely faults.

➔ See also:

- Sample: create a change request

Work with change requests

The following methods create and retrieve information for change requests.

Note: Change request responses only present changes from the last report and do not represent changes accumulated over a period of time.

Creating a Change Request

The `createTicket` method creates a new FireFlow change request.

Request Type: `createTicket`

Element	Type	Description
`FFWSHeader` *Mandatory*	`FFWSHeader`	Header information. See FFWSHeader Type (see FFWSHeader Type).
`sessionId` *Mandatory*	String	Client's session identifier.

Element	Type	Description
`ticket` *Mandatory*	`ticket`	A `Ticket` object. See Ticket Type (see Ticket Type).

Response Type: `createTicketResponse`

Element	Type	Description
`result` *Mandatory*	Integer	Method result. A value of 1 indicates success.
`message` *Mandatory*	String	A message describing the result.
`ticketId` *Optional*	Integer	ID number of newly created change request.

Retrieving a Change Request

The `getTicket` method retrieves a change request by its ID.

Request Type: getTicket

Element	Type	Description
`FFWSHeader` *Mandatory*	`FFWSHeader`	Header information. See FFWSHeader Type (see FFWSHeader Type).
`sessionId` *Mandatory*	String	Client's session identifier.
`ticketId` *Mandatory*	Integer	ID of requested change request.

Response Type: getTicketResponse

Element	Type	Description
`result` *Mandatory*	Integer	Method result. A value of 1 indicates success.
`ticket` *Optional*	`ticket`	Requested change request. See Ticket Type (see Ticket Type).
`subTicketIds` *Optional*	List of Integer	IDs of change request's sub requests, if any.
`parentTicketId` *Optional*	Integer	ID of the change request's parent request, if exists.

Retrieving Information from a Change Request

The `getFields` method retrieves the content of specific change request fields, by change request ID and field name. For the list of valid fields, see Supported Change Request Field Names (see Supported Change Request Field Names).

Request Type: `getFields`

Element	Type	Description
`FFWSHeader` *Mandatory*	`FFWSHeader`	Header information. See FFWSHeader Type (see FFWSHeader Type).
`sessionId` *Mandatory*	String	Client's session identifier.
`ticketId` *Mandatory*	Integer	ID of requested change request.
`fields` *Mandatory*	`fields`	Requested fields. See Fields Type (see Fields Type).

Response Type: `getFieldsResponse`

Element	Type	Description
`result` *Mandatory*	Integer	Method result. A value of 1 indicates success.
`fields` *Optional*	List of `customField` objects	Returned field values, along with the field's name. See CustomField Type (see CustomField Type).

Request example:

```
<getFields>
    <FFWSHeader>
      <version>1</version>
      <opaque></opaque>
    </FFWSHeader>
    <sessionId>cf420f27e1bd47ec80587aee288f49ca</sessionId>
    <ticketId>1</ticketId>
    <fields>
```

```
      <key>status</key>
      <key>owner</key>
      <key>owning group</key>
      <key>My Custom Field</key>
    </fields>
</getFields>
```

Response example:

```
<getFieldsResponse>
    <result xsi:type="xsd:int">1</result>
    <fields>
      <key>status</key>
      <values>approve</values>
    </fields>
    <fields>
      <key>owner</key>
      <values>admin</values>
    </fields>
    <fields>
      <key>owning group</key>
      <values>Security</values>
    </fields>
    <fields>
      <key>My Custom Field</key>
      <values>value of My Custom Field</values>
    </fields>
</getFieldsResponse>

<getFieldsResponse>
    <result xsi:type="xsd:int">1</result>
    <fields>
      <key>status</key>
      <values>approve</values>
    </fields>
    <fields>
      <key>owner</key>
      <values>admin</values>
    </fields>
    <fields>
      <key>owning group</key>
      <values>Security</values>
    </fields>
    <fields>
```

```
      <key>My Custom Field</key>
      <values>value of My Custom Field</values>
    </fields>
</getFieldsResponse>
```

Managing the Session

The following methods control a Web Service session.

Starting a Session

The `authenticate` method authenticates a user. Once authenticated, the client will receive a session identifier. This identifier will be required as proof of authentication for future requests.

Request Type: `authenticate`

Element	Type	Description
`FFWSHeader` *Mandatory*	`FFWSHeader`	The header information. See FFWSHeader Type (see FFWSHeader Type).
`username` *Mandatory*	String	The client's username.
`password` *Mandatory*	String	The client's password in cleartext.

Response Type: `authenticateResponse`

Element	Type	Description
`result`*Mandatory*	Integer	Authentication result. A value of 1 indicates success.
`sessionId`*Mandatory*	String	Session identifier.
`faSessionId`*Optional*	String	AFA session identifier.
`phpSessionId` *Optional*	String	PHP session identifier.

Element	Type	Description
`faToken` *Optional*	String	AFA token.

Verifying a Session is Active

The `isSessionAlive` method verifies that the current session is alive.

Request Type: **`isSessionAlive`**

Element	Type	Description
`FFWSHeader` *Mandatory*	`FFWSHeader`	The header information. See FFWSHeader Type (see FFWSHeader Type).
`sessionId` *Mandatory*	String	The client's session identifier.

Response Type: **`isSessionAliveResponse`**

Element	Type	Description
`result` *Mandatory*	Integer	Method result. A value of 1 indicates the session is still active.

Working with Custom Fields

The following methods manage values of custom fields for a ticket, user, or group object.

Adding Values to a Custom Field in an Object

The `addObjectCustomField` method adds one or more values to a custom field in a specific object, such as a ticket, user, or group.

Note: If the maximum number of values for a field is exceeded, existing field values are deleted.

Request Type: addObjectCustomField

Element	Type	Description
`sessionId` *Mandatory*	String	Client's session identifier.
`objectType` *Mandatory*	String	Type of object: ■ ticket ■ user ■ group
`objectID` *Mandatory*	Integer	ID of the ticket, user, or group.
`customFields` *Mandatory*	List of `customField`	One or more custom field objects. See CustomField Type (see CustomField Type).

Response Type: addObjectCustomField

Element	Type	Description
`result` *Mandatory*	Integer	Method result. A value of 1 indicates success. Possible failure values are: ■ Session not authenticated ■ Bad object ID ■ Bad custom field name ■ Action failed

Deleting All Values for a Custom Field in an Object

The `deleteObjectCustomField` method deletes all values of one or more custom fields for a specific object, such as a ticket, user, or group.

Request Type: deleteObjectCustomField

Element	Type	Description
`sessionId` *Mandatory*	String	Client's session identifier.

Element	Type	Description
`objectType` *Mandatory*	String	Type of object: ■ ticket ■ user ■ group
`objectID` *Mandatory*	Integer	ID of the ticket, user, or group.
`customFields` *Mandatory*	List of `customField`	One or more custom field objects. See CustomField Type (see CustomField Type).

Response Type: deleteObjectCustomField

Element	Type	Description
`result` *Mandatory*	Integer	Method result. A value of 1 indicates success. Possible failure values are: ■ Session not authenticated ■ Bad object ID ■ Bad custom field name ■ Action failed

Updating a Custom Field in an Object

The `updateObjectCustomField` method replaces the value of one or more custom fields for a specific object, such as a ticket, user, or group.

Request Type: updateObjectCustomField

Element	Type	Description
`sessionId` *Mandatory*	String	Client's session identifier.

Element	Type	Description
`objectType` *Mandatory*	String	Type of object: ■ ticket ■ user ■ group
`objectID` *Mandatory*	Integer	ID of the ticket, user, or group.
`customFields` *Mandatory*	List of `customField`	One or more custom field objects. See CustomField Type (see CustomField Type).

Response Type: updateObjectCustomField

Element	Type	Description
`result` *Mandatory*	Integer	Method result. A value of 1 indicates success. Possible failure values are: ■ Session not authenticated ■ Bad object ID ■ Bad custom field name ■ Action failed

FireFlow SOAP data types

Described below are the data types passed in FireFlow's Web Service messages.

- FFWSHeader Type
- Fields Type
- ObjectChangeLine Type
- Ticket Type
- TrafficLine Type
- TrafficAddress Type
- TrafficService Type

- TrafficNAT Type
- Attachment Type
- CustomField Type

FFWSHeader Type

The following table describes the elements in the `FFWSHeader` type object.

Element	Type	Description
`version` *Mandatory*	String	The API version.
`opaque` *Optional*	String	A value that will be echoed in the response. This value must be a maximum of 1024 characters in length.

➔ See also:

- FireFlow SOAP data types

Fields Type

The following table describes the elements in the `fields` type object:

Element	Type	Description
`key` *Optional*	List of String	List of field names. For valid keys, see Supported Change Request Field Names (see Supported Change Request Field Names).

➔ See also:

- FireFlow SOAP data types

ObjectChangeLine Type

The following table describes the elements in the `objectChangeLine` type object:

Element	Type	Description

`action`
Mandatory
	String	Object change action. One of the following:
		`new`
		`delete`
		`edit`
		`addValues`
		`removeValues`
		See Actions for Service Objects (see Actions for Service Objects) and Actions for Network Objects (see Actions for Network Objects).

`objectType`
Mandatory
	String	Type of object. One of the following values:
		`network`
		`service`

`objectName` *Mandatory*	String	Name of object on which to perform action. See Actions for Service Objects (see Actions for Service Objects) and Actions for Network Objects (see Actions for Network Objects).
`actionTarget` *Mandatory*	String	Target of action. See Actions for Service Objects (see Actions for Service Objects) and Actions for Network Objects (see Actions for Network Objects).
`values` *Mandatory* or *Optional* depending on action	List of String	Values. See Actions for Service Objects (see Actions for Service Objects) and Actions for Network Objects (see Actions for Network Objects).
`customFields` *Optional*	List of `customField` objects	List of user-defined custom fields for object change requests. See CustomField Type (see CustomField Type).

Element	Type	Description
`scope` *Optional*	Integer	Scope. If not provided, device determines scope. ■ 1 = Global ■ 0 = Local **Note:** It is possible to set Global scope for object change requests on local devices (e.g., modules), but it is *not* possible to set Local scope for object change requests on global devices (e.g., Check Point PV1).

Actions for Network Objects

action	device	actionTarget	values	objectName	Description
		host	Single IP		
		group	List of objects.		
	Check Point	network	Single network (CIDR).	Name for new object that does not exist on device.	Create a new network object on device with requested values.
`new`		range	Single range.		
	Non-Check Point	object (not required)	List of IPs.		
		host			
		group			
	Check Point	network			

action	device	actionTarget	values	objectName	Description
`delete`		range	Not required.	Name of existing object on device.	Delete object with given name.
	Non-Check Point	object (not required)			
`addValues`	Check Point	group	List of network objects that do not belong to group.	Name of existing group.	Add values to an existing object.
	Non-Check Point	object (not required)	List of IPs that do not belong to object.	Name of existing object.	
`removeValues`	Check Point	group	List of network objects that belong to group.	Name of existing group.	Remove values from an existing object.
	Non-Check Point	object (not required)	List of IPs that belong to object.	Name of existing object.	
		host	Single IP.		
	Check Point	network	Single network (CIDR).	Name of existing object.	Replace existing value in object with new one.
`edit`		range	Single IP range.		

action	device	actionTarget	values	objectName	Description
	Non-Check Point	`edit` is not currently supported for network change requests on non-Check Point devices.			

Actions for Service Objects

action	actionTarget	values	objectName	Description
`new`	service_group	List of service objects.	Name for new service object that does not exist on device.	Create a new service object on device with specified values.
	service_non_group	Single service.		
`delete`	service_object	Not required.	Name of existing object.	Delete object with given name.
`addValues`	service_group	List of service objects that do not belong to group.	Name of existing group.	Add values to an existing object.
`removeValues`	service_group	List of service objects that belong to group.	Name of existing group.	Remove values in from an existing object.
`edit`	service_non_group	Single service.	Name of existing object.	Replace existing value in object with new one.

➔ See also:

- FireFlow SOAP data types

Ticket Type

The following table describes the elements in a `ticket` type object.

Element	Type	Description
`template` *Mandatory*	String	Ticket template.
`attachments` *Optional*	A list of `attachment` objects	A list of attachments. See Attachment Type (see Attachment Type).
`cc` *Optional*	List of String	A list of email addresses to which the FireFlow system should send copies.
`customFields` *Optional*	List of `customField` objects	A list of user-defined custom fields. See CustomField Type (see CustomField Type).
`description` *Optional*	String	A free text description of the issue.
`devices` *Mandatory* - object change *Optional* - traffic change	List of String	A list of device names, on which the change should be made. **Note:** ■ In traffic change requests, `devices` can be empty, a single value or multiple values. ■ In a createTicket (see Creating a Change Request) with multiple devices, sub requests will be created. ■ In a getTicket (see Retrieving a Change Request) for a parent ticket, multiple devices (all sub request devices) will be returned. ■ In object change requests, `devices` *must* have exactly *one* value.
`due` *Optional*	String	The date by which this change request should be resolved, in the format: `date, GMT`.

Element	Type	Description
`expire` *Optional*	String	The date on which this change request will expire, in the format: `date, GMT`.
`externalId` *Optional*	String	The ID number of an external system change request to which this change request should be linked.
`owner` *Optional*	String	The email address of the change request owner.
`priority` *Optional*	Integer	A number indicating this request's priority, where 0 indicates lowest priority.
`refersTo` *Optional*	Integer	The ID number of a change request to which this change request refers.
`referredBy` *Optional*	Integer	The ID numbers of a change request that refer to this change request.
`requestor` *Mandatory*	String	The email address of the requestor.
`subject` *Mandatory*	String	The change request's title.
`trafficLines` *Optional*	List of `trafficLine` objects	A list of traffic lines. See TrafficLine Type (see TrafficLine Type). **Note:** Relevant only for traffic change requests. In getTicket (see Retrieving a Change Request), if the change request has planned traffic changes as well as requested traffic changes, the planned traffic lines will be returned here.

Element	Type	Description
`objectChangeLines` *Optional*	List of `objectChangeLine` objects	A list of object change lines. See ObjectChangeLine Type (see ObjectChangeLine Type). **Note:** Relevant only for object change tickets. In getTicket (see Retrieving a Change Request), if the change request has planned object changes as well as requested object changes, the planned object change lines will be returned here.
`status` *Optional*	String	Change status. Only relevant for a change request returned by getTicket (see Retrieving a Change Request). Statuses passed to createTicket (see Creating a Change Request) will be ignored.
`id` *Optional*	Integer	Change request ID.

➔ See also:

- FireFlow SOAP data types

TrafficLine Type

The following table describes the elements in the `trafficLine` type object for a single traffic line in a FireFlow change request.

Element	Type	Description
`trafficSource` *Mandatory*	List of `trafficAddress` objects	A list of source IP addresses. See TrafficAddress Type (see TrafficAddress Type).

Element	Type	Description
`trafficDestination` *Mandatory*	List of `trafficAddress` objects	A list of destination IP addresses. See TrafficAddress Type (see TrafficAddress Type).
`trafficService` *Mandatory*	List of `trafficService` objects	A list of traffic services. See TrafficService Type (see TrafficService Type).
`nat` *Optional*	`trafficNAT`	NAT for the defined traffic. See TrafficNAT Type (see TrafficNAT Type).
`action` *Mandatory*	Integer	The device action to perform for the traffic. This can be either of the following: ■ `1` – Allow the traffic ■ `0` – Block the traffic
`customFields` *Optional*	List of `customField` objects	A list of custom fields. See CustomField Type (see CustomField Type).

➔ See also:

- FireFlow SOAP data types

TrafficAddress Type

The following table describes the elements in the `trafficAddress` type object.

Element	Type	Description
`address` *Mandatory*	String	The IP address, IP range, network, device object, or DNS name of the connection source.
`customFields` *Optional*	List of `customField` objects	A list of custom fields. See CustomField Type (see CustomField Type).

➔ See also:

- FireFlow SOAP data types

TrafficService Type

The following table describes the elements in the `trafficService` type object.

Element	Type	Description
`service` *Mandatory*	String	The device service or port for the connection, for example, "http" or "tcp/123".
`customFields` *Optional*	List of `customField` objects	A list of custom fields. See CustomField Type (see CustomField Type).

➔ See also:

- FireFlow SOAP data types

TrafficNAT Type

The following table describes the elements for the `trafficNat` type object which represents the Network Address Translation (NAT) information for a traffic line.

Element	Type	Description
`source` *Mandatory*	String	The source NAT value after translation.
`destination` *Mandatory*	String	The destination NAT value after translation.
`port` *Mandatory*	String	The port value after translation.
`type` *Optional*	Integer	The type of NAT. The possible values are: ■ `0` – Static NAT ■ `1` – Dynamic NAT

➔ See also:

- FireFlow SOAP data types

Attachment Type

The following are the elements for an `attachment` type object in a FireFlow change request.

Element	Type	Description
`fileName` *Mandatory*	String	Name of the file.
`fileContent` *Mandatory*	String	Contents of the file encoded in base 64.

➔ See also:

- FireFlow SOAP data types

CustomField Type

The following are the elements for a `customField` type object in a FireFlow change request.

Element	Type	Description
`key` *Mandatory*	String	Custom field name. For valid keys, see Supported Change Request Field Names (see Supported Change Request Field Names).
`values` *Optional*	List of String	Custom field values.

Supported Change Request Field Names

The following field names are supported to use as the `key` parameter in the `customField` type object:

- User-defined fields under the category '`additional`'.

Note: The *name* of the fields should be used, not the *display name*.

- The following FireFlow fields:
- id
- status
- subject
- requestor

- owner
- cc
- due
- expire
- priority
- devices
- template
- description
- externalId
- refersTo
- refferedBy
- owning group
- additional responsible groups

➔ See also:

- FireFlow SOAP data types

Faults

The returned SOAP fault name is `FireFlowError`.

The following are some of the likely faults that may be thrown on error:

- Session ID is not ID of an active session:
- Code: soap:Authentication
- String: Authentication Failed
- Error occurs during ticket loading and ticket is not returned:
- Code: soap:System
- String containing explanation of fault

- Request has unsupported fields:
- Code: soap:Validation
- String containing explanation of fault

The following example is for a fault thrown when the user does not have permissions on the firewall.

```
<SOAP-ENV:Body>
   <SOAP-ENV:Fault>
      <faultcode>ns1:FF-WS</faultcode>
      <faultstring>[710]  [device [fw3] is not in the list of permitted
devices]</faultstring>
      <faultactor>FF Web Service</faultactor>
      <detail>
         <ns1:ErrorDetails>
            <code>710</code>
            <description>[710]  [device [fw3] is not in the list of
permitted
devices]</description>
         </ns1:ErrorDetails>
      </detail>
   </SOAP-ENV:Fault>
</SOAP-ENV:Body>
```

Sample: create a change request

The following example shows how to create a change request in Python version 2.6.

Note: Before using this example, replace the username, password, and ticket source values with your own values.

You may have to remove some manual line breaks.

```
import ssl
from suds.client import Client

AlgoSecServer=10.20.6.88'
```

```
AlgoSecUser='user'
AlgoSecPasswd='password'
TicketSource='125.125.22.11'
TicketDest='10.0.0.0/8'

# Action - 0 for drop, 1 for allow
TicketAction='0'
TicketService='*'
ActionStr = 'Allow'

ActionStr = 'Allow' if TicketAction == '1' else 'Drop'

# bypass ssl verification - needed only if using self-signed certificates
 (demo machine, etc.)
#ssl._create_default_https_context = ssl._create_unverified_context

# ALGOSEC AFF WSDL is availble here
'https://AFFIP/WebServices/FireFlow.wsdl'
AFF_WSDL = 'https://%s/WebServices/FireFlow.wsdl' % AlgoSecServer

# Setup client
client = Client(AFF_WSDL)

try:
  # Authenticate
  authenticate = client.service.authenticate(username=AlgoSecUser,
password=AlgoSecPasswd)

  # Create ticket and traffic lines objects
  print "Creating change request with source <%s> destination <%s>
service <%s> and
action <%s>" % (TicketSource, TicketDest, TicketService, ActionStr)

  ticket = client.factory.create('ticket')
  trafficLine = client.factory.create('trafficLine')

  src = client.factory.create('trafficAddress')
  src.address=TicketSource
  trafficLine.trafficSource.append(src)

  dst =client.factory.create('trafficAddress')
  dst = client.factory.create('trafficAddress')
  dst.address=TicketDest
```

```
  trafficLine.trafficDestination.append(dst)

  srv = client.factory.create('trafficService')
  srv.service=TicketService
  trafficLine.trafficService.append(srv)

  trafficLine.action=TicketAction

  ticket.trafficLines.append(trafficLine)
  ticket.description='Demo Ticket'
  ticket.requestor='ned@algosec.com'
  ticket.subject='%s Traffic from %s to %s' % (ActionStr, TicketSource,
TicketDest)

except:
  print "A problem occured"

# Actually create the ticket
try:
  ticket_added = client.service.createTicket
(sessionId=authenticate.sessionId,
ticket=ticket)

except:
  print ticket_added.message

# Print success message and ticket URL
print ticket_added.message
print ticket_added.ticketDisplayURL
```

AppViz REST web services

This section describes the AppViz REST web services APIs.

Base URL

The base URL for all REST requests is the following:

```
https://<algosec_server>/BusinessFlow/rest/v1
```

where `<algosec_server>` is the AppViz server URL.

Some of the requests provided in this API are restricted for users with specific permissions. For details, see AppViz Permissions .

Note: Every request must be in JSON format. Each request must include the `content-type` header with the value `application/json`.

Note: The AppViz REST API allows authenticating each request with full credentials or authenticating with a cookie provided by the `login` method. See Logging In (see Logging In). If you choose to authenticate with a cookie, but you are using a development platform that does not automatically handle cookies, you must manually add the cookie. For every request, add a header with the name `Cookie` and the value `JSESSIONID=<jsessionid>`, where `<jsessionid>` is the session ID provided in the response body of the `login` method

Swagger

The AppViz RESTful API includes Swagger support, enabling you to execute simplified API request calls and access full lists of request parameters.

To access Swagger API documentation:

1. In the toolbar, click your username and click **API Documentation**.
2. From the dropdown at the top-right, click **AlgoSec_AppViz**.

AppViz REST API reference

AppViz supports the following REST APIs:

- Logging In
- Logging Out
- /applications
- /network_objects
- /network_services
- /settings/permissions
- Import vulnerability data

➔ See also:

- Add/Remove
- AppViz Permissions
- Request for application flows example

Logging In

To perform many requests, you can authenticate with an authentication cookie. You obtain the cookie with the method described below.

Every request must be in JSON format. Each request must include the `content-type` header with the value `application/json`.

Note: If you are using a development platform that does not automatically handle cookies, you must manually add a header (to every request) with the name `Cookie` with the value `JSESSIONID=<jsessionid>`, where `<jsessionid>` is the session ID provided in the response body of the `login` method.

Note: For a single API call, you can submit any request without logging in. You can send the request with a basic authorization header. Authentication will be for the

individual request only and will not create an authentication cookie/session ID that can be used for other requests.

Resource Name: `/login`

Request Method: POST

Request Header:

Header	Value
`Authorization`	`Basic <encoded_credentials>` where `<encoded_credentials>` is `<user name>:<password>` encoded in base64.

Response Body:

Element	Type	Description
`JSESSIONID`	String	The session ID.

Logging Out

If you obtained an authentication cookie by logging in, you can nullify it with the following method.

Resource Name: `/logout`

Request Method: POST

Response:

Element	Type	Description

`success`	String	One of the following:
		`true`
		`false`

`message`	String	A message indicating the result of the REST call.

Error Codes

When errors occur, a JSON status object and an HTTP status code are returned.

HTTP Status codes:

- 200 - When returning a correct result of an empty set.
- 404 - When an object is not found or the address is incorrect.
- 403 - When the user used for authentication does not have permissions to view a certain object.
- 500 - All other errors.

/applications

The following are requests for application related resources. The base URL for applications is `/BusinessFlow/rest/v1/applications`.

AppViz application GET APIs

- Applications: GET /
- Applications: GET /{id}
- Applications: GET /id/{application_id}/revisions
- Applications: GET /id/{application_id}
- Applications: GET /{id}/authorized_users_and_roles
- GET /{id}/change_requests
- GET /{id}/contacts
- GET /{id}/flows
- GET /{id}/flows/{flowid}
- GET /{id}/revisions
- GET /{id}/vulnerabilities
- GET /name/{appName}
- GET /{id}/risks
- GET /{id}/flows/{flowId}/risks

AppViz application POST APIs

- POST /{id}/apply
- POST /{id}/check_connectivity
- POST /{id}/contacts
- POST /{id}/custom_fields
- POST /{id}/decommission
- POST /{id}/discard
- POST /{id}/flows
- POST /{id}/flows/{flowid}/check_connectivity
- POST /{id}/labels
- POST /{id}/resolve
- POST /new
- POST /{id}/flows/new

AppViz application DELETE APIs

- DELETE /{id}/contacts
- DELETE /{id}/custom_fields
- DELETE /{id}/flows/{flow_id}
- DELETE /{id}/labels

Applications: GET /

Returns a list of all applications.

Returns: An array of Applications. For details, see Application .

➔ See also:

- /applications

Applications: GET /{id}

Returns a single application revision.

Parameters

id. The application revision ID.

Returns

An application. For details, see Application .

➔ See also:

- /applications

Applications: GET /id/{application_id}/revisions

Returns all revisions for the application ID.

Parameters

application_id. The application ID.

Returns

An array of **ApplicationRevision** data. For details, see ApplicationRevision .

➔ See also:

- /applications

Applications: GET /id/{application_id}

Returns the latest revision for the application ID.

Parameters

application_ID. The application ID.

Returns

An application. For details, see Application .

➔ See also:

- /applications

Applications: GET /{id}/authorized_users_and_roles

Gets lists of users and roles that are permitted to view and/or edit a specific application.

Resource name

```
/applications/{id}/authorized_users_and_roles
```

Permissions required

Administrator

Request URL parameters

Parameter	Type	Description
id *Mandatory*	Integer	The application's revision ID.

Returns

Parameter	Type	Description
applicationName	String	Application name.
usersView	Array of String	List of users allowed to view the application.
usersEdit	Array of String	List of users allowed to edit the application.
rolesView	Array of String	List of roles allowed to view application.
rolesEdit	Array of String	List of roles allowed to edit application

Return example

```
{
  "applicationName": "DNS",
  "usersView": [
```

```
      "harry-helpdesk",
      "sue"
    ],
    "rolesView": [
      "dns-applications"
    ],
    "rolesEdit": [
      "admin",
      "reviewer"
    ]
  }
```

➔ See also:

- /applications

GET /{id}/change_requests

Returns a list of change requests for an application revision.

- **Parameters**:

id - The application revision ID.

- **Return**:

Array of ChangeRequest (see ChangeRequest)

➔ See also:

- /applications

GET /{id}/contacts

Returns a list of contacts for the application.

- **Parameters**:

id - The application revision ID.

- **Return**:

Array of ApplicationContactInfo (see ApplicationContactInfo)

➔ See also:

- /applications

GET /{id}/flows

Returns all flows for an application.

- **Parameters**:

id - The application revision ID.

- **Return**:

Array of Flow (see Flow)

➔ See also:

- /applications

GET /{id}/flows/{flowid}

Returns a single flow from an application.

- **Parameters**:

id - The application revision ID.

flowID - The flow ID.

- **Return**:

Flow (see Flow)

➔ See also:

- /applications

GET /{id}/revisions

Returns a list of all revisions for the application.

- **Parameters**:

id - The application revision ID.

- **Return**:

Array of ApplicationRevision (see ApplicationRevision)

➔ See also:

- /applications

GET /{id}/vulnerabilities

Returns a list of vulnerabilities for the application revision.

- **Parameters**:

id - The application revision ID.

- **Return**:

ApplicationVulnerability (see ApplicationVulnerability)

➔ See also:

- /applications

GET /name/{appName}

Returns the latest revision for an application with the specified name.

- **Parameters**:

appName - The application name.

- **Return**:

Application (see Application)

➔ See also:

- /applications

GET /{id}/risks

Returns a list of risks for the application revision.

- **Parameters**:

id - The application revision ID.

- **Return**:

Array of Risk (see Risk)

➔ See also:

- /applications

GET /{id}/flows/{flowId}/risks

Returns a list of risks for a flow.

- **Parameters**:

id - The application revision ID.

flowID - The flow ID.

- **Return**:

Array of Risk (see Risk)

➔ See also:

- /applications

POST /{id}/apply

Applies an application's draft revision.

Resource Name: `/applications/{id}/apply`

Permissions Required:

- Apply draft
- Edit application

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application revision's ID. **Note:** Must be the ID of a draft revision.

Request Body: (optional)

Element	Type	Description
`selectedFlowsIds`	Array of Integer	List of Flow IDs to include in the opened change request. Only changes in the listed flows will be part of the change request. If request body is not passed, all changed flows will be included in change request.

Return:

A ChangeApplicationResponse (see ChangeApplicationResponse) object.

➔ See also:

- /applications

POST /{id}/check_connectivity

Runs connectivity check on all flows of an application revision and returns the results.

Resource Name: `/applications/{id}/check_connectivity`

Permissions Required:

- Update connectivity
- Edit application

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application's revision ID.

Return:

An ApplicationConnectivity (see ApplicationConnectivity) object.

➔ See also:

- /applications

POST /{id}/contacts

Edits an application's contacts.

Resource Name: `/applications/{id}/contacts`

Permissions Required:

- editAllApplications

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The application's revision ID.
`addContacts`	Array of ContactRequest (see ContactRequest)	List of contacts that the user would like to add to the application revision.
`removeContacts`	Array of ContactRequest (see ContactRequest)	List of contacts that the user would like to remove from application revision.

Return:

Parameter	Type	Description
`applicationId`	Integer	Edited application's ID.

Parameter	Type	Description
contacts	Array of ContactRequest (see ContactRequest)	List of all application contacts.

Error Codes:

- 404 (Not found) - Application wasn't found.
- 403 (Forbidden) - User doesn't have permission to edit the application.
- 403 (Forbidden) - User doesn't have permission to edit the application's general information.
- 400 (Bad request) - Contacts do not exist.
- 400 (Bad request) - Invalid role.

Request example:

```
POST <ip:port>/BusinessFlow/rest/v1/application/15/contacts
{
  "addContacts": [
    {
      "email": "test@test.com",
      "role": "General Contact"
    }
  ],
  "removeContacts": [
    {
      "email": "remove@test.com",
      "role": "Business Owner"
    }
  ]
}
```

Return Example:

```
{  "applicationId": 15,  "contacts": [    {      "email": "test@test.com",
     "role": "General Contact"    }  ]}
```

➔ See also:

- /applications

POST /{id}/custom_fields

Edits an application's custom fields.

Resource Name: `/applications/{id}/custom_fields`

Permissions Required:

- editAllApplications

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The application's revision ID.
setCustomFields	Array of KeyValuePair (see KeyValuePair)	List of custom fields that the user would like to add to the application revision.
clearCustomFields	Array of String	List of custom field names to clear from the application.

Return:

Parameter	Type	Description
applicationId	Integer	Edited application's ID.
customFields	Array of KeyValuePair (see KeyValuePair)	List of all the application's custom fields.

Error Codes:

- 404 (Not found) - Application wasn't found.
- 403 (Forbidden) - User doesn't have permission to edit the application.

- 403 (Forbidden) - User doesn't have permission to edit the application general information.
- 400 (Bad request) - Custom fields do not exist.
- 400 (Bad request) - Invalid role.

Request example:

```
POST <ip:port>/BusinessFlow/rest/v1/application/15/custom_fields
{
  "setCustomFields": [
    {
      "name": "customField1",
      "value": "value1"
    }
  ],
  "clearCustomFields": [
    "customField2"
  ]
}
```

Return Example:

```
{  "applicationId": 15,  "customFields": [    {      "name": "customField1",
      "value": "value1"    }  ]}
```

➔ See also:

- /applications

POST /{id}/decommission

Decommissions the application.

Resource Name: `/applications/{id}/decommisson`

Permissions Required:

- Edit application

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application revision's ID.

Return:

A ChangeApplicationResponse (see ChangeApplicationResponse) object.

➔ See also:

- /applications

POST /{id}/discard

Discards an application's draft revision.

Resource Name: `/applications/{id}/discard`

Permissions Required:

- Edit application

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application revision's ID. **Note:** Must be the ID of a draft revision.

Return:

A Status (see Status) object.

➔ See also:

- /applications

POST /{id}/flows

Edits an application's flows.

Resource Name: `/applications/{id}/flows`

Permissions Required:

- editAllApplications
- createSharedFlows

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The application's revision ID.
`flowID`*Mandatory*	Integer	Flow ID.
`name`	String	New flow name.
`comment`	String	New flow comment.
`addSources`	Array of NetworkObject (see NetworkObject)	Sources to add to flow.
`removeSources`	Array of NetworkObject (see NetworkObject)	Sources to remove from flow.
`addNetworkUsers`	Array of String	New user names to add to flow.
`removeNetworkUsers`	Array of String	User names to remove from flow.
`addDestinations`	Array of NetworkObject (see NetworkObject)	Destinations to add to flow.
`removeDestinations`	Array of NetworkObject (see NetworkObject)	Destinations to remove from flow.
`addServices`	Array of NetworkObject (see NetworkObject)	Services to add to flow.

Parameter	Type	Description
removeServices	Array of NetworkObject (see NetworkObject)	Services to remove from flow.
addNetworkApplications	Array of NetworkObject (see NetworkObject)	Network applications to add to flow.
removeNetworkApplications	Array of NetworkObject (see NetworkObject)	Network applications to remove from flow.
setCustomFeidls	Array of KeyValuePair (see KeyValuePair)	Custom fields to assign to flow.
clearCustomFields	Array of String	Custom fields to clear from flow.

Return:

Parameter	Type	Description
success	Boolean	Operation status.
flows	Array of Flow (see Flow)	List of all application flows after change.

Error Codes:

- 404 (Not found) - Application wasn't found.
- 404 (Not found) - Flow ID wasn't found.
- 403 (Forbidden) - User doesn't have permission to edit the application.
- 400 (Bad request) - Flow isn't editable due to status.
- 400 (Bad request) - Duplicate name.
- 400 (Bad request) - Request parameter has wrong or missing value.

Request example:

```
POST <ip:port>/BusinessFlow/rest/v1/application/15/flows
[
  {
```

```
    "flowID": 50,
    "name": "new flow name",
    "addSources": [
      "device": "x_1231_dac",
      "name": "testSource"
    ],
    "removeDestinations": [
      {
        "name": "oldDst"
      }
    ]
    "setCustomFields": [
      {
        "name": "cfKey1",
        "value": "cfValue1"
      }
    ]
  }
]
```

Return Example:

```
{  "success": true,  "flows": [    {      "flowID": 50,
"name": "new flow name",      "flowType": "APPLICATION_FLOW",      …    }  ]}
```

See Flow (see Flow) object for more information.

➔ See also:

- /applications

POST /{id}/flows/{flowid}/check_connectivity

Runs check connectivity on a specific flow and returns the results.

Resource Name: `/applications/{id}/flows/{flowID}/check_connectivity`

Permissions Required:

- Update connectivity
- Edit application

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application's revision ID.
`flowID`	String	The flow's ID.

Return:

A FlowConnectivity (see FlowConnectivity) object.

➔ See also:

- /applications

POST /{id}/labels

Edits an application's labels.

Resource Name: `/applications/{id}/labels`

Permissions Required:

- editAllApplications
- createLabels

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The application's revision ID.
`addLabels`	Array of String	List of labels that the user would like to add to the application revision.
`removeLabels`	Array of String	List of label names that the user would like to remove from application revision.

Return:

Parameter	Type	Description
`applicationId`	Integer	Edited application's ID.
`labels`	Array of String	List of all application label names.

Error Codes:

- 404 (Not found) - Application wasn't found.
- 403 (Forbidden) - User doesn't have permission to edit the application.
- 403 (Forbidden) - User doesn't have permission to edit the application's general information.
- 403 (Forbidden) - User doesn't have permission to add new labels when addLabels request field has unknown labels.
- 400 (Bad request) - User is trying to add system label to application or validation failure.

Request example:

```
POST <ip:port>/BusinessFlow/rest/v1/application/15/labels
{
  "addLabels": [
    "label1",
    "label2"
  ],
  "removeLabels": [
    "label3"
  ]
}
```

Return Example:

```
{  "applicationId": 15,  "labels": [    "label1",    "label2"  ]}
```

➔ See also:

- /applications

POST /{id}/resolve

Resolves blocked flows for an application revision.

Resource Name: `/applications/{id}/resolve`

Permissions Required:

- Edit application

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application's revision ID.

Return:

A ChangeApplicationResponse (see ChangeApplicationResponse) object.

➔ See also:

- /applications

POST /new

Creates a new application.

Resource Name: `/applications/new`

Permissions Required:

- Create new application

Request Body:

Element	Type	Description
`name`	String	The application's name.

Element	Type	Description
`custom_fields`	Empty or list of `CustomField` objects	Existing custom fields to assign to the application. See CustomField (see CustomField).
`contacts`	Empty or list of `ApplicationContact` objects	Existing contacts to assign to the application. See ApplicationContact (see ApplicationContact).
`labels`	Empty or list of strings	Existing labels to assign to the application.
`flows`	Empty or list of `NewFlow` objects	The flows to add to the application. See NewFlow (see NewFlow).

Validation:

- Invalid value for existing application custom field.
- Existing application with the same name.
- No exiting contact with such email.
- No exiting contact role.
- No existing label.

Return:

An Application (see Application) object describing the application that was created.

➔ See also:

- /applications

POST /{id}/flows/new

Adds new flows to an application.

Resource Name: `/applications/{id}/flows/new`

Permissions Required:

- Edit application
- Create shared flow (only required when creating a shared flow)

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application's revision ID.

Request Body:

A list of NewFlow (see NewFlow) objects describing the flows to add to the application.

Application Validation:

- Application does not exist.
- Application is pending decommission/decommissioned.

Flow Validation:

- Existing flow with the same name.
- Application flow with missing mandatory fields.
- Shared flow with empty source and empty destination.
- Shared flow with empty source, but with a user.
- Flow contains non-existing sources/destinations/network applications/services.
- Flow contains an invalid custom field value.
- Subscribed flow does not exist.

Return:

List of Flow (see Flow) objects describing the flows with the updates you made.

➔ See also:

- /applications

DELETE /{id}/contacts

Removes all of an application's contacts.

Resource Name: `/applications/{id}/contacts`

Permissions Required:

- editAllApplications

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The application's revision ID.

Return:

200 - OK

Error Codes:

- 404 (Not found) - Application wasn't found.
- 403 (Forbidden) - User doesn't have permission to edit the application.
- 403 (Forbidden) - User doesn't have permission to edit the application's general information.

➔ See also:

- /applications

DELETE /{id}/custom_fields

Removes all custom fields for an application.

Resource Name: `/applications/{id}/custom_fields`

Permissions Required:

- editAllApplications

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The application's revision ID.

Return:

200 OK

Error Codes:

- 404 (Not found) - Application wasn't found.
- 403 (Forbidden) - User doesn't have permission to edit the application.

- 403 (Forbidden) - User doesn't have permission to edit the application general information.

Note: The system field **'application lifecycle phase'** will not be cleared.

➔ See also:

- /applications

DELETE /{id}/flows/{flow_id}

Deletes a flow from an application revision.

Resource Name: `/applications/{id}/flows/{flow_id}/`

Permissions Required:

- Edit application

Request URL Parameters:

Parameter	Type	Description
`id`	String	The application's revision ID.
`flow_id`	String	The flow's ID.

Validation:

- Existing application.
- Existing flow.

Return:

A Status (see Status) object.

➔ See also:

- /applications

DELETE /{id}/labels

Removes all user-defined application labels from an application.

Resource Name: `/applications/{id}/labels`

Permissions Required:

- editAllApplications

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The application's revision ID.

Return:

200 - OK

Error Codes:

- 404 (Not found) - Application wasn't found.
- 403 (Forbidden) - User doesn't have permission to edit the application.
- 403 (Forbidden) - User doesn't have permission to edit the application's general information.

➔ See also:

- /applications

/network_objects

The following are requests for network object related resources. The base URL for network objects is `/BusinessFlow/rest/v1/network_objects`.

- GET /
- GET /{id}
- GET /{id}/applications
- GET /{id}/vulnerabilities
- GET /name/{name}
- GET /find

- GET /find/applications
- DELETE /{id}
- POST /{id}
- POST /{id}/replace
- POST /new

GET /

Returns a list of network objects.

- **Parameters**:

page_size - The number of results per page (Default is 1000).

page_number - The page number you want to return (Default = 1). For example, if you set this parameter to 2, only the second page of objects will be returned.

Return:

Array of NetworkObject (see NetworkObject)

➔ See also:

- /network_objects

GET /{id}

Returns a network object by ID.

- **Parameters**:

id - The network object revision ID.

Return:

NetworkObject (see NetworkObject)

➔ See also:

- /network_objects

GET /{id}/applications

Returns all relevant applications for the network object.

- **Parameters**:

id - The network object revision ID.

- **Return**:

Array of Application (see Application)

➔ See also:

- /network_objects

GET /{id}/vulnerabilities

Returns vulnerabilities for the network object.

- **Parameters**:

id - The network object revision ID.

- **Return**:

ObjectVulnerability (see ObjectVulnerability)

➔ See also:

- /network_objects

GET /name/{name}

Returns a network object by name.

- **Parameters**:

name - The network object (exact) name.

- **Return**:

String of NetworkObject (see NetworkService)

➔ See also:

- /network_objects

GET /find

Finds network objects related to IP addresses.

- **Parameters**:

address - The IP address or subnet

(optional) type - The search method for the address. One of the following:

- INTERSECT (Default)
- CONTAINED
- CONTAINING
- EXACT
- **Return**:

Array of NetworkObject (see NetworkObject)

➔ See also:

- /network_objects

GET /find/applications

Finds applications containing network objects related to IP addresses.

- **Parameters**:

address - The IP address or subnet

(optional) type - The search method for the address. One of the following:

- INTERSECT (Default)
- CONTAINED
- CONTAINING
- EXACT
- **Return**:

Array of Application (see Application)

➔ See also:

- /network_objects

DELETE /{id}

Deletes a network object by ID.

Note: When AppViz is configured to manage changes to device objects with traffic changes only (the default configuration), AppViz does not support deleting device objects. Using this request to delete a device object will succeed in deleting the object from AppViz, but because the object will never be deleted from the device, the object will be automatically recreated with the next device object update.

Note: When AppViz is configured to manage device objects on their devices, this request can be used to delete device objects on their device when the object is not currently used in any application, in a project, or as a member of a device group.

Resource Name: `/network_objects/{id}/`
Permissions Required:

- Edit network object

Request URL Parameters:

Parameter	Type	Description
`id`	String	The network object's revision ID.

Validation:

- Existing object.

Return:

- For non-device objects: A Status (see Status) object.
- For device objects: A DeleteDeviceObjectResponse (see DeleteDeviceObjectResponse) object.

➔ See also:

- /network_objects

POST /{id}

Edits network object.

Resource Name: `/network_objects/{id}`

Permissions Required:

- editNetworkObjects

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The network object ID.
`name`	String	New flow name.
`content`	String	New network object content.
`addMembers`	Array of NetworkObject (see NetworkObject)	New members to add to the network object group. **Note**: Only applied when network object is defined as a group.

Parameter	Type	Description
removeMembers	Array of NetworkObject (see NetworkObject)	Members to remove from network object group. **Note**: Only applied when network object is defined as a group.
setCustomFields	Array of KeyValuePair (see KeyValuePair)	Custom fields to assign to network object.
clearCustomFields	Array of String	Custom fields to clear from network object.

Return:

Parameter	Type	Description
changeRequest	ChangeRequest (see ChangeRequest)	Opened change request, if needed.
networkObject	NetworkObjectEntity (see NetworkObject)	Network object after changes applied.

Error Codes:

Errors: A failure status with the reasons or the network object's new representation.

- 404 (Not found) – Network object wasn't found
- 403 (Forbidden) - User doesn't have permission to edit network object
- 400 (Bad request) – Revision ID is not the latest revision.
- 400 (Bad request) – Object isn’t editable due to status.
- 400 (Bad request) – Duplicate name
- 400 (bad request) – Request parameter has wrong or missing value.

Request example:

```
POST <ip:port>/BusinessFlow/rest/v1/network_objects/15

[
```

```
  {
    "name": "new network object name",
    "content": "10.6.9.14"
  }
]
```

Return Example:

```
{  "networkObject": {    "revisionID": 15,    "objectID": "2",
"name": "new network object name",    …  }  }
```

See NetworkObject (see NetworkObject) for more information.

➔ See also:

- /network_objects

POST /{id}/replace

Replaces an abstract object with a real object.

Resource Name: `/network_objects/{id}/replace`

Permissions Required:

- editNetworkObjects

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The network object ID.
`replaceWith`*Mandatory*	NetworkObject (see NetworkObject)	Existing network object that will be replacing the abstract object.
`replaceInApplications`	Array of String	Application names in which the abstract object should be replaced. If list is empty or null, all affected applications will be replaced by the abstract object.

Return:

Parameter	Type	Description
`replaceInApplications`	Array of Integer	Applications in which the abstract object was replaced.
`changeRequestId`	Integer	Change request ID, if opened.

Error Codes:

Errors: A failure status with the reasons.

- 404 (Not found) - Network object wasn't found
- 403 (Forbidden) - User doesn't have permission to edit network object
- 403 (Forbidden) - User doesn't have permission to edit applications.
- 400 (Bad request) - replaceWith object is not valid.

Request example:

```
POST <ip:port>/BusinessFlow/rest/v1/network_objects/15/replace{
"replaceWith": {    "name": "netobe1",    "device": "x_123fv_spo"   },
"replaceInApplications": [    "app1",    "app2"   ]}
```

Return Example:

```
{  "replacedInApplications": [    44,    69   ],  "changeRequestId": 411 }
```

➔ See also:

- /network_objects

POST /new

Creates a new network object. The created network object's origin will appear in the Web Interface as "from file".

Resource Name: `/network_objects/new`

Permissions Required:

- Edit network object

Request Body:

Element	Type	Description
`name`	String	The network object's name.

`type`	String	One of the following:
		`Host`
		`Range`
		`Group`
		`Abstract`

`content`	For Host: String	The IP Address for the object.
	For Range: String	The Range or CIDR for the object.
	For Group: List of `ExistingNetworkObject` objects and/or `NewNetworkObject` objects.	The members for the group. The list of objects can include existing or new network objects. For existing network objects, see ExistingNetworkObject (see ExistingNetworkObject). For new network objects, add this object within itself.
	For Abstract: Empty	

Validation:

- Existing network object with the same name.
- Invalid value for custom field.
- Non-existing member network object.
- Invalid IP.
- Invalid range.
- Invalid CIDR.
- Invalid content for the type.

Return:

A NetworkObject (see NetworkObject) object describing the network object that was created.

➔ See also:

- /network_objects

/network_services

The following are requests for service object related resources. The base URL for service objects is `/BusinessFlow/rest/v1/network_services`.

- GET /
- GET /{id}
- GET /name/{name}
- DELETE /{id}
- POST /{id}
- POST /new

GET /

Returns a list of the service objects.

- **Parameters**:

(optional) page_size - The number of results per page (Default is 1000).

(optional) page_number - The page number you want to return (Default is 1). For example, if you set this parameter to 2, only the second page of objects will be returned.

Return:

Array of NetworkService (see NetworkService).

➔ See also:

- /network_services

GET /{id}

Returns a service object by ID.

- **Parameters**:

id - The service object ID.

- **Return**:

NetworkService (see NetworkService)

➔ See also:

- /network_services

GET /name/{name}

Returns service objects by name.

- **Parameters**:

name - The name of the service object.

- **Return**:

Array of NetworkService (see NetworkService)

➔ See also:

- /network_services

DELETE /{id}

Deletes a service object by ID.

> **Note:** AppViz does not support deleting device service objects. Using this request to delete a device object will succeed in deleting the object from AppViz, but because the object will never be deleted from the device, the object will be automatically recreated with the next device object update.

Resource Name: `/network_services/{id}/`
Permissions Required:

- Edit service object

Request URL Parameters:

Parameter	Type	Description
`id`	String	The service object's revision ID.

Validation:

- Existing object.

Return:

- A Status (see Status) object.

➔ See also:

- /network_services

POST /{id}

Edits a service object.

Resource Name: `/network_services/{id}`

Permissions Required:

- editServiceObjects

Request URL Parameters:

Parameter	Type	Description
`id`*Mandatory*	String	The network service ID.
`name`	String	New network service name.
`addContent`	Array of ServiceObject (see ServiceObject)	New network object content to add.
`removeContent`	Array of ServiceObject (see ServiceObject)	Content to remove from network service object.
`setCustomFields`	Array of KeyValuePair (see KeyValuePair)	Custom fields to assign to service object.
`clearCustomFields`	Array of String	Ciustom fields to clear from service object.

Return:

Parameter	Type	Description
revisionID	Integer	ID of revision.
serviceID	Integer	ID of service object.
name	String	New service object name.

Error Codes:

Errors: A failure status with the reasons or the network service object's new representation.

- 404 (Not found) – Network service object wasn't found
- 403 (Forbidden) - User doesn't have permission to edit network service object
- 400 (Bad request) – Revision ID is not the latest revision.
- 400 (Bad request) – Object isn’t editable due to status.
- 400 (Bad request) – Duplicate name.
- 400 (bad request) – Request parameter has wrong or missing value.

Request example:

```
POST <ip:port>/BusinessFlow/rest/v1/network_services/15
{
  "name": "new service object name",
  "addContent": [
    {
      "port": "8080",
      "protocol": "TCP"
    }
  ]
}
```

Return Example:

```
{  "revisionID": 15,  "serviceID": 2,  "name": "new service object name",}
```

See NetworkService (see NetworkService) for more information.

➔ See also:

- /network_services

POST /new

Creates a new service object. The created service object's origin will appear in the Web Interface as "from file".

Resource Name: `/network_services/new`

Permissions Required:

- Edit service object

Request Body:

Element	Type	Description
`name`	String	The service object's name.
`content`	List of `Service` objects	The services to include in the object. See Service (see Service).
`custom_fields`	List of `CustomField` objects or empty	The custom fields to include for the object. See CustomField (see CustomField).

Validation:

- Existing service object with the same name.
- Invalid value for custom field.
- Invalid protocol.
- Invalid port.

Return:

A NetworkService (see NetworkService) object describing the service object that was created.

➔ See also:

- /network_services

/settings/permissions

The following are requests related to permissions for users and roles. The base URL is `/BusinessFlow/rest/v1/settings/permissions`.

- GET /default
- GET /role
- GET /user
- DELETE /role
- POST /role
- POST /role/new
- POST /user

Note: When ASMS is configured to fetch user data from an LDAP server, the current permissions in the LDAP may not reflect the current permissions in ASMS. The current permissions in ASMS will reflect the LDAP permissions at the time ASMS last fetched the information from the LDAP. Each user's information is fetched and updated upon login; this includes the list of roles the user is assigned, the list of permissions the user inherits, and the list of users assigned the fetched roles.

Note: Permissions APIs can only be run by administrator users. Other users who attempt to use the APIs will receive an error.

Note: Administrator users cannot be edited. An attempt to edit the permissions of administrator users through the API will result in an error. This is true even though administrator users can be retrieved using the GET /user (see GET /user)

permissions API.

GET /default

Gets the default permissions of new users.

Resource Name: `/settings/permissions/default`

Permissions Required:

- administrator

Return:

Parameter	Type	Description
`requestor`	Array of NameAllowedPair (see NameAllowedPair)	Default permissions for requestor user.
`privileged`	Array of NameAllowedPair (see NameAllowedPair)	Default permissions for privileged user.

Return Example:

```
{
  "requestor": [
    {
      "name": "viewChangeRequests",
      "allowed": true
    },
    {
      "name": "createNewApplications",
      "allowed": true
    },
…
  ],
  "privileged": [
```

```
    {
      "name": " viewChangeRequests ",
      "allowed": true
    },
    {
      "name": " createNewApplications ",
      "allowed": true
    },
…
  ]
}
```

➔ See also:

- /settings/permissions

GET /role

Gets the permissions of a specific role.

Resource Name: `/settings/permissions/role`

Permissions Required:

- administrator

Request URL Parameters:

Parameter	Type	Description
`name`*Mandatory*	String	Role name.

Return:

Parameter	Type	Description
`name`	String	Role name.

Parameter	Type	Description
authorizedViewsAndActions	Array of NameAllowedPair (see NameAllowedPair)	View and action permissons.
authorizedApplications	Array of authorizedApplications (see authorizedApplications)	Permissions on applications.
roleUsers	Arrary of String	Associated user names according to last login.
enabled	Boolean	Whether role is enabled: true or false.

Return Example:

```
{
  "name": "DNS-role",
  "authorizedViewsAndActions": [
    {
      "name": "viewActivityLog",
      "allowed": false
    },
    {
      "name": "applyDrafts",
      "allowed": true
    },
...
  ],
  "authorizedApplications": [
    {
      "applicationID": 1,
      "name": "DNS",
```

```
      "permission": "view"
    },
    {
      "applicationID": 2,
      "name": "Backup",
      "permission": "edit"
    }
  ],
  "roleUsers": [
    "Sue","Joe"
  ],
  "enabled": true
}
```

➔ See also:

- /settings/permissions

GET /user

Gets the permissions of a specific user.

Resource Name: `/settings/permissions/user`

Permissions Required:

- administrator

Request URL Parameters:

Parameter	Type	Description
`name`*Mandatory*	String	User name.

Return:

Parameter	Type	Description
`name`	String	User name.
`fullName`	String	User full name.
`privileged`	Boolean	Whether user is priviileged.
`authorizedViewsAndActions`	Array of NameAllowedInherited (see NameAllowedInherited)	View and action permissons.
`authorizedApplications`	Array of authorizedApplications (see authorizedApplications)	Permissions on applications.
`roles`	Arrary of String	Associated role names according to last login.
`inheritedAuthorizedApplications`	Array of authorizedApplications (see authorizedApplications)	Permissions on applications, inherited from associated roles.

Return Example:

```
{
  "name": "Joe",
  "authorizedViewsAndActions": [
    {
      "name": "updateObjectFromDevice",
      "allowed": false,
      "inherited": false
    },
    {
```

```
      "name": "createNewApplications",
      "allowed": true,
      "inherited": false
    }
...
  ],
  "authorizedApplications": [
    {
      "applicationID": 1,
      "name": "DNS",
      "permission": "view"
    }
  ],
  "fullName": "Joe Smith",
  "roles": [
    "DNS-role"
  ],
  "inheritedAuthorizedApplications": [
    {
      "applicationID": 1,
      "name": "DNS",
      "permission": "view"
    },
    {
      "applicationID": 2,
      "name": "Backup",
      "permission": "edit"
    }
  ],
```

```
    "privileged": false
  }
```

➔ See also:

- /settings/permissions

DELETE /role

Deletes a specific role.

Resource Name: `/settings/permissions/role`

Permissions Required:

- administrator

Request URL Parameters:

Parameter	Type	Description
`name`*Mandatory*	String	Role name.

➔ See also:

- /settings/permissions

POST /role

Edits the permissions of a specific role.

Resource Name: `/settings/permissions/role`

Permissions Required:

- administrator

Request URL Parameters:

Parameter	Type	Description
`name`*Mandatory*	String	Role name.

Request Body Parameters:

Parameter	Type	Description
`authorizedApplicationsChanges`	Array of Add/Remove (see Add/Remove)	List of application permissions to add (ID, permission). List of application IDs to remove from permissions.
`authorizedViewsAndActionChanges`	Array of Add/Remove (see Add/Remove)	List of views and actions to add. List of views and actions to remove.
`users`	Array of Add/Remove (see Add/Remove)	Support only if LDAP role association is **not** configured. List of users to associate with role. List of users to disassociate from role.

Return:

Parameter	Type	Description
`name`	String	User name
`authorizedViewsAndActions`	Array of NameAllowedPair (see NameAllowedPair)	View and action permissons.
`authorizedApplications`	Array of authorizedApplications (see authorizedApplications)	Permissions on applications.
`roleUsers`	Arrary of String	Associated user names according to last login.
`enabled`	Boolean	Whether role is enabled.

Request example:

```
{
"authorizedApplicationsChanges": {
"add": [
{
"applicationID": 10,
"permission": "view"
},
{
"applicationID": 11,
"permission": "edit"
}
],
"remove": [
13,14
]
},
"authorizedViewsAndActionChanges": {
"add": [
"viewActivityLog",”applyDrafts”
],
"remove": [
"viewChangeRequests",”createNewApplications”
]
},
"users": {
"add": [
"Sue",”Joe”
],
"remove": [
"Eric",”John”
]
}
```

```
}
```

Return Example:

```
{
  "name": "DNS-role",
  "authorizedViewsAndActions": [
    {
      "name": "viewActivityLog",
      "allowed": true
    },
    {
      "name": "applyDrafts",
      "allowed": true
    },
...
  ],
  "authorizedApplications": [
    {
      "applicationID": 1,
      "name": "Backkup",
      "permission": "view"
    },
    {
      "applicationID": 2,
      "name": "DNS",
      "permission": "edit"
    }
  ],
  "roleUsers": [
```

```
      "Sue","Joe"
    ],
    "enabled": true
  }
```

➔ See also:

- /settings/permissions

POST /role/new

Creates a new role.

Resource Name: `/settings/permissions/role/new`

Permissions Required:

- administrator

Request Body Parameters:

Parameter	Type	Description
`name` *Mandatory*	String	Role name.
`description`	String	Role description.
`enabled`	Boolean	Whether role is enabled. Default is true.
`ldapGroupDN`	String	LDAP group DN. Supported only if LDAP role association is configured.
`users`	Array of String	List of users to associate. Supported only if LDAP role association is **not** configured.
`authorizedApplications`	Array of authorizedApplications (see authorizedApplications)	List of application permissions (ID, permission).

Parameter	Type	Description
authorizedViewsAndAction	Array of String	List of permitted views and actions.

Return:

Parameter	Type	Description
name	String	Role name.
authorizedViewsAndActions	Array of NameAllowedPair (see NameAllowedPair)	View and action permissions.
authorizedApplications	Array of authorizedApplications (see authorizedApplications)	Permissions on applications.
roleUsers	Array of String	Associated user names according to last login.
enabled	Boolean	Whether role is enabled: true or false.

Request example:

```
{
  "authorizedApplications": [
    {
      "applicationID": 1,
      "permission": "view"
    },
    {
      "applicationID": 2,
      "permission": "edit"
    }
  ],
```

```
  "authorizedViewsAndActions": [
    "applyDrafts","viewActivityLog"
  ],
  "description": "PCI role",
  "enabled": true,
  "name": "pci",
  "users": [
    "Eric","Steve"
  ]
}
```

Return Example:

```
{
  "name": "pci",
  "authorizedViewsAndActions": [
    {
      "name": "viewActivityLog",
      "allowed": true
    },
    {
      "name": "applyDrafts",
      "allowed": true
    },
...
  ],
  "authorizedApplications": [
    {
      "applicationID": 1,
      "name": "DNS",
```

```
        "permission": "view"
      },
      {
        "applicationID": 2,
        "name": "Backup",
        "permission": "edit"
      }
    ],
    "roleUsers": [
      "Eric","Steve"
    ],
    "enabled": true
  }
```

➔ See also:

- /settings/permissions

POST /user

Edits the permissions of a specific user.

Resource Name: `/settings/permissions/user`

Permissions Required:

- administrator

Request URL Parameters:

Parameter	Type	Description
`name`*Mandatory*	String	User name.

Request Body Parameters

Parameter	Type	Description

`authorizedApplicationsChanges`	Array of Add/Remove (see Add/Remove)	List of application permissions to add (ID, permission). List of application IDs to remove from permissions.
`authorizedViewsAndActionChanges`	Array of Add/Remove (see Add/Remove)	List of permissions to add. List of permissions to remove.

Return:

Parameter	Type	Description
`authorizedApplicationsChanges`	String	Application name.
`rolesEdit`	Array of String	List of roles allowed to edit application.

Request example:

```
{
  "authorizedApplicationsChanges": {
    "add": [
      {
        "applicationID": 10,
        "permission": "view"
      },
      {
        "applicationID": 11,
        "permission": "edit"
      }
    ],
    "remove": [
      13,14
```

```
    ]
  },
  "authorizedViewsAndActionChanges": {
    "add": [
      "viewActivityLog","applyDrafts"
    ],
    "remove": [
      "viewChangeRequests","createNewApplications"
    ]
  }
}
```

Return Example:

```
{
  "name": "Sue",
  "authorizedViewsAndActions": [
    {
      "name": "updateObjectFromDevice",
      "allowed": false,
      "inherited": false
    },
    {
      "name": "createNewApplications",
      "allowed": false,
      "inherited": false
    }
...
  ],
  "authorizedApplications": [
```

```
    {
      "applicationID": 10,
      "name": "DNS",
      "permission": "view"
    }
  ],
  "fullName": "Sue Smith",
  "privileged": false
}
```

➔ **See also**:

- /settings/permissions

Import vulnerability data

Use the following request methods to import vulnerability data into ASMS, or delete data previously imported.

Import specific vulnerability data

The `importVulnerabilityKb` method enables you to import specific vulnerability data, as opposed to all data from a specific host.

Note: You must use this API before using the hosts API.

Resource name: `/ms-vulnerabilities/v1/api/import/kbs`

Request method: `POST`

Request body:

Element	Description
`deleteOldImportedData`	Boolean. Determine whether to fist delete older imported data.
`vulnerabilityKbs`	An array of vulnerability KBs. Each object includes: `kbId`. String. The string ID of a specific KB. You will use the same ID in the **hosts** API. `summary`. String. The summary of a KB. `description`. String. A string that describes the vulnerability. `cvssScore`. Floating integer: The vulnerability's CVSS score. `cves`. A list of vulnerability CVEs. Each CVE includes: • `name`. String. The name of an individual vulnerability CVE.

Response parameters:

Element	Description
`status`	Describes the response status, including the following elements: `data`. Object. If the operation failed, this object includes a validation message and index integer. `error`. String. The error that occurs, if relevant. `msg`. String. The message displayed `status`. String. The status returned. `success`. Boolean. Determines whether the API was successful. `type`. String.

Note: Vulnerabilities with a CVSS score of **0** are not supported and fail the validation.

Import specific vulnerability data request example

```
{
 "deleteOldImportedData": false,
 "vulnerabilityKbs": [
  {
   "cvssScore": 7.5,
   "description": "ssh in OpenSSH before 4.7 does not properly handle
when an untrusted cookie cannot be created and
    uses a trusted X11 cookie instead, which allows attackers to violate
intended policy and gain privileges by causing
    an X client to be treated as trusted.",
   "kbId": "openssh-x11-cookie-auth-bypass",
   "summary": "OpenSSH X11 Cookie Local Authentication Bypass
Vulnerability",
   "cves": [
    "CVE-9990"
    ]
   }
  ]
}
```

Import specific vulnerability data response example

```
{
"status": null
"type": null
"msg": "Vulnerability KBs saved successfully"
"success": true
"error": null,
"data": {},
"files": null
}

Errors:  a failure status with the reasons or the application labels new
representation
403 (forbidden) - user doesn't have admin permission to use the micro
service API.
400 (bad request) - Input validation failures.
```

Import vulnerabilities from hosts

The `importVulnerabilityHosts` method allows you to import vulnerability data from specified scanners, defined in the API as host servers.

Note: Before using this API, you must call the kbs API.

Resource name: `/ms-vulnerabilities/v1/api/import/hosts`

Request method: `POST`

Request body:

A list of vulnerability hosts, as detailed by the following elements.

Element	Description
`ip`	String. The IP address of the host. Mandatory.
`kbId`	String. The string ID of a specific KB. This must be a KB that was already imported using the kbs API, and have the same ID. Mandatory.
`date`	Number. The UNIX date and time stamp in milliseconds that the KB was identified on the host. Optional. Default is the current date and time.

Response parameters:

Element	Description
`status`	Describes the response status, including the following elements: `data`. Object. If the operation failed, this object includes a validation message and index integer. `error`. String. The error that occurs, if relevant. `msg`. String. The message displayed `status`. String. The status returned. `success`. Boolean. Determines whether the API was successful. `type`. String.

Note: Vulnerabilities with a CVSS score of **0** are not supported and fail the

validation.

Import vulnerability data from hosts request example:

```
[
 {
  "ip": "10.30.31.25",
  "kbId": "openssh-x11-cookie-auth-bypass",
  "date": 1560170116543
 }
]
```

Import vulnerability data from hosts response example

```
Response:
{
"status": null
"type": null
"msg": "Vulnerability Hosts saved successfully"
"success": true
"error": null,
"data": {},
"files": null
}

Errors:  a failure status with the reasons or the application labels new
representation
403 (forbidden) - user doesn't have admin permission to use the micro
service API.
400 (bad request) - Input validation failures.
```

Delete imported vulnerability data

The `deleteImportedVulnerabilityData` method enables you to delete vulnerability data imported from files.

Resource name: /ms-vulnerabilities/v1/api/import/delete

Request method: `DELETE`

Request query parameters: None.

Response parameters:

Element	Description
`status`	Describes the response status, including the following elements: `data`. String `error`. String. The error that occurs, if relevant. `msg`. String. The message displayed `status`. String. The status returned. `success`. Boolean. Determines whether the API was successful. `type`. String.

Delete imported vulnerability data response example

```
{
        "data": {},
        "error": "string",
        "msg": "string",
        "status": "string",
        "success": true,
        "type": "string"
}
```

AppViz data types

The following is a reference of AppViz data types used in the AppViz REST API:

- Add/Remove
- Application
- ApplicationConnectivity
- ApplicationContact
- ApplicationContactInfo
- ApplicationRevision
- ApplicationVulnerability
- APISubscribedFlowContent

- authorizedApplications
- ChangeApplicationResponse
- ChangeRequest
- ContactRequest
- CustomField
- CustomFieldInfo
- DeleteDeviceObjectResponse
- ExistingNetworkObject
- ExistingNetworkApplication
- ExistingServiceObject
- Flow
- FlowConnectivity
- KeyValuePair
- NameAllowedInherited
- NameAllowedPair
- NamedObject
- NetworkObject
- NetworkService
- NewFlow
- ObjectVulnerability
- Risk
- Service
- ServiceObject
- Status
- Vulnerability

Add/Remove

Element	Type	Description
add	Array of Array	Depending on parent node: ■ `authorizedApplicationsChanges` - List of permissions to add to application ID: ■ `applicationID` - Integer ■ `permission` - String - Permission, such as 'view', edit'. ■ `authorizedViewsAndActionChanges` - Array of String - List of authorized views and actions to add.
remove	Array of Array	Depending on parent node: ■ `authorizedApplicationsChanges` - Array of Integer - List of applicationIDs to remove permissions from. ■ `authorizedViewsAndActionChanges` - Array of String - List of authorized views and actions to remove.

➔ See also:

- AppViz data types

Application

Element	Type	Description
revisionID	Integer	ID of revision.
createdDate	Integer	Date created. Format: UTC_MILLISEC
lifecyclePhase	String	Phase of life cycle.
lastUpdateDate	Integer	Date of last update .Format: UTC_MILLISEC
customFields	Array of CustomFieldInfo (see CustomFieldInfo) objects	List of application properties and values.
name	String	Name of application.

Element	Type	Description
revisionStatus	String	Status of revision.
securityRating	Integer	Security rating of application.
applicationId	Integer	ID of application.
connectivityStatus	String	Status of connectivity.
contacts	Array of ApplicationContactInfo (see ApplicationContactInfo) objects	List of application contacts.

➔ See also:

- AppViz data types

ApplicationConnectivity

Element	Type	Description
flows	Array of FlowConnectivity (see FlowConnectivity)	List of flow connectivity.
status	String	Status.

➔ See also:

- AppViz data types

ApplicationContact

Element	Type	Description
`email`	String	The email address for the contact.
`role`	String	The role of the contact.

➔ See also:

- AppViz data types

ApplicationContactInfo

Element	Type	Description
role	String	Contact role.
name	String	Name of contact.
email	String	Email of contact.

➔ See also:

- AppViz data types

ApplicationRevision

Element	Type	Description
revisionID	Integer	ID of revision.
createdDate	Integer	Date created. Format: UTC_MILLISEC
revisionStatus	String	Status of revision

➔ See also:

- AppViz data types

ApplicationVulnerability

Element	Type	Description
findings	Array of ObjectVulnerability (see ObjectVulnerability)	List of vulnerabilities.
missinginformation	Array of NamedObject (see NamedObject)	List of missing information.

➔ See also:

- AppViz data types

APISubscribedFlowContent

Element	Type	Description
`shared_flow_name`	String	The name of the shared flow or `ALL` to subscribe to all of the shared application's flows.
`placeholder_network_object`	List of `ExistingNetworkObject` objects	The network objects to be inserted into the placeholder field. See ExistingNetworkObject (see ExistingNetworkObject).
`users`	List of strings or empty	The users to be inserted into the user field. Only relevant when the placeholder field is the source.
`comment`	String or empty	A comment for the shared flow.
`custom_fields`	List of `CustomField` objects or empty	Custom fields for the shared flow. See CustomField (see CustomField).

➔ See also:

- AppViz data types

authorizedApplications

Element	Type	Description
applicationID	String	ID of application.
name	String	Name of application.
permission	String	Permission.

➔ See also:

- AppViz data types

ChangeApplicationResponse

Element	Type	Description
Application	Application (see Application)	The changed application.
ChangeRequest	ChangeRequest (see ChangeRequest)	The change request opened to change the application.

➔ See also:

- AppViz data types

ChangeRequest

Element	Type	Description
openedDate	Integer	Date request opened. Format: UTC_MILLISEC
subject	String	Subject of change request.
id	Integer	ID of change request.
requestor	String	Requestor.
status	String	Status of request.

➔ See also:

- AppViz data types

ContactRequest

Element	Type	Description
email	String	Email of contact.

Element	Type	Description
role	String	Role. Allowed values are: ■ Business Owner ■ Primary Technical Contact ■ Secondary Technical Contact ■ General Contact

➔ See also:

- AppViz data types

CustomField

Element	Type	Description
name	String	The name of the custom field.
value	String	The value of the custom field.

➔ See also:

- AppViz data types

CustomFieldInfo

Element	Type	Description
name	String	Name of property.
link *Only for Link custom fields*	String	The compounded URL template.
value	String	Value of property.

➔ See also:

- AppViz data types

DeleteDeviceObjectResponse

Element	Type	Description
NetworkObject	NetworkObject (see NetworkObject)	The deleted device object.
ChangeRequest	ChangeRequest (see ChangeRequest)	The change request opened to delete the device object.

➔ See also:

- AppViz data types

ExistingNetworkObject

Element	Type	Description
`name`	String	The name of the network object.
`device`*Optional*	String	The device the network object is defined on.

➔ See also:

- AppViz data types

ExistingNetworkApplication

Element	Type	Description
`name`	String	The name of the network application.
`device`*Optional*	String	The device the network application is defined on.

➔ See also:

- AppViz data types

ExistingServiceObject

Element	Type	Description
`name`	String	The name of the service object.
`device`*Optional*	String	The device the service object is defined on.

➔ See also:

- AppViz data types

Flow

Element	Type	Description
createdDate	Integer	Date the flow was created in UTC_MILLISEC format.
sources	Array of NetworkObject (see NetworkObject)	The flow's sources.
flowType	String	The flow's type.
templateID	String	ID of template.
customFields	Array of CustomFieldInfo (see CustomFieldInfo)	The flow's custom fields and their values.
lastUpdateDate	Integer	Date the flow was last updated in UTC_MILLISEC format.
destinations	Array of NetworkObject (see NetworkObject)	The flow's destinations.
name	String	The flow's name.
subscribedApplication	String	The flow's subscribed application.
comment	String	The flow's comment.
services	Array of NetworkService (see NetworkService)	The flow's services.

Element	Type	Description
flowID	Integer	The flow's ID.
connectivityStatus	String	The flow's connectivity status.

➔ See also:

- AppViz data types

FlowConnectivity

Element	Type	Description
relevantDevices	Array of String	List of relevant devices.
queryLink	String	Query link.
flowID	Integer	ID of flow.
status	String	Status.

➔ See also:

- AppViz data types

KeyValuePair

Element	Type	Description
name	String	Custom field name.
value	String	Custom field value.

➔ See also:

- AppViz data types

NameAllowedInherited

Element	Type	Description
name	String	Name of permission.
allowed	String	Whether permission is allowed: true or false.
inherited	String	Whether permission is inherited: true or false.

➔ See also:

- AppViz data types

NameAllowedPair

Element	Type	Description
name	String	Name of permission.
allowed	String	Whether permission is allowed: true or false.

➔ See also:

- AppViz data types

NamedObject

Element	Type	Description
name	String	Name of object.
id	Integer	ID of object.

➔ See also:

- AppViz data types

NetworkObject

Element	Type	Description
revisionID	Integer	ID of revision.

Element	Type	Description
createdDate	Integer	Date created. Format: UTC_MILLISEC
devices	Array of String	List of devices.
customFields	Array of CustomFieldInfo (see CustomFieldInfo)	List of network object custom fields.
lastUpdateDate	Integer	Date of last update. Format: UTC_MILLISEC
orgin	String	Origin.
members	Array of NamedObject (see NamedObject)	List of members.
name *Mandatory*	String	Name of network object.
ipAddresses	Array of String	List of IP addresses.
securityRating	Integer	Security rating.
objectID	Integer	ID of object.
objectType	String	Type of object.

➔ See also:

- AppViz data types

NetworkService

Element	Type	Description
revisionID	Integer	ID of revision.
createdDate	Integer	Date created. Format: UTC_MILLISEC
devices	Array of String	List of devices.

Element	Type	Description
lastUpdateDate	Integer	Date of last update. Format: UTC_MILLISEC
origin	String	Origin.
name	String	Name of network service.
services	Array of String	List of services.
customFields	Array of CustomFieldInfo (see CustomFieldInfo)	List of service object custom fields.
serviceID	Integer	ID of service.

➔ See also:

- AppViz data types

NewFlow

Element	Type	Description

`type`	String	One of the following:
		`APPLICATION`
		`SHARED`
		`SUBSCRIBED`

For application and shared flows only:		
`name`	String or empty	The name of the flow.

Element	Type	Description
`sources`	List of `ExistingNetworkObject` objects or empty.	The sources for the flow. See ExistingNetworkObject (see ExistingNetworkObject). For shared flows, leave this field empty to indicate it should be the placeholder. This field is mandatory for application flows and for shared flows where the destination is the placeholder.
`users`	List of strings or empty	The users for the flow.
`destinations`	List of `ExistingNetworkObject` objects or empty.	The destinations for the flow. See ExistingNetworkObject (see ExistingNetworkObject). For shared flows, leave this field empty to indicate it should be the placeholder. This field is mandatory for application flows and for shared flows where the source is the placeholder.
`network_ applications`	List of `ExistingNetworkApplication` objects or empty.	The network applications for the flow. See ExistingNetworkApplication (see ExistingNetworkApplication).
`services`	List of `ExistingServiceObject` objects or empty.	The services for the flow. See ExistingServiceObject (see ExistingServiceObject). This field must be `application default` when the `network_ applications` field has a value.
`comment`	String or empty	Comment for the flow.

Element	Type	Description
`custom_fields`	List of CustomField (see CustomField) objects or empty	Custom fields for the flow.
For subscribed flows only:		
`shared_application_name`	String	The name of the shared application.
`subscribed_flows`	List of `APISubscribedFlowContent` objects.	The flows to subscribe to . See APISubscribedFlowContent (see APISubscribedFlowContent).

➔ See also:

- AppViz data types

ObjectVulnerability

Element	Type	Description
objectName	String	Name of object.
vulnerabilities	Array of Vulnerability (see Vulnerability)	List of object vulnerabilities.
objectID	Integer	ID of object.

➔ See also:

- AppViz data types

Risk

Element	Type	Description
riskId	Integer	ID of the risk object.

Element	Type	Description
code	Integer	The specific risk's code, as it appears in AFA.
level	String	The risk's severity.
title	String	The risk's title/description.
profile	String	The risk's profile name.

➔ See also:

- AppViz data types

Service

Element	Type	Description
`protocol`	String	The service's protocol.
`port`	String	The service's port.

➔ See also:

- AppViz data types

ServiceObject

Element	Type	Description
port	String	Service object port.
protocol	String	Service object protocol.

➔ See also:

- AppViz data types

Status

Element	Type	Description
success	Boolean	Whether status is success.
message	String	Status message.
errors	Object *additionalProperties*	Error properties.

➔ See also:

- AppViz data types

Vulnerability

Element	Type	Description
ip	String	IP.
description	String	Description of vulnerability.
id	String	ID of vulnerability.
title	String	Title.
cvss	Integer	Computer Vulnerability Scoring System score.

➔ See also:

- AppViz data types

AppViz Permissions

Following are the names of all AppViz permissions. These permissions grant a user or role the ability to view content and/or perform actions.

- viewAllApplications - Can view all applications.
- editAllApplications - Can edit all applications.
- createNewApplications - Can create applications.
- refreshConnectivity - Can refresh connectivity.

- viewVulnerability - Can view vulnerabilities.
- refreshVulnerability - Can refresh vulnerabilities.
- editNetworkObjects - Can edit network objects.
- createSharedFlows - Can create shared flows.
- createLabels - Can create labels for applications.
- refreshRisksData - Can refresh risk data.
- viewRisksData - Can view risk data.
- editServiceObjects - Can edit service objects.
- applyDrafts - Can apply drafts to applications.
- updateObjectFromDevice - Can update objects from a device.
- viewActivityLog - Can view activity logs.
- viewChangeRequests - Can view change requests.
- EditApplicationInformation - Can edit application information.

Request for application flows example

The following is an example of a request for application flows and the JSON response.

Get flows for an application

```
GET /applications/{id}/flows
```

This API call returns all flows of a specific application revision.

To run it, provide a revision ID for an application, and it will return an array of JSON Flow (see Flow) objects.

Flow is a complex JSON object that contains reference to other JSON objects, such as NetworkObject (see NetworkObject).

CURL Request example:

```
curl -u admin:algosec -k https://10.20.1.1/BusinessFlow/rest/v1/applications/
238/flows
```

Get flows response

The curl call produces the following JSON output:

```
[
 {
  "flowID":3282,
  "name":"7",
  "connectivityStatus":"None",
  "comment":"",      …
```

The output includes all relevant information on the application's flows.

Send us feedback

Let us know how we can improve your experience with the API Guide.

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online ASMS Tech Docs.