SecDevice 10.0.0
REST API Reference

November, 2024

Table of Contents

Overview

The SecDevice API (aGAPI) is a programmatic interface that allows you to securely connect and programmatically control SecDevice. Based on Representational State Transfer (REST), aGAPI allows you to do most of the configuration and monitoring operations as you would through SecDevice's Graphical User Interface (GUI).

aGAPI is particularly useful in allowing you to do the following:

- Maintain your own management console while accessing and displaying DDoS attack and mitigation information from SecDevice.
- Dynamically trigger DDoS mitigation using the TPS mitigator through SecDevice when an attack is detected by a (non-A10) third-party detection system.

The following topics are covered:

Getting Started with aGAPI

To use aGAPI, you must submit a key-based authentication. The following process is used for signing and authenticating Rest API requests:

Step 1: Request a signature for authentication

Send a POST request to the URI `agapi/auth/login` using the credentials for the SecDevice. This request retrieves an authorization signature to be used to authenticate API calls.

```
https://<SecDevice management ip>/agapi/auth/login/
```

See Login for a python login example.

Step 2: Configure and monitor the SecDevice system

Use methods (such as GET, POST, PUT, and so on) along with the authorization signature retrieved in Step 1 to configure and monitor the SecDevice system.

Step 3: Log out of session.

Log out to inform the API that authorization is no longer needed for the signature retrieved in Step 1.

Send a POST request to the URI `/agapi/auth/logout` indicating that all aGAPI operations have been completed for the current authorized session.

NOTE: aGAPI operates over an encrypted HTTPS connection.

Field Types

Following are the standard field types used:

- UUID: Universally Unique Identifier
- String: Up to 255 alphanumeric characters
- Boolean: A value of True (or 1) or False (or 0)
- Integer: Whole numbers

- DateTime: Used for data and time. Uses the ISO 8601 W3C format (YYYY-MM-DDThh:mmTZD).
- URL: A URL represented as a string

Common Response Codes

When a client sends its request to a server, the server sends status codes as its responses to those requests. Following are the standard HTTP status codes returned:

- **200 OK**

  The request has been succeeded. The information returned depends on the HTTP method used in the request. For example, in a GET request, this status code indicates that the response contains the requested resource.

- **201 Created**

  The request has been fulfilled resulting in a new resource being created.

- **202 Accepted**

  The request has been accepted for processing, but the processing has not been completed. When the processing occurs, the request may or may not be completed.

- **204 No Content**

  The server has successfully received the request but is not returning any response.

- **400 Bad Request**

  The server cannot process the request because of a client error.

- **401 Unauthorized**

  The response is sent when authentication is required or failed.

- **403 Forbidden**

  The request is valid, but the server is refusing to react to the request.

- **404 Not Found**

The requested resource cannot be found but could be available in the future.

- **500 Internal server Error**

  The server encountered an unexpected condition which prevented the server from fulfilling the request.

aGAPI Request Format

This section describes the aGAPI header, supported methods, data, and return codes.

aGAPI provides access to resources via URI. To use aGAPI, the application must make an HTTP request and parse the response. By default, JavaScript Object Notation (JSON) is used as a format for input payload and response data.

Use the following syntax for requesting aGAPI:

```
https://<SecDevice IP or DNS name>/<resourceURI>?<queryString>
Host: agapi.a10networks.com
Date: <date>
Accept: application/json
...
Authorization: <signature>

{
... <JSON object in POST body> ...
}
```

In the above syntax,

- <method> represents one of the following HTTP methods: POST, GET, PUT, DELETE, OPTIONS.
- <resourceURI> denotes the URI of the resource on SecDevice. The URI format is /agapi/<version>/<resource>/
- The current version of the aGAPI URI starts with /agapi/**v1**/...
- <queryString> is the list of parameters that may be used to filter the output of the command.
- <signature> identifies the authorization token that allows access to the resource.

Login

The following python login example authenticates your use of API endpoint:

```
import json
from pprint import pformat as pf

import requests

BASE_URL = 'http://<agalaxy-ip>/'
client = requests.session()

#if your SecDevice does not have a signed certificate
#the connection client will complain about the untrusted cert
#So, you can bypass a signed cert by setting the verify flag as False
client.verify = False

# Set up the headers for the JSON content type
headers = {
    'content-type': 'application/json',
    'accept': 'application/json',
}

client.headers.update(headers)
payload = {"credentials": {
    'username': 'admin',
    'password': 'a10'
}}


url = BASE_URL + 'agapi/auth/login/'
# POST the login
login_response = client.post(url, data=json.dumps(payload))
print pf(login_response.json())


# After a successful authentication with the requests client
# agapi endpoints can be accessed. For example,

# Get the list of devices
```

```
url = BASE_URL + 'agapi/v1/device/'
resp = client.get(url)
devices = resp.json()
print pf(devices)

# aGAPI handles session-management via cookies
# To reuse the session with another requests client
# refer to following example.

# Fetch the aGAPI session from cookie `agapisession`
token = client.cookies.get('agapisession')

# Initialize another client
client2 = requests.session()
# Turn off SSL verification for unsigned certs
client2.verify = False
# Update the headers
client2.headers.update(headers)

# Create and set cookie to send with `client2`
cookies = requests.cookies.create_cookie('agapisession', token)
client2.cookies.set_cookie(cookies)

# Access aGAPI with `client2`
url = BASE_URL + 'agapi/v1/device/'
resp = client2.get(url)
devices = resp.json()
print pf(devices)
```

Log Out

Log out to inform the API that authorization is no longer needed. Send a POST request to the URI `/agapi/auth/logout` indicating to the ACOS device that all aGAPI operations have been completed for the current authorized session.

Method	URL
POST	https://<host IP>/auth/logout/

Session Timeout

The session timeout specifies the time-out duration assigned for the aGAPI session objects, in minutes. The session ends if the user does not refresh or request a page within the time-out period.

By default, the session timeout value is 30 minutes.

Using the Browser-based SecDevice API (aGAPI)

SecDevice provides an on-box aGAPI browser which allows you to view the REST API documentation and quickly perform simple REST operations.

To login to the browser, go to the following URL:

```
https://<SecDevice management ip>/agapi/auth/doc/login/
```

NOTE: Do not forget to add “/” after `/login`.

To access resources using the aGAPI browser, go to the following URL:

```
https://<SecDevice management ip address>/agapi/<version>/<resource>/
```

In the above URL:

- `<SecDevice management ip address>` is the SecDevice’s management IP address.
- `<version>` is the current version of the aGAPI.
- `<resource>` is the resource you wish to access.

For example, if your SecDevice IP address is 192.0.2.0 and you want to access the list of devices for aGAPI version 1, type:

```
https://192.0.2.0/agapi/v1/device/
```

For information on API resources, see aGAPI Management Resources.

NOTE: Do not forget to add “/” after the <resource>.

HTTP Request Methods

SecDevice supports the followings HTTP request methods:

- **GET**—Requests a specific resource or a list of resources. A successful HTTP request returns a status code of “200 OK”.
- **POST**—Creates a new resource. A successful HTTP creation returns a status code of “201 Created”.
- **PUT**—Replaces the specified resource. A successful update returns a status code of “200 OK”.

NOTE: If you need to modify only a subset of parameters, first use GET and then use PUT to replace the resource. Occasionally, aGAPI uses a POST request to perform an update.

- **DELETE**—Deletes the specified resources. A successful deletion returns a status code of “200 OK”.
- **OPTIONS**—Describes the communication options for obtaining the attributes and its properties for the target resource. Sending this type of request to the endpoint will return schema information (e.g. value types and ranges).

aGAPI Filters

You can use various types of filter (such as pagination, object count, search, and ordering/sorting) to help you configure and manage devices and data with granularity.

NOTE: Query parameters are available (where noted) on list endpoints.

Getting Count

Following is an example of getting a total count of objects:

```
HTTP GET/agapi/v1/ddos/ zone/?total=True
HTTP 200 OK
    Content-Type: application/json
    Vary: Accept
    Allow: GET, OPTIONS

    {
        "total": 20
    }
```

This request returns the following status:

```
HTTP 200{“total”:<integer>}
```

Pagination

By default, GET queries in aGAPI for a collection of objects returns 20 objects. You can adjust the default count by using the start and count option for the set of results.

```
HTTP GET  /agapi/v1/ddos/zone/?start=0&count=10(first page of 10 objects)
HTTP GET /agapi/v1/ddos/zone/?start=10&count=10(second page of 10 objects)
```

The example below shows an adjustment in pagination:

```
GET /agapi/v1/event/?start=0&count=2
HTTP 200 OK
    Content-Type: application/json
    Vary: Accept
    Allow: GET, OPTIONS

    {
        "event_list": [
            {
                "acknowledged_time": null,
                "url": "http://agalaxy/agapi/v1/event/",
                "logical_device": null,
                "description": "Discovery via management action",
                "source_ip": "192.168.212.124",
                "id": "29286eb4-79ce-4a89-9d16-61eb00d2fcc8",
                "source_machine": null,
                "created_time": "2015-06-19 11:08:41",
                "type": "a10.agalaxy.rpc.asynchronized_publish.executor_
device_management_discovery",
                "event_data": null,
                "acknowledging_user_id": null,
                "severity": 1
            },
            {
                "acknowledged_time": null,
                "url": "http://agalaxy/agapi/v1/event/",
                "logical_device": "2e324486-4b58-42a9-b6e3-aa0cbc14",
                "description": "Automatic device config backup",
                "source_ip": "10.6.7.8",
                "id": "35948baf-19b1-4092-8549-c26185f6e669",
                "source_machine": null,
                "created_time": "2015-06-19 10:39:27",
                "type": "a10.agalaxy.rpc.asynchronized_publish.executor_
device_configuration_backup_to_database",
                "event_data": null,
                "acknowledging_user_id": null,
                "severity": 1
            }
        ]
    }
```

Searching

The Search feature is case-insensitive:

```
HTTP GET /agapi/v1/ddos/zone/?search=<string>
```

Ordering results

Prefixing the field with a hyphen will reverse the order:

```
HTTP GET  /agapi/v1/ddos/zone/?ordering=created
HTTP GET /agapi/v1/ddos/zone/?ordering=-created
```

aGAPI Management Resources

This chapter provides an overview of how you use endpoints in SecDevice to configure and monitor the SecDevice system.

The API is broken down to the following categories. Within each of these categories, you can use methods to manage many resources.

The following topics are covered:

SecDevice System

To access the SecDevice system, use the following endpoint:

Method	URL Path
GET	https://<host IP>/agapi/v1/system/

This endpoint provides information on the software version, platform model, and so on. For information on the standard API fields and returns codes, refer to Field Types and Common Response Codes.

Sample Request:

```
HTTP GET /agapi/v1/system/
```

Sample Response:

```
HTTP 200 OK
{    "platform": {
"serial_number": "",
       "product_name": "VMware"
   },
"ha": {
       "status": "Unknown",
"pace_maker_online_status_code": "3",
"pace_maker_online_status": "Both Down",
"local_hostname": "AG-192-168-212-125",
       "local_mgmt_ip_info": "192.168.212.125/24",
"active": "false",
"local_ha_ip_info": "192.168.122.1/24"
},
   "version": "5.0.0.163",
"uuid": "52334ac4-6738-4faa-b339-bb10866e5ad5",
   "license": {
       "max_devices": 20,
"max_partitions": 99999999,
       "expires_at": null,
       "max_objects": 99999999,
"platform_type": "any",
       "license_type": "agalaxy_tps"
}
}
```

Device Management

You can manage a single device or a group of devices.

The following topics are covered:

Device

This section covers several endpoints to allow you to manage devices that acts as a detector and a mitigator.

Operation	Method	URL Path	Payload
List all Devices	GET	/agapi/v1/device/	List of Device
Retrieve a Device	GET	/agapi/v1/device/{device-id}	Device
Add a Device	POST	/agapi/v1/device/	Device
Delete a Device	DELETE	/agapi/v1/device/{device-id}	

Device Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
ax_api_version: string(1...32), read-only, optional, Ax api version
mgmt_ip_address: string(1...256), read-only, optional, Mgmt ip address
boot_version: string(1...32), read-only, optional, Boot version
dns_name: string(1...64), read-only, optional, Dns name
id: string(1...), read-only, optional, Id
device_add_time: string(1...32), read-only, optional, Device add time
device_credentials: nested object(s), read-write, optional, Device
credentials
```

```
device_groups: list, read-only, optional, Device groups
boot_device: string(1...32), read-only, optional, Boot device
model: string(1...32), read-only, optional, Model
partitions: list, read-only, optional, Partitions
```

Sample Request:

```
HTTP GET /agapi/v1/device/
```

Sample Response:

```
HTTP GET /agapi/v1/device/
{
    "device_list": [
        {
            "boot_version": "3.2.3, build 125 ",
            "mgmt_ip_address": "192.168.212.136",
            "ax_api_version": "3.0",
            "url": "https://192.168.212.125/agapi/v1/device/006521cc-8510-
4f6a-a109-9a07165096be/",
            "dns_name": "TPS323-136",
            "model": "vThunder",
            "device_add_time": "2018-10-09 22:37:44",
            "device_credentials": {
                "cli_credentials": {
                    "password": "kNTso23pwoPt4QTRS9Cq2NmsTA==",
                    "enable_password": "u87N_QIufHy-4kKw5P_PbQ=="
                },
                "snmp_credentials": {},
                "https_credentials": {
                    "username": "admin",
                    "password": "tm3EPGYCbAKdPoLWlJ5En8G9zg=="
                }
            },
            "device_groups": [
                {
                    "id": "22b3b891-b65e-437d-a987-0b2b0828b227",
                    "group_name": "TPS323-136"
                },
                {
                    "id": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
                    "group_name": "All Mitigators"
                }
            ],
            "boot_device": "HD_PRIMARY",
            "id": "006521cc-8510-4f6a-a109-9a07165096be",
            "partitions": [
                "shared"
            ]
        },
        {
            "boot_version": "4.1.4-P2, build 185 ",
            "mgmt_ip_address": "10.0.7.137",
            "ax_api_version": "3.0",
            "url": "https://192.168.212.125/agapi/v1/device/2f45d2ce-b791-
430f-ad58-cc6ca8d19009/",
            "dns_name": "ThunderADC-137",
            "model": "vThunder",
            "device_add_time": "2018-10-21 03:32:51",
            "device_credentials": {
                "cli_credentials": {
                    "password": "bAaqwLWC9qyMYXK2jezpC7pzdw==",
                    "enable_password": "fch1cxGoDwrYbdarJmtV6Q=="
                },
                "snmp_credentials": {},
                "https_credentials": {
                    "username": "admin",
                    "password": "9XB950j0a4paIySp9LEHDKKoMw=="
                }
            },
            "device_groups": [],
            "boot_device": "HD_SECONDARY",
            "id": "2f45d2ce-b791-430f-ad58-cc6ca8d19009",
            "partitions": [
                "shared"
            ]
        },
        {
            "boot_version": "3.2.2-P5, build 94 ",
            "mgmt_ip_address": "192.168.212.137",
            "ax_api_version": "3.0",
            "url": "https://192.168.212.125/agapi/v1/device/9d100660-5b17-
4d8e-8dc0-d7d0f0071e16/",
            "dns_name": "TPS322-137",
            "model": "vThunder",
            "device_add_time": "2018-10-09 22:37:43",
            "device_credentials": {
                "cli_credentials": {
                    "password": "junfSb2zmvtBDTYnywagfs8-KA==",
                    "enable_password": "eTgUsrfeyEQiA33gRLo9DQ=="
                },
                "snmp_credentials": {},
                "https_credentials": {
                    "username": "admin",
                    "password": "XZ9HWKFTl_0OkhIfu9JUqP0dVA=="
                }
            },
            "device_groups": [
                {
                    "id": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
                    "group_name": "All Mitigators"
                },
                {
                    "id": "e1c33fd8-c511-480d-99e6-c5b23395e6b3",
                    "group_name": "TPS322-137"
                }
            ],
            "boot_device": "HD_SECONDARY",
            "id": "9d100660-5b17-4d8e-8dc0-d7d0f0071e16",
            "partitions": [
                "shared"
            ]
        },
        {
            "boot_version": "3.2.3, build 150 ",
            "mgmt_ip_address": "192.168.212.135",
            "ax_api_version": "3.0",
            "url": "https://192.168.212.125/agapi/v1/device/d650045e-b433-
4a3e-8af5-33458c2100c5/",
            "dns_name": "TPS323-DET-135",
            "model": "vThunder",
            "device_add_time": "2018-10-09 22:37:44",
            "device_credentials": {
                "cli_credentials": {
                    "password": "zBbk0b5xZW70mTF7F3pY3p0RRQ==",
                    "enable_password": "SiZr-P9F-XVJPfnujX-x6w=="
                },
                "snmp_credentials": {},
                "https_credentials": {
                    "username": "admin",
                    "password": "Pls277-oGaYXu7TB8VydGZjZFQ=="
                }
            },
            "device_groups": [],
            "boot_device": "HD_PRIMARY",
            "id": "d650045e-b433-4a3e-8af5-33458c2100c5",
            "partitions": [
                "shared"
            ]
        }
    ]
}
```

Sample Request:

```
HTTP GET /agapi/v1/device/{device-id}/
```

Sample Response:

```
HTTP 200 OK
{
    "device": {
        "boot_version": "3.2.3, build 150 ",
        "mgmt_ip_address": "192.168.212.135",
        "ax_api_version": "3.0",
        "url": "https://192.168.212.125/agapi/v1/device/d650045e-b433-
4a3e-8af5-33458c2100c5/",
        "dns_name": "TPS323-DET-135",
        "model": "vThunder",
        "device_add_time": "2018-10-09 22:37:44",
        "device_credentials": {
            "cli_credentials": {
                "password": "yyM3Ll4j_4U62NT1HXfph_Ws9Q==",
                "enable_password": "TfRZasx1DxQRLlQCU3jiJQ=="
            },
            "snmp_credentials": {},
            "https_credentials": {
                "username": "admin",
                "password": "xay-t6BL7hS7VD0nQuZmG_MHRQ=="
            }
        },
        "device_groups": [],
        "boot_device": "HD_PRIMARY",
        "id": "d650045e-b433-4a3e-8af5-33458c2100c5",
        "partitions": [
            "shared"
        ]
    }
}
```

Device Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

device_host: string(1...1024), read-write, required, Device host

device_credentials: nested object(s), read-write, optional, Device credentials

Sample Request:

```
HTTP POST /agapi/v1/device/
{
    "device_host": "192.168.212.136",
    "device_credentials": {
        "cli_credentials": {
            "username": "",
            "password": "",
            "enable_password": ""
        },
        "https_credentials": {
            "username": "admin",
            "password": "a10"
        },
        "snmp_credentials": {
            "read_community": ""
        }
    }
}
```

Sample Response:

```
HTTP 202 Accepted
{
    "message": "Device discovery submitted",
    "code": 202,
    "scheduled_task_id": "1c2ef899-fe67-41f3-8297-8c6053f63e3b"
}
```

Device Object Attributes

Sample Request:

```
HTTP DELETE /agapi/v1/device/{device-id}/
```

Sample Response:

```
HTTP 204 No Content
```

Device Groups

Device Groups are used on SecDevice to group managed devices together for operations and/or actions. A common use of Device Groups is when associating a TPS Zone with a group of TPS Mitigator devices. This section covers several endpoints to allow you to manage device groups.

Operation	Method	URL	Payload
List all Device	GET	/agapi/v1/device-group/	List of Device

Operation	Method	URL	Payload
Groups			Group
Retrieve a Device Group	GET	/agapi/v1/device-group/{device-group-id}	Device Group
Create a Device Group	POST	/agapi/v1/device-group/	Device Group
Update a Device Group	POST	/agapi/v1/device-group/	Device Group

Device Group Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
device_list: list, read-write, required, Device list
group_name: string(1...64), read-write, required, Group name
device_group_type: integer(1...3), read-write, optional, Device group type
description: string(1...256), read-write, optional, Description
```

Sample Request: List All Device Group

```
HTTP GET /agapi/v1/device-group/
```

Sample Response:

```
HTTP 200 OK
{
    "device_group_list": [
        {
            "url": "https://192.168.212.125/agapi/v1/device-
group/22b3b891-b65e-437d-a987-0b2b0828b227/",
            "device_group_type": 1,
            "group_name": "TPS323-136",
            "description": "",
            "device_list": [],
            "id": "22b3b891-b65e-437d-a987-0b2b0828b227"
        },
        {
            "url": "https://192.168.212.125/agapi/v1/device-
group/7d08a417-b5e5-49f2-a94a-e37d896ae8de/",
            "device_group_type": 1,
            "group_name": "All Mitigators",
            "description": "",
            "device_list": [
                {
                    "dns_name": "TPS322-137",
                    "mgmt_ip_address": "192.168.212.137",
                    "id": "9d100660-5b17-4d8e-8dc0-d7d0f0071e16",
                    "boot_version": "3.2.2-P5, build 94 "
                }
            ],
            "id": "7d08a417-b5e5-49f2-a94a-e37d896ae8de"
        },
        {
            "url": "https://192.168.212.125/agapi/v1/device-
group/e1c33fd8-c511-480d-99e6-c5b23395e6b3/",
            "device_group_type": 1,
            "group_name": "TPS322-137",
            "description": "",
            "device_list": [
                {
                    "dns_name": "TPS322-137",
                    "mgmt_ip_address": "192.168.212.137",
                    "id": "9d100660-5b17-4d8e-8dc0-d7d0f0071e16",
                    "boot_version": "3.2.2-P5, build 94 "
                }
            ],
            "id": "e1c33fd8-c511-480d-99e6-c5b23395e6b3"
        }
    ]
}
```

Sample Response: Retrieve Device Group

```
HTTP 200 OK
{
    "device_group": {
        "url": "https://192.168.212.125/agapi/v1/device-group/22b3b891-
b65e-437d-a987-0b2b0828b227/",
        "device_group_type": 1,
        "group_name": "TPS323-136",
        "description": "",
        "device_list": [],
        "id": "22b3b891-b65e-437d-a987-0b2b0828b227"
    }
}
```

Device Group Object Attributes

```
device_list, (list), required, Device list
group_name, string(1....64), required, Group name
device_group_type, integer(1....3), optional, Device group type
description, string(1....256), optional, Description
```

Sample Request: Create Device Group

```
HTTP POST /agapi/v1/device-group/
{
    "device_group_type": 1,
    "group_name": "All-TPS-Mitigators",
    "description": "All TPS mitigator devices",
    "device_list": ["9d100660-5b17-4d8e-8dc0-d7d0f0071e16", "f11fac66-
6b36-4148-abc2-a22845adb091"]
}
```

Sample Response:

```
HTTP 201 Created
{
    "id": "4caa0f15-2e90-4f1a-9685-def34f086c1f",
    "url": "https://192.168.212.125/agapi/v1/device-group/4caa0f15-2e90-
4f1a-9685-def34f086c1f/",
    "description": "All TPS mitigator devices",
    "device_list": [
        {
            "dns_name": "TPS322-137",
            "mgmt_ip_address": "192.168.212.137",
            "id": "9d100660-5b17-4d8e-8dc0-d7d0f0071e16",
            "boot_version": "3.2.2-P5, build 94 "
        },
        {
            "dns_name": "TPS323-136",
            "mgmt_ip_address": "192.168.212.136",
            "id": "f11fac66-6b36-4148-abc2-a22845adb091",
            "boot_version": "3.2.3, build 144 "
        }
    ],
    "group_name": "All-TPS-Mitigators"
}
```

Sample Request: Update Device Group

```
HTTP POST /agapi/v1/device-group/
{
    "device_group_type": 1,
    "group_name": "All-TPS-Mitigators",
    "description": "All TPS mitigator devices",
    "device_list": ["9d100660-5b17-4d8e-8dc0-d7d0f0071e16", "f11fac66-
6b36-4148-abc2-a22845adb091"]
}
```

Sample Response:

```
HTTP 200 OK
{
    "url": "https://192.168.212.125/agapi/v1/device-group/4caa0f15-2e90-
4f1a-9685-def34f086c1f/",
    "group_name": "Main Mitigators",
    "description": "Main TPS Mitigator Devices",
    "device_list": [
        {
            "dns_name": "TPS322-137",
            "mgmt_ip_address": "192.168.212.137",
            "id": "9d100660-5b17-4d8e-8dc0-d7d0f0071e16",
            "boot_version": "3.2.2-P5, build 94 "
        },
        {
            "dns_name": "TPS323-136",
            "mgmt_ip_address": "192.168.212.136",
            "id": "f11fac66-6b36-4148-abc2-a22845adb091",
            "boot_version": "3.2.3, build 144 "
        }
    ],
    "id": "4caa0f15-2e90-4f1a-9685-def34f086c1f"
}
```

Protected Objects

A protected object is an IP address of the attacker you want to stop or the target (servers) you want to protect.

The following topics are covered:

Protected Zone

A protected zone is an object comprised of a group of IP addresses and/or subnets, ports, and protocols that provide a service and are protected as a single entity.

Operation	Method	URL Path	Payload
List Zones	GET	/agapi/v1/ddos/zone/	List of Protected Zones
Create a Zone	POST	/agapi/v1/ddos/zone/	Protected Zone
Retrieve a specific Zone	GET	/agapi/v1/ddos/zone/{zone-id}/	Protected Zone
Update a specific Zone	PUT	/agapi/v1/ddos/zone/{zone-id}	Protected Zone
Delete a specific Zones	DELETE	/agapi/v1/ddos/zone/{zone-id}	
Retrieve a Zone Chart	GET	/agapi/v1/ddos/zone/{zone-id}/charts/	
Retrieve a Zone	GET	/agapi/v1/ddos/zone/{zone-	

Operation	Method	URL Path	Payload
Service Chart		id}/service/{service}/charts/	

Protected Zone Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
zone_name: string(1...63), read-write, required, Zone name
port_range_list: nested object(s), read-write, optional, Port range list
packet_capture_policy: string(1...63), read-write, optional, Packet
capture policy
device_group: string(1...), read-write, optional, Device group
detection: nested object(s), read-write, optional, Detection
inbound_forward_dscp: integer(1...63), read-write, optional, Inbound
forward dscp
profile_name: string(1...63), read-write, optional, Profile name
outbound_forward_dscp: integer(1...63), read-write, optional, Outbound
forward dscp
id: string(1...), read-only, optional, Id
advertised_enable: boolean, read-write, optional, Advertised enable
domain_id: string(1...), read-only, optional, Domain id
ip_proto_list: nested object(s), read-write, optional, Ip proto list
src_port: nested object(s), read-write, optional, Src port
ip_list: list, read-write, optional, Ip list
hw_blacklist_blocking: nested object(s), read-write, optional, Hw
blacklist blocking
zone_template: nested object(s), read-write, optional, Zone template
port: nested object(s), read-write, optional, Port
operational_mode_error: boolean, read-only, optional, Operational mode
error
detector_group: string(1...), read-write, optional, Detector group
zone_oper_policy: string(1...63), read-write, optional, Zone oper policy
creating_user_id: string(1...), read-only, optional, Creating user id
status: choice, read-only, optional, Status
continuous_learning: boolean, read-write, optional, Continuous learning
operational_mode: choice, read-write, optional, Operational mode
description: string(1...63), read-write, optional, Description
glid: string(1...63), read-write, optional, Glid
log_enable: boolean, read-write, optional, Log enable
oper_status: string(1...63), read-only, optional, Oper status
```

```
src_port_range_list: nested object(s), read-write, optional, Src port
range list
zone_level_topk_dest_num_records: integer(1...100), read-write, optional,
Zone level topk dest num records
zone_level_topk_num_records: integer(1...100), read-write, optional, Zone
level topk num records
telemetry_enable: boolean, read-write, optional, Telemetry enable
dynamic_params: nested object(s), read-write, optional, Dynamic params
created: datetime, read-only, optional, Created
url: nested object(s), read-only, optional, Url
modified: datetime, read-only, optional, Modified
log_periodic: boolean, read-write, optional, Log periodic
```

List Zones

Get a list of all zones.

Method	URL
GET , OPTIONS	/agapi/v1/ddos/zone/

Filter Fields:

You can identify a specific parameter using the filter field.

Field	Notes
zone_name	Zone name
status	Zone status (normal, mitigation, error)
device_group	Mitigation device group ID
detector_group	Detector device group ID

Ordering Fields:

You can sort parameter by the following types:

Field	Notes
name	Order by zone name

Field	Notes
status	Order by zone status
created	Order by creation timestamp
modified	Order by last modified timestamp

Sample Request:

```
[
{
"packet_capture_policy": "A10_Default",
"uuid_dict": {
"638450c7-f997-4975-ba37-253daa2533a8": {
"zone": "8d4f023a-4118-11eb-b3a4-931241a9b2ad",
"service": {
"53+tcp": {
"indicator": "8d50248a-4118-11eb-b3a4-931241a9b2ad",
"general": "8d4ff29e-4118-11eb-b3a4-931241a9b2ad"
}
}
},
"d71dc0c6-8ce0-4fd9-a0cd-ccd7d2ad4c16": {
"zone": "8ccef52c-4118-11eb-917e-c3d6ed50a64a",
"service": {
"53+tcp": {
"indicator": "8ccffa94-4118-11eb-917e-c3d6ed50a64a",
"general": "8ccfe734-4118-11eb-917e-c3d6ed50a64a"
}
}
}
},
"device_group": null,
"modified": "2020-12-18T10:18:40Z",
"id": "457052c2-a31e-4378-ae47-a155b54e6339",
"zone_name": "172.140.4..98",
"advertised_enable": false,
"domain_id": null,
"ip_proto_list": [],
"src_port": {
"zone_src_port_other_list": [],
"zone_src_port_list": []
},
"ip_list": [
"172.140.4.98"
],
"zone_template": "A10_LOGGING_Basic",
"port_range_list": [],
"port": {
"zone_service_list": [
{
"deny": false,
"protocol": "tcp",
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"topk_num_records": 20,
"port": 53,
"src_based_policy_list": []
}
],
"zone_service_other_list": []
},
"operational_mode_error": false,
"detector_id": null,
"zone_oper_policy": "QA_Policy_Flowspec",
"creating_user_id": null,
"status": "normal",
"operational_mode": "monitor",
"account_id": null,
"log_enable": true,
"oper_status": "ok",
"src_port_range_list": [],
"telemetry_enable": false,
"dynamic_params": [
{
"indicators": [
{
"name": "conn-miss-rate",
"value": 0.0
},
{
"name": "syn-fin-ratio",
"value": 0.0
},
{
"name": "pkt-rate",
"value": 100.0
},
{
"name": "concurrent-conns",
"value": 0.0
},
{
"name": "small-window-ack-rate",
"value": 0.0
},
{
"name": "rst-rate",
"value": 0.0
},
{
"name": "fin-rate",
"value": 0.0
},
{
"name": "empty-ack-rate",
"value": 0.0
},
{
"name": "syn-rate",
"value": 0.0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "small-payload-rate",
"value": 0.0
},
{
"name": "pkt-drop-rate",
"value": 0.0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
}
],
"protocol": "tcp",
"port": "53"
}
],
"created": "2020-12-18T10:05:23Z",
"url": "https://10.64.1.72/agapi/v1/ddos/zone/457052c2-a31e-4378-ae47-
a155b54e6339/",
"controller_id": "af795eea-4fa9-4444-b5d7-9ee352ac3ca3",
"log_periodic": false
},
{
"packet_capture_policy": "A10_Default",
"uuid_dict": {
"a949f8a8-d4a9-4516-969f-bb8c13c4a3fc": {
"zone": "7d2c4614-518b-11eb-9698-b9767ec9423b",
"service": {
"80+http": {
"indicator": "7d2ec3ee-518b-11eb-9698-b9767ec9423b",
"general": "7d2eafb2-518b-11eb-9698-b9767ec9423b"
},
"25+tcp": {
"indicator": "7d2e4662-518b-11eb-9698-b9767ec9423b",
"general": "7d2e2d6c-518b-11eb-9698-b9767ec9423b"
},
"ip-proto+other": {
"indicator": "7d2e054e-518b-11eb-9698-b9767ec9423b",
"general": "7d2df3a6-518b-11eb-9698-b9767ec9423b"
},
"ip-proto+icmp-v4": {
"indicator": "7d2dc78c-518b-11eb-9698-b9767ec9423b",
"general": "7d2db436-518b-11eb-9698-b9767ec9423b"
},
"1004+1010+tcp": {
"indicator": "7d2f0430-518b-11eb-9698-b9767ec9423b",
"general": "7d2ef076-518b-11eb-9698-b9767ec9423b"
},
"53+dns-tcp": {
"indicator": "7d2e8384-518b-11eb-9698-b9767ec9423b",
"general": "7d2e7038-518b-11eb-9698-b9767ec9423b"
}
}
},
"49519b96-3e77-4e9b-b1e1-716d55948cf4": {
"service": {
"80+http": {
"indicator": "74e927ce-518b-11eb-ba18-7d68941ec461",
"general": "74e8f538-518b-11eb-ba18-7d68941ec461"
},
"25+tcp": {
"indicator": "74e6531e-518b-11eb-ba18-7d68941ec461",
"general": "74e6351e-518b-11eb-ba18-7d68941ec461"
},
"ip-proto+other": {
"indicator": "74e5ee42-518b-11eb-ba18-7d68941ec461",
"general": "74e5d56a-518b-11eb-ba18-7d68941ec461"
```

```
},
"ip-proto+icmp-v4": {
"indicator": "74e583bc-518b-11eb-ba18-7d68941ec461",
"general": "74e4e6a0-518b-11eb-ba18-7d68941ec461"
},
"1004+1010+tcp": {
"indicator": "74e9cb34-518b-11eb-ba18-7d68941ec461",
"general": "74e99506-518b-11eb-ba18-7d68941ec461"
},
"53+dns-tcp": {
"indicator": "74e6cb82-518b-11eb-ba18-7d68941ec461",
"general": "74e6a350-518b-11eb-ba18-7d68941ec461"
}
},
"zone": "74e3ea02-518b-11eb-ba18-7d68941ec461"
}
},
"device_group": null,
"modified": "2021-01-08T08:29:17Z",
"id": "26506db4-4f27-4a0c-9845-e2f487af86e9",
"zone_name": "172.140.4.105",
"advertised_enable": false,
"domain_id": null,
"ip_proto_list": [
{
"protocol": "icmp-v4",
"drop_frag_pkt": false,
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
```

```
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"src_based_policy_list": [],
"topk_num_records": 20
},
{
"protocol": "other",
"drop_frag_pkt": false,
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"src_based_policy_list": [],
"topk_num_records": 20
}
],
"src_port": {
"zone_src_port_other_list": [],
"zone_src_port_list": []
},
"ip_list": [
"172.140.4.105",
"172.140.4.106",
"172.140.4.107"
],
"zone_template": "A10_LOGGING_Basic",
"port_range_list": [
{
"deny": false,
"port_range_end": 1010,
"protocol": "tcp",
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"port_range_start": 1004,
"topk_num_records": 20,
"src_based_policy_list": []
}
],
"port": {
"zone_service_list": [
{
"deny": false,
"protocol": "dns-tcp",
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"topk_num_records": 20,
"port": 53,
"src_based_policy_list": []
},
{
"deny": false,
"protocol": "http",
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"topk_num_records": 20,
"port": 80,
"src_based_policy_list": []
},
{
"deny": false,
"protocol": "tcp",
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"topk_num_records": 20,
"port": 25,
"src_based_policy_list": []
}
],
"zone_service_other_list": []
},
"operational_mode_error": false,
"detector_id": null,
"zone_oper_policy": "QA_Flowspec_auto_enable",
"creating_user_id": null,
"status": "mitigation",
"operational_mode": "monitor",
"account_id": null,
"log_enable": false,
"oper_status": "ok",
"src_port_range_list": [],
"telemetry_enable": false,
"dynamic_params": [
{
"indicators": [
{
"name": "conn-miss-rate",
"value": 0
},
{
"name": "syn-fin-ratio",
"value": 0.0
},
{
"name": "pkt-rate",
"value": 100
},
{
"name": "concurrent-conns",
"value": 0
},
{
"name": "small-window-ack-rate",
"value": 0
},
{
"name": "rst-rate",
"value": 0
},
{
"name": "fin-rate",
"value": 0
},
{
```

```
"name": "empty-ack-rate",
"value": 0
},
{
"name": "syn-rate",
"value": 0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "small-payload-rate",
"value": 0
},
{
"name": "pkt-drop-rate",
"value": 0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
}
],
"protocol": "dns-tcp",
"port": "53"
},
{
"indicators": [
{
"name": "conn-miss-rate",
"value": 0
},
{
"name": "syn-fin-ratio",
"value": 0.0
},
{
"name": "pkt-rate",
"value": 100
```

```
},
{
"name": "concurrent-conns",
"value": 0
},
{
"name": "small-window-ack-rate",
"value": 0
},
{
"name": "rst-rate",
"value": 0
},
{
"name": "fin-rate",
"value": 0
},
{
"name": "empty-ack-rate",
"value": 0
},
{
"name": "syn-rate",
"value": 0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "small-payload-rate",
"value": 0
},
{
"name": "pkt-drop-rate",
"value": 0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
```

```
}
],
"protocol": "http",
"port": "80"
},
{
"indicators": [
{
"name": "pkt-rate",
"value": 100
},
{
"name": "frag-rate",
"value": 0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "pkt-drop-rate",
"value": 0
}
],
"protocol": "icmp-v4"
},
{
"indicators": [
{
"name": "pkt-rate",
"value": 100
},
{
"name": "frag-rate",
"value": 0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "pkt-drop-rate",
"value": 0
}
],
"protocol": "other"
},
{
"indicators": [
{
"name": "conn-miss-rate",
"value": 0
},
{
"name": "syn-fin-ratio",
"value": 0.0
},
{
"name": "pkt-rate",
"value": 100
},
{
"name": "concurrent-conns",
"value": 0
},
{
"name": "small-window-ack-rate",
"value": 0
},
{
"name": "rst-rate",
"value": 0
```

```
},
{
"name": "fin-rate",
"value": 0
},
{
"name": "empty-ack-rate",
"value": 0
},
{
"name": "syn-rate",
"value": 0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "small-payload-rate",
"value": 0
},
{
"name": "pkt-drop-rate",
"value": 0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
}
],
"protocol": "tcp",
"port": "25"
},
{
"indicators": [
{
"name": "conn-miss-rate",
"value": 0
},
{
```

```
"name": "syn-fin-ratio",
"value": 0.0
},
{
"name": "pkt-rate",
"value": 100
},
{
"name": "concurrent-conns",
"value": 0
},
{
"name": "small-window-ack-rate",
"value": 0
},
{
"name": "rst-rate",
"value": 0
},
{
"name": "fin-rate",
"value": 0
},
{
"name": "empty-ack-rate",
"value": 0
},
{
"name": "syn-rate",
"value": 0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "small-payload-rate",
"value": 0
},
{
```

```
"name": "pkt-drop-rate",
"value": 0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
}
],
"port_range_end": 1010,
"protocol": "tcp",
"port_range_start": 1004
}
],
"created": "2021-01-08T08:27:57Z",
"url": "https://10.64.1.72/agapi/v1/ddos/zone/26506db4-4f27-4a0c-9845-
e2f487af86e9/",
"controller_id": "37eb6b10-a4a5-4677-9c15-622479a9bee2",
"log_periodic": false
}
]
```

NOTE: The “operational_mode” field is read-only. To transition between zone modes, use the endpoints in the Zone Actions section.

NOTE: Use HTTP OPTIONS to get the schema for the nested fields

Response Codes

See Common Response Codes.

Create Zones

When creating a new zone, a zone oper policy can be associated to the zone.

Method	URL
POST	/agapi/v1/ddos/zone/

Sample Request:

```
HTTP POST /agapi/v1/ddos/zone/
{
    "zone_name": "zone_111",
    "device_group": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
    "advertised_enable": false,
    "ip_proto_list": [
        {
            "profile_name": null,
            "protocol": "icmp-v4",
            "drop_frag_pkt": false
        },
        {
            "profile_name": null,
            "protocol": "icmp-v6",
            "drop_frag_pkt": false
        }
    ],
    "src_port": {
        "zone_src_port_other_list": [],
        "zone_src_port_list": []
    },
    "ip_list": [
        "111.1.1.1"
    ],
    "zone_template": {
        "logging": ""
    },
    "port_range_list": [],
    "port": {
        "zone_service_list": [
            {
                "deny": false,
                "profile_name": null,
                "protocol": "http",
                "port": 80
            }
        ],
        "zone_service_other_list": []
    },
    "zone_oper_policy": null,
    "operational_mode": "monitor",
    "log_enable": true,
    "src_port_range_list": [],
    "telemetry_enable": false,
    "log_periodic": true
}
```

NOTE: The “operational_mode" field is read-only.To transition between zone modes, use the endpoints in the Zone Actions section.

NOTE: Use HTTP OPTIONS to get the schema for the nested fields

Sample Response:

```
HTTP 201 Created
{
    "device_group": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
    "id": "1569dc02-f064-4d39-b4c8-810c343a7cc6",
    "zone_name": "zone_111",
    "advertised_enable": false,
    "port_range_list": [],
    "ip_proto_list": [
        {
            "profile_name": null,
            "protocol": "icmp-v4",
            "drop_frag_pkt": false
        },
        {
            "profile_name": null,
            "protocol": "icmp-v6",
            "drop_frag_pkt": false
        }
    ],
    "src_port": {
        "zone_src_port_other_list": [],
        "zone_src_port_list": []
    },
    "ip_list": [
        "111.1.1.1"
    ],
    "zone_template": {
        "logging": ""
    },
    "domain_id": "default",
    "port": {
        "zone_service_list": [
            {
                "deny": false,
                "profile_name": null,
                "protocol": "http",
                "port": 80
            }
        ],
        "zone_service_other_list": []
    },
    "operational_mode_error": false,
    "zone_oper_policy": null,
    "creating_user_id": "1e03df12-bb02-4b81-8840-092836577de5",
    "status": "normal",
    "operational_mode": "monitor",
    "log_enable": true,
    "oper_status": "unknown",
    "src_port_range_list": [],
    "telemetry_enable": false,
    "created": "2018-11-06T21:51:27.609Z",
    "url": "https://192.168.212.125/agapi/v1/ddos/zone/1569dc02-f064-4d39-
b4c8-810c343a7cc6/",
    "modified": "2018-11-06T21:51:27.609Z",
    "log_periodic": true
}
```

Response Codes

See Common Response Codes.

Create a Zone using Expand Subnet

NOTE: Add "is_per_addr_glid_set": true in zone payload for enabling Limit per address feature.

Sample Payload:

```
{
        "packet_capture_policy": "A10_Default",
        "domain_id": null,
        "device_group": null,
        "detection": {},
        "zone_name": "A10_S_Z1",
        "advertised_enable": false,
        "port": {
            "zone_service_list": [
                {
                    "deny": false,
                    "protocol": "tcp",
                    "enable_class_list_overflow": false,
                    "topk_dst_num_records": 10,
                    "glid_cfg": {
                        "glid_action": "drop",
                        "glid": "100"
                    },
                    "topk_num_records": 20,
                    "port": 25
                }
            ]
        },
        "is_per_addr_glid_set": true,
        "obj_type": "dst_zone",
        "zone_level_topk_num_records": 20,
        "zone_template": {
            "logging": "A10_LOGGING_Basic"
        },
        "id": "f8fe1219-eb6a-4a56-a464-e24c659e208c",
        "detector_group": null,
        "detector_id": null,
        "zone_oper_policy": "A10_Default",
        "creating_user_id": null,
        "status": "normal",
        "continuous_learning": false,
        "operational_mode": "monitor",
        "glid": "100",
        "log_enable": true,
        "oper_status": "ok",
        "zone_level_topk_dest_num_records": 10,
        "ip_list": [
            "10.22.5.0/24 expand-subnet dynamic",
            "2.3.4.2"
        ],
        "telemetry_enable": false,
        "dynamic_params": [],
        "created": "2022-11-16T11:17:17Z",
        "url": "https://10.64.1.205/agapi/v1/ddos/zone/f8fe1219-eb6a-4a56-
a464-e24c659e208c/",
        "modified": "2023-04-19T07:29:56Z",
        "log_periodic": false
    }
```

Response Codes

See Common Response Codes.

Retrieve Zones

Retrieve a zone object,.

Method	URL
GET, OPTIONS	*/agapi/v1/ddos/zone/{zone-id}/*

Sample Request:

```
HTTP GET /agapi/v1/ddos/zone/{zone-id}/
```

Sample Response:

```
{
"packet_capture_policy": "A10_Default",
"uuid_dict": {
"638450c7-f997-4975-ba37-253daa2533a8": {
"zone": "8d4f023a-4118-11eb-b3a4-931241a9b2ad",
"service": {
```

```
"53+tcp": {
"indicator": "8d50248a-4118-11eb-b3a4-931241a9b2ad",
"general": "8d4ff29e-4118-11eb-b3a4-931241a9b2ad"
}
}
},
"d71dc0c6-8ce0-4fd9-a0cd-ccd7d2ad4c16": {
"zone": "8ccef52c-4118-11eb-917e-c3d6ed50a64a",
"service": {
"53+tcp": {
"indicator": "8ccffa94-4118-11eb-917e-c3d6ed50a64a",
"general": "8ccfe734-4118-11eb-917e-c3d6ed50a64a"
}
}
}
},
"device_group": null,
"modified": "2020-12-18T10:18:40Z",
"id": "457052c2-a31e-4378-ae47-a155b54e6339",
"zone_name": "172.140.4..98",
"advertised_enable": false,
"domain_id": null,
"ip_proto_list": [],
"src_port": {
"zone_src_port_other_list": [],
"zone_src_port_list": []
},
"ip_list": [
"172.140.4.98"
],
"zone_template": "A10_LOGGING_Basic",
"port_range_list": [],
"port": {
"zone_service_list": [
{
"deny": false,
"protocol": "tcp",
"level_list": [
{
"level_num": "0",
"indicator_list": [
{
"zone_threshold_num": 100,
"score": 100,
"type": "pkt-rate"
}
],
"zone_template": {}
},
{
"level_num": "1",
"indicator_list": [],
"zone_template": {}
}
],
"profile_name": null,
"topk_num_records": 20,
"port": 53,
"src_based_policy_list": []
}
],
"zone_service_other_list": []
},
"operational_mode_error": false,
"detector_id": null,
"zone_oper_policy": "QA_Policy_Flowspec",
"creating_user_id": null,
"status": "normal",
"operational_mode": "monitor",
"account_id": null,
"log_enable": true,
"oper_status": "ok",
"src_port_range_list": [],
"telemetry_enable": false,
"dynamic_params": [
{
"indicators": [
{
"name": "conn-miss-rate",
"value": 0.0
```

```
},
{
"name": "syn-fin-ratio",
"value": 0.0
},
{
"name": "pkt-rate",
"value": 100.0
},
{
"name": "concurrent-conns",
"value": 0.0
},
{
"name": "small-window-ack-rate",
"value": 0.0
},
{
"name": "rst-rate",
"value": 0.0
},
{
"name": "fin-rate",
"value": 0.0
},
{
"name": "empty-ack-rate",
"value": 0.0
},
{
"name": "syn-rate",
"value": 0.0
},
{
"name": "bytes-to-bytes-from-ratio",
"value": 0.0
},
{
"name": "small-payload-rate",
"value": 0.0
```

```
},
{
"name": "pkt-drop-rate",
"value": 0.0
},
{
"name": "pkt-drop-ratio",
"value": 0.0
}
],
"protocol": "tcp",
"port": "53"
}
],
"created": "2020-12-18T10:05:23Z",
"url": "https://10.64.1.72/agapi/v1/ddos/zone/457052c2-a31e-4378-ae47-
a155b54e6339/",
"controller_id": "af795eea-4fa9-4444-b5d7-9ee352ac3ca3",
"log_periodic": false
}
```

Response Codes

See Common Response Codes.

Update Zones

When updating a zone object, you can add/remove a reference to a zone oper policy by name.

Method	URL Path
PUT	/agapi/v1/ddos/zone/{zone-id}/

Response Codes

See Common Response Codes.

Patch a Zone

When patching a zone object, it is permissible to set specific attributes related to the zone object, instead of entire payload.

Method	URL Path
PATCH	/agapi/v1/ddos/zone/{zone-id}/

Filter Fields:

Name	Required	Type	Description
ip_list	No	Array	If ip_list attribute has at least one IP address/subnet, it is seen as static IP list. Otherwise, it is seen as learnt from BGP peers. For example: ["10.10.10.10","10.10.10.11"]
description	No	String	Describe the zone.
zone_oper_policy	No	String	Zone operation policy that is applied to the zone.
glid	No	String	GLID object that is applied to the zone .
zone_level_topk_num_records	No	Number	Number of zone level top-k records. The value should be between 1 to 100.
zone_level_topk_dest_num_records	No	Number	Number of zone level top-k records of destination. The value should be between 1 to 100.
continuous_learning	No	Boolean	Continuous learning flag can either be true of false.
src_port	No	Nested Object (s)	Source port object
src_port_range_lis	No	Nested Object (s)	Source port object in range

Name	Required	Type	Description
operational_ mode	No	String	Can be one of following: “idle”, “monitor” or “learning”
profile_ name	No	String	Profile name

Sample Request:

```
{
    "ip_list": ["10.10.10.10"],
    "glid": "A10_1Gbps",
    "profile_name": "",
    "description": "This is a test zone",
    "src_port": {
        "zone_src_port_other_list": [
            {
                "deny": true,
                "protocol": "tcp",
                "port_other": "other",
                "zone_template": {
                    "src_tcp": "",
                    "src_udp": ""
                },
                "glid_cfg": {
                    "glid_action": null,
                    "glid": "A10_10Mbps"
                }
            }
        ],
        "zone_src_port_list": [
            {
                "deny": true,
                "protocol": "tcp",
                "port": 1023,
                "zone_template": {
                    "src_tcp": "",
                    "src_udp": ""
                },
                "glid_cfg": {
                    "glid_action": null,
                    "glid": "A10_10Mbps"
                }
            }
        ]
    }
}
```

Response Codes

See Common Response Codes.

Delete a Specific Zone

Allows you to delete a zone even if it is under mitigation.

Method	URL Path
DELETE	/agapi/v1/ddos/zone/{zone_id}

Query Parameters:

Name	Required	Type	Description
force_delete	No	Boolean	Deletes a zone regardless if set to True.

Sample Output (?force_delete=False):

```
{
"message": "Unable to delete zone because it is in mitigation status.",
"code": 400
}
```

Sample Output (?force_delete= True):

```
{
"message": "The zone: test1 is successfully deleted.",
"code": 200
}
```

Response Codes

See Common Response Codes.

Retrieve a Zone Chart

Use the following method and URL to retrieve a zone chart:

Method	URL
GET, OPTIONS	*/agapi/v1/ddos/zone/{zone-id}/charts*

Filter Fields:

You can use the following query parameters:

Field	Notes
device_ id	The device ID for retrieving a specific device. By default, all devices are displayed. You can enter multiple options separated by comma.
chart_ type	The types of charts associated with the zone. The chart types displayed are packets per second (pps), bytes per second (bps), and all (default). For the "all" option, you can enter the multiple options separated by comma.
start_ time	Start time in the format “%Y-%m-%dT%H:%M:%S"
end_ time	End time in the format “%Y-%m-%dT%H:%M:%S"
duration	Duration of the charts in milliseconds. The minimum value is 3600 for the last 1 hour and the maximum value is 86400 for the last 24 hours. **Note:** Duration is not applicable with start time and end time.

Retrieve a Zone Service Chart

Use the following method and URL to retrieve a zone service chart:

Method	URL
GET, OPTIONS	*/agapi/v1/ddos/zone/{zone-id}/service/{service}/charts/*

Filter Fields:

You can use the following query parameters:

Field	Notes
device_id	The device ID for retrieving information from a specific device. By default, the information is retrieved from all devices. You can enter multiple device IDs separated by comma.
chart_ type	The chart type for retrieving specific type of chart data associated with the zone. You can use:

Field	Notes
	Packets Per Second (pps) - Retrieve chart data for only pps chart type. Bytes Per Second (bps) - Retrieve chart data for only bps chart type. All - By default, chart data for both pps and bps chart types are retrieved. You can enter multiple chart types separated by comma.
start_ time	Start time in the format “%Y-%m-%dT%H:%M:%S"
end_time	End time in the format “%Y-%m-%dT%H:%M:%S"
duration	Duration of the charts in milliseconds. The minimum value is 3600 for the last 1 hour and the maximum value is 86400 for the last 24 hours. **Note:** Duration is not applicable with start time and end time.
include_ indicators	Indicator for retrieving indicator chart data. Set the value to true to retrieve indicator chart data. By default, the value is set to false.

Response Codes

See Common Response Codes.

Protected Destination

A protected destination is an object comprised of a group of destination IP addresses and/or subnets, and ports and protocols that provide a service and are protected as a single entity.

Operation	Method	URL Path	Payload
List Protected Destinations	GET	/agapi/v1/ddos/dst/	List of Protected Destinations
Create a Protected Destination	POST	/agapi/v1/ddos/dst/	Protected Destinations
Retrieve a specific Protected Destination	GET	/agapi/v1/ddos/dst/<dst-id>/	Protected Destinations

Operation	Method	URL Path	Payload
Update a specific Protected Destination	PUT	/agapi/v1/ddos/dst/<dst-id>/	Protected Destinations
Delete a specific Protected Destination	DELETE	/agapi/v1/ddos/dst/<dst-id>/	

DST Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
name: string(1...63), read-write, required, Name
mitigation_template: string(1...255), read-write, optional, Mitigation
template
ipv6_addr: string(1...256), read-write, optional, Ipv6 addr
ip_addr: string(1...36), read-write, optional, Ip addr
device_list: list, read-write, optional, Device list
device_group_id: string(1...36), read-write, optional, Device group id
operational_mode: string(1...255), read-write, optional, Operational mode
topk_dest_num_records: integer(1...100), read-write, optional, Topk dest
num records
uuid_mapping: string(1...255), read-only, optional, Uuid mapping
id: string(1...255), read-only, optional, Id
```

Protected Network Object

Network Object-based detection provides automated network discovery and attack detection.

Operation	Method	URL Path	Payload
List Network Objects	GET	/agapi/v1/ddos/network-object/	
Create Network Object	POST	/agapi/v1/ddos/network-object/	List of Protected Network Object
Retrieve Network Object	GET	/agapi/v1/ddos/network-object/*<network-obj-id>*/	Network Objects
Update Network Object	PUT	/agapi/v1/ddos/network-object/*<network-obj-id>*/	Network Objects

List Network Objects

Get a list of all network objects.

Method	URL
GET, OPTIONS	/agapi/v1/ddos/network-object/

Sample Request:

```
[
    {
        "relative_auto_break_down_threshold": {
            "network_percentage": 10,
            "permil": 1
        },
        "zone_config_profile": null,
        "disable_source_discovery": false,
        "device_group": null,
        "service_break_down_threshold_local": {
            "svc_percentage": 5
        },
        "victim_ip_mitigation_zone": "use_existing_zones",
        "id": "588b33fa-ea55-41b0-9b5e-2713a942eccd",
        "host_anomaly_threshold_packet_rate": 12,
        "ip_list": [
            "43.32.0.0/18"
        ],
        "network_object_anomaly_threshold_packet_rate": 43,
        "detector_group": "ff8503be-aac4-4da1-bbfc-847d53ccd3f7",
        "zone_oper_policy": null,
        "disable_service_discovery": true,
        "static_anomaly_detection_only": true,
        "host_anomaly_threshold_bit_rate": 9888,
        "histogram_mode": "off",
        "oper_status": "ok",
        "enable_topk_dest_sort_key": "average",
        "name": "cbtest_net_obj",
        "url": "https://10.64.1.224/agapi/v1/ddos/network-object/588b33fa-
ea55-41b0-9b5e-2713a942eccd/",
        "threshold_sensitivity": "off",
        "sub_network_conf": [
            {
                "subnet_anomaly_threshold_packet_rate": 43,
                "host_anomaly_threshold_packet_rate": 35,
                "breakdown_subnet_threshold_bit_rate": 19999,
                "host_anomaly_threshold_bit_rate": 1999,
                "subnetwork_breakdown": 26,
                "subnetwork_ip": "43.32.0.0/24",
                "subnet_anomaly_threshold_bit_rate": 999,
                "breakdown_subnet_threshold_packet_rate": 67
            },
            {
                "subnet_anomaly_threshold_packet_rate": 3,
                "host_anomaly_threshold_packet_rate": 4,
                "breakdown_subnet_threshold_bit_rate": "",
                "host_anomaly_threshold_bit_rate": "",
                "subnetwork_breakdown": 30,
                "subnetwork_ip": "43.32.1.0/24",
                "subnet_anomaly_threshold_bit_rate": "",
                "breakdown_subnet_threshold_packet_rate": 5
            },
            {
                "subnet_anomaly_threshold_packet_rate": 3,
                "host_anomaly_threshold_packet_rate": 3,
                "breakdown_subnet_threshold_bit_rate": "",
                "host_anomaly_threshold_bit_rate": "",
                "subnetwork_breakdown": 31,
                "subnetwork_ip": "43.32.2.1/30",
                "subnet_anomaly_threshold_bit_rate": "",
                "breakdown_subnet_threshold_packet_rate": 3
            }
        ],
        "network_object_anomaly_threshold_bit_rate": 988,
        "oper_mode": "learning"
    }

]
```

Response Codes

See Common Response Codes.

Create Network Object

When creating a network object, associate a zone configuration profile, mitigator group, detector group, and zone operational policy.

Method	URL
POST, OPTIONS	/agapi/v1/ddos/network-object/

Sample Request:

```
{
    "relative_auto_break_down_threshold": {
        "network_percentage": 10,
        "permil": 1
    },
    "zone_config_profile": null,
    "disable_source_discovery": false,
    "device_group": null,
    "service_break_down_threshold_local": {
        "svc_percentage": 5
    },
    "victim_ip_mitigation_zone": "use_existing_zones",
    "id": "588b33fa-ea55-41b0-9b5e-2713a942eccd",
    "host_anomaly_threshold_packet_rate": 12,
    "ip_list": [
        "43.32.0.0/18"
    ],
    "network_object_anomaly_threshold_packet_rate": 43,
    "detector_group": "ff8503be-aac4-4da1-bbfc-847d53ccd3f7",
    "zone_oper_policy": null,
    "disable_service_discovery": true,
    "static_anomaly_detection_only": true,
    "host_anomaly_threshold_bit_rate": 9888,
    "histogram_mode": "off",
    "enable_topk_dest_sort_key": "average",
    "name": "cbtest_net_obj",
    "threshold_sensitivity": "off",
    "sub_network_conf": [
        {
            "subnet_anomaly_threshold_packet_rate": 43,
            "host_anomaly_threshold_packet_rate": 35,
            "breakdown_subnet_threshold_bit_rate": 19999,
            "host_anomaly_threshold_bit_rate": 1999,
            "subnetwork_breakdown": 26,
            "subnetwork_ip": "43.32.0.0/24",
            "subnet_anomaly_threshold_bit_rate": 999,
            "breakdown_subnet_threshold_packet_rate": 67
        },
        {
            "subnet_anomaly_threshold_packet_rate": 3,
            "host_anomaly_threshold_packet_rate": 4,
            "breakdown_subnet_threshold_bit_rate": "",
            "host_anomaly_threshold_bit_rate": "",
            "subnetwork_breakdown": 30,
            "subnetwork_ip": "43.32.1.0/24",
            "subnet_anomaly_threshold_bit_rate": "",
            "breakdown_subnet_threshold_packet_rate": 5
        },
        {
            "subnet_anomaly_threshold_packet_rate": 3,
            "host_anomaly_threshold_packet_rate": 3,
            "breakdown_subnet_threshold_bit_rate": "",
            "host_anomaly_threshold_bit_rate": "",
            "subnetwork_breakdown": 31,
            "subnetwork_ip": "43.32.2.1/30",
            "subnet_anomaly_threshold_bit_rate": "",
            "breakdown_subnet_threshold_packet_rate": 3
        }
    ],
    "network_object_anomaly_threshold_bit_rate": 988,
    "oper_mode": "learning"
}
```

Sample Response:

```
{
    "message": "Network Object created successfully"
}
```

The following table provides the description for the attributes:

Name	Description
relative_auto_break_down_threshold	Per mille value for the network-object traffic rate.
zone_config_pro-	Name of the ZCP that the associated zones will use. Man-

Name	Description
file	datory field.
disable_source_discovery	Source discovery associated with the network object. By default, the value is set to false.
device_group	Group ID of the mitigator group associated with the network object. Mandatory field.
service_break_down_threshold_local	Threshold configured for service break down.
victim_ip_mitigation_zone	Zone-based detection for victim IP address.
id	ID of the network object to be configured.
host_anomaly_threshold_packet_rate	Packet rate for host anomaly threshold.
ip_list	List of subnets that will be protected by the network object. Max of 10 subnets per network object. Mandatory Field.
network_object_anomaly_threshold_packet_rate	Packet rate for network object anomaly threshold.
detector_group	Group ID of the detector group associated with the network object. Mandatory field.
zone_oper_policy	Zone Oper. Policy name associated with the network object. This Zone Oper. Policy must have the option for "**victim-ip**" enabled. Mandatory field.
disable_service_discovery	Service discovery rule associated with the network objects. By default, the value is set to false.
static_anomaly_detection_only	Static threshold for anomaly detection.
host_anomaly_threshold_bit_rate	Bit rate for host anomaly threshold.
histogram_mode	Histogram mode such as off, monitor, and observe. Observe

Name	Description
	is the default setting.
enable_topk_dest_sort_key	Top-k destination sorted by sort key.
name	Name of the network object to be configured. Mandatory field.
threshold_sensitivity	Threshold indicator for traffic sensitivity.
sub_network_conf	Configuration setting for sub-networks.
network_object_anomaly_threshold_bit_rate	Bit rate threshold for network object anomaly.
oper_mode	Zone operational mode. Learning mode is the default mode.

Response Codes

See Common Response Codes.

Retrieve Network Object

Retrieve a network object.

Method	URL
GET, OPTIONS	/agapi/v1/ddos/network-object/<*network-obj-id*>/

Response Codes

See Common Response Codes.

Update Network Object

Update a network object.

Method	URL
PUT, OPTIONS	/agapi/v1/ddos/network-object/<*network-obj-id*>/

Sample Request:

```
{
    "relative_auto_break_down_threshold": {
        "network_percentage": 10,
        "permil": 1
    },
    "zone_config_profile": null,
    "disable_source_discovery": false,
    "device_group": null,
    "service_break_down_threshold_local": {
        "svc_percentage": 5
    },
    "victim_ip_mitigation_zone": "use_existing_zones",
    "id": "588b33fa-ea55-41b0-9b5e-2713a942eccd",
    "host_anomaly_threshold_packet_rate": 12,
    "ip_list": [
        "43.32.0.0/18"
    ],
    "network_object_anomaly_threshold_packet_rate": 43,
    "detector_group": "ff8503be-aac4-4da1-bbfc-847d53ccd3f7",
    "zone_oper_policy": null,
    "disable_service_discovery": true,
    "static_anomaly_detection_only": true,
    "host_anomaly_threshold_bit_rate": 9888,
    "histogram_mode": "off",
    "enable_topk_dest_sort_key": "average",
    "name": "cbtest_net_obj",
    "threshold_sensitivity": "off",
    "sub_network_conf": [
        {
            "subnet_anomaly_threshold_packet_rate": 43,
            "host_anomaly_threshold_packet_rate": 35,
            "breakdown_subnet_threshold_bit_rate": 19999,
            "host_anomaly_threshold_bit_rate": 1999,
            "subnetwork_breakdown": 26,
            "subnetwork_ip": "43.32.0.0/24",
            "subnet_anomaly_threshold_bit_rate": 999,
            "breakdown_subnet_threshold_packet_rate": 67
        },
        {
            "subnet_anomaly_threshold_packet_rate": 3,
            "host_anomaly_threshold_packet_rate": 4,
            "breakdown_subnet_threshold_bit_rate": "",
            "host_anomaly_threshold_bit_rate": "",
            "subnetwork_breakdown": 30,
            "subnetwork_ip": "43.32.1.0/24",
            "subnet_anomaly_threshold_bit_rate": "",
            "breakdown_subnet_threshold_packet_rate": 5
        },
        {
            "subnet_anomaly_threshold_packet_rate": 3,
            "host_anomaly_threshold_packet_rate": 3,
            "breakdown_subnet_threshold_bit_rate": "",
            "host_anomaly_threshold_bit_rate": "",
            "subnetwork_breakdown": 31,
            "subnetwork_ip": "43.32.2.1/30",
            "subnet_anomaly_threshold_bit_rate": "",
            "breakdown_subnet_threshold_packet_rate": 3
        }
    ],
    "network_object_anomaly_threshold_bit_rate": 988,
    "oper_mode": "learning"
}
```

Sample Request:

```
{
    "message": "Network object updated successfully"
}
```

Response Codes

See Common Response Codes.

Delete Network Object

Delete a network object.

Method	URL
DELETE, OPTIONS	/agapi/v1/ddos/network-object/<network-obj-id>/

Response Codes

See Common Response Codes.

Zone Policies and Profiles

The following topics are covered:

Zone Configuration Profile

Zone Configuration Profile is a configuration profile that contains the common DDoS protection configurations at the zone and zone service levels.

Operation	Method	URL	Payload
List all zone configuration profiles	GET	/agapi/v1/ddos/zone-cfg-profile/	List of Zone Configuration Profile
Create a zone configuration profile	POST	/agapi/v1/ddos/zone-cfg-profile/	Zone Configuration Profile
Retrieve a specific zone configuration profile	GET	/agapi/v1/ddos/zone-cfg-profile/{zone-cfg-profile-id}/	Zone Configuration Profile
Update a specific zone configuration profile	PUT	/agapi/v1/ddos/zone-cfg-profile/{zone-cfg-profile-id}/	Zone Configuration Profile
Delete a specific zone configuration profile	DELETE	/agapi/v1/ddos/zone-cfg-profile/{zone-cfg-profile-id}/	

Zone Configuration Profile Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
name: string(1...63), read-write, required, Name
continuous_learning: boolean, read-write, optional, Continuous learning
src_port_list: nested object(s), read-write, optional, Src port list
glid: string(1...63), read-write, optional, Glid
created: datetime, read-only, optional, Created
service_list: nested object(s), read-write, optional, Service list
description: string(1...63), read-write, optional, Description
inbound_forward_dscp: integer(1...63), read-write, optional, Inbound
forward dscp
domain_id: string(1...), read-only, optional, Domain id
detection: nested object(s), read-write, optional, Detection
url: nested object(s), read-only, optional, Url
hw_blacklist_blocking: nested object(s), read-write, optional, Hw
blacklist blocking
outbound_forward_dscp: integer(1...63), read-write, optional, Outbound
forward dscp
modified: datetime, read-only, optional, Modified
id: string(1...), read-only, optional, Id
creating_user_id: string(1...), read-only, optional, Creating user id
config: string(1...), read-write, optional, Config
zone_level_topk_dest_num_records: integer(1...100), read-write, optional,
Zone level topk dest num records
zone_level_topk_num_records: integer(1...100), read-write, optional, Zone
level topk num records
```

Zone Service Protection Profile

Zone Service Protection Profile is a configuration profile that contains the common DDoS protection configurations at the zone service levels.

Operation	Method	URL Path	Payload
List all Zone Service Protection profiles	GET	/agapi/v1/ddos/service-port-prot-profile/	List of Zone Service Protection Profile

Operation	Method	URL Path	Payload
Create a Zone Service Protection profile	POST	/agapi/v1/ddos/service-port-prot-profile/	Zone Service Protection Profile
Retrieve a specific Zone Service Protection profile	GET	/agapi/v1/ddos/service-port-prot-profile/{service-port-prot-profile-id}/	Zone Service Protection Profile
Update a specific Zone Service Protection profile	PUT	/agapi/v1/ddos/service-port-prot-profile/{service-port-prot-profile-id}/	Zone Service Protection Profile
Delete Zone Service Protection profile	DELETE	/agapi/v1/ddos/service-port-prot-profile/{service-port-prot-profile-id}/	
List IP addresses for all Zone Service Protection profiles	GET	/agapi/v1/ddos/service-ip-proto-prot-profile/	List of Service IP Protection Profile
Create an IP address for Zone Service Protection profile	POST	/agapi/v1/ddos/service-ip-proto-prot-profile/	Service IP Protection Profile
Retrieve a Zone Service Protection profile for a specific IP address	GET	/agapi/v1/ddos/service-ip-proto-prot-profile/{profile-id}/	Service IP Protection Profile
Update a Zone Service Protection profile for a specific IP address	PUT	/agapi/v1/ddos/service-ip-proto-prot-profile/{profile-id}/	Service IP Protection Profile
Delete Zone Service Protection profile for a specific IP address	DELETE	/agapi/v1/ddos/service-ip-proto-prot-profile/{profile-id}/	

Zone Service Protection Profile Object Attributes

Attribute Name: Type, Optional/Required, Description

```
protocol: choice, read-write, required, Protocol
name: string(1...63), read-write, required, Name
```

```
predefined: boolean, read-write, optional, Predefined
deny: boolean, read-write, optional, Deny
description: string(1...63), read-write, optional, Description
created: datetime, read-only, optional, Created
url: nested object(s), read-only, optional, Url
enable_class_list_overflow: boolean, read-write, optional, Enable class
list overflow
level_list: nested object(s), read-write, optional, Level list
modified: datetime, read-only, optional, Modified
pattern_recognition: nested object(s), read-write, optional, Pattern
recognition
id: string(1...), read-only, optional, Id
stateful: boolean, read-write, optional, Stateful
src_based_policy_list: nested object(s), read-write, optional, Src based
policy list
glid_cfg: nested object(s), read-write, optional, Glid cfg
creating_user_id: string(1...255), read-write, optional, Creating user id
config: string(1...), read-write, optional, Config
domain_id: string(1...255), read-write, optional, Domain id
max_dynamic_entry_count: integer(0...16000000), read-write, optional, Max
dynamic entry count
```

Service IP Protection Profile Object Attributes

Attribute Name: Type, Optional/Required, Description

```
protocol: string(1...), read-write, required, Protocol
name: string(1...63), read-write, required, Name
predefined: boolean, read-write, optional, Predefined
deny: boolean, read-write, optional, Deny
drop_frag_pkt: boolean, read-write, optional, Drop frag pkt
tunnel_decap: boolean, read-write, optional, Tunnel decap
age: integer(2...1023), read-write, optional, Age
level_list: nested object(s), read-write, optional, Level list
modified: datetime, read-only, optional, Modified
created: datetime, read-only, optional, Created
url: nested object(s), read-only, optional, Url
esp_inspect: nested object(s), read-write, optional, Esp inspect
src_based_policy_list: nested object(s), read-write, optional, Src based
policy list
glid_cfg: nested object(s), read-write, optional, Glid cfg
```

```
id: string(1...), read-only, optional, Id
max_dynamic_entry_count: integer(0...16000000), read-write, optional, Max
dynamic entry count
creating_user_id: string(1...255), read-write, optional, Creating user id
config: string(1...), read-write, optional, Config
domain_id: string(1...255), read-write, optional, Domain id
tunnel_rate_limit: boolean, read-write, optional, Tunnel rate limit
description: string(1...63), read-write, optional, Description
```

Zone Operational Policy

Zone Oper Policy lets you specify operational behavior settings in a policy that can be associated to multiple zones. When the policy is updated, the updated settings will propagate to the associated zones.

Operation	Method	URL Path	Payload
List all Zone Oper policies	GET	/agapi/v1/ddos/zone-oper-policy/	List of Zone Operational Policy
Create a Zone Oper policy	POST	/agapi/v1/ddos/zone-oper-policy/	Zone Operational Policy
Retrieve a specific Zone Oper policy	GET	/agapi/v1/ddos/zone-oper-policy/{zone-oper-policy-id}/	Zone Operational Policy
Update a specific Zone Oper policy	PUT	/agapi/v1/ddos/zone-oper-policy/{zone-oper-policy-id}/	Zone Operational Policy
Delete a specific Zone Oper policy	DELETE	/agapi/v1/ddos/zone-oper-policy/{zone-oper-policy-id}	

Zone Operational Policy Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
log_enable, (boolean), required, Log enable
auto_stop_mitigation, (choice), required, Auto stop mitigation
name, string(1....63), required, Name
bgp, (boolean), required, Bgp
log_periodic, (boolean), required, Log periodic
auto_start_mitigation, (choice), required, Auto start mitigation
```

```
class_list_policy, (choice), optional, Class list policy
stop_mitigation_remove_zone, (choice), optional, Stop mitigation remove
zone
auto_enable_flowspec_rules, (boolean), optional, Auto enable flowspec
rules
id, string(1....1), optional, Id
predefined, (boolean), optional, Predefined
bgp_flowspec_top_dest_ip_count, integer(1....20), optional, Bgp flowspec
top dest ip count
zone_template, (nested object(s)), optional, Zone template
domain_id, string(1....255), optional, Domain id
exclude_push_cl_list, (list), optional, Exclude push cl list
creating_user_id, string(1....255), optional, Creating user id
config, string(1....1), optional, Config
bgp_top_dest_ip_count, integer(1....20), optional, Bgp top dest ip count
bgp_flowspec_ip_source, (choice), optional, Bgp flowspec ip source
bgp_prefix_source, (choice), optional, Bgp prefix source
created, (datetime), optional, Created
url, (nested object(s)), optional, Url
modified, (datetime), optional, Modified
bgp_flowspec, (boolean), optional, Bgp flowspec
```

Automatic Entity Discovery

SecDevice supports automatic discovery of entities when using Detection 2.0 detectors. Once the detector is configured by SecDevice, it will send notifications to SecDevice whenever entities are discovered.

Operation	Method	URL Path	Payload
List all discovered entities	GET, OPTIONS	/agapi/v1/discovered-entity/	List of Discovered Entity
Retrieve a specific discovered entity	GET	/agapi/v1/discovered/entity/{discovered-entity-id}/	Discovered Entity
Delete discovered entities	DELETE	/agapi/v1/discovered/entity/{discovered-entity-id}/	

Discovered Entity Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
ip_address: string(1...), read-write, required, Ip address
zone_name: nested object(s), read-write, required, Zone name
status: string(1...), read-write, optional, Status
created: datetime, read-only, optional, Created
service_list: nested object(s), read-write, optional, Service list
object_type: string(1...), read-write, optional, Object type
modified: datetime, read-only, optional, Modified
partition_num: integer(0...10000), read-write, optional, Partition num
id: string(1...), read-only, optional, Id
url: nested object(s), read-only, optional, Url
detector_id: string(1...), read-write, optional, Detector id
creating_user_id: string(1...), read-only, optional, Creating user id
data: string(1...), read-write, optional, Data
domain_id: string(1...), read-only, optional, Domain id
partition_name: string(1...63), read-write, optional, Partition name
```

Sample Request:

```
HTTP GET /agapi/v1/discovered-entity/
```

Sample Response:

```
HTTP 200 OK
[
    {
        "status": "New",
        "created": "2018-10-21T04:20:40Z",
        "service_list": [
            {
                "protocol": "tcp",
                "port": 80
            },
            {
                "protocol": "icmp-v4",
                "port": null
            }
        ],
        "ip_address": "100.1.1.10",
        "object_type": "DST_IP",
        "modified": "2018-10-21T04:20:40Z",
        "partition_num": 0,
        "id": "9a9a0996-6fd5-4db6-a992-6503fcec3a88",
        "url": "https://192.168.212.125/agapi/v1/discovered-
entity/9a9a0996-6fd5-4db6-a992-6503fcec3a88/",
        "detector_id": "7cebfc52-b8da-4830-a918-237a75d2a176",
        "zone_name": null,
        "creating_user_id": null,
        "data": "{\"protocol\": \"icmp-v4\", \"ha-state\": \"Active\",
\"l4-port\": 0, \"entity-key\": \"service\", \"ipv4-addr\":
\"100.1.1.10\", \"entity-metric-list\": [{\"current\": \"3\",
\"threshold\": \"6\", \"metric-name\": \"In-pkt-rate\", \"anomaly\":
\"No\"}, {\"current\": \"3\", \"threshold\": \"6\", \"metric-name\":
\"Out-pkt-rate\", \"anomaly\": \"No\"}, {\"current\": \"252\",
\"threshold\": \"538\", \"metric-name\": \"In-byte-rate\", \"anomaly\":
\"No\"}, {\"current\": \"252\", \"threshold\": \"504\", \"metric-name\":
\"Out-byte-rate\", \"anomaly\": \"No\"}, {\"current\": \"3\",
\"threshold\": \"6\", \"metric-name\": \"In-small-pkt-rate\", \"anomaly\":
\"No\"}, {\"current\": \"3\", \"threshold\": \"6\", \"metric-name\":
\"Out-small-pkt-rate\", \"anomaly\": \"No\"}, {\"current\": \"0\",
\"threshold\": \"1\", \"metric-name\": \"conn-rate\", \"anomaly\":
\"No\"}, {\"current\": \"1.000000\", \"threshold\": \"2.000000\",
\"metric-name\": \"concurrent-conn-rate\", \"anomaly\": \"No\"},
{\"current\": \"1.000000\", \"threshold\": \"2.133333\", \"metric-name\":
\"In-Byte-per-Out-byte-rate\", \"anomaly\": \"No\"}], \"mode\":
\"Monitoring\", \"l4-proto\": \"Icmp\", \"ip_address\": \"100.1.1.10\",
\"port\": null}",
        "domain_id": null,
        "partition_name": "shared"
    },
    {
        "status": "Assigned",
        "created": "2018-11-06T21:12:01Z",
        "service_list": [
            {
                "protocol": "icmp-v4",
                "port": null
            }
        ],
        "ip_address": "178.16.30.1",
        "object_type": "DST_IP",
        "modified": "2018-11-06T21:12:02Z",
        "partition_num": 0,
        "id": "f0918c68-f4c4-4a27-8335-04ff119bc86c",
        "url": "https://192.168.212.125/agapi/v1/discovered-
entity/f0918c68-f4c4-4a27-8335-04ff119bc86c/",
        "detector_id": "e325f201-37a9-4ffd-9037-998719e27350",
        "zone_name": "auto_zone_178_16_30_1",
        "creating_user_id": null,
        "data": null,
        "domain_id": null,
        "partition_name": "shared"
    }
]
```

Response Codes

See Common Response Codes.

Retrieve Discovered Entity

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
ip_address: string(1...), read-write, required, Ip address
zone_name: nested object(s), read-write, required, Zone name
status: string(1...), read-write, optional, Status
created: datetime, read-only, optional, Created
service_list: nested object(s), read-write, optional, Service list
object_type: string(1...), read-write, optional, Object type
modified: datetime, read-only, optional, Modified
partition_num: integer(0...10000), read-write, optional, Partition num
id: string(1...), read-only, optional, Id
url: nested object(s), read-only, optional, Url
detector_id: string(1...), read-write, optional, Detector id
creating_user_id: string(1...), read-only, optional, Creating user id
data: string(1...), read-write, optional, Data
domain_id: string(1...), read-only, optional, Domain id
partition_name: string(1...63), read-write, optional, Partition name
```

Sample Request:

```
HTTP GET /agapi/v1/discovered/entity/{discovered-entity-id}/
```

Sample Response:

```
HTTP 200 OK
{
    "status": "Assigned",
    "created": "2018-11-06T21:12:01Z",
    "service_list": [
        {
            "protocol": "icmp-v4",
            "port": null
        }
    ],
    "ip_address": "178.16.30.1",
    "object_type": "DST_IP",
    "modified": "2018-11-06T21:12:02Z",
    "partition_num": 0,
    "id": "f0918c68-f4c4-4a27-8335-04ff119bc86c",
    "url": "https://192.168.212.125/agapi/v1/discovered-entity/f0918c68-
f4c4-4a27-8335-04ff119bc86c/",
    "detector_id": "e325f201-37a9-4ffd-9037-998719e27350",
    "zone_name": "auto_zone_178_16_30_1",
    "creating_user_id": null,
    "data": null,
    "domain_id": null,
    "partition_name": "shared"
}
```

Response Codes

See Common Response Codes.

Delete Discovered Entity

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
ip_address: string(1...), read-write, required, Ip address
zone_name: nested object(s), read-write, required, Zone name
```

```
status: string(1...), read-write, optional, Status
created: datetime, read-only, optional, Created
service_list: nested object(s), read-write, optional, Service list
object_type: string(1...), read-write, optional, Object type
modified: datetime, read-only, optional, Modified
partition_num: integer(0...10000), read-write, optional, Partition num
id: string(1...), read-only, optional, Id
url: nested object(s), read-only, optional, Url
detector_id: string(1...), read-write, optional, Detector id
creating_user_id: string(1...), read-only, optional, Creating user id
data: string(1...), read-write, optional, Data
domain_id: string(1...), read-only, optional, Domain id
partition_name: string(1...63), read-write, optional, Partition name
```

Sample Request:

```
HTTP DELETE /agapi/v1/discovered/entity/{discovered-entity-id}/
```

Sample Response:

```
HTTP 204 No Content
```

Response Codes

See Common Response Codes.

Zone Service Creation Policy

A Zone Service Creation Policy can be created to control the parameters used when automatically updating a Zone with newly discovered service entities.

Operation	Method	URL Path	Payload
Retrieve a Zone Service Creation policy	GET, OPTIONS	*/agapi/v1/discovered-service/zone-service-creation-policy/*	Zone Service Creation Policy
List a Zone Service Creation policy	GET	*/agapi/v1/discovered-service/zone-service-creation-policy/{zone-service-creation-policy-id}/*	List of Zone Service Creation

Operation	Method	URL Path	Payload
			Policy
Create a Zone Service Creation policy	POST	*/agapi/v1/discovered-service/zone-service-creation-policy/*	Zone Service Creation Policy
Delete a Zone Service Creation policy	DELETE	*/agapi/v1/discovered-service/zone-service-creation-policy/{zone-service-creation-policy-id}/*	

NOTE: The Detector must be configured to perform automatic zone creation.

Zone Service Creation Policy Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
agalaxy_protocol: string(1...63), read-write, required, Agalaxy protocol
discovered_protocol: string(1...63), read-write, required, Discovered
protocol
discovered_port: string(1...63), read-write, optional, Discovered port
created: datetime, read-only, optional, Created
url: nested object(s), read-only, optional, Url
modified: datetime, read-only, optional, Modified
id: string(1...), read-only, optional, Id
service_port_prot_profile_id: string(1...), read-write, optional, Service
port prot profile id
agalaxy_port: string(1...63), read-write, optional, Agalaxy port
creating_user_id: string(1...), read-only, optional, Creating user id
domain_id: string(1...), read-only, optional, Domain id
```

List Zone Service Creation Policies

Retrieve a Zone Service Creation policy.

Method	URL Path
GET, OPTIONS	/agapi/v1/discovered-service/zone-service-creation-policy/

Sample Request:

```
HTTP GET /agapi/v1/discovered-service/zone-service-creation-policy/
```

Sample Response:

```
[
    {
        "discovered_port": 80,
        "created": "2018-10-09T22:44:52Z",
        "url": "https://192.168.212.125/agapi/v1/discovered-service/zone-
service-creation-policy/48d7ec0f-2421-489e-97cb-7a85d8ea2c02/",
        "modified": "2018-10-09T22:44:52Z",
        "id": "48d7ec0f-2421-489e-97cb-7a85d8ea2c02",
        "agalaxy_protocol": "http",
        "service_port_prot_profile_id": null,
        "agalaxy_port": 80,
        "creating_user_id": null,
        "domain_id": null,
        "discovered_protocol": "tcp"
    },
    {
        "discovered_port": 443,
        "created": "2018-10-09T22:45:03Z",
        "url": "https://192.168.212.125/agapi/v1/discovered-service/zone-
service-creation-policy/1d48a175-b8d8-471c-8a3e-c4f6e9c9cabd/",
        "modified": "2018-10-09T22:45:03Z",
        "id": "1d48a175-b8d8-471c-8a3e-c4f6e9c9cabd",
        "agalaxy_protocol": "ssl-l4",
        "service_port_prot_profile_id": null,
        "agalaxy_port": 443,
        "creating_user_id": null,
        "domain_id": null,
        "discovered_protocol": "tcp"
    }
]
```

Response Codes

See Common Response Codes.

Retrieve Zone Service Creation Policies

List a Zone Service Creation policy.

Method	URL Path
GET	*/agapi/v1/discovered-service/zone-service-creation-policy/{zone-service-creation-policy-id}/*

Sample Request:

```
HTTP GET /agapi/v1/discovered-service/zone-service-creation-policy/{zone-
service-creation-policy-id}/
```

Sample Response:

```
HTTP 200 OK
{
    "discovered_port": 80,
    "created": "2018-10-09T22:44:52Z",
    "url": "https://192.168.212.125/agapi/v1/discovered-service/zone-
service-creation-policy/48d7ec0f-2421-489e-97cb-7a85d8ea2c02/",
    "modified": "2018-10-09T22:44:52Z",
    "id": "48d7ec0f-2421-489e-97cb-7a85d8ea2c02",
    "agalaxy_protocol": "http",
    "service_port_prot_profile_id": null,
    "agalaxy_port": 80,
    "creating_user_id": null,
    "domain_id": null,
    "discovered_protocol": "tcp"
}
```

Response Codes

See Common Response Codes.

Create Zone Service Creation Policies

Create a Zone Service Creation policy.

Method	URL Path
POST	/agapi/v1/discovered-service/zone-service-creation-policy/

Sample Request:

```
HTTP POST /agapi/v1/discovered-service/zone-service-creation-policy/
{
    "discovered_port": 53,
    "discovered_protocol": "udp",
    "agalaxy_port": 53,
    "agalaxy_protocol": "dns-udp",
    "service_port_prot_profile_id": null
```

Sample Response:

```
HTTP 201 Created
{
    "discovered_port": 53,
    "created": "2018-11-06T21:42:55.485161Z",
    "url": "https://192.168.212.125/agapi/v1/discovered-service/zone-
service-creation-policy/75723a47-2945-4640-b134-91fa8e052a38/",
    "modified": "2018-11-06T21:42:55.485203Z",
    "id": "75723a47-2945-4640-b134-91fa8e052a38",
    "agalaxy_protocol": "dns-udp",
    "service_port_prot_profile_id": null,
    "agalaxy_port": 53,
    "creating_user_id": null,
    "domain_id": null,
    "discovered_protocol": "udp"
}
```

Response Codes

See Common Response Codes.

Delete Zone Service Creation Policies

Delete a Zone Service Creation policy.

Method	URL Path
DELETE	/agapi/v1/discovered-service/zone-service-creation-policy/{zone-service-creation-policy-id}/

Sample Request:

```
HTTP DELETE /agapi/v1/discovered-service/zone-service-creation-policy/
{zone-service-creation-policy-id}/
```

NOTE: Sample Response:

```
HTTP 204 No Content
```

Response Codes

See Common Response Codes.

Zone Actions

These endpoints are used to transition the zone into different operational modes.

Operation	Method	URL Path
To query for a single device (in the mitigation device group), include the device ID in the URL	GET, OPTIONS	/agapi/v1/ddos/zone/{zone-id}/learning/{device-id}
Start learning on the zone. Optionally, include a payload for scheduling the learning duration	POST	/agapi/v1/ddos/zone/<zone-id>/learning/{device-id}/

Retrieve TPS Zone Indicator Values

Retrieve the live indicator values from the TPS device(s). The values will be retrieved from:

The standalone detector if one is configured for the zone

The devices in the mitigator device group (if no standalone detector is configured)

The response will be keyed by the device ID(s) and contain a list of services and their learned indicator values.

To query for a single device (in the mitigation device group), include the device ID in the URL.

Method	URL
GET, OPTIONS	/agapi/v1/ddos/zone/{zone-id}/learning/{device-id}

Sample Request:

<need example>

Example Response:

```
{
"<device-id>": [
{
"protocol": "<protocol>"|<int>, "port": [int], "port_range_start": [int],
"port_range_end": [int], "indicators": [
{
"max": 30.0,
"rate": 10.0,
"avg": 11.0,
"name": "pkt-rate", "min": 10.0
},
{
"max": 20.0,
"rate": 10.0,
"avg": 1.0,
"name": "syn-rate", "min": 10.0
},
{
"max": 20.0,
"rate": 0.0,
"avg": 1.0,
"name": "fin-rate", "min": 10.0
},
{
"max": 0.0,
"rate": 0.0,
"avg": 0.0,
"name": "rst-rate", "min": 0.0
},
{
"max": 0.0,
"rate": 0.0,
"avg": 0.0,
"name": "small-window-ack-rate", "min": 0.0
},
{
"max": 30.0,
"rate": 0.0,

"avg": 5.0,
"name": "empty-ack-rate", "min": 10.0
},
{
"max": 20.0,
"rate": 0.0,
"avg": 1.0,
"name": "small-payload-rate", "min": 10.0
},
{
"max": 0.0,
"rate": 0.0,
"avg": 0.0,
"name": "bytes-to-bytes-from-ratio", "min": 0.0
},
{
"max": 1.0,
"rate": 0.0,
"avg": 0.015306,
"name": "syn-fin-ratio", "min": 0.0
},
{
"max": 0.0,
"rate": 0.0,
"avg": 0.0,
"name": "conn-miss-rate", "min": 0.0
```

```
},
{
"max": 0.0,
"rate": 0.0,
"avg": 0.0,
"name": "pkt-drop-rate", "min": 0.0
},
{
"max": 0.0,
"rate": 0.0,
"avg": 0.0,
"name": "pkt-drop-ratio", "min": 0.0
},
{
"max": 0.0,
"rate": 0.0,
"avg": 0.0,

"name": "concurrent-conns", "min": 0.0
}
]
}
]
}
```

Field Notes:

Field	Notes
protocol	The service protocol This can be a name: tcp udp http dns-tcp

Field	Notes
	dns-udp ssl-l4 icmp-v4 icmp-v6 gre ipv4-encap ipv6-encap Or, it may be an integer protocol number.
port	Integer port number This field will only be present for port-based services.
port_range_start	Integer port number, the start of the port range This field will only be present for port-range services.
port_range_end	Integer port number, the end of the port range This field will only be present for port-range services.

See Common Response Codes.

Learn Zone

Start learning on the zone. Optionally, include a payload for scheduling the learning duration.

Method	URL
POST	/agapi/v1/ddos/zone/<zone-id>/learning/{device-id}/

NOTE: If the zone transitions from learning to idle or monitor mode, any scheduled learning jobs will be removed. W hile it is possible to schedule multiple learning jobs for the same zone, the first job to trigger will cancel the others.

Example Request:

```
{
"duration ": <int>,
"sensitivity ": "<high|low|default>"
}
```

Field Notes:

Field	Notes
duration	The learning duration in minutes At the end of the learning duration, SecDevice will start monitoring on the zone.
sensitivity	Algorithm for determining the values to apply max : Use the maximum value learned (across all devices where applicable). avg : Use the average of all maximum values learned(across all devices where applicable).

Response Codes

See Common Response Codes.

Zone Creation Policy

A Zone Creation Policy can be created to control the parameters used when automatically creating a Zone from a Discovered Entity.

Operation	**Method**	**URL Path**	**Payload**
List all Zone creation policies	GET, OPTIONS	/agapi/v1/discovered-service/zone-creation-policy/	List of Discovered Service Zone Creation Policy
Retrieve a reference to a zone creation	GET	/agapi/v1/discovered-service/zone-creation-	Discovered Service Zone

Operation	Method	URL Path	Payload
policy by name		policy/	Creation Policy
Create a Zone creation policy	POST	/agapi/v1/discovered-service/zone-creation-policy/{zone-creation-policy-id}/	Discovered Service Zone Creation Policy
Delete a Zone creation policy	DELETE	/agapi/v1/ddos/zone/{zone-id}/	

NOTE: The Detector must be configured to perform automatic zone creation.

Discovered Service Zone Creation Policy Object Attributes

Attribute Name: Type, Read-Write/Read-Only, Optional/Required, Description

```
ip_subnet: string(1...63), read-write, required, Ip subnet
created: datetime, read-only, optional, Created
zone_oper_policy_id: nested object(s), read-write, optional, Zone oper
policy id
zone_name_prefix: string(1...20), read-write, optional, Zone name prefix
modified: datetime, read-only, optional, Modified
device_group: string(1...), read-write, optional, Device group
id: string(1...), read-only, optional, Id
url: nested object(s), read-only, optional, Url
zone_profile_id: nested object(s), read-write, optional, Zone profile id
creating_user_id: string(1...), read-only, optional, Creating user id
domain_id: string(1...), read-only, optional, Domain id
```

List Zone Creation Policy

List all Zone creation policies.

Method	URL Path
GET, OPTIONS	/agapi/v1/discovered-service/zone-creation-policy/

Sample Request:

```
HTTP GET /agapi/v1/discovered-service/zone-creation-policy/
```

Sample Response:

```
HTTP 200 OK
[
    {
        "created": "2018-10-09T22:44:41Z",
        "ip_subnet": "178.16.30.0/24",
        "zone_oper_policy_id": "df304eee-0ac7-4d1c-ae75-64f2c218b22b",
        "modified": "2018-10-09T22:51:19Z",
        "device_group": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
        "id": "080be171-a60c-445c-bde9-9fe1d0cfbd0c",
        "url": "https://192.168.212.125/agapi/v1/discovered-service/zone-creation-policy/080be171-a60c-445c-bde9-9fe1d0cfbd0c/",
        "zone_profile_id": null,
        "creating_user_id": null,
        "domain_id": null
    }
]
```

Response Codes

See Common Response Codes.

Retrieve Zone Creation Policy

Retrieve a reference to a zone creation policy by name.

Method	URL Path
GET	/agapi/v1/discovered-service/zone-creation-policy/

Sample Request:

```
HTTP GET /agapi/v1/discovered-service/zone-creation-policy/{zone-creation-policy-id}
```

Sample Response:

```
HTTP 200 OK
{
    "created": "2018-10-09T22:44:41Z",
    "ip_subnet": "178.16.30.0/24",
    "zone_oper_policy_id": "df304eee-0ac7-4d1c-ae75-64f2c218b22b",
    "modified": "2018-10-09T22:51:19Z",
    "device_group": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
    "id": "080be171-a60c-445c-bde9-9fe1d0cfbd0c",
    "url": "https://192.168.212.125/agapi/v1/discovered-service/zone-
creation-policy/080be171-a60c-445c-bde9-9fe1d0cfbd0c/",
    "zone_profile_id": null,
    "creating_user_id": null,
    "domain_id": null
}
```

Response Codes

See Common Response Codes.

Create Zone Creation Policy

Create a Zone creation policy.

Method	URL
POST	/agapi/v1/discovered-service/zone-creation-policy/{zone-creation-policy-id}/

Sample Request:

```
HTTP POST /agapi/v1/discovered-service/zone-creation-policy/
{
    "ip_subnet": "178.16.40.0/24",
    "zone_oper_policy_id": "df304eee-0ac7-4d1c-ae75-64f2c218b22b",
    "device_group": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
    "zone_profile_id": null
}
```

Sample Response:

```
HTTP 201 Created
{
    "created": "2018-11-06T21:26:30.944230Z",
    "ip_subnet": "178.16.40.0/24",
    "zone_oper_policy_id": "df304eee-0ac7-4d1c-ae75-64f2c218b22b",
    "modified": "2018-11-06T21:26:30.944288Z",
    "device_group": "7d08a417-b5e5-49f2-a94a-e37d896ae8de",
    "id": "11d05526-f521-4592-ab88-fcf6789967fc",
    "url": "https://192.168.212.125/agapi/v1/discovered-service/zone-
creation-policy/11d05526-f521-4592-ab88-fcf6789967fc/",
    "zone_profile_id": null,
    "creating_user_id": null,
    "domain_id": null
}
```

Response Codes

See Common Response Codes.

Delete Zone Creation Policy

Delete a Zone creation policy.

Method	URL
DELETE	/agapi/v1/ddos/zone/{zone-id}/

Sample Request:

```
HTTP DELETE /agapi/v1/discovered-service/zone-creation-policy/{zone-
creation-policy-id}/
```

Sample Response:

```
HTTP 204 No Content
```

Response Codes

See Common Response Codes.

Zone Monitoring

Operation	Method	URL Path	Payload
Retrieve Misc Indicator values	GET	/agapi/v1/ddos/zone/{zone-id}/monitor/	
Start monitoring Misc Indicator values	POST	/agapi/v1/ddos/zone/{zone-id}/monitor/	
Idle zone	POST, OPTIONS	/agapi/v1/ddos/zone/{zone-id}/idle/	
Start zone mitigation	POST	/agapi/v1/ddos/zone/{zone-id}/mitigation/start/	
Stop zone mitigation	POST	/agapi/v1/ddos/zone/{zone-id}/mitigation/stop/	
Asynchronous zone mitigation start	POST	/agapi/v1/ddos/zone/{zone-id}/mitigation/start/schedule	
Asynchronous zone mitigation stop	POST	/agapi/v1/ddos/zone/{zone-id}/mitigation/stop/schedule	

Retrieve Misc Indicator Values

Retrieve the indicator values based on sensitivity and algorithm parameters.If no parameters are provided, the default values indicated in the table below will be used.

Example:HTTP GET /agapi/v1/ddos/zone/<zone-id>/monitor/?algorithm=max&sensitivity=high

Method	URL
GET, OPTIONS	/agapi/v1/ddos/zone/{zone-id}/monitor/

Query Parameters:

Field	Notes
algorithm	Possible values: max, avg Default value: max

Field	Notes
	Algorithm for determining the values to apply max : Use the maximum value learned (across all devices where applicable). avg : Use the average of all maximum values learned (across all devices where applicable).

Field	Notes
sensitivity	Possible values: high,low, default Default value: default The sensitivity level corresponds to a multiplier value: high = 1.5 • low = 5.0 default = 3.0

Response Codes

See Common Response Codes.

Start Monitoring Misc Indicator Values

SecDevice sets the operational mode of the zone to “monitor” and configures threshold values for the zone based on the learned indicator values. The indicator values are retrieved from the off-box detector or devices in the mitigation device group(see “Zone Learning” section for more details).

Configures levels 0 to 3 on all services that have non-zero indicator learnt values:

- Each service will have a zone escalation score of 10.
- Each indicator type will have a score of 20. This ensures that only one indicator type needs to be exceeded to trigger level escalation.
- Each level (0 to 3) will have the same values configured.

NOTE: T he zone may be edited afterward to refine these values.

NOTE: If no payload is provided, SecDevice will only set the operational-mode and not change the zone configuration. This can be used if the user has manually configured the threshold values and only wants to change the operational mode.

Method	URL
POST	*/agapi/v1/ddos/zone/{zone-id}/monitor/*

Query Parameters:

Field	Notes
algorithm	Possible values: max, avg Default value: max Algorithm for determining the values to apply max:Use the maximum value learned (across all devices where applicable). avg:Use the average of all maximum value learned (across all devices where applicable).

Field	Notes
sensitivity	Possible values: high, low, default Default value: default The sensitivity level corresponds to a multiplier value:

Field	Notes

	high = 1.5
	low = 5.0
	default = 3.0

Example Request:

```
{
"algorithm": "max|avg", "sensitivity": "high|low|default", "manual_
thresholds": true|false
}
```

Field Notes:

Field	Notes
algorithm	Algorithm for determining the values to apply max: Use the maximum value learned (across all devices where applicable). avg: Use the average of all maximum values learned (across all devices where applicable).

sensitivity	The sensitivity level corresponds to a multiplier value:
	high = 1.5
	low = 5.0
	default = 3.0
	This multiplier is applied to the max/avg (see algorithm field)indicator

manual_ thresholds	If set to true, SecDevice will just set operational mode to “monitor” without making any automatic configuration of indicator threshold values.

Response Codes

See Common Response Codes.

Idle Zone

Puts the zone into idle operational-mode. No payload is required.

Method	URL
POST, OPTIONS	/agapi/v1/ddos/zone/{zone-id}/idle/

Response Codes

See Common Response Codes.

Start Zone Mitigation

SecDevice places the zone into “mitigation” status and starts mitigation on the zone:

- Pushes BGP configuration to the mitigation device(s)if BGP router commands are configured on the device.
- Zone incidents in "new” status will be put into “ongoing” status.

If part of the operation fails, the zone will be put into “error” status. User may retry start or stop mitigation on the zone.

Method	URL
POST	/agapi/v1/ddos/zone/{zone-id}/mitigation/start/

Response Codes

See Common Response Codes.

Stop Zone Mitigation

SecDevice stops the mitigation on the zone:

- BGP routes are removed from mitigator devices (if configured)
- Countermeasure
- configurations are removed from mitigators (if configured)
- Active
- zone incidents are put into “stopped” status