Partner API SDK

API generic information

The API is organized around REST. Our API has predictable, resource-oriented URLs, and uses HTTP response codes to indicate API errors. We use built-in HTTP features, like HTTP authentication and HTTP verbs, which are understood by off-the-shelf HTTP clients.

Base URL

All URL in examples and documentation bellow are relative to the base URL, which is

https://api.cujo.io/v1/

and

https://sapi.cujo.io/v1/ for the stage environmento

so, for example. the /auth API get the full as url https://api.cujo.io/v1/auth

Errors

The API uses conventional HTTP response codes to indicate the success or failure of an API request. In general, codes in the $2xx$ range indicate success, codes in the $4xx$ range indicate an error that failed given the information provided, and codes in the $5xx$ range indicate an error with servers (these are rare).

HTTP Status code summary

Status Code	Usage description
200 OK	**Response to a successful GET or DELETE.**
201 Created	**Response to a successful creation**
204 No content	**Responses without any content**
400 Bad request	**Used for validation errors**
401 Unauthorized	**When no or invalid authentication details are provided.**
404 Not found	**When requested item is not exist**

409 Conflict	**When trying to add duplicate record (item exists already)**

Every error (4xx) will include the error object as

Example
| ```json
{
   "error": "error message, if there is no error fields",
   "errors": [
      {
         "field1" : "error message"
      },
      {
         "field2" : "error message"
      },
      ...
   ]
}
``` |

HTTP Verbs

Where possible, API v3 strives to use appropriate HTTP verbs for each action.

Verb	Description
GET	Used for retrieving resources.
POST	Used for creating resources.
PUT	Used for updating resources
DELETE	Used for deleting resources.

Pagination

Requests that return multiple items will be paginated to 50 items by default. You can specify further pages with the `?page` parameter.

Example
curl 'https://api.cujo.io/v1/customers?page=2'

Note that page numbering is 0-based and that omitting the `?page` parameter should default to {{?page=0}}.

Agent modes

The agent can have only such modes as

dhcp - the agent is working in DHCP mode.
standby - the agent working in Standby mode
bridge - the agent connected and working Bridge mode.at
gateway - the agent is working in gateway mode. Router is forwarding traffic through the Cujo
unspecified - the agent mode is unknown. Can be for not connected agents.

Agent state

The agent state can be as

unregistered - for not registered agents
disabled - for disabled agents
enabled - for enabled agents

Device properties

hidden - If user hide this device until it comes online. Useful for old devices.
monitored - If CUJO should monitor device
secured - If true CUJO will block automatically when threat detected. Otherwise just threat is created and user notified.
quarantine - If all traffic from device should be blocked
Api is split up into 4 key topics:
- **GENERAL/CORE**
- **DEVICE IDENTIFICATION**
- **SECURITY**
- **PARENTAL CONTROLS**

Endpoints are tagged with required feature to be functional

Auth API

In order to make authorized calls to Cujo APIs, you must first obtain an access token.

POST /oauth/token - Creates the new access token

GENERAL/CORE

Generates the new API token, based on the Client ID and Client Secret keys.

Parameters

Parameter	Description	Format and Validation
client_id	The partner client ID key	Text. Any valid client ID key
client_secret	The partner client secret key	Text. Any valid secret key
grant_type	Grant type	Text. Always client_credentials

Responses

Response	Description
200	successfully get the access token
401	if client ID and client secret combination not found

<div align="center">**Example**</div>

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" -d
'grant_type=client_credentials&client_id=MY_ID&client_secret=MY_SECRET'
"/oauth/token"

200
{
"access_token": "abc...",
"token_type": "bearer",
"expires_in": 86399,
"scope": "public",
"partner": "123",
"jti": "abc-abc-abc-abc-abc"
}
```

GET /token - get the information about access token

GENERAL/CORE

Get the information about access token, used mostly for token validations

<div align="center">**Example**</div>

```
curl -H "Authorization: Bearer 53cf..."  /token


200
{
   "expiresInSeconds": 6812
}
```

Customers API

Allows to view details and manage customers

POST /customers/ - Register a new customer

GENERAL/CORE

Register the new customer and returns the customer object in response.json

Parameters

Parameter	Description	Values and validation	Notes
email	The customer email address	(optional if partnerUserId is not blank) Valid email address. Limited to 255 characters.	
partnerUserId	Some partner user ID stored with customer data	(optional if email is not blank) Text. Can be used to store partner user id. Limited to 255 characters.	Must be unique per partner, if left blank, email is used
phone	The customer phone number	(optional) Valid phone number.	

`phoneCountry`	Customer phone number country code	(optional)	
`password`	Customer password	(optional)	If not specified, you wont be able to login with this customer via mobile API

Responses

Response code	Description
201	Customer record successfully created
400	Not valid parameters email or phone
500	Could not register customer

Example

```
POST /customers
Authorization: Bearer 53cf....

{
"email": "demo@example.com",
"phoneCountry": "+1",
"phone": "23456789",
"partnerUserId": "12345",
"password": "x1y435/sq32"
}

201
{
"id": 345,
"email": "demo@example.com",
"phoneCountry": "+1",
"phone": "23456789",
"partnerUserId": "12345"
}
```

GET /customers - View all customers

GENERAL/CORE

Returns the list of all customers with pagination for 50 items per page.

Returns such information about each customer as:

Parameter	Description
id	The customer id
`email`	The customer email address
`partnerUserId`	Some partner user ID stored with customer data
`phone`	The customer phone number
`phoneCountry`	Customer phone number country code

password	Customer password
timezone	Customer timezone

<div align="center">

Example

</div>

```
GET /customers?page=0
Authorization: Bearer 53cf....

200
[
{
"id": 21,
"partnerUserId": "1",
"email": "taest@test.com",
"phoneCountry": "+1",
"phone": "2345678",
"timezone": "UTC"

},
{
"id": 29,
"partnerUserId": "2",
"email": "some@mail.com",
"phoneCountry": "+1",
"phone": "2345678"
 "timezone": "UTC"
}
]
```

GET /customers/:id - Get details for some customer

Returns the details for some customer as

Parameter	Description
id	The customer id
email	The customer email address
partnerUserId	Some partner user ID stored with customer data
phone	The customer phone number
phoneCountry	Customer phone number country code
password	Customer password
timezone	Customer timezone

PUT /customers/ - Change a customer details

Update the customer details and returns the updated information in response.

Parameters

Parameter	Description	Values and validation	Notes
email	The customer email address	(optional if partnerUserId is not blank) Valid email address. Limited to 255 characters.	
partnerUserId	Some partner user ID stored with customer data	(optional if email is not blank) Text. Can be used to store partner user id. Limited to 255 characters.	Must be unique per partner, if left blank, email is used.
phone	The customer phone number	(optional) Valid phone number with area code.	

Responses

Response code	Description
200	Customer record successfully updated
400	Not valid parameters email or phone

```
PUT /customers/21
Authorization: Bearer 53cf....

{
"partnerUserId": "1",
"email": "taest@test.com",
"phoneCountry": "+1",
"phone": "+12345678"
}

200
{
"id": 21,
"partnerUserId": "1",
"email": "taest@test.com",
"phoneCountry": "+1",
"phone": "2345678"
}
```

GET /customers/:id/agents - Get the list of customer agents

GENERAL/CORE

Returns the list of all customer agents with such information about each agent as

id: the agent id

customerId: the customer id
name: the agent name
agentMode: the agent mode (see modes in API generic section)
cloudMode: the agent mode which is currently configured (see modes in API generic section)
online: true or false, whether agent online or not

macAddress: mac address of and agent

serialNumber: serial number of an agent

lastSeen: the agent last seen time in milliseconds.

```
GET /customers/21/agents
Authorization: Bearer 53cf....

200
[
{
"id": 1034,
"online": true,
"cloudMode": "dhcp",
"agentMode": "standby",
"name": "My cujo",
"lastSeen": 1475153780
},
{
"id": 2379,
"online": false,
"cloudMode": "dhcp",
"agentMode": "dhcp",
"name": "Grandma cujo",
"lastSeen": 1475153793
}
]
```

Agents API

Allows to see details and manage agents

POST /agents/register - Register the new agent

GENERAL/CORE

Register the agent and return the agent information in response

Parameters

Parameter	description	Values and validation
gatewayMacAddress	The mac address for customer gateway	Text. Valid mac with columns
gatewayPublicIp	The ip address (public ip) for the customer gateway	Valid IP address
partnerUserId	User ID in the partner system	Must be not blank if `customerId` is not provided, if this parameter is used instead of `customerId`, a new dummy customer is created instead of returning 404 if no such customer exists.
customerId	the ID of the customer	Most be >= 0, if `partnerUserId` is not provided

Responses

Response	Description
200	Agent successfully activated
404	Agent with passed and mac was not foundip
400	Mac address or IP address is not in correct format
409	Such IP and Mac belongs to agent, which was already activated

---

Example

```
POST /agents/register
Authorization: Bearer 53cf....

{
"gatewayMacAddress": "f9:8b:fc:da:da:1d",
"gatewayPublicIp": "95.151.238.60",
"customerId": 1
}




200

{
   "id": 2379,
"partnerAgentId": "f9:8b:fc:da:da:1d",
"name": "Gradma cujo",
"macAddress": "f9:8b:fc:da:da:1d",
"cloudMode": "dhcp",
"agentMode": "dhcp",
"online": false,
"lastSeen": 129600
}
```

GET /agents/:id - Details for some agent

GENERAL/CORE

Get details for some agent with such information as
id: the agent id
partnerAgentId: external agent/gateway id, used in partner's system
name: the agent name
cloudMode: the agent mode (see modes in API generic section)
agentMode: the current agent mode, can be different to mode in case mode changes requested but not applied yet.
online: yes or no whether agent online or not
lastSeen: the agent last seen time in seconds.

Responses

Response	Description
200	Agent successfully retrieved
404	Agent with passed id was not found

```
                              Example
GET /agents/1

Authorization: Bearer 53cf....



200
{
"id": 1,

"partnerAgentId": "01:23:45:67:89:ab",

"name": "test agent",
"macAddress": "f9:8b:fc:da:da:1d",
"cloudMode": "bridge",
"agentMode": "dhcp",
"online": true,
"lastSeen": 1474991037575,
"customerId": 123,
"partnerUserId": "abc"
}
```

GET /agents/:partner_agent_id - Details for some agent

`GENERAL/CORE`

respone matches GET /agents/:id

Deprecated since v2.33 GET /partner-agents/:partner_agent_id - Details for partner agent

`GENERAL/CORE`

Response payload is identical to GET /agents/:id

Deprecated since v2.33 GET /partner-agents/:partner_agent_id/devices/search - Search devices by user agent.

`DEVICE IDENTIFICATION`

Search devices by user agent

Parameters:

Parameter	description	Values
partnerAgentId	partner agent id	Text
userAgent	user agent	Text
page	page number	int

Responses

Response	Description

200	success
404	Partner agent by partnerAgentId was not found

Data response is the same as in GET /agents/:agent_id/devices/:device_id

<div style="border:1px solid #ccc;">

<div align="center">**Example**</div>

```
GET partner-agents/1/devices/search?userAgent=ExoPlayerOk/17.7.20
(Linux;Android 6.0) ExoPlayerLib/ExoPlayerLib/2.4.1

Authorization: Bearer 53cf....


200
[
    {
        "meta":{
            "score":0,
            "itemType":"CompleteDevice"
        },
        "data":{
            "id":2295046,
            "modelAccuracyLevel":0,
            "quarantine":false,
            "monitored":true,
            "secured":true,
            "hidden":true,
            "operatingSystem":"RemixOS",
            "dhcpHostname":"android-df183f7b1a5a3ba8",
            "gatewayMac":"a0:f3:c1:b7:72:0a",
            "feedback":null,
            "model":"model",
            "brand":"brand",
            "type":null,
            "mac":"9c:5c:f9:8d:bb:10",
            "ip":"192.168.0.2",
            "lastSeen":1507796547362,
            "accurate":null,
            "capabilities":{
                "streaming":false,
                "4k":false
            }
        }
    }
]
```

</div>

GET /agents/:agent_id/devices/search - Search devices by user agent.

DEVICE IDENTIFICATION

Search devices by user agent

Parameters:

Parameter	description	Values

partnerAgentId	partner agent id	Text
userAgent	user agent	Text
page	page number	int
agentId	agent id	int

Responses

Response	Description
200	success
404	Agent with id is not found

Data response is the same as in GET /agents/:agent_id/devices/:device_id

```
GET partner-agents/1/devices/search?userAgent=ExoPlayerOk/17.7.20
(Linux;Android 6.0) ExoPlayerLib/ExoPlayerLib/2.4.1

Authorization: Bearer 53cf....


200
[
    {
        "meta":{
            "score":0,
            "itemType":"CompleteDevice"
        },
        "data":{
            "id":2295046,
            "modelAccuracyLevel":0,
            "quarantine":false,
            "monitored":true,
            "secured":true,
            "hidden":true,
            "operatingSystem":"RemixOS",
            "dhcpHostname":"android-df183f7b1a5a3ba8",
            "gatewayMac":"a0:f3:c1:b7:72:0a",
            "feedback":null,
            "model":"model",
            "brand":"brand",
            "type":null,
            "mac":"9c:5c:f9:8d:bb:10",
            "ip":"192.168.0.2",
            "lastSeen":1507796547362,
            "accurate":null,
            "capabilities":{
                "streaming":false,
                "4k":false
            }
        }
    }
]
```

GET /agents/:partner_agent_id/devices/search - Search devices by partner agent.

DEVICE IDENTIFICATION

response and request matches GET /agents/:agent_id/devices/search

GET /agents?partnerUserId=:id - List of agents under a customer

GENERAL/CORE

Get list of agents under some customer by partner user id.

```
GET /agents?partnerUserId=abc

Authorization: Bearer 53cf....



200

[
{
"id": 1,
"partnerAgentId": "01:23:45:67:89:ab",
"name": "test agent",
"macAddress": "f9:8b:fc:da:da:1d",
"cloudMode": "bridge",
"agentMode": "dhcp",
"online": true,
"lastSeen": 1474991037575
}
]
```

DELETE /agents/:id - Delete agent

`GENERAL/CORE`

Deletes agent by given id

id: the agent id

Responses

Response	Description
200	Agent successfully deleted
404	Agent with passed id was not found

Example

```
DELETE /agents/1

Authorization: Bearer 53cf....



200
```

DELETE /agents/:partner_agent_id - Delete agent

`GENERAL/CORE`

response matches DELETE /agents/:id - Delete agent

Deprecated since v2.33 DELETE /partner-agents/:partner_agent_id - Delete partner agent

Deletes agent by given partnerAgentId.

Response is identical to DELETE /agents/:id

Deprecated since v2.33 DELETE /agents?partnerUserId=:id - Delete agents by partner user id

Deletes all agents under some customer by partner user id.

id: partner user id

Responses

Response	Description
200	Agents successfully deleted
404	Customer with partner user id is not found

Example
| ```
DELETE /agents?partnerUserId=user1

Authorization: Bearer 53cf....



200
``` |

PUT /agents/:id/name - Change agent name

Change the agent name

Parameters

Parameter	description	Values
name	The new agent name	Text.

```
PUT /agents/1
Authorization: Bearer 53cf....

{
"name": "test"
}




{
"id": 1,

"partnerAgentId": "01:23:45:67:89:ab",

"name": "test agent",
"macAddress": "f9:8b:fc:da:da:1d",
"cloudMode": "bridge",
"agentMode": "dhcp",
"online": true,
"lastSeen": 1474991037575
}
```

PUT /agents/:partner_agent_id/name - Change agent name

`GENERAL/CORE`

response matches PUT /agents/:id/name

PUT /agents/:id/mode - Change agent mode

`GENERAL/CORE`

Change the agent mode

Parameters

Parameter	description	Values
mode	The new agent mode	Can be one of standby, dhcp, gateway Switch to DHCP will set default DHCP settings.

<table>
<tr><td align="center">**Example**</td></tr>
<tr><td>

```
PUT /agents/1/mode
Authorization: Bearer 53cf....

{
   "mode": "dhcp"
}



200

{
"id": 1,

"partnerAgentId": "01:23:45:67:89:ab",

"name": "test agent",
"macAddress": "f9:8b:fc:da:da:1d",
"cloudMode": "bridge",
"agentMode": "dhcp",
"online": true,
"lastSeen": 1474991037575
}
```

</td></tr>
</table>

PUT /agents/:partner_agent_id/mode - Change agent mode

GENERAL/CORE

response matches PUT /agents/:id/mode

POST /agents/:id/reboot - Reboot the agent

GENERAL/CORE

Initiate the agent reboot

Parameters

Parameter	description	Values
delayTime	The reboot delay time in seconds	(Optional) Number of seconds.

<table>
<tr><td align="center">**Example**</td></tr>
<tr><td>

```
POST /agents/1/reboot
Authorization: Bearer 53cf....

{
"delayTime": 360
}



204
```

</td></tr>
</table>

POST /agents/:partner_agent_id/reboot - Reboot the agent

response matches POST /agents/:id/reboot

PUT /agents/:id/network- Setup agent network

Setup network configuration for agent. Creates new or update existing.

Parameters

Parameter	description	Values
gatewayIp	the gateway IP	Valid IP
agentIp	the agent IP	Valid IP
networkMask	the mask	Valid network mask
broadcast	the broadcast	Valid IP

<table>
<tr><td align="center">Example</td></tr>
</table>

```
PUT /agents/1/network
Authorization: Bearer 53cf....


{

"gatewayIp": "10.0.0.1",
"agentIp": "10.0.0.2",
"networkMask": "255.0.0.0",

"broadcast": "10.0.0.255"

}


201

{

"gatewayIp": "10.0.0.1",
"agentIp": "10.0.0.2",
"networkMask": "255.0.0.0",

"broadcast": "10.0.0.255"


}
```

PUT /agents/:partner_agent_id/network- Setup agent network

response and request matches PUT /agents/:id/network

GET /agents/:id/network- Get agent network setup

Get network configuration for agent

Parameters:

gatewayIp: the gateway IP
agentIp: the agent IP
networkMask: the network mask
broadcast: the broadcast

Example
| ```
GET /agents/1/network
Authorization: Bearer 53cf....


200
{

"gatewayIp": "10.0.0.1",
"agentIp": "10.0.0.2",
"networkMask": "255.0.0.0",

"broadcast": "10.0.0.255"


}
``` |

GET /agents/:partner_agent_id/network- Get agent network setup

response matches GET /agents/:id/network

GET /agents/:id/dhcp - get the agent DHCP settings

Get the agent DHCP settings, such as DHCP server IP, lease time and etc.

serverIp: the address for the DHCP server (cujo device ip)
networkMask: the network mask
leaseTime: the lease time in seconds
startIp: the start IP address for DHCP leases
endIp: the end for DHCP leasesipaddresesleasesipaddreses
primaryDnsIp: the address for primary DNS server ipip
secondaryDnsIp: the address for secondary DNS server

routerNetwork: the router-agent network configuration

routerIp: the router ip
agentIp: the cujo-agent ip
networkMask: the router network mask

GET /agents/:partner_agent_id/dhcp - get the agent DHCP settings

`GENERAL/CORE`

response matches GET /agents/:id/dhcp

PUT /agents/:id/dhcp - Set the agent DHCP settings

`GENERAL/CORE`

Set (updates) the agent DHCP settings

Parameters

Parameter	Description	Values
`serverIp`	the address for the DHCP server (ipcujo device ip)ipcujoip	Valid IP address
`networkMask`	the network mask	Valid network mask
`leaseTime`	the lease time in seconds	Integer. values from 60 till 604800 (one week)
`startIp`	the start IP address for DHCP leases	Valid IP address within network mask smaller than end_ip
`endIp`	the end for DHCP leasesipaddreses	Valid IP address within network mask Greater than start_ip
`primaryDnsIp`	the address for primary DNS serverip	Valid IP address
`secondaryDnsIp`	the ip address for secondary DNS server ip	Valid IP address
routerNetwork	the router network configuration	Router network configuration properties to change. Optional
routerNetwork.routerIp	the ip address of the router in the router network	Valid IP address

routerNetwork.agentIp	the ip address of the cujo-agent device in the router network	Valid IP address
routerNetwork.networkMask	the router network mask	Valid network mask

Example

```
PUT /agents/1/dhcp
Authorization: Bearer 53cf....

{
"serverIp": "192.168.0.1",
"leaseTime": 3600,
"networkMask": "255.255.255.0",
"startIp": "192.168.0.2",
"endIp": "192.168.0.254",
"primaryDnsIp": "8.8.8.8",
"secondaryDnsIp": "4.4.4.4",

"routerNetwork": {
"routerIp": "10.0.0.1",
"agentIp": "10.0.0.2",
"networkMask": "255.0.0.0"
}

}



200
{
"leaseTime": 3600,
"serverIp": "192.168.0.1",
"networkMask": "255.255.255.0",
"startIp": "192.168.0.2",
"endIp": "192.168.0.254",
"secondaryDnsIp": "8.8.8.8",
"primaryDnsIp": "8.8.9.9",

"routerNetwork": {
"routerIp": "10.0.0.1",
"agentIp": "10.0.0.2",
"networkMask": "255.0.0.0"
}

}
```

PUT /agents/:partner_agent_id/dhcp - Set the agent DHCP settings

GENERAL/CORE

request and response matches PUT /agents/:id/dhcp

GET /agents/:id/static-ips - Get the agent devices with static IPs

DEVICE IDENTIFICATION

Get the list of devices with defined static IP addresses with such information about each item as
id: the ID of device
staticIp: the static IP assigned

name: the name of the device
mac: the mac addresses of the device

<div align="center">Example</div>

```
GET /agents/1/static-ips
Authorization: Bearer 53cf....

200
[
{
"id": 1,
"name": "Test name",
"mac": "aabbccddee",
"staticIp": "192.168.0.1"
},
{
"id": 2,
"name": "Test name",
"mac": "aabbccddee",
"staticIp": "192.168.0.1"
}
]
```

GET /agents/:partner_agent_id/static-ips - Get the agent devices with static IPs

DEVICE IDENTIFICATION

response matches GET /agents/:id/static-ips

PUT /agents/:id/static-ips - Set the agent Static IP addresses

GENERAL/CORE

Set (updates) the agent static IP address

Parameters

Parameters	Description	Values
id	the ID of device	valid device ID
staticIp	the static IP assigned	valid IP address which matched DHCP settings as for IP range and network mask

Example

```
PUT /agents/1/static-ips
Authorization: Bearer 53cf....

{
"devices": [

{
"id": 1,
"staticIp": "192.168.0.1"
},

{
"id": 2,
"staticIp": "192.168.0.2"
}

]
}


200

[
{
 "id": 1,
"name": "Test name",
 "mac": "aa:bb:cc:dd:ee",
"staticIp": "192.168.0.1"
},
{
"id": 2,
"name": "Test name",
"mac": "aa:bb:cc:dd:ee",
"staticIp": "192.168.0.2"
 }
]
```

PUT /agents/:partner_agent_id/static-ips - Set the agent Static IP addresses

`GENERAL/CORE`

request and response matches PUT /agents/:id/static-ips

Features API

`SECURITY`

View and control agent features.

Parameters

Parameter	Description	Type
security	Is security enabled or disabled for agent	boolean

GET /agents/:id/features - Get agent features

Example
| ```
GET /agents/1/features
Authorization: Bearer 53cf....

{

"security": true

}
``` |

GET /agents/:partner_agent_id/features - Get agent features

response matches GET /agents/:id/features

PUT /agents/:id/features - Update agent features

Example
| ```
PUT /agents/1/features
Authorization: Bearer 53cf....

{

"security": false

}

200

{

"security": false

}
``` |

PUT /agents/:partner_agent_id/features - Update agent features

response and request matches PUT /agents/:id/features

GET /agents/:id/listen-only-mode - Get listen only mode status for agent

`SECURITY`

Get agent's listen only mode status as
enabled: true if agent is working in listen only mode
netflowData: true if recent agent netflow activity was registered (default timespan is 3 days)

```
GET /agents/1/listen-only-mode
Authorization: Bearer 53cf....

200

{

"enabled": true,
"netflowData": true

}
```

GET /agents/:partner_agent_id/listen-only-mode - Get listen only mode status for partner agent

SECURITY

respone matches GET /agents/:id/listen-only-mode

POST /agents/listen-only-mode - Toggle listen only mode for a batch of agents

SECURITY

Enables or disables listen only mode for a batch of agents, identified by partner agent id.

Parameters

Parameters	Description	Values
enabled	should given agents be set to listen-only mode	true/false
agents	batch of agents for which to toggle the feature	A batch of partner agent ids. Batch size is not larger than 5000

	Example

```
POST /agents/listen-only-mode
Authorization: Bearer 53cf....

{

"enabled": true,
"agents": ["aaaaaaaaaaaa", "aaaaaaaaaaab"]

}

200
```

Devices API

GET /agents/:agent_id/devices/:device_id - Get agent device

DEVICE IDENTIFICATION

Get one device information.

Parameter	Description	Values

id	Device id	long
hidden	**Is device hidden or not.** **Set to true, If user hide this device until it comes online.**	**boolean**
monitored	Is device set to monitored. If CUJO should monitor device	boolean
secured	If true CUJO will block automatically when threat detected. Otherwise just threat is created and user notified.	boolean
quarantine	If all traffic from device should be blocked	boolean
dhcpHostname	Hostname (network name)	String
mac	Device mac address	String
ip	Device IP address	String
lastSeen	When was the last time we received traffic from this device	long
modelAccuracyLevel	Accuracy level of model finger printing (0-10). Level 0: No model found Level 1: Vendor: {vendor} Level 2: Vendor generic Level 3: type Level 4: Vendor type Level 5: WURFL Level 6: more concrete generic prediction Level 7: Model of a series Level 8: Computer OS Level 9: Concrete model Level 10: Concrete model (Specified)	int
feedback	Feedback about device fingerprinting	String. Maximum length is 255 characters
accurate	Is device fingerprint accurate or not	true, false, null
operatingSystem	Device operating system	String
model	Device model	String. Maximum length is 255 characters
brand	Device brand	String. Maximum length is 255 characters
type	Device type	String. Maximum length is 255 characters. Can be one of the following: "Game Console", "Phone", "Alarm System", "Baby Monitor", "Web Camera", "Key Lock / E-doors", "Computer", "Other", "Router" "Tablet"
capabilities	Device capabilities based on device model	Object

GET /agents/:partner_agent_id/devices/:device_id - Get agent device

DEVICE IDENTIFICATION

response matches GET /agents/:agent_id/devices/:device_id

GET /agents/:id/devices - Get all agent devices

Get list of all detected agent devices.

<div align="center">Example</div>

```
GET /agents/1/devices

Authorization: Bearer 53cf....

200

[
{
"id": 1,
"quarantine": true,
"monitored": true,
"secured": true,
"hidden": false,
"dhcpHostname": "Chromecast",
"mac": "aa:aa:aa:aa:aa:aa",
"ip": "192.168.0.1",
"lastSeen": "1478761546",
"modelAccuracyLevel": 2,
"accurate": true,
"operatingSystem": "Windows 8.1",
"model": "abc",
"feedback": "feedback"
"brand": "routers",
"type": "router",
"capabilities": {
"streaming": true,
"4k": true
}
}
]
```

GET /agents/:partner_agent_id/devices - Get all agent devices

response matches GET /agents/:id/devices

PUT /agents/:agent_id/devices/:device_id - Update device information

Change the information for some device.

PUT /agents/:partner_agent_id/devices/:device_id - Update device information

DEVICE IDENTIFICATION

response and request matches PUT /agents/:agent_id/devices/:device_id

DELETE /agents/:id/devices/:deviceId - Delete device

DEVICE IDENTIFICATION

Deletes device by the given id

id: the agent id

deviceId: the device id

Responses

Response	Description
200	Device successfully deleted
404	Device with passed id was not found

<div align="center">Example</div>

```
DELETE /agents/1/devices/2

Authorization: Bearer 53cf....



200
```

DELETE /agents/:partner_agent_id/devices/:deviceId - Delete device

`DEVICE IDENTIFICATION`

response matches DELETE /agents/:id/devices/:deviceId

DELETE /agents/:id/devices - Delete all devices for agent

`DEVICE IDENTIFICATION`

Deletes all devices for the given agent

id: the agent id

Responses

Response	Description
200	Devices successfully deleted
404	Agent with passed id was not found

<div align="center">Example</div>

```
DELETE /agents/1/devices

Authorization: Bearer 53cf....



200
```

DELETE /agents/:id/devices - Delete all devices for agent

DEVICE IDENTIFICATION

request and response matches DELETE /agents/:partner_agent_id/devices

GET /agents/:id/devices/:deviceId/stats/bundle - Device statistics

DEVICE IDENTIFICATION   **SECURITY**

Get combined device traffic statistics for last 24h

Request parameters:

Parameter	Description	Values
id	Agent ID	long
deviceId	Device ID	long

Response parameters:

Parameter	Description	Values
mac	Device mac address	long
in	Incomming traffic	
out	Outgoing traffic	
combined	Combined (incomming + outgoing) traffic	
size	Traffic in bytes	long
packets	Number of packets	long
ips	List of source and destination IP's	
collectionTime	Collection timestamp in UUID format	String
sourceIp	Source IP address	String
destinationIp	Destination IP addess	String

Example response

```
GET /agents/1/devices/2/stats/bundle
Authorization: Bearer 53cf....


200
{
    "mac": "00:14:22-01:23:45",
    "in": {
        "size": 3201106316,
        "packets": 2189114
    },
    "out": {
        "size": 53101400,
        "packets": 908440
    },
    "combined": {
        "size": 3254207716,
        "packets": 3097554
    },
    "ips": [
        {
            "collectionTime": "1f1d1fe4-cb64-11e7-ac1d-67f1fff69572",
            "sourceIp": "10.0.0.1",
            "destinationIp": "192.168.0.3"
        },
        {
            "collectionTime": "1f1d1fe3-cb64-11e7-ac1d-67f1fff69572",
            "sourceIp": "10.0.0.1",
            "destinationIp": "192.168.0.3"
        },
        {
            "collectionTime": "1f1d1fe2-cb64-11e7-ac1d-67f1fff69572",
            "sourceIp": "10.0.0.1",
            "destinationIp": "192.168.0.3"
        }
    ]
}
```

GET /agents/:partner_agent_id/devices/:deviceId/stats/bundle - Device statistics

DEVICE IDENTIFICATION   SECURITY

response matches GET /agents/:id/devices/:deviceId/stats/bundle

Firmware API

GET /agents/:id/firmware - Get the current and available firmware agent versions

GENERAL/CORE

Receive the current agent firmware version with the list of available versions to upgrade, if any available

currentVersion: the current firmware version
availableVersions: the list of available version, if any available

<table>
<tr><td align="center">Example</td></tr>
<tr><td>

```
GET /agents/1/firmware
Authorization: Bearer 53cf....


200

{
"message": "Upgrade message.",
"currentVersion": 66,
"availableVersions": [
{
"message": "Other upgrade message",
"version": 67
}
]
}
```

</td></tr>
</table>

GET /agents/:partner_agent_id/firmware - Get the current and available firmware agent versions

GENERAL/CORE

response matches GET /agents/:agent_id/firmware

POST /agents/:id/firmware - Initiate agent firmware upgrade

GENERAL/CORE

initiate the upgrade to specified version or to the latest if no version specified

Parameters

Parameter	Description	Value
version	The version to upgrade to	(Optional) the valid firmware version from /firmwareGET

```
POST /agents/1/firmware
Authorization: Bearer 53cf....

{
"version": "2004"
}



204
```

POST /agents/:partner_agent_id/firmware - Initiate agent firmware upgrade

`GENERAL/CORE`

request and response matches POST /agents/:id/firmware

Threats API

Get the information about threats for the agents and customers

GET /agents/:id/threats - get all threats for the agent

`SECURITY`

Get the list of all threats detected for some agent. Returns such information about each threat item as

Field	Description
id	Threat id
agentId	Agent id
partnerAgentId	External agent/gateway id, used in partner's system
type	Threat type
interactionType	Interaction type (INTERACTIVE, NOTIFICATION)
description	Threat description
level	Threat level
action	Is blocking threat (block, ignore)
customerAction	Customer action for threat (NO_ACTION, BLOCK, UNBLOCK)
startedAt	Threat started timestamp
endedAt	Threat ended timestamp
geolocation	Country
direction	Direction (IN, OUT)

Parameters:

parameter	Description	value
type	Filter threats by type	Optional. Can be SAFE_BROWSING, IP_REPUTATION, DOS, REMOTE_ACCESS, MODEL_PROFILE

action	Filter threats by action	Optional. Can be ignore or block

```
GET /agents/1/threats
Authorization: Bearer 53cf....


200
[
{
"id": 22,
"agentId": 546,
"partnerAgentId": "01:23:45:67:89:ab",
"type": "SAFE_BROWSING",
"interactionType": "NOTIFICATION",
"description": "Stopped attempt to visit "api.example.com". This potential
threat is categorized as Malware Distribution Point",
"level": "low"
"action":"block"
},

{
"id": 28,
"agentId": 456,
"partnerAgentId": "04:23:dd:67:89:ab",
"type": "REMOTE_ACCESS",
"interactionType": "INTERACTIVE",
"description": "We blocked an unauthorized attempt to access device "IP
Camera" from IP "111.111.65.1"",
"level": "critical"
"action": "block"
}

]
```

Example

GET /agents/:partner_agent_id/threats - get all threats for the agent

SECURITY

response matches GET /agents/:id/threats

Deprecated since v2.33 GET /partner-agents/:partner_agent_id/threats - get all threats for the partner agent

SECURITY

Response payload is Identical to GET /agents/:id/threats.

PUT /agents/:agent_id/threats/:threat_id - Change the action for some threat

SECURITY

Change the action (ignore or block) for some specific threat.

Parameters

Parameter	Description	Values

action	The action to take for threats	Can be only ignore or block

Example
| ```
PUT /agents/1/threats/28
Authorization: Bearer 53cf....

{
"action": "ignore"
}




200

{
"id": 28,
"agentId": 456,
"partnerAgentId": "04:23:dd:67:89:ab",
"type": "remote access",
"interactionType": "INTERACTIVE",
"description": "We blocked an unauthorized attempt to access device "IP
Camera" from IP "111.111.65.1"",
"level": "critical"
"action": "ignore"
}
``` |

PUT /agents/:partner_agent_id/threats/:threat_id - Change the action for some threat

SECURITY

request and response matches PUT /agents/:agent_id/threats/:threat_id

Deprecated since v2.33 PUT /partner-agents/:partner_agent_id/threats/:threat_id - Change the action for a threat

SECURITY

Payloads are identical to PUT /agents/:agent_id/threats/:threat_id.

GET /agents/:id/threats/:id - Get details for some threat

SECURITY

Get the details for some specific threat, returns such information as

Field	Description
id	Threat id
agentId	Agent id
partnerAgentId	External agent/gateway id, used in partner's system
type	Threat type
interactionType	Interaction type (INTERACTIVE, NOTIFICATION)
description	Threat description
level	Threat level

action	Is blocking threat (block, ignore)
customerAction	Customer action for threat (NO_ACTION, BLOCK, UNBLOCK)
startedAt	Threat started timestamp
endedAt	Threat ended timestamp
geolocation	Country
direction	Direction (IN, OUT)
deviceId	Device, to which threat is generated for, id
deviceMac	Device, to which threat is generated for, mac
seen	Has customer seen the threat

metadata	For Safe Browsing type threats:
	    url: \<string\> ("http://www.hostname.com")
	    categories: [\<string\>] (Spam Source, BotNet, Scanner, Phishing, ...)
	
	For Ip Reputation type threats:
	    inbound: \<boolean\>
	    ip: \<string\>
	    category: \<string\> (Spam Source, BotNet, Scanner, Phishing, ...)
	
	For DOS type threats:
	    ip: \<string\>
	
	For Remote Access type threats:
	    ip: \<string\>
	    port: \<integer\>
	
	For Model Profile type threats:
	    ip: \<string\>
	    port: \<integer\>
	    asn: \<string\>
	    broadcast: \<boolean\>
	    multicast: \<boolean\>

Example

```
GET /agents/1/threats
Authorization: Bearer 53cf....


200
{
"id": 22,
"agentId": 65,
"partnerAgentId": "aa:aa:aa:aa:aa:aa",
"type": "Safe browsing",
"interactionType": "NOTIFICATION",
"description": "Stopped attempt to visit "api.example.com". This potential
threat is categorized as Malware Distribution Point",
"level": "low"
"action": "block"
"startedAt": 1475148966,
"endedAt": 1475148966,
"deviceId": 12,
"seen": false
}
```

GET /agents/:partner_agent_id/threats/:id - Get details for some threat

response matches GET /agents/:agent_id/threats/:id

GET /partner-agents/:partner_agent_id/threats/:threat_id - Get details for a threat

Response payload is identical to GET /agents/:agent_id/threats/:threat_id.

Stats API

Get various statistics for threats, agents and customers.

GET /stats/customers - Get stats for customers

Receive the current statistics for the customers as "total number of customers".

Example
| ```
GET /stats/customers
Authorization: Bearer 53cf....

200
{
"total": 234
}
``` |

GET /stats/agents - Get stats for Cujo agents

Receive the current state statistics for the agents as
  online: the current number of agent online
  offline: the current number of offline agents
  enabled: the current number of enabled agents
  disabled: the current number of disabled agents
  security: number of agent with security enabled
  total: the total number of activated agents at the current time
  modeArp: the current number of agents in ARP mode
  modeDhcp: the current number of agents in DHCP mode
  modeBridge: the current number of agents in Bridge mode
  modeStandby: the current number of agents in Standby mode
  modeGateway: the current number of agents in gateway mode
  modeUnspecified: the current number of agents in Unspecified mode

```
GET /stats/agents
Authorization: Bearer 53cf....

200
{
"disabled": 100,
"enabled": 200,
"security: 22,
"offline": 100,
"online": 200,
"total": 300,
"modeUnspecified": 0,
"modeStandby": 120,

"modeGateway": 120,

"modeBridge": 60,
"modeDhcp": 120,
"modeArp": 0
}
```

GET /stats/threats - Get stats for threats

SECURITY

receive the statistics for the threats for the selected time period. If parameters not specified, returns data for last 30 days period.

total: the total number of threats detected
actionBlock: the number of blocked threats
actionIgnore: the number of ignored threats
typeDdos: the number of DDOS threats detected
typeSafeBrowsing: the number of safe browsing threats detected
typeDnsReputation: the number of DNS threats detected
typeIpReputation: the number of IP threats detected
typeRemoteAccess: the number of "remote access" threats detected
typeMalware: the number of malware threats detected
typeSuspiciousActivity: the number of suspicious activity threats detected
typeSuspiciousConnection: the number of suspicious connection threats detected
typeVulnerability: the number of vulnerabilities detected

Parameters

Parameter	Description	Values
fromDate	The from date to return threats stats	(Optional) The valid date
toDate	The to date to return threats stats	(Optional) The valid date
agentId	The agent to return threats stats	(Optional) long
deviceId	The device to return threats stats	(Optional) long

```
GET /stats/threats
Authorization: Bearer 53cf....


200
{
actionBlock: 234,
  actionIgnore: 12367,
  typeDdos: 12,
typeDnsReputation: 1,
typeIpReputation: 13,
typeRemoteAccess: 0,
typeMalware: 12,
typeSuspiciousActivity: 0,
typeSuspiciousConnection: 1,
typeVulnerability: 0
}
```

IP reputation API

IP reputation

SECURITY

Query IP reputation data.

Example

```
POST /reputation/ip
Authorization: Bearer 53cf....
{
"ip": "123.123.123.123"
}

200

{
"status": "INVALID",
"data": {
"threatCategories": [
"Proxy",
"Botnets"
],
"threatLevel": 95
}
}
```

Parameters

Name	Possible values
status	VALID, INVALID

threatCategories	Spam Sources, Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy, Mobile Threats, Tor proxy

Vulnerability Scan API

Provides information about scheduled vulnerability scans

GET /scans/schedule

Retrieves scan schedules by partner id with pagination for 50 items per page.

Example

```
GET /scans/schedule?partnerId=1&page=0
Authorization: Bearer 53cf....

200
[
    {
        "weekDays": [1, 2, .. 7],
        "scanStartTime": "3:00",
   "scanFinishTime": "7:00"
    }, ...
]
```

PUT /scans/schedule

Creates scan schedules by partner id

Example

```
PUT /scans/schedule?partnerId=1
Authorization: Bearer 53cf....
{
 "weekDays": [1, 2, .. 7],
 "scanStartTime": "3:00",
 "scanFinishTime": "7:00"
}

200
[
 {
  "deviceId": 1,
  "weekDays": [1, 2, .. 7],
  "scanStartTime": "3:00",
  "scanFinishTime": "7:00"
 }, ...
]
```

GET /scans

SECURITY

Returns vulnerability scan results with pagination for 50 items per page.

Example

```
GET /scans?partnerId=1&page=0
Authorization: Bearer 53cf....

200
[
 {
  "date": 1475148966,
  "agentId": 1,
  "deviceId": 1,
  "vulnerabilities":
  [
   {
    "threat": "HIGH|MEDIUM|LOW|LOG|DEBUG|UNKNOWN",
    "severity": 2.0,
    "port": "",
    "name": "",
    "recommendation": "",
    "nvtFamily": "",
    "cve": "",
    "xref": ""
   }, ...
  ]
 }, ...
]
```

GET /agents/:agentId/scans

SECURITY

Returns vulnerability scan results for agent with pagination for 50 items per page.

```
GET /agents/1/scans?partnerId=1&page=0
Authorization: Bearer 53cf....

200
[
 {
  "date": 1475148966,
  "deviceId": 1,
  "vulnerabilities":
  [
   {
    "threat": "HIGH|MEDIUM|LOW|LOG|DEBUG|UNKNOWN",
    "severity": 2.0,
    "port": "",
    "name": "",
    "recommendation": "",
    "nvtFamily": "",
    "cve": "",
    "xref": ""
   }, ...
  ]
 }, ...
]
```

GET /agents/:partner_agent_id/scans

SECURITY

response matches GET /agents/:agentId/scans

GET /agents/:agentId/scans/schedule

SECURITY

Provides information about on-demand vulnerability scan status

state: SCHEDULED, FINISHED, NONE

devicesId: device ID

lastScan: last scan time

```
GET /agents/1/scans/schedule
Authorization: Bearer 53cf....

200
[
    {
        "state": "SCHEDULED|FINISHED|NONE",
   "deviceId": 12,
   "lastScan": 1475148966
    }, ...
]
```

PUT /agents/:agentId/scans/schedule

SECURITY

Enable on-demand vulnerability scan for given agent

deviceIds: list of device ID or empty list to scan all

```
PUT /agents/1/scans/schedule
Authorization: Bearer 53cf....
{
 "deviceIds": [12, 15, 90]
}

200
[
 {
  "state": "SCHEDULED|FINISHED|NONE",
  "deviceId": 12,
  "lastScan": 1475148966
 }, ...
]
```

PUT /agents/:partner_agent_id/scans/schedule

SECURITY

request and response matches PUT /agents/:agentId/scans/schedule

Notifications API

Notifications are implemented via web-hooks. Each web-hook should subscribe to a particular **object.** After subscribing to a certain type of objects, **POST HTTP** requests will be sent to provided URL once any **object** of that type is updated or created.

Webhook structure

The following table represents the web-hook object structure.

Web-hook

```
{
    "fullData":    boolean,
    "id":          long,
    "object":      String,
    "url":         String,
 "event":    String,
    "authentication": {
        String: Object,


        ...
    },
    "properties" : {
        String: Object,


        ...
    }
}
```

The following table describes web-hook object properties.

Name	Description	Possible values
fullData	Wether full object data should be included when sending notification via web-hook or only minimal details.	false, true
object	Which object is the web-hook subscribed to.	DEVICE, THREAT, FINGERPRINTED_DEVICE
url	Where to send data via HTTP request.	any string
id	Unique internal web-hook id.	any long number
event	Specific event to listen to	CREATE, UPDATE, ALL
authentication	Key - value pair of authentication properties.	key is of string type and value is any valid json type
properties	Key - value pair of properties. Some endpoints can support additional properties	key is of string type and value is any valid json type

The following table describes the `authentication` object properties.

Name	Description	Possible values
type	Authentication type	OAUTH
apiKey	The API authentication key	any string

apiSecret	The API authentication secret	any string

The following table describes the `properties` object properties.

Name	Value	Description	Supported object type
modelAccuracyLevel	1..10	Webhook will be triggered when submitted model level is reached for the new device	FINGERPRINTED_DEVICE
waitDuration	<int>	Time to wait for expected model level in seconds	FINGERPRINTED_DEVICE

GET /webhooks

GENERAL/CORE

Retrieves all created web-hooks.

Example

```
GET /webhooks
Authorization: Bearer 53cf....

200
[
    {
        "fullData": true,
        "object": "DEVICE",
        "event": "ALL",
        "url": "https://www.example.com",
        "id": 121
    }
]
```

GET /webhooks/:id

GENERAL/CORE

Retrieves existing created web-hook by its unique id.

```
GET /webhooks/121
Authorization: Bearer 53cf....

200
{
    "fullData": true,
    "object": "DEVICE",
    "event": "ALL",
    "url": "https://www.example.com",
    "id": 121
}
```

This call can have the following response codes.

Response	Description
200	Success.
404	Web-hook does not exist.

POST /webhooks

GENERAL/CORE

Creates a new web-hook for desired object.

```
POST /webhooks
Authorization: Bearer 53cf....
{
    "fullData": true,
    "object": "DEVICE",
    "event": "CREATE",
    "url": "https://www.example.com"
}

201
{
    "fullData": true,
    "object": "DEVICE",
    "event": "CREATE",
    "url": "https://www.example.com",
    "id": 121
}
```

PUT /webhooks/:id

Updates existing web-hook by using its unique id.

Example

```
PUT /webhooks/121
Authorization: Bearer 53cf....
{
    "fullData": true,
    "object": "DEVICE",
    "event": "CREATE",
    "url": "https://www.example.com"
}

201
{
    "fullData": true,
    "object": "DEVICE",
    "event": "CREATE",
    "url": "https://www.example.com",
    "id": 121
}
```

This call can have the following response codes.

Response	Description
201	Web-hook successfully updated.
409	Web-hook with passed URL and object type already exist (URL case is ignored).

DELETE /webhooks/:id

Deletes a web-hook by using its unique id.

```
DELETE /webhooks/121
Authorization: Bearer 53cf....

200
```

This call can have the following response codes.

Response	Description

200	Webhook successfully deleted.
404	Webhook with passed id was not found.

Webhook exchange protocol

Once desired web-hooks are created, appropriate notifications will be sent to those URLs. Data submitted to web-hook URLS will have **applicatio n/json** content type header. The requests will be sent using POST method. Data provided to these URLs will differ based on subscribed object type. There are two types of web-hook notifications (excluding type **ALL**), **CREATE** and **UPDATE**.

Structure

General notification structure can be described as the following.

Notification structure

```
{
    "object": String,
    "event":  String,
    "data": {
        "agentId": long,
        "id":      long,

        ...
    },
    "changes": {
        "old": {
            "propertyName": String,

            ...
        },
        "new": {
            "propertyName": String,

            ...
        }
    }
}
```

The following table describes properties of notification structure.

Nane	Description	Possible values
`object`	Object which generated the notification.	`DEVICE, THREA T`
`event`	What type of event was generated.	`CREATE, UPDATE`
`data`	Data which will be specific to subscribed object, for any object there will always be included an object `id` and `agentId`. Based on web-hook configuration, the `data` object may or may not include full details of the subscribed object. For example full threat or device details.	

changes	This indicates changes that were made to the subscribed object. The `changes` object will include property names of subscribed object and will show the changes that were made to this object. These details will only be included in `UPDATE` notifications.

UPDATE DEVICE example

Example for `UPDATE` notification type and device object (web-hook is configured with `fullObject=true`).

UPDATE event example

```json
{
  "object": "DEVICE",
  "event": "UPDATE",
  "data": {
    "agentId": 1,
 "partnerAgentId": "48:47:8f:9r",
    "id": 2,
    "quarantine": true,
    "monitored": true,
    "secured": true,
    "hidden": false,
    "dhcpHostname": "hostname",
    "mac": "aa:bb:cc:dd:ee:ff",
    "lastSeen": 1499061855,
    "modelAccuracyLevel": 2,
    "model": "Some model",
    "brand": "Some brand",
    "type": "Some type",
    "operatingSystem": "Some system",
  "gatewayMac": "64:d1:54:ce:fa:52",
  "feedback": "some feedback",
  "ip": "10.2.1.175",
  "accurate": true,
    "capabilities": {
        "streaming": true,
        "4k": true
    }
  },
  "changes": {
    "old": {
      "quarantine": false
    },
    "new": {
      "quarantine": true
    }
  }
}
```

CREATE DEVICE example

Example for CREATE notification type and device object (web-hook is configured with `fullObject=true`).

CREATE event example

```json
{
  "object": "DEVICE",
  "event": "CREATE",
  "data": {
    "agentId": 1,
    "partnerAgentId": "48:47:8f:9r",
    "id": 2,
    "quarantine": true,
    "monitored": true,
    "secured": true,
    "hidden": false,
    "dhcpHostname": "hostname",
    "mac": "aa:bb:cc:dd:ee:ff",
    "lastSeen": 1499061855,
    "modelAccuracyLevel": 2,
    "model": "Some model",
    "brand": "Some brand",
    "type": "Some type",
    "operatingSystem": "Some system",
    "gatewayMac": "4d:f7:d5:sf:47",
    "feedback": "feedback",
    "ip": "192.168.50.50",
    "accurate": false,
    "capabilities": {
        "streaming": true,
        "4k": true
    }
  }
}
```

CREATE THREAT example

Example for CREATE notification type and threat object (web-hook is configured with `fullObject=true`).

```
{
 "object":"THREAT",
 "event":"CREATE",
 "data": {
  "partnerAgentId":"6742b3bc41692673c83385235484030b02",
  "deviceId":2797216,
  "deviceMac":"b8:27:eb:29:77:4b",
  "seen":false,
  "metadata":{"ip":"42.7.26.16","port":22},
  "id":343859,
  "agentId":2797203,
  "partnerAgentId":"6742b3bc41692673c83385235484030b02",
  "type":"REMOTE_ACCESS",
  "description":"We detected an unauthorized attempt to access your
device \"Generic CUJO IoT device\" on port 22 from an IP 42.7.26.16
which originates from China.",
  "level":"CRITICAL",
  "action":"block",
  "geolocation":"China",
  "customerAction":"NO_ACTION",
  "startedAt":1524133474538,
  "endedAt":1524133474538
 }
}
```

Fingerprint device API

Fingerprint device model with passed in fingerprints list.

Possible types: MAC, USER_AGENT, DHCP, DHCP_VENDOR, DHCP_HOSTNAME, VENDOR, DNS, SSDP_HEADER, SSDP_RESPONSE, HTTP, MDNS, ROUTER.

POST /fingerprint - Fingerprint device (WARNING: Endpoint is deprecated and will be removed with release 2.32)

DEVICE IDENTIFICATION

Example

```
POST /fingerprint
Authorization: Bearer 53cf....

[
 {
  "type": "MAC",
  "value": "4c:8d:79:99:99:99"
 },
 {
  "type": "USER_AGENT",
  "value": "iPhone5,2"
 },
 {
  "type": "DNS",
  "value": "icloud.com"
 }
]


200

{
 "vendor": "Apple",
 "model": {
  "name": "iPhone 5",

"description": "Apple iPhone 5",

"defaultName": "Apple iPhone 5",

"brandName": "Apple",

"deviceTypeName": "Phone",

"deviceTypeDescription": "Phone"
 }
}
```

Countries API

API to retrieve available countries and manage agent threat country blacklists.

Country structure

Country

```
{
    "name": String,
    "id":   long
}
```

Country property descriptions.

Name	Description	Possible values
`name`	Formatted country name	Any string.
`id`	Internal country id	Any long number.

GET /countries

Retrieve all available countries.

```
GET /countries
Authorization: Bearer 53cf....

[
    {
        "name": "Some name",
        "id":   123
    }
]
```

GET /agents/:id/countries/blacklists

Retrieve countries which are added to a specific agents blacklist.

```
GET /agents/countries/:id/blacklists
Authorization: Bearer 53cf....

[
    {
        "name": "Some name",
        "id":   123
    }
]
```

GET /agents/:partner_agent_id/countries/blacklists

response matches GET /agents/:id/countries/blacklists

PUT /agents/:id/countries/blacklists

Update country blacklist for a specific agent.

```
PUT /agents/:id/countries/blacklists
Authorization: Bearer 53cf....
[
    123
]


200
[
    {
        "name": "Some name",
        "id":   123
    }
]
```

PUT /agents/:partner_agent_id/countries/blacklists

request and response matches PUT /agents/:id/countries/blacklists

Access profiles API

AccessProfileRequest:

```
{
    "id":                   long,
    "categoryCount":        int,
    "deviceCount":          int,
    "allowedDomainCount":   int,
 "blockedDomainCount":   int,
    "color":                String,
    "name":                 String,
    "internetPausedUntil":  Long,
    "avatar": {
        "id":           long,
        "modifiable":   boolean,
        "url":          String
    },
 "scheduleCount":   int,
    "activeSchedule": {
        "id":     long,
        "name":   String,
        "type":   String
    }
}
```

Properties:

Name	Description	Default value
internetPausedUntil	Until when the internet is paused for this access profile	null
activeSchedule	Schedule which is currently active for this profile	null

Get access profiles

PARENTAL CONTROLS

Endpoint

```
GET /access-profiles?agentId={agentId}
GET /access-profiles?partnerAgentId={partnerAgentId}
```

Response body

AccessProfileRequest

Get access profile

PARENTAL CONTROLS

Endpoint

```
GET /access-profiles/{accessProfileId}
```

Response body

AccessProfileRequest

Create access profile

PARENTAL CONTROLS

Endpoint

```
POST /access-profiles
```

Request body

Note that `color` and `name` properties must not be blank, `color` is limited to 6 characters and `name` is limited to 255. Also if {{pauseInternetSeconds}} is 0 or below 0, the internet for this profile will be un-paused.

```
{
    "agentId":             long,
    "partnerAgentId":      long,
 "color":                  String,
    "name":                String,
    "avatarId":            Long,
    "pauseInternetSeconds": int
}
```

Response body

AccessProfileRequest

Update access profile

PARENTAL CONTROLS

Endpoint

```
PUT /access-profiles/{id}
```

Request body

Note that if {{pauseInternetSeconds}} is 0 or below 0, the internet for this profile will be un-paused.

```
{
 "agentId":              long,
    "partnerAgentId":       long,
 "color":                String,
    "name":                 String,
    "avatarId":             Long,
    "pauseInternetSeconds": int
}
```

Response body

Access profile object. The format can be seen here.

Delete access profile

PARENTAL CONTROLS

Endpoint

```
DELETE /access-profiles/{accessProfileId}
```

Get access profile content categories

PARENTAL CONTROLS   SECURITY

Endpoint

```
GET /access-profiles/{accessProfileId}/categories
```

Response body

```
[
    {
        "id":           long,
        "selected":     boolean,
        "description":  String,
        "name":         String,
        "icon":    IconJson
    }
]
```

Manage access profile categories

Endpoint

```
PUT /access-profiles/{accessProfileId}/categories
```

Request body

Include the list of preferred content categories for this profile, all previous categories will be replaced by the provided ones.

```
[
 long, ...
]
```

Response body

The response body will include updated list of all content categories assigned to this access profile.

```
[
    {
        "id":           long,
        "selected":     boolean,
        "description":  String,
        "name":         String,
        "icon":    IconJson
    }
]
```

Get access profile devices

Endpoint

```
GET /access-profiles/{accessProfileId}/devices
```

Request body

Include the list of access profile devices ID's.

```
[
 long, ...
]
```

Response body

Note that this call will return all devices under the agent, which is assigned to this access profile. Weather a device is assigned to a profile or not, can be found out using the `selected` flag.

```
[
    {
        "id":           long,
        "selected":     boolean,
        "name":         String,
   "ip":      String,
        "icon": {
            // Standard icon object.
        }
    }
]
```

Manage access profile devices

Endpoint

```
PUT /access-profiles/{accessProfileId}/devices
```

Request body

Same as for content categories, include the list of preferred devices categories for this profile.

```
[
 long, ...
]
```

Response body

```
[
    {
        "id":          long,
        "selected":     boolean,
        "ip":   String,
        "name":          String,
        "icon":    IconJson
    }
]
```

Profile activity logs

`PARENTAL CONTROLS` `SECURITY`

Get blocked domains by access profile id and additional query parameters.

Endpoint

```
GET /access-profiles/{accessProfileId}/activity-logs
```

Filtering

When making this request, you can specify query parameters which will be used to filter blocked domains.

Name	Description	Type	Default value
profileName	Access profile name	String	
domain	Blocked domain name	String	
categories	Array of content category ids	Long[]	
fromDays	Start of the interval, from where to query the blocked domains in days	Integer	1
toDays	End of the interval in days	Integer	

Example

```
GET
/access-profiles/1/activity-logs?profileName=test&domain=test&categories
=1&categories=2&fromDays=2&toDays=1
```

Response body

```
[
 {
  "allowed":      boolean,
  "domain":     String,
  "id":     String,
  "createdOn":  Date,
  "device":   ActivityLogDevice,
  "categories":  List<ContentCategory>
 },
 {
  ...
 },
 ...
]
```

ActivityLogDevice:

```
{
 "id":    long,
 "name":  String,
 "icon":  IconJson
}
```

ContentCategory:

```
{
 "id":      long,
 "name":    String,
 "description":  String
 "icon":    IconJson
}
```

IconJson:

```
{
 "id":     long,
 "name":   String,
 "prefix":   String
 "icons":  Map<String, String>
}
```

Allowed/blocked domains

Access profile allowed domains list

`PARENTAL CONTROLS`   `SECURITY`

Endpoint

```
GET /access-profiles/{accessProfileId}/domain/allowed
```

Response body

```
[
    String
]
```

Add allowed domain

`PARENTAL CONTROLS`   `SECURITY`

Add allowed domain for an access profile.

Endpoint

```
POST /access-profiles/{accessProfileId}/domain/allowed
```

Request body

```
{
    "domain":  String
}
```

Remove allowed domain

PARENTAL CONTROLS   SECURITY

Remove allowed domain from access profile.

Endpoint

```
DELETE /access-profiles/{accessProfileId}/domain/allowed
```

Request body

```
{
    "domain":  String
}
```

Blocked domains list

PARENTAL CONTROLS   SECURITY

Get list of blocked domains for an access profile.

Endpoint

```
GET /access-profiles/{accessProfileId}/domain/blocked
```

Response body

```
[
    String
]
```

Add blocked domain

PARENTAL CONTROLS   SECURITY

Add blocked domain for an access profile.

Endpoint

```
POST /access-profiles/{accessProfileId}/domain/blocked
```

Request body

```
{
    "domain":  String
}
```

Remove blocked domain

`PARENTAL CONTROLS` `SECURITY`

Remove blocked domain from access profile.

Endpoint

```
DELETE /access-profiles/{accessProfileId}/domain/blocked
```

Request body

```
{
    "domain":  String
}
```

Remove blocked and allowed domains

`PARENTAL CONTROLS` `SECURITY`

This request allows to remove `allowed` and `blocked` domains in bulk.

Endpoint

```
DELETE /access-profiles/{accessProfileId}/bulk-domains
```

Request body

```
{
    "allowed": [
        String,

        ...
    ],
    "blocked": [
        String,

        ...
    ]
}
```

Response body

Response will include updated `allowed` and `blocked` domain lists for this access profile.

Change blocked and allowed domains

PARENTAL CONTROLS   SECURITY

This request allows to update or modify `allowed` and `blocked` domain lists. **Note** if you provide an `allowed` domain which is in `blocked` list (on back-end). The domain from `blocked` list will be moved to `allowed` list (the same goes for `blocked` list).

Endpoint

```
PUT /access-profiles/{id}/bulk-domains
```

Request body

```
{
    "allowed": [
        String,

        ...
    ],
    "blocked": [
        String,

        ...
    ]
}
```

Response body

Response will include updated `allowed` and `blocked` domain lists for this access profile.

Avatar

Get access profile avatars

Get all available access profile avatars.

Endpoint

```
GET
/access-profiles/avatars?includeModifiable={includeModifiable}?partnerUs
erId=1
```

Parameters

Name	Description	Type	Default value
includeModifiable	Should modifiable avatars be included	boolean	false
partnerUserId	user id in partner environment	long	

Response body

The `modifiable` property indicates weather this avatar can be modified via `PUT` request (avatars with `modifiable = false` are default avatars).

```
[
    {
        "id":          long,
        "url":         String,
        "modifiable": boolean
    }
]
```

Get access profile avatar

Get access profile avatar details or the avatar image itself.

Endpoint

```
GET /access-profiles/avatars/{id}?partnerUserId=1
```

Response body

Note that the response body will vary based on provided **Accept** header**.** If **Accept** header is set to `image/png`, this call will return the image itself instead of `JSON` response. If no **Accept** header is provided, a regular `JSON` response will be returned.

```
{
    "id":          long,
    "url":         String,
    "modifiable":  boolean
}
```

Create access profile avatar

`PARENTAL CONTROLS`

Create a new access profile avatar under customer account.

Endpoint

```
POST /access-profiles/avatars?partnerUserId=1
```

Request body

The `image` property must be a Base64 encoded image content.

```
{
    "customerId": long,
    "image": String
}
```

Response body

```
{
    "id":          long,
    "url":         String,
    "modifiable":  boolean
}
```

Update access profile avatar

`PARENTAL CONTROLS`

Update existing access profile avatar details.

Endpoint

```
PUT /access-profiles/avatars/{id}?partnerUserId=1
```

Request body

The `image` property must be valid Base64 encoded image content, same as in access profile avatar creation.

```
{
    "customerId": long,
    "image": String
}
```

Response body

```
{
    "id":         long,
    "url":        String,
    "modifiable": boolean
}
```

Delete access profile avatar

`PARENTAL CONTROLS`

Delete existing access profile avatar.

Endpoint

```
DELETE /access-profiles/avatars/delete?id=1&partnerUserId=123
```

Access profile statistics

Get speficied access profile statistics.

`PARENTAL CONTROLS`   `SECURITY`

Endpoint

```
GET /access-profiles/{profileId}/statistics?days={days}
```

Request parameters

Name	Description	Type	Default value
profileId	Profile, whose statistics to query, id	long	
days	Optional parameter which indicates how many days of statistics should be queried	int	7

Response body consist of map with date string as key and deviceCount as a value.

Response body example

```
{
 "2017-03-23": 5,
 "2017-03-22": 12,
 ...
}
```

Schedules

`PARENTAL CONTROLS` `SECURITY`

ScheduleRequest:

```
{
    "weekDay":    Set<Integer>,
    "startTime":  Date,
    "endTime":    Date,
    "title":   String,
    "enabled":   boolean,
    "pauseInternet":  boolean
}
```

enabled: mandatory

pauseInternet: mandatory

ScheduleResponse:

```
{
    "id": long,
    "profileId": long,
    "agentId": long,
    "title": String,
    "enabled": boolean,
    "scheduleType": ScheduleType,
    "startTime": Date,
    "endTime": Date,
    "weekDay": Set<Integer>,
    "pauseInternet": boolean,
    "categories": List<AccessProfileContentCategory>,
    "allowedDomains": Set<String>,
    "blockedDomains": Set<String>
}
```

weekDay: valid list values: 1..7, valid list size: 1 <= size <= 7

Date

Millis from epoch start, ie 1493972959329

BulkDomainsDetails

```
{
    "allowed": Set<String>,
    "blocked": Set<String>
}
```

BulkDomains

```
{
    "allowed": Set<String>,
    "blocked": Set<String>
}
```

Create schedule

PARENTAL CONTROLS   SECURITY

Endpoint

```
POST /schedules
```

Request body

```
{
    "weekDay":    Set<Integer>,
    "startTime":  Date,
    "endTime":    Date,
    "profileId":  long,
    "agentId":    long,
    "title":    String,
    "enabled":   boolean,
    "pauseInternet": boolean
}
```

Response body

ScheduleResponse

Get schedules for profile

Endpoint

```
GET /schedules?profileId={profileId}
```

Response body

List of ScheduleResponse

Get schedule by id

Endpoint

```
GET /schedules/{scheduleId}
```

Response body

ScheduleResponse

Get active schedule for profile

Endpoint

```
GET /schedules/active?profileId={profileId}
```

Response body

ScheduleResponse

Update schedule

Endpoint

```
PUT /schedules/{scheduleId}
```

Request body

ScheduleRequest

Response body

ScheduleResponse

Delete schedule

Endpoint

```
DELETE /schedules/{scheduleId}
```

Get categories for schedule

Endpoint

```
GET /schedules/{scheduleId}/categories
```

Response body

List of AccessProfileContentCategory

Update categories for schedule

Endpoint

```
PUT /schedules/{scheduleId}/categories
```

Request body

Collection of category Id's. Type of category Id is Long.

Response body

List of AccessProfileContentCategory

Get domains for schedule

`PARENTAL CONTROLS`   `SECURITY`

Endpoint

```
GET /schedules/{scheduleId}/domains
```

Response body

BulkDomains

Update domains for schedule

`PARENTAL CONTROLS`   `SECURITY`

Endpoint

```
PUT /schedules/{scheduleId}/domains
```

Request body

BulkDomainsDetails

Response body

BulkDomains

Usage cases

Device registration and switching to DHCP

1. Add customer (POST /customers)
2. Register CUJO (agent) to new customer (POST /agents/register)
3. Change CUJO mode from STANDBY to DHCP (PUT /agents/:id/mode)
4. Switch off dhcp server in router (Comcast API)
5. Reboot CUJO using (POST /agents/:id/reboot)
6. Check CUJO mode (GET /agents/:id)

Curl example

```
Please note you will need to put authorization token in every call  -H 'Authorization: Bearer
token'.

<API BASU URL> - the API full url.

https://sapi.cujo.io/v1 - for the stage

https://api.cujo.io/v1 - for the production
```

```
// Add customer
curl -X POST -d '{"email": "demo@example.com", "phoneCountry": "+1", \
 "phone": "23456789", "partnerUserId": "12345"}' \
 -H 'Content-Type: application/json' -H 'Authorization: Bearer...'
 <API BASU URL>/customers

// Register CUJO. POST /agents/register
curl -X POST -d '{"gatewayMacAddress": "00:00:00:00:00:00", \
 "gatewayPublicIp": "1.1.1.1", "customerId": 287796}' \
 -H 'Content-Type: application/json' \
 -H 'Authorization: Bearer...'
<API BASU URL>/agents/register



// Change mode to DHCP. PUT /agents/:id/mode
curl -X PUT -d '{"mode": "dhcp"}' \
   -H 'Content-Type: application/json' \
   -H 'Authorization: Bearer... '
<API BASU URL>/agents/1/mode

// Reboot CUJO. POST /agents/:id/reboot
curl -X POST -d '{"delayTime": 300}' \
   -H 'Content-Type: application/json' \
   -H 'Authorization: Bearer...'
<API BASU URL>/agents/1/reboot




// Check status. GET /agents/:id
curl -H 'Authorization: Bearer...' <API BASU URL>//agents/1
```

Bash example

In example bellow required to replace the data in <> with your data received from Cujo.

<cliendID> - the Client ID received
<clientSecret> - the Client Secret received

<API BASU URL> - the API full url.

```
https://sapi.cujo.io/v1 - for the stage
```

```
https://api.cujo.io/v1 - for the production
```

```bash
token=$(curl -s -X POST -F 'grant_type=client_credentials' \
-F 'client_id=<cliendID>' -F 'client_secret=<clientSecret>'\
<API BASU URL>/oauth/token | jq -r .access_token)
echo "Logged into CUJO Cloud. Got token: $token"$'\n'

json="Content-Type: application/json"

auth="Authorization: Bearer $token"


read -p "Add customer [y/N]?" -n 1 -r

if [[ $REPLY =~ ^[Yy]$ ]]

then

  companyUserId=$RANDOM

  echo $'\n'"Adding customer ($companyUserId)"

  body='{"phoneCountry": "+1", "phone": "12345", \
    "partnerUserId": "'$companyUserId'"}'

  customerId=$(curl -s -X POST -d "$body" -H "$auth" -H "$json" \
    <API BASU URL>/customers | jq -r .id)

  echo "Customer id: $customerId"$'\n'

else

  customerId=288535

fi


read -p "Register agent [y/N]?" -n 1 -r

if [[ $REPLY =~ ^[Yy]$ ]]

then

 gatewayMac=$(arp -n | grep `route -n | awk '/UG/{print $2}'` | awk
'{print $3}')

 gatewayPublicIp=$(wget http://ipinfo.io/ip -qO -)

 body='{"gatewayMacAddress": "'$gatewayMac'", \
   "gatewayPublicIp": "'$gatewayPublicIp'", \
```

```
  "customerId": '$customerId'}'

 response=$(curl -s -X POST -d "$body" -H "$auth" -H "$json" \
   <API BASU URL>/agents/register)

 agentId=$(echo $response | jq -r .id)

 error=$(echo $response | jq -r .error)

 echo $'\n'"Registered agent id: $agentId error: $error"

else

 agentId=1619519

fi


read -p $'\n'"Do you want to switch to DHCP mode [y/N]?" -n 1 -r

if [[ $REPLY =~ ^[Yy]$ ]]

then

  curl -X PUT -d '{"mode": "dhcp"}' -H "$json" -H "$auth" \
    <API BASU URL>/agents/$agentId/mode

  curl -X POST -d '{"delayTime": 10}' -H "$json" -H "$auth" \
```

```
        <API BASU URL>/agents/$agentId/reboot

    fi
```

Device registration and switching to GATEWAY mode

1. Add customer (POST /customers)
2. Register CUJO (agent) to new customer (POST /agents/register)
3. Change CUJO network configuration (PUT /agents/:id/network)
4. Change CUJO mode from STANDBY to GATEWAY (PUT /agents/:id/mode)
5. Reboot CUJO using (POST /agents/:id/reboot)
6. Check CUJO mode (GET /agents/:id)