RST Threat Feed REST API

Overview

Version information

Version : 1.0.0

URI scheme

Host : api.rstcloud.net
BasePath : /v1
Schemes : HTTPS

Security

api_key

Type : apiKey
Name : x-api-key
In : HEADER

Paths

an API enedpoint to test if authentication is successful or not

```
GET /auth/check
```

Description

If http status code 200 is returned, then authentication is successulf. If an error is returnm then auth key needs to be replaced.

Responses

HTTP Code	Description	Schema
200	200 response	CorrectAPIKey
503	503 access denied	RST503

Consumes

- `application/json`

Produces

- `application/json`

Tags

- Connectivity

Security

Type	Name
apiKey	**api_key**

Get a daily database snapshot of Domain Feed

```
GET /domain
```

Description

Fetch a daily database snapshot of Domain Feed in CSV or JSON formats comressed in gzip for a certain date (latest or any custom date)

Parameters

Type	Name	Description	Schema	Default
Header	**Accept** *optional*	use the following header: Accept:*/*	string	
Query	**date** *optional*	could be either a date in format %Y%m%d or a keyword 'latest' that forces to get the latest file available	string	`"latest"`
Query	**type** *optional*		enum (json, csv)	`"json"`

Responses

HTTP Code	Description	Schema
302	302 response will redirect to a presigned URL to download the gzip file **Headers** : `Location` (string) : a URL to download the gzip file.	emptyFile
400	400 response	RST400
500	500 response	RST500
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Get the latest timestamp for Domain Feed

```
HEAD /domain
```

Description

Get the latest timestamp for Domain Feed file availabe to be downloaded

Parameters

Type	Name	Schema
Header	**Accept** *required*	string
Query	**type** *required*	string

Responses

HTTP Code	Description	Schema
200	200 response **Headers** : `Last-Modified` (string) `Content-Length` (string) `Timestamp` (string) `Content-Type` (string)	emptyFile
400	400 response	RSTERROR
500	500 response	No Content
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Get a daily database snapshot of Hash Feed

```
GET /hash
```

Description

Fetch a daily database snapshot of Hash Feed in CSV or JSON formats comressed in gzip for a certain date (latest or any custom date)

Parameters

Type	Name	Description	Schema	Default
Header	**Accept** *optional*	use the following header: Accept:*/*	string	
Query	**date** *optional*	could be either a date in format %Y%m%d or a keyword 'latest' that forces to get the latest file available	string	`"latest"`

Type	Name	Description	Schema	Default
Query	**type** *optional*		enum (json, csv)	`"json"`

Responses

HTTP Code	Description	Schema
302	302 response will redirect to a presigned URL to download the gzip file **Headers** : `Location` (string) : a URL to download the gzip file.	emptyFile
400	400 response	RST400
500	500 response	RST500
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Get the latest timestamp for Hash Feed

```
HEAD /hash
```

Description

Get the latest timestamp for Hash Feed file availabe to be downloaded

Parameters

Type	Name	Schema
Header	**Accept** *required*	string

Type	Name	Schema
Query	**type** *required*	string

Responses

HTTP Code	Description	Schema
200	200 response **Headers** : `Last-Modified` (string) `Content-Length` (string) `Timestamp` (string) `Content-Type` (string)	emptyFile
400	400 response	RSTERROR
500	500 response	No Content
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Submit an indicator

```
POST /ioc
```

Description

Submit an indicator to request to include it into the RST Threat Feed

Responses

HTTP Code	Description	Schema
200	200 response	RSTIOCSubmit
400	400 response	RSTIOC400
500	500 response	RSTIOCSubmit500
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed API

Security

Type	Name
apiKey	**api_key**

Search for an indicator

```
GET /ioc
```

Description

Look up an indicator (IP, Domain, URL, MD5, SHA1, SHA256) in RST Cloud

Parameters

Type	Name	Schema
Query	**value** *required*	string

Responses

HTTP Code	Description	Schema
200	200 response: the output always includes: ioc_value, ioc_type, collect, fseen, lseen, description, id, title, score, tags, threat fields. Other fields are populated depending on the type of IoCs requested. Some fields may be present with empty values.	RSTThreatData

HTTP Code	Description	Schema
400	400 response	RSTIOC400
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed API

Security

Type	Name
apiKey	**api_key**

Submit a False Posistive indicator

```
PUT /ioc
```

Description

Submit a value that looks like a False Positive indicator to request to exlude it from RST Threat Feed

Responses

HTTP Code	Description	Schema
200	200 response	RSTIOCSubmit
400	400 response	RSTIOC400
500	500 response	RSTIOCSubmit500
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed API

Security

Type	Name
apiKey	**api_key**

Get a daily database snapshot of IP Feed

```
GET /ip
```

Description

Fetch a daily database snapshot of IP Feed in CSV or JSON formats comressed in gzip for a certain date (latest or any custom date)

Parameters

Type	Name	Description	Schema	Default
Header	**Accept** *optional*	use the following header: Accept:*/*	string	
Query	**date** *optional*	could be either a date in format %Y%m%d or a keyword 'latest' that forces to get the latest file available	string	`"latest"`
Query	**type** *optional*		enum (json, csv)	`"json"`

Responses

HTTP Code	Description	Schema
302	302 response will redirect to a presigned URL to download the gzip file **Headers** : `Location` (string) : a URL to download the gzip file.	emptyFile
400	400 response	RST400
500	500 response	RST500
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Get the latest timestamp for IP Feed

```
HEAD /ip
```

Description

Get the latest timestamp for IP Feed file availabe to be downloaded

Parameters

Type	Name	Schema
Header	**Accept** *required*	string
Query	**type** *required*	string

Responses

HTTP Code	Description	Schema
200	200 response **Headers** : `Last-Modified` (string) `Content-Length` (string) `Timestamp` (string) `Content-Type` (string)	emptyFile
400	400 response	RSTERROR
500	500 response	No Content
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Get a daily database snapshot of URL Feed

```
GET /url
```

Description

Fetch a daily database snapshot of URL Feed in CSV or JSON formats comressed in gzip for a certain date (latest or any custom date)

Parameters

Type	Name	Description	Schema	Default
Header	**Accept** *optional*	use the following header: Accept:*/*	string	
Query	**date** *optional*	could be either a date in format %Y%m%d or a keyword 'latest' that forces to get the latest file available	string	`"latest"`
Query	**type** *optional*		enum (json, csv)	`"json"`

Responses

HTTP Code	Description	Schema
302	302 response will redirect to a presigned URL to download the gzip file **Headers** : `Location` (string) : a URL to download the gzip file.	emptyFile
400	400 response	RST400
500	500 response	RST500
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Get the latest timestamp for URL Feed

```
HEAD /url
```

Description

Get the latest timestamp for URL Feed file availabe to be downloaded

Parameters

Type	Name	Schema
Header	**Accept** *required*	string
Query	**type** *required*	string

Responses

HTTP Code	Description	Schema
200	200 response **Headers** : `Last-Modified` (string) `Content-Length` (string) `Timestamp` (string) `Content-Type` (string)	emptyFile
400	400 response	RSTERROR
500	500 response	No Content
503	503 access denied	RST503

Produces

- `application/json`

Tags

- RST Threat Feed Daily DB Snapshot

Security

Type	Name
apiKey	**api_key**

Get WHOIS information for a given domain name

```
GET /whois/{domain}
```

Description

Get actual WHOIS information for a given domain name (cached up to 24 hours)

Parameters

Type	Name	Schema
Path	**domain** *required*	string

Responses

HTTP Code	Description	Schema
200	200 response	RSTWhoisData
400	400 response	RSTWHOIS400
503	503 access denied	RST503

Tags

- RST Whois API

Security

Type	Name
apiKey	**api_key**

Example HTTP response

Response 400

```
"Bad Request"
```

Definitions

CorrectAPIKey

Name	Schema
check *optional*	check

check

Name	Description	Schema
name *optional*	**Example** : `"CheckApiKey"`	string
status *optional*	**Example** : `"valid"`	string

RST400

Name	Description	Schema
error *optional*	**Example** : `"Bad Request"`	string

RST500

Name	Description	Schema
error *optional*	**Example** : `"Unexpected Server Exception"`	string

RST503

Name	Description	Schema
message *optional*	**Example** : `"Forbidden"`	string

RSTERROR

Name	Schema
message *optional*	string

RSTIOC400

Name	Description	Schema
ioc_value *optional*	**Example** : `"domain.local"`	string
status *optional*	**Example** : `"Bad Request"`	string

RSTIOCSubmit

Name	Description	Schema
ioc_value *optional*	**Example** : `"domain.local"`	string
status *optional*	**Example** : `"submitted"`	string

RSTIOCSubmit500

Name	Description	Schema
ioc_value *optional*	**Example** : `"domain.local"`	string
status *optional*	**Example** : `"Server Error"`	string

RSTThreatData

Name	Description	Schema
collect *optional*		integer
description *optional*		string
fseen *optional*		integer

Name	Description	Schema
id *optional*	**Example** : `"UUID"`	string
ioc_type *optional*	**Example** : `"domain"`	string
ioc_value *optional*	**Example** : `"domain.local"`	string
lseen *optional*		integer
tags *optional*	**Example** : `[ "malware", "phishing" ]`	object
threat *optional*	**Example** : `[ "emotet" ]`	object
title *optional*	**Example** : `"RST Threat feed. IOC: domain.local"`	string

RSTWHOIS400

Type : string

RSTWhoisData

Name	Description	Schema
age *optional*	**Example** : `365`	integer
created_on *optional*	**Example** : `"2022-01-01 00:00:00"`	string
expires_on *optional*	**Example** : `"2023-01-01 00:00:00"`	string
nameservers *optional*	**Example** : `"ns1.domain.com,ns2.domain.com"`	string
registered? *optional*	**Example** : `"true"`	string
registrant *optional*	**Example** : `"Registrant Name"`	string
registrar *optional*	**Example** : `"Registrar Name"`	string
status *optional*	**Example** : `"registered"`	string

Name	Description	Schema
updated_on *optional*	**Example** : `"2022-01-01 00:00:00"`	string

an empty response

Type : object