

INFOWATCH

InfoWatch Traffic Monitor SDK. Uploading DB unloadings

13/07/2018

© JSC “InfoWatch”

Tel/Fax +7 (495) 229-00-22

http://www.infowatch.com

Table of Contents

1 Purpose of REST API programming interface 4

2 General description of REST API programming interface 5

2.1 Creating a sample unloading 5

2.2 Updating a sample unloading 5

2.3 Adding contents to a sample unloading 5

2.4 Getting state of a sample unloading 5

2.5 Initiating deployment of new contents of uploaded sample documents to analysis modules 5

2.6 Getting interface version that is supported by Traffic Monitor 6

3 Sample unloading format 7

4 Registering external component 8

4.1 Registration file format of external component 8

5 Configuring REST API programming interface 10

6 Typical usage scenarios 11

6.1 Typical scenario of creating a sample unloading 11

6.2 Typical scenario of updating a sample unloading 12

6.3 Typical scenario of adding data to the unloading 12

6.4 Implementation of completion of loading a sample unloading 13

7 Functional description of REST API programming interface 14

7.1 Common headings for GET/POST requests 14

7.2 Working with configuration 14

7.2.1 Distribution of REST API configuration 14

7.3 Working with sample unloadings 14

7.3.1 Creating the unloading 15

7.3.2 Updating data of the unloading 16

7.3.3 Adding data for the unloading 17

7.3.4 Getting state of the unloading 17

7.3.5 Getting current version 18

7.4 Common errors 20

7.4.1 Successful response 20

7.4.2 Data/version validation error 20

7.4.2.1 Error format in case of incorrect version of API (JSON Scheme) 20
7.4.2.2 Response format in case of request validation error (JSON Scheme) 21
7.4.2.3 Example of error when incorrect version is specified 23
7.4.2.4 Example of error when checking uniqueness of a sample unloading name 23
7.4.3 Authorization is required 24
7.4.4 Insufficient permissions 24
7.4.5 Entity is not found 24
7.4.6 Request body is too large 24
7.4.7 Number of server requests is exceeded 24
7.4.8 System error 25
7.4.9 Server is temporarily unavailable 26

1 Purpose of REST API programming interface

This programming interface is designed to integrate third-party components with InfoWatch Traffic Monitor (Traffic Monitor). Third-party components can generate documents which represent "Database sample unloadings" and pass them to Traffic Monitor using the provided interface. After that, the passed unloadings will be detected in data streams that are analyzed by Traffic Monitor. Rules for detection of unloadings are set in Traffic Monitor console. A third-party component can only upload and update contents of the uploading. The third-party component must be registered in the system according to the procedure that is described in "Registering REST API external component".

2 General description of REST API programming interface

The programming interface is a REST API, that is a sequence of requests to a web server. The programming interface provides the following features:

- Creating a sample unloading
- Updating a sample unloading
- Adding contents to a sample unloading
- Getting state of a sample unloading
- Initiating deployment of new contents of uploaded sample documents to analysis modules
- Getting interface version that is supported by Traffic Monitor

2.1 Creating a sample unloading

```
FingerPrintDsc Create(string name, string[] columns)
```

The function creates a sample unloading with a specified name and a list of column names of the sample unloading. Returns a description of the created sample object (FingerPrint).

2.2 Updating a sample unloading

```
FingerPrintDsc UpdateContent(string FingerPrintId,string[]content)
```

The function allows you to upload contents to an existing sample object (unloading). The sample object is determined by its identifier (FingerPrintDsc field of the structure). Returns a description of the sample object (FingerPrint). Once the contents are uploaded, the process of converting and saving the contents is initiated. This function completely replaces the contents of a sample object.

2.3 Adding contents to a sample unloading

```
FingerPrintDsc AddContent(string FingerPrintId, string[] content)
```

The function allows you to add extra contents to an existing sample object (unloading). The sample object is determined by its identifier (FingerPrintDsc field of the structure). Returns a description of the sample object (FingerPrint). Once the contents are uploaded, the process of converting and saving the contents is initiated. This function completely replaces the contents of a sample object.

2.4 Getting state of a sample unloading

```
FingerPrintDsc GetInfo(string FingerPrintId)
```

The function allows you to get information about an existing sample unloading. Returns a description of the sample object (FingerPrint). An important result of calling this function is a field with a status of the sample unloading.

2.5 Initiating deployment of new contents of uploaded sample documents to analysis modules

```
Void Ditribute()
```

The function initiates the procedure of deploying new contents of sample unloadings to modules of analysis. The function is synchronous. Once the function is executed, Traffic Monitor is ready to detect new contents in data streams it analyzes.

2.6 Getting interface version that is supported by Traffic Monitor

```
VersionInfo GetInterfaceVersion()
```

The function allows you to get information about the interface supported by Traffic Monitor.

Each part of the unloading, which is uploaded to Traffic Monitor, passes stages of conversion to an internal format and saving to a database. After that, an external component initiates passing the new unloading to Traffic Monitor systems of analysis. Thus, a sufficiently large unloading can be uploaded in parts. That is, it takes several requests to upload the unloading and then a single command is used to deploy it to systems of analysis.

Each step of processing the uploaded sample unloading takes some time. At each step, an error may occur.

The programming interface allows you to track the steps of processing a sample unloading and respond to errors that may occur during processing.

3 Sample unloading format

A sample unloading is a sequence of rows in UTF-8 encoding. The rows should be separated by CRLF or LF characters. Cell values in the row should be separated by TAB or ‘,’ (comma) characters. Actually, it follows TSV (Tab separated values) CSV (Comma separated values) format. The number of cells in all rows must be the same. When you create an unloading, the number of cells must be specified.It is equal to the number of column names, which are passed to the *Create* function. It is only possible to upload contents to an existing sample unloading if the number of cells is equal to the number specified during the unloading creation. If a different number of cells is specified it will make the unloading invalid.

4 Registering external component

To integrate an external interception module with Traffic Monitor system, perform the following steps:

1. Register the identifier string of the component vendor with InfoWatch company. This will link the vendor company with a license that will be installed in Traffic Monitor system;
2. Get a developer license linked with the company identifier. This will enable loading sample unloadings from this vendor to Traffic Monitor. The developer license allows you to load any sample unloadings;
3. Create a file for registering the external component. The file format is described below. By this moment, data source names for the sample unloading that will be generated by the external component must be already defined. The license obtained at step 2 is added to the registration file;
4. Load the registration file of the external component to Traffic Monitor system via Traffic Monitor console interface. For details, see the "Plugins" section in "Traffic Monitor. Administration Guide";
5. In the properties of the loaded external component, get an access token.

Now the System is ready to receive generated sample unloadings from the specified vendor company with the specified source of the sample unloading.

4.1 Registration file format of external component

The plugin is an archive in a ZIP format. The archive includes:

- **licenses** folder that contains license files;
- **icon** folder that contains files with pictograms for registered events (optionally);
- **manifest.json** file with information about the plugin.

For external source systems, **manifest.json** file should contain the following information:

Name	Is required	Description
Version	Yes	Plugin version
Vendor identifier	Yes	Matches the company name in the license
Name	Yes	Plugin name
Description	No	Plugin description
"Preset" attribute	No	Whether plugin is included in the System
Data source name for the sample unloading	Yes	Row selected by the plugin vendor for identifying the source of the sample unloading
Unique identifier	Yes	Unique 128 bit identifier (UUID) of plugin

Important!

The file contains an expired license. To use the sample file for registration of a plugin, you need to obtain a new license.

A full JSON scheme is a part of SDK samples (see "Description of PushAPI SDK samples"). A sample file of the module registration is included in the SDK.

5 Configuring REST API programming interface

The following parameters participate in configuring the programming interface:

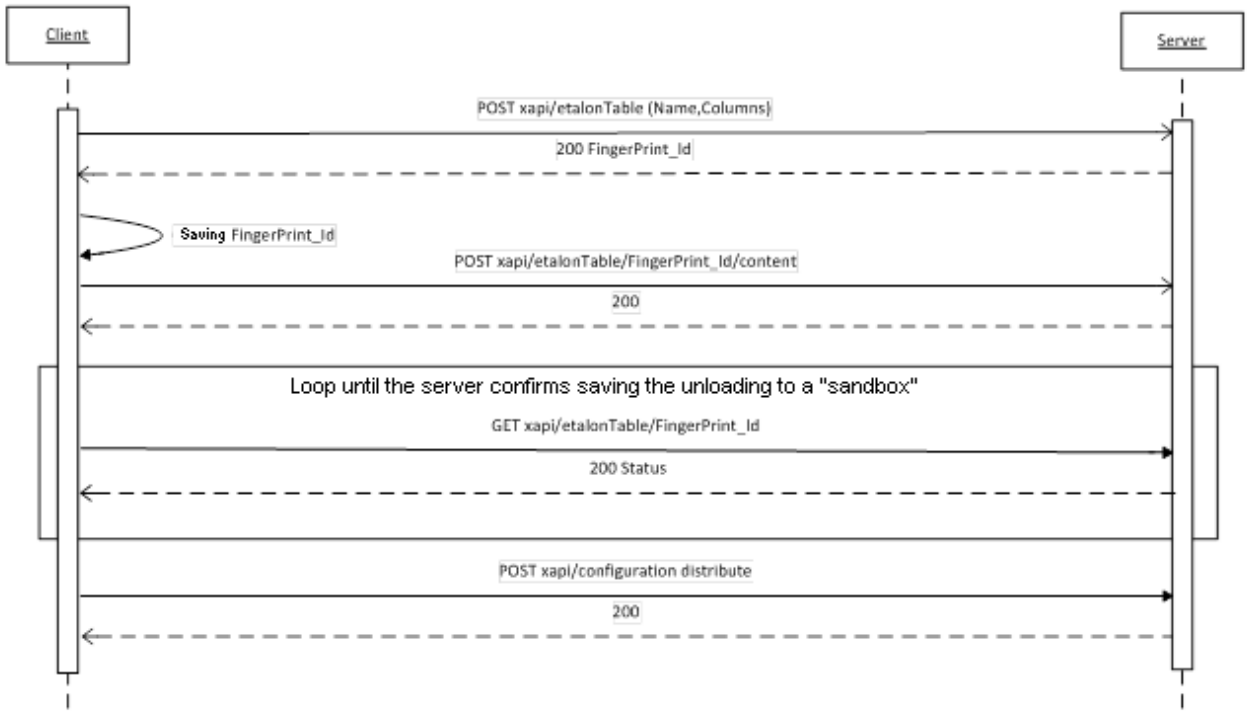
- Address for connection to the SDK service (network address, port);
- "Authorization" token. A string of characters, which allows you to authorize components that use the SDK. This string can be obtained in the control panel by external automated systems in Traffic Monitor management console;
- Identifier of transmitted data. A string received by a vendor of the external component from InfoWatch. This string describes the type of transmitted data and is used in the licensing policy;
- Identifier of a vendor of the external component. A string received by a vendor of the external component from InfoWatch. This string describes the vendor and is used in the licensing policy.

6 Typical usage scenarios

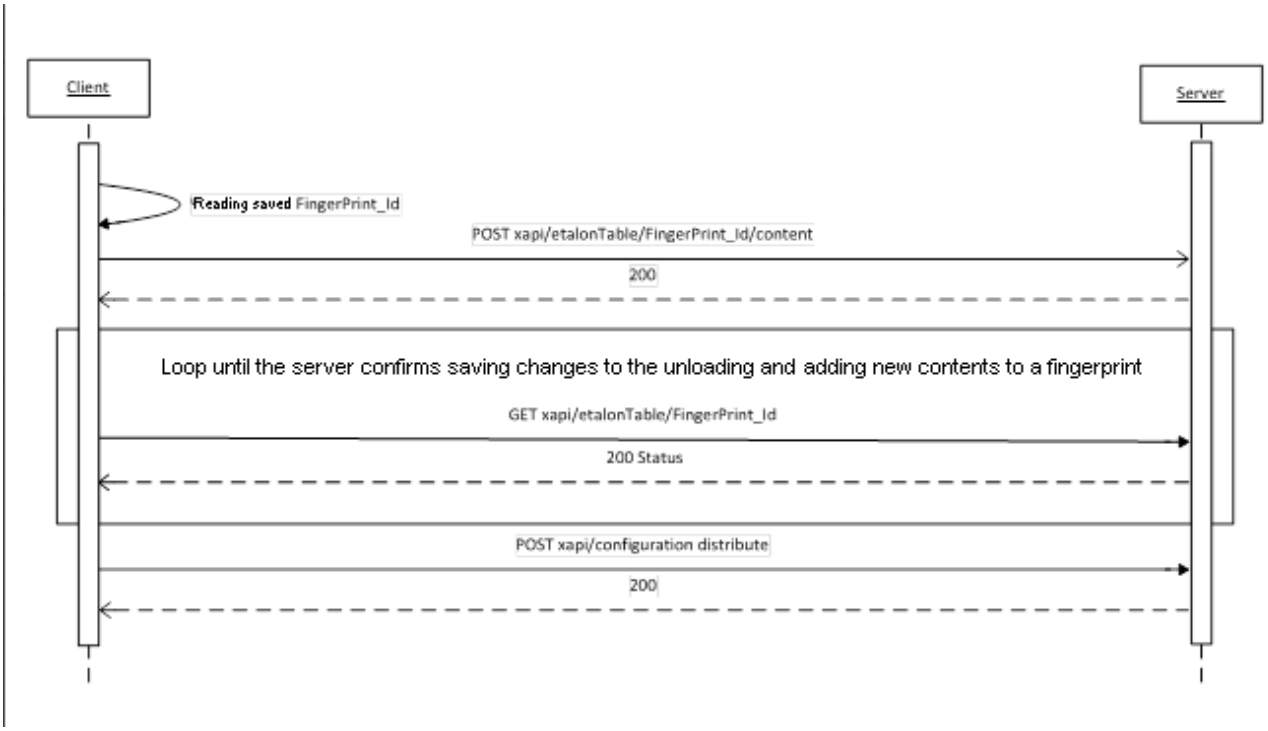
Below you can find sequence diagrams which represent typical scenarios of using REST API:

- Typical scenario of creating a sample unloading
- Typical scenario of updating a sample unloading
- Typical scenario of adding data to the unloading
- Implementation of completion of loading a sample unloading

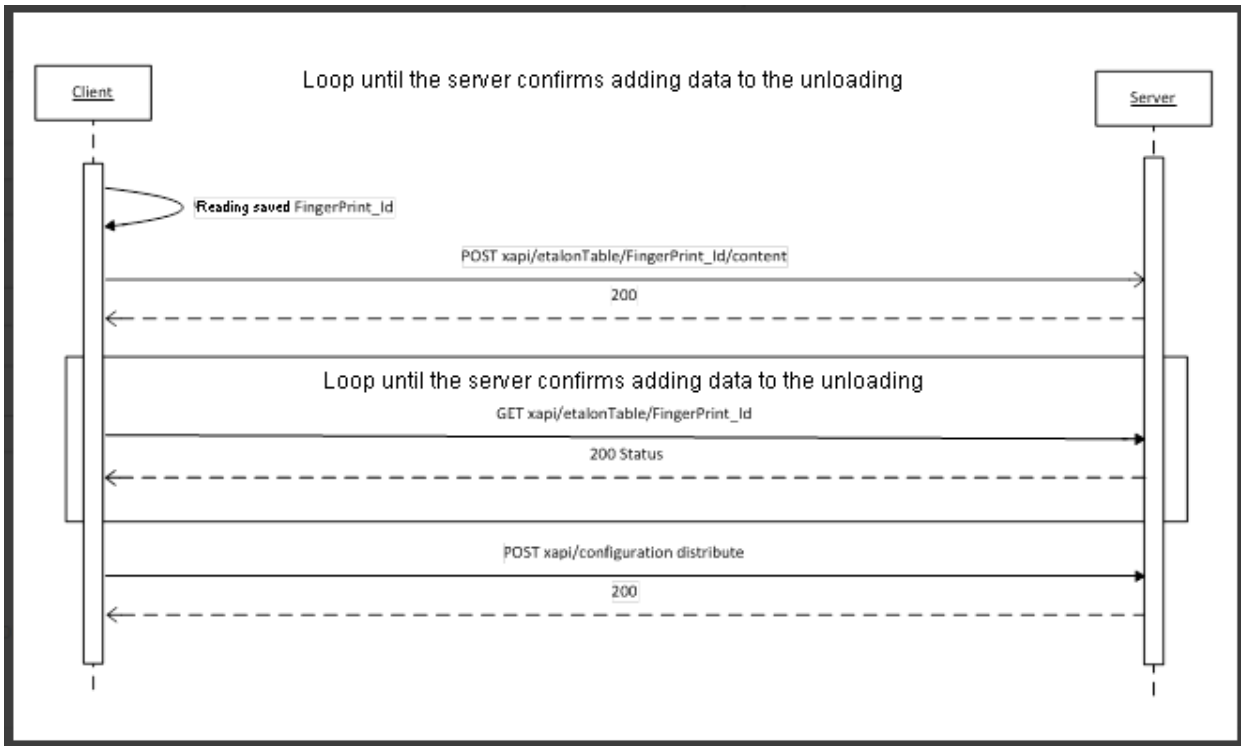
6.1 Typical scenario of creating a sample unloading



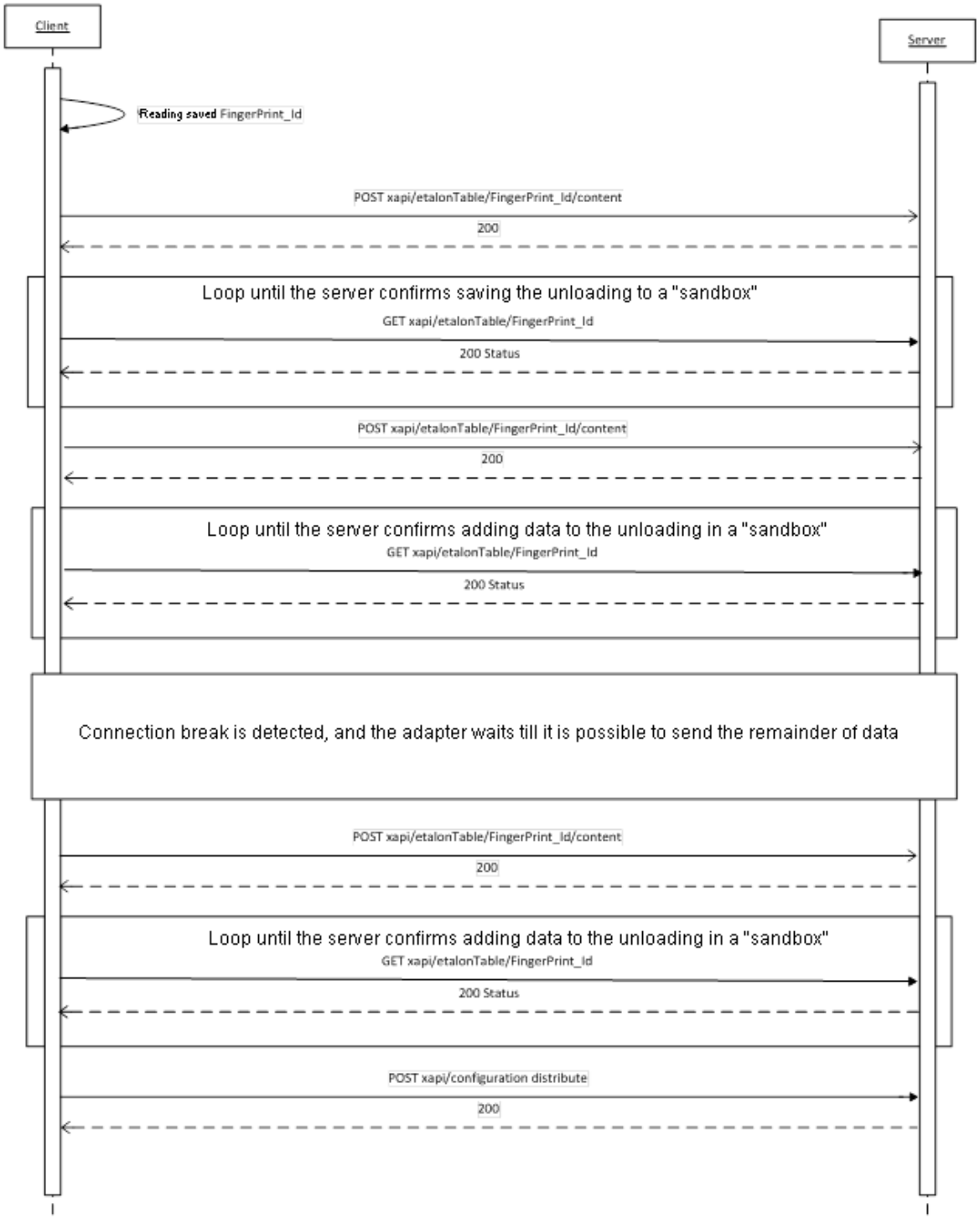
6.2 Typical scenario of updating a sample unloading



6.3 Typical scenario of adding data to the unloading



6.4 Implementation of completion of loading a sample unloading



7 Functional description of REST API programming interface

The programming interface is a REST API, that is a sequence of GET/POST requests to a specific resource of a web server and responses to them. The request and response formats are described below. Data protection during the transfer is carried out through the SSL/TLS protocol without the client's authorization. Transferring unencrypted data is not supported. For data transfer, a UTF-8 encoding is used.

7.1 Common headings for GET/POST requests

Each request to the server must contain the following obligatory headings:

- X-API-Auth-Token – the authorization token is specified;
- X-API-DataType – an identifier of the transferred data type is specified;
- X-API-CompanyId – an identifier of the vendor is specified;
- X-API-Version – a version of the programming interface is specified. For now, we use number 1.

7.2 Working with configuration

After the content of the sample unloading has been sent to the SDK and successfully compiled, you can initiate distribution of the modified configuration to the analysis systems.

7.2.1 Distribution of REST API configuration

Description: the method is required to distribute configuration to analysis subsystems.

Method features: POST, synchronous.

Resource: xapi/configuration.

JSON Scheme request body:

```
{
    "STATUS": "distribute"
}
```

In case of success – the return code is "200" and the response body is as follows:

```
{
    "STATUS": "distributed"
}
```

In case of an error – the return code is "500". Possible values of the `code` field:

- error – cannot apply the configuration.

7.3 Working with sample unloadings

The chapter contains the following information:

- Creating the unloading
- Updating data of the unloading
- Adding data for the unloading
- Getting state of the unloading
- Getting current version

7.3.1 Creating the unloading

Description: the method is required to add a new unloading without filling it with data. The data will be added with a separate method.

Method features: POST, synchronous.

Resource: xapi/etalonTable.

JSON Scheme request body:

```
{
    "properties": {
        "DISPLAY_NAME": {
            "description": "Name of unloading",
            "type": "string",
            "errors": ["required", "not_match", "not_unique_field"]
        },
        "CONDITION_COLUMNS": {
            "description": "a string, an encoded JSON array with column names, e.g. [\"first_column\", \"second_column\"]",
            "type": "string",
            "errors": ["required", "not_valid_json"]
        },
        "NOTE": {
            "description": "Arbitrary description of the unloading",
            "type": "string"
        }
    },
    "required": [
        "DISPLAY_NAME",
        "CONDITION_COLUMNS"
    ]
}
```

In case of success – the return code is "200" and the response body is as follows:

```
{
    "FINGERPRINT_ID":    "string",
    "TYPE":              "string",
    "SOURCE":            "string",
    "DISPLAY_NAME":      "string",
    "NOTE":              "string",
    "CONDITION_COLUMNS": "string",
```

```
    "CREATE_DATE":      "string",
    "CHANGE_DATE":      "string",
    "STATUS":           "string"
}
```

> **Important!**
>
> The number of columns that was specified when creating the unloading cannot be changed. When loading the contents, the number of columns in the rows being loaded should match the value that was specified when creating the sample unloading.

7.3.2 Updating data of the unloading

Description: the method is required to update the unloading contents. All entries of the sample unloading will be deleted, and then, a new entry will be added. This method can be used for the initial filling of the unloading.

> **Important!**
>
> The filling should have an integer number of rows.
> The minimum number of row for filling is 2.
> The minimum number of columns is 2.
> The minimum byte size of loadable content is 128 byte.
> The minimum byte size of loadable content is 2GB.

Methods features: POST, asynchronous.

Resource: xapi/etalonTable/{id}/content/replace.

Parameters:

- id – fingerprint_id of the object being edited.

Example: enatalonTable/0123456789ABCDEF/content/replce

Content-type of the request body should be not `application/json`, but `multipart/form-data` (for more details, see: https://tools.ietf.org/html/rfc2388).

Content-Disposition that will include the file should have the `name` field with CONTENT value and `filename` attribute with the file name and TSV or CSV extension depending on the file format, separated with Tab or commas respectively.

Possible values of errors for the CONTENT field:

- not_valid – the file has an invalid signature;
- not_allowed_file_extension – an unauthorized file extension, for now. only 2 formats are supported: TSV and CSV;
- too_long_size – the file size is too large;
- duplicate – this file already exists in the system.

In case of success – the return code is "200" and the response body is as follows:

```
{
    "FINGERPRINT_ID":    "string",
```

```
    "TYPE":              "string",
    "SOURCE":            "string",
    "DISPLAY_NAME":      "string",
    "NOTE":              "string",
    "CONDITION_COLUMNS": "string",
    "CREATE_DATE":       "string",
    "CHANGE_DATE":       "string",
    "STATUS":            "string"
}
```

After getting the "200" return code, you should take the FINGERPRINT_ID field and use it for the checking the unloading state, until the state changes to "ready".

> **Important!**
>
> The number of cells in loadable rows should match the number of columns that was specified when creating the unloading.
> When you delete the unloading through Traffic Monitor console, it is considered existing until you distribute the configuration, i.e. you can update this unloading and add contents to it.
> When loading "erroneous" content, i.e. the content which duplicates an already loaded unloading (or its part) or the content whose rows contain an incorrect number of cells, the whole sample object gets an invalid status. The external subsystem should stop loading this content and go to the next one. Loading the correct content changes the sample object status to the correct one. Incorrect content never reaches the analysis modules.

7.3.3 Adding data for the unloading

Description: the method is used for adding content to the unloading. All content entries will be saved, and a new entry will be added.

Method features: POST.

Resource: xapi/etalonTable/{id}/content.

For details, see "Updating data of the unloading".

7.3.4 Getting state of the unloading

Description: the method is required to get information about the state of a single unloading.

Method features: GET.

Ресурс: xapi/etalonTable/{id}.

Parameters:

- id – fingerprint_id of the object being edited.

Example: etalonTable/0123456789ABCDEF

Response body:

```
{
```

```
    "FINGERPRINT_ID":    "string",
    "TYPE":              "string",
    "SOURCE":            "string",
    "DISPLAY_NAME":      "string",
    "NOTE":              "string",
    "CONDITION_COLUMNS": "string",
    "CREATE_DATE":       "string",
    "CHANGE_DATE":       "string",
    "STATUS":            "string"
    "content":           [
        {
            "CONTENT_ID":   "string",
            "CHECKSUM":     "string",
            "CONTENT_SIZE": "integer",
            "CONTENT_MIME": "string"
        }
    ]
}
```

The `status` field can have the following values:

- sending – sending data to the compiler;
- sent – data has been sent to the compiler, and compilation has been started;
- compiling – the document is being compiled;
- compiled – the document is ready;
- saving – the document is being saved;
- ready – the document has been saved, it is ready for further changes and does not block applying the configuration;
- fatal_error – an error occurred when saving the document, the operation cannot be repeated or continued;
- duplicate – the content data is duplicated (loading the content can be continued);
- not_match_delimiter – rows in the unloading do not contain delimiters (COMMA or TAB);
- wrong_column_count – the number of columns in the row does not match the number of columns that was specified when creating the unloading;
- error – a temporary error, you can try the operation again in some time (better in an hour);
- max_words - the maximum number of words is exceeded;
- max_columns - the maximum number of columns is exceeded.

7.3.5 Getting current version

Description: the method is required for getting supported versions.

If the return code is "200", you can continue working with the system.

You can use this method to check a license, a version or the authorization. In case of success, the return code is "200". In case of an error, the error code is returned.

Method features: GET.

Resource: xapi/version.

Response body:

```
{
    "data":       [
        {
            "NAME":    "string",
            "STATUS": "supported|deprecated|removed"
        }
    ]
}
```

An example of response if incorrect version is specified:

HTTP/1.1 400 Bad Request

Content-Type: application/json

```
{
    "error": {
        "code": "unsupported_version",
        "meta": {
            "versions": [
                {
                    "NAME":   "1.0.0",
                    "STATUS": "removed"
                },
                {
                    "NAME":   "2.0.0",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "3.0.0",
                    "STATUS": "supported"
                }
            ]
        }
    }
}
```

7.4 Common errors

Description of possible errors:

- not_unique_field – not a unique value;
- unique – a unique value;
- too_short – too short value;
- too_long – too long value;
- wrong_length – the value has incorrect length;
- repeat_exactly – the value does not match the value in a different field;
- required – the field value is required;
- not_exist_in_list – the value is not in the list;
- invalid – invalid value;
- contains_child – the node has child elements;
- contains_items – the category node contains entities;
- parent_own_child – the parent contains child elements;
- parent_self_set_current – the object tries to set itself its parent;
- not_valid_json – invalid JSON;
- invalid_cron_format – incorrect cron format;
- read_only – the object is readonly;
- empty – the value cannot be empty.

7.4.1 Successful response

The return code is "200".

Response format:

```
{
    "data": "mixed",
    "meta": "mixed"
}
```

7.4.2 Data/version validation error

The return code is "400".

Error format in case of incorrect version of API (JSON Scheme)

```
{
    "properties": {
        "error": {
            "description": "Error container",
            "properties":  {
                "code":       {
                    "description": "General description of error",
                    "type":        "string",
```

```
                "value":       "unsupported_version"
            },
            "meta": {
                "description": "Additional information on error",
                "type":        "object",
                "properties":  {
                    "supported_versions": {
                        "description": "Array of supported versions",
                        "type":        "array",
                        "items": {
                            "description": "Supported version",
                            "type": "string"
                        }
                    }
                }
            }
        }
    }
}
```

Response format in case of request validation error (JSON Scheme)

```
{
    "properties": {
        "error": {
            "description": "Error container",
            "properties":  {
                "code":       {
                    "description": "General description of error",
                    "type":        "string",
                    "value":       "validation"
                },
                "meta": {
                    "description": "Additional information on error",
                    "type":        "object",
                    "properties":  {
                        "validation": {
```

```
                        "description": "Names of model fields",
                        "type":        "object",
                        "properties":  {
                            "field":     {
                                "description": "Model field",
                                "type":        "array",
                                "items":       {
                                    "description": "Error",
                                    "type":        "string",
                                    "values": [
                                        "not_unique_field",
                                        "too_short",
                                        "too_long",
                                        "wrong_length",
                                        "repeat_exactly",
                                        "required",
                                        "not_exist_in_list",
                                        "invalid",
                                        "contains_child",
                                        "contains_items",
                                        "parent_own_child",
                                        "unique",
                                        "not_valid_json",
                                        "invalid_cron_format",
                                        "read_only",
                                        "parent_self_set_current",
                                        "empty"
                                    ]
                                }
                            },
                            "sub_model": {
                                "description": "Name of nested model",
                                "type":        "object",
                                "$ref":       "#/properties/error/properties/meta/
properties/validation"
                            }
                        }
```

```
                        }
                    }
                }
            }
        }
    }
}
```

Example of error when incorrect version is specified

```
{
    "error": {
        "code": "unsupported_version",
        "meta": {
            "supported_versions": ["2", "3"]
        }
    }
}
```

Example of error when checking uniqueness of a sample unloading name

```
{
    "error": {
        "code": "validation",
        "meta": {
            "validation":    {
                "DISPLAY_NAME": ["unique"]
            },
            "unique_models": [
                {
                    "FINGERPRINT_ID": "0123456789ABCDEF",
                    "DISPLAY_NAME":   "test"
                }
            ]
        }
    }
}
```

7.4.3 Authorization is required

The return code is "401".

Description: is returned in all requests which require authorization.

Response body: no.

7.4.4 Insufficient permissions

The return code is "403".

Description: is returned for all requests if the current user does not have sufficient permissions to perform a given operation.

Response body: no.

7.4.5 Entity is not found

The return code is "404".

Description: is returned if a particular model is not found in the system. For example, a sample unloading is not found.

Response body: no.

7.4.6 Request body is too large

The return code is "413".

Description: is returned if a too large request is transferred.

Response body: no.

7.4.7 Number of server requests is exceeded

The return code is "429".

Description: is returned if too many requests have been sent to the server over a certain period. May include Retry-After heading which specifies in how much time you can repeat the request.

Response body (JSON Scheme):

```
{
    "properties": {
        "error": {
            "description": "Error container",
            "properties":  {
                "code": {
                    "description": "General description of error",
                    "type":        "string",
                    "value":       "too_many_requests "
```

```
                },
                "meta": {
                    "description": "Additional information on error",
                    "type":        "object",
                    "properties":  {
                        "time": {
                            "description": "HTTP date or an integer in seconds, are which
you can repeat the request",
                            "type":        "string"
                        }
                    }
                }
            }
        }
    }
}
```

7.4.8 System error

The return code is "500".

Description: is returned if a logical error has occurred in the system, and the request execution cannot be continued.

Response body (JSON Scheme):

```
{
    "properties": {
        "error": {
            "description": "Error container",
            "properties":  {
                "code": {
                    "description": "General description of error",
                    "type":        "string"
                },
                "meta": {
                    "description": "Additional information on error",
                    "type":        "object"
                }
            }
        }
    }
```

```
}
```

7.4.9 Server is temporarily unavailable

The return code is "503".

Description: informs that currently is not possible to execute requests and the server is down for maintenance. The Retry-After heading contains estimated time of completion of maintenance (the heading value can be either HTTP-date or an integer in seconds).

Response body (JSON Scheme):

```
{
    "properties": {
        "error": {
            "description": "Error container",
            "properties":  {
                "code": {
                    "description": "General description of error",
                    "type":        "string",
                    "value":       "maintains"
                },
                "meta": {
                    "description": "Additional information on error",
                    "type":        "object",
                    "properties":  {
                        "time": {
                            "description": "HTTP-date or integer in seconds after which
you can repeat the request",
                            "type":        "string"
                        }
                    }
                }
            }
        }
    }
}
```