Fudo Enterprise 5.4 - API documentation

Fudo Security

20.03.2024

Contents

CHAPTER 1

About documentation

Documentation Structure

This API documentation consists of:

- *API overview* section providing an overview of key concepts that clarify important topics, such as API purpose, nomenclature, request format, methods, possible responses, endpoints and objects specification, parameters and attribute's properties.
- Sections describing endpoints related to individual objects and Fudo Enterprise functionalities.

Conventions and symbols

This documentation is written using the following conventions:

- *italic* - this formatting is used to mark user interface elements.
- `example` - this formatting is used to write example value of a parameter, API method name or code example.
- Note field:

Note: Note field usually contains additional information closely related with described topic, e.g. suggestion concerning given procedure step; additional conditions which have to be met.

- Warning field:

Warning: Warning field usually contains essential information concerning system's operation. Not adhering to this information may have irreversible consequences.

Disclaimer

CHAPTER 2

API overview

The purpose of Fudo Enterprise Application Programming Interface (API) is to provide users and administrators with the ability to speed up and automate time-consuming tasks related to remote access management. This API can be used to retrieve data about objects, manage large numbers of objects or integrate Fudo Enterprise with external systems.

Note: Please note that there are two versions of the Fudo Enterprise API, and use of each of them depend on the actual objects that need to be operated on:

- **APIv1** handles system authentication and operations on Password Changers and Password Changer Policies.
- **APIv2** handles system authentication and operations on all the other objects.

APIv1 is being systematically replaced with APIv2 and ultimately only APIv2 will remain in use.

2.1 API purpose

Fudo API provides a wide range of functionality for administrators, including:

- Retrieving data from and about Fudo objects, like users, servers, accounts, safes, listeners, etc.
- Searching and filtering objects.
- Adding, editing and deleting large numbers of objects and their attributes.
- Automatization of time-consuming admin tasks related to managing objects.
- Integration with external systems.

2.2 API nomenclature

For a better understanding of our API, please refer to the terminology we have adopted:

- **object** - the main elements of the API, on which endpoints operate. For example, user, account, listener, server, etc.
- **attribute** - a feature of the object. For example, the attributes of the object `account` include `id`, `name`, `description`, etc.
- **property** - an attribute property in the object specification. For example, the attribute `name` properties of the `account` object are: `type`, `required`, `ignore_case` and `unique`.

Pattern example:

```
"object": {
        "attribute": {
            "property0": "value",
            "property1": "value",
            "property2": "value",
            "property3": "value",
        },
}
```

Partial code example:

```
"account": {
          "id": {
              "type": "string",
              "readonly": true,
              "grant": "account",
              "unique": true
          },
          "name": {
              "type": "string",
              "required": true,
              "ignore-case": true,
              "unique": true
          },
          "description": {
              "type": "string"
          }
}
```

2.3 Request format

Please note that the query path differs depending on the API endpoints version you are using.

Note: **APIv1** request format:

<method> http://<fudo_address>/api/system/<endpoint>[?<params>] <body>

APIv2 request format:

<method> http://<fudo_address>/api/v2/<endpoint>[?<params>] <body>

Where:

- <method> - is HTTP method (GET, POST, PATCH or DELETE only allowed),
- <fudo address> - is Fudo Enterprise IP address (e.g., `10.0.0.0`),
- <endpoint> - is chosen endpoint (e.g., `/objspec/user`),
- <params> - is URL parameters available for a specific method (e.g., `filter`, `offset`, `limit`),
- <body> - is request body in JSON format.

An example of the request that returns a list of available users (with no parameters specified and no body needed):

```
GET https://10.0.0.0/api/v2/user
```

An example of the request that creates user with *user* role and *test-user* name:

```
POST https://10.0.0.0/api/v2/user
```

```
{
  "role": "user",
  "name": "test-user"
}
```

2.4 Methods

Please find below list of allowed methods while using this API.

`GET`	For reading data of an existing object. No request body is allowed.
`POST`	For creating an object. Requires a request body, specified in JSON format, that contains the values for properties of the object that is about to be created. The exception is `/session/<session_id>/backup/<backup_id>` endpoint, which does not require a body.
`PATCH`	For modifying an existing object. Requires a request body, specified in JSON format, that contains the values for properties of the object.
`DELETE`	For removing an existing object. No request body is allowed.

2.5 Possible responses

Please find below list of possible responses to API queries.

Code	Status	Description
200	success	`OK`
201	success	`CREATED`
400	failure	`BAD REQUEST`; message examples: • `Unrecognized endpoint` • `Request body is not allowed for this endpoint`
401	failure	`UNAUTHORIZED`; message example: • `Unauthorized request` • `Missing session key` • `Missing %s header` • `Referer mismatch` • `Unable to find the user` • `User is blocked`
403	failure	`FORBIDDEN`; message example: `Permission denied`
404	failure	`NOT FOUND`; message example: `Object not found`
500	failure	`INTERNAL SERVER ERROR`; message example: `Database error`
503	failure	`SERVICE UNAVAILABLE`; message example: `Fudo is unhealthy`

2.6 Endpoints and objects specification

To better understand Fudo Enterprise API functionality, we can group endpoints according to object types defined in Fudo Enterprise data model.

Object type	Endpoints example
user	• /user • /user/<id> • /user/safe/time_policy • /user/safe • ...
server	• /server • /server/<id> • ...

Continued on next page

Table 1 – continued from previous page

Object type	Endpoints example
account	• /account • /account/<id> • /account/safe/listener • ...
safe	• /safe • /safe/<id> • /grant/safe • ...
listener	• /listener • /listener/<id> • /grant/listener • ...

We can also distinguish additional types of endpoint groups corresponding to the objects listed below:

- pool
- external_authentication
- session
- remote_app

...and also groups of functional methods, like:

- objspec
- grant
- batch
- network

Let's take a closer look at the last four types in the following paragraphs.

Objspec

The `objspec` type, used only with the `GET` method, enables administrators to retrieve specifications of objects on which endpoints operate, e.g.:

- `/objspec/user` request will return attributes of *user* object type,
- `/objspec/remote_app` request will return attributes of *remote_app* object type.

Below you can find an example of information returned for `GET https://10.0.0.0/api/v2/objspec/remote_app` request.

```
{
    "result": "success",
```

(continues on next page)

(continued from previous page)

```
    "remote_app": {
        "id": {
            "type": "string",
            "readonly": true,
            "unique": true
        },
        "name": {
            "type": "string",
            "required": true,
            "ignore_case": true,
            "unique": true
        },
        "path": {
            "type": "string",
            "required": true
        },
        "arguments": {
            "type": "string"
        },
        "created_at": {
            "type": "string",
            "readonly": true
        },
        "modified_at": {
            "type": "string",
            "readonly": true
        },
        "removed": {
            "type": "boolean",
            "readonly": true
        }
    }
}
```

As you can see on the above example, `remote_app` possess following attributes: `id`, `name`, `path`, `arguments`, `created_at`, `modified_at` and `removed`.

Batch

Fudo API's `batch` powerfull functionality enables administrators to send batch requests, allowing them to perform nested operations with different methods. Please refere to section *API v2: Batch requests*.

Grant

This group, used with the `GET`, `POST` and `DELETE` methods, allows granting management privileges for users to selected accounts, pools, other users, listeners, safes, or servers.

Network

The *Network* functionality allows to retrieve network settings such as DNS address(es), Admin Panel's address, Access Gateway's address, global configuration parameters, network interfaces configuration or routing configuration. It is used only with the `GET` method. To learn more, please refer to *API v2: Network* section.

2.7 Parameters

You can add a query string just after the endpoint, preceded by a question mark. This provides a string of information that will specify special parameters for your query. In this chapter, you will find a description of the **URL parameters** available for specific methods to be included within a path.

Fields

This parameter is used to specify only desired object fields in the query. `Null` values are skipped, unless explicitly requested.

If query has no `fields` parameter specified:

- `GET` method will return all attributes of an object except those set to `Null`,
- `POST` method will show only `id` fields,
- `PATCH` method will not return any fields.

When using `fields` parameter with no value (`fields=`):

- `GET` method will return `id` field only,
- `POST` and `PATCH` will not return any fields.

Duplicated fields are ignored, e.g., `fields=id,name,name,protocol` will be treated like `fields=id,name,protocol`.

The example below utilizes the `fields` and `filter` parameters to narrow down the result to servers that include the string `test` in the `name` field, returning only the `id`, `name` and `protocol` fields in the response:

```
GET https://10.0.0.0/api/v2/server?fields=id,name,protocol&filter=name.match(test)
```

Filter

Note: Please note that certain filters are applied automatically depending on the user's role.

This parameter narrows out the result with available additions:

- `.in()` - include possible attribute values,
- `.iin()` - case insensitive version of `.in()`,
- `.contains()` - include possible fields containing specified values, only applies to arrays (e.g., `account?filter=server_ids.contains(345)`),

---

Note:

- When using `.in()`, `.iin()`, and `.contains()`, we can input multiple values with a comma as a separator (e.g., `server?filter=protocol.in(ssh,rdp,vnc)`, `account?filter=server_ids.contains(1,2,3)`). In this situation, at least one of the given conditions must be met.
- We can also use multiple conditions separated with comma (e.g., `server?filter=server_ids.contains(1),server_ids.contains(2)`). In such cases, all given conditions must be met. This rule applies to all parameters.

- `.match()` - include a regular expression to be searched in field values,
- `.imatch()` - case insensitive version of `.match()`,
- `.eq()` - equal (`name.eq(foo)`),
- `.ieq()` - case insensitive version of `.eq()`,
- `.ne()` - not equal,
- `.ine()` - case insensitive version of `.ne()`,
- `.lt()` - less than,
- `.le()` - less or equal,
- `.gt()` - greater than,
- `.ge()` - greater than or equal,
- `<attribute>` - filter objects based on attributes of type `boolean` set to `true`,
- `!<attribute>` - filter objects based on attributes of type `boolean` set to `false`,

Note: The example filter `filter=protocol.eq(ssh),!legacy_crypto,tls_enabled` filters out objects with the `protocol` equal to `ssh`, boolean type attribute `legacy_crypto` set to `false` and boolean type attribute `tls_enabled` set to `true`.

- `.isnull()` - filter objects with empty values in specified fields (e.g., `description.isnull()`),
- `.isempty()` - filter objects with empty values in specified fields, only applies to arrays.

Note: Every filter can be negated with <!>. For instance, the query `filter=!protocol.eq(ssh)` will skip all objects with the protocol attribute set to `ssh`. This example is equivalent of `protocol.ne(ssh)`.

Note: While using `DELETE` method:

- negation <!> cannot be used,
- for safety reasons, at least one unique filter value must be used in the query (e.g., `id`, `name`),

- if an object does not have a unique attribute, uniqueness is determined based on a set of attributes (e.g., `filter=account_id.eq(123456),safe_id.eq(345567),listener_id.eq(789012)`).

Search in "all" attributes

The special attribute `all.` enables searching for a specified value in all attributes of type `number` and `string`.

Note: Only `.match()` and `.imatch()` methods can be used on this special attribute.

The example below searches for the string `rdp` in all eligible attributes of the `server` objects. As a result, it will return all servers that have the string `rdp` included in fields such as `name`, `protocol`, `description`, or `reason`.

```
GET https://10.0.0.0/api/v2/server?filter=all.imatch(rdp)
```

Order

This parameter specifies the order of returned data.

Note: You can reverse the order with an exclamation mark <!>.

Example below will return all servers `id`, `name` and `protocol` fields, sorted first by `protocol`, and next by reverse `id` order:

Example request

```
GET https://10.0.0.0/api/v2/server?fields=id,name,protocol&order=protocol,!id
```

Response


```
{
    "result": "success",
    "server": [
        {
            "id": "9187343239835811 88",
            "name": "RDP_server_2",
            "protocol": "rdp"
        },
        {
            "id": "9187343239835811 87",
            "name": "RDP_server",
            "protocol": "rdp"
        },
        {
            "id": "9187343239835811 86",
            "name": "windows.example.org",
            "protocol": "rdp"
        },
        {
            "id": "9187343239835811 89",
            "name": "SSH_server",
```


(continues on next page)

(continued from previous page)

```
            "protocol": "ssh"
        },
        {
            "id": "9187343239835811185",
            "name": "linux.example.org",
            "protocol": "ssh"
        }
    ]
}
```

Offset

This parameter is used to exclude from a response the first N items of a resource collection. Example below skips first 5 objects on the query response:

```
GET https://10.0.0.0/api/v2/user?offset=5
```

For predictable results, use this parameter in conjunction with `order` parameter.

Limit

This query parameter specifies the number of instances that a single response contains. Example below limits the list of returned objects to 10 (by ID order):

```
GET https://10.0.0.0/api/v2/user?fields=id,name&order=id&filter=role.eq(user)&limit=10
```

Note:

- If the limit is not specified in a query, the API will automatically return 1000 records by default.
- Setting the limit value above 1000 results in a Bad Request error.

Debug

This parameter is used to diagnose a query. Example below returns query with debugging data:

```
GET https://10.0.0.0/api/v2/server?fields=id,name,protocol&order=protocol,!id&debug
```

```
{
    "result": "success",
    "server": [
        {
            "id": "9187343239835811188",
            "name": "RDP_server_2",
            "protocol": "rdp"
        },
        {
            "id": "9187343239835811187",
            "name": "RDP_server",
            "protocol": "rdp"
        },
        {
            "id": "9187343239835811186",
```

(continues on next page)

(continued from previous page)


```
            "name": "windows.example.org",
            "protocol": "rdp"
        },
        {
            "id": "918734323983581189",
            "name": "SSH_server",
            "protocol": "ssh"
        },
        {
            "id": "918734323983581185",
            "name": "linux.example.org",
            "protocol": "ssh"
        }
    ],
    "debug": {
        "timings": {
            "total start": null,
            "receive start": null,
            "receive duration": "0.000142s",
            "endpoint_verify start": null,
            "endpoint_verify duration": "0.000003s",
            "endpoint_execute start": null,
            "database_request (SELECT) start": null,
            "database_request (SELECT) duration": "0.001976s",
            "endpoint_execute duration": "0.002087s",
            "total duration": "0.008025s"
        }
    }
}
```


Total_count

This parameter returns the total number of objects, taking into account the filters applied in the query, but at the same time ignoring `limit` and `offset` parameters. In the case of large amounts of objects it can be expensive to use.

Estimated_total_count

This parameter can be inaccurate, so it is useful just to estimate quantities. It is much less expensive to use than `total_count`, includes deleted and hidden objects, ignores `filter` parameters and is only available for *superadmin* role.

Reveal

This parameter enables to view objects with the following states:

- `active`,
- `removed`,
- `visible`,
- `hidden`,
- `all`.

By default `reveal` is set to `active` and `visible` states (`?reveal=active,visible`). If we do not specify it as `active` or `removed` (e.g., `?reveal=visible`) it will return only `active` objects.

The same situation occurs in the case of `visible` and `hidden` pair of parameters. If we do not specify `reveal` as `visible` or `hidden`, it will by default take the `visible` value and return only `visible` objects.

2.8 Attribute's properties

We can distinguish the following features of attributes used in object specification:

Table 2: `Attribute's properties`

Property	Possible values	Default value	Description
type	• `boolean` • `number` • `string` • `number-array` • `string-array`	`string`	Attribute's type in JSON requests.
readonly	• `true` • `false`	`false`	When set to `true`, it cannot be set during POST or modified during PATCH.
immutable	• `true` • `false`	`false`	When set to `true`, it can be set only during POST, but cannot be modified during PATCH.
ignore-case	• `true` • `false`	`false`	When set to `true`, `apid` will ignore letters case when filtering by this attribute.
allow-empty	• `true` • `false`	`false`	When set to `true`, this string attribute can be set to an empty string.
default	`<value>`	No default	Attribute's default value.
protected	• `true` • `false`	`false`	The attribute's value is a secret and shouldn't be returned to the caller.
grant	`<objtype>`	No default	Require grant on `<objtype>` and use this attribute as an ID for the `<objtype>` object.
required	• `true` • `false`	`false`	When set to `true`, the attribute is always required.

Continued on next page

Table 2 – continued from previous page

Property	Possible values	Default value	Description
required-by	`{ <attribute>: <value>, ... }`	No default	• List of attributes and their values that require this attribute. • If the value is an empty object then this attribute is required whenever the given attribute exists. • Multiple `''required-by''` properties can be specified.
requires	`{ <attribute>: <value>, ... }`	No default	• List of attributes and their values required by this attribute. • If the value is an empty object then the given attribute is required, but value doesn't matter. • Multiple `''requires''` properties can be specified. If that is the case then at least one of them has to be met.
values	• `<value>` or: • `[ <value>, ... ]`	No default	Value or an array of possible values for this attribute.
value-labels	`[ <label>, ... ]`	No default	User-friendly names for all the values, used in graphical user interfaces.
value-range	`[ <minval>, <maxval> ]`	No default	Value range for a numeric attribute.
value-regexp	`<regular expression>`	No default	Regular expression that the value has to match.
unique	• `true` • `false` or: • `<attribute>` or: • `[ <attribute>, ... ]`	`false`	The given attribute is unique by itself (when `true`) or is unique when combined with other attributes.

Continued on next page

Table 2 – continued from previous page

Property	Possible values	Default value	Description
expensive	• `true` • `false`	`false`	The given attribute is expensive to retrieve because it requires an additional operations in the database or a subquery.
description	`string`	No default	Short description of the attribute.

2.8.1 Selected use examples

Required-by

Description:

In the following example, the attribute is required when `protocol` is set to either `ssh` or `rdp`.

Example:

```
"required-by": { "protocol": [ "ssh", "rdp" ] }
```

Description:

Example below shows that when `"external_port"` is defined, this attribute is required.

Example:

```
"required-by": { "external_port": { } }
```

Description:

Multiple `"required-by"` properties can be specified. Two equivalent examples below shows that this attribute is required either:

- when `protocol` is `"ssh"` or
- when `protocol` is `http` or `rdp` and `tls_enabled` is `true`.

Example:

```
"required-by": { "protocol": "ssh" },
"required-by": { "protocol": [ "http", "rdp" ], "tls_enabled": true }
```

Equivalent example:

```
"required-by": { "protocol": "ssh" },
"required-by": { "protocol": "http", "tls_enabled": true },
"required-by": { "protocol": "rdp", "tls_enabled": true }
```

Requires

Description:

Following example shows that this attribute requires `protocol` to be set to `ssh` or `rdp`.

Example:

```
"requires": { "protocol": [ "ssh", "rdp" ] }
```

Description:

Following example shows that `"external_port"` is required to exist, but its value is not important.

Example:

```
"requires": { "external_port": { } }
```

Description:

Following example shows that this attribute requires `protocol` to be set to `rdp` and `"tls_enabled"` to be set to `true`.

Example:

```
"requires": { "protocol": "rdp", "tls_enabled": true }
```

Unique

Description:

Example of unique attribute with no dependencies.

Example:

```
"id": {"unique": true}
```

Description:

Example of unique attribute with single dependency - a pair of those attributes is unique.

Example:

```
"safe_id": {
        "unique": "user_id"
},
"user_id": {
        "unique": "safe_id"
}
```

Description:

Example of unique attribute with double dependency - three attributes together are unique.

Example:

```
"account_id": {
        "unique": [ "listener_id", "safe_id" ]
},
"listener_id": {
        "unique": [ "account_id", "safe_id" ]
},
"safe_id": {
        "unique": [ "account_id", "listener_id" ]
}
```

CHAPTER 3

API v1: Authentication

Deprecated since version 5.4

- Please be informed that the endpoints outlined within this section have been deprecated and are scheduled for removal in the next major release.
- It is recommended to switch to the APIv2 *API Key* authentication method as soon as possible.

Accessing Fudo Enterprise data structures over API interface requires a *user* object defined in the local database. The same access rights restrictions apply to the API interface as in case of administration panel access.

Role	Access rights
user	• Connecting to servers through assigned safes. • Loggin to the User Portal (requires adding the user to the `portal` safe). • Fetching servers' passwords (requires additional access right).
service	• Accessing SNMP information.

Continued on next page

Table 1 – continued from previous page

Role	Access rights
operator	• Logging in to the administration panel. • Browsing objects: servers, users, safes, accounts, to which the user has been assigned sufficient access permisions. • Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions. • Generating reports on demand and subscribing to periodic reports. • Managing email notifications. • Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. • Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart.
admin	• Logging in to the administration panel. • Managing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions. • Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions. • Generating reports on demand and subscribing to periodic reports. • Activating/deactivating email notifications. • Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned management privileges. • Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. • Managing policies. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart.

Role	Access rights
superadmin	• Full access rights to objects management. • Full access rights to system configuration options. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart, license, system events log.

Request

Method

```
POST
```

Path

```
/api/system/login
```

Headers

```
Content-Type: Application/JSON
```

Body

```
{
        username: username,
        password: password
}
```

Response

Status

```
200 OK
```

Headers

```
Content-Type: Application/JSON
```

Body

```
{
        sessionid: ygmd2env50zgr2nblypmrfcvarggn0uf
}
```

Response

Status

```
401 UNAUTHORIZED
```

Example request

```
curl -k -X POST -H "Accept:application/json" -H "Content-Type:application/json"
https://fudo.whl/api/system/login -d
{"username": "api_user", "password": "api_password"}

Result: {"sessionid":"oz2jfky042kz7d3zc2gos1ahxouxehk3"}
```

After successful authentication, include the key `Authorization` with the received value of the“sessionsid“ into the Headers of the future requests.

CHAPTER 4

API v1: Password changers

Deprecated since version 5.4

Please be informed that the endpoints outlined within this section have been deprecated and are scheduled for removal in the next major release.

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); password changing policy as well as the password changer itself.

4.1 Data structures

Table 1: `PasswordChangerModel`

Attribute	Type	Description
id	string	Object identifier. Read only.
name	string	Required.
timeout	int	Script's execution time limit expressed in seconds. Required.
transport	string{LDAP, SSH, Telnet, WinRM, plugin}	Transport layer specifier. Required.
changer_type	string{change,verify}	Script type. Required.
variables	VariablesModel	Required.
commands	CommandsModel	Required.

Table 2: `VariablesModel`

Attribute	Type	Description
id	string	Object identifier.
name	string	Required.
description	string	
encrypt	bool	• `true` - encrypt variable value, • `false` - store variable value in plain text.
required	bool	• `true` - specifying this value is required, • `false` - specyfing this value is not required.
object_type	string	
object_property	string	

Table 3: `CommandsModel`

Attribute	Type	Description
id	string	Object identifier. Read only.
command	string	Required if command_type==INPUT.
expected	string	Required if command_type==EXPECTED
delay	int	Delay after running the command before executing the next one. Required if command_type==DELAY
comment	string	Optional commentary.
position	int	required

Table 4: `account_password_changer`

Attribute	Type	Description
id	string	Object identifier.
position	int	Password changer position in execution queue.
account	string	Account identifier.
password_changer	string	Password changer identifier
timeout	int	Script's execution time limit.
accountvariable_set		

Table 5: `accountvariable_set`

Attribute	Type	Description
id	string	Object identifier.
password_changer_variable	string	
value	string	Variable value.
account_id	string	Account identifier.
server_id	string	Server identifier.
account_password_changer_id	string	
server_address_id	string	

4.2 Creating a password changer

Request

Method

```
POST
```

Path

```
/api/system/password_changers
```

Headers

```
Content-Type: Application/JSON
```

Body

```
PasswordChangerModel
```

Possible Response

Status

```
201 CREATED
```

Headers

```
Content-Type: Application/JSON
```

Body

```
PasswordChangerModel
```

Description

```
Object successfully created. Resultant object's attributes
are included in response body.
```

Possible Response

Status	400 BAD REQUEST
Headers	Content-Type: Application/JSON
Body	ValidationErrors
Description	Validation didn't pass.

Example: Creating a WinRM password changer

```
    { "name": "test_changer_00567",
"timeout": 300,
"transport": "WinRM",
"changer_type": "change",
"variables": [
    {
        "id": "7394910588142354434",
        "name": "transport_bind_ip",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "bind_ip"
    },
    {
        "id": "7394910588142354435",
        "name": "transport_ca_certificate",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "transport_ca_certificate"
    },
    {
        "id": "7394910588142354436",
        "name": "transport_encoding",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": null,
        "object_property": null
    },
    {
        "id": "7394910588142354437",
        "name": "transport_host",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
```

(continues on next page)

(continued from previous page)


```
        "object_property": "address"
    },
    {
        "id": "7394910588142354438",
        "name": "transport_login",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_account",
        "object_property": "login"
    },
    {
        "id": "7394910588142354439",
        "name": "transport_port",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "port"
    },
    {
        "id": "7394910588142354440",
        "name": "transport_secret",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_account",
        "object_property": "secret"
    },
    {
        "id": "7394910588142354441",
        "name": "x",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": null,
        "object_property": null
    }
],
"commands": [
    {
        "id": "7394910588142354434",
        "command": "echo %%x%%",
        "expected": null,
        "delay": null,
        "comment": null,
        "position": 0
    }]}
```


4.3 Retrieving password changers list

Request

Method	`GET`
Path	`/api/system/password_changers`

Note: Results pagination

Every `GET` request, which returns a collection of objects can be optionally paginated. To achieve it add a pagination parameter to the request path:

```
/api/system/objects?page=3&page_size=10
```

Table 6: Pagination parameters

page	int
page_size	int

Possible Response

Status	`200 OK`
Headers	`Content-Type: Application/JSON`

Body	`[`
	`PasswordChangerModel,`
	`...`
	`]`

Example

```
curl -k -X GET
"https://10.0.150.150/api/system/password_changers?sessionid={{sessionid}}"
```

Response

```
[{
"id": "1",
"name": "Unix/SSH changer",
"timeout": 300,
"transport": "SSH",
"changer_type": "change",
"variables": [
    {
        "id": "1",
        "name": "transport_host",
```

(continues on next page)

(continued from previous page)


```
        "description": null,
        "encrypt": false,
        "required": true,
        "object_type": "fudo_server",
        "object_property": "address"
    },
    {
        "id": "2",
        "name": "transport_bind_ip",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "bind_ip"
    },
    {
        "id": "3",
        "name": "transport_port",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": "fudo_server",
        "object_property": "port"
    },
    {
        "id": "4",
        "name": "transport_login",
        "description": null,
        "encrypt": false,
        "required": true,
        "object_type": "fudo_account",
        "object_property": "login"
    },
    {
        "id": "5",
        "name": "transport_secret",
        "description": null,
        "encrypt": true,
        "required": true,
        "object_type": "fudo_account",
        "object_property": "secret"
    },
    {
        "id": "6",
        "name": "transport_method",
        "description": null,
        "encrypt": false,
        "required": true,
        "object_type": "fudo_account",
        "object_property": "method"
    },
    {
        "id": "7",
        "name": "transport_host_public_key",
        "description": null,
        "encrypt": false,
```


(continues on next page)

(continued from previous page)


```
        "required": false,
        "object_type": "fudo_server",
        "object_property": "ssh_public_key"
    },
    {
        "id": "8",
        "name": "transport_password_prompt",
        "description": null,
        "encrypt": false,
        "required": false,
        "object_type": null,
        "object_property": null
    },
    {
        "id": "9",
        "name": "account_login",
        "description": "Login for the account for which password will be changed.",
        "encrypt": false,
        "required": true,
        "object_type": "fudo_account",
        "object_property": "login"
    }
],
"commands": [
    {
        "id": "1",
        "command": null,
        "expected": "Last login:",
        "delay": null,
        "comment": null,
        "position": 1
    },
    {
        "id": "2",
        "command": "passwd %%account_login%%",
        "expected": null,
        "delay": null,
        "comment": null,
        "position": 2
    },
    {
        "id": "3",
        "command": null,
        "expected": "[Pp]assword:",
        "delay": null,
        "comment": null,
        "position": 3
    },
    {
        "id": "4",
        "command": "%%account_new_secret%%",
        "expected": null,
        "delay": null,
        "comment": null,
        "position": 4
    },
```


(continues on next page)

(continued from previous page)


```
    {
        "id": "5",
        "command": null,
        "expected": "[Pp]assword:",
        "delay": null,
        "comment": null,
        "position": 5
    },
    {
        "id": "6",
        "command": "%%account_new_secret%%",
        "expected": null,
        "delay": null,
        "comment": null,
        "position": 6
    },
    {
        "id": "7",
        "command": null,
        "expected": "successfully",
        "delay": null,
        "comment": null,
        "position": 7
    },
    {
        "id": "8",
        "command": "logout",
        "expected": null,
        "delay": null,
        "comment": null,
        "position": 8
    },
    {
        "id": "9",
        "command": null,
        "expected": "closed",
        "delay": null,
        "comment": null,
        "position": 9
    }]}]
```


4.4 Retrieving a password changer

Request

Method	
	`GET`

Path	
	`/api/system/password_changers/id`

Possible Response

Status
200 OK
Headers
Content-Type: Application/JSON
Body
PasswordChangerModel

Possible Response

Status
404 NOT FOUND
Not found.

Example

```
curl -k -X GET "https://10.0.150.150/api/system/password_changers/1?sessionid={
↪{sessionid}}"
```

Response

```
curl -k -X POST -H "Content-Type:application/json"
https://10.0.150.150/api/system/password_changers/68719476747?sessionid={{sessionid}}␣
↪-d
{
"id": "986756453423132"
"name":"New name",
"timeout":300,
"transport":"Telnet",
"changer_type":"verify",
"variables":
        [{
        "name":"transport_host",
        "description":null,
        "encrypt":false,
        "required":true,
        "object_type":"fudo_server_address_property",
        "object_property":"host"
        },{
        "name":"transport_port",
        "description":null,
        "encrypt":false,
        "required":false,
        "object_type":"fudo_server_address_property",
        "object_property":"port"
        },{
        "name":"transport_bind_ip",
        "description":null,
```

(continues on next page)

(continued from previous page)

```
        "encrypt":false,
        "required":false,
        "object_type":"fudo_server_address_property",
        "object_property":"bind_ip"
        }],
"commands":
        [{
        "command":"command 1 %%transport_bind_ip%%",
        "expected": null,
        "position": 1,
        "delay":null,
        "command_type":"INPUT"
        },{
        "command":"command 2 %%transport_port%%",
        "expected": null,
        "position": 2,
        "delay":null,
        "command_type":"INPUT"
        },{
        "command":"command 3 %%transport_host%%",
        "expected":null,
        "position": 3,
        "delay":null,
        "command_type":"INPUT"
        }]}
```

4.5 Modifying password changers

Request

Method	`PUT`
Path	`/api/system/password_changers/id`

Possible Response

Status	`200 OK`
Headers	`Content-Type: Application/JSON`
Body	`PasswordChangerModel`

Possible Response

Status	400 BAD REQUEST
Headers	Content-Type: Application/JSON
Body	PasswordChangerModel

Possible Response

Status	404 NOT FOUND
Description	Object not found.

4.6 Deleting a password changer

Request

Method	DELETE
Path	/api/system/password_changers/id

Possible Response

Status	204 NO CONTENT

Possible Response

Status	404 NOT FOUND
Description	Object not found.

Example:

```
curl -k -X DELETE
https://10.0.150.150/api/system/password_changers/687194776746?sessionid={{sessionid}}
```

4.7 Retrieving account-password changers assignments list

Request

Method	`GET`
Path	`/api/system/account_password_changers`

Note: Results pagination

Every `GET` request, which returns a collection of objects can be optionally paginated. To achieve it add a pagination parameter to the request path:

```
/api/system/objects?page=3&page_size=10
```

Table 7: Pagination parameters

page	int
page_size	int

Possible Response

Status	`200 OK`
Headers	`Content-Type: Application/JSON`

Body	`[`
	`  AccountSafeAssignmentModel,`
	`  ...`
	`]`

Example:

```
curl -k -X GET
"https://10.0.150.150/api/system/account_password_changers?sessionid={{sessionid}}"
```

4.8 Adding a password changer to account

Request

Method	POST
Path	/api/system/account_password_changers
Body	account_password_changer

Possible Response

Status	201 CREATED
Headers	Content-Type: Application/JSON
Body	AccountPasswordChanger

Possible Response

Status	400 BAD REQUEST
Headers	Content-Type: Application/JSON
Body	ValidationErrors

Possible Response

Status	404 NOT FOUND

Example:

```
curl -k -X POST
https://10.0.8.89/api/system/account_password_changers?sessionid={{sessionid}} -d
{
  "account": 1992864825347,
  "accountvariable_set": [
        {
```

(continues on next page)

(continued from previous page)


```
        "account_id": 1992864825347,
        "password_changer_variable": 109,
        "server_address_id": null,
        "server_id": null,
        "value": null
      },
      {
        "account_id": 1992864825347,
        "password_changer_variable": 110,
        "server_address_id": null,
        "server_id": null,
        "value": null
      },
      {
        "account_id": null,
        "password_changer_variable": 102,
        "server_address_id": null,
        "server_id": 1992864825347,
        "value": null
      },
      {
        "account_id": 1992864825347,
        "password_changer_variable": 103,
        "server_address_id": null,
        "server_id": null,
        "value": null
      },
      {
        "account_id": null,
        "password_changer_variable": 101,
        "server_address_id": 1992864825351,
        "server_id": null,
        "value": null
      },
      {
        "account_id": 1992864825347,
        "password_changer_variable": 106,
        "server_address_id": null,
        "server_id": null,
        "value": null
      },
      {
        "account_id": null,
        "password_changer_variable": 107,
        "server_address_id": null,
        "server_id": 1992864825347,
        "value": null
      },
      {
        "account_id": 1992864825347,
        "password_changer_variable": 104,
        "server_address_id": null,
        "server_id": null,
        "value": null
      },
      {
```


(continues on next page)

(continued from previous page)


```
            "account_id": null,
            "password_changer_variable": 105,
            "server_address_id": null,
            "server_id": null,
            "value": "base1"
        }
  ],
  "password_changer": 13,
  "position": 0,
  "timeout": 300
}
```


4.9 Deleting an account-password changer assignment

Request

Method	DELETE
Path	/api/system/account_password_changers/id

Possible Response

Status	204 NO CONTENT

Possible Response

Status	404 NOT FOUND

Example:

```
curl -k -X DELETE
https://10.0.150.150/api/system/account_password_changers/687194776738?sessionid={
↪{sessionid}}
```

CHAPTER 5

API v1: Password changer policy

Deprecated since version 5.4

Please be informed that the endpoints outlined within this section have been deprecated and are scheduled for removal in the next major release.

Password changer policy defines specifics of how frequently the password should be changed and password complexity requirements.

Password changer policy can't be created via API, but can be assigned to a particular Account.

5.1 Adding a password changer policy to account

Request

Method	`POST`
Path	`/api/system/accounts`
Body	`AccountModel`

Possible Response

Status	
	200 OK

Headers	
	Content-Type: Application/JSON

Body	
	AccountModel

Possible Response

Status	
	400 BAD REQUEST

Headers	
	Content-Type: Application/JSON

Body	
	ValidationErrors

Possible Response

Status	
	404 NOT FOUND

Example:

```
    curl -k -X PUT -H "Accept:application/json" -H "Content-Type:application/json"
    https://fudo.whl/api/system/accounts/755918023667220708?sessionid={{sessionid}} -
↪d
    {
"credentials": {
    "login":"",
    "method": "password",
    "password_change_policy_id": "75594322023667220482"
},
"server_id": "755918764677220677",
"password_change_request": "0001-01-01T00:00:00",
"type": "regular",
"name": "TestAccount" }
```

CHAPTER 6

API v2: Authentication

To access Fudo Enterprise data structures via the API interface, you need a *user* object defined in the local database with the *API Key* authentication method specified. To obtain the *API Key*, please follow below steps in the Fudo Enterprise Admin Panel:

- Create new *user* or edit existing *admin* user definition.
- Specify the *API Key* authentication method for this *user*.
- Generate the *API Key* value, copy it, and archive it for future API requests.

Note: The API Key cannot be retrieved after saving this authentication method.

For more detailed information, please refer to the *Users* section of the Fudo Enterprise Documentation.

6.1 How To Authenticate Using an API Key

For successful authentication, include the key `Authorization` with the generated *API Key* value in the *Headers* of your API requests.

Example request

```
curl -k -X GET -H
↪"Authorization:KEDVOgernOHGpiOmAksvegNDFVWihUy9vknnqCoYDU6X5fiaOmvLU9237LuEjFsc"␣
↪https://10.0.0.0/api/v2/user
```

6.2 Access Rights Restrictions

The same access rights restrictions apply to the API interface as in case of Administration Panel access. Outlined in the table below are the access rights specified for each of the roles available

in Fudo Enterprise.

Role	Access rights
user	• Connecting to servers through assigned safes. • Loggin to the User Portal (requires adding the user to the `portal` safe). • Fetching servers' passwords (requires additional access right).
service	• Accessing SNMP information.
operator	• Logging in to the administration panel. • Browsing objects: servers, users, safes, accounts, to which the user has been assigned sufficient access permisions. • Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions. • Generating reports on demand and subscribing to periodic reports. • Managing email notifications. • Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. • Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart.
admin	• Logging in to the administration panel. • Managing objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions. • Blocking/unblocking objects: servers, users, safes, listeners, accounts, to which the user has been assigned sufficient access permisions. • Generating reports on demand and subscribing to periodic reports. • Activating/deactivating email notifications. • Viewing live and archived sessions involving objects (user, safe, account, server), to which the user has been assigned management privileges. • Converting sessions and downloading converted content involving objects (user, safe, account, server), to which the user has been assigned sufficient access permissions. • Managing policies. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart.

Role	Access rights
superadmin	• Full access rights to objects management. • Full access rights to system configuration options. • Available dashboard widgets: concurrent sessions, suspicious sessions, account alerts, active users, cluster status, concurrent sessions chart, license, system events log.

CHAPTER 7

API v2: Accounts

Account defines the privileged account existing on the monitored server. It specifies the actual login credentials, user authentication mode: anonymous (without user authentication), regular (with login credentials substitution) or forward (with login and password forwarding); password changing policy as well as the password changer itself.

7.1 Data structures

Table 1: `AccountModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
name	string	yes	Unique account's name
description	string	no	Object description
blocked	boolean; default value `false`	yes	
reason	string	if `blocked` == `true`	
type	string {regular, forward, anonymous}	yes	Immutable
hotseat	boolean; default value `false`	if `type` == `regular`	Enable to be informed about existing connections via the Access Gateway. Available for the server with `protocol` == `rdp`
login	string; may be empty	if `type` == `regular`	

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
domain	string	if `type == regular || forward`	
forward_domain	boolean; default value `false`	if `type == forward`	
servauth	boolean; default value `false`	if `type == forward`	Authentication against server
method	string {account, passvn, password, sshkey}	if `type == regular || forward`	Authentication method
account_id	string	if `method == account`	
passvn_id	string	if `method == passvn`	
category	string {nonprivileged, privileged}		
server_id	string	yes	
server_name	string		Read-only; expensive to use
server_address	string		Read-only; expensive to use
server_mask	number		Read-only; expensive to use
server_port	number		Read-only; expensive to use
pool_id	string	yes	
pool_name	string		Read-only; expensive to use
secret	string; may be empty	no	
dump_mode	string {all, none, raw, noraw}; default value `noraw`	yes	Session recording options
retention_locked	boolean; default value `false`	yes	
timestamp_enabled	boolean; default value `false`	yes	
ocr_enabled	boolean; default value `false`	yes	
ocr_lang	string {eng, pol, deu, hun, nor, rus, ukr}; if more than 1, separated by the + symbol	if `ocr_enabled == true`	
ssh_agent	boolean; default value `false`	yes	
retention_remove	number		
retention_external	number		
password_lastupdate	datetime		Read-only

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
password_lastcheck	datetime		Read-only
password_change_policy_id	string	if `type` == `regular`	
password_checkout_time_limit	datetime (h:m:s)	if `password_change_on_checkin` == `true`	
password_change_on_checkin	boolean		If set, password will be changed after last password checkin.
password_change_on_session_end	boolean		If set, password will be changed after session finishes.
password_recovery	boolean		If set and password verification detects unknown password, password changer will try to recover the password to a known value.
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
last_login	datetime		Read-only; expensive to use
safes	object-array		Read-only; expensive to use; JSON object array containing `id`, `name`, and `position` of assigned safes.
servers	object-array		Read-only; expensive to use; JSON object array containing `id`, `mask`, `name`, `port` and `address` of assigned servers.
builtin	boolean		Read-only; expensive to use; if `true`, the object is not editable.
hidden	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.
state	string		Account's discovery state: discovered, onboarded, quarantined or created (for manually created accounts). Read-only. Expensive to use.

Request for retrieving available attributes of the AccountModel

Method	
	`GET`
Path	
	`/api/v2/objspec/account`

Table 2: `AccountSafeListenerAssignmentModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
account_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `account_id` with attributes `safe_id` and `listener_id`.
safe_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attributes `account_id` and `listener_id`.
listener_id	string	no	Immutable. Uniqueness is required in the combination of attribute `listener_id` with attributes `account_id` and `safe_id`.
account_name	string		Read-only; expensive to use
account_type	string		Read-only; expensive to use
protocol	string		Read-only; expensive to use
server_id	string		Read-only; expensive to use; `null` if pool is assigned.
server_name	string		Read-only; expensive to use; `null` if pool is assigned.
pool_id	string		Read-only; expensive to use; `null` if server is assigned.
pool_name	string		Read-only; expensive to use; `null` if server is assigned.
safe_name	string		Read-only; expensive to use
listener_name	string		Read-only; expensive to use
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
builtin	boolean		Read-only; expensive to use; if `true`, the object is not editable.
hidden	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.

Request for retrieving available attributes of the AccountSafeListenerAssignmentModel

Method	
	`GET`
Path	
	`/api/v2/objspec/account_safe_listener`

Table 3: `AccountGrantAssignmentModel`

Attribute	Type	Required	Description
id	string		Read-only, protected object Identifier
to_user_id	string	yes	Immutable. Expects unique `for_account_id`
for_account_id	string	yes	Immutable. Expects unique `to_user_id`
for_account_name	string		Read-only, expensive to use
to_user_name	string		Read-only, expensive to use
to_user_role	string		Read-only, expensive to use
created_at	string		Read-only
modified_at	string		Read-only
removed	boolean		Read-only

Request for retrieving available attributes of the AccountGrantAssignmentModel

Method	
	`GET`
Path	
	`/api/v2/objspec/account_grant`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the Account objects.

7.2 Creating an account

Request

Method	`POST`
Path	`/api/v2/account`
Headers	`Content-Type: Application/JSON`
Body	`AccountModel`

Example request

Sending `POST https://10.0.0.0/api/v2/account`

```
{
"name": "test-account",
"type": "regular",
"server_id": "1234567890",
"method": "password",
"login":"test-account-login",
"domain": "my-domain"
        }
```

Response

```
    {
"result": "success",
"account": {
    "id": "1234567890123456"
            }}
```

7.3 Retrieving accounts list

Request

Method	`GET`
Path	`/api/v2/account`

7.4 Retrieving an account

Request

Method	`GET`
Path	`/api/v2/account/<id>`

7.5 Modifying an account

Request

Method	`PATCH`
Path	`/api/v2/account/<id>`
Headers	`Content-Type: Application/JSON`
Body	`AccountModel`

Example request: Enable OCR with German, English and Polish languages for an account

Sending `PATCH https://10.0.0.0/api/v2/account/1234567890123456`

```
    { "ocr_enabled": true,
"ocr_lang": "deu+eng+pol"}
```

Response

```
{"result": "success"}
```

7.6 Granting access for user to account

Request

Method	`POST`
Path	`/api/v2/grant/account`
Headers	`Content-Type: Application/JSON`

Body	`{`
	`to_user_id: 1234567890,`
	`for_account_id: 1234567891`
	`}`

7.7 Adding a password changer policy to account

Password changer policy can't be created via API, but can be assigned to a particular Account. It requires a password changer or/and password verifier assigned according to it's enabled options.

By default there is an existing password policy named *Static, without restrictions* with `id = 1`, which has no password change or verification functions assigned.

Request

Method	`PATCH`
Path	`/api/v2/account/<id>`
Headers	`Content-Type: Application/JSON`
Body	`AccountModel`

Example request

Sending `https://10.0.0.0/api/v2/account/1234567890123456`

```
{"domain":null, "password_change_policy_id":"2345678901234567"}
```

Response

```
{"result": "success"}
```

7.8 Modifying password change parameters for account

Request

Method	`PATCH`
Path	`/api/v2/account/<id>`
Headers	`Content-Type: Application/JSON`
Body	`AccountModel`

Example request

Sending `https://10.0.0.0/api/v2/account/1234567890123456798`

```
{
   "domain":null,
   "password_change_policy_id":"2345678901234567989",
   "password_checkout_time_limit":"06:59:00",
   "password_change_on_session_end":true,
   "password_change_on_checkin":true,
   "password_recovery":true
}
```

Response

```
{"result": "success"}
```

7.9 Creating an account-safe-listener assignments

Request

Method	`POST`
Path	`/api/v2/account/safe/listener`
Headers	`Content-Type: Application/JSON`
Body	`AccountSafeListenerAssignmentModel`

Example request

Sending `POST https://10.0.0.0/api/v2/account/safe/listener`

```
    { "account_id": 1232678819172646919,
"safe_id": 123267881917264613,
"listener_id": 1232678819172646914 }
```

Response

```
    { "result": "success",
"account_safe_listener": {} }
```

7.10 Deleting an account-safe-listener assignment

Request

Method	`DELETE`
Path	`/api/v2/account/<account_id>/safe/<safe_id>/listener/<listener_id>`

7.11 Deleting an account

Request

Method	`DELETE`
Path	`/api/v2/account/<id>`

CHAPTER 8

API v2: Users

User defines a subject entitled to connect to servers within monitored IT infrastructure. Detailed object definition (i.e. unique login and domain combination, full name, email address etc.) enables precise accountability of user actions when login and password are substituted with a shared account login credentials.

8.1 Data structures

Table 1: `UserModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
name	string	yes	Unique user's name
blocked	boolean; default value `false`	yes	
reason	string	if `blocked == true`	
domain	string	no	User's domain
role	string {admin, operator, service, superadmin, user}	yes	
full_name	string	no	User's full name
email	string	no	User's email address
organization	string	no	User's organization name
phone	string	no	User's phone number
ad_domain	string	no	User's AD domain
ldap_base	string	no	User's LDAP base
language	string {en, pl, ru, ua, kk}; default value `en`	yes	Interface language

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
previous_success	datetime		Read-only
last_success	datetime		Read-only
last_failure	datetime		Read-only
failures	number; default value `0`	yes	Number of authentication failures
password_complexity	boolean; default value `false`	yes	Enable password complexity settings
external_sync	boolean; default value `false`	yes	
valid_since	datetime (h:m:s); default value `-infinity`	yes	Beginning access time
valid_to	datetime (h:m:s); default value `infinity`	yes	Ending access time
ldap_server_id	string	no	Id of the user's LDAP server
source_ip	string	no	
snmp_enabled	boolean; default value `false`	if `role == service`	
snmp_authentication		if `role == service` & `snmp_enabled == true`	
snmp_encryption		if `role == service` & `snmp_enabled == true`	
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
safes	object-array		Read-only; expensive to use; JSON object array containing `id`, `name`, and `position` of assigned safes.
authentication_methods	object-array		Read-only; expensive to use; JSON object array containing `id`, `type`, and `position` of configured authentication methods.
builtin	boolean		Read-only; expensive to use; if `true`, the object is not editable.
hidden	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.

Request for retrieving available attributes of the UserModel

Method	
	`GET`
Path	
	`/api/v2/objspec/user`

Table 2: `UserSafeAssignmentModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier.
user_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `safe_id`.
safe_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `user_id`.
blocked	boolean; default value `false`	yes	
position	number		
password_visible	boolean; default value `false`	yes	Allow a user to use Secret Checkout feature and view passwords in the Access Gateway.
use_time_policy	boolean; default value `false`	yes	
valid_since	datetime (h:m:s); default value `-infinity`	yes	Beginning access time.
valid_to	datetime (h:m:s); default value `infinity`	yes	Ending access time.
user_name	string		Read-only; Expensive to use.
safe_name	string		Read-only; Expensive to use.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.
builtin	boolean		Read-only; Expensive to use; If `true`, the object is not editable.
hidden	boolean		Read-only; Expensive to use; If `true`, the object is hidden in UI.

Request for retrieving available attributes of the UserSafeAssignmentModel

Method	
	`GET`
Path	
	`/api/v2/objspec/user_safe`

Table 3: `UserSafeTimePolicyAssignmentModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier.
user_safe_id	string		Read-only object Identifier.
user_id	string	yes	Immutable.
safe_id	string	yes	Immutable.
day_of_week	number	yes	Value range from `1` to `7`.
valid_from	datetime (h:m:s)	yes	Beginning access time.
valid_to	datetime (h:m:s)	yes	Ending access time.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.

Request for retrieving available attributes of the UserSafeTimePolicyAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/user_safe_time_policy`

Table 4: `UserGrantAssignmentModel`

Attribute	Type	Required	Description
id	string		Read-only, protected object Identifier
to_user_id	string	yes	Immutable. Expects unique `for_user_id`
for_user_id	string	yes	Immutable. Expects unique `to_user_id`
for_user_name	string		Read-only, expensive to use
to_user_name	string		Read-only, expensive to use
to_user_role	string		Read-only, expensive to use
created_at	string		Read-only
modified_at	string		Read-only
removed	boolean		Read-only

Request for retrieving available attributes of the UserGrantAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/user_grant`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the User objects.

8.2 Creating a user

Request

Method	`POST`
Path	`/api/v2/user`
Headers	`Content-Type: Application/JSON`
Body	`UserModel`

Example request

Sending `POST https://10.0.0.0/api/v2/user`

```
{
"role": "user",
"name": "test-user",
"language":"en"
 }
```

Response

```
    {
"result": "success",
"user": {
    "id": "12345678901234567890"
}}
```

8.3 Retrieving users list

Request

Method	
	`GET`

Path	
	`/api/v2/user`

Example request

Sending `GET https://10.0.0.0/api/v2/user`

Response


```
    {
"result": "success",
"user": [
    {
        "id": "1234567891012345",
        "name": "tet",
        "blocked": false,
        "role": "user",
        "full_name": "",
        "email": "",
        "phone": "",
        "ad_domain": "",
        "ldap_base": "",
        "language": "en",
        "failures": 0,
        "password_complexity": false,
        "external_sync": false,
        "valid_since": "-infinity",
        "valid_to": "infinity",
        "created_at": "2022-10-20 02:09:49.818029-07",
        "modified_at": "2022-10-20 02:09:49.818029-07"
    },
    {
        "id": "12345678910123456",
        "name": "admin",
        "blocked": false,
        "role": "superadmin",
        "language": "en",
        "previous_success": "2022-10-25 05:33:19.377878-07",
        "last_success": "2022-10-25 06:03:39.084783-07",
        "last_failure": "2022-10-24 04:19:35.204557-07",
        "failures": -1,
        "password_complexity": false,
        "external_sync": false,
        "valid_since": "-infinity",
        "valid_to": "infinity",
        "created_at": "2022-10-20 02:01:32.093269-07",
        "modified_at": "2022-10-25 06:03:39.085472-07"
    }
]}
```

8.4 Retrieving a user

Request

Method	`GET`
Path	`/api/v2/user/<id>`

8.5 Modifying a user

Request

Method	`PATCH`
Path	`/api/v2/user/<id>`
Headers	`Content-Type: Application/JSON`
Body	`UserModel`

Example request: Changing user login

Sending `PATCH https://10.0.0.0/api/v2/user/12345678901234567890`

```
{
"name": "new-user"
}
```

Response

```
{ "result": "success"}
```

Example request: Blocking a user

Sending `PATCH https://10.0.0.0/api/v2/user/12345678901234567890`

```
{"blocked": true,
 "reason": "lost rights"}
```

Response

```
{ "result": "success" }
```

8.6 Retrieving user's management privileges

Request

Method

```
GET
```

Path

```
/api/v2/grant/<to_user_id>/user/<for_user_id>
/api/v2/grant/<to_user_id>/server/<for_server_id>
/api/v2/grant/<to_user_id>/safe/<for_safe_id>
/api/v2/grant/<to_user_id>/pool/<for_pool_id>
/api/v2/grant/<to_user_id>/listener/<for_listener_id>
/api/v2/grant/<to_user_id>/account/<for_account_id>
```

8.7 Revoking user's management privileges

Request

Method

```
DELETE
```

Path

```
/api/v2/grant/<to_user_id>/user/<for_user_id>
/api/v2/grant/<to_user_id>/server/<for_server_id>
/api/v2/grant/<to_user_id>/safe/<for_safe_id>
/api/v2/grant/<to_user_id>/pool/<for_pool_id>
/api/v2/grant/<to_user_id>/listener/<for_listener_id>
/api/v2/grant/<to_user_id>/account/<for_account_id>
```

8.8 Granting access for user to another user

Request

Method	POST
Path	/api/v2/grant/user
Headers	Content-Type: Application/JSON
Body	{ to_user_id: 1234567890, for_user_id: 1234567891 }

8.9 Retrieving user-safe assignments list

Request

Method	GET
Path	/api/v2/user/safe

8.10 Creating a user-safe assignment

Request

Method	POST
Path	/api/v2/user/safe
Body	UserSafeAssignment

Example request

Sending `PATCH https://10.0.0.0/api/v2/user/safe`

```
{ "user_id": "1232678819172646915",
        "safe_id": "1232678819172646913" }
```

Response

```
    { "result": "success",
"user_safe": {} }
```

8.11 Retrieving users' time policy settings within safes

Request

Method	
	`GET`
Path	
	`/api/v2/user/safe/time_policy`

Example request

Sending `GET https://10.0.0.0/api/v2/user/safe/time_policy`

Response (User's time policy is declared separately for each day)

```
    {
"result": "success",
"user_safe_time_policy": [
    {
        "id": "4602678819172646913",
        "safe_id": "4602678819172646913",
        "user_id": "4602678819172646914",
        "day_of_week": 2, <--- A user has access to the safe on Tuesday
        "valid_from": "09:00:00", <--- User's access starts at 9:00
        "valid_to": "14:00:00", <--- and ends at 14:00
        "created_at": "2022-10-26 02:25:19.155648-07",
        "modified_at": "2022-10-26 02:30:40.677788-07"
    },
    {
        "id": "4602678819172646914",
        "safe_id": "4602678819172646913",
        "user_id": "4602678819172646914",
        "day_of_week": 3, <--- A user has access to the safe on Wednesday
        "valid_from": "09:15:00", <--- User's access starts at 9:15
        "valid_to": "14:15:00", <--- and ends at 14:15
        "created_at": "2022-10-26 02:32:11.781045-07",
        "modified_at": "2022-10-26 02:32:11.781045-07"
    }]}
```

8.12 Modifying user's time policy settings within a safe

Request

Method	PATCH
Path	/api/v2/user/safe/time_policy/<id>
Body	UserSafeTimePolicyAssignment

Example request: Changing the day of user's access to Monday

Sending `PATCH https://10.0.0.0/api/v2/user/safe/time_policy/1232678819172646913`

```
{ "day_of_week": 1}
```

Response

```
{ "result": "success" }
```

8.13 Creating user's time policy settings within a safe

Request

Method	POST
Path	/api/v2/user/safe/time_policy
Body	UserSafeTimePolicyAssignment

Example request: Creating user's access to the the safe for Thursday from 16:00 till 23:00

Sending `POST https://10.0.0.0/api/v2/user/safe/time_policy`

```
{ "user_id": "1232678819172646915",
"safe_id": "1232678819172646913",
"day_of_week": 4,
"valid_from": "16:00:00",
"valid_to": "23:00:00"
}
```

Response

```
    { "result": "success",
"user_safe_time_policy": {
    "id": "1232678819172646915" }}
```

8.14 Deleting a user-safe assignment

Request

Method	`DELETE`
Path	`/api/v2/user/<user_id>/safe/<safe_id>`

8.15 Deleting a user

Request

Method	`DELETE`
Path	`/api/v2/user/<id>`

CHAPTER 9

API v2: User authentication methods management

Table 1: `UserAuthenticationMethodModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
type	string {password, oath, extauth, sshkey, certificate, duo, sms, apikey, mobiletoken}	yes	Immutable
user_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `position`.
user_name	string		Read-only; Expensive to use
position	number	yes	Uniqueness is required in the combination of attribute `position` with attribute `user_id`.
external_sync	boolean; default value `false`	yes	
secret	string	if `type` == `duo` || `mobiletoken` || `oath` || `password` || `sms` || `sshkey`	

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
needs_change	boolean; default value `false`	yes	
external_authentication_id	string	if `type` == `duo` || `extauth` || `oath` || `sms`	
apikey_key	string	if `type` == `apikey`	Protected
certificate_subject	string	if `type` == `certificate`	
duo_user_id	string	if `type` == `duo`	
duo_username	string	if `type` == `duo`	
OATH	OATHAuthenticationMethodAttributes	if `type` == `oath`	OATH authentication method properties
mobiletoken_device_id	string	if `type` == `mobiletoken`	Read-only; Expensive to use
mobiletoken_device_platforms	string	if `type` == `mobiletoken`	Read-only; Expensive to use
mobiletoken_device_pushid	string	if `type` == `mobiletoken`	Read-only; Expensive to use
sms_token	string	if `type` == `sms`	Read-only; Protected
sshkey_user_presence_required	boolean; default value `true`	if `type` == `sshkey`	
sshkey_verification_required	boolean; default value `false`	if `type` == `sshkey`	
sshkey_counter	number	if `type` == `sshkey`	Read-only
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only

Table 2: `OATHAuthenticationMethodAttributes`

Attribute	Type	Required	Description
oath_type	string {HOTP, TOTP}	yes	Immutable.
oath_initialized	boolean; default value `false`	yes	
oath_secret	string	yes	Protected.
oath_tokenlen	number	yes	Immutable; value range: [4, 16].
oath_timestep	number {30, 45, 60, 90, 120, 180, 300}	If `oath_type` == `TOTP`	
oath_counter	number; default value `0`	yes	Read-only.
oath_timeshift	number; default value `0`	If `oath_type` == `TOTP`	Read-only.
oath_url	null		Read-only.
oath_qrcode	null		Read-only.

Request for retrieving available attributes of the UserAuthenticationMethodModel

Method	`GET`
Path	`/api/v2/objspec/user_authentication_method`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the User objects.

9.1 Listing user's authentication methods

Request

Method	`GET`
Path	`/api/v2/user/<user_id>/authentication`

Example request

Sending `GET https://10.0.0.0/api/v2/user/12345678901234567890/authentication`

Response


```
{
  "result": "success",
  "user_authentication_method": [
    {
      "id": "12345612345123",
      "user_id": "12345678901234567890",
      "type": "password",
      "needs_change": false,
      "position": 0,
      "external_sync": false,
      "created_at": "2022-10-25 06:35:12.95741-07",
      "modified_at": "2022-10-25 06:35:12.95741-07",
      "user_name": "test-user"
    },
    {
      "id": "1234561234512357466",
      "user_id": "12345678901234567890",
      "type": "sshkey",
      "needs_change": false,
      "position": 1,
      "external_sync": false,
      "sshkey_user_presence_required": true,
      "sshkey_verification_required": false,
      "sshkey_counter": 0,
      "created_at": "2022-10-25 06:37:54.913056-07",
      "modified_at": "2022-10-25 06:37:54.913056-07",
      "user_name": "test-user"
    }
  ]
}
```


9.2 Creating user authentication method

Request

Method	`POST`
Path	`/api/v2/user/<user_id>/authentication`
Headers	`Content-Type: Application/JSON`
Body	`UserAuthenticationMethodModel`

Example request: Setting user authentication method - Static Password

Sending `POST https://10.0.0.0/api/v2/user/12345678901234567890/authentication`

```
{
  "type": "password",
  "secret": "test-password"
}
```

Response

```
{
  "result": "success",
  "user_authentication_method": {
    "id": "12345612345123"
  }
}
```

Example request: Setting user authentication method - API Key

---

Note: When creating *API Key* authentication method, you can:

- set `apikey_key=null` or skip this attribute in the request - API will generate an `apikey_key` and return it in the response.
- set `apikey_key=<plaintext>` - API will save provided plaintext without returning it in the response.
- set `apikey_key=sha512:<hash-base64-encoding>` - API will save provided hash. Please be informed that the *SHA512* hash should be encoded in *Base64* formatting.

Note: You can use following command to generate an `apikey_key` and its hash. The `apikey_key` will be saved in the `apikey.txt` file, and the hash will be saved in the `apikey.sha512` file.

```
(umask 077 && echo sha512:$(openssl rand 48 | openssl base64 | tee apikey.txt | dd␣
↪bs=64 count=1 | openssl sha512 -binary | openssl base64 -A) > apikey.sha512)
```

Request:

Sending `POST https://10.0.0.0/api/v2/user/12345678901234567890/authentication`

```
{
    "type": "apikey"
}
```

Response:

```
{
    "result": "success",
    "user_authentication_method": {
        "id": "8511803295730237450",
        "apikey_key":
↪"Ah08ibgN98TAUsa8f7o3MDsJXnliodphdtSz5xzTsnVI4DLv0dfUn6s3BEubse7O"
    }
}
```

Request:

Sending `POST https://10.0.0.0/api/v2/user/12345678901234567891/authentication`

```
{
    "type": "apikey",
    "position": 1,
    "apikey_key": "sha512:rPXbZAJ5q/
↪4GcHTC7Z0x8a568eVqrXuhzmmPjqHPMGovdbCaczEI7WxLw8oyAzKkUV2qWlr9n9g+70K4p12xKw=="
}
```

Response:

```
{
    "result": "success",
    "user_authentication_method": {
        "id": "8511803295730237478"
    }
}
```

Note: The `apikey_key` plain text is available only during authentication method creation process. Please remember to copy and archive it if needed.

9.3 Modifying user authentication method

Request

Method	`PATCH`
Path	`/api/v2/user/<user_id>/authentication/<id>`
Headers	`Content-Type: Application/JSON`
Body	`UserAuthenticationMethodModel`

Example request

Request

Sending `PATCH https://10.0.0.0/api/v2/user/12345678901234567890/authentication/12345612345123`

```
{
  "position": 1
}
```

Response

```
{
  "result": "success"
}
```

9.4 Deleting user authentication method

Request

Method	`DELETE`
Path	`/api/v2/user/<user_id>/authentication/<id>`

Example request

Sending `DELETE https://10.0.0.0/api/v2/user/12345678901234567890/authentication/1234561234512357466`

Response

```
{
  "result": "success"
}
```

CHAPTER 10

API v2: External authentication

10.1 Data structures

Table 1: `ExternalAuthenticationModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
type	string {cerb, radius, ldap, ad}	yes	Immutable
address	string	yes	
port	number {from `1` to `65535`}	yes	
bindto	string	no	Bind address. Include labels like 'fudo:label:test' or ip address
cerb	ExternalAuthentication-CerbModel	If `type` == `cerb`	Cerb object definiton
radius	ExternalAuthentication-RadiusModel	If `type` == `radius`	Radius object definiton
ldap	ExternalAuthentication-LdapModel	If `type` == `ldap`	LDAP object definiton
ad	ExternalAuthentication-AdModel	If `type` == `ad`	Active Directory object definiton
tls_enabled	boolean	no	Enable TLS protocol
tls_certificate	string	If `tls_enabled` == `true`	
second_factor_type	string {duo, oath, sms}	no	
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only

Table 2: `ExternalAuthenticationCerbModel`

Attribute	Type	Description
secret	string	Password to cerb provider; required; write-only
radius_nasid	string	Correct value of NAS id of Cerb provider

Table 3: `ExternalAuthenticationRadiusModel`

Attribute	Type	Description
secret	string	Password to cerb provider; required; write-only
radius_nasid	string	Correct value of NAS id of Radius provider

Table 4: `ExternalAuthenticationLdapModel`

Attribute	Type	Description
ldap_binddn	string	Bind domain to LDAP provider; required

Table 5: `ExternalAuthenticationAdModel`

Attribute	Type	Description
login	string	
secret	string	Password to cerb provider; required; write-only
ad_domain	string	Bind domain to AD provider; required

Request for retrieving available attributes of the ExternalAuthenticationModel

Method	`GET`
Path	`/api/v2/objspec/external_authentication`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the External Authentication objects.

10.2 Retrieving external authentication methods list

Request

Method	
	`GET`

Path	
	`/api/v2/external_authentication`

Example request

Sending `GET https://10.0.0.0/api/v2/external_authentication`

Response


```
    {
"result": "success",
"external_authentication": [
    {
        "id": "1234538875067072557",
        "type": "ad",
        "port": 636,
        "ad_domain": "jdoe.local",
        "created_at": "2021-08-09 19:40:05.171853+02",
        "modified_at": "2021-08-09 19:40:05.171853+02",
        "address": "10.0.139.100",
        "tls_enabled": true,
        "tls_certificate": "-----BEGIN CERTIFICATE-----\r\nMIIFrTCCBJWgAwIBAg...
↪ic=\r\n-----END CERTIFICATE-----\r\n"
    },
    {
        "id": "12345138875067072517",
        "type": "ldap",
        "port": 389,
        "ldap_binddn": "dc=qa-ldap,dc=null",
        "created_at": "2021-03-03 14:11:52.245683+01",
        "modified_at": "2021-03-03 14:14:46.052855+01",
        "address": "10.0.235.1",
        "tls_enabled": false,
        "tls_certificate": ""
    },
    {
        "id": "12345067072573",
        "type": "cerb",
        "port": 1812,
        "created_at": "2022-10-19 10:23:11.29545+02",
        "modified_at": "2022-10-19 10:58:12.325396+02",
        "address": "10.0.234.21",
        "radius_nasid": "",
        "tls_enabled": false,
        "tls_certificate": ""
    },
    {
        "id": "3234566775067072572",
        "type": "radius",
        "port": 1812,
        "created_at": "2022-10-19 10:08:23.160433+02",
        "modified_at": "2022-10-19 10:19:50.525671+02",
```


(continues on next page)

(continued from previous page)

```
        "second_factor_type": "oath",
        "address": "10.0.0.1",
        "radius_nasid": "abcdeg",
        "tls_enabled": true,
        "tls_certificate": "-----BEGIN CERTIFICATE-----\r\nMIIG5jC...
↪2MOXV1x+eQAmOVy\r\n-----END CERTIFICATE-----\r\n"
    }]}
```

10.3 Modifying external authentication method

Request

Method	`PATCH`
Path	`/api/v2/external_authentication/<id>`
Headers	`Content-Type: Application/JSON`
Body	`ExternalAuthenticationModel`

Example request: Adding SMS authentication for second factor to AD authentication

Sending `PATCH https://10.0.0.0/api/v2/external_authentication/1234538875067072557`

```
{"second_factor_type": "sms"}
```

Response

```
{ "result": "success"}
```

10.4 Creating an external authentication method

Request

Method	`POST`
Path	`/api/v2/external_authentication`
Headers	`Content-Type: Application/JSON`
Body	`ExternalAuthenticationModel`

Example request: Creating Cerb definition with second factor OATH authentication

Sending `POST https://10.0.0.0/api/v2/external_authentication`

```
{ "type": "cerb",
"port": 1812,
"address": "10.0.234.21",
"radius_nasid": "abcds",
"secret": "my-password",
"tls_enabled": false,
 "second_factor_type": "oath" }
```

Response

```
    { "result": "success",
"external_authentication": {
    "id": "1234568191726469l3" }}
```

10.5 Deleting an external authentication method

Request

Method	`DELETE`
Path	`/api/v2/external_authentication/<id>`

CHAPTER 11

API v2: Servers

Server is a definition of the IT infrastructure resource, which can be accessed over one of the specified protocols.

11.1 Data structures

Table 1: `ServerModel`

Attribute	Type	Required	Description
id	string	yes	Unique, read-only object Identifier.
name	string	yes	Unique server's name.
description	string	no	Object description.
blocked	boolean; default value `false`	yes	
reason	string	if `blocked` == `true`	
bind_ip	string		Required format: IP address or `fudo:label:<ip_label_name>` for labeled IP addresses.
address	string	yes	IP address. Uniqueness is required in the combination of attribute `address` with attributes `mask` and `port`.

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
mask	number {from 0 to 128}	no	Uniqueness is required in the combination of attribute `mask` with attributes `address` and `port`.
port	number {from 1 to 65535}	yes	Uniqueness is required in the combination of attribute `port` with attributes `address` and `mask`.
legacy_crypto	boolean; default value `false`	If `protocol == rdp` || `ssh` || `http` || `telnet` || `tn3270` || `tn5250` & `tls_enabled == true`	Enabling legacy cryptographic protocols and settings.
protocol	string{http, modbus, mysql, rdp, ssh, system, tcp, tds, telnet, tn3270, tn5250, vnc}	yes	Immutable, case insensitive.
http	HTTPServerAttributes	If `protocol == http`	HTTP protocol properties.
rdp	RDPServerAttributes	If `protocol == rdp`	RDP protocol properties.
tls	TLSServerAttributes	If `tls_enabled == true`	TLS protocol properties.
ssh_public_key	string	If `protocol == ssh`	SSH public key.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.
last_login	datetime		Read-only; Expensive to use.
pools	object-array		Read-only; Expensive to use; JSON object array containing `id` and `name` of assigned pools.
state	string		Server's discovery state: onboarded, quarantined or created (for manually created accounts). Read-only. Expensive to use.
discovered_at	datetime		Read-only. Expensive to use.

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
onboarded_at	datetime		Read-only. Expensive to use.
onboarded_by_id	string		Read-only. Expensive to use. Unique identifier of the user who performed the onboarding.
onboarded_by_name	string		Read-only. Expensive to use. Name of the user who performed the onboarding.
quarantined_at	datetime		Read-only. Expensive to use.
quarantined_by_id	string		Read-only. Expensive to use. Unique identifier of the user who performed the quarantine.
quarantined_by_name	string		Read-only. Expensive to use. Name of the user who performed the quarantine.
scanner_id	string		Read-only. Expensive to use. Unique identifier of a scanner used to discover this server.
scanner_name	string		Read-only. Expensive to use. Name of a scanner used to discover this server.
builtin	boolean		Read-only; Expensive to use; If `true`, the object is not editable.
hidden	boolean		Read-only; Expensive to use; If `true`, the object is hidden in UI.

Table 2: `HTTPServerAttributes`

Attribute	Type	Required	Description
http_host	string	yes	HTTP host header value.
http_timeout	number {seconds}	yes	Period of inactivity, after which the user will have to authenticate again.
http_authentication	boolean; default value `false`	no	
http_authentication_method	string {Asana, Azure, Facebook, HPE BladeSystem, HPE iLO, HTTP Authentication, LinkedIn, Salesforce, Twitter}; Default value `null`	If `http_authentication` == `true`	Case insensitive.
http_username_element	string	If `http_authentication` == `true` & `http_authentication_method` == `null`	Custom login page details.
http_press_enter	boolean; default value `false`	If `http_authentication` == `true` & `http_authentication_method` == `null`	The *Press the enter key prior to password* option.
http_password_element	string	If `http_authentication` == `true` & `http_authentication_method` == `null`	Custom login page details.
http_signon_realm	string	If `http_authentication` == `true` & `http_authentication_method` == `null`	Custom login page details.

Table 3: `RDPServerAttributes`

Attribute	Type	Required	Description
rdp_hotseat	boolean; default value `false`	yes	The option to have the users informed that other users are connected to the server, they are trying to connect to.
rdp_nla_enabled	boolean; default value `true`	If `protocol` == `rdp` & `tls_enabled` == `true`.	
rdp_public_key	string	If `protocol` == `rdp` & `tls_enabled` == `false`	RDP public key.

Table 4: `TLSServerAttributes`

Attribute	Type	Required	Description
tls_enabled	boolean; default value `true`	If `protocol == rdp` || `http` || `telnet` || `tn3270` || `tn5250`	Enabling the TLS protocol.
tls_ca_certificate	string	If `protocol == rdp` || `http` || `telnet` || `tn3270` || `tn5250` & `tls_enabled == true`	TLS CA certificate.
tls_certificate	string	If `protocol == rdp` || `http` || `telnet` || `tn3270` || `tn5250` & `tls_enabled == true`	TLS certificate.

Request for retrieving available attributes of the ServerModel

Method	`GET`
Path	`/api/v2/objspec/server`

Table 5: `ServerPoolModel`

Attribute	Type	Required	Description
id	number	yes	Read-only object Identifier.
pool_id	number	yes	Immutable. Uniqueness is required in the combination of attribute `pool_id` with attribute `server_id`.
server_id	number	yes	Immutable. Uniqueness is required in the combination of attribute `server_id` with attribute `pool_id`.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.

Request for retrieving available attributes of the ServerPoolModel

Method	
	`GET`
Path	
	`/api/v2/objspec/pool_server`

Table 6: `ServerGrantAssignmentModel`

Attribute	Type	Required	Description
id	string		Read-only, protected object Identifier
to_user_id	string	yes	Immutable. Expects unique `for_server_id`
for_server_id	string	yes	Immutable. Expects unique `to_user_id`
for_server_name	string		Read-only, expensive to use
to_user_name	string		Read-only, expensive to use
to_user_role	string		Read-only, expensive to use
created_at	string		Read-only
modified_at	string		Read-only
removed	boolean		Read-only

Request for retrieving available attributes of the ServerGrantAssignmentModel

Method	
	`GET`
Path	
	`/api/v2/objspec/server_grant`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the Server objects.

11.2 Creating a server

Request

Method	`POST`
Path	`/api/v2/server`
Headers	`Content-Type: Application/JSON`
Body	`ServerModel`

Example request

Sending `POST https://10.0.0.0/api/v2/server`

```
     {
"name": "my-1st-rdp-server",
"protocol": "rdp",
"address": "10.0.2.0",
"port": 3389,
"legacy_crypto": false
     }
```

Response

```
    { "result": "success",
"server": {
    "id": "41234678819172646916" }}
```

11.3 Retrieving servers list

Request

Method	`GET`
Path	`/api/v2/server`

11.4 Retrieving a server

Request

Method	`GET`
Path	`/api/v2/server/<id>`

Example request

Sending `GET https://10.0.0.0/api/v2/server/41234678819172646916`


```
    {
"result": "success",
"server": {
    "id": "4602678819172646916",
    "name": "my-1st-rdp-server",
    "blocked": false,
    "address": "10.0.2.0",
    "mask": 32,
    "port": 3389,
    "protocol": "rdp",
    "legacy_crypto": false,
    "rdp_hotseat": false,
    "rdp_nla_enabled": true,
    "tls_enabled": true,
    "tls_use_ca_store": false,
    "created_at": "2022-10-27 01:43:39.688273-07",
    "modified_at": "2022-10-27 01:43:39.688273-07",
    "last_login": "-infinity"
}}
```


11.5 Modifying a server

Request

Method	`PATCH`
Path	`/api/v2/server/<id>`
Headers	`Content-Type: Application/JSON`
Body	`ServerModel`

Example request: Enable using CA store for server verification

Sending `PATCH https://10.0.0.0/api/v2/server/41234678819172646916`

```
{"tls_use_ca_store": true}
```

Response

```
{ "result": "success" }
```

11.6 Adding a server to the pool

Request

Method	`POST`
Path	`/api/v2/pool/server`
Headers	`Content-Type: Application/JSON`
Body	`ServerPoolModel`

Example request

Sending `POST https://10.0.0.0/api/v2/pool/server`

```
    { "pool_id": "122678819172646916",
"server_id": "123402678819172646914"}
```

Response

```
   { "result": "success",
"pool_server": {} }
```

11.7 Deleting a server from a pool

Request

Method	`DELETE`
Path	`/api/v2/pool/<pool_id>/server/<server_id>`

11.8 Retrieving users allowed to manage servers

Request

Method	`GET`
Path	`/api/v2/grant/server`

Example request

Sending `GET https://10.0.0.0/api/v2/grant/server`

Response


```
    { "result": "success",
"server_grant": [
    {
        "for_server_id": "4602678819172646916",
        "to_user_id": "4602678819172646914",
        "created_at": "2022-10-27 01:51:15.839452-07",
        "modified_at": "2022-10-27 01:51:15.839452-07" }]}
```


11.9 Granting management privileges

Request

Method	`POST`
Path	`/api/v2/grant/server`
Body	`{ to_user_id: 1234567890, for_server_id: 1234567891 }`

11.10 Deleting a server

Request

Method	`DELETE`
Path	`/api/v2/server/<id>`

CHAPTER 12

API v2: Pools

Pools serve grouping purposes for the server objects based on the same protocol to be managed within other objects (for example, accounts) as one server.

12.1 Data structures

Table 1: `PoolModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
name	string	yes	Unique pool's name
description	string	no	
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
servers	object-array		Read-only; expensive to use; JSON object array containing `id`, `mask`, `name`, `port` and `address` of assigned servers.
protocol	string		Read-only; expensive to use.
builtin	boolean		Read-only; expensive to use; if `true`, the object is not editable.
hidden	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.

Request for retrieving available attributes of the PoolModel

Method	
	`GET`
Path	
	`/api/v2/objspec/pool`

Table 2: `ServerPoolModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier.
pool_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `pool_id` with attribute `server_id`.
server_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `server_id` with attribute `pool_id`.
pool_name	string		Read-only; Expensive to use.
server_name	string		Read-only; Expensive to use.
server_protocol	string		Read-only; Expensive to use.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.

Request for retrieving available attributes of the ServerPoolModel

Method	
	`GET`
Path	
	`/api/v2/objspec/pool_server`

Table 3: `PoolGrantAssignmentModel`

Attribute	Type	Required	Description
id	string		Read-only, protected object Identifier
to_user_id	string	yes	Immutable. Expects unique `for_pool_id`
for_pool_id	string	yes	Immutable. Expects unique `to_user_id`
for_pool_name	string		Read-only, expensive to use
to_user_name	string		Read-only, expensive to use
to_user_role	string		Read-only, expensive to use
created_at	string		Read-only
modified_at	string		Read-only
removed	boolean		Read-only

Request for retrieving available attributes of the PoolGrantAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/pool_grant`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the Pool objects.

12.2 Retrieving pools list

Request

Method	`GET`
Path	`/api/v2/pool`

Example request

Sending `GET https://10.0.0.0/api/v2/pool`

Response


```
    {
"result": "success",
"pool": [
    {
        "id": "1232678819172646913",
        "name": "Linux servers",
        "description": "Example Linux pool",
        "created_at": "2022-10-20 02:01:38.373501-07",
        "modified_at": "2022-10-20 02:01:38.373501-07",
        "servers": [
            "1202678819172646913"
        ]
    },
    {
        "id": "41232678819172646914",
        "name": "Windows servers",
        "description": "Example Windows pool",
```


(continues on next page)

(continued from previous page)


```
        "created_at": "2022-10-20 02:01:38.376251-07",
        "modified_at": "2022-10-20 02:01:38.376251-07",
        "servers": [
            "1202678819172646914"
        ]
    },
    {
        "id": "1232678819172646915",
        "name": "test-pool",
        "created_at": "2022-10-24 06:34:53.510281-07",
        "modified_at": "2022-10-24 06:34:53.510281-07",
        "servers": [
            "1202678819172646913"
        ]}]}
```


12.3 Retrieving a pool

Request

Method
`GET`

Path
`/api/v2/pool/<id>`

Example request

Sending `GET https://10.0.0.0/api/v2/pool/1232678819172646915`

Response


```
    {
"result": "success",
"pool": {
    "id": "1232678819172646915",
    "name": "test-pool",
    "created_at": "2022-10-24 06:34:53.510281-07",
    "modified_at": "2022-10-24 06:34:53.510281-07",
    "servers": [
        "1202678819172646913"
    ]}}
```


12.4 Creating a pool

Request

Method	`POST`
Path	`/api/v2/pool`
Headers	`Content-Type: Application/JSON`
Body	`PoolModel`

Example request

Sending `POST https://10.0.0.0/api/v2/pool`

```
{"name": "my-2nd-pool"}
```

Response

```
    { "result": "success",
"pool": {
    "id": "1202678819172646916" }}
```

12.5 Modifying a pool

Request

Method	`PATCH`
Path	`/api/v2/pool/<id>`
Headers	`Content-Type: Application/JSON`
Body	`PoolModel`

Example request

Sending `PATCH https://10.0.0.0/api/v2/pool/1202678819172646916`

```
{"name": "my-cool-pool"}
```

Response

```
{ "result": "success" }
```

12.6 Retrieving server pools

Request

Method	
	`GET`
Path	
	`/api/v2/pool/server`

Example request

Sending `GET https://10.0.0.0/api/v2/pool/server`

Response

```
    {
"result": "success",
"pool_server": [
    {
        "pool_id": "1232678819172646913",
        "server_id": "1232678819172646913",
        "created_at": "2022-10-20 02:01:38.374809-07",
        "modified_at": "2022-10-20 02:01:38.374809-07"
    },
    {
        "pool_id": "1232678819172646914",
        "server_id": "1232678819172646914",
        "created_at": "2022-10-20 02:01:38.376536-07",
        "modified_at": "2022-10-20 02:01:38.376536-07"
    },
    {
        "pool_id": "1232678819172646915",
        "server_id": "1232678819172646913",
        "created_at": "2022-10-24 06:51:46.780733-07",
        "modified_at": "2022-10-24 06:51:46.780733-07"
    }]}
```

12.7 Adding a server to the pool

Request

Method	`POST`
Path	`/api/v2/pool/server`
Headers	`Content-Type: Application/JSON`
Body	`ServerPoolModel`

Example request

Sending `POST https://10.0.0.0/api/v2/pool/server`

```
    { "pool_id": "4602678819172646916",
"server_id": "4602678819172646914"}
```

Response

```
   { "result": "success",
"pool_server": {} }
```

12.8 Deleting a server from a pool

Request

Method	`DELETE`
Path	`/api/v2/pool/<pool_id>/server/<server_id>`

12.9 Retrieving users allowed to manage pools

Request

Method	`GET`
Path	`/api/v2/grant/pool`

Example request

Sending `GET https://10.0.0.0/api/v2/grant/pool`

Response


```
    {
"result": "success",
"pool_grant": [
    {
        "for_pool_id": "1232678819172646916",
        "to_user_id": "1232678819172646915",
        "created_at": "2022-10-26 04:08:38.907148-07",
        "modified_at": "2022-10-26 04:08:38.907148-07"
    }]}
```


12.10 Granting access for user to a pool

Request

Method	`POST`
Path	`/api/v2/grant/pool`
Headers	`Content-Type: Application/JSON`

Body	`{`
	`to_user_id: 1234567890,`
	`for_pool_id: 1234567891`
	`}`

12.11 Deleting a pool

Request

Method	`DELETE`
Path	`/api/v2/pool/<id>`

CHAPTER 13

API v2: Safes

Safe directly regulates user access to monitored servers. It specifies available protocols' features, policies and other details concerning users and servers relations.

13.1 Data structures

Table 1: `SafeModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
name	string	yes	Unique safe's name
blocked	boolean; default value `false`	yes	
reason	string	if `blocked` == `true`	
login_reason	boolean; default value `false`	yes	Enable sending login reason for connection
use_ticketing_system	boolean; default value `false`	yes	
require_confirmation	boolean; default value `false`	yes	Enable confirmation of each connection
otp_in_access_gateway	boolean; default value `true`	yes	Enable generating OTP in the Access Gateway
webclient	boolean; default value `true`	yes	Enable connecting to the session in browser

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
confirmation_timeout	number; default value `5`	yes	
inactivity_limit	number; default value `0`	yes	
time_limit	number; default value `0`	yes	
note_access	string {none, read, write}; default value `none`	Access level to the notes	
required_votes	number; default value `0`	yes	How many voters will be voting for the access request
backup_id	string	no	Target destination ID for storing session data
rdp	SafeRDPAttributes	If `protocol == rdp`	
ssh	SafeSSHAttributes	If `protocol == ssh`	
vnc	SafeVNCAttributes	If `protocol == vnc`	
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
last_login	datetime		Read-only
accounts	object-array		Read-only; expensive to use; JSON object array containing `id`, `name`, and `type` of assigned accounts.
builtin	boolean		Read-only; expensive to use; if `true`, the object is not editable.
hidden	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.

Table 2: `SafeRDPAttributes`

Attribute	Type	Required	Description
rdp_audin	boolean; default value `true`	yes	Audio input redirection
rdp_cliprdr	boolean; default value `true`	yes	Clipboard redirection
rdp_depth	number	no	Max. color depth
rdp_rdpdr	boolean; default value `true`	yes	
rdp_rdpsnd	boolean; default value `true`	yes	Sound redirection
rdp_rdrynvc	boolean; default value `true`	yes	
rdp_resolution	string	no	Max. resolution
rdp_suspend	boolean; default value `true`	yes	Enable content to not be available for viewing when the user minimizes its client application
rdp_tsmf	boolean; default value `true`	yes	

Table 3: `SafeSSHAttributes`

Attribute	Type	Required
ssh_agent	boolean; default value `true`	yes
ssh_environment	boolean; default value `true`	yes
ssh_exec	boolean; default value `true`	yes
ssh_port_forwarding	boolean; default value `true`	yes
ssh_scp	boolean; default value `true`	yes
ssh_session	boolean; default value `true`	yes
ssh_shell	boolean; default value `true`	yes
ssh_sftp	boolean; default value `true`	yes
ssh_terminal	boolean; default value `true`	yes
ssh_x11	boolean; default value `true`	yes

Table 4: `SafeVNCAttributes`

Attribute	Type	Required	Description
vnc_clipcli	boolean; default value `true`	yes	Enable a user to be allowed to paste text into the VNC server computer
vnc_clipsrv	boolean; default value `true`	yes	Enable a user to be allowed to copy and paste text from the VNC server computer into the user's computer

Request for retrieving available attributes of the SafeModel

Method

```
GET
```

Path

```
/api/v2/objspec/safe
```

Table 5: `UserSafeAssignmentModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier.
user_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `safe_id`.
safe_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `user_id`.
blocked	boolean; default value `false`	yes	
position	number		
password_visible	boolean; default value `false`	yes	Allow a user to use Secret Checkout feature and view passwords in the Access Gateway.
use_time_policy	boolean; default value `false`	yes	
valid_since	datetime (h:m:s); default value `-infinity`	yes	Beginning access time.
valid_to	datetime (h:m:s); default value `infinity`	yes	Ending access time.
user_name	string		Read-only; Expensive to use.
safe_name	string		Read-only; Expensive to use.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.
builtin	boolean		Read-only; Expensive to use; If `true`, the object is not editable.
hidden	boolean		Read-only; Expensive to use; If `true`, the object is hidden in UI.

Request for retrieving available attributes of the UserSafeAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/user_safe`

Table 6: `UserSafeTimePolicyAssignmentModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier.
user_safe_id	string		Read-only object Identifier.
user_id	string	yes	Immutable.
safe_id	string	yes	Immutable.
day_of_week	number	yes	Value range from `1` to `7`.
valid_from	datetime (h:m:s)	yes	Beginning access time.
valid_to	datetime (h:m:s)	yes	Ending access time.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.

Request for retrieving available attributes of the UserSafeTimePolicyAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/user_safe_time_policy`

Table 7: `AccountSafeListenerAssignmentModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
account_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `account_id` with attributes `safe_id` and `listener_id`.
safe_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attributes `account_id` and `listener_id`.
listener_id	string	no	Immutable. Uniqueness is required in the combination of attribute `listener_id` with attributes `account_id` and `safe_id`.
account_name	string		Read-only; expensive to use
account_type	string		Read-only; expensive to use
protocol	string		Read-only; expensive to use
server_id	string		Read-only; expensive to use; `null` if pool is assigned.
server_name	string		Read-only; expensive to use; `null` if pool is assigned.
pool_id	string		Read-only; expensive to use; `null` if server is assigned.
pool_name	string		Read-only; expensive to use; `null` if server is assigned.
safe_name	string		Read-only; expensive to use
listener_name	string		Read-only; expensive to use
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
builtin	boolean		Read-only; expensive to use; if `true`, the object is not editable.
hidden	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.

Request for retrieving available attributes of the AccountSafeListenerAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/account_safe_listener`

Table 8: `SafeGrantAssignmentModel`

Attribute	Type	Required	Description
id	string		Read-only, protected object Identifier
to_user_id	string	yes	Immutable. Expects unique `for_safe_id`
for_safe_id	string	yes	Immutable. Expects unique `to_user_id`
for_safe_name	string		Read-only, expensive to use
to_user_name	string		Read-only, expensive to use
to_user_role	string		Read-only, expensive to use
created_at	string		Read-only
modified_at	string		Read-only
removed	boolean		Read-only

Request for retrieving available attributes of the SafeGrantAssignmentModel

Method

```
GET
```

Path

```
/api/v2/objspec/safe_grant
```

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the Safe objects.

13.2 Retrieving safes list

Request

Method

```
GET
```

Path

```
/api/v2/safe
```

Example request

Sending `GET https://10.0.0.0/api/v2/safe`

Response

```
    { "result": "success",
"safe": [
    {
        "id": "123678819172646913",
        "name": "main",
        "blocked": false,
        "login_reason": false,
        "use_ticketing_system": false,
        "require_confirmation": false,
        "otp_in_access_gateway": true,
        "webclient": true,
        "confirmation_timeout": 5,
        "inactivity_limit": 0,
        "time_limit": 0,
        "note_access": "none",
        "required_votes": 0,
        "rdp_audin": true,
        "rdp_cliprdr": true,
        "rdp_rdpdr": true,
        "rdp_rdpsnd": true,
        "rdp_rdrynvc": true,
        "rdp_suspend": true,
        "rdp_tsmf": true,
        "ssh_agent": true,
        "ssh_environment": true,
        "ssh_exec": true,
        "ssh_port_forwarding": true,
        "ssh_scp": true,
        "ssh_session": true,
        "ssh_shell": true,
        "ssh_sftp": true,
        "ssh_terminal": true,
        "ssh_x11": true,
        "vnc_clipcli": true,
        "vnc_clipsrv": true,
        "created_at": "2022-10-20 02:01:38.366865-07",
        "modified_at": "2022-10-26 03:26:45.530129-07",
        "last_login": "-infinity",
        "accounts": [
            "122678819172646913",
            "1232678819172646914",
            "1232678819172646919"
        ]}]}
```


13.3 Creating a safe

Request

Method	`POST`
Path	`/api/v2/safe`
Headers	`Content-Type: Application/JSON`
Body	`SafeModel`

Example request

Sending `POST https://10.0.0.0/api/v2/safe`

```
{ "name": "my-1st-safe" }
```

Response

```
    { "result": "success",
"safe": {
    "id": "1232678819172646915" }}
```

13.4 Retrieving a safe

Request

Method	`GET`
Path	`/api/v2/safe/<id>`

Example request

Sending `GET https://10.0.0.0/api/v2/safe/1232678819172646915`

Response

```
    { "result": "success",
"safe": {
    "id": "1232678819172646915",
    "name": "my-1st-safe",
    "blocked": false,
    "login_reason": false,
    "use_ticketing_system": false,
    "require_confirmation": false,
```

(continues on next page)

(continued from previous page)


```
    "otp_in_access_gateway": true,
    "webclient": true,
    "confirmation_timeout": 5,
    "inactivity_limit": 0,
    "time_limit": 0,
    "note_access": "none",
    "required_votes": 0,
    "rdp_audin": true,
    "rdp_cliprdr": true,
    "rdp_rdpdr": true,
    "rdp_rdpsnd": true,
    "rdp_rdrynvc": true,
    "rdp_suspend": true,
    "rdp_tsmf": true,
    "ssh_agent": true,
    "ssh_environment": true,
    "ssh_exec": true,
    "ssh_port_forwarding": true,
    "ssh_scp": true,
    "ssh_session": true,
    "ssh_shell": true,
    "ssh_sftp": true,
    "ssh_terminal": true,
    "ssh_x11": true,
    "vnc_clipcli": true,
    "vnc_clipsrv": true,
    "created_at": "2022-10-27 02:26:22.951762-07",
    "modified_at": "2022-10-27 02:26:22.951762-07",
    "last_login": "-infinity" }}
```


13.5 Modifying a safe

Request

Method	`PATCH`
Path	`/api/v2/safe/<id>`
Headers	`Content-Type: Application/JSON`
Body	`SafeModel`

Example request: Enabling the Just-in-Time feature for a safe that would wait for 5 authorized users to vote for access

Sending `PATCH https://10.0.0.0/api/v2/safe/1232678819172646915`

```
{ "required_votes": 5}
```

Response

```
{ "result": "success" }
```

13.6 Retrieving users' time policy settings within safes

Request

Method	`GET`
Path	`/api/v2/user/safe/time_policy`

Example request

Sending `GET https://10.0.0.0/api/v2/user/safe/time_policy`

Response (User's time policy is declared separately for each day)

```
    {
"result": "success",
"user_safe_time_policy": [
    {
        "id": "4602678819172646913",
        "safe_id": "4602678819172646913",
        "user_id": "1232678819172646915",
        "day_of_week": 2, <--- A user has access to the safe on Tuesday
        "valid_from": "09:00:00", <--- User's access starts at 9:00
        "valid_to": "14:00:00", <--- and ends at 14:00
        "created_at": "2022-10-26 02:25:19.155648-07",
        "modified_at": "2022-10-26 02:30:40.677788-07"
    },
    {
        "id": "4602678819172646914",
        "safe_id": "4602678819172646913",
        "user_id": "1232678819172646915",
        "day_of_week": 3, <--- A user has access to the safe on Wednesday
        "valid_from": "09:15:00", <--- User's access starts at 9:15
        "valid_to": "14:15:00", <--- and ends at 14:15
        "created_at": "2022-10-26 02:32:11.781045-07",
        "modified_at": "2022-10-26 02:32:11.781045-07"
    }]}
```

13.7 Modifying a user's time policy settings within a safe

Request

Method	`PATCH`
Path	`/api/v2/user/safe/time_policy/<id>`
Body	`UserSafeTimePolicyAssignment`

Example request: Changing the day of user's access to Monday

Sending `PATCH https://10.0.0.0/api/v2/user/safe/time_policy/1232678819172646913`

```
{ "day_of_week": 1}
```

Response

```
{ "result": "success" }
```

13.8 Retrieving user's settings within a safe

Request

Method	`GET`
Path	`/api/v2/user/<user_id>/safe/<safe_id>`

13.9 Modifying a user within a safe

Request

Method	`PATCH`
Path	`/api/v2/user/<user_id>/safe/<safe_id>`
Body	`UserSafeAssignment`

Example request: Allow a user to use Secret Checkout feature and view passwords in the Access Gateway

Sending PATCH https://10.0.0.0/api/v2/user/1232678819172646914/safe/1230267881917264691 3

```
{"password_visible": true}
```

Response

```
{ "result": "success" }
```

13.10 Deleting a user from a safe

Request

Method	DELETE
Path	/api/v2/user/<user_id>/safe/<safe_id>

13.11 Retrieving users allowed to manage selected safe

Request

Method	GET
Path	/api/v2/user/safe

13.12 Granting management privileges

Request

Method	POST
Path	/api/v2/grant/safe
Body	{ to_user_id: 1234567890, for_safe_id: 1234567891 }

13.13 Retrieving account-safe-listener assignments list

Request

Method	`GET`
Path	`/api/v2/account/safe/listener`

13.14 Creating an account-safe-listener assignments

Request

Method	`POST`
Path	`/api/v2/account/safe/listener`
Headers	`Content-Type: Application/JSON`
Body	`AccountSafeListenerAssignmentModel`

Example request

Sending `POST https://10.0.0.0/api/v2/account/safe/listener`

```
    { "account_id": 1232678819172646919,
"safe_id": 1232678819172646913,
"listener_id": 1232678819172646914 }
```

Response

```
    { "result": "success",
"account_safe_listener": {} }
```

13.15 Deleting an account-safe-listener assignment

Request

Method	`DELETE`
Path	`/api/v2/account/<account_id>/safe/<safe_id>/listener/<listener_id>`

13.16 Deleting a safe

Request

Method	`DELETE`
Path	`/api/v2/safe/<id>`

CHAPTER 14

API v2: Discovery

The *Discovery* feature enables to search for servers and accounts on domain controllers and local accounts on Windows servers.

14.1 Data structures

Table 1: `DiscoveryModel`

Attribute	Type	Required	Description
account_id	number		Unique and read-only ID of the account to onboard/quarantine
server_id	number		Unique and read-only ID of the server to onboard/quarantine
rule_id	number		Read-only, protected ID of the rule used to onboard/quarantine
handled_by	number		Read-only, protected object identifier
state	string {onboarded, quarantined}	yes	Desired discovery state to be set
reason	string, may be empty	if `type == quarantined`	Quarantine reason description

Request for retrieving available attributes of the DiscoveryModel

Method	`GET`
Path	`/api/v2/objspec/discovery`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

14.2 Changing server's discovery state

Request

Method	`PATCH`
Path	`/api/v2/server/<server_id>/discovery`
Headers	`Content-Type: Application/JSON`
Body	`DiscoveryModel`

Example request

Sending `PATCH https://10.0.0.0/api/v2/server/1234567890123456798/discovery`

```
{
    "state": "onboarded"
}
```

Response

```
{
    "result": "success"
}
```

Example request

Sending `PATCH https://10.0.0.0/api/v2/server/1234567890123456789/discovery`

```
{
    "state":" quarantined",
    "reason": "Example text"
}
```

Response

```
{
    "result": "success"
}
```

Batch request example

```
{
    "requests": {
        "onboard_o": {
            "method": "PATCH",
            "endpoint": "/server/1234567890123456789/discovery",
            "data": {
                "state": "onboarded"
            }
        },
        "onboard_q": {
            "method": "PATCH",
            "endpoint": "/server/1234567890123456790/discovery",
            "data": {
                "state": "quarantined",
                "reason": "A quarantine reason"
            }
        }
    }
}
```

14.3 Changing account's discovery state

Request

Method	`PATCH`
Path	`/api/v2/account/<account_id>/discovery`
Headers	`Content-Type: Application/JSON`
Body	`DiscoveryModel`

Example request

Sending `PATCH https://10.0.0.0/api/v2/account/1234567890123456798/discovery`

```
{
    "state": "onboarded"
}
```

Response

```
{
    "result": "success"
}
```

Example request

Sending `PATCH https://10.0.0.0/api/v2/account/1234567890123456789/discovery`

```
{
    "state":" quarantined",
    "reason": "Example text"
}
```

Response

```
{
    "result": "success"
}
```

CHAPTER 15

API v2: Remote applications

Fudo Enterprise enables direct connection over the RDP protocol to a remote application using Remote Applications feature.

15.1 Data structures

Table 1: `RemoteApplicationsModel`

Attribute	Type	Required	Description
id	string		Read-only unique object Identifier
name	string	yes	Unique, case insensitive application name
path	string	yes	Path to application executable file
arguments	string		Definitions of which object and what property of object to use
created_at	string		Read-only
modified_at	string		Read-only
removed	boolean		Read-only

Request for retrieving available attributes of the RemoteApplicationsModel

Method	`GET`
Path	`/api/v2/objspec/remote_app`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

15.2 Retrieving remote applications definitions list

Request

Method	`GET`
Path	`/api/v2/remote_app`

Example request

Sending `GET https://10.0.0.0/api/v2/remote_app`


```
"result": "success",
"remote_app": [
    {
        "id": "1936547839769313283",
        "name": "RemoteApp1",
        "path": "/foldername/application1_executable_file",
        "created_at": "2022-12-13 02:53:32.427697-08",
        "modified_at": "2022-12-13 02:53:32.427697-08"
    },
    {
        "id": "1936547839769313284",
        "name": "RemoteApp2",
        "path": "/foldername/application2_executable_file",
        "created_at": "2022-12-13 02:53:44.722701-08",
        "modified_at": "2022-12-13 02:53:44.722701-08" }]
```


15.3 Deleting a remote application definition

Request

Method	`DELETE`
Path	`/api/v2/remote_app/<id>`

CHAPTER 16

API v2: Sessions management

16.1 Data structures

Note: The following data structure contains `read-only` fields for retrieving session data.

Table 1: `SessionsModel`

Attribute	Type	Description
id	string	Object Identifier
leader_session_id	string	Object Identifier
account_id	string	Account's Identifier, which was used for connection
listener_id	string	Listener's Identifier, which was used for connection
safe_id	string	Safe's Identifier, which was used for connection
server_id	string	Server's Identifier, which was used for connection
user_id	string	User's Identifier, which was used for connection
started_at	string	Datetime of the session's start
finished_at	string	Datetime of the session's end
handled_by	string	Object Identifier
-marked_safe_by	string	
terminate_at	string	Datetime of the session's termination
dump_mode	string {all, none, raw, noraw}	Session recording options

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Description
protocol	string{http, modbus, mysql, rdp, ssh, system, tcp, tds, telnet, tn3270, tn5250, vnc}	Used protocol for connection
source_ip	string	Source IP address
source_port	number	Port of the source IP address
destination_ip	string	Destination IP address
destination_port	number	Port of the destination IP address
paused	boolean	
retention_locked	boolean	
indexed	number	
-trusted_timestamp	string	
size	number	
reason	string	Reason of the session's termination or rejection
status	string {approved, disconnected, expired, rejected, terminated, waiting}	
active_time	number	
ml (Machine Learning)	SessionsMLModel	
pending_delete	boolean	
password_change	boolean	
checkout_forced	boolean	
created_at	string	Datetime of the record creation
modified_at	string	Datetime of the record modification
removed	boolean	
login_reason	string	Reason for user's connection
bits_per_pixel	string	Resolution options
height	string	Resolution options
width	string	Resolution options
command	string	Given command during a session
type	string	Session's type
subsystem	string	For example, `sftp`

Table 2: `SessionsMLModel`

Attribute	Type	Description
ml_threat_level	number	Detected threat level
ml_threat_level_min	number	Min threat level value
ml_threat_level_max	number	Max threat level value
ml_converted_at	string	Datetime of the session's processing
ml_finished_at	string	End datetime of the session's processing

Request for retrieving available attributes of the SessionsModel

Method	
	`GET`
Path	
	`/api/v2/objspec/session`

Table 3: `SessionBackupAssignmentModel`

Attribute	Type	Description
session_id	string	ID of the session to backup. Requires `backup_id": {}` or `backup_name: {}`.
session_ids	string-array	IDs of the sessions to backup. Requires `backup_id": {}` or `backup_name: {}`.
backup_id	string	ID of the backup target. Requires `session_id": {}` or `session_ids: {}`.
backup_name	string	Name of the backup target. Requires `session_id": {}` or `session_ids: {}`.

Request for retrieving available attributes of the SessionBackupAssignmentModel

Method	
	`GET`
Path	
	`/api/v2/objspec/session_backup`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the Sessions objects.

16.2 Retrieving sessions list

Request

Method	
	`GET`
Path	
	`/api/v2/session`

16.3 Retrieving a session

Request

Method	`GET`
Path	`/api/v2/session/<id>`

Example request

Sending `GET https://10.0.0.0/api/v2/session/41234678819172646916`


```
    {
"result": "success",
"session": {
    "id": "3927138875067084301",
    "leader_session_id": "3927138875067084301",
    "listener_id": "3927138875067073099",
    "user_id": "3927138875067072685",
    "safe_id": "3927138875067072584",
    "account_id": "3927138875067088645",
    "server_id": "3927138875067072586",
    "started_at": "2022-04-05 16:06:07.313862+02",
    "finished_at": "2022-04-05 16:07:58.65701+02",
    "dump_mode": "all",
    "protocol": "vnc",
    "source_ip": "10.2.0.0",
    "source_port": 65331,
    "destination_ip": "10.0.0.1",
    "destination_port": 5900,
    "paused": false,
    "retention_locked": false,
    "indexed": 2,
    "size": 371712,
    "status": "approved",
    "active_time": 60,
    "password_change": false,
    "checkout_forced": false,
    "created_at": "2022-04-05 16:06:07.316523+02",
    "modified_at": "2022-04-08 08:16:02.009606+02",
    "height": "768",
    "width": "1024"
}}
```


16.4 Modifying a session

Request

Method	`PATCH`
Path	`/api/v2/session/<id>`

16.5 Mark existing session for back up

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/backup/<backup_id>`

Example request

Sending `POST https://10.0.0.0/api/v2/session/2345678901234567890/backup/12345617890123456789`

Request

Method	`POST`
Path	`/api/v2/session_backup`
Headers	`Content-Type: Application/JSON`
Body	`SessionBackupAssignmentModel`

Example request

Sending `POST https://10.0.0.0/api/v2/session_backup`

```
{
"backup_name": "Backup_Target_Name",
"session_ids": [
        "2345678901234567890",
        "2345678901234567891"
]
}
```

Response


```
{
"result": "success",
"session_ids": [
        "2345678901234567890",
        "2345678901234567891"
        ]
}
```

CHAPTER 17

API v2: Listeners

Listener determines server connection mode (proxy, gateway, transparent, bastion) as well as its specifics.

17.1 Data structures

Table 1: `ListenerModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
name	string	yes	Unique listener's name
blocked	boolean; default value `false`	yes	
reason	string	if `blocked` == `true`	
announcement	string	no	
ignore_case	boolean; default value `false`	If `protocol` == `vnc` || `ssh`	
legacy_crypto	boolean; default value `false`	If `protocol` == `ssh` || `http` || `rdp` & `tls_enabled` == `true`	Enabling legacy cryptographic protocols and settings
protocol	string {http, modbus, mysql, rdp, ssh, system, tcp, tds, telnet, tn3270, tn5250, vnc}	yes	Immutable, case insensitive
mode	string {bastion, gateway, proxy, transparent}	yes	Case insensitive

Continued on next page

Table 1 – continued from previous page

Attribute	Type	Required	Description
listen_interface	string	If `mode` == `gateway` || `transparent`	Network interface for user connections
listen_ip	string; default value `0.0.0.0`	If `mode` == `bastion` || `proxy`	IP address for user connections
listen_port	number; value range from `1` to `60000`	If `mode` == `bastion` || `proxy`	Port number for user connections
external_address	string	with `external_port`	Listener address to present in Access Gateway
external_port	number; value range from `1` to `65535`	with `external_address`	Listener port to present in Access Gateway
http_render	boolean; default value `true`	If `protocol` == `http`	Is graphical representation for HTTP(S) sessions enabled?
private_key_passphrase	string	with `rdp_private_key` or `ssh_private_key` or `tls_private_key`	Passphrase to use to decrypt private key.
rdp	ListenerRDPAttributes	If `protocol` == `rdp`	RDP protocol properties
ssh	ListenerSSHAttributes	If `protocol` == `ssh`	SSH protocol properties
tls	ListenerTLSAttributes	If `protocol` == `http` || `rdp`	TLS protocol properties
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
builtin	boolean		Read-only; Expensive to use; If `true`, the object is not editable.
hidden	boolean		Read-only; Expensive to use; If `true`, the object is hidden in UI.

Table 2: `ListenerRDPAttributes`

Attribute	Type	Required	Description
rdp_private_key	string	If `protocol` == `rdp` & `tls_enabled` == `false`	RDP private key
rdp_public_key	string	If `protocol` == `rdp` & `tls_enabled` == `false`	RDP public key

Table 3: `ListenerSSHAttributes`

Attribute	Type	Required	Description
ssh_private_key	string	yes	SSH private key
ssh_proxyjump	boolean; default value `false`	yes	Is SSH ProxyJump function enabled?
ssh_public_key	string	yes	Read-only SSH public key
ssh_fingerprint_sha256	string	If `protocol == ssh`	Read-only, expensive to use, SSH key SHA256 fingerprint

Table 4: `ListenerTLSAttributes`

Attribute	Type	Required	Description
tls_enabled	boolean; default value `true`	If `protocol == http || rdp`	Enabling the TLS protocol
tls_private_key	string	If `protocol == http || rdp` & `tls_enabled == true`	TLS private key
tls_certificate	string	If `protocol == http || rdp` & `tls_enabled == true`	TLS certificate
tls_certificate_commonname	string	If `protocol == http || rdp` & `tls_enabled == true`	Read-only, expensive to use, TLS certificate `commonName`
tls_certificate_fingerprint_sha1	string	If `protocol == http || rdp` & `tls_enabled == true`	Read-only, expensive to use, TLS certificate SHA1 fingerprint
tls_certificate_fingerprint_sha256	string	If `protocol == http || rdp` & `tls_enabled == true`	Read-only, expensive to use, TLS certificate SHA256 fingerprint

Request for retrieving available attributes of the ListenerModel

Method

```
GET
```

Path

```
/api/v2/objspec/listener
```

Table 5: `AccountSafeListenerAssignmentModel`

Attribute	Type	Required	Description
id	string	yes	Read-only object Identifier
account_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `account_id` with attributes `safe_id` and `listener_id`.
safe_id	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attributes `account_id` and `listener_id`.
listener_id	string	no	Immutable. Uniqueness is required in the combination of attribute `listener_id` with attributes `account_id` and `safe_id`.
account_name	string		Read-only; expensive to use
account_type	string		Read-only; expensive to use
protocol	string		Read-only; expensive to use
server_id	string		Read-only; expensive to use; `null` if pool is assigned.
server_name	string		Read-only; expensive to use; `null` if pool is assigned.
pool_id	string		Read-only; expensive to use; `null` if server is assigned.
pool_name	string		Read-only; expensive to use; `null` if server is assigned.
safe_name	string		Read-only; expensive to use
listener_name	string		Read-only; expensive to use
created_at	datetime		Read-only
modified_at	datetime		Read-only
removed	boolean		Read-only
builtin	boolean		Read-only; expensive to use; if `true`, the object is not editable.
hidden	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.

Request for retrieving available attributes of the AccountSafeListenerAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/account_safe_listener`

Table 6: `ListenerGrantAssignmentModel`

Attribute	Type	Required	Description
id	string		Read-only, protected object Identifier
to_user_id	string	yes	Immutable. Expects unique `for_listener_id`
for_listener_id	string	yes	Immutable. Expects unique `to_user_id`
for_listener_name	string		Read-only, expensive to use
to_user_name	string		Read-only, expensive to use
to_user_role	string		Read-only, expensive to use
created_at	string		Read-only
modified_at	string		Read-only
removed	boolean		Read-only

Request for retrieving available attributes of the ListenerGrantAssignmentModel

Method	`GET`
Path	`/api/v2/objspec/listener_grant`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

Refer to the *Batch operations* topic to create nested requests for operating on the Listener objects.

17.2 Retrieving listeners list

Request

Method	`GET`
Path	`/api/v2/listener`

Example request

Sending `GET https://10.0.0.0/api/v2/listener`

```
    "result": "success",
"listener": [
    {
        "id": "1234138875067073217",
        "name": "rdp_list_fd_10647",
        "protocol": "rdp",
        "mode": "bastion",
        "listen_ip": "0.0.0.0",
        "listen_port": 3388,
        "blocked": false,
        "created_at": "2022-10-15 14:52:30.980597+02",
        "modified_at": "2022-10-15 14:52:30.980597+02",
        "legacy_crypto": false,
        "tls_enabled": true,
        "tls_certificate": "-----BEGIN CERTIFICATE-----\nMIIEODCCArigAwIBAgIUSGWBY/C..
↪.0w/BXGR\n-----END CERTIFICATE-----"
    },
    {
        "id": "1234138875067073219",
        "name": "telnet_proxy_3",
        "protocol": "telnet",
        "mode": "proxy",
        "listen_ip": "0.0.0.0",
        "listen_port": 2236,
        "blocked": false,
        "created_at": "2022-10-17 09:34:32.582169+02",
        "modified_at": "2022-10-17 09:34:32.582169+02"
    },
    {
        "id": "12348875067073220",
        "name": "mssql_proxy",
        "protocol": "tds",
        "mode": "proxy",
        "listen_ip": "0.0.0.0",
        "listen_port": 8874,
        "blocked": false,
        "created_at": "2022-10-17 10:50:53.209773+02",
        "modified_at": "2022-10-17 10:50:53.209773+02" }]
```


17.3 Creating a listener

Request

Method	`POST`
Path	`/api/v2/listener`
Headers	`Content-Type: Application/JSON`
Body	`ListenerModel`

17.4 Retrieving a listener

Request

Method	`GET`
Path	`/api/v2/listener/<id>`

17.5 Modifying a listener

Request

Method	`PATCH`
Path	`/api/v2/listener/<id>`
Headers	`Content-Type: Application/JSON`
Body	`ListenerModel`

Example request: Changing the listener's address

Sending `PATCH https://10.0.0.0/api/v2/listener/12345678819172646915`

```
{ "listen_ip": "10.0.2.0" }
```

Response

```
{ "result": "success" }
```

17.6 Retrieving users allowed to manage given listener

Request

Method	`GET`
Path	`/api/v2/grant/listener`

17.7 Granting management privileges

Request

Method	`POST`
Path	`/api/v2/grant/listener`

Body	`{`
	`to_user_id: 1234567890,`
	`for_listener_id: 1234567891`
	`}`

17.8 Creating an account-safe-listener assignments

Request

Method	`POST`
Path	`/api/v2/account/safe/listener`
Headers	`Content-Type: Application/JSON`
Body	`AccountSafeListenerAssignmentModel`

Example request

Sending `POST https://10.0.0.0/api/v2/account/safe/listener`

```
    { "account_id": 1232678819172646919,
"safe_id": 1232678819172646913,
"listener_id": 1232678819172646914 }
```

Response

```
    { "result": "success",
"account_safe_listener": {} }
```

17.9 Deleting an account-safe-listener assignment

Request

Method	`DELETE`
Path	`/api/v2/account/<account_id>/safe/<safe_id>/listener/<listener_id>`

17.10 Deleting a listener

Request

Method	`DELETE`
Path	`/api/v2/listener/<id>`

CHAPTER 18

API v2: Batch requests

Fudo Enterprise allows using its API for sending a batch request by which an administrator can perform nested operations with different methods. Creating an account and assigning an authentication method to it or defining 100 servers in one request is possible with an endpoint `/batch`.

Note: The `/batch` endpoint is available to use on objects of API v2 only.

18.1 Data structures

Table 1: `BatchModel`

Batch operation element	Possible values / Request variant	Description
`atomic`	`true`, `false`	Set a global value `atomic=true` to ensure that all requests within a batch operation are executed. In case of failure of any request, the entire operation will be reverted.
`variables`		Define variables to facilitate future referencing of responses.
`requests:`		Remember to give your request a unique ID that consist of characters matching any single character from the following set: lowercase letters (a-z), uppercase letters (A-Z), digits (0-9), hyphens (-), colons (:), or underscores (_).
	`method`	Use one of the available methods per request.
	`endpoint`	Use one of the available endpoints per request.
	`params`	Include optional URL parameters.

Continued on next page

Table 1 – continued from previous page

Batch operation element	Possible values / Request variant	Description
	`data`	Include optional attributes values or variables for the future responses of the previous requests.
	`atomic`	Override global `atomic=true` with a local `atomic=false`.

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

18.2 Creating a batch operation

Request

Method	`POST`
Path	`/api/v2/batch`
Headers	`Content-Type: Application/JSON`
Body	`BatchModel`

Example of a batch operation that contains four requests:

- `request0` returns a list of users' IDs and names, where the user's `name` == `test`,
- `request1` deletes the first user that was on the list of the `request0`'s response,
- `request2` creates a new user with `name` of the first user from the `request0`'s response and assigns a role `user` to it,
- `request3` assigns `password` as an authentication method for the user that was created in the `request2`

Example request

```
{
  "requests": {
    "request0": {
      "method": "GET",
      "endpoint": "/user",
      "params": {
        "filter": "name.eq(test)",
        "fields": "id,name"
```

(continues on next page)

(continued from previous page)

```
      }
    },
    "request1": {
      "method": "DELETE",
      "endpoint": "/user/{responses.request0.user[0].id}"
    },
    "request2": {
      "method": "POST",
      "endpoint": "/user",
      "data": {
        "name": "{responses.request0.user[0].name}",
        "role": "user"
      }
    },
    "request3": {
      "method": "POST",
      "endpoint": "/user/{responses.request2.user.id}/authentication",
      "data": {
        "type": "password",
        "position": 0,
        "secret": "abcd.8"
      }
    }
  }
}
```

Response

```
{
    "result": "success",
    "responses": {
        "request0": {
            "result": "success",
            "status-code": 200,
            "user": [
                {
                    "id": "8511803295730237462",
                    "name": "test"
                }
            ]
        },
        "request1": {
            "result": "success",
            "status-code": 200
        },
        "request2": {
            "result": "success",
            "status-code": 201,
            "user": {
                "id": "8511803295730237463"
            }
        },
        "request3": {
            "result": "success",
            "status-code": 201,
            "user_authentication_method": {
```

(continues on next page)

(continued from previous page)

```
                "id": "8511803295730237489"
            }
        }
    }
}
```

18.3 Creating a batch operation using variable

The example below demonstrates a batch operation with `"username": "jdoe"` variable defined. This variable was used to dynamically populate the `name` field in the `user_1` request. Next, the `user_auth` request includes `{responses.user_1.user.id}` (`{responses.<response-id>.user.id}`), which is a placeholder that will be replaced with the actual `id` value generated from the response of the `user_1` request.

Request

```
{
  "variables": {
    "username": "jdoe"
  },
  "requests": {
    "user_1": {
      "method": "POST",
      "endpoint": "/user",
      "data": {
        "name": "{variables.username}"
      }
    },
    "user_auth": {
      "method": "POST",
      "endpoint": "/user/{responses.user_1.user.id}/authentication",
      "data": {
        "type": "password",
        "position": 0,
        "secret": "test123"
      }
    }
  }
}
```

Response

```
{
    "result": "success",
    "responses": {
        "user_1": {
            "result": "success",
            "status-code": 201,
            "user": {
                "id": "8511803295730237446"
            }
        },
        "user_auth": {
```

(continues on next page)

(continued from previous page)

```
            "result": "success",
            "status-code": 201,
            "user_authentication_method": {
                "id": "8511803295730237442"
            }
        }
    }
}
```

18.4 Atomic functionality

The example below demonstrates a batch operation that includes two requests (`user0` and `user1`) for creating two users, where `user0` request has invalid value (`not_defined`) set for the `role` attribute. While the global `atomic` function is enabled for the batch operation, it is disabled solely for the `user0` request. As a result, only user from the `user1` request will be created.

Example request

```
{
  "atomic": true,
  "variables": {
    "user_name_0": "jdoe",
    "user_name_1": "jsmith"
  },
  "requests": {
    "user0": {
      "method": "POST",
      "endpoint": "/user",
      "atomic": false,
      "data": {
        "name": "{variables.user_name_0}",
        "role": "not_defined"
      }
    },
    "user1": {
      "method": "POST",
      "endpoint": "/user",
      "data": {
        "name": "{variables.user_name_1}",
        "role": "operator"
      }
    }
  }
}
```

Response

```
{
    "result": "success",
    "responses": {
        "user0": {
            "result": "failure",
            "status-code": 400,
```

(continues on next page)

(continued from previous page)


```
            "message": "Invalid value of attribute role: 'not_defined'
                (expected values=[ 'admin', 'operator', 'service', 'superadmin', 'user
↪' ]).",
            "failing_attributes": [
                "role"
            ]
        },
        "user1": {
            "result": "success",
            "status-code": 201,
            "user": {
                "id": "8511803295730237444"
            }
        }
    }
}
```

CHAPTER 19

API v2: External password repository

Fudo Enterprise supports external passwords repositories for managing passwords to monitored servers.

19.1 Data structures

Table 1: `PassvnModel`

Attribute	Type	Required	Description
id	string		Unique, read-only object Identifier
name	string	yes	Unique, case insensitive object name
url	string	yes	URL to the passwords server's API
type	string{cyberark_legacy, cyberark, laps, thycotic}	yes	Immutable
login	string	If `type == laps || thycotic`	
secret	string	If `type == laps || thycotic`	Protected
tls_certificate	string		
cyberark_legacy_account_fmt	string	If `type == cyberark_legacy`	
cyberark_application	string	If `type == cyberark_legacy || cyberark`	id
cyberark_safe	string	If `type == cyberark`	
thycotic_secret_fmt	string	If `type == tyhotic`	
base_dn	string	If `type == laps`	
identity_cert	string		
identity_key	string		Protected
created_at	string		Read-only
modified_at	string		Read-only
removed	string		Read-only

Request for retrieving available attributes of the PassvnModel

Method	`GET`
Path	`/api/v2/objspec/passvn`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

The next chapter describes procedures for creating separate requests.

19.2 Creating external password repository

Request

Method	`POST`
Path	`/api/v2/passvn`
Headers	`Content-Type: Application/JSON`
Body	`PassvnModel`

Example request

Sending `POST https://10.0.0.0/api/v2/passvn`

```
{
    "type": "laps",
    "name": "LAPS Test Name 2",
    "url": "ldaps://10.2.0.1:8636/",
    "login": "cn=admin,dc=fudosecurity,dc=lab",
    "secret": "passwordExample",
    "base_dn": "dc=fudosecurity,dc=lab"
}
```

Response

```
{
    "result": "success",
    "passvn": {
        "id": "123456789012345678"
```

(continues on next page)

(continued from previous page)

```
    }
}
```

19.3 Retrieving external password repositories list

Request

Method	
	`GET`

Path	
	`/api/v2/passvn`

Example request

Sending `GET https://10.0.0.0/api/v2/passvn`

Response

```
"result": "success",
"passvn": [
    {
        "id": "123456789012345679",
        "name": "LDAP Test Name",
        "url": "ldaps://10.2.0.100:8636/",
        "type": "laps",
        "login": "cn=admin,dc=fudosecurity,dc=lab",
        "base_dn": "dc=fudosecurity,dc=lab",
        "created_at": "2023-06-16 02:53:08.930597-07",
        "modified_at": "2023-06-16 02:53:08.930597-07"
    }
]
```

19.4 Deleting an external password repository definition

Request

Method	
	`DELETE`

Path	
	`/api/v2/passvn/<id>`

19.5 Changing external password repository configuration

Request

Method	`PATCH`
Path	`/api/v2/passvn/<id>`
Headers	`Content-Type: Application/JSON`
Body	`PassvnModel`

Example request

Sending `PATCH https://10.0.0.0/api/v2/passvn/123456789012345679`

```
{
   "login": "cn=admin,dc=fudosecurity,dc=com",
   "base_dn": "dc=fudosecurity,dc=com"
}
```

Response

```
{
   "result": "success"
}
```

CHAPTER 20

API v2: Network

Fudo Enterprise allows retrieving network settings within its API.

Note: Network settings are accessible for the users with `superadmin` privileges.

20.1 Data structures

Table 1: `NetworkModel`

Attribute	Type	Description
hostname	string	
dns	address	DNS address(es)
management	address	Admin Panel's address
access_gateway	address	Access Gateway's address
labels	string	Global configuration parameters
interfaces		Network interfaces configuration
	name	
	ether	
	active {true, false}	
	use_dhcp {true, false}	
	routing_table	
	inet	
routing		Routing configuration
	tables_max_count	Max number of the routing tables is 8
	tables {table[id]}	ID of the routing table
	routes {network, gateway}	Network and gateway addresses

20.2 Retrieving network settings

Request

Method	`GET`
Path	`/api/v2/network`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

CHAPTER 21

API v2: Healthcheck

By using *healthcheck*, you can check the overall Fudo Enterprise health and verify its proper functioning. This method is accessible without authentication.

Note:

- *Healthcheck* is disabled by default. Please go to *Settings* > *System*, and enable the *API health check* option on the *General* tab, under the *Maintenance and supervision section*.

21.1 Retrieving healthcheck status

Request

Method	`GET`
Path	`/api/v2/healthcheck`

Example request

Sending `GET https://10.0.0.0/api/v2/healthcheck`

Response - positive

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

Response - negative

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

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

CHAPTER 22

API v2: Status

The *Status* method allows retrieving detailed information about the Fudo Enterprise status including:

- Cluster status.
- The temperature of CPU cores in degrees Celsius.
- Database server status.
- Disks status.
- Fudo unique identifier.
- System load.
- Device memory utilization.
- Power supply units status.
- Device serial number.
- Number of currently active sessions.
- Status of last system shutdown or reboot.
- SMART attributes of disks.
- Device storage utilization.
- Status of last attempted firmware upgrade.
- System uptime.
- Firmware version.

Note:

- The *Status* method requires authentication.
- It is accessible for every user role.

22.1 Retrieving status information

Request

Method	`GET`
Path	`/api/v2/status`

Example request

Sending `GET https://10.0.0.0/api/v2/status`

Note: To check allowed methods, available URL parameters and possible responses please refer to the *API overview* section.

CHAPTER 23

API usage examples

Refer to the particular object page to see actual examples.

Inform us if more examples is needed.