Fudo Enterprise 6.2 - API documentation

Fudo Security

27.08.2026

GETTING STARTED

CHAPTER

ONE

TABLE OF CONTENTS

1.1 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

All trademarks, product names, and company names or logos cited in this document are the property of their respective owners and are used for information purpose only.

1.2 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**
>
> You may still come across references to **APIv1** in some materials. This older version has been fully retired starting from Fudo Enterprise 5.6. The current interface is called **APIv2** to distinguish it from the legacy version that was in use earlier.

1.2.1 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.

1.2.2 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"
          }
}
```

1.2.3 Request Format

> **Note**
>
> You may still come across references to **APIv1** in some materials. This older version has been fully retired starting from Fudo Enterprise 5.6. The current interface is called **APIv2** to distinguish it from the legacy version that was in use earlier.

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 /api/v2/user

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user' \
```

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

POST /api/v2/user

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
      -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/user' \
  -d '{
        "role": "user",
        "name": "test-user"
  }'
```

1.2.4 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.

1.2.5 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`

1.2.6 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 • ...

continues on next page

Table 1 – continued from previous page

Object type	Endpoints example
server	• /server • /server/<id> • ...
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",
    "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 refer to section *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 *Network* section.

1.2.7 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:

Example Request

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

Filter

This parameter defines the criteria used to limit the results returned in the query response.

> **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

Search parameter defines a search phrase and limits the search to specific attributes.

Note

Please note that certain search constraints are applied automatically depending on the user's role.

This parameter narrows out the result with available additions:

- `search.match()` - include a regular expression to be searched in selected fields,
- `search.imatch()` - case insensitive version of `search.match()`.

Note

When using the `search` parameter with multiple attributes separated by a comma (e.g., `search=name,address`), the search condition applies to all given attributes. In this situation, at least one of the given attributes must match the condition.

Example Request

```
GET https://10.0.0.0/api/v2/server?\
    search=name,address&filter=search.imatch(ssh)
```

Example Request

```
GET https://10.0.0.0/api/v2/user?\
    search=name,login&filter=search.match(^admin)
```

Search can be combined with other filters. In such cases, all given conditions must be met.

Example Request

```
GET https://10.0.0.0/api/v2/server?\
    search=name,address&filter=search.imatch(prod),port.eq(22)
```

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`.

Example Request

```
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": "918734323983581188",
             "name": "RDP_server_2",
             "protocol": "rdp"
         },
         {
             "id": "918734323983581187",
```

(continues on next page)

(continued from previous page)


```
            "name": "RDP_server",
            "protocol": "rdp"
        },
        {
            "id": "918734323983581186",
            "name": "windows.example.org",
            "protocol": "rdp"
        },
        {
            "id": "918734323983581189",
            "name": "SSH_server",
            "protocol": "ssh"
        },
        {
            "id": "918734323983581185",
            "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:

Example Request

```
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):

Example Request

```
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:

Example Request

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

Response


```
{
    "result": "success",
    "server": [
        {
            "id": "918734323983581188",
            "name": "RDP_server_2",
            "protocol": "rdp"
        },
        {
            "id": "918734323983581187",
            "name": "RDP_server",
            "protocol": "rdp"
        },
        {
            "id": "918734323983581186",
            "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",
```


(continues on next page)

(continued from previous page)

```
            "endpoint_execute duration": "0.002087s",
            "total duration": "0.008025s"
        }
    }
}
```

Total Count

`total_count` 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

`estimated_total_count` 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.

1.2.8 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-a` • `string-a`	`string`	Attribute's type in JSON requests.

continues on next page

Table 2 – continued from previous page

Property	Possible values	Default value	Description
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.
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.

continues on next page

Table 2 – continued from previous page

Property	Possible values	Default value	Description
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: • `<attribu` or: • `[ <attribu ... ]`	`false`	The given attribute is unique by itself (when `true`) or is unique when combined with other attributes.
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.
capability	`{ objtype: <string>, <HTTP method>: <right>, ... }`	None	Defines role-based access requirements (RBAC) for accessing or modifying the object via a specific API method. The object type (objtype) specifies the protected resource (e.g. account), while each HTTP method (e.g. GET, POST, PATCH, DELETE) maps to a required right (e.g. read, write). For example, GET: read on account means that to retrieve object via GET, the user must have the read right on the account object type.

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" ]
}
```

1.2.9 API BETA Endpoints

Endpoints in the `/beta` and `/internal` namespace are subject to change without notice. These endpoints are considered experimental and may undergo modifications, deprecations, or removals as we continue to refine and improve the API.

It is recommended to use these endpoints with caution and not to rely on them for production-level applications. Always check for updates and changes regularly when using `/beta` or `/internal` endpoints.

Note

For production environments, it is advisable to use the stable endpoints. The `/beta` and `/internal` endpoints are intended for testing and development purposes only.

1.3 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.

1.3.1 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 -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/user'
```

1.3.2 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.

1.4 Role-Based Access Control and User Groups

Roles implement Role-Based Access Control (RBAC), providing granular and flexible control over user permissions.

The **RBAC (Role-Based Access Control)** functionality in Fudo Enterprise allows system administrators to define precise roles with specific access permissions tailored to objects and operations. This enables the creation of roles designed for particular tasks, such as a role that grants permissions solely for user management—allowing the creation, editing, and deletion of users—without affecting other areas of the system.

1.4.1 Definitions

Privilege A permission to perform a specific action in the system. It may apply to all objects of a given type (e.g., modifying secret changers, creating servers) or be unrelated to any object (e.g., upgrading Fudo).

Capability Access granted to a subject for a specific object. A capability defines on which object the assigned privileges can be used.

Right A specific permission within a capability — it defines what operations can be performed on the assigned object (e.g., the ability to block a user specified by the capability).

Subject The entity that holds permissions — either a user or a group.

Object The target of the permissions. Currently supported object types are: user, safe, account, pool, group, and server.

1.4.2 Privileges

Data Structures

Table 3: `PrivilegeModel`

Attribute	Type	Required	Description
`bit`	number	yes	Unique; Read-only; hidden.
`name`	string	yes	Unique; Read-only.
`description`	string	yes	Read-only.

Retrieve Available Attributes of the *PrivilegeModel*

Request

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

GET /api/v2/objspec/privilege

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/privilege'
```

Get List of Available Privileges

Request

Method	`GET`
Path	`/api/v2/privilege`

GET /api/v2/privilege

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/privilege'
```

Response


```
{
    "result": "success",
    "privilege": [
        {
            "name": "account-create",
            "description": ""
        },
        {
            "name": "account-read",
            "description": ""
        },
        {
            "name": "account-modify",
            "description": ""
        },
        {
            "name": "account-delete",
            "description": ""
        },
        {
            "name": "account-block",
            "description": ""
        },
        {
            "name": "group-create",
            "description": ""
        },
        {
            "name": "webapp-session-timeout",
            "description": "Fudo Admin Panel and User Access Gateway session␣
↪timeout configuration"
        }
        // ... more privileges
    ]
}
```


1.4.3 Roles

Data Structures

Table 4: `RoleModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier.
`name`	string	yes	Case-insensitive. Unique.
`description`	string		
`in_use`	boolean		Read-only; expensive to use.
`privs`	string-array	yes	Read-write; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

Retrieve Available Attributes of the *RoleModel*

Request

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

GET /api/v2/objspec/role

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/role'
```

Get Roles List

Request

Method	`GET`
Path	`/api/v2/role`

GET /api/v2/role

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/role'
```

Response

```
{
    "result": "success",
    "role": [
        {
            "id": "9115285645797883905",
            "name": "superadmin",
            "privs": [
                "account-create",
                "account-read",
                "account-modify",
                "..."
            ],
            "created_at": "2025-04-25 01:40:11.204397-07",
            "modified_at": "2025-04-25 01:40:11.204397-07",
            "builtin": false,
            "hidden": false
        },
        {
            "id": "9115285645797883910",
            "name": "viewer",
            "privs": [
                "user-session-view",
                "dashboard"
            ],
            "created_at": "2025-04-25 01:40:11.20449-07",
            "modified_at": "2025-04-25 01:40:11.20449-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```


Get Role by ID

Request

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

GET /api/v2/role/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/role/9115285645797883910'
```

Response

```
{
    "result": "success",
    "role": {
        "id": "9115285645797883910",
        "name": "viewer",
        "privs": [
            "user-session-view",
            "dashboard"
        ],
        "created_at": "2025-04-25 01:40:11.20449-07",
        "modified_at": "2025-04-25 01:40:11.20449-07",
        "builtin": false,
        "hidden": false
    }
}
```


Create Role

Request

Method	`POST`
Path	`/api/v2/role`
Headers	`Content-Type: application/json`
Body	`RoleModel`

POST /api/v2/role

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/role' \
  -d'{"name": "Role_Session_Viewer","privs": ["user-session-view","dashboard"]}'
```

Response


```
{
    "result": "success",
    "role": {
        "id": "9115285645797883911"
    }
}
```


Modify Role

Request

Method	PATCH
Path	/api/v2/role/<id>
Headers	Content-Type: application/json
Body	RoleModel

PATCH /api/v2/role/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/role/9115285645797883911' \
  -d'{"name": "Role_Session_Manager","privs": ["session-read","session-modify",
↪"session-delete","session-encode","session-file-read","session-file-download",
↪"session-file-delete","session-movie-read","session-movie-download","session-
↪share-view","session-share-join","session-comment-read","session-comment-write
↪","session-terminate","session-export"]}'
```

Response

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

Grant Privileges to Role

Request

Method	PATCH
Path	/api/v2/role/<id>/grant
Headers	Content-Type: application/json
Body	RoleModel

PATCH /api/v2/role/<id>/grant

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/role/9115285645797883912/grant' \
  -d'{"privs": ["session-read","session-modify"]}'
```

Response

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

Revoke Privileges from Role

Request

Method	`PATCH`
Path	`/api/v2/role/<id>/revoke`
Headers	`Content-Type: application/json`
Body	`RoleModel`

PATCH /api/v2/role/<id>/revoke

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/role/9115285645797883912/revoke' \
  -d'{"privs": ["session-read","session-modify"]}'
```

Response

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

Delete Role

Request

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

DELETE /api/v2/role/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/role/9115285645797883911'
```

Response

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

1.4.4 User-Role Assignment

Data Structures

Table 5: `UserRoleModel`

Attribute	Type	Required	Description
`id`	string		Read-only; protected. Unique identifier.
`user_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `role_id`. Requires `read` right on the `user` object for GET requests.
`role_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `role_id` with attribute `user_id`.
`role_name`	string		Read-only; expensive to use.
`user_name`	string		Read-only; expensive to use.
`user_blocked`	boolean		Read-only; expensive to use; `blocked` state of the assigned user.
`privs`	string-array		Read-only; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

Retrieve Available Attributes of the *UserRoleModel*

Request

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

GET /api/v2/objspec/user_role

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/user_role'
```

Get User-Role Assignment List

Request

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

GET /api/v2/user/role

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user/role'
```

Response


```
{
  "result": "success",
  "user_role": [
    {
      "user_id": "9115285645797883905",
      "role_id": "9115285645797883905",
      "role_name": "superadmin",
      "user_name": "admin",
      "privs": [
        "account-create",
        "account-read",
        "account-modify",
        "..."
      ],
      "created_at": "2025-04-25 01:40:11.204397-07",
      "modified_at": "2025-04-25 01:40:11.204397-07",
      "builtin": false,
      "hidden": false
    },
    {
      "user_id": "9115285645797883908",
      "role_id": "9115285645797883908",
      "role_name": "operator",
      "user_name": "remoteapp",
      "privs": [
        "user-session-view",
        "listener-read",
        "notification-filter-create",
        "notification-filter-read",
        "..."
      ],
      "created_at": "2025-05-07 05:17:40.584837-07",
      "modified_at": "2025-05-07 05:17:40.584837-07",
      "builtin": false,
      "hidden": false
    }
  ]
}
```

Get Role Assigned to a User by Their IDs

Request

Method	GET
Path	/user/<user_id>/role/<role_id>

GET /api/v2/user/<user_id>/role/<role_id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user/9115285645797883905/role/9115285645797883905'
```

Response

```
{
    "result": "success",
    "user_role": {
        "user_id": "9115285645797883905",
        "role_id": "9115285645797883905",
        "role_name": "superadmin",
        "user_name": "admin",
        "privs": [
            "account-create",
            "account-read",
            "account-modify",
            "account-delete",
                        "..."
        ],
        "created_at": "2025-04-25 01:40:11.206421-07",
        "modified_at": "2025-04-25 01:40:11.206421-07",
        "builtin": false,
        "hidden": false
    }
}
```

Create User-Role Assignment

Request

Method	POST
Path	/api/v2/user/role
Headers	Content-Type: Application/json
Body	UserRoleModel

POST /api/v2/user/role

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
      -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/user/role' \
      -d'{"user_id":"9115285645797883905","role_id":"9115285645797883908"}'
```

Response

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

Delete User-Role Assignment

Request

Method	DELETE
Path	/api/v2/user/<user_id>/role/<role_id>

DELETE /api/v2/user/<user_id>/role/<role_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/user/9115285645797883905/role/
↪9115285645797883908'
```

Response

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

1.4.5 Groups

Endpoints in this section allow you to create groups and modify their name and description. To assign safes, users, and configure object permissions, refer to the following sections: *Group-Safe Assignment*, *Group-Safe-TimePolicy Management*, and *Group-User Assignment*.

Data Structures

Table 6: `GroupModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier. Requires rights to perform operations on the `group` object: `read` for GET, `modify` for PATCH, `delete` for DELETE.
`name`	string	yes	Unique. Case-insensitive.
`description`	string		
`scim_managed`	boolean	yes	Default: false.
`external_id`	string		Unique.
`rights`	string-array		Read-only. List of rights the subject has to this object.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *GroupModel*

Request

GET /api/v2/objspec/group

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/group'
```

Get Groups List

Request

Method	`GET`
Path	`/api/v2/group`

GET /api/v2/group

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group'
```

Response

```
{
    "result": "success",
    "group": [
```

(continues on next page)

(continued from previous page)


```
        {
            "id": "9115285645797883905",
            "name": "admin",
                        "scim_managed": false,
            "rights": [
                "read",
                "modify",
                "delete",
                "user-add",
                "user-remove"
            ],
            "created_at": "2025-04-28 03:59:56.247996-07",
            "modified_at": "2025-04-28 03:59:56.247996-07"
        },
        {
            "id": "9115285645797883906",
            "name": "QA_team",
                        "scim_managed": false,
            "rights": [
                "read",
                "modify",
                "delete",
                "user-add",
                "user-remove"
            ],
            "created_at": "2025-04-30 02:18:18.651517-07",
            "modified_at": "2025-04-30 02:18:18.651517-07"
        }
    ]
}
```


Get Group by ID

Request

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

GET /api/v2/group/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group/9115285645797883905'
```

Response

```
{
    "result": "success",
    "group": {
        "id": "9115285645797883905",
        "name": "admin",
                "scim_managed": false,
        "rights": [
            "read",
            "modify",
            "delete",
            "user-add",
            "user-remove"
        ],
        "created_at": "2025-04-28 03:59:56.247996-07",
        "modified_at": "2025-05-07 23:55:40.907653-07"
    }
}
```


Create Group

Request

Method	`POST`
Path	`/api/v2/group`
Headers	`Content-Type: Application/json`
Body	`GroupModel`

POST /api/v2/group

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/group' \
  -d'{"name": "QA_Team","description": "Members of QA responsible for..."}'
```

Response


```
{
    "result": "success",
    "group": {
        "id": "9115285645797883908"
    }
}
```

Modify Group

Request

Method	PATCH
Path	/api/v2/group/<id>
Headers	Content-Type: Application/json
Body	GroupModel

PATCH /api/v2/group/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/group/9115285645797883911' \
  -d'{"name": "Dev_Team","description": "Members of DEV responsible for..."}'
```

Response

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

Delete Group

Request

Method	DELETE
Path	/api/v2/group/<id>

DELETE /api/v2/group/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/group/9115285645797883911'
```

Response

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

1.4.6 Group-Safe Assignment

Endpoints in this section allow you to assign safes to groups.

Data Structures

Table 7: `GroupSafeModel`

Attribute	Type	Required	Description
`id`	string		Read-only; protected. Unique identifier.
`group_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `group_id` with attribute `safe_id`. Requires `read` right on the `group` object for all operations.
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `group_id`. Requires rights on the `safe` object: `read` for GET, `group-add` for POST and PATCH, `group-remove` for DELETE.
`password_visib`	boolean; default value `false`	yes	
`use_time_polic`	boolean; default value `false`	yes	
`blocked`	boolean; default value `false`	yes	Access to this safe is disabled for the group.
`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.
`group_name`	string		Read-only; expensive to use.
`safe_name`	string		Read-only; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

Retrieve Available Attributes of the *GroupSafeModel*

Request

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

GET /api/v2/objspec/group_safe

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/objspec/group_safe'
```

Get Group-Safe Assignment List

Request

Method	GET
Path	/api/v2/group/safe

GET /api/v2/group/safe

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group/safe'
```

Response


```
{
    "result": "success",
    "group_safe": [
        {
            "group_id": "9115285645797883905",
            "safe_id": "9115285645797883906",
            "password_visible": false,
            "use_time_policy": false,
            "group_name": "admin",
            "safe_name": "RDP",
            "created_at": "2025-05-07 23:56:15.424739-07",
            "modified_at": "2025-05-07 23:56:15.424739-07",
            "builtin": false,
            "hidden": false
        },
        {
            "group_id": "9115285645797883905",
            "safe_id": "9115285645797883907",
            "password_visible": false,
            "use_time_policy": false,
            "group_name": "admin",
            "safe_name": "SSH",
            "created_at": "2025-05-07 23:56:15.450435-07",
            "modified_at": "2025-05-07 23:56:15.450435-07",
            "builtin": false,
            "hidden": false
        }
```


(continues on next page)

(continued from previous page)

```
    ]
}
```

Get Safe Assigned to a Group by Their IDs

Request

Method	`GET`
Path	`/group/<group_id>/safe/<safe_id>`

GET /api/v2/group/<group_id>/safe/<safe_id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group/9115285645797883905/safe/9115285645797883906
↪'
```

Response

```
{
    "result": "success",
    "group_safe": {
        "group_id": "9115285645797883905",
        "safe_id": "9115285645797883906",
        "password_visible": false,
        "use_time_policy": false,
        "group_name": "admin",
        "safe_name": "RDP",
        "created_at": "2025-05-07 23:56:15.424739-07",
        "modified_at": "2025-05-07 23:56:15.424739-07",
        "builtin": false,
        "hidden": false
    }
}
```

Create Group-Safe Assignment

Request

Method	`POST`
Path	`/api/v2/group/safe`
Headers	`Content-Type: Application/json`
Body	`GroupSafeModel`

POST /api/v2/group/safe

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/group/safe' \
  -d'{"group_id":"9115285645797883905","safe_id":"9115285645797883906","use_
↪time_policy": true}'
```

Response

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

Modify Group-Safe Assignment

Request

Method	PATCH
Path	/api/v2/group/<group_id>/safe/<safe_id>
Headers	Content-Type: Application/json
Body	GroupSafeModel

PATCH /api/v2/group/<group_id>/safe/<safe_id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/group/9115285645797883911/safe/
↪9115285645797883908' \
  -d'{"password_visible": true,"use_time_policy": false}'
```

Response

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

Delete Group-Safe Assignment

Request

Method	DELETE
Path	/api/v2/group/<group_id>/safe/<safe_id>

DELETE /api/v2/group/<group_id>/safe/<safe_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/group/9115285645797883905/safe/
↪9115285645797883908'
```

Response

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

1.4.7 Group-Safe-TimePolicy Management

Endpoints in this section allow you to manage the time policy for accessing safes assigned to a group.

Data Structures

Table 8: `GroupSafeTimePolicyModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier.
`group_safe_id`	string		Read-only; protected.
`group_id`	string	yes	Immutable. Requires rights on the `group` object: `read` for GET, `modify` for POST, PATCH, and DELETE.
`safe_id`	string	yes	Immutable. Requires `read` right on the `safe` object for all operations.
`group_name`	string		Read-only; expensive to use.
`safe_name`	string		Read-only; expensive to use.
`day_of_week`	number	yes	Value range from `1` to `7`.
`valid_from`	datetime	yes	Daily access start time.
`valid_to`	datetime	yes	Daily access end time.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *GroupSafeTimePolicyModel*

Request

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

GET /api/v2/objspec/group_safe_time_policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/objspec/group_safe_time_policy'
```

Get Group-Safe-TimePolicy Assignment List

Request

Method	GET
Path	/api/v2/group/safe/time_policy

GET /api/v2/group/safe/time_policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group/safe/time_policy'
```

Response


```
{
    "result": "success",
    "group_safe_time_policy": [
        {
            "id": "9115285645797883905",
            "group_id": "9115285645797883906",
            "safe_id": "9115285645797883907",
            "group_name": "QA_team",
            "safe_name": "SSH",
            "day_of_week": 1,
            "valid_from": "06:00:00",
            "valid_to": "08:00:00",
            "created_at": "2025-05-08 03:12:37.235474-07",
            "modified_at": "2025-05-08 03:12:37.235474-07"
        },
        {
            "id": "9115285645797883906",
            "group_id": "9115285645797883906",
            "safe_id": "9115285645797883907",
            "group_name": "QA_team",
            "safe_name": "SSH",
            "day_of_week": 1,
            "valid_from": "10:00:00",
            "valid_to": "12:00:00",
            "created_at": "2025-05-08 03:12:37.254555-07",
            "modified_at": "2025-05-08 03:12:37.254555-07"
        },
        {
            "id": "9115285645797883909",
```


(continues on next page)

(continued from previous page)

```
            "group_id": "9115285645797883906",
            "safe_id": "9115285645797883907",
            "group_name": "QA_team",
            "safe_name": "SSH",
            "day_of_week": 2,
            "valid_from": "08:00:00",
            "valid_to": "10:00:00",
            "created_at": "2025-05-08 03:12:37.302277-07",
            "modified_at": "2025-05-08 03:12:37.302277-07"
        },
    ]
}
```

Get Group-Safe-TimePolicy Assignment by ID

Request

Method	GET
Path	/group/safe/time_policy/<id>

GET /api/v2/group/safe/time_policy/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group/safe/time_policy/9115285645797883909'
```

Response

```
{
    "result": "success",
    "group_safe_time_policy": {
        "id": "9115285645797883909",
        "group_id": "9115285645797883906",
        "safe_id": "9115285645797883907",
        "group_name": "QA_team",
        "safe_name": "SSH",
        "day_of_week": 2,
        "valid_from": "08:00:00",
        "valid_to": "10:00:00",
        "created_at": "2025-05-08 03:12:37.302277-07",
        "modified_at": "2025-05-08 03:12:37.302277-07"
    }
}
```

Create Group-Safe-TimePolicy Assignment

Request

Method	POST
Path	/api/v2/group/safe/time_policy
Headers	Content-Type: Application/json
Body	GroupSafeTimePolicyModel

POST /api/v2/group/safe/time_policy

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/group/safe/time_policy' \
  -d'{"group_id":"9115285645797883906","safe_id":"9115285645797883907","day_of_
↪week":5,"valid_from":"06:00:00","valid_to":"12:00:00"}'
```

Response

```
{
    "result": "success",
    "group_safe_time_policy": {
        "id": "9115285645797883914"
    }
}
```

Modify Group-Safe-TimePolicy Assignment

Request

Method	PATCH
Path	/api/v2/group/safe/time_policy/<id>
Headers	Content-Type: Application/json
Body	GroupSafeTimePolicyModel

PATCH /api/v2/group/safe/time_policy/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/group/safe/time_policy/9115285645797883915' \
  -d'{"day_of_week":3,"valid_from":"06:00:00","valid_to":"12:00:00"}'
```

Response

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

Delete Group-Safe-TimePolicy Assignment

Request

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

DELETE /api/v2/group/safe/time_policy/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/group/safe/time_policy/9115285645797883915'
```

Response

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

1.4.8 Group-User Assignment

Endpoints in this section allow you to assign users to groups.

Data Structures

Table 9: `GroupUser`

Attribute	Type	Required	Description
`id`	string		Read-only; protected. Unique identifier.
`group_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `group_id` with attribute `user_id`. Requires rights on the `group` object: `read` for GET, `user-add` for POST, `user-remove` for DELETE.
`user_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `group_id`. Requires `read` right on the `user` object for all operations.
`group_name`	string		Read-only; expensive to use.
`user_name`	string		Read-only; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *GroupUser*

Request

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

GET /api/v2/objspec/group_user

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/objspec/group_user'
```

Get Group-User Assignment List

Request

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

GET /api/v2/group/user

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group/user'
```

Response

```
{
    "result": "success",
    "group_user": [
        {
            "group_id": "9115285645797883906",
            "user_id": "9115285645797883906",
            "group_name": "QA_team",
            "user_name": "User_1",
            "created_at": "2025-05-07 23:56:45.451806-07",
            "modified_at": "2025-05-07 23:56:45.451806-07"
        },
        {
            "group_id": "9115285645797883906",
            "user_id": "9115285645797883907",
            "group_name": "QA_team",
            "user_name": "User_2",
            "created_at": "2025-05-07 23:56:45.462326-07",
            "modified_at": "2025-05-07 23:56:45.462326-07"
        }
```

(continues on next page)

(continued from previous page)

```
    ]
}
```

Get Group-User Assignment by Their IDs

Request

Method	GET
Path	/group/<group_id>/user/<user_id>

GET /api/v2/group/<group_id>/user/<user_id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/group/9115285645797883906/user/9115285645797883907
↪'
```

Response

```
{
    "result": "success",
    "group_user": {
        "group_id": "9115285645797883906",
        "user_id": "9115285645797883907",
        "group_name": "QA_team",
        "user_name": "User_2",
        "created_at": "2025-05-07 23:56:45.462326-07",
        "modified_at": "2025-05-07 23:56:45.462326-07"
    }
}
```

Create Group-User Assignment

Request

Method	POST
Path	/api/v2/group/user
Headers	Content-Type: Application/json
Body	GroupUser

POST /api/v2/group/user

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
```

(continues on next page)

(continued from previous page)

```
  'https://10.0.214.98/api/v2/group/user' \
  -d'{"group_id":"9115285645797883906","user_id":"9115285645797883909"}'
```

Response

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

Delete Group-User Assignment

Request

Method	`DELETE`
Path	`/api/v2/group/<group_id>/user/<user_id>`

DELETE /api/v2/group/<group_id>/user/<user_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/group/9115285645797883906/user/
↪9115285645797883909'
```

Response

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

1.4.9 Object Rights

Data Structures

Table 10: `ObjectRightsModels`

Attribute	Type	Required	Description
`bit`	number	yes	Read-only. Unique. Hidden.
`name`	string	yes	Read-only.
`description`	string	yes	Read-only.

Retrieve Available Attributes of the *ObjectRightsModels*

Request

Method	GET
Path	/api/v2/objspec/{objtype}_right
Variants	• /api/v2/objspec/account_right • /api/v2/objspec/collection_right • /api/v2/objspec/group_right • /api/v2/objspec/pool_right • /api/v2/objspec/safe_right • /api/v2/objspec/server_right • /api/v2/objspec/user_right

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

Get Available Rights Values for Object Types

Request

Method	GET
Path	/api/v2/capability/right/{objtype}
Variants	• /api/v2/capability/right/account • /api/v2/capability/right/collection • /api/v2/capability/right/group • /api/v2/capability/right/pool • /api/v2/capability/right/safe • /api/v2/capability/right/server • /api/v2/capability/right/user

Example Request

GET /api/v2/capability/right/account

```
curl -s -k -X GET \
  -H 'Authorization:sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/capability/right/account'
```

Response

```
{
    "result": "success",
    "account_right": [
        {
            "name": "read",
            "description": ""
        },
        {
            "name": "modify",
```

(continues on next page)

(continued from previous page)

```
            "description": ""
        },
        {
            "name": "delete",
            "description": ""
        },
        {
            "name": "block",
            "description": ""
        }
    ]
}
```

The table below lists the available `rights` values for each object type.

Object type	Available `rights` values
account	• `"read"` • `"modify"` • `"delete"` • `"block"`
collection	• `"read"` • `"modify"` • `"delete"` • `"move"` • `"create"`
group	• `"read"` • `"modify"` • `"delete"` • `"user-add"` • `"user-remove"`
pool	• `"read"` • `"modify"` • `"delete"` • `"server-add"` • `"server-remove"`

continues on next page

Table 11 – continued from previous page

Object type	Available `rights` values
safe	• `"read"` • `"modify"` • `"delete"` • `"block"` • `"account-add"` • `"account-remove"` • `"group-add"` • `"group-remove"` • `"user-add"` • `"user-remove"`
server	• `"read"` • `"modify"` • `"delete"` • `"block"`
user	• `"read"` • `"modify"` • `"delete"` • `"block"` • `"session-view"`

1.4.10 Access Rights

Data Structures

Table 12: `AccessModel`

Attribute	Type	Required	Description
`subject_id`	string		Read-only. Identifier of the subject (e.g., user or group). Uniqueness is required in the combination with attribute `object_id`.
`subject_name`	string		Read-only; expensive to use. Name of the subject.
`object_id`	string		Read-only. Identifier of the target object (e.g., safe, server, account). Uniqueness is required in the combination with attribute `subject_id`.
`object_name`	string		Read-only; expensive to use. Name of the target object.
`rights`	string-array		Read-only. List of assigned rights.
`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.

Retrieve Available Attributes of the *AccessModels*

Request

Method	`GET`
Path	`/api/v2/objspec/{objtype}_access`
Variants	• `/api/v2/objspec/account_access` • `/api/v2/objspec/group_access` • `/api/v2/objspec/pool_access` • `/api/v2/objspec/safe_access` • `/api/v2/objspec/server_access` • `/api/v2/objspec/user_access`

Example Request

GET /api/v2/objspec/account_access

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.117.68/api/v2/objspec/account_access'
```

Get All Access Rules for Selected Object Type

Request

Method	`GET`
Path	`/api/v2/access/{objtype}`
Variants	• `/api/v2/access/account` • `/api/v2/access/group` • `/api/v2/access/pool` • `/api/v2/access/safe` • `/api/v2/access/server` • `/api/v2/access/user`

Example Request

GET /api/v2/access/safe

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.117.68/api/v2/access/safe'
```

Response

```
{
    "result": "success",
    "safe_access": [
        {
```

(continues on next page)

(continued from previous page)


```
            "subject_id": "1",
            "subject_name": "system",
            "object_id": "2",
            "object_name": "portal",
            "rights": [
                "read",
                "modify",
                "delete",
                "block",
                "account-add",
                "account-remove",
                "group-add",
                "group-remove",
                "user-add",
                "user-remove"
            ]
        },
        {
            "subject_id": "1",
            "subject_name": "system",
            "object_id": "8673932882315575297",
            "object_name": "main",
            "rights": [
                "read",
                "modify",
                "delete",
                "block",
                "account-add",
                "account-remove",
                "group-add",
                "group-remove",
                "user-add",
                "user-remove"
            ]
        },
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "2",
            "object_name": "portal",
            "rights": [
                "read",
                "modify",
                "delete",
                "block",
                "account-add",
                "account-remove",
                "group-add",
                "group-remove",
```


(continues on next page)

(continued from previous page)


```
                "user-add",
                "user-remove"
            ]
        },
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "8673932882315575297",
            "object_name": "main",
            "rights": [
                "read",
                "modify",
                "delete",
                "block",
                "account-add",
                "account-remove",
                "group-add",
                "group-remove",
                "user-add",
                "user-remove"
            ]
        }
    ]
}
```


Get Access Rights of a Subject to a Specific Object

Request

Method	`GET`
Path	`/api/v2/access/<subject_id>/{objtype}/<object_id>`
Variants	• `/api/v2/access/<subject_id>/safe/<object_id>` • `/api/v2/access/<subject_id>/group/<object_id>` • `/api/v2/access/<subject_id>/pool/<object_id>` • `/api/v2/access/<subject_id>/safe/<object_id>` • `/api/v2/access/<subject_id>/server/<object_id>` • `/api/v2/access/<subject_id>/user/<object_id>`

Example: Retrieve Access Rights of User <user_id> to Group <group_id>

GET /api/v2/access/<user_id>/group/<group_id>

Note

`<user_id>` – Unique identifier (ID) of the user.

`<group_id>` – Unique identifier (ID) of the group.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.117.68/api/v2/access/8673932882315575297/group/
↪8673932882315575297'
```

Response

```
{
    "result": "success",
    "group_access": {
        "subject_id": "8673932882315575297",
        "subject_name": "admin",
        "object_id": "8673932882315575297",
        "object_name": "Group_1",
        "rights": [
            "read",
            "modify",
            "delete",
            "user-add",
            "user-remove"
        ]
    }
}
```

Examples of Filtered Access Requests

Example 1: Retrieve All Accounts Accessible by User <user_id>

Request

Method	GET
Path	/api/v2/access/account?filter=subject_id.eq(<user_id>)

Note

<user_id> – Unique identifier (ID) of the user.

GET /api/v2/access/account?filter=subject_id.eq(<user_id>)

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.117.68/api/v2/access/account?filter=subject_id.
↪eq(8673932882315575297)'
```

Response

```
{
    "result": "success",
    "account_access": [
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "8673932882315575299",
            "object_name": "ad-user1-windows",
            "rights": [
                "read",
                "modify",
                "delete",
                "block"
            ]
        },
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "8673932882315575300",
            "object_name": "jools-Linux",
            "rights": [
                "read",
                "modify",
                "delete",
                "block"
            ]
        },
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "8673932882315575301",
            "object_name": "root-fudo",
            "rights": [
                "read",
                "modify",
                "delete",
                "block"
            ]
        }
    ]
}
```


Example 2: Retrieve All Users with Access to Safe <safe_id>

Request

Method	`GET`
Path	`/api/v2/access/safe?filter=object_id.eq(<safe_id>)`

Note

<safe_id> – Unique identifier (ID) of the safe.

GET /api/v2/access/safe?filter=object_id.eq(<safe_id>)

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.117.68/api/v2/access/safe?filter=object_id.
↪eq(8673932882315575297)'
```

Response

```
{
    "result": "success",
    "safe_access": [
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "2",
            "object_name": "portal",
            "rights": [
                "read",
                "modify",
                "delete",
                "block",
                "account-add",
                "account-remove",
                "group-add",
                "group-remove",
                "user-add",
                "user-remove"
            ]
        },
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "8673932882315575297",
            "object_name": "main",
            "rights": [
                "read",
                "modify",
                "delete",
                "block",
                "account-add",
                "account-remove",
                "group-add",
                "group-remove",
                "user-add",
```

(continues on next page)

(continued from previous page)

```
                "user-remove"
            ]
        }
    ]
}
```

Example 3: Retrieve Users Who Can Delete Server <server_id>

Request

Method	`GET`
Path	`/api/v2/access/server?filter=object_id.eq(<server_id>), rights.contains(delete)`

Note

`<server_id>` – Unique identifier (ID) of the server.

GET /api/v2/access/server?filter=object_id.eq(<server_id>),rights .contains(delete)

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.117.68/api/v2/access/server?filter=object_id.
↪eq(8673932882315575301),rights.contains(delete)'
```

Response

```
{
    "result": "success",
    "server_access": [
        {
            "subject_id": "1",
            "subject_name": "system",
            "object_id": "8673932882315575301",
            "object_name": "fudo",
            "rights": [
                "read",
                "modify",
                "delete",
                "block"
            ]
        },
        {
            "subject_id": "8673932882315575297",
            "subject_name": "admin",
            "object_id": "8673932882315575301",
```

(continues on next page)

(continued from previous page)

```
            "object_name": "fudo",
            "rights": [
                "read",
                "modify",
                "delete",
                "block"
            ]
        }
    ]
}
```

1.4.11 Role-Based Capabilities

Data Structures

Table 13: `RoleCapabilityModels` :header: "Attribute", "Type", "Required", "Description" :widths: 2, 8, 6, 13

`id`	string		Read-only. Protected.
`subject_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `subject_id` with attribute `object_id`.
`object_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `object_id` with attribute `subject_id`.
`rights`	string-array; Default value `[read]`	yes	Expensive to use.
`object_name`	string		Read-only; expensive to use.
`subject_name`	string		Read-only; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.
`builtin`	boolean		Read-only; expensive to use. Is object built-in? Built-in objects shouldn't be editable.
`hidden`	boolean		Read-only; expensive to use. Shall the object be hidden in UI?

Retrieve Available Attributes of the *RoleCapabilityModels*

Request

Method	`GET`
Paths	• `/api/v2/objspec/role_account_capability` • `/api/v2/objspec/role_collection_capability` • `/api/v2/objspec/role_group_capability` • `/api/v2/objspec/role_pool_capability` • `/api/v2/objspec/role_safe_capability` • `/api/v2/objspec/role_server_capability` • `/api/v2/objspec/role_user_capability`

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

Get Role-Based Capabilities for Objects

Request

Method	`GET`
Paths	• `/api/v2/capability/role/account` • `/api/v2/capability/role/collection` • `/api/v2/capability/role/group` • `/api/v2/capability/role/pool` • `/api/v2/capability/role/safe` • `/api/v2/capability/role/server` • `/api/v2/capability/role/use`

Example Request

GET /api/v2/capability/role/account

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/capability/role/account'
```

Response

```
{
    "result": "success",
    "role_account_capability": [
        {
            "subject_id": "9115285645797883906",
            "object_id": "9115285645797883907",
            "rights": [
                "read"
```

(continues on next page)

(continued from previous page)


```
            ],
            "object_name": "ad-user1-windows",
            "subject_name": "admin",
            "created_at": "2025-04-30 02:08:09.033964-07",
            "modified_at": "2025-04-30 02:08:09.033964-07"
        },
        {
            "subject_id": "9115285645797883906",
            "object_id": "9115285645797883908",
            "rights": [
                "read"
            ],
            "object_name": "jools-Linux",
            "subject_name": "admin",
            "created_at": "2025-04-30 02:12:19.542946-07",
            "modified_at": "2025-04-30 02:12:19.542946-07"
        }
    ]
}
```


Assign Role-Based Capabilities for Objects

Request

Method	`POST`
Paths	• `/api/v2/capability/role/account` • `/api/v2/capability/role/group` • `/api/v2/capability/role/pool` • `/api/v2/capability/role/safe` • `/api/v2/capability/role/server` • `/api/v2/capability/role/user`
Headers	`Content-Type: Application/json`
Body	`RoleCapabilityModels`

Example Request

POST /api/v2/capability/role/user

```
curl -s -k -X POST \
  -H 'Authorization:sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/role/user' \
  -d'{"subject_id":9115285645797883906,"object_id":9115285645797883906}'
```

Response


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


(continues on next page)

(continued from previous page)

```
}
```

Get Rights Assigned to a Role (Subject) for an Object by Their IDs

Request

Method	`GET`
Paths	• `/api/v2/capability/role/<subject_id>/account/<object_id>` • `/api/v2/capability/role/<subject_id>/collection/<object_id>` • `/api/v2/capability/role/<subject_id>/group/<object_id>` • `/api/v2/capability/role/<subject_id>/pool/<object_id>` • `/api/v2/capability/role/<subject_id>/safe/<object_id>` • `/api/v2/capability/role/<subject_id>/server/<object_id>` • `/api/v2/capability/role/<subject_id>/user/<object_id>`

Example Request

GET /api/v2/capability/role/<subject_id>/user/<object_id>

```
curl -s -k -X GET \
  -H 'Authorization:sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/capability/role/9115285645797883906/user/
↪9115285645797883906'
```

Response

```
{
    "result": "success",
    "role_user_capability": {
        "subject_id": "9115285645797883906",
        "object_id": "9115285645797883906",
        "rights": [
            "read",
            "modify",
            "delete",
            "session-view"
        ],
        "object_name": "User_1",
        "subject_name": "admin",
        "created_at": "2025-04-30 02:39:21.424866-07",
        "modified_at": "2025-04-30 03:47:33.568186-07"
    }
}
```

Modify Rights Assigned to a Role (Subject) for an Object by Their IDs

Request

Method	`PATCH`
Paths	• `/api/v2/capability/role/<subject_id>/account/<object_id>` • `/api/v2/capability/role/<subject_id>/collection/<object_id>` • `/api/v2/capability/role/<subject_id>/group/<object_id>` • `/api/v2/capability/role/<subject_id>/pool/<object_id>` • `/api/v2/capability/role/<subject_id>/safe/<object_id>` • `/api/v2/capability/role/<subject_id>/server/<object_id>` • `/api/v2/capability/role/<subject_id>/user/<object_id>`
Headers	`Content-Type: Application/json`
Body	`RoleCapabilityModels`

Example Request

PATCH /api/v2/capability/role/<subject_id>/user/<object_id>

```
curl -s -k -X PATCH \
  -H 'Authorization:sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/role/9115285645797883906/user/
↪9115285645797883906' \
  -d'{"rights":["read","modify","delete","session-view"]}'
```

Note

The `read` right is mandatory and must always be included.

Response

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

Grant Specific Rights to a Role (Subject) for an Object by Their IDs

Request

Method	PATCH
Paths	• /api/v2/capability/role/<subject_id>/account/<object_id>/grant • /api/v2/capability/role/<subject_id>/collection/<object_id>/grant • /api/v2/capability/role/<subject_id>/group/<object_id>/grant • /api/v2/capability/role/<subject_id>/pool/<object_id>/grant • /api/v2/capability/role/<subject_id>/safe/<object_id>/grant • /api/v2/capability/role/<subject_id>/server/<object_id>/grant • /api/v2/capability/role/<subject_id>/user/<object_id>/grant
Headers	Content-Type: Application/json
Body	RoleCapabilityModels

Example Request

PATCH /api/v2/capability/role/<subject_id>/user/<object_id>/grant

```
curl -s -k -X PATCH \
  -H 'Authorization:sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/role/9115285645797883906/user/
↪9115285645797883906/grant' \
  -d'{"rights":["modify","delete","session-view"]}'
```

Response

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

Revoke Specific Rights to a Role (Subject) for an Object by Their IDs

Request

Method	PATCH
Paths	• /api/v2/capability/role/<subject_id>/account/<object_id>/revoke • /api/v2/capability/role/<subject_id>/collection/<object_id>/revoke • /api/v2/capability/role/<subject_id>/group/<object_id>/revoke • /api/v2/capability/role/<subject_id>/pool/<object_id>/revoke • /api/v2/capability/role/<subject_id>/safe/<object_id>/revoke • /api/v2/capability/role/<subject_id>/server/<object_id>/revoke • /api/v2/capability/role/<subject_id>/user/<object_id>/revoke
Headers	Content-Type: Application/json
Body	RoleCapabilityModels

Example Request

PATCH /api/v2/capability/role/<subject_id>/user/<object_id>/revoke

```
curl -s -k -X PATCH \
  -H 'Authorization:sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/role/9115285645797883906/user/
↪9115285645797883906/revoke' \
  -d'{"rights":["modify","delete","session-view"]}'
```

Response

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

Delete Role-Based Capability Assigned to a Role (Subject) for an Object by Their IDs

Request

Method	DELETE
Paths	• /api/v2/capability/role/<subject_id>/account/<object_id> • /api/v2/capability/role/<subject_id>/collection/<object_id> • /api/v2/capability/role/<subject_id>/group/<object_id> • /api/v2/capability/role/<subject_id>/pool/<object_id> • /api/v2/capability/role/<subject_id>/safe/<object_id> • /api/v2/capability/role/<subject_id>/server/<object_id> • /api/v2/capability/role/<subject_id>/user/<object_id>

Example Request

DELETE /api/v2/capability/role/<subject_id>/user/<object_id>

```
curl -s -k -X DELETE \
  -H 'Authorization:sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/capability/role/9115285645797883906/user/
↪9115285645797883906'
```

Response

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

1.4.12 User-Based Capabilities

Data Structures

Table 14: `UserCapabilityModels`

Attribute	Type	Required	Description
`id`	string		Read-only, unique policy identifier. Protected.
`subject_id`	string	yes	Read-only; Immutable; Uniqueness is required in the combination of attribute `subject_id` with attribute `object_id`.
`object_id`	string	yes	Read-only; Immutable; Uniqueness is required in the combination of attribute `object_id` with attribute `subject_id`.
`rights`	string-array; read-write; default value `read`	yes	Expensive to use.
`object_name`	string	yes	Expensive to use.
`subject_name`	string	yes	Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.
`builtin`	boolean		Read-only; expensive to use. Is object built-in? Built-in objects shouldn't be editable.
`hidden`	boolean		Read-only; expensive to use. Shall the object be hidden in UI?

Retrieve Available Attributes of the *UserCapabilityModels*

Request

Method	`GET`
Paths	• `/api/v2/objspec/user_account_capability` • `/api/v2/objspec/user_collection_capability` • `/api/v2/objspec/user_group_capability` • `/api/v2/objspec/user_pool_capability` • `/api/v2/objspec/user_safe_capability` • `/api/v2/objspec/user_server_capability` • `/api/v2/objspec/user_user_capability`

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

Get User-Based Capabilities for Objects

Request

Method	`GET`
Paths	• `/api/v2/capability/user/account` • `/api/v2/capability/user/collection` • `/api/v2/capability/user/group` • `/api/v2/capability/user/pool` • `/api/v2/capability/user/safe` • `/api/v2/capability/user/server` • `/api/v2/capability/user/use`

Example Request

GET /api/v2/capability/user/account

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/capability/user/account'
```

Response

```
{
    "result": "success",
    "user_account_capability": [
        {
            "subject_id": "9115285645797883905",
            "object_id": "9115285645797883907",
            "rights": [
                "read",
```

(continues on next page)

(continued from previous page)


```
                "modify",
                "delete",
                "block"
            ],
            "object_name": "ad-user1-windows",
            "subject_name": "admin",
            "created_at": "2025-04-25 01:40:45.013273-07",
            "modified_at": "2025-04-25 01:40:45.013273-07"
        },
        {
            "subject_id": "9115285645797883905",
            "object_id": "9115285645797883908",
            "rights": [
                "read",
                "modify",
                "delete",
                "block"
            ],
            "object_name": "jools-Linux",
            "subject_name": "admin",
            "created_at": "2025-04-25 01:40:45.965614-07",
            "modified_at": "2025-04-25 01:40:45.965614-07"
        }
    ]
}
```


Add User-Based Capabilities for Objects

Request

Method	`POST`
Paths	• `/api/v2/capability/user/account` • `/api/v2/capability/user/collection` • `/api/v2/capability/user/group` • `/api/v2/capability/user/pool` • `/api/v2/capability/user/safe` • `/api/v2/capability/user/server` • `/api/v2/capability/user/user`
Headers	`Content-Type: Application/json`
Body	`UserCapabilityModels`

Example Request

POST /api/v2/capability/user/account

```
curl -s -k -X POST -H \
  'Authorization:<token>' \
```

(continues on next page)

(continued from previous page)

```
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/user/account' \
  -d'{"subject_id":9115285645797883906,"object_id":9115285645797883907}'
```

Response

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

Get Rights Assigned to a User (Subject) for an Object by Their IDs

Request

Method	GET
Paths	• /api/v2/capability/user/<subject_id>/account/<object_id> • /api/v2/capability/user/<subject_id>/collection/<object_id> • /api/v2/capability/user/<subject_id>/group/<object_id> • /api/v2/capability/user/<subject_id>/pool/<object_id> • /api/v2/capability/user/<subject_id>/safe/<object_id> • /api/v2/capability/user/<subject_id>/server/<object_id> • /api/v2/capability/user/<subject_id>/user/<object_id>

Example Request

GET /api/v2/capability/user/<subject_id>/account/<object_id>

```
curl -s -k -X GET \
  -H 'Authorization:<token>' \
  'https://10.31.135.179/api/v2/capability/user/9115285645797883906/account/
↪9115285645797883907'
```

Response

```
{
    "result": "success",
    "user_account_capability": {
        "subject_id": "9115285645797883906",
        "object_id": "9115285645797883907",
        "rights": [
            "read"
        ],
        "object_name": "ad-user1-windows",
        "subject_name": "User_1",
        "created_at": "2025-04-30 05:50:08.533293-07",
        "modified_at": "2025-04-30 05:50:08.533293-07"
    }
}
```

Modify Rights Assigned to a User (Subject) for an Object by Their IDs

Request

Method	`PATCH`
Paths	• `/api/v2/capability/user/<subject_id>/account/<object_id>` • `/api/v2/capability/user/<subject_id>/collection/<object_id>` • `/api/v2/capability/user/<subject_id>/group/<object_id>` • `/api/v2/capability/user/<subject_id>/pool/<object_id>` • `/api/v2/capability/user/<subject_id>/safe/<object_id>` • `/api/v2/capability/user/<subject_id>/server/<object_id>` • `/api/v2/capability/user/<subject_id>/user/<object_id>`
Headers	`Content-Type: Application/json`
Body	`UserCapabilityModels`

Example Request

PATCH /api/v2/capability/user/<subject_id>/account/<object_id>

```
curl -s -k -X PATCH \
  -H 'Authorization:<token>' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/user/9115285645797883906/account/
↪9115285645797883907' \
  -d'{"rights":["read","modify","delete"]}'
```

Note

The `read` right is mandatory and must always be included.

Response

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

Grant Specific Rights to a User (Subject) for an Object by Their IDs

Request

Method	PATCH
Paths	• /api/v2/capability/user/<subject_id>/account/<object_id>/grant • /api/v2/capability/user/<subject_id>/collection/<object_id>/grant • /api/v2/capability/user/<subject_id>/group/<object_id>/grant • /api/v2/capability/user/<subject_id>/pool/<object_id>/grant • /api/v2/capability/user/<subject_id>/safe/<object_id>/grant • /api/v2/capability/user/<subject_id>/server/<object_id>/grant • /api/v2/capability/user/<subject_id>/user/<object_id>/grant
Headers	Content-Type: Application/json
Body	UserCapabilityModels

Example Request

PATCH /api/v2/capability/user/<subject_id>/account/<object_id>/grant

```
curl -s -k -X PATCH \
  -H 'Authorization:<token>' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/user/9115285645797883906/account/
↪9115285645797883907/grant' \
  -d'{"rights":["modify","delete"]}'
```

Response

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

Revoke Specific Rights to a User (Subject) for an Object by Their IDs

Request

Method	PATCH
Paths	• /api/v2/capability/user/<subject_id>/account/<object_id>/revoke • /api/v2/capability/user/<subject_id>/collection/<object_id>/revoke • /api/v2/capability/user/<subject_id>/group/<object_id>/revoke • /api/v2/capability/user/<subject_id>/pool/<object_id>/revoke • /api/v2/capability/user/<subject_id>/safe/<object_id>/revoke • /api/v2/capability/user/<subject_id>/server/<object_id>/revoke • /api/v2/capability/user/<subject_id>/user/<object_id>/revoke
Headers	Content-Type: Application/json
Body	UserCapabilityModels

Example Request

PATCH /api/v2/capability/user/<subject_id>/account/<object_id>/revoke

```
curl -s -k -X PATCH \
  -H 'Authorization:<token>' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/capability/user/9115285645797883906/account/
↪9115285645797883907/revoke' \
  -d'{"rights":["modify","delete"]}'
```

Response

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

Delete User-Based Capability Assigned to a ser (Subject) for an Object by Their IDs

Request

Method	DELETE
Paths	• /api/v2/capability/user/<subject_id>/account/<object_id> • /api/v2/capability/user/<subject_id>/collection/<object_id> • /api/v2/capability/user/<subject_id>/group/<object_id> • /api/v2/capability/user/<subject_id>/pool/<object_id> • /api/v2/capability/user/<subject_id>/safe/<object_id> • /api/v2/capability/user/<subject_id>/server/<object_id> • /api/v2/capability/user/<subject_id>/user/<object_id>

Example Request

DELETE /api/v2/capability/user/<subject_id>/account/<object_id>

```
curl -s -k -X DELETE \
  -H 'Authorization:<token>' \
  'https://10.31.135.179/api/v2/capability/user/9115285645797883906/account/
↪9115285645797883907'
```

Response

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

1.5 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.

1.5.1 Data Structures: *UserModel*

Table 15: `UserModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only object identifier. Requires `read`, `modify`, or `delete` right on object type `user`, depending on the HTTP method used (`GET`, `PATCH`, or `DELETE` respectively).
`name`	string	yes	Unique user's name
`blocked`	boolean; default value `false`	yes	
`reason`	string		
`domain`	string		User's domain
`privileges`	string-array		Read-only
`full_name`	string		User's full name
`email`	string		User's email address
`organization`	string		User's organization name
`phone`	string		User's phone number
`ad_domain`	string		User's AD domain. Also used as the UPN suffix when the user is identified during an OpenID Connect sign-in.
`ldap_base`	string		User's LDAP base
`language`	string; default value `en`	yes	Interface language
`previous_success`	datetime		Read-only

continues on next page

Table 15 – continued from previous page

Attribute	Type	Required	Description
previous_success_loc	string		Read-only
last_success	datetime		Read-only
last_success_locatic	string		Read-only
last_failure	datetime		Read-only
last_failure_locatic	string		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	
scim_managed	boolean; default value false	yes	
fudo_blocked	boolean		Read-only
scim_blocked	boolean		Read-only
external_id	string		Unique external identifier
scim_username	string		Unique SCIM username (case-insensitive)
scim_email_type	string		Type of the email address provisioned over SCIM, for example work.
scim_phone_type	string		Type of the phone number provisioned over SCIM, for example work.
first_name	string	`	
last_name	string	`	
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_directory_id	string		Id of the user's LDAP server
source_ip	string	`	
fido2_user_handle	string		Read-only
fudo_network_status	string {disabled, invited, untrusted, trusted}		Read-only. Fudo ShareAccess membership state, derived from the user's fnet authentication method. Value disabled means the user has no such method.
fudo_network_usernar	string		Read-only. Fudo ShareAccess user name (the X-Signed-By value) taken from the user's fnet authentication method. null when the user has no such method.

continues on next page

Table 15 – continued from previous page

Attribute	Type	Required	Description
`fudo_network_method_`	string		Read-only. Id of the `fnet` authentication method carrying the user's Fudo ShareAccess identity. Use it to address the method on the `/user/<user_id>/authentication/<id>` endpoint. `null` when the user has no such method.
`fudo_network_pubkey_`	string		Read-only; expensive to use. SHA256 fingerprint of the user's Fudo ShareAccess key pair. `null` when the user has no `fnet` authentication method or has not uploaded their keys yet.
`oidc_subs`	object-array		OpenID Connect sub claims. Read-only; expensive to use.
`roles`	object-array		Read-only; expensive to use.
`role_names`	string-array		Read-only; hidden; expensive to use.
`role_ids`	string-array		Read-only; hidden; expensive to use.
`safes`	object-array		Read-only; expensive to use; JSON object array containing `id`, `name`, and `position` of assigned safes.
`safe_ids`	string-array		Read-only; hidden; expensive to use
`safe_names`	string-array		Read-only; hidden; expensive to use
`group_ids`	string-array		IDs of the groups the user belongs to. Read-only; hidden; expensive to use.
`authentication_metho`	object-array		Read-only; expensive to use; JSON object array containing `id`, `type`, and `position` of configured authentication methods.
`authentication_metho`	string-array		Types of authentication methods used by this user. Read-only; hidden; expensive to use.
`external_authenticat`	string-array		IDs of external authentications used by this user. Read-only; hidden; expensive to use.

continues on next page

Table 15 – continued from previous page

Attribute	Type	Required	Description
`analysis_context`	string		AI analysis context. Given to the AI that analyzes this user's sessions. Describe what is normal here so expected activity is not flagged as a risk.
`rights`	string-array		Read-only; list of rights the subject has to this object.
`module_psm_enabled`	boolean; default value `true`	yes	If the user is enabled in the PSM module. Value false disables licence auto-activation.
`module_psm_last_acti`	datetime		Timestamp of the last activity of the user in the PSM module. Last established session or secret checkout via account. Read-only.
`module_psm_status`	string {active, inactive, disabled}	yes	User activation status in the PSM module. Read-only; expensive to use.
`module_vault_enable`	boolean; default value `true`	yes	If the user is enabled in the Vault module. Value false disables licence auto-activation.
`module_vault_last_a`	datetime		Timestamp of the last activity of the user in the Vault module. Last secret checkout in password vault. Read-only.
`module_vault_status`	string {active, inactive, disabled}	yes	User activation status in the Vault module. Read-only; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

1.5.2 Get Available Attributes of the *UserModel*

Request

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

1.5.3 Data Structures: *UserSafeAssignmentModel*

Table 16: `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`. Requires `read` right on object type `user` for `GET`, `POST`, `PATCH`, and `DELETE` requests.
`roles`	object-array		Read-only; expensive to use.
`role_names`	string-array		Read-only; hidden; expensive to use.
`role_ids`	string-array		Read-only; hidden; expensive to use.
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `user_id`. Requires `read` right on object type `safe` for `GET` requests, `user-add` right for `POST` and `PATCH`, and `user-remove` right for `DELETE` requests.
`blocked`	boolean; default value `false`	yes	Access to this safe is disabled for the user.
`position`	number		
`password_visible`	boolean; default value `false`	yes	Allow a user to use Secret Checkout feature and view passwords in the User Access Gateway.
`time_policy_che`	string		Read-only; expensive to use. Checksum computed from time policies used for this user-safe connection.
`use_time_policy`	boolean; default value `false`	yes	Enables the daily access policy for this user-safe connection. On a Safe with `jit_mode` set to `time_policy` it also decides when an access request is required - see *Safes*.
`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.
`user_domain`	string		Read-only; expensive to use.
`user_email`	string		Read-only; expensive to use.

continues on next page

Table 16 – continued from previous page

Attribute	Type	Required	Description
user_organizatic	string		Read-only; expensive to use.
safe_name	string		Read-only; expensive to use.
user_blocked	boolean		Read-only; expensive to use; blocked state of the assigned user.
safe_blocked	boolean		Read-only; expensive to use; blocked state of the assigned safe.
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.

1.5.4 Retrieve Available Attributes of the *UserSafeAssignmentModel*

Request

Method	GET
Path	/api/v2/objspec/user_safe

1.5.5 Data Structures: *UserSafeTimePolicyAssignmentModel*

Table 17: 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. Requires read right on object type user for GET requests, and modify right for POST, PATCH, and DELETE requests.
safe_id	string	yes	Immutable. Requires read right on object type safe for GET, POST, and PATCH requests.
user_name	string		Read-only; expensive to use.
user_role	string		Read-only; expensive to use.
safe_name	string		Read-only; expensive to use.
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.

1.5.6 Retrieve Available Attributes of the *UserSafeTimePolicy - Assignment-Model*

Request

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

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

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

1.5.7 Create a User

Request

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

Example Request

POST /api/v2/user

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

Response

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

1.5.8 Get Users List

Request

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

Example Request

GET /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"
    }
]}
```


1.5.9 Get a User

Request

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

1.5.10 Modify a User

Request

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

Example Request: Changing User Login

PATCH /api/v2/user/<id>

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

Response

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

Example Request: Blocking a User

PATCH /api/v2/user/<id>

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

Response

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

1.5.11 Get User-Safe Assignments List

Request

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

1.5.12 Create a User-Safe Assignment

Request

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

Example Request

POST /api/v2/user/safe

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

Response

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

1.5.13 Get Users' Time Policy Settings Within Safes

Request

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

Example Request

GET /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"
    }]}
```

1.5.14 Get Users' Time Policy Settings Within Safes by ID

Request

Method	GET
Path	/api/v2/user/safe/time_policy/<id>

Example Request

GET /api/v2/user/safe/time_policy/<id>

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

```
   {
"result": "success",
"user_safe_time_policy": [
   {
       "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"
   }]}
```

1.5.15 Modify 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

PATCH /api/v2/user/safe/time_policy/<id>

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

Response

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

1.5.16 Create 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

POST /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" }}
```

1.5.17 Delete User's Time Policy Settings Within a Safe

Request

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

1.5.18 Delete User-Safe Assignment

Request

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

1.5.19 Delete User

Request

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

1.6 User Authentication Methods Management

Table 18: `UserAuthenticationMethodModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only object Identifier

continues on next page

Table 18 – continued from previous page

Attribute	Type	Required	Description
`type`	string {password, oath, extauth, sshkey, certificate, duo, sms, apikey, fido2, fnet}	yes	Immutable. Type `fnet` carries the user's Fudo ShareAccess identity and cannot be created with a `POST` request - the method is created by the Fudo ShareAccess invitation flow.
`description`	string		Optional description of the authentication method.
`user_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `position`. Requires `read` right on object type `user` for `GET` requests, and `modify` right for `DELETE`, `PATCH`, and `POST` requests.
`user_name`	string		Read-only; expensive to use
`position`	number		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` || `oath` || `password` || `sms` || `sshkey`	Protected
`needs_change`	boolean; default value `false`	yes	
`external_authentication_id`	string	if `type` == `duo` || `extauth` || `oath` || `sms`	
`apikey_device_id`	string	if `type` == `apikey`	Read-only; expensive to use
`apikey_device_platfor`	string	if `type` == `apikey`	Read-only; expensive to use
`apikey_device_pushid`	string	if `type` == `apikey`	Read-only; expensive to use

continues on next page

Table 18 – continued from previous page

Attribute	Type	Required	Description
`apikey_key`	string	if `type` == `apikey`	Protected
`apikey_hint`	string	if `type` == `apikey`	The first four and the last four plain text characters of the API key if it is at least 32 characters long. Read-only; expensive to use
`apikey_expires_at`	datetime	if `type` == `apikey`	Expiration date and time for the API key. NULL means the key never expires.
`certificate_subject`	string	if `type` == `certificate`	
`duo_user_id`	string	if `type` == `duo`	
`duo_username`	string	if `type` == `duo`	
OATH	OATHAuthentication-MethodAttributes	if `type` == `oath`	OATH authentication method properties
`sms_token`	string	if `type` == `sms`	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`	
`sshkey_publickey`	string	if `type` == `sshkey`	User's SSH public key. Read-only; expensive to use
`fido2_credential_id`	string	if `type` == `fido2`	Unique identifier for the registered FIDO2 credential (base64url-encoded). Read-only
`fido2_public_key`	string	if `type` == `fido2`	COSE-format public key used to verify authentication signatures (base64url-encoded). Read-only
`fido2_counter`	number	if `type` == `fido2`	Signature counter for clone detection; must increase on each authentication. Read-only

continues on next page

Table 18 – continued from previous page

Attribute	Type	Required	Description
`fido2_aaguid`	string	if `type` == `fido2`	Authenticator Attestation GUID identifying the authenticator make/model. Read-only
`fido2_transports`	string	if `type` == `fido2`	Supported transports: usb, nfc, ble, internal, hybrid, smart-card. Read-only
`fn_username`	string	if `type` == `fnet`	Fudo ShareAccess user name (the `X-Signed-By` value). Required for type `fnet`. Unique, case-insensitive.
`fn_pubkey_ec`	string	if `type` == `fnet`	EC P-521 public key (PEM), submitted by the user when accepting the Fudo ShareAccess invitation. Read-only
`fn_pubkey_rsa`	string	if `type` == `fnet`	RSA public key (PEM), submitted by the user when accepting the Fudo ShareAccess invitation. Read-only
`fn_pubkey_trusted_by`	string	if `type` == `fnet`	Id of the administrator who attested the keys. Set it to grant trust, set it to `null` to revoke trust. The value must be equal to the id of the user making the request.
`fn_pubkey_trusted_at`	datetime	if `type` == `fnet`	Time when the trust was attested. Read-only
`fn_invite_code`	string	if `type` == `fnet`	One-time Fudo ShareAccess invitation code. Read-only
`fn_invite_code_expire`	datetime	if `type` == `fnet`	Expiration date and time of the invitation code. Read-only
`fn_invited_by`	string	if `type` == `fnet`	Id of the administrator who issued the invitation. Read-only

continues on next page

Table 18 – continued from previous page

Attribute	Type	Required	Description
`fn_pubkey_fingerprint`	string	if `type` == `fnet`	SHA256 fingerprint of the (EC, RSA) key pair. `null` until the user uploads their keys. Read-only; expensive to use
`created_at`	datetime		Read-only
`modified_at`	datetime		Read-only
`removed`	boolean		Read-only

Table 19: `OATHAuthenticationMethodAttributes`

Attribute	Type	Required	Description
`oath_type`	string {HOTP, TOTP}	yes	Immutable.
`oath_initialize`	boolean; default value `false`	yes	
`oath_secret`	string		Protected. Value format: ^[A-Z2-7]+$
`oath_tokenlen`	number	yes	Immutable; value range: [4, 16].
`oath_timestep`	number {30, 45, 60, 90, 120, 180, 300}	If `oath_type` == `TOTP`	Immutable
`oath_counter`	number; default value `0`	yes	Read-only.
`oath_timeshift`	number; default value `0`	If `oath_type` == `TOTP`	Read-only.
`oath_reuse`	boolean; default value `false`	If `oath_type` == `TOTP`	Allow reuse of TOTP tokens within the same time window.
`oath_url`	string		Read-only; protected
`oath_qrcode`	string		Read-only; protected

1.6.1 Retrieve Available Attributes of the *UserAuthentication - MethodModel*

Request

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

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

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

1.6.2 Listing User Authentication Configurations

Request

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

Example Request

GET /api/v2/user/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"
    }
  ]
}
```


1.6.3 Listing Authentication Configurations for User

Request

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

Example Request

GET /api/v2/user/<id>/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"
    }
  ]
}
```


1.6.4 Retrieve User Authentication Configuration by ID

Request

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

Example Request

GET /api/v2/user/<id>/authentication/<id>`

Response


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


(continues on next page)

(continued from previous page)


```
  "user_authentication_method": [
    {
      "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"
    }
  ]
}
```


1.6.5 Create 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

POST /api/v2/user/<id>/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:

POST /api/v2/user/<id>/authentication`

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

Response:

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

Request:

POST /api/v2/user/<id>/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.

1.6.6 Modify User Authentication Method

Request

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

Example Request

Request

PATCH /api/v2/user/<id>/authentication/<id>`

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

Response

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

1.6.7 Deleting User Authentication Method

Request

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

DELETE /api/v2/user/<id>/authentication/<id>`

Response

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

1.7 Location Policies NEW

A location policy decides whether a user may connect from a given place. The policy holds a list of entries - countries or networks - and a mode saying whether those locations are the only ones allowed or the ones blocked. Policies are applied to users through groups.

A built-in `Default` policy applies to every user. Policies bound to groups apply on top of it, so a user's effective set is the built-in policy plus one policy for each of their groups that has one.

1.7.1 Data Structures

Table 20: `LocationPolicyModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Location policy identifier. Uniqueness is required.
`name`	string	yes	Location policy name. Case-insensitive. Uniqueness is required.
`mode`	string {allow_from, block_from}; default value `block_from`		`allow_from` - connections are accepted only from the listed locations. `block_from` - connections from the listed locations are refused. Case-insensitive.
`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.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 21: `LocationPolicyEntryModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`location_policy_`	string	yes	Immutable. Owning location policy.
`policy_name`	string		Read-only; expensive to use. Name of the owning location policy.
`country`	string		ISO 3166-1 alpha-2 country code, uppercase. Set either `country` or `network`; the attribute that is not set is omitted from the response.
`network`	string		CIDR network with no host bits set. Set either `network` or `country`.
`description`	string		Free-text entry description.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 22: `GroupLocationPolicyModel`

Attribute	Type	Required	Description
`id`	string		Read-only; protected.
`group_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `group_id` with attribute `location_policy_id`. Requires `read` right on the `group` object for `GET`, and `modify` for `POST` and `DELETE`.
`location_policy_`	string	yes	Immutable. Uniqueness is required in the combination of attribute `location_policy_id` with attribute `group_id`.
`group_name`	string		Read-only; expensive to use.
`policy_name`	string		Read-only; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.7.2 Retrieve Available Attributes

Request

Method	`GET`
Path	`/api/v2/objspec/location_policy`, `/api/v2/objspec/location_policy_entry`, `/api/v2/objspec/group_location_policy`

GET /api/v2/objspec/location_policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/objspec/location_policy'
```

1.7.3 List Location Policies

Request

Method	GET
Path	/api/v2/location_policy

GET /api/v2/location_policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy'
```

Response


```
{
    "result": "success",
    "location_policy": [
        {
            "id": "1",
            "name": "Default",
            "mode": "block_from",
            "builtin": true,
            "hidden": false,
            "created_at": "2026-08-14 07:29:06.226046-07",
            "modified_at": "2026-08-14 07:29:06.226046-07"
        }
    ]
}
```


1.7.4 Get a Location Policy

Request

Method	GET
Path	/api/v2/location_policy/<id>

GET /api/v2/location_policy/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/4638707616191610881'
```

Response


```
{
    "result": "success",
    "location_policy": {
        "id": "4638707616191610881",
        "name": "Corporate networks",
        "mode": "allow_from",
        "builtin": false,
        "hidden": false,
        "created_at": "2026-08-18 02:17:59.338924-07",
        "modified_at": "2026-08-18 02:17:59.338924-07"
    }
}
```


1.7.5 Create a Location Policy

Request

Method	POST
Path	/api/v2/location_policy
Body	LocationPolicyModel

POST /api/v2/location_policy

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"name":"Corporate networks","mode":"allow_from"}' \
  'https://10.33.3.191/api/v2/location_policy'
```

Response


```
{
    "result": "success",
    "location_policy": {
        "id": "4638707616191610881"
    }
}
```


1.7.6 Modify a Location Policy

Request

Method	PATCH
Path	/api/v2/location_policy/<id>
Body	LocationPolicyModel

PATCH /api/v2/location_policy/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"name":"Corporate networks and Poland"}' \
  'https://10.33.3.191/api/v2/location_policy/4638707616191610881'
```

Response

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

1.7.7 Delete a Location Policy

Request

Method	DELETE
Path	/api/v2/location_policy/<id>

DELETE /api/v2/location_policy/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/4638707616191610881'
```

Response

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

1.7.8 List Location Policy Entries

Request

Method	GET
Path	/api/v2/location_policy/entry

GET /api/v2/location_policy/entry

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/entry'
```

Response

```
{
    "result": "success",
    "location_policy_entry": [
        {
            "id": "4638707616191610881",
            "location_policy_id": "4638707616191610881",
            "policy_name": "Corporate networks",
            "country": "PL",
            "description": "Head office country.",
            "created_at": "2026-08-18 02:17:59.441966-07",
            "modified_at": "2026-08-18 02:17:59.441966-07"
        },
        {
            "id": "4638707616191610882",
            "location_policy_id": "4638707616191610881",
            "policy_name": "Corporate networks",
            "network": "10.33.0.0/16",
            "description": "Corporate LAN.",
            "created_at": "2026-08-18 02:17:59.514519-07",
            "modified_at": "2026-08-18 02:17:59.514519-07"
        }
    ]
}
```


Note

The first entry is a country entry and carries no `network` attribute; the second is a network entry and carries no `country` attribute.

1.7.9 Get a Location Policy Entry

Request

Method	`GET`
Path	`/api/v2/location_policy/entry/<id>`

GET /api/v2/location_policy/entry/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/entry/4638707616191610882'
```

Response


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


(continues on next page)

(continued from previous page)


```
        "id": "4638707616191610882",
        "location_policy_id": "4638707616191610881",
        "policy_name": "Corporate networks and Poland",
        "network": "10.33.0.0/16",
        "description": "Corporate LAN.",
        "created_at": "2026-08-18 02:17:59.514519-07",
        "modified_at": "2026-08-18 02:17:59.514519-07"
    }
}
```


1.7.10 Create a Location Policy Entry

Request

Method	POST
Path	/api/v2/location_policy/entry
Body	LocationPolicyEntryModel

POST /api/v2/location_policy/entry

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"location_policy_id":"4638707616191610881","network":"10.33.0.0/16",
↪"description":"Corporate LAN."}' \
  'https://10.33.3.191/api/v2/location_policy/entry'
```

Response


```
{
    "result": "success",
    "location_policy_entry": {
        "id": "4638707616191610882"
    }
}
```


1.7.11 Modify a Location Policy Entry

Request

Method	PATCH
Path	/api/v2/location_policy/entry/<id>
Body	LocationPolicyEntryModel

PATCH /api/v2/location_policy/entry/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"description":"Corporate LAN (data centre)."}' \
  'https://10.33.3.191/api/v2/location_policy/entry/4638707616191610882'
```

Response

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

1.7.12 Delete a Location Policy Entry

Request

Method	DELETE
Path	/api/v2/location_policy/entry/<id>

DELETE /api/v2/location_policy/entry/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/entry/4638707616191610882'
```

Response

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

1.7.13 List Group Assignments

Request

Method	GET
Path	/api/v2/location_policy/group

GET /api/v2/location_policy/group

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/group'
```

Response

```
{
    "result": "success",
    "group_location_policy": [
        {
            "group_id": "4638707616191610881",
            "location_policy_id": "4638707616191610881",
            "group_name": "Remote operators",
            "policy_name": "Corporate networks",
            "created_at": "2026-08-18 02:18:14.718902-07",
            "modified_at": "2026-08-18 02:18:14.718902-07"
        }
    ]
}
```


1.7.14 Get a Group Assignment

Request

Method	GET
Path	/api/v2/location_policy/<location_policy_id>/group/<group_id>

GET /api/v2/location_policy/<location_policy_id>/group/<group_id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/4638707616191610881/group/
↪4638707616191610881'
```

Response


```
{
    "result": "success",
    "group_location_policy": {
        "group_id": "4638707616191610881",
        "location_policy_id": "4638707616191610881",
        "group_name": "Remote operators",
        "policy_name": "Corporate networks",
        "created_at": "2026-08-18 02:18:14.718902-07",
        "modified_at": "2026-08-18 02:18:14.718902-07"
    }
}
```


1.7.15 Assign a Location Policy to a Group

Request

Method	POST
Path	/api/v2/location_policy/group
Body	GroupLocationPolicyModel

POST /api/v2/location_policy/group

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"group_id":"4638707616191610881","location_policy_id":
↪"4638707616191610881"}' \
  'https://10.33.3.191/api/v2/location_policy/group'
```

Response

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

1.7.16 Remove a Location Policy from a Group

Request

Method	DELETE
Path	/api/v2/location_policy/<location_policy_id>/group/<group_id>

DELETE /api/v2/location_policy/<location_policy_id>/group/<group_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/location_policy/4638707616191610881/group/
↪4638707616191610881'
```

Response

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

1.7.17 Get the Policies Effective for a User

Request

Method	GET
Path	/api/v2/user/<user_id>/effective_location_policy

GET /api/v2/user/<user_id>/effective_location_policy

Returns every location policy that applies to the user: the built-in policy, which applies to everyone and reports an empty `groups` array, plus one entry for each of the user's groups that has a policy assigned, with the groups that brought it in.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/user/4638707616191610882/effective_location_policy
↪'
```

Response


```
{
    "effective_location_policy": [
        {
            "id": "1",
            "name": "Default",
            "mode": "block_from",
            "builtin": true,
            "groups": []
        },
        {
            "id": "4638707616191610881",
            "name": "Corporate networks",
            "mode": "allow_from",
            "builtin": false,
            "groups": [
                {
                    "id": "4638707616191610881",
                    "name": "Remote operators"
                }
            ]
        }
    ],
    "result": "success"
}
```

1.8 User Devices

1.8.1 Data Structures

Table 23: `UserDeviceModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier. Protected.
`user_authentic`	string		Read-only. Unique identifier of the associated authentication method.
`platform`	string	yes	Mobile device platform. It cannot be changed once it has been initialized. Available values: `android`, `ios`.
`pushid`	string	yes	A mobile device identifier necessary to address the device we want to send a push notification. Protected.
`user_id`	string	yes	Immutable. Unique per device. Requires `read` right on the `user` object for `PATCH` requests.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.8.2 Retrieve Available Attributes of the *UserDeviceModel*

Request

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

GET /api/v2/objspec/user_device

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/user_device'
```

1.8.3 Update Mobile Device for Authentication Method

Request

Method	`PATCH`
Path	`/api/v2/user/<user_id>/authentication/ <user_authentication_method_id>/device`
Headers	`Content-Type: Application/json`
Body	`UserDeviceModel`

PATCH /api/v2/user/<user_id>/authentication/<user_authentication_method_id> /device

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/user/9115285645797883905/authentication/
↪9115285645797883999/device' \
  -d '{"pushid": "cihaz-uuid-1234abcd"}'
```

Response

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

1.9 User Mobile Access (Fudo Officer)

1.9.1 Get the User Mobile Access Status

This endpoint returns information about the availability of mobile access for the specified user.

Note

If the **Call Home** feature is disabled, mobile access is not supported and application binding and unbinding operations are unavailable (`is_supported`, `can_bind`, `can_unbind` set to `false`). If the **Call Home** feature is enabled, mobile access is supported and both binding and unbinding operations are available (`true` for all fields).

Request

Method	`GET`
Path	`/api/v2/user/<user_id>/mobile/access`
Headers	`Content-Type: Application/json`

GET /api/v2/user/<user_id>/mobile/access

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user/1224979098644774913/mobile/access'
```

Response

```
{
    "result": "success",
    "mobile_access": {
        "is_supported": true,
        "can_bind": true,
        "can_unbind": true
```

(continues on next page)

(continued from previous page)

```
    }
}
```

1.9.2 Delete User Mobile Access Binding

This endpoint removes (unbinds) the mobile access binding for the specified user.

Request

Method	`DELETE`
Path	`/api/v2/user/<user_id>/mobile/access`
Headers	`Content-Type: Application/json`

DELETE /api/v2/user/<user_id>/mobile/access

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user/1224979098644774913/mobile/access'
```

Response

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

1.10 User Organization

1.10.1 Data Structures

Table 24: `UserOrganizationModel`

Attribute	Type	Required	Description
`organization`	string		Read-only. Unique organization name.

1.10.2 Retrieve Available Attributes of the *UserOrganizationModel*

Request

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

GET /api/v2/objspec/user_organization

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/objspec/user_organization'
```

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

Note

The `user_organization` object provides information about organizations associated with users. This is a read-only object that helps identify organizational affiliations within the system.

1.10.3 List User Organizations

Request

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

GET /api/v2/user/organization

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/user/organization'
```

Response

```
{
    "result": "success",
    "user_organization": [
        {
            "organization": "Engineering"
        },
        {
            "organization": "Security"
        },
        {
            "organization": "Operations"
        }
    ]
}
```

Note

This endpoint returns a list of all organizations that users in the system are associated with. Organizations help categorize and manage user access based on organizational structure.

Warning

Organization information is managed at the system level and cannot be modified through this API endpoint. Organizations are typically configured during user provisioning or through external authentication systems.

1.11 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); secret changing policy as well as the secret changer itself.

1.11.1 Data Structures: *AccountModel*

Table 25: `AccountModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only object Identifier. Requires rights to perform operations on the `account` object: `read` for GET, `modify` for PATCH, and `delete` for DELETE.
`name`	string	yes	Unique account's name
`description`	string		Object description
`note`	string		Read-only; expensive to use
`blocked`	boolean; default value `false`	yes	
`reason`	string	if `blocked` == `true`	
`type`	string {regular, forward, anonymous}	yes	Immutable
`category`	string {nonprivileged, privileged}		
`protocol`	string		Protocol of the pool or server which the account is assigned to. Read-only; expensive to use.
`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

continues on next page

Table 25 – continued from previous page

Attribute	Type	Required	Description
server_port_first	number		Read-only; expensive to use
server_port_last	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
hotseat	boolean; default value false	if type == regular	Enable to be informed about existing connections via the User Access Gateway. Available for the server with protocol == rdp
method	string {account, passvn, password, sshkey, vault}	if type == regular || forward	Authentication method
domain	string	if type == regular || forward	
login	string; may be empty	if type == regular	
secret	string; may be empty	if method == password || sshkey	
secret_passphrase	string	with sshkey	Passphrase to use to decrypt SSH private key.
ssh_public_key	string		SSH public key. Read-only; expensive to use.
ssh_fingerprint_sha256	string		SSH key SHA256 fingerprint. Read-only; expensive to use.
forward_domain	boolean; default value false	if type == forward	
servauth	boolean; default value false	if type == forward	Authentication against server
account_id	string	if method == account	
passvn_id	string	if method == passvn	
passvn_name	string		Read-only; expensive to use

continues on next page

Table 25 – continued from previous page

Attribute	Type	Required	Description
`dump_mode`	string {all, none, raw, noraw}; default value `noraw`	yes	Session recording options. Deprecated for protocols that support the FBS format: starting with version 6.3 such sessions are no longer recorded in RAW, so `all` and `raw` stop producing a RAW dump. Database protocols (Oracle, PostgreSQL, MySQL, MSSQL) are recorded in RAW only and are not affected.
`retention_locked`	boolean; default value `false`	yes	
`retention_remove`	number		Value range from `1` to `2147483647`.
`retention_external`	number		Value range from `1` to `2147483647`.
`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	
`rdp_remote_apps_only`	boolean; default value `false`	yes	Restrict access to the account exclusively through remote applications.
`password_lastupdate`	datetime		Read-only
`password_lastcheck`	datetime		Read-only
`password_change_policy_id`	string	if `type` == `regular`	Password change policy identifier.
`password_change_policy_name`	string		Password change policy name. Read-only; expensive to use.
`password_checkout_time_limit`	datetime (h:m:s)	if `password_change_on_checkin` == `true`	

continues on next page

Table 25 – continued from previous page

Attribute	Type	Required	Description
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_change_trigger_pending	boolean		Waiting for password change after triggered. Read-only; expensive to use.
password_change_trigger_available	boolean		Can manually trigger password change request? Read-only; expensive to use.
password_changer_ids	string-array		Read-only; hidden; expensive to use
password_recovery	boolean		If set and password verification detects unknown password, secret changer will try to recover the password to a known value.
last_login	datetime		Read-only; expensive to use
safes	object-array		JSON object array containing id, name, and position of assigned safes. Read-only; expensive to use.
safe_ids	string-array		Read-only; hidden; expensive to use
safe_names	string-array		Read-only; hidden; expensive to use
servers	object-array		Read-only; expensive to use; JSON object array containing id, mask, name, port and address of assigned servers.
server_ids	string-array		Read-only; hidden; expensive to use
server_names	string-array		Read-only; hidden; expensive to use

continues on next page

Table 25 – continued from previous page

Attribute	Type	Required	Description
`state`	string {created, discovered, onboarded, quarantined}		Account's discovery state: discovered, onboarded, quarantined, or created (for manually created accounts). Read-only. Expensive to use.
`discovered_at`	datetime		Account discovered at timestamp. Read-only; expensive to use
`onboarded_at`	datetime		Account onboarded at timestamp. Read-only; expensive to use.
`onboarded_by_id`	string		User identifier who onboarded this account. Read-only; expensive to use.
`onboarded_by_name`	string		User name who onboarded this account. Read-only; expensive to use.
`quarantined_at`	datetime		Account quarantined at timestamp. Read-only; expensive to use.
`quarantined_by_id`	string		User identifier who quarantined this account. Read-only; expensive to use.
`quarantined_by_name`	string		User name who quarantined this account. Read-only; expensive to use.
`quarantine_reason`	string		Quarantine reason. Read-only; expensive to use.
`scanner_id`	string		Scanner identifier. Read-only; expensive to use.
`scanner_name`	string		Scanner name. Read-only; expensive to use.

continues on next page

Table 25 – continued from previous page

Attribute	Type	Required	Description
secret_exposed	boolean		Determines if there is a user who checked out the current password and now has lost access to the account, e.g. the user is now blocked, deleted, or there is no longer a safe containing both the user and the account, and gives the user secret check out rights. Read-only; expensive to use.
secret_id	string	if method == vault	Password vault secret id.
collection_id	string		Password vault collection id. Read-only; hidden; expensive to use.
secret_name	string		Password vault secret name. Read-only; hidden; expensive to use.
secret_login	string		Password vault secret login. Read-only; hidden; expensive to use.
secret_domain	string		Password vault secret domain. Read-only; hidden; expensive to use.
use_domain_from_secre	boolean; default value false	if method == vault	Use the domain from the linked vault secret for session authentication.
use_login_from_secret	boolean; default value false	if method == vault	Use the login from the linked vault secret for session authentication.
analysis_context	string		AI analysis context. Given to the AI that analyzes sessions using this account. Describe what is normal here so expected activity is not flagged as a risk.
rights	string-array		Read-only; list of rights the subject has to this object.
created_at	datetime		Read-only. Timestamp of creation.

continues on next page

Table 25 – continued from previous page

Attribute	Type	Required	Description
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

1.11.2 Retrieve Available Attributes of the *AccountModel*

Request

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

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

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

1.11.3 Create an Account

Request

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

Example Request

POST /api/v2/account

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/account' \
  -d '{
    "name": "test-account",
    "type": "regular",
    "server_id": "1234567890",
    "method": "password",
    "login": "test-account-login",
    "domain": "my-domain"
  }'
```

Response

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

1.11.4 Get Accounts List

Request

Method	GET
Path	/api/v2/account

1.11.5 Get an Account

Request

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

1.11.6 Modify 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

PATCH /api/v2/account/<id>

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

Response

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

1.11.7 Adding a Secret Changer Policy to Account

Secret Change Policy can't be created via API, but can be assigned to a particular Account. It requires a secret changer or/and Secret verifier assigned according to it's enabled options.

By default there is an existing secret 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

PATCH /api/v2/account/<id>

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

Response

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

1.11.8 Modify Password Change Parameters for Account

Request

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

Example Request

PATCH /api/v2/account/<id>

```
{
   "domain":null,
   "password_change_policy_id":"23456789012345679 89",
   "password_checkout_time_limit":"06:59:00",
   "password_change_on_session_end":true,
   "password_change_on_checkin":true,
   "password_recovery":true
}
```

Response

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

1.11.9 Delete an Account

Request

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

1.11.10 Managing Security Alerts

Request

Method	POST
Path	/api/v2/account/<account_id>/mark_sessions_as_safe

1.12 Account-Safe-Listener Assignment

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); secret changing policy as well as the secret changer itself.

1.12.1 Data Structures: *AccountSafeListenerAssignmentModel*

Table 26: `AccountSafeListenerAssignmentModel`

Attribute	Type	Required	Description
`id`	string		Read-only; protected. Unique identifier.
`account_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `account_id` with attributes `safe_id` and `listener_id`. Requires `read` right on the `account` object for GET, POST, PATCH and DELETE operations.
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attributes `account_id` and `listener_id`. Requires `read` right on the `safe` object for GET, `account-add` right for POST and PATCH, and `account-remove` for DELETE.
`listener_id`	string	yes	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
`account_blocked`	boolean		Read-only; expensive to use; `blocked` state of the assigned account.
`safe_blocked`	boolean		Read-only; expensive to use; `blocked` state of the assigned safe.
`listener_blocke`	boolean		Read-only; expensive to use; `blocked` state of the assigned listener.
`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.

1.12.2 Retrieve Available Attributes of the *AccountSafeListener- Assignment-Model*

Request

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

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

1.12.3 Get Account-Safe-Listener Assignment List

Request

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

Example Request

GET /api/v2/account/safe/listener

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/account/safe/listener'
```

Response


```
{
    "result": "success",
    "account_safe_listener": [
        {
            "account_id": "1224979098644774915",
            "safe_id": "1224979098644774913",
            "listener_id": "1224979098644774914",
            "account_name": "ad-user1-windows",
            "account_type": "regular",
            "protocol": "rdp",
            "server_id": "1224979098644774915",
            "server_name": "windows",
            "safe_name": "main",
            "listener_name": "RDP:bastion",
            "created_at": "2025-08-25 05:08:28.879241-07",
            "modified_at": "2025-08-25 05:08:28.879241-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```

1.12.4 Get Account-Safe-Listener Assignment by ID's

Request

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

Example Request

GET /api/v2/account/<account_id>/safe/<safe_id>/listener/<listener_id>

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/account/1232678819172646919/safe/
↪1232678819172646913/listener/1232678819172646914'
```

Response

```
{
    "result": "success",
    "account_safe_listener": {
        "account_id": "1232678819172646919",
        "safe_id": "1232678819172646913",
        "listener_id": "1232678819172646914",
        "account_name": "VNC_Admin",
        "account_type": "regular",
        "protocol": "vnc",
        "server_id": "1224979098644774918",
        "server_name": "VNC_Server",
        "safe_name": "VNC",
        "listener_name": "VNC_Listen",
        "created_at": "2025-09-22 03:03:08.656825-07",
        "modified_at": "2025-09-22 03:03:14.808987-07",
        "builtin": false,
        "hidden": false
    }
}
```

1.12.5 Create an Account-Safe-Listener Assignments

Request

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

Example Request

POST /api/v2/account/safe/listener

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

Response

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

1.12.6 Modify an Account-Safe-Listener Assignment

Request

Method	`PATCH`
Path	`/api/v2/account/<account_id>/safe/<safe_id>/listener/<listener_id>`
Headers	`Content-Type: Application/json`
Body	`AccountSafeListenerAssignmentModel`

Example Request

PATCH /api/v2/account/<account_id>/safe/<safe_id>/listener/<listener_id>

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
      -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/account/1232678819172646919/safe/
↪1232678819172646913/listener/1232678819172646914' \
      -d '{"listener_id":1232678819172646916}'
```

Response

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

1.12.7 Delete an Account-Safe-Listener Assignment

Request

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

Example Request

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

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/account/1232678819172646919/safe/
↪1232678819172646913/listener/1232678819172646914'
```

Response

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

1.13 Managing Secret Changers and Remote Apps in Accounts

Account Script–related endpoints allow you to manage Secret Changers and Remote Apps within the Accounts configuration.

Note

If you want to learn how to obtain the IDs of Secret Changers and Remote Apps, see the following sections: *Remote Applications*, *Secret Changers*.

1.13.1 Data Structures

Table 27: `AccountScriptModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique. Account Secret ChangerID.
`account_id`	string	yes	Immutable. AccountID. Requires rights on the `account` object: `read` for GET, `modify` for POST, PATCH, and DELETE.
`password_chan`	string		Immutable. Secret ChangerID.
`remote_app_id`	string		Read-only; expensive to use. Remote applicationID.
`password_chan_name`	string	yes	Case-insensitive. Read-only; expensive to use. Secret changer name.
`password_chan_type`	string {`change`, `verify`, `remoteapp`}		Type of secret changer / verifier. Can be assigned only to accounts of type `regular`, using the `password` method, and with a defined `login`. An account can have multiple secret changers, but only one Secret verifier. Read-only.

continues on next page

Table 27 – continued from previous page

Attribute	Type	Required	Description
password_chan _transport	string {LDAP, SSH, Telnet, WinRM}	if password_ _type == change || verify	Read-only; expensive to use. Transport layer for secret changer.
remote_app_pa	string	if password_ _type == remoteapp	Read-only; expensive to use. Binary path for remote app.
remote_app _arguments	string	if password_ _type == remoteapp	Read-only; expensive to use. Binary arguments for remote app.
position	number	if password_ _type == change	Execution order of secret changers. Value range from 0 to 2147483647. Uniqueness is required in the combination of attribute position with attribute account_id.
timeout	number		The execution timeout in seconds. Value range from 0 to 2147483647.
created_at	datetime		Read-only. Timestamp of creation.
modified_at	datetime		Read-only. Timestamp of modification.
removed	boolean		Read-only.

1.13.2 Retrieve Available Attributes of the *AccountScriptModel*

Request

Method	GET
Path	/api/v2/objspec/account_script

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

1.13.3 Get Secret Changers and Remote Apps Assigned to Accounts

Request

Method	GET
Path	/api/v2/account_script

GET /api/v2/account_script

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/account_script'
```

Response


```
{
    "account_script": [
        {
            "account_id": "5683542729741565961",
            "created_at": "2025-06-06 01:00:34.800512-07",
            "id": "5683542729741565967",
            "modified_at": "2025-06-06 01:00:34.800512-07",
            "password_changer_id": "5683542729741565961",
            "password_changer_name": "powershell",
            "password_changer_type": "remoteapp",
            "remote_app_id": "5683542729741565961",
            "remote_app_path": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\
↪powershell.exe"
        },
        {
            "account_id": "5683542729741565959",
            "created_at": "2025-06-06 00:57:09.61763-07",
            "id": "5683542729741565965",
            "modified_at": "2025-06-06 00:57:09.61763-07",
            "password_changer_id": "5683542729741565963",
            "password_changer_name": "putty-defined-variables",
            "password_changer_type": "remoteapp",
            "remote_app_arguments": "-l %%login%% -pw %%password%% -P %%port%% %
↪%host%%",
            "remote_app_id": "5683542729741565963",
            "remote_app_path": "C:\\Windows\\System32\\putty.exe"
        },
        {
            "account_id": "5683542729741565959",
            "created_at": "2025-06-06 00:57:09.628782-07",
            "id": "5683542729741565966",
            "modified_at": "2025-06-06 00:57:09.628782-07",
            "password_changer_id": "5683542729741565964",
            "password_changer_name": "tightvnc",
            "password_changer_type": "remoteapp",
            "remote_app_id": "5683542729741565964",
            "remote_app_path": "C:\\Program Files\\TightVNC\\tvnviewer.exe"
        }
    ],
    "result": "success"
}
```

1.13.4 Get Secret Changer or Remote App Assigned to an Account by Assignment ID

Request

Method	GET
Path	/api/v2/account_script/<id>

GET /api/v2/account_script/<id>

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/account_script/5683542729741565967'
```

Response

```
{
    "account_script": {
        "id": "5683542729741565967",
        "account_id": "5683542729741565961",
        "password_changer_id": "5683542729741565961",
        "remote_app_id": "5683542729741565961",
        "password_changer_type": "remoteapp",
        "password_changer_name": "powershell",
        "remote_app_path": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\
↪powershell.exe",
        "variables": [ ],
        "created_at": "2025-06-06 01:00:34.800512-07",
        "modified_at": "2025-06-06 01:00:34.800512-07"
    },
    "result": "success"
}
```

1.13.5 Assign Secret Changer or Remote App to an Account

Request

Method	POST
Path	/api/v2/account_script
Headers	Content-Type: Application/json
Body	AccountScriptModel

POST /api/v2/account_script

Example Request

```
curl -s -k -X POST  \
-H 'Authorization:<token>'  \
-H 'Content-Type: application/json'  \
```

(continues on next page)

(continued from previous page)

```
https://10.31.96.188/api/v2/account_script \
-d'{"account_id": "5683542729741565961","remote_app_id": "5683542729741565957"}'
```

Response

```
{
    "account_script": {
        "id": "5683542729741565970"
    },
    "result": "success"
}
```

1.13.6 Modify Secret Changer or Remote App Assignment for an Account

Request

Method	PATCH
Path	/api/v2/account_script/<id>
Headers	Content-Type: Application/json
Body	AccountScriptModel

PATCH /api/v2/account_script/<id>

Example Request

```
curl -s -k -X PATCH  \
-H 'Authorization:<token>'  \
-H 'Content-Type: application/json'  \
https://10.31.96.188/api/v2/account_script/5683542729741565969 \
-d'{"account_id": "5683542729741565961","remote_app_id": "5683542729741565957"}'
```

Response

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

1.13.7 Delete Secret Changer or Remote App Assignment from an Account

Request

Method	DELETE
Path	/api/v2/account_script/<id>

DELETE /api/v2/account_script/<id>

Example Request

```
curl -s -k -X DELETE \
-H 'Authorization:<token>' \
https://10.31.96.188/api/v2/account_script/5683542729741565970
```

Response

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

1.14 Account Notes

Account notes related endpoints enable managing messages displayed to users in the User Portal (Access Gateway).

1.14.1 Data Structures

Table 33: `AccountNoteModel`

Attribute	Type	Required	Description
`id`	string		Read-only; protected. Account note identifier.
`account_id`	string	yes	Immutable. ID of the account to which the note is assigned. Requires rights to perform operations on the `account` object: `read` for GET, `modify` for POST, PATCH, and DELETE.
`note`	string	yes	Note.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.14.2 Retrieve Available Attributes of the *AccountNoteModel*

Request

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

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

1.14.3 Get a Note From Account

Request

Method	`GET`
Path	`/api/v2/account/<account_id>/note`

Example Request

GET /api/v2/account/<id>/note

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/account/9124292845052624908/note'
```

Response

```
{
    "note": "Note content.",
    "result": "success"
}
```

1.14.4 Assign Note to an Account

Request

Method	POST
Path	/api/v2/account/<account_id>/note
Headers	Content-Type: Application/json
Body	AccountNoteModel

Example Request

POST /api/v2/account/<id>/note

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/account/9124292845052624908/note' \
  -d'{"note":"Note content."}'
```

Response

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

1.14.5 Modify a Note

Request

Method	PATCH
Path	/api/v2/account/<account_id>/note
Headers	Content-Type: Application/json
Body	AccountNoteModel

Example Request

PATCH /api/v2/account/<id>/note

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/account/9124292845052624908/note' \
  -d'{"note":"Note modified content."}'
```

Response

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

1.14.6 Deleting a Note

Request

Method	DELETE
Path	/api/v2/account/<account_id>/note

Example Request

DELETE /api/v2/account/<id>/note

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/account/9124292845052624908/note'
```

Response

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

1.15 Servers

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

1.15.1 Data Structures

Table 34: `ServerModel`

Attribute	Type	Required	Description
`id`	string	yes	Unique, read-only object identifier. Requires `read` right on object type `server` for `GET` requests, `modify` for `PATCH` requests, and `delete` for `DELETE` requests.
`name`	string	yes	Unique server's name.
`description`	string		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`, `port_first` and `port_last`
`mask`	number {from 0 to 128}		Uniqueness is required in the combination of attribute `mask` with attributes `address`, `port_first` and `port_last`.
`port_first`	number		Value-format: port. Uniqueness is required in the combination of attribute `port_first` with attributes `address`, `mask` and `port_last`.

continues on next page

Table 34 – continued from previous page

Attribute	Type	Required	Description
port_last	number		Value-format: port. Uniqueness is required in the combination of attribute port_last with attributes address, mask and port_first.
port	number	yes	Value-format: port. Server port number if no port range. Read-write; Expensive to use.
legacy_crypto	boolean; default value false	If protocol == ssh || (protocol == http || mysql || oracle || pgsql || telnet || tn3270 || tn5250 || rdp || vnc & tls_enabled == true)	Enabling legacy cryptographic protocols and settings.
tunneled	boolean; default value false	yes	
tunnel_key	string	If tunneled == true	SSH public key for tunneled connections. Value-format: ssh-public-key.
protocol	string {http, modbus, mysql, oracle, pgsql, rdp, ssh, tcp, tds, telnet, tn3270, tn5250, vnc}	yes	Immutable; case insensitive.
http	HTTPServerAttributes	If protocol == http	HTTP protocol properties.
mysql	MySQLServerAttributes	If protocol == mysql	MySQL 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. Value-format: ssh-public-key.
last_login	datetime		Read-only; Expensive to use.

continues on next page

Table 34 – continued from previous page

Attribute	Type	Required	Description
pools	object-array		Read-only; Expensive to use; JSON object array containing id and name of assigned pools.
pool_ids	string-array		Read-only; Hidden; Expensive to use.
pool_names	string-array		Read-only; Hidden; Expensive to use.
state	string {created, discovered, onboarded, quarantined}		Discovery state. Read-only; Expensive to use.
discovered_at	datetime		Read-only; Expensive to use. Server discovered at timestamp.
onboarded_at	datetime		Read-only; Expensive to use. Server onboarded at timestamp.
onboarded_by_id	string		Read-only; Expensive to use. User identifier who onboarded this server.
onboarded_by_na	string		Read-only; Expensive to use. User name who onboarded this server.
quarantined_at	datetime		Read-only; Expensive to use. Server quarantined at timestamp.
quarantined_by_	string		Read-only; Expensive to use. User identifier who quarantined this server.
quarantined_by_	string		Read-only; Expensive to use. User name who quarantined this server.

continues on next page

Table 34 – continued from previous page

Attribute	Type	Required	Description
scanner_id	string		Read-only; Expensive to use. Scanner identifier.
scanner_name	string		Read-only; Expensive to use. Scanner name.
analysis_contex	string		AI analysis context. Given to the AI that analyzes sessions on this server. Describe what is normal here so expected activity is not flagged as a risk.
rights	string-array		Read-only. List of rights the subject has to this object.
created_at	datetime		Read-only.
modified_at	datetime		Read-only.
removed	boolean		Read-only.
builtin	boolean		Read-only; Expensive to use. Is object built-in? Built-in objects shouldn't be editable.
hidden	boolean		Read-only; Expensive to use. Shall the object be hidden in UI?

Table 35: `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`		
`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 36: `MySQLServerAttributes`

Attribute	Type	Required	Description
`mysql_tls_required`	boolean; default value `false`	If `protocol` == `mysql` & `tls_enabled` == `true`	Require TLS for MySQL connections.

Table 37: `RDPServerAttributes`

Attribute	Type	Required	Description
`rdp_hotseat`	boolean; default value `false`	If `protocol` == `rdp`	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. Value-format: public-key.

Table 38: `TLSServerAttributes`

Attribute	Type	Required	Description
`tls_enabled`	boolean; default value `true`	If `protocol` == `http` || `mysql` || `oracle` || `pgsql` || `telnet` || `tn3270` || `tn5250` || `rdp` || `vnc`	Enabling the TLS protocol.
`tls_ca_certifica`	string	If `protocol` == `http` || `mysql` || `oracle` || `pgsql` || `telnet` || `tn3270` || `tn5250` || `rdp` || `vnc` & `tls_enabled` == `true`	TLS CA certificate. Value-format: x509-ca-certificate.
`tls_certificate`	string	If `protocol` == `http` || `mysql` || `oracle` || `pgsql` || `telnet` || `tn3270` || `tn5250` || `rdp` || `vnc` & `tls_enabled` == `true`	TLS certificate. Value-format: x509-certificate.
`tls_verify_hostn`	boolean	If `tls_enabled` == `true` & `tls_ca_certificate` is set	Verify that the host name of the server matches the name in the certificate presented by it.

1.15.2 Retrieve Available Attributes of the *ServerModel*

Request

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

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

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

1.15.3 Create a Server

Request

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

Example Request

POST /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" }}
```

1.15.4 Get Servers List

Request

Method	GET
Path	/api/v2/server

1.15.5 Get a Server

Request

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

Example Request

GET /api/v2/server/<id>

```
   {
"result": "success",
"server": {
   "id": "46026788191726469 16",
   "name": "my-1st-rdp-server",
```

(continues on next page)

(continued from previous page)


```
    "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"
}}
```


1.15.6 Modify 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

PATCH /api/v2/server/<id>

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

Response

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

1.15.7 Deleting a Server

Request

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

1.16 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.

1.16.1 Data Structures

Table 39: `PoolModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only object identifier. Requires the following rights on object type `pool` depending on the HTTP method used: `GET` → `read`, `PATCH` → `modify`, `DELETE` → `delete`.
`name`	string	yes	Unique pool's name
`description`	string		
`servers`	object-array		Read-only; expensive to use; JSON object array containing `id`, `mask`, `name`, `port` and `address` of assigned servers.
`server_ids`	string-array		Read-only; hidden; expensive to use
`server_names`	string-array		Read-only; hidden; expensive to use
`protocol`	string		Read-only; expensive to use.
`rights`	string-array		Read-only. List of rights the subject has to this object.
`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.

1.16.2 Retrieve Available Attributes of the *PoolModel*

Request

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

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

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

1.16.3 Get Pools List

Request

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

Example Request

GET /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",
        "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"
        ]}]}
```


1.16.4 Get a Pool

Request

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

Example Request

GET /api/v2/pool/<id>

Response


```
    {
"result": "success",
"pool": {
    "id": "1232678819172646915",
```


(continues on next page)

(continued from previous page)

```
    "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"
    ]}}
```

1.16.5 Create a Pool

Request

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

Example Request

POST /api/v2/pool

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

Response

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

1.16.6 Modify a Pool

Request

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

Example Request

PATCH /api/v2/pool/<id>

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

Response

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

1.16.7 Deleting a Pool

Request

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

1.17 Pool-Server Assignment

1.17.1 Data Structures

Table 40: `ServerPoolModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only object identifier. Requires the following rights on object type `pool` depending on the HTTP method used: `GET` → `read`, `POST` → `server-add`, `DELETE` → `server-remove`.
`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`. Requires the following rights on object type `server` depending on the HTTP method used: `GET`, `POST`, `DELETE` → `read`.
`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.

1.17.2 Retrieve Available Attributes of the *ServerPoolModel*

Request

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

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

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

1.17.3 Get Pool-Server Assignment List

Request

Method	GET
Path	/api/v2/pool/server

Example Request

GET /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"
    }]}
```


1.17.4 Get Pool-Server Assignment List by ID's

Request

Method	GET
Path	/api/v2/pool/<pool_id>/server/<server_id>

Example Request

GET /api/v2/pool/<pool_id>/server/<server_id>

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/pool/1232678819172646915/server/
↪1232678819172646913'
```

Response

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


1.17.5 Adding a Server to the Pool

Request

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

Example Request

POST /api/v2/pool/server


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


Response


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


1.17.6 Deleting a Server From a Pool

Request

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

1.18 Listeners

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

1.18.1 Data Structures

Table 41: `ListenerModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Listener identifier.
`name`	string	yes	Listener name. Uniqueness is required.
`blocked`	boolean; Default value `false`	yes	
`reason`	string	if `blocked` == `true`	
`announcement`	string		
`ignore_case`	boolean; Default value `false`	if `protocol` == `ssh` || `vnc`	
`legacy_crypto`	boolean; Default value `false`	if `mode` == `tunnel` || `protocol` == `ssh` || (`protocol` == `http` || `mysql` || `oracle` || `pgsql` || `rdp` || `vnc` & `tls_enabled` == `true`)	Are legacy cryptographic protocols and settings enabled?
`protocol`	string {http, modbus, mysql, oracle, pgsql, rdp, ssh, tcp, tds, telnet, tn3270, tn5250, vnc}	yes	Immutable. Protocol used.
`mode`	string {bastion, proxy, tunnel}	yes	Mode of operation.
`listen_ip`	string; Default value `0.0.0.0`	if `mode` == `bastion` || `proxy` || `tunnel`	IP address for user connections
`listen_port`	number {1-60000}	if `mode` == `bastion` || `proxy` || `tunnel`	Port number for user connections.
`external_addres`	string	with `external_port`	Listener address to present in Access Gateway
`external_port`	number	with `external_address`	Value-format: port. Listener port to present in Access Gateway.
`http_render`	boolean; Default value `true`	if `mode` == `tunnel` & `protocol` == `http`	Is graphical representation for HTTP(S) sessions enabled?
`rdp_config_doma`	string		Domain suffix for RDP configuration files. Requires `protocol` == `rdp`.
`rdp`	ListenerRDPAttributes	If `protocol` == `rdp`	RDP protocol properties
`ssh`	ListenerSSHAttributes	If `protocol` == `ssh`	SSH protocol properties

continues on next page

Table 41 – continued from previous page

Attribute	Type	Required	Description
`tds`	ListenerTDSAttributes	If `protocol == tds`	TDS protocol properties
`tls`	ListenerTLSAttributes	If `protocol == http || mysql || oracle || pgsql || rdp || vnc`	TLS protocol properties
`created_at`	datetime		Read-only. Object creation time.
`modified_at`	datetime		Read-only. Object last modification time.
`removed`	boolean		Read-only. Is the object removed?
`builtin`	boolean		Read-only; expensive to use. Is object built-in? Built-in objects shouldn't be editable.
`hidden`	boolean		Read-only; expensive to use. Shall the object be hidden in UI?

Table 42: `ListenerRDPAttributes`

Attribute	Type	Required	Description
`rdp_legacy`	boolean	if `mode == tunnel || protocol == rdp`	Use the legacy RDP implementation instead of the current one.
`rdp_nla_enabled`	boolean; default value `false`	if `mode == tunnel && protocol == rdp && tls_enabled == true`	Enables RDP Network Level Authentication (NLA).
`rdp_private_key`	string	if `mode == tunnel && protocol == rdp && tls_enabled == false`	RDP private key. Protected. Format: `private-key`.
`rdp_private_key_p`	string	if `rdp_private_key` is set	Passphrase to decrypt RSA private key. Protected.
`rdp_public_key`	string		RDP public key. Read-only. Expensive to retrieve. Requires `rdp_private_key` and either `mode == tunnel` or `protocol == rdp && tls_enabled == false`.

Table 43: `ListenerSSHAttributes`

Attribute	Type	Required	Description
`ssh_private_key`	string	if `mode == tunnel || protocol == ssh`	SSH private key. Protected. Format: `ssh-private-key`.
`ssh_private_key_p`	string	if `ssh_priva` is set	Passphrase to decrypt SSH private key. Protected.
`ssh_proxyjump`	boolean; default value `false`	if `protocol == ssh && mode == proxy || bastion`	Is SSH ProxyJump function enabled?
`ssh_public_key`	string		SSH public key. Read-only. Expensive to retrieve. Requires `protocol == ssh` or `mode == tunnel`.
`ssh_fingerprint_s`	string		SHA256 fingerprint of SSH key. Read-only. Expensive to retrieve. Requires `protocol == ssh` or `mode == tunnel`.

Table 44: `ListenerTDSAttributes`

Attribute	Type	Required	Description
`tds_cd_enabled`	boolean; default value `false`	if `mode == tunnel && protocol == tds`	Is constrained delegation enabled for TDS?
`tds_cd_spn`	string	if `tds_cd_en == true`	Service principal name, for use with constrained delegation.
`tds_cd_keytab`	string	if `tds_cd_en == true`	Contents of the keytab file (Base64-encoded), for use with constrained delegation.

Table 45: `ListenerTLSAttributes`

Attribute	Type	Required	Description
`tls_enabled`	boolean; default value `true`	if `mode == proxy || bastion && protocol == http || mysql || pgsql || rdp || vnc`	Is TLS protocol enabled?
`tls_private_key`	string	if `mode == tunnel || (tls_enabled == true && protocol == http || mysql || pgsql || rdp || vnc &&` `tls_certificate` is set)	TLS private key. Protected. Format: `private-key`.
`tls_private_key_p`	string	if `tls_private_key` is set	Passphrase to decrypt TLS private key. Protected.
`tls_certificate`	string	if `mode == tunnel || (tls_enabled == true && protocol == http || mysql || pgsql || rdp || vnc &&` `tls_private_key` is set)	TLS certificate. Format: `x509-chain`.
`tls_certificate_c`	string		Read-only; expensive to use. TLS certificate commonName. Requires `mode == tunnel || (protocol == http || mysql || pgsql || rdp || vnc && tls_enabled == true`).
`tls_certificate_f`	string		Read-only; expensive to use. TLS certificate SHA1 fingerprint. Requires `mode == tunnel || (protocol == http || mysql || pgsql || rdp || vnc && tls_enabled == true`).
`tls_certificate_f`	string		Read-only; expensive to use. TLS certificate SHA256 fingerprint. Requires `mode == tunnel || (protocol == http || mysql || pgsql || rdp || vnc && tls_enabled == true`).

1.18.2 Retrieve Available Attributes of the *ListenerModel*

Request

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

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

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

1.18.3 Get Listeners List

Request

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

Example Request

GET /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-----\
↪nMIIE0DCCArigAwIBAgIUSGWBY/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"
```


(continues on next page)

(continued from previous page)


```
    },
    {
        "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" }]
```


1.18.4 Create a Listener

Request

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

1.18.5 Get a Listener

Request

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

1.18.6 Modify a Listener

Request

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

Example Request: Changing the Listener's Address

PATCH /api/v2/listener/<id>

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

Response

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

1.18.7 Delete a Listener

Request

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

1.19 Safes

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

1.19.1 Data Structures

Table 46: `SafeModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only object identifier. Requires the following rights on object type `safe` depending on the HTTP method used: `GET` → `read`, `PATCH` → `modify`, `DELETE` → `delete`.
`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 User Access Gateway
`webclient`	boolean; default value `true`	if `fudo_network` == `true`	Enable connecting to the session in browser
`fudo_network`	boolean; default value `false`	yes	
`confirmation_timeout`	number; default value `5`	yes	
`inactivity_limit`	number; default value `0`	yes	

continues on next page

Table 46 – continued from previous page

Attribute	Type	Required	Description
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
jit_mode	string {always, time_policy}; default value always		Just-in-time access mode. always - an approved access request is always required. time_policy - approval is skipped during the daily access policy hours and required only outside them.
backup_id	string		Target destination ID for storing session data
backup_name	string		Read-only; expensive to use
allow_user_sharing	boolean; default value false	yes	Allow users to share their own live sessions from the User Access Gateway
live_supervision_requi	boolean	if allow_user_sha == true	Require live supervision of the sessions established through the safe. Can be set only when allow_user_sharing is true
min_supervisors	number	if live_supervisi == true	Number of supervisors required; minimum value 1. Can be set only when live_supervision_required is true
http_rendered_file_dow	boolean; default value false	yes	Enable file download in HTTP-rendered sessions
http_rendered_file_upl	boolean; default value false	yes	Enable file upload in HTTP-rendered sessions

continues on next page

Table 46 – continued from previous page

Attribute	Type	Required	Description
`http_rendered_file_quo`	number; default value 524288000	yes	File quota in bytes for HTTP-rendered sessions
`http_rendered_mode`	string {kiosk, full_browser}; default value `kiosk`	yes	Browser mode for HTTP-rendered sessions
`http_rendered_redirect`	boolean; default value `true`	if `http_rendered_ == full_browser`	Enable popup redirection in HTTP-rendered sessions
`http_rendered_kiosk_ur`	string {hidden, readonly, editable}; default value `hidden`	if `http_rendered_ == kiosk`	
`http_rendered_kiosk_ma`	number; default value `1`		Maximum number of tabs available in kiosk mode. Set to null for an unlimited number of tabs
`rdp`	SafeRDPAttributes	If `protocol == rdp`	
`ssh`	SafeSSHAttributes	If `protocol == ssh`	
`vnc`	SafeVNCAttributes	If `protocol == vnc`	
`analysis_context`	string		AI analysis context. Given to the AI that analyzes sessions in this safe. Describe what is normal here so expected activity is not flagged as a risk.
`rights`	string-array		Read-only. List of rights the subject has to this object.
`created_at`	datetime		Read-only
`modified_at`	datetime		Read-only
`removed`	boolean		Read-only
`last_login`	datetime		Read-only; expensive to use
`accounts`	object-array		Read-only; expensive to use; JSON object array containing `id`, `name`, and `type` of assigned accounts.

continues on next page

Table 46 – continued from previous page

Attribute	Type	Required	Description
`account_ids`	string-array		Read-only; hidden; expensive to use
`account_names`	string-array		Read-only; hidden; expensive to use
`users`	object-array		Read-only; expensive to use
`user_ids`	string-array		Read-only; hidden; expensive to use
`user_names`	string-array		Read-only; hidden; expensive to use
`listeners`	object-array		Read-only; expensive to use
`listener_ids`	number-array		Read-only; hidden; expensive to use
`listener_names`	string-array		Read-only; hidden; expensive to use
`group_ids`	string-array		IDs of the groups granted access to the safe. Read-only; hidden; 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.

Table 47: `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_cliprdr_fi`	boolean; default value `true`	yes	Allow file transfer over the redirected clipboard. Set to `false` to keep clipboard redirection enabled for text while blocking files.
`rdp_config`	string		Custom content to be added to the RDP configuration file when the native client RDP connection is requested via Access Gateway.
`rdp_depth`	number {8, 16, 24, 32}		Max. color depth
`rdp_rdpdr`	boolean; default value `true`	yes	
`rdp_rdpsnd`	boolean; default value `true`	yes	Sound redirection
`rdp_sndrec`	boolean; default value `true`	yes	Record the RDP audio stream into the session dump.
`rdp_drdynvc`	boolean; default value `true`	yes	
`rdp_resolution`	string {800x600, 1024x600, 1024x768, 1152x864, 1280x720, 1280x768, 1280x800, 1280x960, 1280x1024, 1360x768, 1400x1050, 1440x900, 1600x900, 1680x1050, 1600x1200, 1920x1080, 1920x1200, 2048x1152, 2560x1440, 2560x1600}		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 48: `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_record_file_transfer`	boolean; default value `true`	yes
`ssh_record_port_forwardin`	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 49: `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

1.19.2 Get Available Attributes of the `SafeModel`

Request

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

1.19.3 Data Structures: *UserSafeAssignmentModel*

Table 50: `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`. Requires `read` right on object type `user` for `GET`, `POST`, `PATCH`, and `DELETE` requests.
`roles`	object-array		Read-only; expensive to use.
`role_names`	string-array		Read-only; hidden; expensive to use.
`role_ids`	string-array		Read-only; hidden; expensive to use.

continues on next page

Table 50 – continued from previous page

Attribute	Type	Required	Description
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `user_id`. Requires `read` right on object type `safe` for `GET` requests, `user-add` right for `POST` and `PATCH`, and `user-remove` right for `DELETE` requests.
`blocked`	boolean; default value `false`	yes	Access to this safe is disabled for the user.
`position`	number		
`password_visible`	boolean; default value `false`	yes	Allow a user to use Secret Checkout feature and view passwords in the User Access Gateway.
`time_policy_che`	string		Read-only; expensive to use. Checksum computed from time policies used for this user-safe connection.
`use_time_policy`	boolean; default value `false`	yes	Enables the daily access policy for this user-safe connection. On a Safe with `jit_mode` set to `time_policy` it also decides when an access request is required - see *Safes*.
`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.
`user_domain`	string		Read-only; expensive to use.
`user_email`	string		Read-only; expensive to use.
`user_organizatic`	string		Read-only; expensive to use.
`safe_name`	string		Read-only; expensive to use.
`user_blocked`	boolean		Read-only; expensive to use; `blocked` state of the assigned user.
`safe_blocked`	boolean		Read-only; expensive to use; `blocked` state of the assigned safe.
`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.

1.19.4 Retrieve Available Attributes of the *UserSafeAssignmentModel*

Request

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

1.19.5 Data Structures: *UserSafeTimePolicyAssignmentModel*

Table 51: `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. Requires `read` right on object type `user` for `GET` requests, and `modify` right for `POST`, `PATCH`, and `DELETE` requests.
`safe_id`	string	yes	Immutable. Requires `read` right on object type `safe` for `GET`, `POST`, and `PATCH` requests.
`user_name`	string		Read-only; expensive to use.
`user_role`	string		Read-only; expensive to use.
`safe_name`	string		Read-only; expensive to use.
`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.

1.19.6 Retrieve Available Attributes of the *UserSafeTimePolicy - AssignmentModel*

Request

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

Table 52: `SafePolicyAssignmentModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only, protected object Identifier
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attributes `policy_id`. Requires `read` right on object type `safe` for `GET` requests, and `modify` right for `DELETE` and `POST` requests.
`policy_id`	string		Immutable. Uniqueness is required in the combination of attribute `policy_id` with attributes `safe_id`.
`safe_name`	string		Read-only; expensive to use
`policy_name`	string		Read-only; expensive to use
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.19.7 Retrieve Available Attributes of the *SafePolicyAssignmentModel*

Request

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

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

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

1.19.8 Get Safes List

Request

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

Example Request

GET /api/v2/safe

Response

```
   { "result": "success",
"safe": [
   {
       "id": "123678819172646913",
       "name": "main",
       "blocked": false,
       "login_reason": false,
```

(continues on next page)

(continued from previous page)


```
        "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,
        "jit_mode": "always",
        "rdp_audin": true,
        "rdp_cliprdr": true,
        "rdp_rdpdr": true,
        "rdp_rdpsnd": true,
        "rdp_drdynvc": 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"
        ]}]}
```


1.19.9 Create a Safe

Request

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

Example Request

POST /api/v2/safe

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

Response

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

1.19.10 Get a Safe

Request

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

Example Request

GET /api/v2/safe/<id>

Response

```
    { "result": "success",
"safe": {
    "id": "1232678819172646915",
    "name": "my-1st-safe",
    "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,
    "jit_mode": "always",
    "rdp_audin": true,
    "rdp_cliprdr": true,
    "rdp_rdpdr": true,
    "rdp_rdpsnd": true,
    "rdp_drdynvc": 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,
```

(continues on next page)

(continued from previous page)

```
    "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" }}
```

1.19.11 Modify 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

PATCH /api/v2/safe/<id>

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

To require approval only outside the daily access policy hours of the user-safe assignment, set `jit_mode` to `time_policy` as well:

```
{ "required_votes": 5, "jit_mode": "time_policy" }
```

Response

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

1.19.12 Delete a Safe

Request

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

1.19.13 Get Users' Time Policy Settings Within Safes

Request

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

Example Request

GET /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"
   }]}
```

1.19.14 Modify 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

PATCH /api/v2/user/safe/time_policy/<id>

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

Response

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

1.19.15 Get User's Settings Within a Safe

Request

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

1.19.16 Modify 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 User Access Gateway

PATCH /api/v2/user/<user_id>/safe/<safe_id>

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

Response

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

1.19.17 Delete a User From a Safe

Request

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

1.19.18 Get Users Allowed to Manage Selected Safe

Request

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

1.19.19 Get Account-Safe-Listener Assignments List

Request

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

1.19.20 Create an Account-Safe-Listener Assignments

Request

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

Example Request

POST /api/v2/account/safe/listener

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

Response

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

1.19.21 Delete an Account-Safe-Listener Assignment

Request

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

1.19.22 Get Safe-Policy Assignments List

Request

Method	GET
Path	/api/v2/safe/policy

Example Request

GET /api/v2/safe/policy/

```
curl -s -k -X GET -H 'Authorization: <token>' /api/v2/safe/policy
```

Response

```
{
    "result": "success",
    "safe_policy": [
        {
            "safe_id": "9124292845052624898",
```

(continues on next page)

(continued from previous page)

```
            "policy_id": "9124292845052624898",
            "safe_name": "RDP_Safe",
            "policy_name": "AI_Policy_1",
            "created_at": "2024-06-21 06:15:12.135699-07",
            "modified_at": "2024-06-21 06:15:12.135699-07"
        }
    ]
}
```

1.19.23 Checking Safe-Policy Assignment by ID

Request

Method	`GET`
Path	`/api/v2/safe/<safe_id>/policy/<policy_id>`
Headers	`Content-Type: Application/json`
Body	`PolicyModel`

Example Request

GET /api/v2/safe/<safe_id>/policy/<policy_id>

```
curl -s -k -X GET -H 'Authorization: <token>' /api/v2/safe/9124292845052624898/
↪policy/9124292845052624898
```

Response

```
{
    "result": "success",
    "safe_policy": [
        {
            "safe_id": "9124292845052624898",
            "policy_id": "9124292845052624898",
            "safe_name": "RDP_Safe",
            "policy_name": "AI_Policy_1",
            "created_at": "2024-06-21 06:15:12.135699-07",
            "modified_at": "2024-06-21 06:15:12.135699-07"
        }
    ]
}
```

1.19.24 Create an Safe-Policy Assignments

Request

Method	`POST`
Path	`/api/v2/safe/policy`
Headers	`Content-Type: Application/json`
Body	`SafePolicyAssignmentModel`

Example Request

POST /api/v2/safe/policy

```
curl -s -k -X POST -H 'Authorization: <token>' /api/v2/safe/policy \
-H 'Content-Type: application/json' \
-d '{"safe_id":"9124292845052624898","policy_id":"9124292845052624898"}'
```

Response

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

1.19.25 Delete a Safe-Policy Assignment

Request

Method	DELETE
Path	/api/v2/safe/<safe_id>/policy/<policy_id>

Example Request

DELETE /api/v2/safe/<safe_id>/policy/<policy_id>

```
curl -s -k -X DELETE -H 'Authorization: <token>' /api/v2/safe/
↪9124292845052624898/policy/9124292845052624898
```

Response

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

1.20 Safe Notifications

1.20.1 Data Structures

Table 53: `SafeNotificationUserModel`

Attribut	Type	Required	Description
`safe_`	string		Read-only. Unique safe identifier.
`user_`	string		Read-only. Unique user identifier.
`user_`	string		Read-only. Username for notification recipient.
`user_`	string		Read-only. User domain.
`user_`	string		Read-only. User email address.
`emai`	number		Read-only. Email notification count or status.
`push_`	number		Read-only. Push notification count or status.
`roles`	object-array		Read-only. User roles related to safe notifications.
`role_`	string-array		Read-only. Hidden attribute. Array of role names.
`role_`	string-array		Read-only. Hidden attribute. Array of role identifiers.

1.20.2 Retrieve Available Attributes of the *SafeNotificationUsersModel*

Request

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

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

1.20.3 Get Safe Notification Settings for Users

Request

Method	`GET`
Path	`/api/v2/safe/<safe_id>/notification_user`

GET /api/v2/safe/<safe_id>/notification_user

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/safe/2/notification_user'
```

Response


```
{
    "result": "success",
    "safe_notification_user": [
        {
            "safe_id": "2",
            "user_id": "user456",
            "user_name": "security.admin",
            "user_domain": "internal.com",
            "user_email": "security.admin@internal.com",
            "email_notifications": 5,
            "push_notifications": 3,
            "roles": [
                {
                    "id": "role789",
                    "name": "Safe Administrator"
                }
            ]
        }
    ]
}
```


1.21 User Group Safe

1.21.1 Data Structures

Table 54: `UserGroupSafeModel`

Attribute	Type	Required	Description
`user_id`	string	yes	Immutable. Unique with `safe_id`. ID of the user assigned to safe through groups.
`user_name`	string		Read-only. Username of the user assigned to safe through groups.
`safe_id`	string	yes	Immutable. Unique with `user_id`. ID of the safe to which user is assigned through groups.
`safe_name`	string		Read-only. Name of the safe to which user is assigned through groups.
`groups`	object-array		Read-only. List of groups through which user is assigned to safe.
`group_ids`	string-array		Read-only. Hidden. List of group IDs through which user is assigned to safe.
`group_names`	string-array		Read-only. Hidden. List of group names through which user is assigned to safe.
`group_names_al`	string		Read-only. Hidden; expensive to use. All group names, separated by space.

1.21.2 Retrieve Available Attributes of the *UserGroupSafeModel*

Request

Method	GET
Path	/api/v2/objspec/user_group_safe

GET /api/v2/objspec/user_group_safe

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/objspec/user_group_safe'
```

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

Note

The `user_group_safe` object represents the relationship between users and safes through group membership. This provides an indirect way to grant safe access through group assignments rather than direct user-to-safe assignments.

1.21.3 List User Group Safe Assignments

Request

Method	GET
Path	/api/v2/user/group/safe

GET /api/v2/user/group/safe

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/user/group/safe'
```

Response

```
{
    "result": "success",
    "user_group_safe": [
        {
            "user_id": "8754997675608244225",
            "user_name": "admin",
            "safe_id": "8754997675608244225",
            "safe_name": "main",
            "groups": [
```

(continues on next page)

(continued from previous page)


```
                {
                    "id": "8754997675608244225",
                    "name": "DevTeam"
                }
            ]
        },
        {
            "user_id": "8754997675608244227",
            "user_name": "jdoe",
            "safe_id": "8754997675608244225",
            "safe_name": "main",
            "groups": [
                {
                    "id": "8754997675608244225",
                    "name": "DevTeam"
                }
            ]
        }
    ]
}
```


Note

This endpoint provides a comprehensive view of how users gain access to safes through group membership. It's particularly useful for:

- **Access auditing**: Understanding the complete chain of access from user to safe through groups
- **Compliance reporting**: Tracking indirect access permissions for security audits
- **Access management**: Identifying which groups grant access to specific safes

Warning

The `user_group_safe` relationships are read-only and automatically calculated based on:

- Current user-to-group assignments
- Current group-to-safe assignments
- Active group memberships and safe permissions

To modify these relationships, use the appropriate group management or safe permission endpoints.

1.22 Group-Derived Safe Access Policies NEW

A user can reach a safe directly or through a group. This resource holds a per-user override for access a user has **through a group**: it narrows the group's grant for that one user without touching the group itself or the other members.

The override can only be created for a user who already reaches the safe through a group. Creating it for a user with no such path fails with `{"result": "failure", "message": "User does not reach the safe through any group."}`.

> **Note**
>
> The override lives only as long as the group path does. When the last group granting the user access to the safe is removed, the override is removed with it.

1.22.1 Data Structures

Table 55: `UserGroupSafePolicyModel`

Attribute	Type	Required	Description
`id`	string		Read-only; protected.
`user_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `safe_id`. Requires `read` right on object type `user` for all methods.
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `user_id`. Requires `read` right on object type `safe` for `GET`, `user-add` for `POST` and `PATCH`, and `user-remove` for `DELETE`.
`blocked`	boolean; default value `false`	yes	Access to this safe is disabled for the user.
`use_time_polic`	boolean; default value `false`	yes	Restrict the user's access to the hours defined by the time policy entries.
`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. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 56: `UserGroupSafePolicyTimePolicyModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`user_group_safe_p`	string		Read-only; protected. Owning override.
`user_id`	string	yes	Immutable. Requires `read` right on object type `user` for `GET`, and `modify` for the other methods.
`safe_id`	string	yes	Immutable. Requires `read` right on object type `safe`.
`user_name`	string		Read-only; expensive to use.
`safe_name`	string		Read-only; expensive to use.
`day_of_week`	number	yes	Day the entry applies to. Value range from 1 to 7.
`valid_from`	datetime (h:m:s)	yes	Beginning access time on that day.
`valid_to`	datetime (h:m:s)	yes	Ending access time on that day.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.22.2 Retrieve Available Attributes

Request

Method	`GET`
Path	`/api/v2/objspec/user_group_safe_policy`, `/api/v2/objspec/user_group_safe_policy_time_policy`

GET /api/v2/objspec/user_group_safe_policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/objspec/user_group_safe_policy'
```

1.22.3 List Overrides

Request

Method	`GET`
Path	`/api/v2/user/group/safe/policy`

GET /api/v2/user/group/safe/policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/user/group/safe/policy'
```

Response


```
{
    "result": "success",
    "user_group_safe_policy": [
        {
            "user_id": "4638707616191610882",
            "safe_id": "4638707616191610881",
            "blocked": false,
            "use_time_policy": true,
            "valid_since": "-infinity",
            "valid_to": "infinity",
            "user_name": "user_1",
            "safe_name": "main",
            "created_at": "2026-08-18 02:19:48.717365-07",
            "modified_at": "2026-08-18 02:19:48.717365-07"
        }
    ]
}
```


1.22.4 Get the Override for a User and Safe

Request

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

GET /api/v2/user/<user_id>/group/safe/<safe_id>/policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/user/4638707616191610882/group/safe/
↪4638707616191610881/policy'
```

Response


```
{
    "result": "success",
    "user_group_safe_policy": [
        {
            "user_id": "4638707616191610882",
            "safe_id": "4638707616191610881",
            "blocked": true,
            "use_time_policy": true,
```


(continues on next page)

(continued from previous page)


```
            "valid_since": "-infinity",
            "valid_to": "infinity",
            "user_name": "user_1",
            "safe_name": "main",
            "created_at": "2026-08-18 02:19:48.717365-07",
            "modified_at": "2026-08-18 02:25:55.003527-07"
        }
    ]
}
```


Note

This endpoint returns an array, not a single object, and an empty array when the user has no override for that safe.

1.22.5 Create an Override

Request

Method	POST
Path	/api/v2/user/group/safe/policy
Body	UserGroupSafePolicyModel

POST /api/v2/user/group/safe/policy

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"user_id":"4638707616191610882","safe_id":"4638707616191610881","use_
↪time_policy":true,"blocked":false}' \
  'https://10.33.3.191/api/v2/user/group/safe/policy'
```

Response


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


1.22.6 Modify an Override

Request

Method	PATCH
Path	/api/v2/user/<user_id>/group/safe/<safe_id>/policy
Body	UserGroupSafePolicyModel

PATCH /api/v2/user/<user_id>/group/safe/<safe_id>/policy

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"blocked":true}' \
  'https://10.33.3.191/api/v2/user/4638707616191610882/group/safe/
↪4638707616191610881/policy'
```

Response

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

1.22.7 Delete an Override

Request

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

DELETE /api/v2/user/<user_id>/group/safe/<safe_id>/policy

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/user/4638707616191610882/group/safe/
↪4638707616191610881/policy'
```

Response

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

1.22.8 List Time Policy Entries

Request

Method	GET
Path	/api/v2/user/group/safe/policy/time_policy

GET /api/v2/user/group/safe/policy/time_policy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/user/group/safe/policy/time_policy'
```

Response


```
{
    "result": "success",
    "user_group_safe_policy_time_policy": [
        {
            "id": "4638707616191610881",
            "user_id": "4638707616191610882",
            "safe_id": "4638707616191610881",
            "user_name": "user_1",
            "safe_name": "main",
            "day_of_week": 1,
            "valid_from": "08:00:00",
            "valid_to": "16:00:00",
            "created_at": "2026-08-18 02:19:56.790642-07",
            "modified_at": "2026-08-18 02:19:56.790642-07"
        }
    ]
}
```


1.22.9 Get a Time Policy Entry

Request

Method	GET
Path	/api/v2/user/group/safe/policy/time_policy/<id>

GET /api/v2/user/group/safe/policy/time_policy/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/user/group/safe/policy/time_policy/
↪4638707616191610881'
```

Response


```
{
    "result": "success",
    "user_group_safe_policy_time_policy": {
        "id": "4638707616191610881",
        "user_id": "4638707616191610882",
        "safe_id": "4638707616191610881",
        "user_name": "user_1",
        "safe_name": "main",
        "day_of_week": 1,
        "valid_from": "08:00:00",
        "valid_to": "16:00:00",
        "created_at": "2026-08-18 02:19:56.790642-07",
        "modified_at": "2026-08-18 02:19:56.790642-07"
```


(continues on next page)

(continued from previous page)

```
    }
}
```

1.22.10 Create a Time Policy Entry

Request

Method	POST
Path	/api/v2/user/group/safe/policy/time_policy
Body	UserGroupSafePolicyTimePolicyModel

POST /api/v2/user/group/safe/policy/time_policy

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"user_id":"4638707616191610882","safe_id":"4638707616191610881","day_of_
↪week":1,"valid_from":"08:00:00","valid_to":"16:00:00"}' \
  'https://10.33.3.191/api/v2/user/group/safe/policy/time_policy'
```

Response

```
{
    "result": "success",
    "user_group_safe_policy_time_policy": {
        "id": "4638707616191610881"
    }
}
```

1.22.11 Modify a Time Policy Entry

Request

Method	PATCH
Path	/api/v2/user/group/safe/policy/time_policy/<id>
Body	UserGroupSafePolicyTimePolicyModel

PATCH /api/v2/user/group/safe/policy/time_policy/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"valid_to":"18:00:00"}' \
  'https://10.33.3.191/api/v2/user/group/safe/policy/time_policy/
↪4638707616191610881'
```

Response

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

1.22.12 Delete a Time Policy Entry

Request

Method	DELETE
Path	/api/v2/user/group/safe/policy/time_policy/<id>

DELETE /api/v2/user/group/safe/policy/time_policy/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/user/group/safe/policy/time_policy/
↪4638707616191610881'
```

Response

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

1.23 Internal Fetch

The internal fetch endpoint enables retrieving server public keys and certificates (SSH/RDP) for establishing secure connections to target servers. This endpoint is used to fetch cryptographic material from remote servers for authentication and encryption purposes.

Warning

The endpoints described in this section belong to the `/internal` API group and may change without prior notice. These interfaces are intended for internal use and are not guaranteed to be stable between releases. For more details refer to the *API BETA Endpoints* section.

1.23.1 Data Structures

Table 57: `FetchModel`

Attribute	Type	Required	Description
`protocol`	string	yes	Connection protocol. Immutable. Allowed values: `http`, `mysql`, `pgsql`, `rdp`, `ssh`, `telnet`, `tls`, `tn3270`, `tn5250`, `vnc`. Case-insensitive. Filterable.
`address`	string	yes	Address to connect to. Filterable.
`port`	number	yes	Port to connect to. Value format: port. Filterable.
`bindip`	string		IP address to bind to when connecting. Filterable.
`servername`	string		Server name for SNI. Requires protocol to be one of: `http`, `mysql`, `pgsql`, `rdp`, `telnet`, `tls`, `tn3270`, `tn5250`, `vnc`. Filterable.
`rdp_secproto`	string		RDP security protocol. Immutable. Default value: `nla`. Allowed values: `nla`, `std`, `tls`. Required when protocol is `rdp`. Filterable.

1.23.2 Retrieve Available Attributes of the *FetchModel*

Request

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

GET /api/v2/objspec/fetch

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.138.59/api/v2/objspec/fetch'
```

1.23.3 Fetch SSH Server Public Key

Request

Method	`POST`
Path	`/api/v2/internal/fetch`
Headers	`Content-Type: application/json`
Body	`FetchModel`

POST /api/v2/internal/fetch

Example Request - SSH

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"protocol": "ssh", "address": "10.0.0.1", "port": 22}' \
  'https://10.31.138.59/api/v2/internal/fetch'
```

Response - SSH

```
{
    "result": "success",
    "ssh_public_key": {
        "public_key": "ssh-ed25519␣
↪AAAAC3NzaC1lZDI1NTE5AAAAIGvHcVf1Ii7m5p2zoW5JjlPw0dwJogykoMYmW8OTMGwa",
        "fingerprint_sha1":
↪"SHA1:30:c6:e3:08:28:61:61:d7:97:ab:92:05:1f:ea:51:38:ec:ab:01:39",
        "fingerprint_sha256":
↪"SHA256:hJY17iobERovVViFUGo9bGrcT3f8OyiBtED49A4z41U"
    }
}
```

1.23.4 Fetch RDP Server Certificate

Request

Method	`POST`
Path	`/api/v2/internal/fetch`
Headers	`Content-Type: application/json`
Body	`FetchModel`

POST /api/v2/internal/fetch

Example Request - RDP with TLS

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"protocol": "rdp", "address": "10.0.0.2", "port": 3389, "rdp_secproto":
↪"tls"}' \
  'https://10.31.138.59/api/v2/internal/fetch'
```

Response - RDP with TLS

```
{
    "result": "success",
    "tls_certificate": {
        "certificate": "-----BEGIN CERTIFICATE-----\nMIIDXTCCAkWgAwIBAgIJAKn...\
↪n-----END CERTIFICATE-----",
        "fingerprint_sha1":
↪"SHA1:a5:b6:c7:d8:e9:f0:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee",
        "fingerprint_sha256":
```

(continues on next page)

(continued from previous page)

```
↪"SHA256:1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcd",
        "subject": "CN=rdp.example.com",
        "issuer": "CN=rdp.example.com",
        "valid_from": "2024-01-01T00:00:00Z",
        "valid_to": "2025-01-01T00:00:00Z"
    }
}
```

Example Request - RDP Standard

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"protocol": "rdp", "address": "10.0.0.3", "port": 3389, "rdp_secproto":
↪"std"}' \
  'https://10.31.138.59/api/v2/internal/fetch'
```

Response - RDP Standard

```
{
    "result": "success",
    "rdp_public_key": {
        "public_key": "308201...base64_encoded_key...",
        "fingerprint_sha1":
↪"SHA1:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff:00:11:22:33:44",
        "fingerprint_sha256":
↪"SHA256:abcdef1234567890abcdef1234567890abcdef1234567890abcdef12345678"
    }
}
```

1.24 Fetch and Store Server Keys/Certificates

This example demonstrates how to use batch operations to fetch SSH/RDP server public keys or certificates and store them in server objects.

1.24.1 Fetch SSH Key and Update Server

The following batch operation fetches an SSH public key from a remote server and updates the corresponding server object:

Example Request - Fetch and Store SSH Key

```
{
  "atomic": true,
  "requests": {
    "fetch_ssh_key": {
      "method": "POST",
      "endpoint": "/internal/fetch",
      "data": {
        "protocol": "ssh",
```

(continues on next page)

(continued from previous page)

```
        "address": "192.168.1.100",
        "port": 22
      }
    },
    "update_server": {
      "method": "PATCH",
      "endpoint": "/server/{server_id}",
      "data": {
        "ssh_public_key": "{responses.fetch_ssh_key.ssh_public_key.public_key}"
      }
    }
  }
}
```

Response

```
{
    "result": "success",
    "responses": {
        "fetch_ssh_key": {
            "result": "success",
            "status-code": 200,
            "ssh_public_key": {
                "public_key": "ssh-ed25519␣
↪AAAAC3NzaC1lZDI1NTE5AAAAIGvHcVf1Ii7m5p2zoW5JjlPw0dwJogykoMYmW80TMGwa",
                "fingerprint_sha1":
↪"SHA1:30:c6:e3:08:28:61:61:d7:97:ab:92:05:1f:ea:51:38:ec:ab:01:39",
                "fingerprint_sha256":
↪"SHA256:hJY17iobERovVViFUGo9bGrcT3f8OyiBtED49A4z41U"
            }
        },
        "update_server": {
            "result": "success",
            "status-code": 200
        }
    }
}
```

1.24.2 Fetch RDP Certificate and Update Server

For RDP servers with TLS security, the batch operation fetches the TLS certificate:

Example Request - Fetch and Store RDP Certificate

```
{
  "atomic": true,
  "variables": {
    "server_address": "192.168.1.200",
    "server_port": 3389,
    "server_id": "{server_id}"
```

(continues on next page)

(continued from previous page)

```
  },
  "requests": {
    "fetch_rdp_cert": {
      "method": "POST",
      "endpoint": "/internal/fetch",
      "data": {
        "protocol": "rdp",
        "address": "{variables.server_address}",
        "port": "{variables.server_port}",
        "rdp_secproto": "tls"
      }
    },
    "update_server": {
      "method": "PATCH",
      "endpoint": "/server/{variables.server_id}",
      "data": {
        "tls_certificate": "{responses.fetch_rdp_cert.tls_certificate.
↪certificate}"
      }
    }
  }
}
```

Response

```
{
    "result": "success",
    "responses": {
        "fetch_rdp_cert": {
            "result": "success",
            "status-code": 200,
            "tls_certificate": {
                "certificate": "-----BEGIN CERTIFICATE-----\
↪nMIIDXTCCAkWgAwIBAgIJAKn...\n-----END CERTIFICATE-----",
                "fingerprint_sha1":
↪"SHA1:a5:b6:c7:d8:e9:f0:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee",
                "fingerprint_sha256":
↪"SHA256:1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcd"
            }
        },
        "update_server": {
            "result": "success",
            "status-code": 200
        }
    }
}
```

1.24.3 Batch Fetch Multiple Server Keys

This example shows how to fetch and store keys for multiple servers in a single batch operation:

Example Request - Multiple Servers

```
{
  "atomic": false,
  "requests": {
    "server1_fetch": {
      "method": "POST",
      "endpoint": "/internal/fetch",
      "atomic": false,
      "data": {
        "protocol": "ssh",
        "address": "10.0.0.1",
        "port": 22
      }
    },
    "server1_update": {
      "method": "PATCH",
      "endpoint": "/server/{server_id_1}",
      "atomic": false,
      "data": {
        "ssh_public_key": "{responses.server1_fetch.ssh_public_key.public_key}"
      }
    },
    "server2_fetch": {
      "method": "POST",
      "endpoint": "/internal/fetch",
      "atomic": false,
      "data": {
        "protocol": "rdp",
        "address": "10.0.0.2",
        "port": 3389,
        "rdp_secproto": "tls"
      }
    },
    "server2_update": {
      "method": "PATCH",
      "endpoint": "/server/{server_id_2}",
      "atomic": false,
      "data": {
        "tls_certificate": "{responses.server2_fetch.tls_certificate.
↪certificate}"
      }
    }
  }
}
```

Note

- The `/internal/fetch` endpoint requires appropriate permissions to access remote servers
- Set `atomic: false` for individual requests when processing multiple servers to prevent one failure from blocking all operations
- The fetched keys/certificates should match the server's configured protocol
- For RDP servers, ensure the `rdp_secproto` parameter matches the server's security configuration

1.25 Access Request

1.25.1 Data Structures

Table 58: `AccessRequestModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only object Identifier
`activated`	boolean		Read-only
`immediate_interval`	number {1-24}	if `type == immediate`	The amount of time the user will have access to the account, expressed in hours and counted from the moment the session is initiated. Read-only, expensive to use.
`starts_at`	string	if `type == scheduled`	The time from which the access period starts.
`expires_at`	string	if `type == scheduled`	The time at which the access expires.
`reason`	string	yes	Read-only.
`revoke_reason`	string		Read-only.
`required_votes`	number		Read-only. Number of votes required to acquire access to the account.
`status`	string {expired, granted, pending, rejected, revoked}		Read-only; expensive to use.
`operation`	string {account_access, account_share, secret_view, secret_share}	yes	Immutable.

continues on next page

Table 58 – continued from previous page

Attribute	Type	Required	Description
type	string {immediate, scheduled, preview}	yes	
account_id	string		Read-only. Requires read right on object type account for GET requests.
account_name	string		Read-only; expensive to use.
safe_id	string		Read-only. Requires read right on object type safe for GET requests.
safe_name	string		Read-only; expensive to use.
pool_id	string		Read-only; expensive to use. Requires read right on object type pool for GET requests.
pool_name	string		Read-only; expensive to use.
protocol	string		Read-only; expensive to use.
server_id	string		Read-only; expensive to use. Requires read right on object type server for GET requests.
server_name	string		Read-only; expensive to use.
secret_id	string		Read-only.
secret_name	string		Read-only; expensive to use.
secret_domain	string		Read-only; expensive to use.
secret_login	string		Read-only; expensive to use.
secret_type	string		Read-only; expensive to use.
secret_description	string		Read-only; expensive to use.
secret_uris	object-array		Read-only; expensive to use.
collection_id	string		Read-only; expensive to use. Requires read right on object type collection for GET requests.
collection_name	string		Read-only; expensive to use.
listeners	object-array		Read-only; expensive to use. JSON object array containing id, mode, name, hidden status, builtin status, and protocol of assigned listeners.
listener_ids	number-array		Read-only; expensive to use.
listener_names	string-array		Read-only; expensive to use.
user_id	string	yes	Immutable. Requires read right on object type user for GET requests.
user_domain	string		Read-only; expensive to use.
user_name	string		Read-only; expensive to use.
requested_for_user_	string		Read-only.
requested_for_user_	string		Read-only; expensive to use.
requested_for_user_	string		Read-only; expensive to use.
votes	object-array		Read-only; expensive to use. JSON object array containing reason, user_id, acceptance status, user_name, user_role, and user_domain of the voting user.

continues on next page

Table 58 – continued from previous page

Attribute	Type	Required	Description
`webclient`	boolean		Read-only; expensive to use. Indicates if access is available via the web client.
`handled`	boolean		Read-only. Hidden; expensive to use. Has the request been handled (accepted by the current user or granted)?
`revoked_at`	string		Read-only.
`revoked_by_id`	string		Read-only. The identifier of the user who revoked the access obtained through this request.
`revoked_by_name`	string		Read-only; expensive to use. The name of the user who revoked the access obtained through this request.
`archival`	boolean	yes	Read-only; expensive to use. Is the request archival (i.e. expired, rejected or revoked)?
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.
`builtin`	boolean		Read-only; expensive to use. Is object built-in? Built-in objects shouldn't be editable.
`hidden`	boolean		Read-only; expensive to use. Shall the object be hidden in UI?

1.25.2 Retrieve Available Attributes of the *AccessRequestModel*

Request

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

Table 59: `AccessRequestVoteModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only object Identifier. Protected.
`access_request_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `access_request_id` with attribute `user_id`.
`accepted`	boolean	yes	
`reason`	string	if `accepted` == `false`	

continues on next page

Table 59 – continued from previous page

Attribute	Type	Required	Description
`user_id`	string		Protected; read-only. Uniqueness is required in the combination of attribute `user_id` with attribute `access_request_id`. Requires `read` right on object type `user` for `POST` requests.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.25.3 Retrieve Available Attributes of the *AccessRequestVoteModel*

Request

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

Table 60: `AccessRequestRevokeModel`

Attribute	Type	Required	Description
`access_request_id`	string	yes	
`revoke_reason`	string	yes	

1.25.4 Retrieve Available Attributes of the *AccessRequestRevokeModel*

Request

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

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

1.25.5 Get Access Requests List

Request

Method	`GET`
Path	`/api/v2/access_request`

Example Request

GET /api/v2/access_request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/access_request'
```

1.25.6 Revoking Access Requests

Request

Method	POST
Path	/api/v2/access_request/<access_request_id>/revoke
Headers	Content-Type: Application/JSON
Body	AccessRequestRevokeModel

Example Request

POST /api/v2/access_request/<id>/revoke

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/access_request/5620492334958379010/revoke' \
  -d'{"revoke_reason":"AD maintenance."}'
```

Response

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

1.25.7 Responding to a Pending Access Request

Request

Method	POST
Path	/api/v2/access_request/<access_request_id>/vote
Headers	Content-Type: Application/json
Body	AccessRequestVoteModel

Example Request

POST /api/v2/access_request/<id>/vote

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/access_request/5620492334958379011/vote' \
  -d'{"accepted":true}'
```

Response

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

1.26 Access Request Reason Formats NEW

A reason format turns the free-text justification of an access request into a set of named fields the requester fills in. Formats are defined here and referenced by the `reason_format_id` attribute when an access request is created in the User Access Gateway.

1.26.1 Data Structures

Table 61: `AccessRequestReasonFormatModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Reason format identifier. Uniqueness is required.
`name`	string	yes	Reason format name. Case-insensitive. Uniqueness is required.
`description`	string		Reason format description shown to the requester.
`fields`	object-array	yes	Fields the requester fills in. See the `ReasonFormatFieldModel` table. At least one field is required. Returned by `GET` on a single format only - the collection listing omits it.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 62: `ReasonFormatFieldModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Field identifier. Referenced by `field_id` in the `reason_fields` attribute of an access request.
`name`	string	yes	Field label shown to the requester.
`type`	string {text, number, constant}	yes	`text` and `number` are filled in by the requester; `constant` carries a fixed value supplied here.
`value`	string	If `type` == `constant`	Fixed value of a `constant` field. `null` for `text` and `number` fields.

Warning

`PATCH` replaces the whole format, including its fields, and the replaced fields are assigned **new identifiers**. Any access request that stored `field_id` values from the previous revision keeps

referring to the old ones. Read the format back after modifying it if you need the current field identifiers.

1.26.2 Retrieve Available Attributes of the *AccessRequestReasonFormatModel*

Request

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

GET /api/v2/objspec/access_request_reason_format

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/objspec/access_request_reason_format'
```

Note

The object specification does not list the `fields` attribute, but it is required when creating or modifying a format and is returned when a single format is read.

1.26.3 List Reason Formats

Request

Method	`GET`
Path	`/api/v2/access_request_reason_format`

GET /api/v2/access_request_reason_format

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/access_request_reason_format'
```

Response


```
{
    "result": "success",
    "access_request_reason_format": [
        {
            "id": "4638707616191610881",
            "name": "Incident handling",
            "description": "Reason format used for incident related requests.",
            "created_at": "2026-08-17 07:27:42.705608-07",
            "modified_at": "2026-08-17 07:27:42.705608-07"
```


(continues on next page)

(continued from previous page)

```
        },
        {
            "id": "4638707616191610882",
            "name": "Change window",
            "description": "Reason format used for planned maintenance requests.
↪",
            "created_at": "2026-08-18 02:14:39.691012-07",
            "modified_at": "2026-08-18 02:14:39.691012-07"
        }
    ]
}
```

1.26.4 Get a Reason Format

Request

Method	GET
Path	/api/v2/access_request_reason_format/<id>

GET /api/v2/access_request_reason_format/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/access_request_reason_format/4638707616191610881'
```

Response

```
{
    "access_request_reason_format": {
        "id": "4638707616191610881",
        "name": "Incident handling",
        "description": "Reason format used for incident related requests.",
        "fields": [
            {
                "id": "4638707616191610881",
                "name": "Ticket number",
                "type": "text",
                "value": null
            },
            {
                "id": "4638707616191610882",
                "name": "Priority",
                "type": "number",
                "value": null
            },
            {
                "id": "4638707616191610883",
```

(continues on next page)

(continued from previous page)


```
                "name": "Source system",
                "type": "constant",
                "value": "Service Desk"
            }
        ],
        "created_at": "2026-08-17 07:27:42.705608-07",
        "modified_at": "2026-08-17 07:27:42.705608-07"
    },
    "result": "success"
}
```


1.26.5 Create a Reason Format

Request

Method	POST
Path	/api/v2/access_request_reason_format
Body	AccessRequestReasonFormatModel

POST /api/v2/access_request_reason_format

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"name":"Change window","description":"Reason format used for planned␣
↪maintenance requests.","fields":[{"name":"Change number","type":"text"},{"name
↪":"Approved by","type":"text"},{"name":"Source system","type":"constant",
↪"value":"Change Manager"}]}' \
  'https://10.33.3.191/api/v2/access_request_reason_format'
```

Response


```
{
    "access_request_reason_format": {
        "id": "4638707616191610882"
    },
    "result": "success"
}
```


Note

Omitting `fields`, or sending an empty array, fails with `{"result": "failure", "message": "At least one field is required."}`.

1.26.6 Modify a Reason Format

Request

Method	PATCH
Path	/api/v2/access_request_reason_format/<id>
Body	AccessRequestReasonFormatModel

PATCH /api/v2/access_request_reason_format/<id>

The request body must carry the complete format - `name` and `fields` are required even when only the description changes. A body without them is rejected.

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"name":"Change window","description":"Reason format used for planned␣
↪change windows.","fields":[{"name":"Change number","type":"text"},{"name":
↪"Approved by","type":"text"},{"name":"Source system","type":"constant","value
↪":"Change Manager"}]}' \
  'https://10.33.3.191/api/v2/access_request_reason_format/4638707616191610882'
```

Response

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

1.26.7 Delete a Reason Format

Request

Method	DELETE
Path	/api/v2/access_request_reason_format/<id>

DELETE /api/v2/access_request_reason_format/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/access_request_reason_format/4638707616191610882'
```

Response

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

1.27 Password Vault

1.27.1 Collection Management

Overview

Collections are organizational containers for secrets in Fudo Enterprise's vault system. They provide hierarchical structure, permission management, and access control for secret storage. Collections support both organizational vaults and personal vaults, with comprehensive permission inheritance and granular access policies.

Data Structures

Table 63: `CollectionModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique secret collection identifier.
`name`	string	yes	Collection name. Uniqueness is required in the combination with `parent_id` (case-insensitive).
`parent_id`	string		Parent collection identifier for hierarchical structure. Uniqueness is required in the combination with `name`.
`owner_id`	string		Read-only. Hidden. Protected. User ID of the personal vault owner.
`inherit_permis`	boolean		Inherit permissions from parent collection.
`inheritance_ta`	string		Read-only. ID of the collection that permissions are inherited from.
`subcollections`	number		Read-only. Number of direct child collections.
`secrets_count`	number		Read-only. Number of descendant secrets.
`path_to_root_i`	string-array		Read-only. Hidden. Ordered list of ancestor collection IDs.
`path_to_root_n`	string-array		Read-only. Hidden. Ordered list of ancestor collection names.
`accessible_par`	string		Read-only. Hidden. Accessible parent collection ID.
`vault`	string		Read-only. Hidden. Vault type (organization, personal).
`contains_expos`	boolean		Read-only. Indicates whether the collection contains secrets with exposure alerts.
`rights`	string-array		Read-only. List of rights the subject has to this object.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *CollectionModel*

Request

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

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

Note

Collections support hierarchical organization with parent-child relationships. Permission inheritance allows collections to automatically inherit access policies from parent collections.

List Collections

Request

Method	`GET`
Path	`/api/v2/collection`

GET /api/v2/collection

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/collection'
```

Response

```
{
    "result": "success",
    "collection": [
        {
            "id": "8754997675608244225",
            "name": "Development Team",
            "inherit_permissions": false,
            "inheritance_target_collection_id": "8754997675608244225",
            "subcollections_count": 2,
            "secrets_count": 2,
            "contains_exposed_secrets": true,
            "rights": [
                "create",
                "delete",
                "modify",
                "move",
                "read"
            ],
```

(continues on next page)

(continued from previous page)

```
            "created_at": "2026-03-25 01:46:50.823004-07",
            "modified_at": "2026-04-03 06:36:25.545952-07"
        }
    ]
}
```

Get Collection by ID

Request

Method	GET
Path	/api/v2/collection/<id>

GET /api/v2/collection/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/collection/8754997675608244225'
```

Response

```
{
    "result": "success",
    "collection": {
        "id": "8754997675608244225",
        "name": "Development Team",
        "inherit_permissions": false,
        "inheritance_target_collection_id": "8754997675608244225",
        "subcollections_count": 2,
        "secrets_count": 2,
        "contains_exposed_secrets": true,
        "rights": [
            "create",
            "delete",
            "modify",
            "move",
            "read"
        ],
        "created_at": "2026-03-25 01:46:50.823004-07",
        "modified_at": "2026-04-03 06:36:25.545952-07"
    }
}
```

Create Collection

Request

Method	POST
Path	/api/v2/collection
Body	CollectionModel

POST /api/v2/collection

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "Database Credentials",
    "parent_id": "8754997675608244225",
    "inherit_permissions": true
  }' \
  'https://10.31.135.179/api/v2/collection'
```

Response

```
{
    "result": "success",
    "collection": [
        {
            "id": "8754997675608244228",
            "name": "Database Credentials",
            "parent_id": "8754997675608244225",
            "inherit_permissions": true,
            "inheritance_target_collection_id": "8754997675608244225",
            "subcollections_count": 0,
            "secrets_count": 0
        }
    ]
}
```

Update Collection

Request

Method	PATCH
Path	/api/v2/collection/<id>
Body	CollectionModel

PATCH /api/v2/collection/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "Database Credentials",
    "inherit_permissions": false
  }' \
  'https://10.31.135.179/api/v2/collection/8754997675608244228'
```

Response


```
{
    "result": "success",
    "collection": [
        {
            "id": "8754997675608244228",
            "name": "Database Credentials",
            "parent_id": "8754997675608244225",
            "inherit_permissions": false,
            "inheritance_target_collection_id": "8754997675608244228",
            "modified_at": "2026-04-17T14:45:00Z"
        }
    ]
}
```


Delete Collection

Request

Method	DELETE
Path	/api/v2/collection/<id>

DELETE /api/v2/collection/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/collection/8754997675608244228'
```

Response


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

Import Secrets to Collection

This endpoint imports secrets from a CSV file into a collection. The CSV file must be constructed according to the following rules:

- The first row is a *header row* containing names corresponding to the API fields names (refer to *API Documentation:* Secrets).
- The *header row* must include all fields that are required when manually creating a secret of specific type. Other fields are optional and can be left empty.
- A comma (,) has to be used as a field separator.

Example CSV file:

```
name,type,login,domain,secret,uri
login,login,admin,portal.example.com,SuperSecure123!,https://portal.example.com/
↪login
login2,login,db_admin,db.example.com,DbPassword2024,https://db.example.com/admin
note,note,,,Quarterly meeting notes: Q4 targets discussed.,
api_key,apikey,aws_service_account,api.aws.amazon.com,AKIAIOSFODNN7EXAMPLE,
↪https://api.aws.amazon.com
cert,certificate,,,,
ssh_key,sshkey,,,,
```

Note

SSH private keys and certificates are typically stored in multi-line PEM format. When importing them from a CSV file, enclose the entire value in double quotes ("") so it is treated as a single CSV field.

Example CSV for a certificate secret:

```
name,type,login,domain,certificate,secret
"secret-1","certificate","","","-----BEGIN CERTIFICATE-----
MIID...EXAMPLE...DATA
-----END CERTIFICATE-----","-----BEGIN PRIVATE KEY-----
MIIE...EXAMPLE...DATA
-----END PRIVATE KEY-----"
```

Request

Method	`POST`
Path	`/api/v2/collection/<id>/secret_import`
Headers	`Content-Type: multipart/form-data`
Body	`CSV file upload`

POST /api/v2/collection/<id>/secret_import

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -F 'file=@secrets.csv' \
  'https://10.31.135.179/api/v2/collection/8754997675608244225/secret_import'
```

Note

The CSV file should contain a header row with columns such as `name`, `type`, `login`, `password`, `url`, `notes`, etc.

Response


```
{
    "result": "success",
    "imported_count": 2,
    "failed_count": 0,
    "details": [
        {
            "name": "Database Admin",
            "status": "imported",
            "secret_id": "3260606130216239118"
        },
        {
            "name": "API Key",
            "status": "imported",
            "secret_id": "3260606130216239119"
        }
    ]
}
```


1.27.2 Collections Permissions

Data Structures

Table 64: `CollectionPermissionModel`

Attribute	Type	Required	Description
`collection_id`	string		Read-only. The collection ID. Uniqueness is required in the combination with `user_id` and `group_id`.
`subject_type`	string {user, group}	yes	Read-only. Type of permission subject.
`subject_name`	string	yes	Read-only. User or group name.
`access_policy`	string {view_on_request, view, edit_on_request, full_edit}	yes	Read-only. Access policy level.
`user_id`	string	If `subject_t` == `user`	Read-only. User ID when subject_type is 'user'. Uniqueness is required in the combination with `collection_id` and `group_id`.
`group_id`	string	If `subject_t` == `group`	Read-only. Group ID when subject_type is 'group'. Uniqueness is required in the combination with `collection_id` and `user_id`.
`group_users_co`	number	If `subject_t` == `group`	Read-only. Hidden. Number of users in the group.
`group_users_na`	string	If `subject_t` == `group`	Read-only. Hidden. Comma separated string of user names in the group (for filtering purposes).

Retrieve Available Attributes of the *CollectionPermissionModel*

Request

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

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

Get Collection Permissions

Request

Method	`GET`
Path	`/api/v2/collection/<collection_id>/permission`

GET /api/v2/collection/<collection_id>/permission

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/collection/8754997675608244225/permission'
```

Response


```
{
    "result": "success",
    "collection_permission": [
        {
            "collection_id": "8754997675608244225",
            "subject_type": "user",
            "subject_name": "admin",
            "access_policy": "view_on_request",
            "user_id": "8754997675608244225"
        },
        {
            "collection_id": "8754997675608244225",
            "subject_type": "user",
            "subject_name": "jdoe",
            "access_policy": "view",
            "user_id": "8754997675608244227"
        }
    ]
}
```


1.27.3 User Collection Management

Overview

User collection management provides direct assignment of users to collections with specific access policies. This complements group-based access and allows for granular per-user collection permissions outside of role-based access control.

Data Structures

Table 65: `UserCollectionModel`

Attribute	Type	Required	Description
`id`	string		Read-only. User collection access identifier.
`user_id`	string	yes	Immutable. User identifier. Uniqueness is required in the combination of attribute `user_id` with attribute `collection_id`.
`collection_id`	string	yes	Immutable. Collection identifier. Uniqueness is required in the combination of attribute `collection_id` with attribute `user_id`.
`access_policy`	string {view_on_request, view, edit_on_request, full_edit}; Default value `view_on_request`	yes	Access policy level.
`user_name`	string		Read-only; expensive to use. User name.
`collection_nam`	string		Read-only; expensive to use. Collection name.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *UserCollectionModel*

Request

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

GET /api/v2/objspec/user_collection

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/objspec/user_collection'
```

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

List User Collections

Request

Method	GET
Path	/api/v2/user/collection

GET /api/v2/user/collection

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/user/collection'
```

Response


```
{
    "result": "success",
    "user_collection": [
        {
            "id": "8754997675608244225",
            "user_id": "8754997675608244225",
            "collection_id": "8754997675608244225",
            "access_policy": "view_on_request",
            "user_name": "admin",
            "collection_name": "Development Team",
            "created_at": "2026-03-25T02:02:41Z"
        }
    ]
}
```


Create User Collection Assignment

Request

Method	POST
Path	/api/v2/user/collection
Body	UserCollectionModel

POST /api/v2/user/collection

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "user_id": "8754997675608244227",
    "collection_id": "8754997675608244225",
    "access_policy": "edit_on_request"
```

(continues on next page)

(continued from previous page)

```
  }' \
  'https://10.31.135.179/api/v2/user/collection'
```

Response

```
{
    "result": "success",
    "user_collection": [
        {
            "id": "8754997675608244230",
            "user_id": "8754997675608244227",
            "collection_id": "8754997675608244225",
            "access_policy": "edit_on_request",
            "user_name": "jdoe",
            "collection_name": "Development Team"
        }
    ]
}
```

Update User Collection Assignment

Request

Method	`PATCH`
Path	`/api/v2/user/<user_id>/collection/<collection_id>`
Body	`UserCollectionModel`

PATCH /api/v2/user/<user_id>/collection/<collection_id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "access_policy": "full_edit"
  }' \
  'https://10.31.135.179/api/v2/user/8754997675608244227/collection/
↪8754997675608244225'
```

Response

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

Remove User Collection Assignment

Request

Method	DELETE
Path	/api/v2/user/<user_id>/collection/<collection_id>

DELETE /api/v2/user/<user_id>/collection/<collection_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/user/8754997675608244227/collection/
↪8754997675608244225'
```

Response

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

Note

User collection management provides:

- **Direct user assignments**: Bypass group membership for specific collection access
- **Flexible access policies**: Four levels from view-on-request to full-edit
- **Individual control**: Per-user customization of collection access
- **Audit capabilities**: Track direct user-to-collection relationships

Warning

Access policy levels:

- `view_on_request`: Users must request access to view secrets
- `view`: Users can view secrets without approval
- `edit_on_request`: Users must request access to modify secrets
- `full_edit`: Users can modify secrets without approval

User collection assignments complement but do not override group-based permissions or role capabilities.

1.27.4 Assigning Collections to Groups

Overview

Collections are organizational containers for secrets in Fudo Enterprise's vault system. They provide hierarchical structure, permission management, and access control for secret storage. Collections support both organizational vaults and personal vaults, with comprehensive permission inheritance and granular access policies.

Data Structures

Table 66: `GroupCollectionModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique group collection access identifier.
`group_id`	string	yes	Immutable. Group identifier. Uniqueness is required in the combination of attribute `group_id` with attribute `collection_id`.
`collection_id`	string	yes	Immutable. Collection identifier. Uniqueness is required in the combination of attribute `collection_id` with attribute `group_id`.
`access_policy`	string {view_on_request, view, edit_on_request, full_edit}; Default value `view_on_request`	yes	Access policy level.
`group_name`	string		Read-only; expensive to use. Group name.
`collection_nam`	string		Read-only; expensive to use. Collection name.
`group_users`	object-array		Read-only; expensive to use. Users assigned to the group.
`created_at`	datetime		Read-only. Object creation time.
`modified_at`	datetime		Read-only. Object last modification time.
`removed`	boolean		Read-only. Is the object removed?

Retrieve Available Attributes of the *GroupCollectionModel*

Request

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

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

List Group Collections

Request

Method	GET
Path	/api/v2/group/collection

GET /api/v2/group/collection

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/group/collection'
```

Response

```
{
    "result": "success",
    "group_collection": [
        {
            "id": "8754997675608244226",
            "group_id": "8754997675608244225",
            "collection_id": "8754997675608244225",
            "access_policy": "view",
            "group_name": "DevTeam",
            "collection_name": "Development Team"
        }
    ]
}
```

Assign Group to Collection

Request

Method	POST
Path	/api/v2/group/collection
Body	GroupCollectionModel

POST /api/v2/group/collection

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "group_id": "8754997675608244225",
    "collection_id": "8754997675608244225",
    "access_policy": "edit_on_request"
```

(continues on next page)

(continued from previous page)

```
  }' \
  'https://10.31.135.179/api/v2/group/collection'
```

Response

```
{
    "result": "success",
    "group_collection": [
        {
            "id": "8754997675608244227",
            "group_id": "8754997675608244225",
            "collection_id": "8754997675608244225",
            "access_policy": "edit_on_request"
        }
    ]
}
```

Update Group Collection Access

Request

Method	PATCH
Path	/api/v2/group/<group_id>/collection/<collection_id>
Body	GroupCollectionModel

PATCH /api/v2/group/<group_id>/collection/<collection_id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "access_policy": "full_edit"
  }' \
  'https://10.31.135.179/api/v2/group/8754997675608244225/collection/
↪8754997675608244225'
```

Response

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

Remove Group from Collection

Request

Method	DELETE
Path	/api/v2/group/<group_id>/collection/<collection_id>

DELETE /api/v2/group/<group_id>/collection/<collection_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/group/8754997675608244225/collection/
↪8754997675608244225'
```

Response

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

1.27.5 Collection Notifications

Overview

Collection notification management allows you to configure which users receive notifications for events related to specific collections. This provides targeted alerting for collection-specific activities such as secret access, modifications, or security events.

Data Structures

Table 67: `CollectionNotificationUserModel`

Attribute	Type	Required	Description
`collection_id`	string		Read-only. Unique collection identifier.
`user_id`	string		Read-only. Unique user identifier.
`user_name`	string		Read-only. Username for notification recipient.
`user_domain`	string		Read-only. User domain.
`user_email`	string		Read-only. User email address.
`email_notifica`	boolean		Read-only. Whether email notifications are enabled.
`push_notificat`	boolean		Read-only. Whether push notifications are enabled.

Retrieve Available Attributes of the *CollectionNotificationUsersModel*

Request

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

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

Get Collection Notification Users

Request

Method	GET
Path	/api/v2/collection/<collection_id>/notification_user

GET /api/v2/collection/<collection_id>/notification_user

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/collection/8754997675608244225/notification_user
↪'
```

Response

```
{
    "result": "success",
    "collection_notification_user": [
        {
            "collection_id": "8754997675608244225",
            "user_id": "8754997675608244225",
            "user_name": "admin",
            "email_notifications": false,
            "push_notifications": false
        },
        {
            "collection_id": "8754997675608244225",
            "user_id": "8754997675608244226",
            "user_name": "remoteapp",
            "email_notifications": false,
            "push_notifications": false
        }
    ]
}
```

1.27.6 Collection Access

Data Structures

Table 68: `CollectionAccessModel`

Attribute	Type	Required	Description
`subject_id`	string		Read-only. Subject identifier. Uniqueness is required in the combination of attribute `subject_id` with attribute `object_id`.
`subject_name`	string		Read-only; expensive to use. Subject name.
`object_id`	string		Read-only. Object identifier. Uniqueness is required in the combination of attribute `object_id` with attribute `subject_id`.
`object_name`	string		Read-only; expensive to use. Object name.
`rights`	string-array		Read-only. List of access rights.
`builtin`	boolean		Read-only; expensive to use. Is object built-in? Built-in objects shouldn't be editable.
`hidden`	boolean		Read-only; expensive to use. Shall the object be hidden in UI?

Retrieve Available Attributes of the *CollectionAccessModel*

Request

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

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

List Collection Access

Request

Method	`GET`
Path	`/api/v2/access/collection`

GET /api/v2/access/collection

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/access/collection'
```

Response

```
{
    "result": "success",
    "collection_access": [
        {
            "subject_id": "8754997675608244225",
            "subject_name": "admin",
            "object_id": "8754997675608244225",
            "object_name": "Development Team",
            "rights": [
                "read",
                "modify",
                "delete",
                "move",
                "create"
            ],
            "builtin": false,
            "hidden": false
        }
    ]
}
```


Get Specific Collection Access

Request

Method	GET
Path	/api/v2/access/<subject_id>/collection/<object_id>

GET /api/v2/access/<subject_id>/collection/<object_id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/access/8754997675608244225/collection/
↪8754997675608244225'
```

Response


```
{
    "result": "success",
    "collection_access": {
        "subject_id": "8754997675608244225",
        "subject_name": "admin",
        "object_id": "8754997675608244225",
        "object_name": "Development Team",
        "rights": [
            "read",
            "modify",
            "delete",
```


(continues on next page)

(continued from previous page)

```
            "move",
            "create"
        ],
        "builtin": false,
        "hidden": false
    }
}
```

1.27.7 Secret Management

Overview

Secrets are encrypted data items stored in collections within Fudo Enterprise's vault system. They support various types including login credentials, SSH keys, API keys, certificates, and secure notes. Secrets provide comprehensive access tracking, automatic secret changing, and exposure monitoring.

Data Structures

Table 69: `SecretModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique secret identifier.
`name`	string	yes	Secret name. Case-insensitive. Uniqueness is not required - a collection can hold several secrets with the same name.
`collection_id`	string	yes	Parent collection identifier.
`owner_id`	string		Read-only. Hidden. Protected; expensive to use. User ID of the personal vault owner.
`collection_nam`	string		Read-only. Hidden; expensive to use. Collection name.
`type`	string {login, sshkey, note, apikey, certificate}	yes	Immutable. Secret type.
`description`	string		Not encrypted secret description.
`login`	string	If `type` == `login` | `sshkey` | `apikey`	Username (for login, sshkey, apikey types).
`domain`	string	If `type` == `login` | `sshkey` | `apikey`	Domain (for login, sshkey, apikey types).

continues on next page

Table 69 – continued from previous page

Attribute	Type	Required	Description
certificate	string	If type == certifica	X.509 certificate (for certificate type).
x509_pubkey _fingerprint_s	string		Read-only; expensive to use. Public key SHA256 fingerprint derived from certificate.
secret	string		Protected. Encrypted secret (password, private key, etc).
secret_passphr	string	If type == certifica | sshkey	Protected. Passphrase to use to decrypt SSH private key.
has_secret	boolean		Read-only; expensive to use. Indicates whether a secret value is set.
ssh_public_key	string		Read-only; expensive to use. SSH public key derived from private key.
ssh_fingerprin _sha256	string		Read-only; expensive to use. SSH key SHA256 fingerprint derived from private key.
key_pubkey _fingerprint_s	string		Read-only; expensive to use. TLS key SHA256 fingerprint derived from private key.
path_to_root_i	string-array		Read-only. Hidden; expensive to use. Ordered list of ancestor collection IDs, starting with the root collection.
path_to_root_n	string-array		Read-only. Hidden; expensive to use. Ordered list of ancestor collection names, starting with the root collection.
policy_complia	boolean		Read-only. Hidden; expensive to use. Indicates whether the secret conforms to global vault configuration requirements.
policy_complia _partial	boolean	If type == login	Read-only. Hidden. Protected.

continues on next page

Table 69 – continued from previous page

Attribute	Type	Required	Description
`compromised`	boolean	Read-only. Hidden; expensive to use. Indicates whether the secret is known to be compromised.	
`vault`	string		Read-only. Hidden; expensive to use. Vault type (organization, personal).
`secret_seen`	boolean	yes	Read-only; expensive to use. Indicates whether anyone has viewed the current secret version.
`secret_exposed`	boolean	yes	Read-only; expensive to use. Indicates whether the secret has exposure alerts (users who viewed it and lost access).
`secret_exposed_user_count`	number	yes	Read-only; expensive to use. Number of users who viewed the current secret version but lost access to it.
`has_changer`	boolean		Read-only; expensive to use. Indicates whether the secret has secret changer assigned.
`password_chang_awaiting`	boolean		Read-only; expensive to use. Indicates whether the assigned secret changer was triggered manually and is awaiting execution.
`checkout_exclu`	boolean		Whether the secret uses exclusive checkout; Default value `false`.
`checkout_time_`	number	If `checkout_exclusiv` == `true`	Time limit for checking out the secret in seconds.
`last_change_at`	datetime		Read-only. Hidden. Last successful secret change.
`last_verificat`	datetime		Read-only. Hidden. Last successful password verification.
`checked_out_by_users_ids`	string-array		Read-only. Hidden; expensive to use. List of user IDs who currently have an active checkout of the secret.
`rights`	string-array		Read-only. List of rights the subject has to this object.
`created_at`	datetime		Read-only.
`modified_at`	datetime		Read-only.

continues on next page

Table 69 – continued from previous page

Attribute	Type	Required	Description
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SecretModel*

Request

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

GET /api/v2/objspec/secret

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/objspec/secret'
```

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

Note

Secret types available:

- **login**: Username/password credentials
- **sshkey**: SSH private/public key pairs
- **note**: Secure text notes
- **apikey**: API tokens and keys
- **certificate**: X.509 certificates with private keys

List Secrets

Request

Method	`GET`
Path	`/api/v2/secret`

GET /api/v2/secret

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret'
```

Response

```
{
    "result": "success",
    "secret": [
        {
            "id": "8754997675608244226",
            "name": "Dev Database Admin",
            "collection_id": "8754997675608244225",
            "type": "sshkey",
            "login": "Admin",
            "has_secret": true,
            "secret_seen": true,
            "secret_exposed": true,
            "secret_exposed_user_count": 1,
            "has_changer": false,
            "password_changer_awaiting": false,
            "checkout_exclusive": false,
            "created_at": "2026-04-01T01:27:09Z",
            "modified_at": "2026-04-01T01:27:09Z",
            "ssh_public_key": "ssh-ed25519␣
↪AAAAC3NzaC1lZDI1NTE5AAAAIDlMLtN5D1WX5VkurlIrMA2oZpDuNMCLInwwAYHfT1SX",
            "ssh_fingerprint_sha256": "SHA256:6P7SXlQju7HD6tStTgINCYbmXYW/
↪3anjf3lV/DyQxu4"
        }
    ]
}
```


Get Secret by ID

Request

Method	GET
Path	/api/v2/secret/<id>

GET /api/v2/secret/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/8754997675608244226'
```

Response


```
{
    "result": "success",
    "secret": {
        "id": "8754997675608244226",
        "name": "Dev Database Admin",
        "collection_id": "8754997675608244225",
        "type": "sshkey",
```


(continues on next page)

(continued from previous page)


```
        "login": "Admin",
        "has_secret": true,
        "secret_seen": true,
        "secret_exposed": true,
        "secret_exposed_user_count": 1,
        "has_changer": false,
        "password_changer_awaiting": false,
        "checkout_exclusive": false,
        "created_at": "2026-04-01T01:27:09Z",
        "modified_at": "2026-04-01T01:27:09Z",
        "ssh_public_key": "ssh-ed25519␣
↪AAAAC3NzaC1lZDI1NTE5AAAAIDlMLtN5D1WX5VkurlIrMA2oZpDuNMCLInwwAYHfT1SX",
        "ssh_fingerprint_sha256": "SHA256:6P7SXlQju7HD6tStTgINCYbmXYW/3anjf3lV/
↪DyQxu4"
    }
}
```


Create Secret

Request

Method	POST
Path	/api/v2/secret
Body	SecretModel

POST /api/v2/secret

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "Staging Database",
    "collection_id": "8754997675608244225",
    "type": "login",
    "description": "Staging environment database",
    "login": "staging_user",
    "domain": "staging.example.com",
    "secret": "StrongPassword123!"
  }' \
  'https://10.31.135.179/api/v2/secret'
```

Response


```
{
    "result": "success",
    "secret": [
        {
```


(continues on next page)

(continued from previous page)


```
            "id": "8754997675608244226",
            "name": "Staging Database",
            "collection_id": "8754997675608244225",
            "type": "login",
            "created_at": "2026-04-17T15:00:00Z"
        }
    ]
}
```


Update Secret

Request

Method	PATCH
Path	/api/v2/secret/<id>
Body	SecretModel

PATCH /api/v2/secret/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "description": "Updated staging database credentials",
    "secret": "NewStrongPassword456!"
  }' \
  'https://10.31.135.179/api/v2/secret/8754997675608244226'
```

Response


```
{
    "result": "success",
    "secret": [
        {
            "id": "8754997675608244226",
            "modified_at": "2026-04-17T15:30:00Z"
        }
    ]
}
```


Delete Secret

Request

Method	DELETE
Path	/api/v2/secret/<id>

DELETE /api/v2/secret/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/8754997675608244226'
```

Response

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

See also

Related API documentation:

- *Secret Access Management* - Managing secret access and checkout
- *Secret Exposure Monitoring* - Monitoring secret exposure
- *Secret Changer Management* - Automatic password rotation
- *Secret URI Management* - Managing secret URIs

Warning

Security considerations for secret management:

- Secret values are encrypted and protected in transit and at rest
- Access is logged and monitored for compliance and security auditing
- Use appropriate secret types for different kinds of sensitive data

1.27.8 Secret Changer Management

Overview

Secret changer management allows automatic rotation of secret passwords based on configured policies. Secret changers can be assigned to secrets to periodically update credentials on target systems, ensuring compliance with security policies and reducing the risk of compromised credentials.

Data Structures

Table 70: `SecretPasswordChangerModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique secret secret changer assignment identifier.
`secret_id`	string	yes	Immutable. Secret identifier. Uniqueness is required in the combination of attribute `secret_id` with attribute `password_changer_id`.
`secret_name`	string		Read-only; expensive to use.
`password_chang`	string		Immutable. Password changer identifier. Uniqueness is required in the combination of attribute `password_changer_id` with attribute `secret_id`.
`password_chang`	string	yes	Read-only; expensive to use. Password changer name.
`password_chang`	string {change, verify}	yes	Read-only; expensive to use. Password changer type. Only single verify can be assigned to the secret.
`password_chang`	string {LDAP, SSH, Telnet, WinRM}	yes	Read-only; expensive to use. Transport layer for secret changer.
`collection_id`	string	yes	Read-only; expensive to use. Collection identifier.
`collection_nam`	string		Read-only; expensive to use. Collection name.
`position`	number	If `password_` == `change`	Execution order of secret changers. Uniqueness is required in the combination of attribute `position` with attribute `secret_id`.
`policy_complia`	boolean		Read-only. Hidden; expensive to use. Indicates whether the secret conforms to global vault configuration requirements.
`created_at`	datetime		Read-only. Record creation timestamp.
`modified_at`	datetime		Read-only. Record modification timestamp.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SecretPasswordChangerModel*

Request

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

GET /api/v2/objspec/secret_password_changer

Note

This endpoint may not be available if secret_password_changer doesn't have a separate object specification.

List Secret Secret Changers

Request

Method	GET
Path	/api/v2/secret/password_changer

GET /api/v2/secret/password_changer

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/password_changer'
```

Response


```
{
    "result": "success",
    "secret_password_changer": [
        {
            "id": "8754997675608244225",
            "secret_id": "8754997675608244226",
            "secret_name": "Dev Database Admin",
            "password_changer_id": "8754997675608244235",
            "password_changer_name": "ver",
            "password_changer_type": "verify",
            "password_changer_transport": "SSH",
            "collection_id": "8754997675608244225",
            "collection_name": "Development Team",
            "created_at": "2026-04-03T04:36:24Z",
            "modified_at": "2026-04-03T04:36:24Z"
        }
    ]
}
```


Get Secret Changers for Secret

Request

Method	GET
Path	/api/v2/secret/<secret_id>/password_changer

GET /api/v2/secret/<secret_id>/password_changer

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/8754997675608244225/password_changer'
```

Response


```
{
    "result": "success",
    "secret_password_changer": [
        {
            "id": "8754997675608244225",
            "secret_id": "8754997675608244225",
            "password_changer_id": "8754997675608244226",
            "password_changer_name": "Windows AD Changer",
            "password_changer_type": "change",
            "position": 1
        }
    ]
}
```


Assign Secret Changer to Secret

Request

Method	POST
Path	/api/v2/secret/<secret_id>/password_changer
Body	SecretPasswordChangerModel

POST /api/v2/secret/<secret_id>/password_changer

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "password_changer_id": "8754997675608244227",
    "position": 2
  }' \
  'https://10.31.135.179/api/v2/secret/8754997675608244225/password_changer'
```

Response


```
{
    "result": "success",
    "secret_password_changer": [
        {
            "id": "8754997675608244228",
            "secret_id": "8754997675608244225",
            "password_changer_id": "8754997675608244227",
```


(continues on next page)

(continued from previous page)

```
            "position": 2
        }
    ]
}
```

Trigger Password Change

Request

Method	POST
Path	/api/v2/secret/<id>/trigger_password_changer

POST /api/v2/secret/<id>/trigger_password_changer

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/8754997675608244225/trigger_password_
↪changer'
```

Response

```
{
    "result": "success",
    "message": "Password change initiated",
    "job_id": "8754997675608244229"
}
```

Update Secret Secret Changer

Request

Method	PATCH
Path	/api/v2/secret/<secret_id>/password_changer/<password_changer_id>
Body	SecretPasswordChangerModel

PATCH /api/v2/secret/<secret_id>/password_changer/<password_changer_id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "position": 3
  }' \
  'https://10.31.135.179/api/v2/secret/8754997675608244225/password_changer/
↪8754997675608244226'
```

Response

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

Remove Secret Changer from Secret

Request

Method	DELETE
Path	/api/v2/secret/<secret_id>/password_changer/<password_changer_id>

DELETE /api/v2/secret/<secret_id>/password_changer/<password_changer_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/875499767560824422 5/password_changer/
↪8754997675608244226'
```

Response

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

Note

Password changer features:

- **Automatic rotation**: Passwords are changed based on configured schedules and policies
- **Multiple changers**: Secrets can have multiple secret changers for different systems
- **Execution order**: Use the position parameter to control the order of execution
- **Policy compliance**: Track whether passwords meet security policy requirements

Warning

Important considerations:

- Password changes are asynchronous operations that may take time to complete
- Failed password changes will be logged and may require manual intervention
- Always test secret changers in non-production environments first
- Ensure proper rollback procedures are in place before enabling automatic rotation

1.27.9 Secret Access Management

Overview

Secret access management tracks and controls who accesses secrets in collections. It provides audit trails, exclusive checkout capabilities, time-based access control, and the ability to mark accesses as safe for exposure monitoring.

Data Structures

Table 71: `SecretAccessModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique secret access identifier.
`user_id`	string	yes	Read-only. User identifier.
`secret_id`	string	yes	Read-only. Secret identifier.
`secret_name`	string		Read-only. Hidden; expensive to use. Secret name.
`secret_removed`	boolean		Read-only; expensive to use. Indicates whether the secret has been removed.
`secret_history`	string	yes	Read-only. Secret value version identifier.
`collection_id`	string	yes	Read-only; expensive to use. Collection identifier.
`collection_nam`	string		Read-only. Hidden; expensive to use. Collection name.
`collection_rem`	boolean		Read-only; expensive to use. Indicates whether the collection has been removed.
`source_ip`	string		Read-only. Client IP address at checkout time.
`source_port`	number		Read-only. Client port at checkout time.
`accessed_at`	datetime	yes	Read-only. When the checkout started.
`checked_in_at`	datetime		Read-only. When user checked in.
`expires_at`	datetime		Read-only. When access was set to expire. Uses secret checkout_time_limit attribute.
`exclusive`	boolean	yes	Read-only. Whether this was an exclusive checkout that locks the secret. Uses secret checkout_exclusive attribute.
`forced`	boolean	yes	Read-only. Whether user forced checkout while another user had exclusive access.
`user_name`	string		Read-only; expensive to use. User name.
`active`	boolean	yes	Read-only; expensive to use. Whether the checkout is still active and can be checkin.
`marked_safe`	boolean		Read-only; expensive to use. Whether the this access was marked as safe.
`marked_safe_by`	string		Read-only. User ID who marked this access as safe.
`marked_safe_by`	string		Read-only; expensive to use. Name of the user who marked this access as safe.
`marked_safe_at`	datetime		Read-only. Timestamp when access was marked as safe.
`user_blocked`	boolean		Read-only; expensive to use. Indicates whether the user who accessed the secret is blocked.
`user_removed`	boolean		Read-only; expensive to use. Indicates

Retrieve Available Attributes of the *SecretAccessModel*

Request

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

GET /api/v2/objspec/secret_access

> **Note**
>
> This endpoint may not be available if secret_access doesn't have a separate object specification.

List Secret Access Records

Request

Method	`GET`
Path	`/api/v2/secret/access`

GET /api/v2/secret/access

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/access'
```

Response


```
{
    "result": "success",
    "secret_access": [
        {
            "id": "1",
            "user_id": "8754997675608244225",
            "secret_id": "8754997675608244229",
            "secret_removed": false,
            "secret_history_id": "8754997675608244228",
            "collection_id": "8754997675608244227",
            "collection_removed": false,
            "source_ip": "10.2.0.182",
            "source_port": 55033,
            "accessed_at": "2026-04-02T23:56:21Z",
            "checked_in_at": "2026-04-02T23:56:21Z",
            "exclusive": false,
            "forced": false,
            "user_name": "admin",
            "active": false,
```


(continues on next page)

(continued from previous page)


```
            "marked_safe": false,
            "user_blocked": false,
            "user_removed": false,
            "user_lost_access": false
        }
    ]
}
```


Get Secret Access for Specific Secret

Request

Method	GET
Path	/api/v2/secret/<secret_id>/access

GET /api/v2/secret/<secret_id>/access

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/8754997675608244229/access'
```

Response


```
{
    "result": "success",
    "secret_access": [
        {
            "id": "1",
            "user_id": "8754997675608244225",
            "secret_id": "8754997675608244229",
            "secret_removed": false,
            "secret_history_id": "8754997675608244228",
            "collection_id": "8754997675608244227",
            "source_ip": "10.2.0.182",
            "source_port": 55033,
            "accessed_at": "2026-04-02T23:56:21Z",
            "checked_in_at": "2026-04-02T23:56:21Z",
            "exclusive": false,
            "forced": false,
            "user_name": "admin",
            "active": false,
            "marked_safe": false,
            "user_blocked": false,
            "user_removed": false,
            "user_lost_access": false
        }
    ]
}
```

Check In Secret Access

Request

Method	POST
Path	/api/v2/secret/access/<access_id>/checkin

POST /api/v2/secret/access/<access_id>/checkin

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/access/1/checkin'
```

Response


```
{
    "result": "success",
    "secret_access": [
        {
            "id": "1",
            "checked_in_at": "2026-04-02T23:56:21Z",
            "active": false
        }
    ]
}
```


Mark Secret as Safe

Request

Method	POST
Path	/api/v2/secret/<secret_id>/mark_safe

POST /api/v2/secret/<secret_id>/mark_safe

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/875499767560824422 9/mark_safe'
```

Response


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

> **Note**
>
> The mark_safe endpoint is used to mark a secret as safe after it has been reviewed for potential exposure. This updates the secret's exposure status and clears any exposure alerts.

1.27.10 Secret Exposure Monitoring

Overview

Secret exposure monitoring tracks users who have accessed secrets but subsequently lost permissions to those secrets. This helps identify potential security risks when former authorized users may still have knowledge of secret values.

Data Structures

Table 72: `SecretExposureModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier of the secret access.
`secret_id`	string		Read-only. Unique identifier of the secret that was exposed.
`user_id`	string		Read-only. Unique identifier of the user who previously accessed the secret.
`user_name`	string		Read-only; expensive to use. Display name of the user who previously accessed the secret.
`collection_id`	string		Read-only. Unique identifier of the collection that the secret belongs to.
`reason`	string {user_blocked, user_removed, user_lost_access}		Read-only. The security event that triggered this exposure alert.
`last_access_at`	datetime		Read-only. Timestamp of the user's most recent access to this secret before the security event.
`created_at`	datetime		Read-only. Timestamp when this exposure alert was created.
`modified_at`	datetime		Read-only. Timestamp when this exposure record was last updated.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SecretExposureModel*

Request

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

GET /api/v2/objspec/secret_exposure

> **Note**
>
> This endpoint may not be available if secret_exposure doesn't have a separate object specification.

Get Secret User Exposure

Request

Method	`GET`
Path	`/api/v2/secret/<secret_id>/user_exposure`

GET /api/v2/secret/<secret_id>/user_exposure

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/8754997675608244226/user_exposure'
```

Response

```
{
    "result": "success",
    "secret_exposure": [
        {
            "id": "41",
            "secret_id": "8754997675608244226",
            "user_id": "8754997675608244227",
            "user_name": "jdoe",
            "collection_id": "8754997675608244225",
            "reason": "user_blocked",
            "last_access_at": "2026-04-14T05:07:55Z",
            "created_at": "2026-04-14T05:07:55Z",
            "modified_at": "2026-04-14T05:07:55Z"
        }
    ]
}
```

1.27.11 Secret URI Management

Overview

Secret URI management allows associating secrets with specific URIs (URLs, connection strings, etc.). This enables linking credentials to their target applications, APIs, or services for automated authentication and access control.

Data Structures

Table 73: `SecretUriModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique secret URI identifier.
`secret_id`	string	yes	Immutable. Secret identifier.
`secret_name`	string		Read-only. Hidden; expensive to use.
`collection_id`	string		Read-only. Hidden; expensive to use.
`uri`	string	yes	URL/connection string assigned to the secret.
`host`	string		Read-only. Hidden. Host extracted from the provided uri.
`port`	number		Read-only. Hidden. Port extracted from the provided uri.
`vault`	string		Read-only. Hidden; expensive to use. Vault type (organization, personal).
`created_at`	datetime		Read-only.
`modified_at`	datetime		Read-only.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SecretUriModel*

Request

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

GET /api/v2/objspec/secret_uri

Note

This endpoint may not be available if secret_uri doesn't have a separate object specification.

List Secret URIs

Request

Method	`GET`
Path	`/api/v2/secret/uri`

GET /api/v2/secret/uri

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/uri'
```

Response


```
{
    "result": "success",
    "secret_uri": [
        {
            "id": "8754997675608244225",
            "secret_id": "8754997675608244225",
            "uri": "https://api.example.com/v1",
            "host": "api.example.com",
            "port": 443,
            "created_at": "2026-04-17T10:00:00Z"
        }
    ]
}
```


Get Secret URIs for Specific Secret

Request

Method	GET
Path	/api/v2/secret/<secret_id>/uri

GET /api/v2/secret/<secret_id>/uri

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/8754997675608244225/uri'
```

Response


```
{
    "result": "success",
    "secret_uri": [
        {
            "id": "8754997675608244229",
            "secret_id": "8754997675608244226",
            "uri": "https://database.example.com/api",
            "created_at": "2026-04-17T05:01:14Z",
            "modified_at": "2026-04-17T05:01:14Z"
        }
    ]
}
```


Add URI to Secret

Request

Method	POST
Path	/api/v2/secret/<secret_id>/uri
Body	SecretUriModel

POST /api/v2/secret/<secret_id>/uri

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "uri": "https://backup-api.example.com/v2"
  }' \
  'https://10.31.135.179/api/v2/secret/8754997675608244225/uri'
```

Response

```
{
    "result": "success",
    "secret_uri": [
        {
            "id": "8754997675608244226",
            "secret_id": "8754997675608244225",
            "uri": "https://backup-api.example.com/v2",
            "host": "backup-api.example.com",
            "port": 443
        }
    ]
}
```

Update Secret URI

Request

Method	PATCH
Path	/api/v2/secret/<secret_id>/uri/<id>
Body	SecretUriModel

PATCH /api/v2/secret/<secret_id>/uri/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "uri": "https://new-api.example.com/v3"
  }' \
```

(continues on next page)

(continued from previous page)

```
  'https://10.31.135.179/api/v2/secret/875499767560824225/uri/
↪8754997675608244226'
```

Response

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

Delete Secret URI

Request

Method	DELETE
Path	/api/v2/secret/<secret_id>/uri/<id>

DELETE /api/v2/secret/<secret_id>/uri/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/secret/875499767560824225/uri/
↪8754997675608244226'
```

Response

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

1.28 Secret Changers

Secret changers manage credentials for privileged accounts on monitored servers. They operate on various transport layers: SSH, LDAP, Telnet, or WinRM. You can use built-in options or create custom scripts.

1.28.1 Data Structures

Table 74: PasswordChangerModel

Attribute	Type	Required	Description
id	string		Read-only. Password change identifier. Uniqueness is required.
type	string {change, verify, remoteapp}	yes	Password changer type.

continues on next page

Table 74 – continued from previous page

Attribute	Type	Required	Description
`name`	string	yes	Password changer name. Case-insensitive. Uniqueness is required.
`target`	string {account, secret, secret-login, secret-sshkey}; Default value `account`	yes	Immutable. Password changer target.
`transport`	string {LDAP, SSH, Telnet, WinRM}	if `type == change || verify`	Transport layer for secret changer.
`timeout`	number {0 - 2147483647}	if `type == change || verify`	Script's execution time limit expressed in seconds.
`remote_app_pat`	string	if `type == remoteapp`	Read-only; expensive to use. Binary path for remote app.
`remote_app_arg`	string	if `type == remoteapp`	Read-only; expensive to use. Binary arguments for remote app.
`builtin`	boolean		Read-only; expensive to use. Is object built-in? Built-in objects shouldn't be editable.
`hidden`	boolean		Read-only; expensive to use; if `true`, the object is hidden in UI.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`password_chang`	string	if `target == secret`	Secret Change Policy id.
`change_on_chec`	boolean		If set, password will be changed after last password checkin. Requires `target == secret`.
`change_on_sess`	boolean		If set, password will be changed after session finishes. Requires `target == secret`.
`recovery`	boolean		Waiting for secret change after triggered. Requires `target == secret`.
`removed`	boolean		Read-only.

1.28.2 Retrieve Available Attributes of the *PasswordChangerModel*

Request

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

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

1.28.3 Get Secret Changers List

Request

Method	`GET`
Path	`/api/v2/password_changer`

Example Request

GET /api/v2/password_changer`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/password_changer'
```

Response


```
{
    "result": "success",
    "password_changer": [
        {
            "id": "1",
            "type": "change",
            "name": "Unix\/SSH changer",
            "transport": "SSH",
            "timeout": 300,
            "builtin": true,
            "hidden": false,
            "created_at": "2024-06-10 05:59:22.99706-07",
            "modified_at": "2024-06-10 05:59:22.99706-07"
        },
        {
            "id": "2",
            "type": "verify",
            "name": "Unix\/SSH verifier",
            "transport": "SSH",
            "timeout": 300,
            "builtin": true,
            "hidden": false,
            "created_at": "2024-06-10 05:59:22.997876-07",
            "modified_at": "2024-06-10 05:59:22.997876-07"
        }
    ]
}
```

1.28.4 Get Secret Changer by ID

Request

Method	GET
Path	/api/v2/password_changer/<id>

Example Request

GET /api/v2/password_changer/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/password_changer/1'
```

Response

```
{
    "password_changer": {
        "id": "1",
        "name": "Unix\/SSH changer",
        "type": "change",
        "transport": "SSH",
        "timeout": 300,
        "variables": [
            {
                "name": "transport_bind_ip",
                "description": "An IP on Fudo interface that will be used as␣
↪source address.",
                "object_type": "server",
                "object_property": "bind_ip",
                "encrypted": false,
                "optional": true,
                "transport": true,
                "value": {
                    "value_type": "self"
                }
            },
            {
                "name": "transport_host",
                "description": "An address to which secret changer\/verifier␣
↪connects.",
                "object_type": "server",
                "object_property": "address",
                "encrypted": false,
                "optional": false,
                "transport": true,
                "value": {
                    "value_type": "self"
                }
            }
```

(continues on next page)

(continued from previous page)


```
        ],
        "commands": [
            {
                "type": "expected",
                "value": "Last login:",
                "description": null
            },
            {
                "type": "input",
                "value": "passwd %%account_login%%",
                "description": null
            }
        ],
        "builtin": true,
        "hidden": false,
        "created_at": "2024-06-10 05:59:22.99706-07",
        "modified_at": "2024-06-10 05:59:22.99706-07"
    },
    "result": "success"
}
```


1.28.5 Defining Secret Changer

Request

Method	`POST`
Path	`/api/v2/password_changer`
Headers	`Content-Type: Application/json`
Body	`PasswordChangerModel`

Example Request

POST /api/v2/password_changer`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/password_changer' \
  -d'{"name":"Password_Changer_WinRM","type":"change","transport":"WinRM",
↪"timeout":1000,"commands":[{"type":"input","value":"net user \"%%account_login
↪%%\" \"%%new_secret_value%%\"","description":"Description text."}]}'
```

Response


```
{
    "password_changer": {
        "id": "9124292845052624933"
    },
    "result": "success"
}
```

1.28.6 Modify Secret Changer

Request

Method	`PATCH`
Path	`/api/v2/password_changer/<id>`
Headers	`Content-Type: Application/json`
Body	`PasswordChangerModel`

Example Request: Change Basic Properties

PATCH /api/v2/password_changer/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/password_changer/9124292845052624927' \
  -d'{"type":"verify","transport":"SSH","timeout":1000}'
```

Example Request: Modifying Commands

PATCH /api/v2/password_changer/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/password_changer/9124292845052624933' \
  -d'{"commands":[{"type":"input","value":"net user \"%%account_login%%\" \"%
↪%new_secret_value%%\"","description":"Description."}]}'
```

Example Request: Adding Variable

PATCH /api/v2/password_changer/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/password_changer/9124292845052624933' \
  -d'{"variables":[{"name":"transport_bind_ip","object_type":"server","object_
↪property":"name","value":{"value_type":"self"}}]}'
```

Response

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

1.28.7 Triggering Password Change for the Account

Request

Method	`POST`
Path	`/api/v2/account/<id>/trigger_password_changer`

Example Request

POST /api/v2/account/<id>/trigger_password_changer`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/account/9124292845052624908/trigger_password_
↪changer'
```

Response

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

1.28.8 Deleting Secret Changer

Request

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

Example Request

DELETE /api/v2/password_changer/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/password_changer/9124292845052624927'
```

Response

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

1.29 Secret Changer Policy

Secret Change Policy defines specifics of how frequently the password should be changed and password complexity requirements.

1.29.1 Data Structures

Table 75: `PasswordPolicyModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Secret change policy identifier. Uniqueness is required.

continues on next page

Table 75 – continued from previous page

Attribute	Type	Required	Description
`name`	string	yes	Secret change policy name. Case-insensitive. Uniqueness is required.
`change_frequency`	number {0 - 2147483647}	with `complexity_length` `` and ``ssh_keytype`	Time in minutes after which password should be changed.
`verification_frequer`	number {0 - 2147483647}		Time in minutes after which password should be verified.
`complexity_length`	number {0 - 2147483647}		Total password length.
`ssh_keytype`	string {ed25519, ecdsa, rsa, rsa2048, rsa4096, rsa8192, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521}		SSH key algorithm. Case-insensitive. Default: `ed25519`.
`password_changer_ena`	boolean		Read-only; expensive to use. Is secret changer enabled for this policy?
`password_verifier_er`	boolean		Read-only; expensive to use. Is Secret verifier enabled for this policy?
`complexity_lowercase`	number {0 - 2147483647}		Number of lower case characters in password. Requires `complexity_length`.
`complexity_uppercase`	number {0 - 2147483647}		Number of upper case characters in password. Requires `complexity_length`.
`complexity_numeric`	number {0 - 2147483647}		Number of numeric characters in password. Requires `complexity_length`.
`complexity_nonalnum`	number {0 - 2147483647}		Number of special characters in password. Requires `complexity_length`.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

continues on next page

Table 75 – continued from previous page

Attribute	Type	Required	Description
`builtin`	boolean		Read-only; expensive to use. Is object built-in? Built-in objects shouldn't be editable.
`hidden`	boolean		Read-only; expensive to use. Shall the object be hidden in UI?

1.29.2 Retrieve Available Attributes of the *PasswordPolicyModel*

Request

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

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

1.29.3 Get Secret Changer Policies List

Request

Method	`GET`
Path	`/api/v2/password_change_policy`

Example Request

GET /api/v2/password_change_policy`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/password_change_policy'
```

Response

```
{
    "result": "success",
    "password_change_policy": [
        {
            "id": "1",
            "name": "Static, without restrictions",
            "password_changer_enabled": false,
            "password_verifier_enabled": false,
            "created_at": "2024-06-10 05:59:22.994431-07",
            "modified_at": "2024-06-10 05:59:22.994431-07",
            "builtin": true,
            "hidden": false
        },
```

(continues on next page)

(continued from previous page)

```
        {
            "id": "9124292845052624897",
            "name": "Pass Changing Enabled",
            "change_frequency": 2,
            "complexity_length": 8,
            "password_changer_enabled": true,
            "password_verifier_enabled": false,
            "complexity_lowercase": 1,
                        "ssh_keytype": "ed25519",
            "created_at": "2024-06-11 23:29:24.511416-07",
            "modified_at": "2024-06-12 02:16:38.410347-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```

1.29.4 Get Secret Change Policy by ID

Request

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

Example Request

GET /api/v2/password_change_policy/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/password_change_policy/9124292845052624897'
```

Response

```
{
    "result": "success",
    "password_change_policy": {
        "id": "9124292845052624897",
        "name": "Pass Changing Enabled",
        "change_frequency": 2,
        "complexity_length": 8,
        "password_changer_enabled": true,
        "password_verifier_enabled": false,
        "complexity_lowercase": 1,
        "created_at": "2024-06-11 23:29:24.511416-07",
        "modified_at": "2024-06-12 02:16:38.410347-07",
        "builtin": false,
        "hidden": false
    }
}
```

1.29.5 Defining Secret Change Policy

Request

Method	`POST`
Path	`/api/v2/password_change_policy`
Headers	`Content-Type: Application/json`
Body	`PasswordPolicyModel`

Example Request

POST /api/v2/password_change_policy`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/password_change_policy' \
  -d'{"name":"Password_Verif_1","change_frequency":2,"complexity_length":8,
↪"complexity_lowercase":2}'
```

Response

```
{
    "result": "success",
    "password_change_policy": {
        "id": "9124292845052624898"
    }
}
```

1.29.6 Modify Secret Change Policy

Request

Method	`PATCH`
Path	`/api/v2/password_change_policy/<id>`
Headers	`Content-Type: Application/json`
Body	`PasswordPolicyModel`

Example Request

PATCH /api/v2/password_change_policy/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/password_change_policy/9124292845052624897' \
  -d'{"change_frequency":4,"complexity_lowercase":2}'
```

Response

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

1.29.7 Deleting Secret Change Policy

Request

Method	DELETE
Path	/api/v2/password_change_policy/<id>

Example Request

DELETE /api/v2/password_change_policy/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/password_change_policy/9124292845052624897'
```

Response

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

1.30 Policies and Regular Expressions

Policies are patterns definitions facilitating proactive session monitoring. In case a defined pattern is detected, Fudo Enterprise can automatically take respective actions and notify the administrator about the current situation.

1.30.1 Regular Expressions

Data Structures

Table 76: RegExpModel

Attribute	Type	Required	Description
id	string		Read-only, unique regular expression identifier.
name	string	yes	Unique, case-insensitive regular expression name.
type	string {ml, regexp}	yes	Immutable. Policy type.
regexp	string	yes	Regular expression content.
created_at	datetime		Read-only. Timestamp of creation.
modified_at	datetime		Read-only. Timestamp of modification.
removed	boolean		Read-only.

Retrieve Available Attributes of the *RegExpModel*

Request

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

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

Get Regular Expressions List

Request

Method	`GET`
Path	`/api/v2/regexp`

Example Request

GET /api/v2/regexp`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/regexp'
```

Response

```
{
    "result": "success",
    "regexp": [
        {
            "id": "9124292845052624897",
            "name": "Reg_ex_1",
            "regexp": "(^|[^a-zA-Z])rm[[:space:]]",
            "created_at": "2024-06-14 05:46:25.34634-07",
            "modified_at": "2024-06-14 05:46:25.34634-07"
        }
    ]
}
```

Get Regular Expression by ID

Request

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

Example Request

GET /api/v2/regexp/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/regexp/9124292845052624897'
```

Response

```
{
    "result": "success",
    "regexp": {
        "id": "9124292845052624897",
        "name": "Reg_ex_1",
        "regexp": "(^|[^a-zA-Z])rm[[:space:]]",
        "created_at": "2024-06-14 05:46:25.34634-07",
        "modified_at": "2024-06-14 05:46:25.34634-07"
    }
}
```

Defining Regular Expression

Request

Method	`POST`
Path	`/api/v2/regexp`
Headers	`Content-Type: Application/json`
Body	`RegExpModel`

Example Request

POST /api/v2/regexp`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/regexp' \
  -d'{"name":"Reg_ex_2","regexp":"(^|[^a-zA-Z])rm[[:space:]]"}'
```

Response

```
{
    "result": "success",
    "regexp": {
        "id": "9124292845052624900"
    }
}
```

Modify Regular Expression

Request

Method	PATCH
Path	/api/v2/regexp/<id>
Headers	Content-Type: Application/json
Body	RegExpModel

Example Request

PATCH /api/v2/regexp/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/regexp/9124292845052624897' \
  -d'{"regexp":"(^|[^a-zA-Z])rm[[:space:]]"}''
```

Response

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

Deleting Regular Expression

Request

Method	DELETE
Path	/api/v2/regexp/<id>

Example Request

DELETE /api/v2/regexp/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/regexp/9124292845052624897'
```

Response

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

1.30.2 Policies

Data Structures

Table 77: *PolicyModel*

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`name`	string	yes	Case-insensitive. Uniqueness is required.
`type`	string {ai_summary, live_analysis, ml, regexp, sudo}	yes	Immutable.
`priority`	string {critical, high, medium, low}	yes	Expensive to use.
`email_send`	boolean; Default value `false`	yes	
`push_send`	boolean; Default value `false`	yes	
`input_match`	boolean; Default value `false`	yes	
`snmp_trap`	boolean; Default value `false`	yes	
`session_pause`	boolean; Default value `false`	yes	
`session_terminate`	boolean; Default value `false`	yes	
`user_block`	boolean; Default value `false`	yes	
`ml_threat_probabilit`	string {avg, max, min}	if `type` == `ml`	
`ml_threat_threshold`	string	if `type` == `ml`	
`ai_summary_min_threa`	number	if `type` == `ai_summar`	
`live_analysis_min_co`	number	if `type` == `live_anal`	Minimum number of findings that must be reported by live LLM session analysis before the policy fires.
`live_analysis_min_se`	string {high, medium}	if `type` == `live_anal`	Minimum severity of a finding reported by live LLM session analysis for the policy to fire.
`sudo_runas_user`	string	if `type` == `sudo`	
`sudo_runas_group`	string	if `type` == `sudo`	
`created_at`	datetime		Read-only. Record creation timestamp.
`modified_at`	datetime		Read-only. Record modification timestamp.
`removed`	boolean		Read-only. Record is removed.

Request for Retrieving Available Attributes

Request

Method	GET
Path	/api/v2/objspec/policy

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

Get Policies List

Request

Method	GET
Path	/api/v2/policy

Example Request

GET /api/v2/policy

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.0.214.98/api/v2/policy'
```

Response

```
{
    "result": "success",
    "policy": [
        {
            "id": "9124292845052624897",
            "name": "PCP",
            "type": "regexp",
            "priority": "medium",
            "email_send": true,
            "input_match": false,
            "snmp_trap": false,
            "session_pause": false,
            "session_terminate": false,
            "user_block": false,
            "created_at": "2024-06-11 22:52:18.44898-07",
            "modified_at": "2024-06-11 22:52:18.44898-07"
        },
        {
            "id": "9124292845052624898",
            "name": "AI_Policy_1",
            "type": "regexp",
            "priority": "low",
            "email_send": false,
```

(continues on next page)

(continued from previous page)

```
            "input_match": false,
            "snmp_trap": false,
            "session_pause": false,
            "session_terminate": false,
            "user_block": false,
            "created_at": "2024-06-14 15:15:58.534771-07",
            "modified_at": "2024-06-14 15:15:58.534771-07"
        }
    ]
}
```

Get Policy by ID

Request

Method	GET
Path	/api/v2/policy/<id>

Example Request

GET /api/v2/policy/<id>

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.0.214.98/api/v2/policy/9124292845052624897'
```

Response

```
{
    "result": "success",
    "policy": {
        "id": "9124292845052624897",
        "name": "PCP",
        "type": "regexp",
        "priority": "medium",
        "email_send": true,
        "input_match": false,
        "snmp_trap": false,
        "session_pause": false,
        "session_terminate": false,
        "user_block": false,
        "created_at": "2024-06-11 22:52:18.44898-07",
        "modified_at": "2024-06-11 22:52:18.44898-07"
    }
}
```

Create Policy

Request

Method	`POST`
Path	`/api/v2/policy`
Headers	`Content-Type: Application/json`
Body	`PolicyModel`

Example Request

POST /api/v2/policy

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/policy' \
  -d'{"name":"Policy_1","type":"regexp","priority":"medium","email_send":true,
↪"session_pause":true}'
```

Response

```
{
    "result": "success",
    "policy": {
        "id": "9124292845052624899"
    }
}
```

Modify Policy

Request

Method	`PATCH`
Path	`/api/v2/policy/<id>`
Headers	`Content-Type: Application/json`
Body	`PolicyModel`

Example Request

PATCH /api/v2/policy/<id>

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/policy/9124292845052624927' \
  -d'{"priority":"low","email_send":false,"user_block":true}'
```

Response

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

Deleting Policy

Request

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

Example Request

DELETE /api/v2/policy/<id>

```
curl -s -k -X DELETE -H 'Authorization: <token>' https://10.0.214.98/api/v2/
↪policy/9124292845052624899
```

Response

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

1.30.3 Managing Regular Expressions Assignment

Data Structures

Table 78: `RegExpPolicyModel`

Attribute	Type	Required	Description
`id`	string		Read-only, unique regular expression policy identifier.
`policy_id`	string	yes	Immutable policy identifier.
`regexp_id`	string	yes	Immutable regular expression identifier.
`policy_name`	string		Read-only, expensive to use.
`regexp_name`	string		Read-only, expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *RegExpPolicyModel*

Request

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

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

Get the List of Regular Expression Assignments for Policies

Request

Method	GET
Path	/api/v2/policy/regexp

Example Request

GET /api/v2/policy/regexp`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/policy/regexp'
```

Response


```
{
    "result": "success",
    "regexp_policy": [
        {
            "policy_id": "9124292845052624899",
            "regexp_id": "9124292845052624897",
            "policy_name": "Policy_1",
            "regexp_name": "Reg_ex_1",
            "created_at": "2024-06-20 03:34:38.425893-07",
            "modified_at": "2024-06-20 03:34:38.425893-07"
        },
        {
            "policy_id": "9124292845052624897",
            "regexp_id": "9124292845052624900",
            "policy_name": "Policy_2",
            "regexp_name": "Reg_ex_2",
            "created_at": "2024-06-20 06:56:17.452651-07",
            "modified_at": "2024-06-20 06:56:17.452651-07"
        },
        {
            "policy_id": "9124292845052624897",
            "regexp_id": "9124292845052624897",
            "policy_name": "Policy_2",
            "regexp_name": "Reg_ex_1",
            "created_at": "2024-06-20 06:56:17.452652-07",
            "modified_at": "2024-06-20 06:56:17.452652-07"
        },
        {
            "policy_id": "9124292845052624900",
            "regexp_id": "9124292845052624900",
            "policy_name": "Policy_3",
            "regexp_name": "Reg_ex_2",
            "created_at": "2024-06-20 06:56:35.335851-07",
            "modified_at": "2024-06-20 06:56:35.335851-07"
```


(continues on next page)

(continued from previous page)

```
        }
    ]
}
```

Assigning Regular Expression to a Policy

Request

Method	`POST`
Path	`/api/v2/policy/regexp`
Headers	`Content-Type: Application/json`
Body	`RegExpPolicyModel`

Example Request

POST /api/v2/policy/regexp`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/policy/regexp' \
  -d'{"policy_id":"9124292845052624899","regexp_id":"9124292845052624900"}'
```

Response

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

Checking Regular Expression Assignment With a Policy

Request

Method	`GET`
Path	`/api/v2/policy/<policy_id>/regexp/<regexp_id>`
Headers	`Content-Type: Application/json`
Body	`PolicyModel`

Example Request

GET /api/v2/policy/<id>/regexp/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/policy/9124292845052624899/regexp/
↪9124292845052624897'
```

Response

```
{
    "result": "success",
    "regexp_policy": {
        "policy_id": "9124292845052624899",
        "regexp_id": "9124292845052624897",
        "policy_name": "Policy_1",
        "regexp_name": "Reg_ex_1",
        "created_at": "2024-06-20 03:16:15.126665-07",
        "modified_at": "2024-06-20 03:16:15.126665-07"
    }
}
```


Deleting Regular Expression Assignment to a Policy

Request

Method	DELETE
Path	/api/v2/policy/<policy_id>/regexp/<regexp_id>

Example Request

DELETE /api/v2/policy/<id>/regexp/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/policy/9124292845052624899/regexp/
↪9124292845052624897'
```

Response


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


1.31 Secret Audit NEW

Secret audit checks password vault secrets against a database of compromised passwords. The database (hashdb) is built from a file uploaded to Fudo Enterprise; only one hashdb is active at a time and uploading a new one replaces it.

1.31.1 Data Structures

Table 79: `SecretAuditModel`

Attribute	Type	Required	Description
`filename`	string	yes	Read-only. Original filename of the uploaded file, taken from the `X-Fudo-Filename` header.
`format`	string {plain, sha1}	yes	Read-only. Upload format the hashdb was built from.
`uploaded_at`	datetime	yes	Read-only. UTC timestamp when the upload that built this hashdb completed.
`original_bytes`	number	yes	Read-only. Size of the uploaded file in bytes, before hashing and deduplication.
`store_bytes`	number	yes	Read-only. Total on-disk size of the active hashdb.
`hash_count`	number	yes	Read-only. Number of unique SHA-1 hashes in the active hashdb.
`sha256`	string	yes	Read-only. SHA-256 of the uploaded file's bytes, for integrity verification.
`origin_node_seri`	string	yes	Read-only. Serial of the cluster node the hashdb was uploaded on. Deletion is only permitted on that node.
`can_delete`	boolean	yes	Read-only. Whether this node may delete the hashdb. `true` only on the node it was uploaded on.

1.31.2 Retrieve Available Attributes of the *SecretAuditModel*

Request

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

GET /api/v2/objspec/secret_audit

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/objspec/secret_audit'
```

1.31.3 Get the Active Hash Database

Request

Method	`GET`
Path	`/api/v2/secret_audit`

GET /api/v2/secret_audit

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/secret_audit'
```

Response

```
{
    "secret_audit": {
        "filename": "weakpass-small.txt",
        "format": "plain",
        "uploaded_at": "2026-08-18T09:17:25.525286050Z",
        "original_bytes": 2627,
        "store_bytes": 4020,
        "hash_count": 201,
        "sha256":
↪"966e38d2f060a4697737e626309bef06bba916ec3a12a34aa619d334a660695d",
        "origin_node_serial": "83457314",
        "can_delete": true
    },
    "result": "success"
}
```

Note

When no database has been uploaded, the endpoint answers `{"result": "failure", "message": "No hashdb uploaded yet."}`.

1.31.4 Upload a Hash Database

Request

Method	`POST`
Path	`/api/v2/secret_audit/upload/<format>`
Body	Raw file bytes

POST /api/v2/secret_audit/upload/<format>

`<format>` is `plain` for a file of newline-separated passwords, or `sha1` for a file of SHA-1 hashes. Any other value is rejected with `{"result": "failure", "message": "invalid format"}`.

The file name must be supplied in the `X-Fudo-Filename` header; without it the request fails with `{"result": "failure", "message": "X-Fudo-Filename header is required."}`. The upload replaces the currently active database.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'X-Fudo-Filename: weakpass-small.txt' \
```

(continues on next page)

(continued from previous page)

```
  -H 'Content-Type: application/octet-stream' \
  --data-binary '@weakpass-small.txt' \
  'https://10.33.3.191/api/v2/secret_audit/upload/plain'
```

Response

Unlike other endpoints, the upload streams progress as newline-delimited JSON objects while the database is built. Each line is a separate object; the final line has `"phase": "done"`.

```
{"phase":"sorting","progress":0,"bytes_done":0,"bytes_total":4020}
{"phase":"sorting","progress":100,"bytes_done":4020,"bytes_total":4020}
{"phase":"finalizing","progress":0,"bytes_done":0,"bytes_total":4020}
{"phase":"finalizing","progress":100,"bytes_done":4020,"bytes_total":4020}
{"phase":"auditing"}
{"phase":"done","hashes":201,"compromised_total":0,"scanned_total":0,"elapsed_ms
↪":14,"invalid_utf8_count":0}
```

Table 80: Progress event fields

Field	Type	Description
`phase`	string {sorting, finalizing, auditing, done}	Stage the upload has reached.
`progress`	number	Percentage of the current phase completed.
`bytes_done`	number	Bytes processed in the current phase.
`bytes_total`	number	Total bytes to process in the current phase.
`hashes`	number	Final event only. Number of unique hashes stored.
`scanned_total`	number	Final event only. Number of secrets checked against the new database.
`compromised_tota`	number	Final event only. Number of secrets found in the new database.
`elapsed_ms`	number	Final event only. Total processing time in milliseconds.
`invalid_utf8_cou`	number	Final event only. Number of input lines skipped as invalid UTF-8.

Note

A client must not parse the response as a single JSON document - it is a stream of objects. Read it line by line and treat the `done` event as the result.

1.31.5 Delete the Hash Database

Request

Method	DELETE
Path	/api/v2/secret_audit

DELETE /api/v2/secret_audit

Only permitted on the node the database was uploaded on - the one reported by `origin_node_serial`, where `can_delete` is `true`.

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/secret_audit'
```

Response

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

1.32 Discovery

The *Discovery* feature is able to search for accounts with different privilege levels on domain controllers, servers on domain controllers, and local accounts on Windows servers.

The Discovery function needs two objects to provide the most efficient results:

1. A *scanner* with configuration of the target server and an account to connect, and a schedule for running the scanner automatically.
2. A *rule* to specify what the scanner should do in terms of its discovery.

1.32.1 Discovery Scanner

Data Structures

Table 81: `DiscoveryScannerModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier.
`name`	string	yes	Case-insensitive. Unique.
`description`	string		
`type`	string {ldap_accour ldap_server, lo- cal_account}	yes	
`pool_id`	string	if `type` == `ldap_acco` || `ldap_serv`	Requires `read` right on the `pool` object for GET, POST, PATCH, and DELETE requests.
`server_id`	string	if `type` == `ldap_acco` || `ldap_serv`	Requires `read` right on the `server` object for GET, POST, PATCH, and DELETE requests.
`account_id`	string	yes	Requires `read` right on the `account` object for GET, POST, PATCH, and DELETE requests.
`enabled`	boolean; de- fault value `false`	yes	
`category`	string {priv- ileged, nonpriv- leged, all}	if `type` == `ldap_acco`	
`filter_base`	string	if `type` == `ldap_acco` || `ldap_serv`	
`filter_group`	string	if `type` == `ldap_acco` || `ldap_serv`	
`server_tls_ca_ ificate`	string	if `type` == `ldap_serv`	Value-format: x509-ca-certificate.
`schedule_dow`	number {1 - 7}	with `schedule_`	Schedule day of week. Value-range: 1 to 7.
`schedule_time`	string	with `schedule_`	
`last_scan`	string		Read-only. Timestamp of the last scan.
`next_scan`	string		Read-only. Timestamp of the next scan.
`next_manual_sc`	string		Read-only. Timestamp of the next manual scan.
`password_chang`	string	if `type` == `ldap_acco` || `local_acc`	

Retrieve Available Attributes of the *DiscoveryScannerModel*

Request

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

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

Get Scanners List

Request

Method	`GET`
Path	`/api/v2/scanner`

Example Request

GET /api/v2/scanner`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/scanner'
```

Response

```
{
    "result": "success",
    "scanner": [
        {
            "id": "5620492334958379009",
            "name": "LDAP_scanner",
            "type": "ldap_account",
            "pool_id": "5620492334958379010",
            "server_id": "5620492334958379011",
            "account_id": "5620492334958379011",
            "enabled": true,
            "category": "nonprivileged",
                        "schedule_dow": 1,
                        "schedule_time": "23:00:00-07",
            "last_scan": "-infinity",
            "next_scan": "infinity",
                        "next_manual_scan": "infinity",
            "connection_port": 636,
            "created_at": "2024-06-24 04:25:40.966955-07",
            "modified_at": "2024-06-24 04:25:40.966955-07"
        }
    ]
}
```

Get Scanner by ID

Request

Method	GET
Path	/api/v2/scanner/<id>

Example Request

GET /api/v2/scanner/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/scanner/5620492334958379009'
```

Response


```
{
    "result": "success",
    "scanner": [
        {
            "id": "5620492334958379009",
            "name": "LDAP_scanner",
            "type": "ldap_account",
            "pool_id": "5620492334958379010",
            "server_id": "5620492334958379011",
            "account_id": "5620492334958379011",
            "enabled": true,
            "category": "nonprivileged",
                        "schedule_dow": 1,
                        "schedule_time": "23:00:00-07",
            "last_scan": "-infinity",
            "next_scan": "infinity",
                        "next_manual_scan": "infinity",
            "connection_port": 636,
            "created_at": "2024-06-24 04:25:40.966955-07",
            "modified_at": "2024-06-24 04:25:40.966955-07"
        }
    ]
}
```


Create Scanner

Request

Method	POST
Path	/api/v2/scanner
Headers	Content-Type: Application/json
Body	DiscoveryScannerModel

Example Request

POST /api/v2/scanner`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/scanner' \
  -d'{"name":"LDAP_Scanner","type":"ldap_account","pool_id":"5620492334958379010
↪","server_id":"5620492334958379011","account_id":"5620492334958379011",
↪"enabled":false,"category":"nonprivileged","connection_port": 636}'
```

Response

```
{
    "result": "success",
    "scanner": {
        "id": "5620492334958379010"
    }
}
```

Modify Scanner

Request

Method	PATCH
Path	/api/v2/scanner/<id>
Headers	Content-Type: Application/json
Body	DiscoveryScannerModel

Example Request

PATCH /api/v2/scanner/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/scanner/5620492334958379010' \
  -d'{"category":"privileged"}'
```

Response

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

Starting Scan

Request

Method	POST
Path	/api/v2//scanner/<scanner_id>/start

Example Request

POST /api/v2/scanner/<id>/start`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/scanner/5620492334958379010/start'
```

Response

```
{
    "result": "success",
    "next_manual_scan": "2025-05-05 01:53:54.923673-07"
}
```

Deleting Scanner

Request

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

Example Request

DELETE /api/v2/scanner/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/scanner/5620492334958379010'
```

Response

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

1.32.2 Discovery Rule

Data Structures

Table 82: `DiscoveryRuleModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier.
`name`	string	yes	Case-insensitive. Unique.
`description`	string		
`type`	string {account, server}	yes	
`enabled`	boolean; default value `true`	yes	
`category`	string {privileged, nonprivileged, all}		
`action`	string{onboar quarantine}	yes	
`filter_type`	string{consist ends_with, starts_with}	with `filter_va`	
`filter_value`	string	with `filter_ty`	
`scanners`	object-array		Read-only; expensive to use.
`scanner_ids`	string-array		Read-only; expensive to use; hidden.
`scanner_names`	string-array		Read-only; expensive to use; hidden.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

1.32.3 Retrieve Available Attributes of the *DiscoveryRuleModel*

Request

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

GET /api/v2/objspec/rule

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

1.32.4 Get Rules List

Request

Method	GET
Path	/api/v2/discovery/rule

GET /api/v2/discovery/rule

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule'
```

Response


```
{
    "result": "success",
    "rule": [
        {
            "id": "9115285645797883905",
            "name": "Rule_1",
            "type": "account",
            "enabled": true,
            "category": "privileged",
            "action": "onboard",
            "filter_type": "starts_with",
            "filter_value": "admin",
            "created_at": "2025-05-06 00:27:11.928953-07",
            "modified_at": "2025-05-06 00:27:11.928953-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```


1.32.5 Get Rule by ID

Request

Method	GET
Path	/api/v2/discovery/rule

GET /api/v2/discovery/rule/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883905'
```

Response


```
{
    "result": "success",
    "rule": [
        {
            "id": "9115285645797883905",
            "name": "Rule_1",
            "type": "account",
            "enabled": true,
            "category": "privileged",
            "action": "onboard",
            "filter_type": "starts_with",
            "filter_value": "admin",
            "created_at": "2025-05-06 00:27:11.928953-07",
            "modified_at": "2025-05-06 00:27:11.928953-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```


1.32.6 Create Rule

Request

Method	`POST`
Path	`/api/v2/discovery/rule`
Headers	`Content-Type: application/json`
Body	`DiscoveryRuleModel`

POST /api/v2/discovery/rule

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/rule' \
  -d'{"name": "Rule_2","type": "account","enabled": true,"category": "privileged
↪","action": "onboard","filter_type": "starts_with","filter_value": "admin"}'
```

Response


```
{
    "result": "success",
    "rule": {
        "id": "9115285645797883906"
    }
}
```

1.32.7 Modify Rule

Request

Method	PATCH
Path	/api/v2/discovery/rule/<id>
Headers	Content-Type: application/json
Body	DiscoveryRuleModel

PATCH /api/v2/discovery/rule/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/scanner/9115285645797883906' \
  -d'{"action":"quarantine","filter_type":"starts_with","filter_value":"fudo_
↪admin"}'
```

Response

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

1.32.8 Delete Rule

Request

Method	DELETE
Path	/api/v2/discovery/rule/<id>

DELETE /api/v2/discovery/rule/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883906'
```

Response

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

1.32.9 Discovery Scanner-Rule Assignment

Data Structures

Table 83: `DiscoveryScannerRuleModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Protected.
`scanner_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `scanner_id` with attribute `rule_id`.
`rule_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `rule_id` with attribute `scanner_id`.
`position`	number		
`scanner_name`	string		Read-only; Expensive to use.
`rule_name`	string		Read-only; Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *DiscoveryScannerRuleModel*

Request

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

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

Get List of Scanner-Rule Assignment

Request

Method	`GET`
Path	`/api/v2/scanner/rule`

Example Request

GET /api/v2/scanner/rule`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/scanner/rule'
```

Response

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

(continues on next page)

(continued from previous page)


```
    "scanner_rule": [
        {
            "scanner_id": "9115285645797883907",
            "rule_id": "9115285645797883905",
            "position": 0,
            "scanner_name": "LDAP_Scanner",
            "rule_name": "Rule_1",
            "created_at": "2025-05-06 02:58:54.21643-07",
            "modified_at": "2025-05-06 02:58:54.21643-07"
        },
        {
            "scanner_id": "9115285645797883907",
            "rule_id": "9115285645797883906",
            "position": 1,
            "scanner_name": "LDAP_Scanner",
            "rule_name": "Rule_2",
            "created_at": "2025-05-06 02:58:54.227576-07",
            "modified_at": "2025-05-06 02:58:54.227576-07"
        }
    ]
}
```


Get Scanner-Rule Assignment by ID

Request

Method	`GET`
Path	`/api/v2/scanner/<scanner_id>/rule/<rule_id>`

Example Request

GET /api/v2/discovery/scanner/<id>/rule/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/scanner/9115285645797883907/rule/
↪9115285645797883906'
```

Response


```
{
    "result": "success",
    "scanner_rule": [
        {
            "scanner_id": "9115285645797883907",
            "rule_id": "9115285645797883906",
            "position": 1,
            "scanner_name": "LDAP_Scanner",
            "rule_name": "Rule_2",
```


(continues on next page)

(continued from previous page)

```
            "created_at": "2025-05-06 02:58:54.227576-07",
            "modified_at": "2025-05-06 02:58:54.227576-07"
        }
    ]
}
```

Create Scanner-Rule Assignment

Request

Method	`POST`
Path	`/api/v2/scanner/rule`
Headers	`Content-Type: Application/json`
Body	`DiscoveryScannerRuleModel`

Example Request

POST /api/v2/scanner/rule`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/scanner/rule' \
  -d'{"scanner_id":"9115285645797883907","rule_id":"9115285645797883908"}'
```

Response

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

Modify Scanner–Rule Assignment Attributes

Request

Method	`PATCH`
Path	`/api/v2/scanner/<scanner_id>/rule/<rule_id>`
Headers	`Content-Type: Application/json`
Body	`GroupSafeModel`

PATCH /api/v2/scanner/<scanner_id>/rule/<rule_id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.31.135.179/api/v2/scanner/9115285645797883907/rule/
```

(continues on next page)

(continued from previous page)

```
↪9115285645797883908' \
  -d'{"position": 1}'
```

Response

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

Deleting Scanner-Rule Assignment

Request

Method	`DELETE`
Path	`/api/v2/scanner/<scanner_id>/rule/<rule_id>`

Example Request

DELETE /api/v2/scanner/<id>/rule/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/scanner/9115285645797883907/rule/
↪9115285645797883908'
```

Response

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

1.32.10 Discovery Rule-Listener Assignment

Data Structures

Table 84: `DiscoveryRuleListenerModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Protected.
`rule_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `rule_id` with attribute `listener_id`.
`listener_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `listener_id` with attribute `rule_id`.
`rule_name`	string		Read-only; Expensive to use.
`listener_name`	string		Read-only; Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *DiscoveryRuleListenerModel*

Request

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

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

Get List of Rule-Listener Assignment

Request

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

Example Request

GET /api/v2/discovery/rule/listener`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/listener'
```

Response

```
{
    "result": "success",
    "rule_listener": [
        {
            "rule_id": "9115285645797883905",
            "listener_id": "9115285645797883906",
            "rule_name": "Rule_1",
            "listener_name": "RDP:bastion",
            "created_at": "2025-05-06 00:27:11.982267-07",
            "modified_at": "2025-05-06 00:27:11.982267-07"
        }
    ]
}
```

Get Rule-Listener Assignment by ID

Request

Method	`GET`
Path	`/api/v2/discovery/rule/<rule_id>/listener/<listener_id>`

Example Request

GET /api/v2/discovery/rule/<id>/listener/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883905/listener/
↪9115285645797883906'
```

Response

```
{
    "result": "success",
    "rule_listener": [
        {
            "rule_id": "9115285645797883905",
            "listener_id": "9115285645797883906",
            "rule_name": "Rule_1",
            "listener_name": "RDP:bastion",
            "created_at": "2025-05-06 00:27:11.982267-07",
            "modified_at": "2025-05-06 00:27:11.982267-07"
        }
    ]
}
```

Create Rule-Listener Assignment

Request

Method	`POST`
Path	`/api/v2/discovery/rule/listener`
Headers	`Content-Type: Application/json`
Body	`DiscoveryRuleListenerModel`

Example Request

POST /api/v2/discovery/rule/listener`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/rule/listener' \
  -d'{"rule_id":"9115285645797883906","listener_id":"9115285645797883906"}'
```

Response

```
{
    "result": "success",
    "rule": {
        "id": "9115285645797883906"
    }
}
```

Deleting Rule-Listener Assignment

Request

Method	`DELETE`
Path	`/api/v2/discovery/rule/<rule_id>/listener/<listener_id>`

Example Request

DELETE /api/v2/discovery/rule/<id>/listener/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883906/listener/
↪9115285645797883906'
```

Response

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

1.32.11 Discovery Rule-Pool Assignment

Data Structures

Table 85: `DiscoveryRulePoolModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Protected.
`rule_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `rule_id` with attribute `pool_id`.
`pool_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `pool_id` with attribute `rule_id`.
`rule_name`	string		Read-only; Expensive to use.
`pool_name`	string		Read-only; Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *DiscoveryRulePoolModel*

Request

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

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

Get List of Rule-Pool Assignment

Request

Method	GET
Path	/api/v2/discovery/rule/pool

Example Request

GET /api/v2/discovery/rule/pool`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/pool'
```

Response

```
{
    "result": "success",
    "rule_pool": [
        {
            "rule_id": "9115285645797883905",
            "pool_id": "9115285645797883906",
            "rule_name": "Rule_1",
            "pool_name": "RDP:bastion",
            "created_at": "2025-05-06 00:27:11.982267-07",
            "modified_at": "2025-05-06 00:27:11.982267-07"
        }
    ]
}
```

Get Rule-Pool Assignment by ID

Request

Method	GET
Path	/api/v2/discovery/rule/<rule_id>/pool/<pool_id>

Example Request

GET /api/v2/discovery/rule/<id>/pool/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883906/pool/
↪9115285645797883908'
```

Response

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

(continues on next page)

(continued from previous page)

```
    "rule_pool": {
        "rule_id": "9115285645797883906",
        "pool_id": "9115285645797883908",
        "rule_name": "Rule_2",
        "pool_name": "Pool_RDP",
        "created_at": "2025-05-06 02:34:44.062332-07",
        "modified_at": "2025-05-06 02:34:44.062332-07"
    }
}
```

Create Rule-Pool Assignment

Request

Method	`POST`
Path	`/api/v2/discovery/rule/pool`
Headers	`Content-Type: Application/json`
Body	`DiscoveryRulePoolModel`

Example Request

POST /api/v2/discovery/rule/pool`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/rule/pool' \
  -d'{"rule_id":"9115285645797883906","pool_id":"9115285645797883908"}'
```

Response

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

Deleting Rule-Pool Assignment

Request

Method	`DELETE`
Path	`/api/v2/discovery/rule/<rule_id>/pool/<pool_id>`

Example Request

DELETE /api/v2/discovery/rule/<id>/pool/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
```

(continues on next page)

(continued from previous page)

```
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883906/pool/
↪9115285645797883908'
```

Response

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

1.32.12 Discovery Rule-Safe Assignment

Data Structures

Table 86: `DiscoveryRuleSafeModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Protected.
`rule_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `rule_id` with attribute `safe_id`.
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `rule_id`. Requires `read` right on the `safe` object for GET, POST, and DELETE requests.
`rule_name`	string		Read-only; Expensive to use.
`safe_name`	string		Read-only; Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *DiscoveryRuleSafeModel*

Request

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

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

Get List of Rule-Safe Assignment

Request

Method	`GET`
Path	`/api/v2/discovery/rule/safe`

Example Request

GET /api/v2/discovery/rule/safe`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/safe'
```

Response


```
{
    "result": "success",
    "rule_safe": [
        {
            "rule_id": "9115285645797883905",
            "safe_id": "9115285645797883906",
            "rule_name": "Rule_1",
            "safe_name": "RDP",
            "created_at": "2025-05-06 00:27:11.974136-07",
            "modified_at": "2025-05-06 00:27:11.974136-07"
        }
    ]
}
```


Get Rule-Safe Assignment by ID

Request

Method	GET
Path	/api/v2/discovery/rule/<rule_id>/safe/<safe_id>

Example Request

GET /api/v2/discovery/rule/<id>/safe/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883906/safe/
↪9115285645797883906'
```

Response


```
{
    "result": "success",
    "rule_safe": {
        "rule_id": "9115285645797883906",
        "safe_id": "9115285645797883906",
        "rule_name": "Rule_2",
        "safe_name": "RDP",
        "created_at": "2025-05-06 02:45:22.811459-07",
        "modified_at": "2025-05-06 02:45:22.811459-07"
    }
}
```

Create Rule-Safe Assignment

Request

Method	POST
Path	/api/v2/discovery/rule/safe
Headers	Content-Type: Application/json
Body	DiscoveryRuleSafeModel

Example Request

POST /api/v2/discovery/rule/safe`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/rule/safe' \
  -d'{"rule_id":"9115285645797883906","safe_id":"9115285645797883906"}'
```

Response

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

Deleting Rule-Safe Assignment

Request

Method	DELETE
Path	/api/v2/discovery/rule/<rule_id>/safe/<safe_id>

Example Request

DELETE /api/v2/discovery/rule/<id>/safe/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/discovery/rule/9115285645797883906/safe/
↪9115285645797883906'
```

Response

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

1.32.13 Managing Discovery State

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

Warning

The following endpoints were deprecated and have been removed in Fudo Enterprise 6.2. Please update your integrations accordingly:

- `GET /api/v2/objspec/discovery`
- `PATCH /api/v2/account/<account_id>/discovery`
- `PATCH /api/v2/server/<server_id>/discovery`

To change the discovery state of servers or accounts, use `POST /api/v2/discovery/server/manage` or `POST /api/v2/discovery/account/manage`, described below.

Changing Multiple Server's Discovery State

Request

Method	`POST`
Path	`/api/v2/discovery/server/manage`

Example Request

POST /api/v2/discovery/server/manage`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/server/manage' \
  -d'{"servers":["9115285645797883913","1234567890123456790"],"state":"onboard",
↪"pools":["9115285645797883908"]}'
```

Response

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

Example Request

POST /api/v2/discovery/server/manage`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/server/manage' \
  -d'{"servers":["1234567890123456789","1234567890123456790"],"state":
↪"quarantine","reason":"Example text"}'
```

Response

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

Changing Multiple Account's Discovery State

Request

Method	POST
Path	/api/v2/discovery/account/manage

Example Request

POST /api/v2/discovery/account/manage`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/account/manage' \
  -d'{"accounts":["9115285645797883912","9115285645797883921"],"state":"onboard
↪","safes":["9115285645797883906","9115285645797883907"],"listeners":[
↪"9115285645797883906","9115285645797883905"]}'
```

Response

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

Example Request

POST /api/v2/discovery/account/manage`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/discovery/account/manage' \
  -d'{"accounts":["9115285645797883922","9115285645797883923"],"state":
↪"quarantine","reason":"Example text"}'
```

Response

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

1.33 Sessions

Fudo Enterprise stores all recorded servers access sessions, allowing to playback, review, delete and export to the supported video formats.

Sessions management allows filtering stored user sessions, accessing current users connections and downloading stored sessions. It also provides status information on each session and enables access to session sharing options.

1.33.1 Sessions Management

Data Structures

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

Table 87: `SessionsModel`

Attribute	Type	Description
`id`	string	Read-only. Uniqueness is required.
`leader_session_id`	string	Read-only.
`has_nested_sessions`	boolean	Read-only; expensive to use. Indicates whether the session has at least one nested session.
`is_nested_session`	boolean	Read-only; expensive to use. Indicates whether the session is a nested session.
`account_id`	string	Read-only. Account's Identifier, which was used for connection. Requires `read` right on object type `account` for all methods: `GET`, `PATCH`, and `DELETE`.
`listener_id`	string	Read-only. Listener's Identifier, which was used for connection.
`safe_id`	string	Read-only. Safe's Identifier, which was used for connection. Requires `read` right on object type `safe` for all methods: `GET`, `PATCH`, and `DELETE`.
`server_id`	string	Read-only. Server's Identifier, which was used for connection. Requires `read` right on object type `server` for all methods: `GET`, `PATCH`, and `DELETE`.
`user_id`	string	Read-only. User's Identifier, which was used for connection. Requires `read` right on object type `user` for all methods: `GET`, `PATCH`, and `DELETE`.
`started_at`	string	Read-only. Datetime of the session's start.

continues on next page

Table 87 – continued from previous page

Attribute	Type	Description
finished_at	string	Read-only. Datetime of the session's end.
handled_by	string	Read-only.
marked_safe_by	string	Read-only.
terminate_at	string	Datetime of the session's termination.
dump_mode	string	Read-only. Session recording options.
protocol	string {checkout, http, modbus, mysql, oracle, pgsql, rdp, ssh, tcp, tds, telnet, tn3270, tn5250, vnc}	Read-only. Protocol used 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
destination_address	string	Expensive. Concatenated destination IP and port.
paused	boolean	
retention_locked	boolean	
indexed	number	Session indexing status. Values: 0 = Waiting, 1 = Error, 2 = Indexed. Session is indexed when value is 2.
trusted_timestamp	string	Hidden. Base64 encoded timestamping signature.
size	number	
reason	string	Reason of the session's termination or rejection
status	string {approved, disconnected, expired, rejected, terminated, waiting, waiting_supervision}	
active_time	number	Returns null when the license disables productivity analysis.
ml (Machine Learning)	See the SessionsMLModel table	
pending_delete	boolean	
password_change	boolean	
checkout_forced	boolean	
created_at	datetime	Datetime of the record creation
modified_at	datetime	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
type	string	Session's type

continues on next page

Table 87 – continued from previous page

Attribute	Type	Description
`subsystem`	string	Read-only. Expensive to use. For example, `sftp`.
`user_name`	string	Expensive. User name who created session.
`user_removed`	boolean	Expensive. User is removed.
`user_organization`	string	Expensive. User organization who created session.
`account_name`	string	Expensive. Account name.
`account_removed`	boolean	Expensive. Account is removed.
`server_name`	string	Expensive. Server name.
`server_removed`	boolean	Expensive. Server is removed.
`safe_name`	string	Expensive. Safe name.
`safe_removed`	boolean	Expensive. Safe is removed.
`listener_name`	string	Expensive. Listener name.
`listener_removed`	boolean	Expensive. Listener is removed.
`listener_hidden`	boolean	Read-only. Expensive to use. Listener is hidden in UI (built-in or internal listener).
`secret_exposure_stat`	string {user_blocked, user_removed, user_lost_access, seen}	Expensive. State of user who checked out the current account password. Value 'seen' means that user has seen password and have access to it.
`ocr_enabled`	boolean	Read-only. Expensive. Indicates whether OCR was enabled for the session.
`ocrable`	boolean	Read-only. Expensive. Indicates whether the session is eligible for OCR processing.
`ocred`	boolean	Expensive. Indicates whether OCR has been completed for the session.
`ocr_progress`	number	Read-only. Expensive. Current progress of OCR processing.
`availability`	string {archived, available, downloading, missing}	Expensive. Session availability.
`created_on`	string	Expensive. The serial number of the node where the session was created.
`archived`	boolean	Read-only. Expensive. Session is fully replicated on archive node.
`duration`	number	Expensive. Session duration in seconds.
`activity`	number	Expensive. Session active time in percents. Returns `null` when the license disables productivity analysis.

continues on next page

Table 87 – continued from previous page

Attribute	Type	Description
`time_limit`	number	Expensive. Time in seconds remaining until the session is terminated. Value is available only when terminate_at defined. Value 0 means session is finished or terminated.
`unfinished_archive`	boolean	Read-only. Expensive to use. Indicates whether the session is not fully replicated on the archive node.
`query_text`	string	Read-only. Hidden. Used only for filters. Query text to search for.
`query_input`	boolean	Read-only. Hidden. Used only for filters. Indicates whether to search text in user input.
`query_output`	boolean	Read-only. Hidden. Used only for filters. Indicates whether to search text in output.
`query_comments`	boolean	Read-only. Hidden. Used only for filters. Indicates whether to search text in comments.
`websocket_url`	string	Read-only. Expensive to use. A part of the URL to the websocket that serves the data of this session.
`timestamp_status`	string {none, pending, completed}	Read-only. Expensive to use. Status of timestamping process.
`subprotocol`	string {checkout, http, http_rendered, modbus, mysql, pgsql, rdp, scp, sftp, ssh, ssh_command, tcp, tds, telnet, tn3270, tn5250, vnc, x11}	Read-only. Expensive to use. Session subprotocol.
`local`	boolean	Read-only. Expensive to use. Indicates that the session is running or has a replica on the current cluster node.
`replicated_on_nodes`	string-array	Read-only. Expensive to use. List of nodes that the session was fully replicated on.
`has_comments`	boolean	Read-only. Expensive to use. Indicates whether any comments have been added to the session.
`analysis_status`	string {live, finished, failed}	Read-only. Expensive to use. Status of live LLM session analysis. `null` when the session is not monitored.
`analysis_severity`	string {unknown, low, medium, high}	Read-only. Expensive to use. Current severity reported by live LLM session analysis. Value `unknown` marks a coverage gap: the latest batch could not be analyzed.

continues on next page

Table 87 – continued from previous page

Attribute	Type	Description
analysis_peak_severi	string {unknown, low, medium, high}	Read-only. Expensive to use. Peak severity reported by live LLM session analysis.
analysis_summary	string	Read-only. Expensive to use. Latest summary produced by live LLM session analysis.
analysis_verdict_cou	number	Read-only. Expensive to use. Number of verdicts produced by live LLM session analysis.
summary_status	string {unprocessed, pending, processing, succeeded, failed}	Read-only. Expensive to use. Current processing state of the ML summarizer.
summary_stage	string {transcript, summary}	Read-only. Expensive to use. Current processing stage of the ML summarizer.
summary_processed_ch	number	Read-only. Expensive to use. Number of chunks processed by the ML summarizer.
summary_total_chunks	number	Read-only. Expensive to use. Total number of chunks to be processed by the ML summarizer.
summary_eta	number	Read-only. Expensive to use. Estimated time remaining until the ML summarizer completes, in seconds.
key_risks_count	number	Read-only. Expensive to use. Number of key risks listed in the session summary.
can_play_session	boolean	Read-only. Expensive to use. Indicates whether the session can be played by the current user.
source	string {fsa, fsa_native, uag, uag_native, native}	Read-only. Source IP address

Table 88: 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

Retrieve Available Attributes of the *SessionsModel*

Request

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

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

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

Get Sessions List

Request

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

Example Request

GET /api/v2/session


```
    {
"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",
```


(continues on next page)

(continued from previous page)


```
    "modified_at": "2022-04-08 08:16:02.009606+02",
    "height": "768",
    "width": "1024"
}}
```


Get a Session by ID

Request

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

Example Request

GET /api/v2/session/<id>


```
    {
"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"
}}
```

Modify a Session

Request

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

Delete Session

Request

Method	DELETE
Path	/api/v2/session/<id>

Example Request

DELETE /api/v2/session/<id>

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/session/9124292845052624897'
```

Response

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

1.33.2 Sharing Sessions

Fudo Enterprise enables sharing given session with another user.

Data Structures

Table 89: `SessionShareModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`session_id`	string	yes	Immutable. ID of the session to share.
`user_id`	string		Read-only; hidden; expensive to use. Requires `session-view` right on object type `user` for `GET` and `POST` requests.
`key`	string		Read-only.
`valid_since`	datetime	yes	Immutable. Start date and time of the share validity period.
`valid_to`	datetime		Immutable. End date and time of the share validity period. Omit the attribute to keep the share valid until the session ends - allowed for running sessions only. Required for sessions that have already finished.
`readonly`	boolean	yes	Immutable. `true` - the recipient can only watch the session; `false` - the recipient can also interact with it.
`authenticated`	boolean	yes	Immutable; default value `true`. `true` - the recipient must be signed in and their identity is recorded in the access history; `false` - anonymous access with the key only.
`created_by`	string		Read-only. ID of the user who created the share.
`created_by_nam`	string		Read-only; expensive to use. Name of the user who created the share.
`created_vhost`	string		Read-only. Address the share was created on: `mgmt` or `uag`.
`link`	string		Read-only; expensive to use. Share session link without host prefix.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SessionShareModel*

Request

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

GET /api/v2/objspec/session_share

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_share'
```

Get Session Sharing Information

Request

Method	GET
Path	/api/v2/session/<session_id>/share

GET /api/v2/session/<session_id>/share

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.92.108/api/v2/session/4782822804267466753/share'
{
```

Response

```
{
    "result": "success",
    "session_share": [
        {
            "id": "6953557824660045826",
            "session_id": "4665729213955833860",
            "key":
↪"yKaOzVjAoPZ6Hga6ECFEoVD2yKJXrrcPTDvhYFeUYNfxJaLs8D1piZdhFLIxivcT",
            "valid_since": "2025-05-14 05:11:00-07",
            "valid_to": null,
            "readonly": false,
            "authenticated": true,
            "created_by": "6953557824660045827",
            "created_by_name": "user_1",
            "created_vhost": "uag",
            "link": "\/play\/4665729213955833860?
↪key=yKaOzVjAoPZ6Hga6ECFEoVD2yKJXrrcPTDvhYFeUYNfxJaLs8D1piZdhFLIxivcT",
            "created_at": "2025-05-14 05:11:20.443267-07",
            "modified_at": "2025-05-14 05:11:20.443267-07"
        },
        {
            "id": "6953557824660045827",
            "session_id": "4665729213955833860",
            "key":
↪"fEGWO92C3IDki0EaMgpbpOffRFYSNhg6gYa6jYMp2zyfcMtFpIKdMr20S1jGKD3t",
            "valid_since": "2025-05-14 05:16:00-07",
            "valid_to": "2025-05-14 13:16:00-07",
            "readonly": true,
            "authenticated": true,
            "created_by": "6953557824660045825",
            "created_by_name": "admin",
            "created_vhost": "mgmt",
            "link": "\/play\/4665729213955833860?
```

(continues on next page)

(continued from previous page)

```
↪key=fEGWO92C3IDki0EaMgpbpOffRFYSNhg6gYa6jYMp2zyfcMtFpIKdMr20S1jGKD3t",
            "created_at": "2025-05-14 05:18:11.152713-07",
            "modified_at": "2025-05-14 05:18:11.152713-07"
        }
    ]
}
```

Note

The first share in the example was created by a user in the User Access Gateway (`created_vhost`: `uag`). Such shares are always authenticated, always allow interaction with the session (`readonly`: `false`) and have no fixed end of validity (`valid_to`: `null`) - they expire when the session ends.

Share Session

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/share`
Headers	`Content-Type: Application/json`
Body	`SessionShareModel`

POST /api/v2/session/<session_id>/share

Example Request

```
curl -s -k -X POST \
     -H 'Authorization: <token>' \
         -H 'Content-Type: application/json' \
         -d '{"valid_since": "2025-05-15T13:07:00.000Z","valid_to": "2025-05-
↪15T21:07:00.000Z","readonly": true,"authenticated": true}' \
     'https://10.31.92.108/api/v2/session/4665729213955833860/share'
```

Response

```
{
    "result": "success",
    "session_share": {
        "key": "gHJNP5SWFx08lvecW82uotFfxZVYJzOqhIbusRR9q1HmFLF1C7rd5xv7BywSmeOQ
↪"
    }
}
```

Example Request - a share valid until the session ends

Omit `valid_to` to create a share that expires together with the session. The session must still be running.

```
curl -s -k -X POST \
     -H 'Authorization: <token>' \
         -H 'Content-Type: application/json' \
         -d '{"valid_since": "2025-05-15T13:07:00.000Z","readonly": false,
↪"authenticated": true}' \
     'https://10.31.92.108/api/v2/session/4665729213955833860/share'
```

If the session has already finished, the request is rejected.

```
{
    "result": "failure",
    "message": "Attribute valid_to must be defined for finished sessions.",
    "failing_attributes": [
        "valid_to"
    ]
}
```

Note

The `link` attribute returns a path without the host prefix. Prepend the management address or the User Access Gateway address, depending on which one the recipient can reach - both forms use the same key and open the same session.

1.33.3 Session Access History NEW

Fudo Enterprise records every connection made to a session through a share link. Each connection is a separate entry containing the viewer's identity, the address the link was opened on and the times the viewer started watching, started interacting and disconnected.

Entries are kept after the share link itself is deactivated, so the access history of a session remains complete.

Data Structures

Table 90: `SessionShareAccessModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`session_id`	string		Read-only. ID of the session that was accessed.
`session_share_`	string		Read-only. ID of the share link used to access the session.
`user_id`	string		Read-only. ID of the viewer; `null` for anonymous viewers.
`user_name`	string		Read-only; expensive to use. Name of the viewer; `null` for anonymous viewers.
`user_extra_id`	string		Read-only; hidden; expensive to use. Session owner; drives the `session-view` capability check on object type `user`.
`address`	string		Read-only. Source IP address of the viewer.
`vhost`	string		Read-only. Address the viewer opened the link on: `mgmt` or `uag`.
`started_at`	datetime		Read-only. When the viewer started watching the session.
`joined_at`	datetime		Read-only. When the viewer first interacted with the session; `null` for view-only access.
`finished_at`	datetime		Read-only. When the viewer disconnected; `null` while still connected.
`last_seen`	datetime		Read-only. Presence heartbeat of the connection.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SessionShareAccessModel*

Request

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

GET /api/v2/objspec/session_share_access

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_share_access'
```

Get the Access History of a Session

Returns every connection made to the session through any of its share links.

Request

Method	GET
Path	/api/v2/session/<session_id>/access

GET /api/v2/session/<session_id>/access

Note

The request requires the **session-read** and **session-share-view** privileges. The **user-session-view** privilege is sufficient on its own.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.92.108/api/v2/session/4665729213955833860/access'
```

Response

```
{
    "result": "success",
    "session_share_access": [
        {
            "id": "6953557824660045825",
            "session_id": "4665729213955833860",
            "session_share_id": "6953557824660045826",
            "user_id": "6953557824660045828",
            "user_name": "user_2",
            "address": "10.33.3.44",
            "vhost": "uag",
            "started_at": "2026-07-29 05:16:54.049977-07",
            "joined_at": "2026-07-29 05:17:31.112004-07",
            "finished_at": null
        },
        {
            "id": "6953557824660045826",
            "session_id": "4665729213955833860",
            "session_share_id": "6953557824660045827",
            "user_id": null,
            "user_name": null,
            "address": "10.33.3.51",
            "vhost": "mgmt",
            "started_at": "2026-07-29 05:20:02.311209-07",
            "joined_at": null,
            "finished_at": "2026-07-29 05:24:48.907712-07"
```

(continues on next page)

(continued from previous page)

```
        }
    ]
}
```

Note

The second entry in the example is an anonymous viewer - `user_id` and `user_name` are `null`, so the connection can be identified only by its source address. A `joined_at` value of `null` means the viewer only watched the session and never interacted with it.

Get the Access History of a Single Share Link

Returns the same entries, limited to one share link.

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/share/<session_share_id>/access`

GET /api/v2/session/<session_id>/share/<session_share_id>/access

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.92.108/api/v2/session/4665729213955833860/share/
↪6953557824660045826/access'
```

1.33.4 Revoking Sharing Sessions

Fudo Enterprise enables sharing given session with another user.

Data Structures

Table 91: `SessionShareRevokeModel`

Attribute	Type	Required	Description
`session_id`	string	yes	ID of the session to OCR. Immutable.
`key`	string		Unique key identifying the shared session URL. Read-only.

Retrieve Available Attributes of the *SessionShareRevokeModel*

Request

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

GET /api/v2/objspec/session_share_revoke

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_share_revoke'
```

Revoke Session Sharing URL

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/share/revoke`
Headers	`Content-Type: Application/json`
Body	`SessionShareRevokeModel`

POST /api/v2/session/<session_id>/share/revoke

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{"key":"yKaOzVjAoPZ6Hga6ECFEoVD2yKJXrrcPTDvhYFeUYNfxJaLs8D1piZdhFLIxivcT"}
↪' \
  'https://10.31.92.108/api/v2/session/4665729213955833860/share/revoke'
```

Response

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

1.33.5 Terminating Sessions

In case the administrator notices access rights misuse, Fudo Enterprise allows to terminate the live session.

Data Structures

Table 92: `SessionTerminateModel`

Attribute	Type	Required	Description
`session_id`	string	yes	ID of the session to terminate.

Retrieve Available Attributes of the *SessionTerminateModel*

Request

Method	GET
Path	/api/v2/objspec/session_terminate

GET /api/v2/objspec/session_terminate

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_terminate'
```

Terminate Live Session

Request

Method	POST
Path	/api/v2/session/<session_id>/terminate

POST /api/v2/session/<session_id>/terminate

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.92.108/api/v2/session/4665729213955833862/terminate'
```

Response

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

1.33.6 Session Text

Data Structures

Table 93: SessionTextModel

Attribute	Type	Required	Description
id	string		Read-only. Unique identifier.
session_id	string		Read-only. ID of the session the text is linked to.
text	string		Read-only. Recorded session text (searchable representation).
user_input	boolean		Read-only. Whether the text was entered by the user.
ms	number		Read-only. Millisecond offset in the session.
created_at	datetime		Read-only. Timestamp of creation.

continues on next page

Table 93 – continued from previous page

Attribute	Type	Required	Description
`created_on`	string		Read-only. Date of creation (UTC).
`modified_at`	datetime		Read-only. Timestamp of last modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SessionTextModel*

Request

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

GET /api/v2/objspec/session_text

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_text'
```

Get Recorded Text From Session

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/text`

GET /api/v2/session/<session_id>/text

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.31.116.195/api/v2/session/8169529724050079760/text
```

Response

```
{
    "result": "success",
    "session_text": [
        {
            "id": "8169529724050079766",
            "session_id": "8169529724050079746",
            "text": "'address':6 'enter':5 'firefox':9 'getting':7 'google':4
↪'new':1 'started':8 'tab':2 'with':3",
            "user_input": false,
            "ms": 1425,
```

(continues on next page)

(continued from previous page)


```
            "created_at": "2025-07-11 03:09:11.304285-07",
            "created_on": "80434736",
            "modified_at": "2025-07-11 03:09:11.304285-07"
        },
        {
            "id": "8169529724050079767",
            "session_id": "8169529724050079746",
            "text": "'correction':1",
            "user_input": false,
            "ms": 1944,
            "created_at": "2025-07-11 03:09:15.284903-07",
            "created_on": "80434736",
            "modified_at": "2025-07-11 03:09:15.284903-07"
        },
        {
            "id": "8169529724050079768",
            "session_id": "8169529724050079746",
            "text": "'search':1",
            "user_input": false,
            "ms": 1973,
            "created_at": "2025-07-11 03:09:18.277803-07",
            "created_on": "80434736",
            "modified_at": "2025-07-11 03:09:18.277803-07"
        }
    ]
}
```


Note

This endpoint returns terminal text captured during the session, including user input and output, if applicable. Useful for text-based audit and search operations.

1.33.7 Session OCR

Recorded RDP, VNC and rendered HTTP sessions can be processed and indexed for full-text search purposes.

Data Structures

Table 94: `SessionOCRModel`

Attribute	Type	Required	Description
`id`	string		Unique, read only object identifier.
`session_id`	string		ID of the session to OCR. Immutable.
`on_node`	string		Shows whether the session has been replicated across nodes, identified by serial numbers. Default value: `current_setting('fudo.serial', true)`
`ocred`	boolean		Read-only. Indicates whether session texts have been OCR-processed.
`lang`	string	yes	Specify OCR languages using `+` as a separator (e.g., `eng+deu+pol`).
`priority`	number	yes	
`created_on`	datetime		Read-only.
`created_at`	datetime		Read-only.
`modified_at`	datetime		Read-only.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SessionOCRModel*

Request

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

GET /api/v2/objspec/session_ocr

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_ocr'
```

Check Session OCR Status

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/ocr`

GET /api/v2/session/<session_id>/ocr

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
```

(continues on next page)

(continued from previous page)

```
  'https://10.31.92.108/api/v2/session/4782822804267466753/ocr'
{
```

Response


```
{
    "result": "success",
    "session_ocr": [
        {
            "id": "4665729213955833858",
            "session_id": "4665729213955833858",
            "on_node": "83329531",
            "ocred": true,
            "lang": "eng+deu+pol",
            "priority": 1,
            "created_on": "83329531",
            "created_at": "2025-05-14 03:22:32.367319-07",
            "modified_at": "2025-05-14 03:24:58.1089-07"
        }
    ]
}
```


Process Session for OCR

Note

- The list of available OCR language codes can be retrieved using the internal API endpoint `GET /api/v2/internal/ocr_lang`.
- The response contains language identifiers (`value`) and their human-readable names (`label`), which should be used when configuring OCR-based session analysis.

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/ocr`
Headers	`Content-Type: Application/json`
Body	`SessionOCRModel`

POST /api/v2/session/<session_id>/ocr

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{"lang": "eng+deu+pol","priority":1}' \
  'https://10.31.92.108/api/v2/session/4665729213955833858/ocr'
```

Response

```
{
    "result": "success",
    "session_ocr": {
        "id": "4665729213955833858"
    }
}
```

1.33.8 Session Comment

Data Structures

Table 95: `SessionCommentModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique.
`parent_id`	string		Immutable.
`session_id`	string	yes	ID of the session to comment. Immutable.
`text`	string	yes	Text content of the session comment.
`start_at`	datetime	yes	Value format: time. Expensive to use.
`finish_at`	datetime	yes	Value format: time. Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`modified_by`	string		Read-only.
`modified_by_na`	string		Read-only. Expensive to use.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *SessionCommentModel*

Request

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

GET /api/v2/objspec/session_comment

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_comment'
```

Get Session Comments

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/comment`

GET /api/v2/session/<session_id>/comment

Example Request

```
curl -s -k -X GET \
     -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
     'https://10.31.92.108/api/v2/session/8169529724050079753/comment'
```

Response


```
{
    "result": "success",
    "session_comment": [
        {
            "id": "8169529724050079745",
            "session_id": "8169529724050079753",
            "text": "Comment no 1",
            "start_at": "00:00:14",
            "finish_at": "00:00:15",
            "created_at": "2025-07-08 14:19:29.001496-07",
            "modified_at": "2025-07-08 14:19:29.001496-07",
            "modified_by": "8169529724050079745",
            "modified_by_name": "admin"
        },
        {
            "id": "8169529724050079746",
            "session_id": "8169529724050079753",
            "text": "Comment no 2",
            "start_at": "00:00:26",
            "finish_at": "00:00:27",
            "created_at": "2025-07-08 14:19:57.31709-07",
            "modified_at": "2025-07-08 14:19:57.31709-07",
            "modified_by": "8169529724050079745",
            "modified_by_name": "admin"
        }
    ]
}
```


Get Session Comment by ID

Request

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

GET /api/v2/session/<session_id>/comment/<id>

Example Request

```
curl -s -k -X GET \
     -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
```

(continues on next page)

(continued from previous page)

```
    'https://10.31.92.108/api/v2/session/8169529724050079753/comment/
↪8169529724050079746'
```

Response

```
{
    "result": "success",
    "session_comment": [
        {
            "id": "8169529724050079746",
            "session_id": "8169529724050079753",
            "text": "Comment no 2",
            "start_at": "00:00:26",
            "finish_at": "00:00:27",
            "created_at": "2025-07-08 14:19:57.31709-07",
            "modified_at": "2025-07-08 14:19:57.31709-07",
            "modified_by": "8169529724050079745",
            "modified_by_name": "admin"
        }
    ]
}
```

Add Session Comment

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/comment`
Headers	`Content-Type: Application/json`
Body	`SessionCommentModel`

POST /api/v2/session/<session_id>/comment

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.92.108/api/v2/session/4665729213955833865/comment \
  -d '{"text": "Text content of the session comment.","start_at":"00:01:00",
↪"finish_at":"00:01:00"}'
```

Response

```
{
    "result": "success",
    "session_comment": {
        "id": "4665729213955833859"
    }
}
```

Modify Session Comment

Request

Method	PATCH
Path	/api/v2/session/<session_id>/comment/<id>
Headers	Content-Type: Application/json
Body	SessionCommentModel

PATCH /api/v2/session/<session_id>/comment/<id>

Example Request

```
curl -s -k -X PATCH \
     -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
         -H 'Content-Type: application/json' \
         https://10.31.92.108/api/v2/session/8169529724050079753/comment/
↪8169529724050079746 \
         -d '{"text": "Changed session comment content.","start_at":"00:01:00",
↪"finish_at":"00:01:00"}'
```

Response

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

Delete Session Comment

Request

Method	DELETE
Path	/api/v2/session/<session_id>/comment/<id>

DELETE /api/v2/session/<session_id>/comment/<id>

Example Request

```
curl -s -k -X DELETE \
     -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
     'https://10.31.92.108/api/v2/session/8169529724050079753/comment/
↪8169529724050079746'
```

Response

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

1.33.9 Sessions Approval

> **Note**
>
> To allow users to accept or reject access requests, the Safe must have the `require_confirmation` attribute set to `true`. This setting enables the approval workflow for access requests.

Data Structures

Approve Object Specification

Table 96: `SessionApproveModel`

Attribute	Type	Required	Description
`session_id`	string	yes	ID of the session to approve.

Retrieve Available Attributes of the *SessionApproveModel*

Request

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

GET /api/v2/objspec/session_approve

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_approve'
```

Reject Object Specification

Table 97: `SessionRejectModel`

Attribute	Type	Required	Description
`session_id`	string	yes	ID of the session to reject.
`reason`	string	yes	The reason why the session is rejected.
`block_user`	boolean; default value `false`		Indicates whether to block the user who established the session.

Retrieve Available Attributes of the *SessionRejectModel*

Request

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

GET /api/v2/objspec/session_reject

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_reject'
```

Approving Session

Request

Method	POST
Path	/api/v2/session/<session_id>/approve

POST /api/v2/session/<session_id>/approve

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.92.108/api/v2/session/4665729213955833862/approve'
```

Response

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

Rejecting Session

Request

Method	POST
Path	/api/v2/session/<session_id>/reject

POST /api/v2/session/<session_id>/reject

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.92.108/api/v2/session/4665729213955833862/reject \
  -d '{"reason": "CODE 1.12", "block_user":true}'
```

Response

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

1.33.10 Restoring Session

If a session's backup version is stored outside of Fudo Enterprise, it can be downloaded to the local Fudo Enterprise instance using the **Restore** option.

Data Structures

Table 98: `SessionRestoreModel`

Attribute	Type	Required	Description
`session_id`	string	yes	Immutable. ID of the session to restore.

Retrieve Available Attributes of the *SessionRestoreModel*

Request

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

GET /api/v2/objspec/session_restore

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_restore'
```

Restoring Session

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/restore`

POST /api/v2/session/<session_id>/restore

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.31.116.195/api/v2/session/8169529724050079760/restore
```

Response

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

1.33.11 Session Last Activity

Data Structures

Table 99: `SessionActivityModel`

Attribute	Type	Required	Description
`session_id`	string	yes	ID of the session. Read-only.
`last_activity_`	number		Indicates how many seconds have passed since the session's last activity. Read-only.
`last_activity_`	string		The absolute timestamp of the session's last activity, formatted according to RFC 3339.
`unavailable`	boolean	yes	Indicates whether the session's last activity time is unavailable—either because the session has ended or is running on a different node. Read-only.

Retrieve Available Attributes of the *SessionActivityModel*

Request

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

GET /api/v2/objspec/session_terminate

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_terminate'
```

Get Get Session Last Activity

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/last_activity`

GET /api/v2/session/<session_id>/last_activity

Example Request

```
curl -s -k -X GET \
     -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
     'https://10.31.92.108/api/v2/session/4665729213955833864/last_activity'
```

Response

```
{
    "last_activity_age": 6,
    "last_activity_at": "2025-05-14T13:32:43.819802+00:00",
    "unavailable": false,
    "result": "success"
}
```


Response if the session has ended


```
{
    "last_activity_age": null,
    "last_activity_at": null,
    "unavailable": true,
    "result": "success"
}
```


1.33.12 Session Data Replication

Additionally to automated session data replication, Fudo Enterprise enables on-demand replication to Fudo Enterprise instances to which the given data is not replicated automatically.

Data Structures

Table 100: `SessionReplicaModel`

Attribute	Type	Required	Description
`id`	string	Read-only. Unique identifier. Protected.	
`session_on`	string	yes	Serial number of the node on which the session has been replicated. The value `archive` indicates that the session is stored as a backup. Immutable. Uniqueness is required in the combination of attribute `session_on` with attribute `session_id`.
`session_id`	string	yes	ID of the session. Immutable. Uniqueness is required in the combination of attribute `session_id` with attribute `session_on`.
`fully_replicat`	boolean; default value `false`	yes	Read-only.
`backup_id`	string		Backup ID, available when the `session_on` attribute is set to `archive`. Read-only.
`dump_directory`	string		Read-only. Protected.
`external_direc`	string		Directory where session backup has been saved. Read-only. Expensive to use.
`node_name`	string		Name of the node on which the session has been replicated. Read-only. Expensive to use.
`backup_name`	string		Read-only. Expensive to use.
`created_at`	datetime	Datetime of the record creation. Read-only.	
`modified_at`	datetime	Datetime of the record modification. Read-only.	
`removed`	boolean	Read-only.	

Retrieve Available Attributes of the *SessionReplicaModel*

Request

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

GET /api/v2/objspec/session_replica

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_replica'
```

Get Session Replication Details

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/replica`

GET /api/v2/session/<session_id>/replica

Example Request

```
curl -s -k -X GET \
     -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
     'https://10.31.92.108/api/v2/session/4665729213955833864/replica'
```

Response

```
{
    "result": "success",
    "session_replica": [
        {
            "session_on": "83329531",
            "session_id": "4665729213955833864",
            "fully_replicated": true,
            "created_at": "2025-05-14 06:32:04.355502-07",
            "modified_at": "2025-05-14 06:32:04.355502-07"
        }
    ]
}
```

Process Session Replication

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/replica`
Headers	`Content-Type: Application/json`
Body	`SessionReplicaModel`

POST /api/v2/session/<session_id>/replica

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"session_on": "83329531"}' \
  'https://10.31.92.108/api/v2/session/4665729213955833858/replica'
```

Response

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

1.33.13 Session Timestamping

Note

To timestamp sessions, first you have to enable and configure the timestamping feature. Go to **Settings** > **System** > **Timestamping**. For more information refer to the Timestamping section of the Fudo Enterprise Documentation.

Data Structures: *SessionTimestampModel*

Table 101: `SessionTimestampModel`

Attribute	Type	Required	Description
`session_id`	string	yes	Immutable. ID of the session to timestamp.
`trusted_timest`	string		Read-only. Timestamp details for the session.

Retrieve Available Attributes of the *SessionTimestampModel*

Request

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

GET /api/v2/objspec/session_timestamp

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_timestamp'
```

Data Structures: *TimestampModel*

Table 102: `TimestampModel`

Attribute	Type	Required	Description
`enabled`	boolean		Indicates whether timestamping is enabled.
`provider`	string{`certum kir`, `pwpw`}		
`pkcs12`	string		PKCS12 file. Protected. Requires `pkcs12_passphrase` attribute.
`pkcs12_passphr`	string	Required by `pkcs12`	Passphrase to use to decrypt PKCS12 file. Protected.
`certificate`	string		Timestamp certificate. Read-only.
`expire_after`	string		Timestamp certificate expiration datetime. Format RFC3339. Read-only.

Retrieve Available Attributes of the *TimestampModel*

Request

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

GET /api/v2/objspec/timestamping

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/timestamping'
```

Get Session Timestamping Details

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/timestamp`

GET /api/v2/session/<session_id>/timestamp

Example Request

```
curl -s -k -X GET \
     -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
     'https://10.31.92.108/api/v2/session/4665729213955833864/timestamp'
```

Response: Session without timestamp

```
{
    "result": "failure",
    "message": "The session does not have a trusted timestamp."
}
```

Response: Timestamped session

```

```

Timestamp Session

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/timestamp`
Headers	`Content-Type: Application/json`
Body	`SessionTimestampModel`

POST /api/v2/session/<session_id>/timestamp

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.31.92.108/api/v2/session/4665729213955833858/timestamp'
```

Response: Timestamping not configured

```
{
    "result": "failure",
    "message": "Sessions timestamping is disabled."
}
```

Response: Timestamping configured

```
{
    "result": "failure",
    "message": "Sessions timestamping is disabled."
}
```

Delete Session Timestamping

Request

Method	DELETE
Path	/api/v2/session/<session_id>/timestamp

DELETE /api/v2/session/<session_id>/timestamp

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/session/4665729213955833858/timestamp'
```

Response

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

1.33.14 Session Download

Request

Method	POST
Path	/api/v2/session/<session_id>/download
Headers	Content-Type: Application/json
Body	SessionDownloadModel

POST /api/v2/session/<session_id>/download

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.92.108/api/v2/session/4665729213955833865/download \
  -d '{"format": "divx5", "resolution": "hd720"}'
```

Response

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

Note

To check available download formats for session recordings, you can use the following internal endpoint: GET /api/v2/internal/session/<session_id>/download_formats. Please note that this is an **internal endpoint**, and its availability and behavior are **not guaranteed to remain stable** across future versions of the API.

1.33.15 Session Backup

Data Structures

Table 103: `SessionBackupModel`

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: {}`.

Retrieve Available Attributes of the *SessionBackupModel*

Request

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

GET /api/v2/objspec/session_backup

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/session_backup'
```

Mark Existing Session for Back Up

Request

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

Example Request

POST /api/v2/session/<session_id>/backup/<backup_id>

Request

Method	`POST`
Path	`/api/v2/session_backup`
Headers	`Content-Type: Application/json`
Body	`SessionBackupModel`

Example Request

PATCH /api/v2/session_backup

```
{
"backup_name": "Backup_Target_Name",
"session_ids": [
        "23456789012345678 90",
        "23456789012345678 91"
]
}
```

Response

```
{
"result": "success",
"session_ids": [
        "23456789012345678 90",
        "23456789012345678 91"
        ]
}
```

1.33.16 Session SCP File

Data Structures

Table 104: `ScpFileModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique identifier.
`session_id`	string		Read-only. Identifier of the session to which the file transfer belongs.
`filename`	string		Read-only. Name of the file.
`file_size`	number		Read-only. Size of the file, in bytes.
`file_origin`	string		Read-only. Origin of the file. Can be either `client` or `server`.
`current_node`	string		Read-only. Indicates if the file is available on the current node.
`created_at`	datetime		Read-only. Timestamp of file registration.

Retrieve Available Attributes of the *ScpFileModel*

Request

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

GET /api/v2/objspec/scp_file

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/scp_file'
```

Get SCP File Transfer List for a Session

Request

Method	GET
Path	/api/v2/session/<session_id>/scp_file

GET /api/v2/session/<session_id>/scp_file

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/session/8673932882315575319/scp_file'
```

Response

```
{
    "scp_file": [
        {
            "id": "0",
            "session_id": "8673932882315575319",
            "filename": "export_import_configuration.txt",
            "file_size": 307175,
            "file_origin": "client",
            "current_node": true,
            "created_at": "2025-07-19 09:26:33.605208-07"
        }
    ],
    "result": "success"
}
```

Download SCP File Content by Session and File ID

Request

Method	GET
Path	/api/v2/session/<session_id>/scp_file/<id>

GET /api/v2/session/<session_id>/scp_file/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/session/8673932882315575319/scp_file/0'
```

Response

```
SCP file content.
```

Note

The endpoint returns raw file content. The response body contains the plain contents of the file identified by file `<id>`.

1.34 Session Summary

1.34.1 Data Structures

Table 105: `SessionSummaryModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Protected. Uniqueness is required.
`session_id`	string	yes	ID of the session this summary is related to. Uniqueness is required.
`status`	string {pending, processing, succeeded, unprocessed, failed}; Default value `pending`		Read-only. Current processing state of the ML summarizer.
`stage`	string {transcript, summary}		Read-only. Current processing stage of the ML summarizer.
`eta`	number		Read-only. Estimated time remaining until completion, in seconds.
`processed_chun`	number		Read-only. Number of chunks processed by the ML summarizer.
`total_chunks`	number		Read-only. Total number of chunks to be processed.
`summary`	string		Read-only. Summary of the session generated by the ML summarizer.
`key_risks`	object-array		Read-only. List of key risks identified in the session.
`provider_model`	string		Read-only. AI Model used in session summary generation.
`provider_name`	string		Read-only. AI provider used in session summary generation.
`provider_url`	string		Read-only. AI provider URL used in session summary generation.
`generated_at`	datetime		Read-only. Timestamp of summary generation.
`user_id`	string		Read-only; hidden; expensive to use. Virtual property, used just to filter out sessions that are not granted to the user. Requires `session-view` right on object type `user` for `GET` and `POST` requests.
`requested_by_i`	string		Read-only. User ID who generated the session summary.
`requested_by_n`	string		Read-only; expensive to use. User name who generated the session summary.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.34.2 Retrieve Available Attributes of the *SessionSummaryModel*

Request

Method	GET
Path	/api/v2/objspec/session_summary

GET /api/v2/objspec/session_summary

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.30.41.207/api/v2/objspec/session_summary'
```

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

Note

The `session_summary` object is used to track AI-generated session summaries and their processing status. The ML summarizer processes sessions in chunks and provides progress tracking through the `eta`, `processed_chunks`, and `total_chunks` fields.

1.34.3 List Session Summaries

Request

Method	GET
Path	/api/v2/session/summary

GET /api/v2/session/summary

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.30.41.207/api/v2/session/summary'
```

Response

```
{
    "result": "success",
    "session_summary": [
        {
            "session_id": "4935945191598063650",
            "status": "succeeded",
            "stage": "transcript",
            "eta": 0,
            "processed_chunks": 1,
```

(continues on next page)

(continued from previous page)


```
            "total_chunks": 1,
            "summary": "No risky activity was detected during the session.",
            "key_risks": [],
            "provider_model": "gpt-5-nano-2025-08-07",
            "provider_name": "openai",
            "provider_url": "https://api.openai.com/v1/chat/completions",
            "generated_at": "2026-04-17 14:55:06.419273+02",
            "requested_by_id": "1666331862127083521",
            "requested_by_name": "admin",
            "created_at": "2026-04-17 14:55:02.442244+02",
            "modified_at": "2026-04-17 14:55:06.419441+02"
        }
    ]
}
```


1.34.4 Get Session Summary by Session ID

Request

Method	GET
Path	/api/v2/session/<session_id>/summary

GET /api/v2/session/<session_id>/summary

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.30.41.207/api/v2/session/4935945191598063650/summary'
```

Response


```
{
    "result": "success",
    "session_summary": {
        "session_id": "4935945191598063650",
        "status": "succeeded",
        "stage": "transcript",
        "eta": 0,
        "processed_chunks": 1,
        "total_chunks": 1,
        "summary": "No risky activity was detected during the session.",
        "key_risks": [],
        "provider_model": "gpt-5-nano-2025-08-07",
        "provider_name": "openai",
        "provider_url": "https://api.openai.com/v1/chat/completions",
        "generated_at": "2026-04-17 14:55:06.419273+02",
        "requested_by_id": "1666331862127083521",
        "requested_by_name": "admin",
```


(continues on next page)

(continued from previous page)

```
        "created_at": "2026-04-17 14:55:02.442244+02",
        "modified_at": "2026-04-17 14:55:06.419441+02"
    }
}
```

1.34.5 Get Session Transcript for Summary

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/summary/transcript`

GET /api/v2/session/<session_id>/summary/transcript

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.30.41.207/api/v2/session/4935945191598063650/summary/transcript'
```

Response

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

Note

This endpoint returns the processed transcript that was used as input for the AI summarizer. The transcript is extracted and formatted specifically for ML processing.

1.34.6 Request Session Summary Generation

Request

Method	`POST`
Path	`/api/v2/session/summary`
Body	JSON object with session parameters

POST /api/v2/session/summary

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
```

(continues on next page)

(continued from previous page)

```
    "session_id": "4935945191598063650"
  }' \
  'https://10.30.41.207/api/v2/session/summary'
```

Response


```
{
    "result": "success",
    "session_summary": {
        "session_id": "4935945191598063650",
        "status": "succeeded",
        "stage": "transcript",
        "eta": 0,
        "processed_chunks": 1,
        "total_chunks": 1,
        "summary": "No risky activity was detected during the session.",
        "key_risks": [],
        "provider_model": "gpt-5-nano-2025-08-07",
        "provider_name": "openai",
        "provider_url": "https://api.openai.com/v1/chat/completions",
        "generated_at": "2026-04-17 14:55:06.419273+02",
        "requested_by_id": "1666331862127083521",
        "requested_by_name": "admin",
        "created_at": "2026-04-17 14:55:02.442244+02",
        "modified_at": "2026-04-17 14:55:06.419441+02"
    }
}
```


Note

This endpoint initiates the AI-powered session summary generation process. The ML summarizer will process the session data in the background, and you can monitor progress using the `status`, `eta`, and chunk progress fields.

Warning

Session summary generation requires:

- Valid session ID with accessible session data
- Configured AI provider (OpenAI, Azure OpenAI, etc.)
- Sufficient system resources for ML processing
- Appropriate permissions to view the session

1.35 Session Commands

Note

Session command endpoints provide access to commands executed during user sessions. This includes sudo commands, shell commands, and other executed operations that were captured and logged by the system during monitored sessions.

1.35.1 Data Structures

Table 106: `SessionCommandModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique command identifier.
`session_id`	string		Read-only. ID of the session this command belongs to.
`occurred_at`	datetime		Read-only. Timestamp when the command was executed.
`command`	string		Read-only. The actual command that was executed.
`runas_user`	string		Read-only. User the command was executed as (for sudo commands).
`runas_group`	string		Read-only. Group the command was executed as (for sudo commands).
`policy_id`	string		Read-only. ID of the policy that was applied to this command.
`regexp_id`	string		Read-only. ID of the regex pattern that matched this command.
`approved`	boolean		Read-only. Expensive to use. Whether the command was approved by policy.
`user_id`	string		Read-only. Hidden. Expensive to use. User ID for permission filtering.
`created_at`	datetime		Read-only. Record creation timestamp.
`modified_at`	datetime		Read-only. Last modification timestamp.
`removed`	boolean		Read-only. Soft delete flag.

1.35.2 Retrieve Available Attributes of the *SessionCommandModel*

Request

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

GET /api/v2/objspec/session_command

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/objspec/session_command'
```

1.35.3 List Session Commands

Retrieve all commands executed during a specific session.

Request

Method	GET
Path	/api/v2/session/<session_id>/command

GET /api/v2/session/<session_id>/command

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/session/5980780305148018689/command'
```

Response (With Commands)

```
{
    "result": "success",
    "session_command": [
        {
            "id": "5980780305148018703",
            "session_id": "5980780305148018739",
            "occurred_at": "2026-06-09 01:09:15.639699-07",
            "command": "\/usr\/bin\/id",
            "runas_user": "testuser1",
            "runas_group": "testuser1",
            "policy_id": "5980780305148018689",
            "regexp_id": "5980780305148018689",
            "approved": true,
            "created_at": "2026-06-09 01:09:15.641225-07",
            "modified_at": "2026-06-09 01:09:15.641225-07"
        },
        {
            "id": "5980780305148018705",
            "session_id": "5980780305148018739",
            "occurred_at": "2026-06-09 01:09:31.990782-07",
            "command": "\/usr\/bin\/id",
            "runas_user": "root",
            "runas_group": "root",
            "policy_id": "5980780305148018689",
            "regexp_id": "5980780305148018689",
            "approved": true,
```

(continues on next page)

(continued from previous page)

```
            "created_at": "2026-06-09 01:09:31.992218-07",
            "modified_at": "2026-06-09 01:09:31.992218-07"
        }
    ]
}
```

1.35.4 Get Specific Session Command

Retrieve details of a specific command executed during a session.

Request

Method	GET
Path	/api/v2/session/<session_id>/command/<id>

GET /api/v2/session/<session_id>/command/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/session/5980780305148018689/command/
↪5980780305148018703'
```

Success Response

```
{
    "result": "success",
    "session_command": [
        {
            "id": "5980780305148018703",
            "session_id": "5980780305148018689",
            "occurred_at": "2026-06-09 01:09:15.639699-07",
            "command": "\/usr\/bin\/id",
            "runas_user": "testuser1",
            "runas_group": "testuser1",
            "policy_id": "5980780305148018689",
            "regexp_id": "5980780305148018689",
            "approved": true,
            "created_at": "2026-06-09 01:09:15.641225-07",
            "modified_at": "2026-06-09 01:09:15.641225-07"
        }
    ]
}
```

1.36 AI Session Analysis Agents NEW

An analysis agent is a named prompt that a large language model applies to live session traffic. Each agent runs on an LLM provider and is attached to the safes whose sessions it should watch. While a session runs, its agents store verdicts describing what they found.

> **Note**
>
> Live session analysis must be switched on globally before any agent runs, and agents only start on sessions established after it was enabled.

1.36.1 Data Structures

Table 107: `AnalysisAgentModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`name`	string	yes	Agent name. Case-insensitive. Uniqueness is required.
`description`	string		One-line summary of what this agent looks for. May be empty.
`system_prompt`	string	yes	The agent's system prompt, combined with the system-owned verdict contract into the analyzer prompt. At most 4000 characters.
`provider_id`	string		LLM provider this agent runs on. An agent without one does not run.
`provider_name`	string		Read-only; expensive to use. Name of the attached LLM provider.
`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.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 108: `SafeAnalysisAgentModel`

Attribute	Type	Required	Description
`id`	string		Read-only; protected.
`safe_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `safe_id` with attribute `agent_id`. Requires `read` right on the `safe` object for `GET`, and `modify` for `POST` and `DELETE`.
`agent_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `agent_id` with attribute `safe_id`.
`safe_name`	string		Read-only; expensive to use.
`agent_name`	string		Read-only; expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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 109: `LiveAnalysisEnableModel`

Attribute	Type	Required	Description
`enabled`	boolean; default value `false`	yes	Live session analysis is enabled. New sessions are monitored while this is on; sessions already running are unaffected by changes.

1.36.2 Retrieve Available Attributes

Request

Method	`GET`
Path	`/api/v2/objspec/analysis_agent`, `/api/v2/objspec/safe_analysis_agent`, `/api/v2/objspec/live_analysis_enable`

GET /api/v2/objspec/analysis_agent

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/objspec/analysis_agent'
```

1.36.3 List Analysis Agents

Request

Method	GET
Path	/api/v2/analysis_agent

GET /api/v2/analysis_agent

Fudo Enterprise ships with built-in agents, reported with `builtin` set to `true`.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/analysis_agent'
```

Response


```
{
    "result": "success",
    "analysis_agent": [
        {
            "id": "2",
            "name": "Privilege escalation",
            "description": "Detects attempts to gain elevated privileges.",
            "system_prompt": "You are watching a live SSH session solely for␣
↪privilege escalation: sudo and su misuse, setuid binaries, kernel or service␣
↪exploits, credential harvesting from files or memory, capability abuse and␣
↪container escapes, and changes to accounts, groups, or authentication␣
↪configuration.",
            "builtin": true,
            "hidden": false,
            "created_at": "2026-08-14 07:29:06.256735-07",
            "modified_at": "2026-08-14 07:29:06.256735-07"
        }
    ]
}
```


Note

The `system_prompt` of the built-in agents is abbreviated in this example.

1.36.4 Get an Analysis Agent

Request

Method	GET
Path	/api/v2/analysis_agent/<id>

GET /api/v2/analysis_agent/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/analysis_agent/4638707616191610881'
```

Response


```
{
    "result": "success",
    "analysis_agent": {
        "id": "4638707616191610881",
        "name": "Database exfiltration",
        "description": "Detects bulk reads from production databases.",
        "system_prompt": "You are watching a live session solely for bulk␣
↪extraction of data from production databases: unbounded SELECTs, dumps to␣
↪local files, and transfers of result sets off the host. Severity: routine␣
↪queries consistent with the session context are low; large unfiltered reads␣
↪are medium; a dump written out or transferred off the host is high.",
        "provider_id": "4638707616191610881",
        "provider_name": "Local Ollama",
        "builtin": false,
        "hidden": false,
        "created_at": "2026-08-18 02:21:19.074407-07",
        "modified_at": "2026-08-18 02:21:19.074407-07"
    }
}
```


1.36.5 Create an Analysis Agent

Request

Method	POST
Path	/api/v2/analysis_agent
Body	AnalysisAgentModel

POST /api/v2/analysis_agent

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"name":"Database exfiltration","description":"Detects bulk reads from␣
↪production databases.","system_prompt":"You are watching a live session␣
↪solely for bulk extraction of data from production databases: unbounded␣
↪SELECTs, dumps to local files, and transfers of result sets off the host.",
↪"provider_id":"4638707616191610881"}' \
  'https://10.33.3.191/api/v2/analysis_agent'
```

Response

```
{
    "result": "success",
    "analysis_agent": {
        "id": "4638707616191610881"
    }
}
```


1.36.6 Modify an Analysis Agent

Request

Method	PATCH
Path	/api/v2/analysis_agent/<id>
Body	AnalysisAgentModel

PATCH /api/v2/analysis_agent/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"description":"Detects bulk reads from production databases and dumps␣
↪taken off the host."}' \
  'https://10.33.3.191/api/v2/analysis_agent/4638707616191610881'
```

Response


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


1.36.7 Delete an Analysis Agent

Request

Method	DELETE
Path	/api/v2/analysis_agent/<id>

DELETE /api/v2/analysis_agent/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/analysis_agent/4638707616191610881'
```

Response

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

1.36.8 List Safe Assignments

Request

Method	GET
Path	/api/v2/safe/analysis_agent

GET /api/v2/safe/analysis_agent

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/safe/analysis_agent'
```

Response

```
{
    "result": "success",
    "safe_analysis_agent": [
        {
            "safe_id": "4638707616191610881",
            "agent_id": "1",
            "safe_name": "main",
            "agent_name": "SSH security",
            "created_at": "2026-08-18 02:19:24.161485-07",
            "modified_at": "2026-08-18 02:19:24.161485-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```

1.36.9 Get a Safe Assignment

Request

Method	GET
Path	/api/v2/safe/<safe_id>/analysis_agent/<agent_id>

GET /api/v2/safe/<safe_id>/analysis_agent/<agent_id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/safe/4638707616191610881/analysis_agent/1'
```

Response


```
{
    "result": "success",
    "safe_analysis_agent": {
        "safe_id": "4638707616191610881",
        "agent_id": "1",
        "safe_name": "main",
        "agent_name": "SSH security",
        "created_at": "2026-08-18 02:19:24.161485-07",
        "modified_at": "2026-08-18 02:19:24.161485-07",
        "builtin": false,
        "hidden": false
    }
}
```


1.36.10 Attach an Agent to a Safe

Request

Method	`POST`
Path	`/api/v2/safe/analysis_agent`
Body	`SafeAnalysisAgentModel`

POST /api/v2/safe/analysis_agent

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"safe_id":"4638707616191610881","agent_id":"1"}' \
  'https://10.33.3.191/api/v2/safe/analysis_agent'
```

Response


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


1.36.11 Detach an Agent from a Safe

Request

Method	`DELETE`
Path	`/api/v2/safe/<safe_id>/analysis_agent/<agent_id>`

DELETE /api/v2/safe/<safe_id>/analysis_agent/<agent_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/safe/4638707616191610881/analysis_agent/1'
```

Response

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

1.36.12 Get the Live Analysis Switch

Request

Method	GET
Path	/api/v2/live_analysis/enable

GET /api/v2/live_analysis/enable

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/live_analysis/enable'
```

Response

```
{
    "enabled": false,
    "result": "success"
}
```

1.36.13 Switch Live Analysis On or Off

Request

Method	PATCH
Path	/api/v2/live_analysis/enable
Body	LiveAnalysisEnableModel

PATCH /api/v2/live_analysis/enable

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
```

(continues on next page)

(continued from previous page)

```
  -d '{"enabled":true}' \
  'https://10.33.3.191/api/v2/live_analysis/enable'
```

Response

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

1.37 AI Session Analysis Results NEW

While a monitored session runs, each analysis agent attached to its safe stores what it found. The results are exposed at two levels: one row per agent summarising its work on the session, and one verdict per finding. An operator can adjudicate a verdict - confirm it or mark it a false positive - and that judgment is recorded as a separate feedback object.

Configuring the agents themselves is described in *AI Session Analysis Agents* ***NEW***.

1.37.1 Data Structures

Table 110: `SessionAnalysisAgentModel`

Attribute	Type	Required	Description
`id`	string		Read-only.
`session_id`	string	yes	ID of the session this analysis belongs to.
`user_id`	string		Read-only; hidden; expensive to use. Virtual attribute that filters out sessions not granted to the subject. Requires `session-view` right on object type `user`.
`agent_id`	string		Read-only. Analysis agent this row describes.
`agent_name`	string		Read-only; expensive to use. Name of the agent. Resolves even after the agent is removed, so old analyses stay attributed.
`status`	string {live, finished, failed}		Read-only; expensive to use. Whether the agent is still analyzing the session. `finished` and `failed` are both terminal.
`current_severi`	string {unknown, low, medium, high}		Read-only; expensive to use. Severity of the agent's latest verdict. `unknown` marks a coverage gap: the latest batch could not be analyzed.
`peak_severity`	string {unknown, low, medium, high}		Read-only; expensive to use. Highest severity the agent reported for the session.
`latest_summary`	string		Read-only. Summary of the agent's latest verdict.
`verdict_count`	number		Read-only. Number of verdicts the agent stored for the session.
`provider_name`	string		Read-only. Name the LLM provider had when the analysis started.
`provider_kind`	string		Read-only. Provider kind the analysis ran on.
`provider_url`	string		Read-only. Endpoint the analysis was sent to.
`provider_model`	string		Read-only. Model that produced the verdicts.
`tokens_in`	number		Read-only. Prompt tokens the agent consumed for the session.
`tokens_out`	number		Read-only. Completion tokens the agent consumed for the session.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 111: `SessionAnalysisVerdictModel`

Attribute	Type	Required	Description
`id`	string		Read-only.
`session_id`	string	yes	ID of the session this verdict belongs to.
`user_id`	string		Read-only; hidden; expensive to use. Virtual attribute that filters out sessions not granted to the subject. Requires `session-view` right on object type `user`.
`severity`	string {unknown, low, medium, high}		Read-only; expensive to use. Severity reported by this verdict. `unknown` marks a batch that could not be analyzed.
`summary`	string		Read-only; expensive to use. Human readable summary of the verdict.
`indicators`	string-array		Read-only; expensive to use. Indicators backing the verdict.
`first_event`	number		Read-only. First session event covered by the verdict.
`last_event`	number		Read-only. Last session event covered by the verdict.
`time_offset_ms`	number		Read-only. Offset within the session, in milliseconds, where the analyzed batch ended - the moment to play, since the activity the verdict describes has happened by then.
`agent_id`	string		Read-only; expensive to use. Agent that produced the verdict.
`agent_name`	string		Read-only; expensive to use. Name of that agent. Resolves even after the agent is removed.
`judgment`	string {confirmed, false_positive}		Read-only; expensive to use. Operator judgment recorded for this verdict, if any.
`override_sever`	string {low, medium, high}		Read-only; expensive to use. Severity the operator considers correct, overriding `severity`.
`judged_by`	string		Read-only; expensive to use. Operator who recorded the judgment.
`feedback_id`	string		Read-only; expensive to use. Identifier of the adjudication row, used to update or retract it.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 112: `SessionAnalysisVerdictFeedbackModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`verdict_id`	string	yes	Immutable. Verdict this adjudication belongs to.
`user_id`	string		Read-only; hidden; expensive to use. Virtual attribute gating access to the session the verdict belongs to. Requires `session-view` right on object type `user`.
`judgment`	string {confirmed, false_positive}	yes	Operator judgment on the verdict.
`override_severit`	string {low, medium, high}		Severity the operator considers correct, overriding the verdict severity.
`note`	string		Free-form operator note explaining the judgment. May be empty.
`judged_by`	string		Immutable. Operator who recorded this judgment.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Note

The session object carries the same results in aggregated form - `analysis_status`, `analysis_severity`, `analysis_peak_severity`, `analysis_summary` and `analysis_verdict_count` on the `SessionModel`. Use those when listing sessions, and the endpoints below when you need the per-agent or per-verdict detail.

1.37.2 Retrieve Available Attributes

Request

Method	`GET`
Path	`/api/v2/objspec/session_analysis_agent`, `/api/v2/objspec/session_analysis_verdict`, `/api/v2/objspec/session_analysis_verdict_feedback`

GET /api/v2/objspec/session_analysis_verdict

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.167/api/v2/objspec/session_analysis_verdict'
```

1.37.3 List Per-Agent Analyses

Request

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

GET /api/v2/session/analysis_agent

Restrict the result to one session with the `filter` parameter, for example `?filter=session_id.eq(<session_id>)`.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.167/api/v2/session/analysis_agent?filter=session_id.
↪eq(549439154539200513)'
```

Response


```
{
    "result": "success",
    "session_analysis_agent": [
        {
            "id": "549439154539200513",
            "session_id": "549439154539200513",
            "agent_id": "549439154539200513",
            "agent_name": "Agent_1",
            "status": "live",
            "current_severity": "medium",
            "peak_severity": "medium",
            "latest_summary": "The user attempts to list theirsudo permissions␣
↪by running `sudo -l`, which requires a password. This action is part of␣
↪administrative tasks and warrants human review.",
            "verdict_count": 1,
            "provider_name": "Fudo_AI",
            "provider_kind": "ollama",
            "provider_url": "http://10.0.240.10:11435/api/chat",
            "provider_model": "qwen2.5",
            "tokens_in": 2878,
            "tokens_out": 105,
            "created_at": "2026-08-18 11:15:17.903392-07",
            "modified_at": "2026-08-18 11:17:09.995082-07"
        }
    ]
}
```


Note

`provider_name`, `provider_kind`, `provider_url` and `provider_model` record what the analy-

sis actually ran on, so the values stay meaningful after the provider is reconfigured or removed. `tokens_in` and `tokens_out` let you attribute model cost to a session.

1.37.4 List Verdicts

Request

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

GET /api/v2/session/analysis_verdict

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.167/api/v2/session/analysis_verdict?filter=session_id.
↪eq(549439154539200513)'
```

Response


```
{
    "result": "success",
    "session_analysis_verdict": [
        {
            "id": "549439154539200513",
            "session_id": "549439154539200513",
            "severity": "medium",
            "summary": "The user attempts to list theirsudo permissions by␣
↪running `sudo -l`, which requires a password. This action is part of␣
↪administrative tasks and warrants human review.",
            "first_event": 78,
            "last_event": 95,
            "time_offset_ms": 102850,
            "agent_id": "549439154539200513",
            "agent_name": "Agent_1",
            "created_at": "2026-08-18 11:17:09.991808-07",
            "modified_at": "2026-08-18 11:17:09.991808-07"
        }
    ]
}
```


Note

Use `time_offset_ms` to position the session player - the activity the verdict describes has already happened by that offset. `first_event` and `last_event` identify the same fragment in terms of session events.

The adjudication attributes - `judgment`, `override_severity`, `judged_by` and `feedback_id` - are absent until a verdict is adjudicated.

1.37.5 Adjudicate a Verdict

Request

Method	`POST`
Path	`/api/v2/session/analysis_verdict/feedback`
Body	`SessionAnalysisVerdictFeedbackModel`

POST /api/v2/session/analysis_verdict/feedback

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"verdict_id":"549439154539200513","judgment":"confirmed","override_
↪severity":"low","note":"Routine sudo -l by an administrator; recorded for␣
↪completeness."}' \
  'https://10.33.3.167/api/v2/session/analysis_verdict/feedback'
```

Response

```
{
    "result": "success",
    "session_analysis_verdict_feedback": {
        "id": "549439154539200513"
    }
}
```

Once the adjudication exists, the verdict reports it:

```
{
    "id": "549439154539200513",
    "severity": "medium",
    "judgment": "confirmed",
    "override_severity": "low",
    "judged_by": "549439154539200513",
    "feedback_id": "549439154539200513"
}
```

Note

`severity` keeps the value the agent reported. `override_severity` records what the operator considers correct, so both the model's answer and the human correction remain visible.

1.37.6 List Adjudications

Request

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

GET /api/v2/session/analysis_verdict/feedback

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.167/api/v2/session/analysis_verdict/feedback'
```

Response


```
{
    "result": "success",
    "session_analysis_verdict_feedback": [
        {
            "id": "549439154539200513",
            "verdict_id": "549439154539200513",
            "judgment": "confirmed",
            "override_severity": "low",
            "note": "Routine sudo -l by an administrator; recorded for␣
↪completeness.",
            "judged_by": "549439154539200513",
            "created_at": "2026-08-18 11:18:16.703842-07",
            "modified_at": "2026-08-18 11:18:16.703842-07"
        }
    ]
}
```


1.37.7 Modify an Adjudication

Request

Method	PATCH
Path	/api/v2/session/analysis_verdict/feedback/<id>
Body	SessionAnalysisVerdictFeedbackModel

PATCH /api/v2/session/analysis_verdict/feedback/<id>

Attributes left out of the body keep their current values.

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"judgment":"false_positive","note":"Reclassified after review: the␣
↪operator was authorised for this check."}' \
  'https://10.33.3.167/api/v2/session/analysis_verdict/feedback/
↪549439154539200513'
```

Response

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

1.37.8 Retract an Adjudication

Request

Method	DELETE
Path	/api/v2/session/analysis_verdict/feedback/<id>

DELETE /api/v2/session/analysis_verdict/feedback/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.167/api/v2/session/analysis_verdict/feedback/
↪549439154539200513'
```

Response

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

Retracting the adjudication clears it from the verdict, which returns to reporting only what the agent found:

```
{
    "id": "549439154539200513",
    "severity": "medium",
    "judgment": null,
    "override_severity": null,
    "feedback_id": null
}
```

1.38 Reports

This section describes the API endpoints related to report management. The reporting functionality is based on three core data models that represent report definitions, report subscriptions, and generated reports.

The following data models are used:

- `ReportModel` – represents a report generated on demand for a specific subset of sessions, defined by filtering parameters.
- `DefinedReportSubscriptionModel` – represents a user-defined subscription for automatic, periodic report generation.

- `DefinedReportModel` – represents a user-defined periodic report definition based on custom filtering parameters.

1.38.1 Data Structures: *ReportModel*

Table 113: `ReportModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only object Identifier
`title`	string		Report title.
`defined_report_id`	string		Defined report identifier.
`report_type`	string		Read-only. Expensive to use.
`generated_at`	string		Read-only. Report generated timestamp.
`created_by`	string		Identifier of the user who created the report.
`query_filter`	string		Query filter used to create the report.
`query_order`	string		Query order of returned values used to create the report.
`created_on`	string		Read-only.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only

1.38.2 Retrieve Available Attributes of the *ReportModel*

Request

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

1.38.3 Data Structures: *DefinedReportSubscriptionModel*

A report subscription is a configuration that enables automatic generation of a report for a user at defined intervals.

Table 114: `DefinedReportSubscriptionModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only report subscription identifier
`defined_report_id`	string		Defined report identifier.
`user_id`	string		Identifier of the user who created the report. Requires `read` right on the `user` object for GET, POST, and DELETE operations.

continues on next page

Table 114 – continued from previous page

Attribute	Type	Required	Description
`period`	string {day, week, month, quarter, year}		Period of generating reports.
`created_by`	string		Identifier of the user who created the report.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only

1.38.4 Retrieve Available Attributes of the *DefinedReportSubscriptionModel*

Request

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

1.38.5 Data Structures: *DefinedReportModel*

Table 115: `DefinedReportModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only object Identifier
`title`	string		Defined report title.
`type`	string		Immutable. Defined report type.
`query_filter`	string		Query filter used to create the report.
`query_order`	string		Query order of returned values used to create the report.
`created_by`	string		Immutable. Identifier of the user who created the report.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

1.38.6 Retrieve Available Attributes of the *DefinedReportModel*

Request

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

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

1.38.7 Get List of Generated Reports

Request

Method	`GET`
Path	`/api/v2/report`

Example Request

GET /api/v2/report

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/report'
```

1.38.8 Get List of Predefined Report Definitions

Request

Method	`GET`
Path	`/api/v2/report/defined`

Example Request

GET /api/v2/report/defined

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/report/defined'
```

1.38.9 Get List of Subscriptions to Periodic Reports

Request

Method	`GET`
Path	`/api/v2/report/subscription`

Example Request

GET /api/v2/report/subscription

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/report/subscription'
```

1.38.10 Get or Download Report File

Request

Method	`GET`
Path	`/api/v2/report/<id>/<ext>`
Path	`/api/v2/report/download/<id>/<ext>`

You can use one of three available extensions: csv, pdf, or html.

Example Request

GET /api/v2/report/<id>/html

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/report/9124292845052624897/html'
```

Response

Report in HTML.

1.38.11 Subscribe to a Periodic Report

This endpoint creates a subscription for a periodic report for the currently authenticated user, enabling automatic report generation based on the configured schedule.

Request

Method	`POST`
Path	`/api/v2/report/subscription`
Headers	`Content-Type: Application/json`
Body	`DefinedReportSubscriptionModel`

In the table below are the `defined_report_id` values and their corresponding titles required to subscribe to a predefined periodic report.

Table 116: `ReportModel`

Value of `defined_report_id`	Periodic Report Type
5	System report
6	Account access report
7	Safe access report
8	Server access report
9	Session approvals by user
10	Session sharing invites by user
11	Session summary
12	Sessions by server report
13	User access report
14	User activity report
15	User privilege report
16	User report

Note

You can also check the list of available defined report ID's using the `GET /api/v2/report/defined` endpoint.

Example Request

POST /api/v2/report/subscription

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/report/subscription' \
  -d'{"period":"day","defined_report_id":"6"}'
```

Response

```
{
    "defined_report_subscription": {
        "id": "9124292845052624899"
    },
    "result": "success"
}
```

1.38.12 Create New Report Definition (Custom Filter)

This endpoint allows defining a new periodic report based on custom filtering parameters. The defined report is visible in the **Sessions** view under the **Custom filters** list and can later be used to create a report subscription.

Request

Method	`POST`
Path	`/api/v2/report/defined`
Headers	`Content-Type: Application/json`
Body	`DefinedReportModel`

Example Request

POST /api/v2/report/defined

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/report/defined' \
  -d'{
     "title": "TestingAAA",
     "type": "system",
             "query_filter": "created_at.ge(2025-12-09T12%3A00%3A51.564Z),
↪created_at.le(2026-01-10T12%3A00%3A51.564Z),subprotocol.iin(rdp),user_id.
↪in(1224979098644774913),retention_locked,!finished_at.isnull(),status.
```

(continues on next page)

(continued from previous page)

```
↪iin(approved)",
            "query_order": "!finished_at"
  }'
```

Response

```
{
    "defined_report": {
        "id": "9124292845052624900"
    },
    "result": "success"
}
```

Note

For details about filtering, see *Parameters*.

1.38.13 Generate User Report on Demand

A report can be generated on demand for a specific subset of sessions, defined by filtering parameters.

Note

You can also check the list of available defined report ID's using the `GET /api/v2/report/defined` endpoint.

Request

Method	`POST`
Path	`/api/v2/report`
Headers	`Content-Type: Application/json`
Body	`ReportModel`

Example Request

POST /api/v2/report

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/report' \
  -d'{"criteria":[{"field":"protocol","value":"ssh"},{"field":"user","value":
↪"5620492334958379010"}]}'
```

Response

```
{
    "report": {
        "id": "5620492334958379016"
    },
    "result": "success"
}
```

1.38.14 Update Report Definition (Custom Filter)

Request

Method	PATCH
Path	/api/v2/report/defined/<id>
Headers	Content-Type: Application/json
Body	DefinedReportModel

Example Request

PATCH /api/v2/report/defined/<id>

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/report/defined/9124292845052624900' \
  -d'{
              "title":"Updated Custom Report",
              "query_filter":"created_at.ge(2025-12-09T12%3A00%3A51.564Z),
↪created_at.le(2026-01-10T12%3A00%3A51.564Z),subprotocol.iin(rdp),user_id.
↪in(1224979098644774913),retention_locked,!finished_at.isnull(),status.
↪iin(approved)",
              "query_order": "!finished_at"
     }'
```

Response

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

1.38.15 Delete Generated User Report

Request

Method	DELETE
Path	/api/v2/report/<id>

Example Request

DELETE /api/v2/report/<id>

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/report/9124292845052624902'
```

Response

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

1.38.16 Delete Report Definition (Custom Filter)

Request

Method	DELETE
Path	/api/v2/report/defined/<id>

Example Request

DELETE /api/v2/report/defined/<id>

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/report/defined/9124292845052624900'
```

Response

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

1.38.17 Unsubscribe from a Recurring Report

Request

Method	DELETE
Path	/api/v2/report/subscription/<id>

Example Request

DELETE /api/v2/report/subscription/<id>

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/report/subscription/9124292845052624902'
```

Response

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

1.39 User Productivity Analytics

Fudo Enterprise provides comprehensive analytics on user productivity and session activity patterns.

Note

If the license disables productivity analysis, all requests to this endpoint are rejected with the `403 Forbidden` status.

1.39.1 Data Structures

Table 117: `ProductivityModel`

Attribute	Type	Required	Description
`user_id`	string		Unique user identifier. Read-only. Group-by enabled. Requires `read` capability on `user` object.
`user_name`	string		User name. Read-only. Group-by enabled.
`user_organizat`	string		User organization. Read-only. Group-by enabled.
`started_at`	datetime		Session start timestamp. Filter-only.
`active_time`	number		Time that user was active. Read-only. Expensive to use.
`total_time`	number		Total time of the session(s). Read-only. Expensive to use.
`idle_time`	number		Time user was inactive. Read-only. Expensive to use.
`productivity`	string		Productivity score/classification. Read-only. Expensive to use.
`session_count`	number		Number of sessions. Read-only. Expensive to use.
`server_count`	number		Number of unique servers accessed. Read-only. Expensive to use.
`daily_aggregat`	object-array		Daily aggregation of time properties and productivity for each day. Read-only. Hidden. Expensive to use.
`active`	boolean		User activity status. Read-only. Filter-only. Expensive to use.
`destination_ip`	string		Destination IP address. Filter-only.
`destination_po`	number		Destination port. Filter-only.
`ml_threat_leve`	number		Machine learning threat level. Filter-only.
`protocol`	string		Protocol used. Filter-only.
`replicated_on_`	string-array		List of nodes that session was fully replicated on. Filter-only. Read-only. Expensive to use.
`retention_lock`	boolean		Retention lock status. Filter-only.
`account_id`	string		Account identifier. Filter-only.
`listener_id`	string		Listener identifier. Filter-only.
`safe_id`	string		Safe identifier. Filter-only.
`server_id`	string		Server identifier. Filter-only.

1.39.2 Retrieve Available Attributes of the *ProductivityModel*

Request

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

GET /api/v2/objspec/productivity

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.124.76/api/v2/objspec/productivity'
```

1.39.3 Get User Productivity Analytics

Request

Method	`GET`
Path	`/api/v2/productivity`

GET /api/v2/productivity

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.124.76/api/v2/productivity'
```

Response

```
{
    "result": "success",
    "productivity": [
        {
            "user_id": "8259601716597489665",
            "user_name": "john.doe",
            "user_organization": "IT Department",
            "active_time": 7200,
            "total_time": 8400,
            "idle_time": 1200,
            "productivity": "37.9844961240310078",
            "session_count": 5,
            "server_count": 2
        }
    ]
}
```

1.40 Logs

System log is an internal registry of users activities which influence system state (login information, administrative actions, etc.).

1.40.1 Data Structures

Table 118: `LogModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`facility_name`	string	yes	Read-only. Uniqueness is required.
`severity_id`	string {2, 3, 4, 6, 7}	yes	Read-only. Values: 2 = Critical, 3 = Error, 4 = Warning, 6 = Info, 7 = Debug.
`type_name`	string	yes	Read-only.
`debuglevel`	string	yes	Read-only.
`message`	string	yes	Read-only.
`account_id`	string		Read-only. Requires `read` right on object type `account` for `GET` requests.
`account_name`	string		Read-only.
`account_removed`	boolean		Read-only.
`account_secret_id`	string		Read-only.
`account_secret_removed`	boolean		Read-only.
`collection_id`	string		Read-only.
`collection_name`	string		Read-only.
`collection_removed`	boolean		Read-only.
`listener_id`	string		Read-only.
`listener_name`	string		Read-only.
`listener_removed`	boolean		Read-only.
`pool_id`	string		Read-only. Requires `read` right on object type `pool` for `GET` requests.
`pool_name`	string		Read-only.
`pool_removed`	boolean		Read-only.
`secret_id`	string		Read-only.
`secret_name`	string		Read-only.
`secret_removed`	boolean		Read-only.
`safe_id`	string		Read-only. Requires `read` right on object type `safe` for `GET` requests.
`safe_name`	string		Read-only.
`safe_removed`	boolean		Read-only.
`session_id`	string		Read-only.
`server_id`	string		Read-only. Requires `read` right on object type `server` for `GET` requests.

continues on next page

Table 118 – continued from previous page

Attribute	Type	Required	Description
`server_name`	string		Read-only.
`server_removed`	boolean		Read-only.
`subject_id`	string		Read-only. ID of the object that is the subject of this log, e.g. superadmin giving operator access to user. Requires `read` right on object type `user` for `GET` requests.
`subject_name`	string		Read-only.
`subject_removed`	boolean		Read-only.
`user_id`	string		Read-only. Requires `read` right on object type `user` for `GET` requests.
`user_name`	string		Read-only.
`user_removed`	boolean		Read-only.
`user_extra_id`	string		Read-only. E.g., ID of the user whose specifications another user was granted access to. Requires `read` right on object type `user` for `GET` requests.
`user_extra_name`	string		Read-only.
`user_extra_removed`	boolean		Read-only.
`node_serial`	string		Read-only.
`node_name`	string		Read-only.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.40.2 Retrieve Available Attributes of the *LogModel*

Request

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

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

1.40.3 Get Log List

Example Request

GET /api/v2/log`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/log'
```

1.41 Syslog Server Management

Note

Syslog server endpoints allow configuring external syslog servers to receive log messages from the system. Supports both TCP and UDP transports with optional TLS encryption for TCP connections.

1.41.1 Data Structures

Table 119: `SyslogServerModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique ID of the syslog server.
`name`	string	yes	Unique. Syslog server name (case-insensitive).
`host`	string	yes	Hostname or IP address.
`port`	number		Port number. Default: 6514.
`transport`	string		Transport protocol: `tcp` or `udp`. Default: `tcp`.
`protocol`	string		Syslog wire format: `rfc3164` or `rfc5424`. Default: `rfc3164`.
`tls`	boolean		Enable TLS encryption (TCP only). Default: false.
`tls_certificate`	string		CA certificate for TLS verification. Requires tls=true.
`enabled`	boolean		Enable or disable this server. Default: true.
`debug`	boolean		Enable debug logging. Default: false.
`object_name`	boolean		Include object names in log messages. Default: false.
`created_at`	datetime		Read-only. Creation timestamp.
`modified_at`	datetime		Read-only. Last modification timestamp.
`removed`	boolean		Read-only. Soft delete flag.

1.41.2 Retrieve Available Attributes of the *SyslogServerModel*

Request

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

GET /api/v2/objspec/syslog_server

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/objspec/syslog_server'
```

1.41.3 List Syslog Servers

Retrieve all configured syslog servers.

Request

Method	GET
Path	/api/v2/syslog_server

GET /api/v2/syslog_server

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/syslog_server'
```

Response (With Servers)

```
{
    "result": "success",
    "syslog_server": [
        {
            "id": "5980780305148018689",
            "name": "primary-syslog",
            "host": "syslog.example.com",
            "port": 514,
            "transport": "udp",
            "protocol": "rfc3164",
            "tls": false,
            "enabled": true,
            "debug": false,
            "object_name": false,
            "created_at": "2026-06-09 05:31:21.487119-07",
            "modified_at": "2026-06-09 05:31:21.487119-07"
        }
    ]
}
```

1.41.4 Get Syslog Server Details

Retrieve details of a specific syslog server.

Request

Method	GET
Path	/api/v2/syslog_server/<id>

GET /api/v2/syslog_server/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/syslog_server/5980780305148018689'
```

Response

```
{
    "result": "success",
    "syslog_server": {
        "id": "5980780305148018689",
        "name": "test-syslog",
        "host": "192.168.1.100",
        "port": 6514,
        "transport": "tcp",
        "protocol": "rfc5424",
        "tls": false,
        "enabled": true,
        "debug": false,
        "object_name": false,
        "created_at": "2026-06-09 05:31:21.487119-07",
        "modified_at": "2026-06-09 05:31:21.487119-07"
    }
}
```

1.41.5 Create Syslog Server

Add a new syslog server configuration.

Request

Method	POST
Path	/api/v2/syslog_server
Headers	Content-Type: application/json
Body	SyslogServerModel (name and host required)

POST /api/v2/syslog_server

Example Request - Basic UDP Configuration

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
```

(continues on next page)

(continued from previous page)

```
    "name": "test-syslog",
    "host": "192.168.1.100",
    "port": 514,
    "transport": "udp"
  }' \
  'https://10.33.2.132/api/v2/syslog_server'
```

Example Request - TLS-Enabled TCP Configuration

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "secure-syslog",
    "host": "syslog.example.com",
    "port": 6514,
    "transport": "tcp",
    "tls": true,
    "tls_certificate": "-----BEGIN CERTIFICATE-----\nMIIC..."
  }' \
  'https://10.33.2.132/api/v2/syslog_server'
```

Example Request - RFC 5424 Log Format

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "siem-syslog",
    "host": "siem.example.com",
    "port": 6514,
    "transport": "tcp",
    "protocol": "rfc5424"
  }' \
  'https://10.33.2.132/api/v2/syslog_server'
```

Success Response

```
{
    "result": "success",
    "syslog_server": {
        "id": "5980780305148018689"
    }
}
```

1.41.6 Update Syslog Server

Modify an existing syslog server configuration.

Request

Method	`PATCH`
Path	`/api/v2/syslog_server/<id>`
Headers	`Content-Type: application/json`
Body	`Partial SyslogServerModel`

PATCH /api/v2/syslog_server/<id>

Example Request - Change Port and Transport

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "port": 514,
    "transport": "udp"
  }' \
  'https://10.33.2.132/api/v2/syslog_server/5980780305148018689'
```

Example Request - Enable TLS

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "transport": "tcp",
    "tls": true,
    "tls_certificate": "-----BEGIN CERTIFICATE-----\n..."
  }' \
  'https://10.33.2.132/api/v2/syslog_server/5980780305148018689'
```

Example Request - Switch the Log Format to RFC 5424

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "protocol": "rfc5424"
  }' \
  'https://10.33.2.132/api/v2/syslog_server/5980780305148018689'
```

Success Response

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

1.41.7 Delete Syslog Server

Remove a syslog server configuration.

Request

Method	DELETE
Path	/api/v2/syslog_server/<id>

DELETE /api/v2/syslog_server/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/syslog_server/5980780305148018689'
```

Success Response

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

1.41.8 Configuration Examples

Example 1: Standard UDP Syslog

```
{
    "name": "standard-syslog",
    "host": "syslog.internal.com",
    "port": 514,
    "transport": "udp",
    "enabled": true
}
```

Example 2: Secure TCP with TLS

```
{
    "name": "secure-syslog",
    "host": "syslog.secure.com",
    "port": 6514,
    "transport": "tcp",
    "tls": true,
    "tls_certificate": "<CA_CERTIFICATE>",
    "enabled": true
}
```

Example 3: Debug Configuration

```
{
    "name": "debug-syslog",
    "host": "10.0.0.100",
    "port": 514,
    "transport": "udp",
    "debug": true,
    "object_name": true,
```

(continues on next page)

(continued from previous page)

```
    "enabled": true
}
```

Example 4: RFC 5424 Log Format over TCP with TLS

```
{
    "name": "siem-syslog",
    "host": "siem.example.com",
    "port": 6514,
    "transport": "tcp",
    "protocol": "rfc5424",
    "tls": true,
    "tls_certificate": "<CA_CERTIFICATE>",
    "enabled": true
}
```

Note

- TLS is only supported with TCP transport
- Default port is 6514 for new servers
- Server names are case-insensitive and must be unique
- The `object_name` option includes object names in log messages for better context
- The `protocol` option selects the wire format used for message delivery. With `rfc5424`, the RFC 5424 header is generated for every message and the structured data field is always empty (-); Fudo Enterprise context data stays in the message content

1.42 Notification Filter

1.42.1 Data Structures

Table 120: `NotificationFilterModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`user_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attributes `event_name`, `event_transport` and `safe_id`. Requires `read` right on object type `user` for `GET`, `POST`, and `DELETE` requests.

continues on next page

Table 120 – continued from previous page

Attribute	Type	Required	Description
safe_id	string	Exactly one of safe_id or collectio	Immutable. Uniqueness is required in the combination of attribute safe_id with attributes event_name, event_transport and user_id. Requires read right on object type safe for GET, POST, and DELETE requests.
collection_id	string	Exactly one of safe_id or collectio	Immutable. Uniqueness is required in the combination of attribute collection_id with attributes event_name, event_transport and user_id. Requires read right on object type collection for GET, POST, and DELETE requests.
collection_nam	string		Read-only; expensive to use.
event_name	string {safe_add_server, safe_add_user, safe_blocked, safe_create, safe_remove, safe_unblocked, server_blocked, server_create, server_remove, server_unblocked, user_blocked, user_create, user_remove, user_unblocked, session_ai_summary, session_finish, session_live_analysis, session_ml, session_regexp, session_start, session_sudo, session_waiting, session_inject_close, session_inject_open, disk_failure, filesystem_full, access_request_pending, access_request_accepted access_request_rejected}	yes	Immutable. Uniqueness is required in the combination of attribute event_name with attributes event_transport, safe_id and user_id.

continues on next page

Table 120 – continued from previous page

Attribute	Type	Required	Description
event_transpor	string {mail, push, slack}	yes	Immutable. Uniqueness is required in the combination of attribute event_transport with attributes event_name, safe_id and user_id.
user_name	string		Read-only; expensive to use.
safe_name	string		Read-only; expensive to use.
created_at	datetime		Read-only. Timestamp of creation.
modified_at	datetime		Read-only. Timestamp of modification.
removed	boolean		Read-only.

1.42.2 Retrieve Available Attributes of the *NotificationFilterModel*

Request

Method	GET
Path	/api/v2/objspec/notification_filter

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

1.42.3 Get Notifications List

Request

Method	GET
Path	/api/v2/notification_filter

Example Request

GET /api/v2/notification_filter`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/notification_filter'
```

Response

```
{
    "result": "success",
    "notification_filter": {
        "id": "9124292845052624897",
        "user_id": "9124292845052624898",
        "safe_id": "9124292845052624898",
        "event_name": "access_request_accepted",
        "event_transport": "mail",
        "created_at": "2024-06-11 22:21:15.750371-07",
```

(continues on next page)

(continued from previous page)

```
        "modified_at": "2024-06-11 22:21:15.750371-07"
    }
}
```

1.42.4 Get Notification Filter by ID

Request

Method	GET
Path	/api/v2/notification_filter/<id>

Example Request

GET /api/v2/notification_filter/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/notification_filter/9124292845052624897'
```

Response

```
{
    "result": "success",
    "notification_filter": {
        "id": "9124292845052624897",
        "user_id": "9124292845052624898",
        "safe_id": "9124292845052624898",
        "event_name": "access_request_accepted",
        "event_transport": "mail",
        "created_at": "2024-06-11 22:21:15.750371-07",
        "modified_at": "2024-06-11 22:21:15.750371-07"
    }
}
```

1.42.5 Create Notification Filter

Request

Method	POST
Path	/api/v2/notification_filter
Headers	Content-Type: Application/json
Body	NotificationFilterModel

Example Request

POST /api/v2/notification_filter`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
```

(continues on next page)

(continued from previous page)

```
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/notification_filter' \
  -d'{"safe_id":"9124292845052624898","user_id":"9124292845052624903","event_
↪name":"safe_add_server","event_transport":"mail"}'
```

Response

```
{
    "result": "success",
    "notification_filter": {
        "id": "9124292845052624914"
    }
}
```

1.42.6 Deleting Notification Filter

Request

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

Example Request

DELETE /api/v2/notification_filter/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/notification_filter/9124292845052624897'
```

Response

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

1.43 Push Notifications

1.43.1 Data Structures

Table 121: `PushNotificationModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique notification identifier.

continues on next page

Table 121 – continued from previous page

Attribute	Type	Required	Description
event_name	string {access_request_accepted access_request_pending, access_request_rejected, session_ai_summary, session_finish, session_inject_close, session_inject_open, session_live_analysis, session_ml, session_regexp, session_start, session_sudo, session_waiting}		Read-only. Name of event that triggered the notification.
event_type	string {access_request, session}		Read-only. Type of event that triggered the notification.
event_transpor	string {mail, push, slack}		Read-only. Transport used to deliver the notification.
event_message	string		Read-only. Additional message associated with the event.
event_argument	string		Read-only; expensive to use. Additional arguments necessary to display the event.
occurred_at	datetime		Read-only. Time when the event occurred.
recipient_id	string		Read-only. ID of the user who is the recipient of the notification.
access_request	string	If event_typ == access_re	Read-only. Access request identifier.
access_request	string	If event_typ == access_re	Read-only. Access request reason.
access_request	string {expired, granted, pending, rejected}	If event_typ == access_re	Read-only; expensive to use. Access request status.
access_request	string {immediate, scheduled, preview}	If event_typ == access_re	Read-only. Access request type.

continues on next page

Table 121 – continued from previous page

Attribute	Type	Required	Description
access_request	number	If event_typ == access_re	Read-only; expensive to use. Access request immediate interval (1-24 hours).
access_request	datetime	If event_typ == access_re	Read-only. When access request starts.
access_request	datetime	If event_typ == access_re	Read-only. When access request expires.
access_request	datetime	If event_typ == access_re	Read-only. When access request was created.
access_request	string	If event_nam == access_re	Read-only. Access request rejection reason.
session_id	string	If event_typ == session	Read-only. Session identifier.
session_source	string	If event_typ == session	Read-only. Session source IP address.
session_destin	string	If event_typ == session	Read-only. Session destination IP address.
session_destin	number	If event_typ == session	Read-only. Session destination port.
session_login_	string	If event_typ == session	Read-only. Session login reason.
session_starte	datetime	If event_typ == session	Read-only. When session started.
session_finish	datetime	If event_typ == session	Read-only. When session finished.

continues on next page

Table 121 – continued from previous page

Attribute	Type	Required	Description
session_analys	string {unknown, low, medium, high}	If event_typ == session	Read-only. Peak severity reported by live LLM session analysis.
session_ml_thr	number	If event_typ == session	Read-only. Session ML threat level.
session_ml_thr	number	If event_typ == session	Read-only. Session ML threat level maximum.
session_ml_thr	number	If event_typ == session	Read-only. Session ML threat level minimum.
session_summar	string	If event_typ == session	Read-only. AI-generated summary of the session.
session_summar	object-array	If event_typ == session	Read-only. Session summary key risks.
session_summar	string {unprocessed, pending, processing, succeeded, failed}	If event_typ == session	Read-only. Current processing state of the AI summarizer.
session_scores	object-array	If event_typ == session	Read-only. Session scores.
account_id	string		Read-only. Account identifier.
account_name	string		Read-only. Account name.
account_login	string		Read-only. Account login.
account_domain	string		Read-only. Account domain.
listener_id	string		Read-only. Listener identifier.
listener_name	string	If event_typ == session	Read-only. Listener name.
pool_id	string		Read-only. Pool identifier.
pool_name	string		Read-only. Pool name.
protocol	string {checkout, http, modbus, mysql, oracle, pgsql, rdp, ssh, tcp, tds, telnet, tn3270, tn5250, vnc}		Read-only. Protocol used.

continues on next page

Table 121 – continued from previous page

Attribute	Type	Required	Description
safe_id	string		Read-only. Safe identifier.
safe_name	string		Read-only. Safe name.
server_id	string		Read-only. Server identifier.
server_name	string		Read-only. Server name.
user_id	string		Read-only. User identifier.
user_domain	string		Read-only. User domain.
user_full_name	string		Read-only. User full name.
user_name	string		Read-only. User name.
user_organizat	string		Read-only. User organization.
user_extra_id	string		Read-only. ID of another user related to the notification: for example user who joined the session.
user_extra_dom	string		Read-only. Extra user domain.
user_extra_nam	string		Read-only. Extra user name.
user_extra_org	string		Read-only. Extra user organization.
policies	object-array	If event_nam == session_a | session_l | session_m | session_r | session_s	Read-only. List of policies that triggered the notification.
webclient	boolean		Read-only; expensive to use. Is the access available via the web client or was the session established using the web client?
secret_id	string		Read-only. Secret identifier.
secret_name	string		Read-only. Secret name.
secret_login	string		Read-only. Secret login.
secret_domain	string		Read-only. Secret domain.
secret_descrip	string		Read-only. Secret description.
secret_uris	string-array		Read-only. Secret URIs.
collection_id	string		Read-only. Collection identifier.
collection_nam	string		Read-only. Collection name.

1.43.2 Get Push Notification Object Specification

Request

Method	GET
Path	/api/v2/objspec/push_notification

GET /api/v2/objspec/push_notification

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/objspec/push_notification'
```

Response

```
{
    "result": "success",
    "push_notification": {
        "id": {
            "type": "string",
            "readonly": true,
            "filterable": true
        },
        "event_name": {
            "type": "string",
            "description": "Name of event that triggered the notification",
            "readonly": true,
            "values": [
                "access_request_accepted", "access_request_pending", "access_
↪request_rejected",
                "session_ai_summary", "session_finish", "session_inject_close",
                "session_inject_open", "session_ml", "session_regexp",
                "session_start", "session_waiting"
            ],
            "filterable": true
        },
        "event_type": {
            "type": "string",
            "description": "Type of event that triggered the notification",
            "readonly": true,
            "values": ["access_request", "session"],
            "filterable": true
        },
        "event_transport": {
            "type": "string",
            "description": "Transport used to deliver the notification",
            "readonly": true,
            "values": ["mail", "push", "slack"],
            "filterable": true
        },
        "event_message": {
            "type": "string",
            "description": "Additional message associated with the event",
            "readonly": true,
            "filterable": true
        },
        "occurred_at": {
            "type": "string",
```

(continues on next page)

(continued from previous page)

```
            "description": "Time when the event occurred",
            "db-subtype": "timestamp",
            "readonly": true,
            "filterable": true
        },
        "session_summary": {
            "type": "string",
            "description": "AI-generated summary of the session.",
            "readonly": true,
            "filterable": true
        }
    }
}
```

1.43.3 List Push Notifications

Request

Method	GET
Path	/api/v2/notification/push

GET /api/v2/notification/push

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/notification/push'
```

Response

```
{
    "result": "success",
    "push_notification": [
        {
            "id": "notif123",
            "event_name": "session_ai_summary",
            "event_type": "session",
            "event_transport": "push",
            "event_message": "AI summary generated for session",
            "occurred_at": "2025-01-15T14:30:00Z",
            "session_id": "session_456",
            "session_summary": "User performed database maintenance tasks with␣
↪elevated privileges.",
            "user_name": "john.doe"
        }
    ]
}
```

1.43.4 Get Push Notification by ID

Request

Method	GET
Path	/api/v2/notification/push/<id>

GET /api/v2/notification/push/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/notification/push/notif123'
```

Response


```
{
    "result": "success",
    "push_notification": [
        {
            "id": "notif123",
            "event_name": "access_request_pending",
            "event_type": "access_request",
            "event_transport": "push",
            "occurred_at": "2025-01-15T14:30:00Z",
            "access_request_id": "ar789",
            "access_request_status": "pending",
            "user_name": "jane.smith",
            "safe_name": "Production Safe"
        }
    ]
}
```


1.44 Downloads

The Fudo Enterprise allows for tracking the conversion progress of session recordings and files transferred during SFTP sessions, previously selected for download.

Note

The Files section is designated for managing the downloads of large files that originate from recorded sessions via the SFTP protocol. If the selected file exceeds the 50 MB threshold, it undergoes an encoding process and subsequently appears in the Files tab, ready for download. Files smaller than 50 MB are directly downloaded through the browser without encoding.

1.44.1 Data Structures

Table 122: `SessionFileModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only object Identifier
`session_id`	string		Read-only. ID of the session to download.
`user_id`	string		Read-only; hidden; expensive to use. Authorization field that forces the join on the session's user. Requires `read` right on object type `user`.
`encode_on`	string		Read-only. Node on which file was encoded.
`handle`	number		Read-only.
`delta`	number		Read-only.
`from_server`	boolean		Read-only.
`error`	string		Read-only. Error when file is not ready for download.
`size`	number		Read-only. Size of downloaded session file in bytes.
`session_user`	string		Read-only. Expensive. Session user name.
`session_user_id`	string		Read-only. Expensive. Session user id.
`session_server`	string		Read-only. Expensive. Session server name.
`session_server_id`	string		Read-only. Expensive. Session server id.
`session_started`	string		Read-only. Expensive. Timestamp. Time when session started.
`is_converted`	boolean		Read-only. Expensive. Encoding is complete and file is ready to download.
`progress`	number		Read-only. Expensive. Progress of session conversion in percentage.
`encode_on_name`	string		Read-only. Expensive. Node name on which session was encoded.

1.44.2 Retrieve available attributes of the *SessionFileModel*

Request

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

Table 123: `SessionMovieModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only object Identifier
`session_id`	string		Read-only. ID of the session to download.

continues on next page

Table 123 – continued from previous page

Attribute	Type	Required	Description
`user_id`	string		Read-only; hidden; expensive to use. Authorization field that forces the join on the session's user. Requires `read` right on object type `user`.
`encode_on`	string		Read-only. Node on which session was encoded.
`video_resolution`	string {auto, hd480, hd720, hd1080}		Read-only.
`video_format`	string {divx5, fbsdir, flv, mjpeg, mpeg2, pcap, text, webm, xvid}		Read-only.
`size`	number		Read-only. Size of downloaded session file in bytes.
`session_user`	string		Read-only. Expensive. Session user name.
`session_user_id`	string		Read-only. Expensive. Session user id.
`session_server`	string		Read-only. Expensive. Session server name.
`session_server_id`	string		Read-only. Expensive. Session server id.
`session_started`	string		Read-only. Expensive. Timestamp. Time when session started.
`is_converted`	boolean		Read-only. Expensive. Encoding is complete and file is ready to download.
`is_downloadable`	boolean		Read-only. Expensive. File is converted and the encoding node is available.
`progress`	number		Read-only. Expensive. Progress of session conversion in percentage.
`encode_on_name`	string		Read-only. Expensive. Node name on which session was encoded.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.44.3 Retrieve Available Attributes of the *SessionMovieModel*

Request

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

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

1.44.4 Get Session Files List

Request

Method	`GET`
Path	`/api/v2/session_file`

Example Request

GET /api/v2/session_file`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/session_file'
```

Response


```
{
    "result": "success",
    "session_file": [
        {
            "id": "1",
            "session_id": "5620492334958379016",
            "encode_on": "82984746",
            "handle": 1,
            "from_server": true,
            "size": 56622199,
            "session_user": "User_1",
            "session_user_id": "562049233495837901O",
            "session_server": "SSH_FTP",
            "session_server_id": "5620492334958379018",
            "session_started": "2024-06-25 02:43:38.152033-07",
            "is_converted": true,
            "is_downloadable": true,
            "progress": 100
        }
    ]
}
```

1.44.5 Get Session Recordings List

Request

Method	GET
Path	/api/v2/session_movie

Example Request

GET /api/v2/session_movie`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/session_movie'
```

Response


```
{
    "result": "success",
    "session_movie": [
        {
            "id": "5620492334958379009",
            "session_id": "5620492334958379015",
            "encode_on": "82984746",
            "video_resolution": "auto",
            "video_format": "fbsdir",
            "size": 2399446,
            "session_user": "User_1",
            "session_user_id": "5620492334958379010",
            "session_server": "SSH_FTP",
            "session_server_id": "5620492334958379018",
            "session_started": "2024-06-25 02:25:26.670768-07",
            "is_converted": true,
                        "is_downloadable": true,
            "progress": 100,
            "created_at": "2024-06-25 02:41:07.835711-07",
            "modified_at": "2024-06-25 02:41:08.047049-07"
        },
        {
            "id": "5620492334958379010",
            "session_id": "5620492334958379017",
            "encode_on": "82984746",
            "video_resolution": "auto",
            "video_format": "divx5",
            "size": 3108346,
            "session_user": "User_1",
            "session_user_id": "5620492334958379010",
            "session_server": "RDP_SERVER",
            "session_server_id": "5620492334958379011",
            "session_started": "2024-06-25 03:03:46.780874-07",
            "is_converted": true,
```


(continues on next page)

(continued from previous page)

```
                        "is_downloadable": true,
            "progress": 100,
            "created_at": "2024-06-25 03:04:10.370597-07",
            "modified_at": "2024-06-25 03:04:17.472475-07"
        }
    ]
}
```

1.44.6 Downloading Session Files

Request

Method	`GET`
Path	`/api/v2/download/session_file/<id>`

Example Request

GET /api/v2/download/session_file/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/download/session_file/1'
```

Response

File download is starting.

1.44.7 Downloading Session Recordings

Request

Method	`GET`
Path	`/api/v2/download/session_movie/<id>`

Example Request

GET /api/v2/download/session_movie/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/download/session_movie/1'
```

Response

Session recording download is starting.

1.44.8 Deleting Session File

Request

Method	DELETE
Path	/api/v2/session_file/<id>

Example Request

DELETE /api/v2/session_file/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/session_file/1'
```

Response

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

1.44.9 Deleting Session Recording

Request

Method	DELETE
Path	/api/v2/session_movie/<id>

Example Request

DELETE /api/v2/session_movie/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/session_movie/1'
```

Response

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

1.45 Machine Learning - Session Scoring

Note

Machine Learning Session Scoring provides anomaly detection capabilities for user sessions. The ML system analyzes session behavior patterns and assigns probability scores to identify potentially anomalous activities.

1.45.1 Data Structures

Table 124: `MLSessionScoreModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Hidden. Internal score identifier.
`session_id`	string	yes	Unique. ID of the session this score is related to.
`user_id`	string		Read-only. Hidden. Expensive to use. Virtual property used to filter sessions by user permissions.
`reject_probabil:`	string		Read-only. Expensive to use. Probability of anomalous behavior (0.0 to 1.0).
`end_time`	datetime		Read-only. Timestamp of the scoring event within the session.
`model`	string		Read-only. Expensive to use. Name of the ML model profile that produced this score.

1.45.2 Retrieve Available Attributes of the *MLSessionScoreModel*

Request

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

GET /api/v2/objspec/ml_session_score

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/objspec/ml_session_score'
```

1.45.3 List ML Session Scores

Retrieve machine learning anomaly scores for analyzed sessions.

Request

Method	`GET`
Path	`/api/v2/ml/session_score`

GET /api/v2/ml/session_score

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/ml/session_score'
```

Response (No Scores)

```
{
    "result": "success",
    "ml_session_score": []
}
```

Response (With Scores)

```
{
    "result": "success",
    "ml_session_score": [
        {
            "session_id": "5980780305148018689",
            "reject_probability": "1",
            "end_time": 88108,
            "model": "Semantic_Behavioral"
        },
        {
            "session_id": "5980780305148018689",
            "reject_probability": "1",
            "end_time": 77533,
            "model": "Semantic_Behavioral"
        }
    ]
}
```

Note

- Scores are generated automatically by the ML system when sessions are analyzed
- The `reject_probability` value ranges from 0.0 (normal) to 1.0 (highly anomalous)
- Higher values indicate greater likelihood of anomalous behavior
- The threshold for alerting is configured in ML settings

1.46 Machine Learning Settings

Manage configuration for the machine learning anomaly detection system.

1.46.1 Data Structures

Table 125: `MLSettingsModel`

Component	Attribute	Type	Description
mld			ML Daemon configuration
	`workers_number`	number	Number of worker processes (default: 1)

continues on next page

Table 125 – continued from previous page

Component	Attribute	Type	Description
	`score_logging`	string	Logging level for scores. One of: `none`, `low`, `high`, `all`
mltraind			ML Training Daemon configuration
	`max_workers`	number	Maximum training workers (-1 for unlimited)
	`node`	string	Node identifier for distributed training
	`train_days`	array	Days of week to run training (0=Sunday, 6=Saturday)
	`train_hour`	number	Hour to start training (0-23)
	`train_minute`	number	Minute to start training (0-59)
	`min_days`	number	Minimum days of data required for training
	`max_days`	number	Maximum days of historical data to use
mlquantd			ML Quantization Daemon configuration
	`tolerance`	number	Tolerance level for quantization
	`report_threshol`	string	Threshold for reporting anomalies (e.g., '0.01')

1.46.2 Get ML Settings

Retrieve current machine learning configuration settings.

Request

Method	`GET`
Path	`/api/v2/ml/settings`

GET /api/v2/ml/settings

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/ml/settings'
```

Response

```
{
    "result": "success",
    "mld": {
        "workers_number": 1,
        "score_logging": "high"
    },
    "mltraind": {
        "max_workers": -1,
        "node": "80840259",
        "train_days": ["0", "1", "2", "3", "4", "5", "6"],
        "train_hour": 4,
        "train_minute": 25,
        "min_days": 1,
```

(continues on next page)

(continued from previous page)

```
        "max_days": 365
    },
    "mlquantd": {
        "tolerance": 3,
        "report_threshold": "0.01"
    }
}
```

1.46.3 Update ML Settings

Modify machine learning configuration settings.

Warning

Changes to ML settings affect the anomaly detection system. Modifying training schedules or thresholds may impact detection accuracy. Always test changes in a non-production environment first.

Request

Method	`POST`
Path	`/api/v2/ml/settings`
Headers	`Content-Type: application/json`
Body	`Complete MLSettingsModel (all components required)`

POST /api/v2/ml/settings

Note

All three components (`mld`, `mltraind`, `mlquantd`) must be provided in the request body, even if you're only changing one setting. Retrieve current settings first, modify what you need, then send the complete configuration.

Example Request - Change Score Logging Level

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "mld": {
        "workers_number": 2,
        "score_logging": "all"
    },
    "mltraind": {
        "max_workers": -1,
        "node": "80840259",
        "train_days": ["0", "1", "2", "3", "4", "5", "6"],
```

(continues on next page)

(continued from previous page)

```
        "train_hour": 4,
        "train_minute": 30,
        "min_days": 1,
        "max_days": 365
    },
    "mlquantd": {
        "tolerance": 3,
        "report_threshold": "0.01"
    }
  }' \
  'https://10.33.2.132/api/v2/ml/settings'
```

Success Response

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

Error Response - Missing Field

```
{
    "result": "failure",
    "message": "Couldn't deserialize body: missing field `workers_number` at␣
↪line 4 column 5"
}
```

Error Response - Invalid Value

```
{
    "result": "failure",
    "message": "Couldn't deserialize body: unknown variant `medium`, expected␣
↪one of `none`, `high`, `low`, `all` at line 4 column 33"
}
```

1.46.4 Configuration Examples

Example 1: Enable Maximum Logging

```
{
    "mld": {
        "workers_number": 4,
        "score_logging": "all"
    }
}
```

Example 2: Configure Training Schedule for Weekends Only

```
{
    "mltraind": {
        "train_days": ["0", "6"],
```

(continues on next page)

(continued from previous page)

```
        "train_hour": 2,
        "train_minute": 0
    }
}
```

Example 3: Adjust Anomaly Reporting Threshold

```
{
    "mlquantd": {
        "tolerance": 5,
        "report_threshold": "0.05"
    }
}
```

1.46.5 Related Endpoints

- `GET /api/v2/session` - View sessions that may have ML scores
- `GET /api/v2/alert` - View alerts triggered by ML anomaly detection
- `GET /api/v2/report` - Generate reports on ML detection performance

1.47 Machine Learning - Model Profiles

Note

ML Model Profiles define different machine learning models used for anomaly detection in user sessions. Each profile targets specific protocols and behavior patterns:

- **Semantic_Behavioral** - Analyzes command patterns in SSH sessions
- **Mouse_Biometric** - Tracks mouse movement patterns in RDP sessions
- **Keyboard_Biometric** - Monitors typing patterns in RDP sessions

1.47.1 Data Structures

Table 126: `MLModelProfileModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique ID of machine learning model profile.
`name`	string		Read-only. Profile name (e.g., Semantic_Behavioral, Mouse_Biometric).
`active`	boolean		Read-only. Whether the profile is enabled for scoring.
`ml_model`	number		Read-only. ID of the currently active ML model for this profile.
`protocol`	string		Read-only. Protocol this profile applies to (ssh, rdp, etc.).

continues on next page

Table 126 – continued from previous page

Attribute	Type	Required	Description
`training_time`	string		Read-only. Expensive to use. Time spent training the current model (seconds).
`session_segments`	string		Read-only. Expensive to use. Number of session segments used for training.
`entities_covered`	number		Read-only. Expensive to use. Number of entities covered by the model.
`tpr`	string		Read-only. Expensive to use. True positive rate of the model (0.0 to 1.0).
`fpr`	string		Read-only. Expensive to use. False positive rate of the model (0.0 to 1.0).
`auroc`	string		Read-only. Expensive to use. Area under ROC curve (0.0 to 1.0, higher is better).
`trained_at`	string		Read-only. Expensive to use. Timestamp when the model was trained.

1.47.2 Retrieve Available Attributes of the *MLModelProfileModel*

Request

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

GET /api/v2/objspec/ml_model_profile

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/objspec/ml_model_profile'
```

1.47.3 List ML Model Profiles

Retrieve all available machine learning model profiles.

Request

Method	`GET`
Path	`/api/v2/ml/profile`

GET /api/v2/ml/profile

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/ml/profile'
```

Response


```
{
    "result": "success",
    "ml_model_profile": [
        {
            "id": "5980780305148018689",
            "name": "Semantic_Behavioral",
            "active": true,
            "ml_model": 5980780305148018733,
            "protocol": "ssh",
            "training_time": "91.651764",
            "session_segments_used": "5400",
            "entities_covered": 6,
            "tpr": "1",
            "fpr": "0",
            "auroc": "1",
            "trained_at": "2026-06-08 08:49:59.795649-07"
        },
        {
            "id": "5980780305148018690",
            "name": "Mouse_Biometric",
            "active": true,
            "ml_model": 5980780305148018731,
            "protocol": "rdp",
            "training_time": "14.345926",
            "session_segments_used": "2357",
            "entities_covered": 12,
            "tpr": "0.9293527",
            "fpr": "0.029565375",
            "auroc": "0.98550755",
            "trained_at": "2026-06-08 08:46:47.652581-07"
        },
        {
            "id": "5980780305148018691",
            "name": "Keyboard_Biometric",
            "active": true,
            "ml_model": 5980780305148018732,
            "protocol": "rdp",
            "training_time": "12.508921",
            "session_segments_used": "2189",
            "entities_covered": 11,
            "tpr": "0.8636141",
            "fpr": "0.039960314",
            "auroc": "0.95361376",
            "trained_at": "2026-06-08 08:47:23.623124-07"
        }
    ]
}
```

1.47.4 Disable ML Model Profile

Disable a specific ML model profile to stop it from scoring new sessions.

Request

Method	POST
Path	/api/v2/ml/profile/<id>/disable

POST /api/v2/ml/profile/<id>/disable

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/ml/profile/5980780305148018691/disable'
```

Success Response

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

1.47.5 Enable ML Model Profile

Enable a previously disabled ML model profile to resume scoring sessions.

Request

Method	POST
Path	/api/v2/ml/profile/<id>/enable

POST /api/v2/ml/profile/<id>/enable

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/ml/profile/5980780305148018691/enable'
```

Success Response

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

1.48 External Authentication

1.48.1 Data Structures

Table 127: `ExternalAuthenticationModel`

Attribute	Type	Required	Description
`id`	string	yes	Read-only object identifier
`name`	string	yes	Unique; case insensitive
`type`	string {cerb, radius, ldap, ad}	yes	Immutable
`address`	string	If `type` == `cerb` || `ldap` || `radius` & `port` is set	Authentication server address. Required for selected types if port is set.
`port`	number	If `type` == `cerb` || `ldap` || `radius` & `address` is set	Server port. Must be used with address. Value format: port.
`bind_ip`	string		Bind address. Include labels like 'fudo:label:test' or ip address
`login`	string	If `type` == `ad` & `secret` is set	Login for AD authentication. Must be used with secret.
`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	If `type` == `ad` || `ldap`	Enable TLS protocol
`tls_certificate`	string	If `type` == `ldap` & `tls_enabled` == `true`	Client TLS certificate. Format: X.509.
`tls_ca_certificate`	string	If `type` == `ad` || `ldap` & `tls_enabled` == `true`	CA certificate for TLS validation. Format: X.509.
`second_factor_type`	string {duo, oath, sms}		
`created_at`	datetime		Read-only
`modified_at`	datetime		Read-only
`removed`	boolean		Read-only

Table 128: `ExternalAuthenticationCerbModel`

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

Table 129: `ExternalAuthenticationRadiusModel`

Attribute	Type	Description
`secret`	string	Password to radius provider; required; write-only
`radius_nasid`	string	Correct value of NAS id of Radius provider; required
`radius_method`	string {chap, mschap, pap}	Authentication method for RADIUS. Values: chap (CHAP), mschap (MS-CHAPv2), pap (PAP). Default: mschap
`radius_message_authen`	boolean	Use Message-Authenticator to mitigate BlastRADIUS vulnerability. Default: `true`
`radius_append_domain`	boolean	Append the user's AD domain to the username sent to the RADIUS server, in the `{name}@{ad_domain}` format. When `false`, the bare username is sent. Default: `true`

Table 130: `ExternalAuthenticationLdapModel`

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

Table 131: `ExternalAuthenticationAdModel`

Attribute	Type	Description
`login`	string	Login for AD authentication. Used with secret.
`secret`	string	Password to AD provider; write-only. Used with login.
`ad_domain`	string	Bind domain to AD provider; required

1.48.2 Retrieve Available Attributes of the *ExternalAuthentication- Model*

Request

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

To check allowed methods, available URL parameters and possible responses please refer to the

API Overview section.

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

1.48.3 Get External Authentication Methods List

Request

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

Example Request

GET /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": "",
```


(continues on next page)

(continued from previous page)


```
                "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",
                "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"
                }
        ]
}
```


1.48.4 Get External Authentication Method by ID

Request

Method	GET
Path	/api/v2/external_authentication/<id>

Example Request

GET /api/v2/external_authentication/<id>`

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"
                }
        ]
}
```

1.48.5 Modify 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

PATCH /api/v2/external_authentication/<id>`

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

Response

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

1.48.6 Create 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

POST /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": "123456819172646913"
        }
}
```

1.48.7 Delete an External Authentication Method

Request

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

1.49 OpenID Connect Configuration

OpenID Connect related endpoints help to create, modify, list and delete OpenID Connect configurations.

1.49.1 Data Structures

Table 132: `OpenIDModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`name`	string	yes	Name of the configuration. Case-insensitive. Uniqueness is required.
`enabled`	boolean; Default value `true`	yes	Enabling configuration.
`bind_to`	string		Bind address.
`configuration_url`	string	yes	This URL is specific for every Identity Provider and allows identifying one for correct configuration. Either the address of the discovery document, or the issuer address alone - in the latter case `/.well-known/openid-configuration` is appended automatically.
`client_id`	string	yes	Client id available after the registration on selected provider.
`client_secret`	string	yes	Client secret available after the registration on selected provider. Protected.
`scope`	string		Custom OIDC scope(s) appended to the base scopes (`openid`, `profile`, `email`) on the authorization request. Space-separated list; leave empty to send only the base scopes.

continues on next page

Table 132 – continued from previous page

Attribute	Type	Required	Description
`fudo_domain`	string		The domain used to identify the user on Fudo. It is not a part of the user's UPN — when set, it only narrows the match to users with that Fudo domain.
`username_mapping`	string		Username mapping is useful when users name has different naming convention.
`email_mapping`	string		Email mapping is useful when users name has different naming convention.
`scope`	string		Custom OIDC scope(s) appended to the base scopes (`openid`, `profile`, `email`) on the authorization request. Space-separated list; leave empty to send only the base scopes. Leading, trailing and repeated spaces are rejected.
`tls_ca_certificate`	string		TLS CA certificate that signed the certificate of the server. Format: `x509-ca-certificate`.
`tls_certificate`	string		TLS certificate of the server. Format: `x509-certificate`.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.49.2 Retrieve Available Attributes of the *OpenIDModel*

Request

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

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

1.49.3 Get Existing OpenID Connect Configurations List

Request

Method	`GET`
Path	`/api/v2/oidc`

Example Request

GET /api/v2/oidc`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/oidc'
```

Response


```
{
    "result": "success",
    "oidc": [
        {
            "id": "9124292845052624897",
            "name": "OKTA",
            "enabled": true,
            "bind_to": "0.0.0.0",
            "configuration_url": "https:\/\/okta.com",
            "client_id": "1234567",
            "created_at": "2024-06-19 07:51:42.988336-07",
            "modified_at": "2024-06-19 07:51:42.988336-07"
        }
    ]
}
```


1.49.4 Get Existing OpenID Connect Configuration by ID

Request

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

Example Request

GET /api/v2/oidc/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/oidc/9124292845052624897'
```

Response


```
{
    "result": "success",
    "oidc": [
        {
            "id": "9124292845052624897",
            "name": "OKTA",
            "enabled": true,
            "bind_to": "0.0.0.0",
            "configuration_url": "https:\/\/okta.com",
            "client_id": "1234567",
            "created_at": "2024-06-19 07:51:42.988336-07",
            "modified_at": "2024-06-19 07:51:42.988336-07"
        }
    ]
}
```

1.49.5 Defining OpenID Connect Configuration

Request

Method	`POST`
Path	`/api/v2/oidc`
Headers	`Content-Type: Application/json`
Body	`OpenIDModel`

Example Request

POST /api/v2/oidc`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/oidc' \
  -d'{"name": "OKTA","enabled": true,"configuration_url":"https:\/\/okta.com",
↪"client_id":"1234567","client_secret":"Secret"}'
```

Response

```
{
    "result": "success",
    "oidc": {
        "id": "9124292845052624898"
    }
}
```

1.49.6 Modify OpenID Connect Configuration

Request

Method	`PATCH`
Path	`/api/v2/oidc/<id>`
Headers	`Content-Type: Application/json`
Body	`OpenIDModel`

Example Request

PATCH /api/v2/oidc/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/oidc/9124292845052624898' \
  -d'{"client_id":"1234567","client_secret":"Secret"}'
```

Response

```
{
    "result": "success",
    "oidc": {
        "id": "9124292845052624898"
    }
}
```

1.49.7 Deleting OpenID Connect Configuration

Request

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

Example Request

DELETE /api/v2/oidc/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/oidc/9124292845052624897'
```

Response

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

1.50 OpenID Connect Users Assignment

User related OpenID Connect endpoints help to create, modify, list and delete OpenID Connect configurations assignment to Users.

1.50.1 Data Structures

Table 133: `UserOpenIDModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Protected. Unique identifier.
`user_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_id` with attribute `oidc_id`. Requires `read` right on object type `user` for `GET` requests, and `modify` right for `DELETE`, `PATCH`, and `POST` requests.
`oidc_id`	string	yes	Immutable. Uniqueness is required in the combination of attribute `oidc_id` with attribute `user_id`.
`oidc_sub`	string	yes	OpenID Connect sub claim.
`user_name`	string		Read-only. Expensive to use.
`user_domain`	string		Read-only. Expensive to use.
`user_email`	string		Read-only. Expensive to use.
`user_organization`	string		Read-only. Expensive to use.
`user_role`	string		Read-only. Expensive to use.
`oidc_name`	string		Read-only. Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`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.

1.50.2 Retrieve Available Attributes of the *UserOpenIDModel*

Request

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

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

1.50.3 Get the List of Existing OpenID Connect Configuration Assignments to Users

Request

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

Example Request

GET /api/v2/user/oidc`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user/oidc'
```

Response

```
{
    "result": "success",
    "user_oidc": [
        {
            "user_id": "9124292845052624898",
            "oidc_id": "9124292845052624898",
            "oidc_sub": "John",
            "user_name": "User_1",
            "user_domain": "zw.local",
            "user_email": "user@fudosecurity.com",
            "user_role": "operator",
            "oidc_name": "OKTA2",
            "created_at": "2024-06-19 08:39:55.351137-07",
            "modified_at": "2024-06-19 08:39:55.351137-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```

1.50.4 Get Existing OpenID Connect Configuration Assigned to User

Request

Method	GET
Path	/api/v2/user/<user_id>/oidc/<oidc_id>

Example Request

GET /api/v2/user/<id>/oidc/<id>`

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user/9124292845052624898/oidc/9124292845052624898'
```

Response

```
{
    "result": "success",
    "user_oidc": [
        {
            "user_id": "9124292845052624898",
            "oidc_id": "9124292845052624898",
```

(continues on next page)

(continued from previous page)


```
            "oidc_sub": "John",
            "user_name": "User_1",
            "user_domain": "zw.local",
            "user_email": "user@fudosecurity.com",
            "user_role": "operator",
            "oidc_name": "OKTA2",
            "created_at": "2024-06-19 08:39:55.351137-07",
            "modified_at": "2024-06-19 08:39:55.351137-07",
            "builtin": false,
            "hidden": false
        }
    ]
}
```


1.50.5 Defining OpenID Connect Configuration Assignment to User

Request

Method	`POST`
Path	`/api/v2/user/oidc`
Headers	`Content-Type: Application/json`
Body	`UserOpenIDModel`

Example Request

POST /api/v2/user/oidc`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/user/oidc' \
  -d'{"user_id":"9124292845052624898","oidc_id":"9124292845052624898","oidc_sub
↪":"John"}'
```

Response


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


1.50.6 Modify OpenID Connect Configuration Assignment to User

Request

Method	`PATCH`
Path	`/api/v2/user/<user_id>/oidc/<oidc_id>`
Headers	`Content-Type: Application/json`
Body	`UserOpenIDModel`

Example Request

PATCH /api/v2/user/<id>/oidc/<id>`

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/user/9124292845052624898/oidc/9124292845052624898
↪' \
  -d'{"oidc_sub":"JohnD"}'
```

Response

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

1.50.7 Deleting OpenID Connect Configuration Assignment to User

Request

Method	DELETE
Path	/api/v2/user/<user_id>/oidc/<oidc_id>

Example Request

DELETE /api/v2/user/<id>/oidc/<id>`

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/user/9124292845052624800/oidc/9124292845052624897'
```

Response

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

1.51 JWT Provider Management NEW

Note

JWT provider endpoints allow configuring upstream token issuers that authenticate Fudo Enterprise users on the request's behalf. A request that carries a signed JWT in the configured HTTP header is verified against the keys published by the issuer, and the claim named by `username_claim` is mapped to an existing user.

1.51.1 Data Structures

Table 134: `JWTProviderModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique ID of the JWT provider.
`name`	string	yes	Unique. JWT provider name (case-insensitive).
`enabled`	boolean; default value `true`	yes	Enable or disable this provider. Disabled providers are ignored during verification.
`issuer`	string	yes	Unique. Expected issuer (`iss`) claim, used to match an incoming JWT to this provider. Must start with `https://`.
`jwks_uri`	string		HTTPS URI of the JSON Web Key Set. If omitted, discovered via the issuer's OpenID Configuration at `<issuer>/.well-known/openid-configuration`.
`audience`	string	yes	Expected audience (`aud`) claim. JWTs with a different audience are rejected.
`username_claim`	string; default value `sub`	yes	JWT claim that contains the Fudo Enterprise user name.
`fudo_domain`	string		Fudo domain to scope the user lookup.
`header`	string; default value `Authorization`	yes	HTTP header that carries the JWT. Configure when fronted by a WAF that injects JWTs into a custom header, for example `X-JWT-Assertion`.
`keys_updated_at`	datetime		Read-only. Timestamp of the last successful key refresh.
`keys`	object-array of `JWTProviderKeyMode`		Read-only; expensive to use. Cached signing keys fetched from the provider's JWKS endpoint. Returned only when requested explicitly.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Table 135: `JWTProviderKeyModel`

Attribute	Type	Required	Description
`kid`	string		Read-only. Key identifier published by the issuer. Used to select the key when a token carries the `kid` header. Empty when the issuer publishes a single unnamed key.
`kty`	string {RSA, EC, OKP}		Read-only. Key type. It has to match the algorithm family of the token: `RSA` for `RS*`, `EC` for `ES*`, `OKP` for `EdDSA`.
`alg`	string		Read-only. Algorithm declared for this key by the issuer. Empty when the issuer does not declare one.
`public_key`	string		Read-only. Public key converted to the PEM format.

1.51.2 Retrieve Available Attributes of the *JWTProviderModel*

Request

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

GET /api/v2/objspec/jwt_provider

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/objspec/jwt_provider'
```

1.51.3 List JWT Providers

Retrieve all configured JWT providers.

Request

Method	`GET`
Path	`/api/v2/jwt_provider`

GET /api/v2/jwt_provider

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/jwt_provider'
```

Response

```
{
    "result": "success",
    "jwt_provider": [
        {
            "id": "2044634230826205185",
            "name": "BIG-IP APM",
            "enabled": true,
            "issuer": "https://apm.example.com",
            "jwks_uri": "https://apm.example.com/f5-oauth2/v1/jwks",
            "audience": "fudo",
            "username_claim": "preferred_username",
            "header": "X-JWT-Assertion",
            "created_at": "2026-08-06 10:58:29.657182-07",
            "modified_at": "2026-08-06 10:58:29.657182-07"
        }
    ]
}
```


Note

The `keys` attribute is expensive to use and is not returned unless it is requested explicitly. Refer to *Get Cached Signing Keys*.

1.51.4 Get JWT Provider Details

Retrieve details of a specific JWT provider.

Request

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

GET /api/v2/jwt_provider/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/jwt_provider/2044634230826205185'
```

Response


```
{
    "result": "success",
    "jwt_provider": {
        "id": "2044634230826205185",
        "name": "BIG-IP APM",
        "enabled": true,
        "issuer": "https://apm.example.com",
```


(continues on next page)

(continued from previous page)

```
        "jwks_uri": "https://apm.example.com/f5-oauth2/v1/jwks",
        "audience": "fudo",
        "username_claim": "preferred_username",
        "header": "X-JWT-Assertion",
        "created_at": "2026-08-06 10:58:29.657182-07",
        "modified_at": "2026-08-06 10:58:29.657182-07"
    }
}
```

1.51.5 Get Cached Signing Keys

Retrieve the signing keys currently cached for a provider. The `keys` attribute is expensive to use, so it is returned only when it is requested explicitly.

Request

Method	`GET`
Path	`/api/v2/jwt_provider/<id>?fields=id,name,keys_updated_at,keys`

GET /api/v2/jwt_provider/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/jwt_provider/20446342308262051 85?fields=id,name,
↪keys_updated_at,keys'
```

Response

```
{
    "result": "success",
    "jwt_provider": {
        "id": "2044634230826205185",
        "name": "BIG-IP APM",
        "keys_updated_at": "2026-08-07 01:32:33.169214-07",
        "keys": [
            {
                "alg": "RS256",
                "kid": "b6dd51e66d36010bd3bbdfb3c91a1a5f6ec6c12c",
                "kty": "RSA",
                "public_key": "-----BEGIN PUBLIC KEY-----\
↪nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A...\n-----END PUBLIC KEY-----\n"
            }
        ]
    }
}
```

Note

An empty `keys` array together with an empty `keys_updated_at` means that no key has been fetched yet. Refer to the events log for the reason.

1.51.6 Create JWT Provider

Add a new JWT provider configuration.

Request

Method	`POST`
Path	`/api/v2/jwt_provider`
Headers	`Content-Type: application/json`
Body	`JWTProviderModel`

POST /api/v2/jwt_provider

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "BIG-IP APM",
    "enabled": true,
    "issuer": "https://apm.example.com",
    "audience": "fudo",
    "jwks_uri": "https://apm.example.com/f5-oauth2/v1/jwks",
    "header": "X-JWT-Assertion",
    "username_claim": "preferred_username"
  }' \
  'https://10.33.2.132/api/v2/jwt_provider'
```

Success Response

```
{
    "result": "success",
    "jwt_provider": {
        "id": "2044634230826205185"
    }
}
```

Failure Response

```
{
    "result": "failure",
    "message": "Issuer must start with https://.",
    "failing_attributes": [
        "issuer"
```

(continues on next page)

(continued from previous page)

```
    ]
}
```

1.51.7 Update JWT Provider

Modify an existing JWT provider configuration.

Request

Method	`PATCH`
Path	`/api/v2/jwt_provider/<id>`
Headers	`Content-Type: application/json`
Body	`Partial JWTProviderModel`

PATCH /api/v2/jwt_provider/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "audience": "fudo-uag"
  }' \
  'https://10.33.2.132/api/v2/jwt_provider/2044634230826205185'
```

Response

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

1.51.8 Refresh Signing Keys

Fetch the signing keys of all configured JWT providers again, for example after an issuer has rotated them. Keys are fetched by every cluster node on its own.

Request

Method	`POST`
Path	`/api/v2/jwt_provider/refresh_keys`

POST /api/v2/jwt_provider/refresh_keys

Note

This endpoint takes no request body. A request that carries one is rejected with `Request body is not allowed for this endpoint.`

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/jwt_provider/refresh_keys'
```

Response

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

Note

The response confirms that the refresh has been started, not that the keys have been fetched. When an issuer cannot be reached, the failure is recorded in the events log and the `keys_updated_at` attribute of that provider stays unchanged.

1.51.9 Delete JWT Provider

Remove a JWT provider configuration.

Request

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

DELETE /api/v2/jwt_provider/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/jwt_provider/2044634230826205185'
```

Response

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

1.52 User Directory

Fudo Enterprise features automatic users synchronization service which enables importing users information from Active Directory servers or other servers compatible with the LDAP protocol.

1.52.1 User Directory Configuration

Data Structures

Table 136: `UserDirectoryModel`

Attribute	Type	Required	Description
`id`	string		Read-only, unique object identifier.
`name`	string	yes	Case-insensitive, unique name.
`type`	string {`AD`, `LDAP`}; default value `AD`	yes	Immutable.
`position`	number		Unique.
`username`	string	yes	Unique.
`password`	string	yes	Protected.
`dn`	string	yes	
`base_user`	string		
`base_group`	string		
`user_domain`	string		
`user_filter`	string; default value `(&(objectclass=user))`	yes	
`group_filter`	string; default value `(&(objectclass=group))`		
`server_lastupdate`	string		Timestamp.
`db_lastupdate`	string		Timestamp.
`login_field`	string; default value `sAMAccountName`	yes	
`mail_field`	string; default value `mail`		
`memberof_field`	string; default value `memberOf`	yes	
`telephone_field`	string; default value `telephoneNumber`		
`company_field`	string; default value `company`		
`displayname_field`	string; default value `displayName`	yes	
`dn_field`	string; default value `distinguishedName`	yes	
`certificate_field`	string; default value `userCertificate`	yes	
`guid_field`	string; default value `objectGUID`	yes	
`auto_block`	boolean; default value `true`	yes	
`x509_certificate_metho`	boolean; default value `false`	yes	
`x509_sshkey_method`	boolean; default value `false`	yes	
`created_at`	datetime		Read-only. Timestamp of creation.

continues on next page

Table 136 – continued from previous page

Attribute	Type	Required	Description
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *UserDirectoryModel*

Request

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

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

Get Existing User Directory Configurations

Request

Method	`GET`
Path	`/api/v2/user_directory`

GET /api/v2/user_directory

Example Request

```
curl -s -k -X GET \
-H 'Authorization: <token>' \
'https://10.0.214.98/api/v2/user_directory'
```

Response

```
{
    "result": "success",
    "user_directory": [
        {
            "id": "9115285645797883905",
            "name": "active-directory-10.0.100.100",
            "type": "AD",
            "position": 0,
            "username": "Administrator",
            "dn": "ad.com",
            "base_user": "dc=ad,dc=com",
            "base_group": "dc=ad,dc=com",
            "user_domain": "fudo-ad.com",
            "user_filter": "(&(objectclass=user))",
            "group_filter": "(&(objectclass=group))",
            "login_field": "sAMAccountName",
```

(continues on next page)

(continued from previous page)

```
            "mail_field": "mail",
            "memberof_field": "memberOf",
            "telephone_field": "telephoneNumber",
            "company_field": "company",
            "displayname_field": "displayName",
            "dn_field": "distinguishedName",
            "certificate_field": "userCertificate",
            "guid_field": "objectGUID",
            "auto_block": true,
            "x509_certificate_method": false,
            "x509_sshkey_method": false,
            "created_at": "2025-05-05 04:51:54.021816-07",
            "modified_at": "2025-05-05 04:51:54.021816-07"
        }
    ]
}
```

Get Existing User Directory Configuration by ID

Request

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

GET /api/v2/user_directory/<id>

Example Request

```
curl -s -k -X GET \
-H 'Authorization: <token>' \
'https://10.0.214.98/api/v2/user_directory/801640733671948289'
```

Response

```
{
    "result": "success",
    "user_directory": {
        "id": "9115285645797883908",
        "name": "ldap-10.0.200.100 [domain: ldap.com]",
        "type": "LDAP",
        "position": 3,
        "username": "cn=admin,dc=ldap,dc=com",
        "dn": "cn=admin,dc=ldap,dc=com",
        "base_user": "dc=ldap,dc=com",
        "base_group": "dc=ldap,dc=com",
        "user_domain": "ldap.com",
        "user_filter": "(objectClass=inetOrgPerson)",
        "group_filter": "(objectClass=groupOfNames)",
        "login_field": "uid",
```

(continues on next page)

(continued from previous page)

```
        "mail_field": "mail",
        "memberof_field": "memberOf",
        "telephone_field": "telephoneNumber",
        "company_field": "o",
        "displayname_field": "displayName",
        "dn_field": "dn",
        "certificate_field": "userCertificate",
        "guid_field": "dn",
        "auto_block": true,
        "x509_certificate_method": false,
        "x509_sshkey_method": false,
        "created_at": "2025-05-05 04:51:54.039467-07",
        "modified_at": "2025-05-05 05:00:18.099246-07"
    }
}
```

Defining User Directory Configuration

Request

Method	`POST`
Path	`/api/v2/user_directory`
Headers	`Content-Type: Application/json`
Body	`UserDirectoryModel`

POST /api/v2/user_directory

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  https://10.31.135.179/api/v2/user_directory \
  -d '{
    "name": "ldap-10.0.100.200 [domain: ldap.com]",
    "type": "LDAP",
    "position": 3,
    "username": "cn=admin,dc=ldap,dc=com",
    "password": "password",
    "dn": "cn=admin,dc=ldap,dc=com",
    "base_user": "dc=ldap,dc=com",
    "base_group": "dc=ldap,dc=com",
    "user_domain": "ldap.com",
    "user_filter": "(objectClass=inetOrgPerson)",
    "group_filter": "(objectClass=groupOfNames)",
    "login_field": "uid",
    "mail_field": "mail",
    "memberof_field": "memberOf",
    "telephone_field": "telephoneNumber",
```

(continues on next page)

(continued from previous page)

```
    "company_field": "o",
    "displayname_field": "displayName",
    "dn_field": "dn",
    "certificate_field": "userCertificate",
    "guid_field": "dn"
  }'
```

Response

```
{
    "result": "success",
    "user_directory": {
        "id": "9115285645797883909"
    }
}
```

Modify User Directory Configuration

Request

Method	`PATCH`
Path	`/api/v2/user_directory/<id>`
Headers	`Content-Type: Application/json`
Body	`UserDirectoryModel`

PATCH /api/v2/user_directory/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  https://10.31.135.179/api/v2/user_directory/9115285645797883909 \
  -d '{
    "name":"ldap-other-name",
    "position":5,
    "password":"different"
  }'
```

Response

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

Deleting User Directory Configuration

Request

Method	DELETE
Path	/api/v2/user_directory/<id>

DELETE /api/v2/user_directory/<id>

Example Request

```
curl -s -k -X DELETE \
-H 'Authorization:vg1ei6rgo58fsbobr7octp0w3afd9vsm' \
https://10.31.135.179/api/v2/user_directory/9115285645797883908
```

Response

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

1.52.2 User Directory Controllers

Data Structures

Table 142: UserDirectoryServerModel

Attribute	Type	Required	Description
id	string		Read-only, unique object identifier.
address	string	yes	Case-insensitive. Uniqueness is required in the combination of attribute address with attributes user_directory_id, and port.
port	number {1 - 65535}	yes	Value format: port. Uniqueness is required in the combination of attribute port with attributes address, and user_directory_id.
user_directory_:	string	yes	Uniqueness is required in the combination of attribute user_directory_id with attributes address, and port.
user_directory_r	string		Read-only. Expensive to use.
user_directory_t	string		Read-only. Expensive to use.
tls_enabled	boolean	yes	
tls_certificate	string	if tls_enabl == true	Value format: x509-certificate.
paged_mode	boolean	yes	
created_at	datetime		Read-only. Timestamp of creation.
modified_at	datetime		Read-only. Timestamp of modification.

continues on next page

Table 142 – continued from previous page

Attribute	Type	Required	Description
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *UserDirectoryServerModel*

Request

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

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

Get Existing User Directory Controllers Configuration

Request

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

GET /api/v2/user_directory/server

Example Request

```
curl -s -k -X GET \
-H 'Authorization: <token>' \
'https://10.0.214.98/api/v2/user_directory/server'
```

Response

```
{
    "result": "success",
    "user_directory_server": [
        {
            "id": "9115285645797883905",
            "address": "10.0.200.100",
            "port": 121,
            "user_directory_id": "9115285645797883905",
            "user_directory_name": "active-directory-10.0.200.100 [domain: ad.
↪com]",
            "user_directory_type": "AD",
            "tls_enabled": false,
            "paged_mode": true,
            "created_at": "2025-05-05 04:51:54.027646-07",
            "modified_at": "2025-05-05 04:51:54.027646-07"
        }
    ]
}
```

Get Controllers Configuration by User Directory ID

Request

Method	GET
Path	/api/v2/user_directory/<user_directory_id>/server

GET /api/v2/user_directory/<user_directory_id>/server

Example Request

```
curl -s -k -X GET \
-H 'Authorization:<token>' \
'https://10.31.135.179/api/v2/user_directory/9115285645797883908/server'
```

Response

```
{
    "result": "success",
    "user_directory_server": [
        {
            "id": "9115285645797883905",
            "address": "10.0.200.100",
            "port": 389,
            "user_directory_id": "9115285645797883905",
            "user_directory_name": "active-directory-10.0.200.100 [domain: ad.
↪com]",
            "user_directory_type": "AD",
            "tls_enabled": false,
            "paged_mode": true,
            "created_at": "2025-05-05 04:51:54.027646-07",
            "modified_at": "2025-05-05 04:51:54.027646-07"
        },
        {
            "id": "9115285645797883910",
            "address": "10.0.232.20",
            "port": 389,
            "user_directory_id": "9115285645797883908",
            "user_directory_name": "ldap-10.0.200.100 [domain: ldap.com]",
            "user_directory_type": "LDAP",
            "tls_enabled": false,
            "paged_mode": true,
            "created_at": "2025-05-05 04:51:54.041014-07",
            "modified_at": "2025-05-05 04:51:54.041014-07"
        }
    ]
}
```

Get Controller Configuration by User Directory and Controller ID

Request

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

GET /api/v2/user_directory/<user_directory_id>/server/<id>

Example Request

```
curl -s -k -X GET \
-H 'Authorization:<token>' \
'https://10.31.135.179/api/v2/user_directory/9115285645797883908/server/
↪9115285645797883910'
```

Response

```
{
    "result": "success",
    "user_directory_server": [
        {
            "id": "9115285645797883910",
            "address": "10.0.200.100",
            "port": 389,
            "user_directory_id": "9115285645797883908",
            "user_directory_name": "ldap-10.0.200.100 [domain: ldap.com]",
            "user_directory_type": "LDAP",
            "tls_enabled": false,
            "paged_mode": true,
            "created_at": "2025-05-05 04:51:54.041014-07",
            "modified_at": "2025-05-05 04:51:54.041014-07"
        }
    ]
}
```

Defining Controller Configuration for Specific User Directory

Request

Method	`POST`
Path	`/api/v2/user_directory/<user_directory_id>/server`
Headers	`Content-Type: Application/json`
Body	`UserDirectoryServerModel`

POST /api/v2/user_directory/<id>/server

Example Request

```
curl -s -k -X POST \
-H 'Authorization:<token>' \
```

(continues on next page)

(continued from previous page)

```
https://10.31.135.179/api/v2/user_directory/9115285645797883909/server \
-H 'Content-Type: application/json' -d'{"address":"10.0.200.100","port":122,
↪"tls_enabled":false,"paged_mode":true}'
```

Response

```
{
    "result": "success",
    "user_directory_server": {
        "id": "9115285645797883911"
    }
}
```

Modify Controller Configuration for Specific User Directory

Request

Method	PATCH
Path	/api/v2/user_directory/<user_directory_id>/server/<id>
Headers	Content-Type: Application/json
Body	UserDirectoryServerModel

PATCH /api/v2/user_directory/<user_directory_id>/server/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  https://10.31.135.179/api/v2/user_directory/9115285645797883909/server/
↪9115285645797883911 \
  -d '{
    "tls_enabled": true,
    "tls_certificate": "-----BEGIN CERTIFICATE-----\\nMIID...\\n...REDACTED␣
↪CERTIFICATE DATA...\\n-----END CERTIFICATE-----"
  }'
```

Response

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

Deleting Controller from User Directory Configuration

Request

Method	DELETE

continues on next page

Table 148 – continued from previous page

Path	/api/v2/user_directory/<user_directory_id>/server/<id>

DELETE /api/v2//user_directory/<user_directory_id>/server/<id>

Example Request

```
curl -s -k -X DELETE \
-H 'Authorization:vg1ei6rgo58fsbobr7octp0w3afd9vsm' \
https://10.31.135.179/api/v2/user_directory/9115285645797883908/server/
↪9115285645797883910
```

Response

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

1.52.3 User Directory - Adding Group Mapping

Data Structures

Table 149: UserDirectoryGroupModel

Attribute	Type	Required	Description
id	string		Read-only, unique object identifier.
group_path	string	yes	Uniqueness is required in the combination of attribute group_path with attributes group_guid, and user_directory_id.
group_guid	string	yes	Uniqueness is required in the combination of attribute group_guid with attributes group_path, and user_directory_id.
user_directory_:	string	yes	Uniqueness is required in the combination of attribute user_directory_id with attributes group_path, and group_guid.
user_directory_r	string		Read-only. Expensive to use.
user_directory_1	string		Read-only. Expensive to use.
groups	object-array		Read-only. Expensive to use.
roles	object-array		Read-only. Expensive to use.
external_authen1	object-array		Read-only. Expensive to use.
created_at	datetime		Read-only. Timestamp of creation.
modified_at	datetime		Read-only. Timestamp of modification.
removed	boolean		Read-only.

Retrieve Available Attributes of the *UserDirectoryGroupModel*

Request

Method	GET
Path	/api/v2/objspec/user_directory_group

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

Get Existing User Directory Groups Configuration

Request

Method	GET
Path	/api/v2/user_directory_group

GET /api/v2/user_directory_group

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/user_directory_group'
```

Response

```
{
    "result": "success",
    "user_directory_group": [
        {
            "id": "5683542729741565953",
            "group_path": "CN=Users,CN=Builtin,DC=example,DC=com",
            "group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\B1\\D0\\E3\\02\
↪\71\\BC\\0E",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "groups": [
                {
                    "id": "5683542729741565958",
                    "name": "Group_A",
                    "description": null
                }
            ],
            "roles": [
                {
```

(continues on next page)

(continued from previous page)

```
                    "id": "5683542729741565964",
                    "name": "Server Admin",
                    "description": null
                }
            ],
            "created_at": "2025-06-02 04:02:29.893151-07",
            "modified_at": "2025-06-02 04:02:29.912421-07"
        }
    ]
}
```

Get Group Configuration by ID

Request

Method	GET
Path	/api/v2/user_directory_group/<id>

GET /api/v2/user_directory_group/<id>

Example Request

```
curl -s -k -X GET  \
-H 'Authorization:<token>'  \
'https://10.31.135.179/api/v2/user_directory_group/5683542729741565953'
```

Response

```
{
    "result": "success",
    "user_directory_group": [
        {
            "id": "5683542729741565953",
            "group_path": "CN=Users,CN=Builtin,DC=example,DC=com",
            "group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\B1\\D0\\E3\\02\
↪\71\\BC\\0E",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "groups": [
                {
                    "id": "5683542729741565958",
                    "name": "Group_A",
                    "description": null
                }
            ],
            "roles": [
                {
```

(continues on next page)

(continued from previous page)

```
                    "id": "5683542729741565964",
                    "name": "Server Admin",
                    "description": null
                }
            ],
            "created_at": "2025-06-02 04:02:29.893151-07",
            "modified_at": "2025-06-02 04:02:29.912421-07"
        }
    ]
}
```

Define Group Configuration for Specific User Directory

Request

Method	`POST`
Path	`/api/v2/user_directory_group`
Headers	`Content-Type: Application/json`
Body	`UserDirectoryGroupModel`

POST /api/v2/user_directory_group

Example Request

```
curl -s -k -X POST  \
-H 'Authorization:<token>'  \
-H 'Content-Type: application/json'  \
https://10.31.96.188/api/v2/user_directory_group \
-d'{"group_path":"CN=Guests,CN=Builtin,DC=example,DC=com","group_guid":
↪"2c5804cc-9bbb-46e5-a0b1-d0e30271bc0e","user_directory_id":
↪"5683542729741565954"}'
```

Response

```
{
    "result": "success",
    "user_directory_group": {
        "id": "5683542729741565956"
    }
}
```

Modify Group Configuration for Specific User Directory

Request

Method	`PATCH`
Path	`/api/v2/user_directory_group/<id>`
Headers	`Content-Type: Application/json`

continues on next page

Table 153 – continued from previous page

Body	`UserDirectoryGroupModel`

PATCH /api/v2/user_directory_group/<id>

Example Request

```
curl -s -k -X PATCH  \
-H 'Authorization:<token>'  \
-H 'Content-Type: application/json'  \
https://10.31.96.188/api/v2/user_directory_group/5683542729741565954 \
-d'{"group_path":"CN=Admins,CN=Builtin,DC=example,DC=com"}'
```

Response

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

Deleting Group from User Directory Configuration

Request

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

DELETE /api/v2/user_directory_group/<id>

Example Request

```
curl -s -k -X DELETE  \
-H 'Authorization:vg1ei6rgo58fsbobr7octp0w3afd9vsm'  \
https://10.31.135.179/api/v2/user_directory_group/5683542729741565954
```

Response

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

1.52.4 User Directory - Group Mapping - Adding to Groups

Data Structures

Table 155: `UserDirectoryGroupGroupModel`

Attribute	Type	Required	Description
`id`	string		Read-only, protected, unique object identifier.

continues on next page

Table 155 – continued from previous page

Attribute	Type	Required	Description
user_directory_g	string	yes	Uniqueness is required in the combination of attribute user_directory_group_id with attribute group_id.
group_id	string	yes	Uniqueness is required in the combination of attribute group_id with attribute user_directory_group_id.
user_directory_:	string		Read-only. Expensive to use.
user_directory_r	string		Read-only. Expensive to use.
user_directory_t	string		Read-only. Expensive to use.
group_name	string		Read-only. Expensive to use.
user_directory_g	string		Read-only. Expensive to use.
user_directory_g	string		Read-only. Expensive to use.
created_at	datetime		Read-only. Timestamp of creation.
modified_at	datetime		Read-only. Timestamp of modification.
removed	boolean		Read-only.

Retrieve Available Attributes of the *UserDirectoryGroupGroupModel*

Request

Method	GET
Path	/api/v2/objspec/user_directory_group_group

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

Get Groups Assigned via Group Mapping

Request

Method	GET
Path	/api/v2/user_directory_group/group

GET /api/v2/user_directory_group/group

Example Request

```
curl -s -k -X GET  \
  -H 'Authorization: <token>'  \
  'https://10.0.214.98/api/v2/user_directory_group/group'
```

Response

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

(continues on next page)

(continued from previous page)


```
    "user_directory_group_group": [
        {
            "user_directory_group_id": "5683542729741565954",
            "group_id": "5683542729741565958",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "group_name": "Group_A",
            "user_directory_group_path": "CN=Guests,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-05 03:14:24.316935-07",
            "modified_at": "2025-06-05 03:14:24.316935-07"
        },
        {
            "user_directory_group_id": "5683542729741565953",
            "group_id": "5683542729741565958",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "group_name": "Group_A",
            "user_directory_group_path": "CN=Users,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-02 04:02:29.903779-07",
            "modified_at": "2025-06-02 04:02:29.903779-07"
        }
    ]
}
```


Get Groups Assigned via a Specific Group Mapping

Request

Method	`GET`
Path	`/api/v2/user_directory_group/<user_directory_group_id>/group`

GET /api/v2/user_directory_group/<user_directory_group_id>/group

Example Request

```
curl -s -k -X GET  \
  -H 'Authorization: <token>'  \
  'https://10.0.214.98/api/v2/user_directory_group/5683542729741565954/group'
```

Response

```
{
    "result": "success",
    "user_directory_group_group": [
        {
            "user_directory_group_id": "5683542729741565954",
            "group_id": "5683542729741565958",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "group_name": "Group_A",
            "user_directory_group_path": "CN=Guests,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-05 03:14:24.316935-07",
            "modified_at": "2025-06-05 03:14:24.316935-07"
        }
    ]
}
```


Get Assigned Group by Group Mapping ID and Group ID

Request

Method	GET
Path	/api/v2/user_directory_group/<user_directory_group_id>/group/<group_id>

GET /api/v2/user_directory_group/<user_directory_group_id>/group/<group_id>

Example Request

```
curl -s -k -X GET  \
  -H 'Authorization: <token>'  \
  'https://10.0.214.98/api/v2/user_directory_group/5683542729741565954/group/
↪5683542729741565958'
```

Response


```
{
    "result": "success",
    "user_directory_group_group": [
        {
            "user_directory_group_id": "5683542729741565954",
            "group_id": "5683542729741565958",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
```


(continues on next page)

(continued from previous page)

```
            "group_name": "Group_A",
            "user_directory_group_path": "CN=Guests,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-05 03:14:24.316935-07",
            "modified_at": "2025-06-05 03:14:24.316935-07"
        }
    ]
}
```

Define Group Assigned via Group Mapping

Request

Method	POST
Path	/api/v2/user_directory_group/<user_directory_group_id>/group
Headers	Content-Type: Application/json
Body	UserDirectoryGroupGroupModel

POST /api/v2/user_directory_group/<user_directory_group_id>/group

Example Request

```
curl -s -k -X POST  \
  -H 'Authorization:<token>'  \
  -H 'Content-Type: application/json'  \
  https://10.31.96.188/api/v2/user_directory_group/5683542729741565954/group \
  -d'{"group_id":"5683542729741565959"}'
```

Response

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

Delete Group Assigned via Group Mapping

Request

Method	DELETE
Path	/api/v2/user_directory_group/<user_directory_group_id>/group/<group_id>

DELETE /api/v2/user_directory_group/<user_directory_group_id>/group/<group_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization:vg1ei6rgo58fsbobr7octp0w3afd9vsm' \
  https://10.31.135.179/api/v2/user_directory_group/5683542729741565954/group/
↪5683542729741565959
```

Response

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

1.52.5 User Directory - Group Mapping - Adding to Roles

Data Structures

Table 161: `UserDirectoryGroupRoleModel`

Attribute	Type	Required	Description
`id`	string		Read-only, protected, unique object identifier.
`user_directory_g`	string	yes	Immutable. Uniqueness is required in the combination of attribute `user_directory_group_id` with attribute `role_id`.
`role_id`	string	yes	Uniqueness is required in the combination of attribute `role_id` with attribute `user_directory_group_id`.
`user_directory_:`	string		Read-only. Expensive to use.
`user_directory_r`	string		Read-only. Expensive to use.
`user_directory_t`	string		Read-only. Expensive to use.
`group_name`	string		Read-only. Expensive to use.
`role_name`	string		Read-only. Expensive to use.
`user_directory_g`	string		Read-only. Expensive to use.
`user_directory_g`	string		Read-only. Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *UserDirectoryGroupRoleModel*

Request

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

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

Get Roles Assigned via Group Mapping

Request

Method	GET
Path	/api/v2/user_directory_group/role

GET /api/v2/user_directory_group/role

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/user_directory_group/role'
```

Response


```
{
    "result": "success",
    "user_directory_group_role": [
        {
            "user_directory_group_id": "5683542729741565953",
            "role_id": "5683542729741565964",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "role_name": "Server Admin",
            "user_directory_group_path": "CN=Users,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-02 04:02:29.911793-07",
            "modified_at": "2025-06-02 04:02:29.911793-07"
        }
    ]
}
```


Get Roles Assigned via a Specific Group Mapping

Request

Method	GET
Path	/api/v2/user_directory_group/<user_directory_group_id>/role

GET /api/v2/user_directory_group/<user_directory_group_id>/role

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/user_directory_group/5683542729741565953/role'
```

Response

```
{
    "result": "success",
    "user_directory_group_role": [
        {
            "user_directory_group_id": "5683542729741565953",
            "role_id": "5683542729741565964",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "role_name": "Server Admin",
            "user_directory_group_path": "CN=Users,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-02 04:02:29.911793-07",
            "modified_at": "2025-06-02 04:02:29.911793-07"
        }
    ]
}
```

Get Assigned Role by Group Mapping ID and Role ID

Request

Method	GET
Path	/api/v2/user_directory_group/<user_directory_group_id>/role/<role_id>

GET /api/v2/user_directory_group/<user_directory_group_id>/role/<role_id>

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/user_directory_group/5683542729741565953/role/
↪5683542729741565964'
```

Response

```
{
    "result": "success",
    "user_directory_group_role": [
        {
```

(continues on next page)

(continued from previous page)

```
            "user_directory_group_id": "5683542729741565953",
            "role_id": "5683542729741565964",
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "role_name": "Server Admin",
            "user_directory_group_path": "CN=Users,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-02 04:02:29.911793-07",
            "modified_at": "2025-06-02 04:02:29.911793-07"
        }
    ]
}
```

Define Role Assigned via Group Mapping

Request

Method	`POST`
Path	`/api/v2/user_directory_group/<user_directory_group_id>/role`
Headers	`Content-Type: Application/json`
Body	`UserDirectoryGroupRoleModel`

POST /api/v2/user_directory_group/<user_directory_group_id>/role

Example Request

```
curl -s -k -X POST  \
-H 'Authorization:<token>'  \
-H 'Content-Type: application/json'  \
https://10.31.96.188/api/v2/user_directory_group/5683542729741565954/role \
-d'{"role_id":"5683542729741565966"}'
```

Response

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

Delete Role Assigned via Group Mapping

Request

Method	`DELETE`

continues on next page

Table 166 – continued from previous page

Path	/api/v2/user_directory_group/<user_directory_group_id>/role/<role_id>

DELETE /api/v2/user_directory_group/<user_directory_group_id>/role/<role_id>

Example Request

```
curl -s -k -X DELETE \
-H 'Authorization:<token>' \
https://10.31.96.188/api/v2/user_directory_group/5683542729741565954/role/
↪5683542729741565966
```

Response

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

1.52.6 User Directory - Group Mapping - Assigning External Authentication

Data Structures

Table 167: UserDirectoryGroupAuthenticationModel

Attribute	Type	Required	Description
id	string		Read-only, protected, unique object identifier.
user_directory_g	string	yes	Immutable. Uniqueness is required in the combination of attribute user_directory_group_id with attribute external_authentication_id.
external_authen	string	yes	Immutable. Uniqueness is required in the combination of attribute external_authentication_id with attribute user_directory_group_id.
position	number		Uniqueness is required in the combination of attribute position with attribute user_directory_group_id.
user_directory_:	string		Read-only. Expensive to use.
user_directory_r	string		Read-only. Expensive to use.
user_directory_t	string		Read-only. Expensive to use.
external_authen	string		Read-only. Expensive to use.
external_authen	string		Read-only. Expensive to use.
external_authen	string		Read-only. Expensive to use.
external_authen	number		Read-only. Expensive to use.
user_directory_g	string		Read-only. Expensive to use.
user_directory_g	string		Read-only. Expensive to use.
created_at	datetime		Read-only. Timestamp of creation.

continues on next page

Table 167 – continued from previous page

Attribute	Type	Required	Description
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *UserDirectoryGroupAuthenticationModel*

Request

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

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

Get External Authentication Assigned via Group Mapping

Request

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

GET /api/v2/user_directory_group/external_authentication

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/user_directory_group/external_authentication'
```

Response

```
{
    "result": "success",
    "user_directory_group_authentication": [
        {
            "user_directory_group_id": "5683542729741565954",
            "external_authentication_id": "5683542729741565953",
            "position": 0,
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "external_authentication_name": "AD",
            "external_authentication_type": "ad",
            "user_directory_group_path": "CN=Guests,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "5683542729741565958",
```

(continues on next page)

(continued from previous page)

```
            "created_at": "2025-06-05 08:50:54.599141-07",
            "modified_at": "2025-06-05 08:50:54.615507-07"
        },
        {
            "user_directory_group_id": "5683542729741565953",
            "external_authentication_id": "5683542729741565954",
            "position": 0,
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "external_authentication_name": "LDAP",
            "external_authentication_type": "ldap",
            "external_authentication_address": "10.0.136.1",
            "external_authentication_port": 389,
            "user_directory_group_path": "CN=Users,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-05 08:29:19.462607-07",
            "modified_at": "2025-06-05 08:51:05.932288-07"
        }
    ]
}
```

Get External Authentication Assigned via a Specific Group Mapping

Request

Method	`GET`
Path	`/api/v2/user_directory_group/<user_directory_group_id>/external_authentication`

GET /api/v2/user_directory_group/<user_directory_group_id>/ external_authentication

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/user_directory_group/5683542729741565953/external_
↪authentication'
```

Response

```
{
    "result": "success",
    "user_directory_group_authentication": [
        {
            "user_directory_group_id": "5683542729741565953",
```

(continues on next page)

(continued from previous page)

```
            "external_authentication_id": "5683542729741565954",
            "position": 0,
            "user_directory_id": "5683542729741565954",
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "external_authentication_name": "LDAP",
            "external_authentication_type": "ldap",
            "external_authentication_address": "10.0.136.1",
            "external_authentication_port": 389,
            "user_directory_group_path": "CN=Users,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-05 08:29:19.462607-07",
            "modified_at": "2025-06-05 08:51:05.932288-07"
        }
    ]
}
```

Get Assigned External Authentication by Group Mapping ID and External Authentication ID

Request

Method	GET
Path	/api/v2/user_directory_group/<user_directory_group_id>/external_authentication/<external_authentication_id>

GET /api/v2/user_directory_group/<user_directory_group_id>/external_authentication/<external_authentication_id>

Example Request

```
curl -s -k -X GET  \
-H 'Authorization: <token>'  \
'https://10.0.214.98/api/v2/user_directory_group/5683542729741565953/external_
↪authentication/5683542729741565954'
```

Response

```
{
    "result": "success",
    "user_directory_group_authentication": [
        {
            "user_directory_group_id": "5683542729741565953",
            "external_authentication_id": "5683542729741565954",
            "position": 0,
            "user_directory_id": "5683542729741565954",
```

(continues on next page)

(continued from previous page)


```
            "user_directory_name": "active-directory-10.0.242.80 [domain:␣
↪example.com]",
            "user_directory_type": "AD",
            "external_authentication_name": "LDAP",
            "external_authentication_type": "ldap",
            "external_authentication_address": "10.0.136.1",
            "external_authentication_port": 389,
            "user_directory_group_path": "CN=Users,CN=Builtin,DC=example,DC=com
↪",
            "user_directory_group_guid": "\\CC\\04\\58\\2C\\BB\\9B\\E5\\46\\A0\\
↪B1\\D0\\E3\\02\\71\\BC\\0E",
            "created_at": "2025-06-05 08:29:19.462607-07",
            "modified_at": "2025-06-05 08:51:05.932288-07"
        }
    ]
}
```


Define External Authentication Assigned via Group Mapping

Request

Method	`POST`
Path	`/api/v2/user_directory_group/<user_directory_group_id>/external_authentication`
Headers	`Content-Type: Application/json`
Body	`UserDirectoryGroupAuthenticationModel`

POST /api/v2/user_directory_group/<user_directory_group_id>/ external_authentication

Example Request

```
curl -s -k -X POST  \
-H 'Authorization:<token>'  \
-H 'Content-Type: application/json'  \
https://10.31.96.188/api/v2/user_directory_group/5683542729741565954/external_
↪authentication \
-d'{"external_authentication_id":"5683542729741565953"}'
```

Response


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


Edit External Authentication Assigned via Group Mapping

Request

Method	PATCH
Path	/api/v2/user_directory_group/<user_directory_group_id>/external_authentication
Headers	Content-Type: Application/json
Body	UserDirectoryGroupAuthenticationModel

PATCH /api/v2/user_directory_group/<user_directory_group_id>/external_authentication

Example Request

```
curl -s -k -X PATCH  \
-H 'Authorization:<token>'  \
-H 'Content-Type: application/json'  \
https://10.31.96.188/api/v2/user_directory_group/5683542729741565954/external_
↪authentication \
-d'{"external_authentication_id":"5683542729741565953"}'
```

Response

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

Delete External Authentication Assigned via Group Mapping

Request

Method	DELETE
Path	/api/v2/user_directory_group/<user_directory_group_id>/external_authentication/<external_authentication_id>

DELETE /api/v2/user_directory_group/<user_directory_group_id>/external_authentication/<external_authentication_id>

Example Request

```
curl -s -k -X DELETE \
-H 'Authorization:<token>' \
https://10.31.96.188/api/v2/user_directory_group/5683542729741565954/external_
↪authentication/5683542729741565953
```

Response

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

1.52.7 User Directory Synchronization Status

Data Structures

Table 174: `UserDirectoryEnableModel`

Attribute	Type	Required	Description
`enabled`	boolean; default value `AD`	yes	Enable User Directory synchronization.
`node`	string	yes	Synchronization is performed on node with given serial number.
`current_node`	boolean		Read-only. Synchronization is performed on current node.

Retrieve Available Attributes of the *UserDirectoryEnableModel*

Request

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

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

Get User Directory Synchronization Status

Request

Method	`GET`
Path	`/api/v2/user_directory/enable`

GET /api/v2/user_directory/enable

Example Request

```
curl -s -k -X GET \
-H 'Authorization:vg1ei6rgo58fsbobr7octp0w3afd9vsm' \
https://10.31.135.179/api/v2/user_directory/enable'
```

Response

```
{
    "enabled": true,
    "node": "86496998",
    "current_node": true,
    "result": "success"
}
```

Enable/Disable User Directory Synchronization

Request

Method	PATCH
Path	/api/v2/user_directory/enable
Headers	Content-Type: Application/json
Body	UserDirectoryEnableModel

PATCH /api/v2/user_directory/enable

Example Request

```
curl -s -k -X PATCH \
-H 'Authorization:vg1ei6rgo58fsbobr7octp0w3afd9vsm' \
https://10.31.135.179/api/v2/user_directory/enable -H 'Content-Type:␣
↪application/json' -d'{"enabled":true}'
```

Response

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

Force Full Synchronization

Request

Method	PATCH
Path	/api/v2/user_directory/<user_directory_id>/force_full_sync

PATCH /api/v2/user_directory/<user_directory_id>/force_full_sync

Example Request

```
curl -s -k -X POST \
-H 'Authorization:vg1ei6rgo58fsbobr7octp0w3afd9vsm' \
https://10.31.135.179/api/v2/user_directory/9115285645797883908/force_full_sync
```

Response

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

1.53 Remote Applications

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

1.53.1 Data Structures

Table 179: `RemoteApplicationsModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`name`	string	yes	Case-insensitive. Uniqueness is required.
`password_changer_id`	string	yes	Password changer identifier assigned to remote app. Uniqueness is required.
`path`	string	yes	
`arguments`	string		
`variables`	object-array		
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.53.2 Retrieve Available Attributes of the *RemoteApplicationsModel*

Request

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

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

1.53.3 Get Remote Applications Definitions List

Request

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

Example Request

GET /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"
    },
    {
```

(continues on next page)

(continued from previous page)

```
        "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" }]
```

1.53.4 Get Remote Applications Definitions List by ID

Request

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

Example Request

GET /api/v2/remote_app/<id>`

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

1.53.5 Defining Remote Applications Definition

Request

Method	`POST`
Path	`/api/v2/remote_app`
Headers	`Content-Type: Application/json`
Body	`RemoteApplicationsModel`

Example Request

POST /api/v2/remote_app`

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/remote_app' \
  -d'{"name":"Putty","password_changer_id":"9115285645797883914","path":"C:\\
↪Windows\\System32\\putty.exe"}'
```

Response

```
{
    "remote_app": {
        "id": "9115285645797883916",
        "name": "Putty",
        "path": "C:\\Windows\\System32\\putty.exe",
        "arguments": null,
        "variables": null,
        "password_changer_id": "9115285645797883916"
    },
    "result": "success"
}
```


1.53.6 Modify Remote Applications Definition

Request

Method	`PATCH`
Path	`/api/v2/remote_app/<id>`
Headers	`Content-Type: Application/json`
Body	`RemoteApplicationsModel`

Example Request

PATCH /api/v2/remote_app/<id>`

```
curl -s -k -X PATCH -H 'Authorization:<token>' https://10.31.135.179/api/v2/
↪remote_app/9115285645797883916 -H 'Content-Type: application/json' -d'{"name":
↪"Putty","path":"C:\\Windows\\System32\\putty_ext.exe"}'
```

Response


```
{
    "remote_app": {
        "id": null,
        "name": "Putty",
        "path": "C:\\Windows\\System32\\putty_ext.exe",
        "arguments": null,
        "variables": null,
        "password_changer_id": null
    },
    "result": "success"
}
```


1.53.7 Deleting a Remote Application Definition

Request

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

1.54 Reverse Proxy

Reverse proxy functionality in Fudo Enterprise allows for secure tunneling and redirection of connections. Reverse proxies can be configured with listeners to handle incoming connections and forward them to remote destinations, providing an additional layer of security and access control.

1.54.1 Reverse Proxy

Data Structures

Table 180: `ReverseProxyModel`

Attribute	Type	Required	Description
`id`	string		Read-only, unique reverse proxy identifier.
`name`	string	yes	Unique reverse proxy name (case-insensitive).
`address`	string	yes	Target address for SSH connection.
`port`	number	yes	SSH host port.
`bind_ip`	string	yes	Local bind address for outgoing connection.
`ssh_public_key`	string		Destination host SSH public key.
`user_login`	string	yes	User to log in as on the remote machine.
`user_private_k`	string	yes	Protected. SSH private key for authentication.
`user_public_ke`	string		Read-only; expensive to use. Public key derived from `user_private_key`.
`uag_address`	string		Remote address used to redirect to UAG.
`uag_port`	number		Remote port used to redirect to UAG.
`last_status`	string {running, degraded, dead, offline}		Read-only. Current connection status.
`last_status_at`	datetime		Read-only. Timestamp of last status update.
`enabled`	boolean	yes	Whether reverse proxy is enabled (default: false).
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *ReverseProxyModel*

Request

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

To check allowed methods, available URL parameters and possible responses please refer to the

API Overview section.

List Reverse Proxies

Request

Method	GET
Path	/api/v2/reverse_proxy

GET /api/v2/reverse_proxy

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/reverse_proxy'
```

Response


```
{
    "result": "success",
    "reverse_proxy": [
        {
            "id": "8754997675608244225",
            "name": "Development SSH Tunnel",
            "address": "192.168.20.100",
            "port": 22,
            "bind_ip": "10.0.2.50",
            "user_login": "dev_tunnel",
            "last_status": "offline",
            "last_status_at": "2026-04-17 01:14:15.686819-07",
            "enabled": true,
            "created_at": "2026-04-17 01:14:15.690472-07",
            "modified_at": "2026-04-17 01:14:15.690472-07",
            "user_public_key": "ssh-ed25519␣
↪AAAAC3NzaC1lZDI1NTE5AAAAIP5n2dVOPlO6DP9uObCxdd9FlNlMFdV6pN87UOAVxdmd"
        }
    ]
}
```


Get Reverse Proxy by ID

Request

Method	GET
Path	/api/v2/reverse_proxy/<id>

GET /api/v2/reverse_proxy/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/reverse_proxy/8754997675608244225'
```

Response


```
{
    "result": "success",
    "reverse_proxy": [
        {
            "id": "8754997675608244225",
            "name": "Development SSH Tunnel",
            "address": "192.168.20.100",
            "port": 22,
            "bind_ip": "10.0.2.50",
            "user_login": "dev_tunnel",
            "last_status": "offline",
            "last_status_at": "2026-04-17 01:14:15.686819-07",
            "enabled": true,
            "created_at": "2026-04-17 01:14:15.690472-07",
            "modified_at": "2026-04-17 01:14:15.690472-07",
            "user_public_key": "ssh-ed25519␣
↪AAAAC3NzaC1lZDI1NTE5AAAAIP5n2dVOPlO6DP9uObCxdd9FlNlMFdV6pN87UOAVxdmd"
        }
    ]
}
```


Create Reverse Proxy

Request

Method	`POST`
Path	`/api/v2/reverse_proxy`
Body	JSON object with reverse proxy parameters

POST /api/v2/reverse_proxy

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "Development SSH Tunnel",
    "address": "192.168.20.100",
    "port": 22,
    "bind_ip": "10.0.2.50",
    "user_login": "dev_tunnel",
    "user_private_key": "-----BEGIN OPENSSH PRIVATE KEY-----\n...\n-----END␣
↪OPENSSH PRIVATE KEY-----",
```

(continues on next page)

(continued from previous page)

```
    "enabled": true
  }' \
  'https://10.31.135.179/api/v2/reverse_proxy'
```

Response

```
{
    "result": "success",
    "reverse_proxy": {
        "id": "8754997675608244225"
    }
}
```

Update Reverse Proxy

Request

Method	`PATCH`
Path	`/api/v2/reverse_proxy/<id>`
Body	JSON object with updated reverse proxy parameters

PATCH /api/v2/reverse_proxy/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "enabled": false,
    "uag_address": "192.168.30.10",
    "uag_port": 8443
  }' \
  'https://10.31.135.179/api/v2/reverse_proxy/8754997675608244225'
```

Response

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

Delete Reverse Proxy

Request

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

DELETE /api/v2/reverse_proxy/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/reverse_proxy/8754997675608244225'
```

Response

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

1.54.2 Reverse Proxy Listeners

Data Structures

Table 181: `ReverseProxyListenerModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique reverse proxy listener identifier.
`reverse_proxy_`	string	yes	Reverse proxy identifier.
`remote_address`	string	yes	Remote address for connection forwarding. Uniqueness is required in the combination of attribute `remote_address` with attribute `remote_port`.
`remote_port`	number	yes	Value-format: port. Remote port for connection forwarding. Uniqueness is required in the combination of attribute `remote_port` with attribute `remote_address`.
`listener_id`	string		Associated listener identifier.
`listener_name`	string		Read-only. Name of the associated listener.
`listener_addre`	string		Read-only. Address of the associated listener.
`listener_port`	number		Read-only. Value-format: port. Port of the associated listener.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

Retrieve Available Attributes of the *ReverseProxyListenerModel*

Request

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

List Listeners for Reverse Proxy

Request

Method	GET
Path	/api/v2/reverse_proxy/<reverse_proxy_id>/listener

GET /api/v2/reverse_proxy/<reverse_proxy_id>/listener

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/reverse_proxy/8754997675608244225/listener'
```

Response

```
{
    "result": "success",
    "reverse_proxy_listener": [
        {
            "id": "8754997675608244226",
            "reverse_proxy_id": "8754997675608244225",
            "remote_address": "192.168.100.20",
            "remote_port": 5432,
            "listener_id": "8754997675608244225",
            "listener_name": "SSH:bastion",
            "listener_address": "0.0.0.0",
            "listener_port": 22,
            "created_at": "2026-04-17 02:13:09.558896-07",
            "modified_at": "2026-04-17 02:13:09.558896-07"
        }
    ]
}
```

Add Listener to Reverse Proxy

Request

Method	POST
Path	/api/v2/reverse_proxy/<reverse_proxy_id>/listener
Body	JSON object with listener parameters

POST /api/v2/reverse_proxy/<reverse_proxy_id>/listener

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
```

(continues on next page)

(continued from previous page)

```
    "remote_address": "192.168.100.20",
    "remote_port": 5432,
    "listener_id": "8754997675608244225"
  }' \
  'https://10.31.135.179/api/v2/reverse_proxy/8754997675608244225/listener'
```

Response

```
{
    "result": "success",
    "reverse_proxy_listener": {
        "id": "8754997675608244226"
    }
}
```

Remove Listener from Reverse Proxy

Request

Method	DELETE
Path	/api/v2/reverse_proxy/<reverse_proxy_id>/listener/<reverse_proxy_listener_id>

DELETE /api/v2/reverse_proxy/<reverse_proxy_id>/listener/<reverse_proxy_listener_id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.135.179/api/v2/reverse_proxy/8754997675608244225/listener/
↪8754997675608244225'
```

Response

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

1.55 External Storage

Fudo Enterprise enables management of external storage devices via fiber channel cards.

1.55.1 Data Structures

Table 182: `ExternalStorageModel`

Attribute	Type	Required	Description
`interface_stat`	object-array		Fiber channel cards status. Read-only.
`external_wwns`	object-array		List of available external storage devices. Read-only.
`connection_mod`	string	yes	Fiber channel cards operating mode. Possible values: `failover`, `loadbalancer`.
`wwn_to_configu`	string		WWN of selected external storage device to configure.
`current_storag`	string		WWN of configured external storage device. Read-only.
`is_configured`	boolean		Is external storage configured? Read-only.
`occupancy`	object		Occupancy of configured external storage device: allocated, capacity, free, size. Read-only.

1.55.2 Retrieve Available Attributes of the *ExternalStorageModel*

Request

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

GET /api/v2/objspec/external_storage

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.124.76/api/v2/objspec/external_storage'
```

1.55.3 Get External Storage Information

Request

Method	`GET`
Path	`/api/v2/external_storage`

GET /api/v2/external_storage

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.124.76/api/v2/external_storage'
```

1.55.4 Get Specific External Storage Device

Request

Method	GET
Path	/api/v2/external_storage/<id>

GET /api/v2/external_storage/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.31.124.76/api/v2/external_storage/5620492334958379016'
```

1.55.5 Configure External Storage

Request

Method	POST
Path	/api/v2/external_storage
Headers	Content-Type: Application/json
Body	ExternalStorageModel

POST /api/v2/external_storage

Example Request

```
curl -s -k -X POST \
     -H 'Authorization: <token>' \
         -H 'Content-Type: application/json' \
         -d '{"connection_mode": "failover", "wwn_to_configure":
↪"50:01:43:80:03:6f:8e:a0"}' \
     'https://10.31.124.76/api/v2/external_storage'
```

1.55.6 Delete External Storage Configuration

Request

Method	DELETE
Path	/api/v2/external_storage/<id>

DELETE /api/v2/external_storage/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.31.124.76/api/v2/external_storage/5620492334958379016'
```

1.56 LLM Providers NEW

An LLM provider is the large language model endpoint that AI session analysis runs on. Analysis agents reference a provider through their `provider_id` attribute; an agent without a provider does not run.

1.56.1 Data Structures

Table 183: `LlmProviderModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`name`	string	yes	Provider name. Case-insensitive. Uniqueness is required.
`provider`	string {anthropic, ollama, openai}	yes	Provider kind the URL speaks.
`url`	string	If `provider` == `ollama`	Endpoint URL. Empty means the provider's canonical SaaS endpoint.
`model`	string	yes	Model name requested from the provider.
`api_key`	string		API key used to authenticate against the provider. Protected; write-only - it is never returned by `GET`.
`temperature`	string		Sampling temperature between 0 and 2. Empty means the provider's default.
`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.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.56.2 Retrieve Available Attributes of the *LlmProviderModel*

Request

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

GET /api/v2/objspec/llm_provider

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/objspec/llm_provider'
```

1.56.3 List LLM Providers

Request

Method	GET
Path	/api/v2/llm_provider

GET /api/v2/llm_provider

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/llm_provider'
```

Response


```
{
    "result": "success",
    "llm_provider": [
        {
            "id": "4638707616191610881",
            "name": "Local Ollama",
            "provider": "ollama",
            "url": "https://llm.example.com:11434",
            "model": "llama3.1:8b",
            "temperature": "0.2",
            "builtin": false,
            "hidden": false,
            "created_at": "2026-08-18 02:16:42.250842-07",
            "modified_at": "2026-08-18 02:16:42.250842-07"
        }
    ]
}
```


1.56.4 Get an LLM Provider

Request

Method	GET
Path	/api/v2/llm_provider/<id>

GET /api/v2/llm_provider/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/llm_provider/4638707616191610881'
```

Response

```
{
    "result": "success",
    "llm_provider": {
        "id": "4638707616191610881",
        "name": "Local Ollama",
        "provider": "ollama",
        "url": "https://llm.example.com:11434",
        "model": "llama3.1:8b",
        "temperature": "0.2",
        "builtin": false,
        "hidden": false,
        "created_at": "2026-08-18 02:16:42.250842-07",
        "modified_at": "2026-08-18 02:16:42.250842-07"
    }
}
```


1.56.5 Create an LLM Provider

Request

Method	POST
Path	/api/v2/llm_provider
Body	LlmProviderModel

POST /api/v2/llm_provider

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"name":"Local Ollama","provider":"ollama","url":"https://llm.example.
↪com:11434","model":"llama3.1:8b","temperature":"0.2"}' \
  'https://10.33.3.191/api/v2/llm_provider'
```

Response


```
{
    "result": "success",
    "llm_provider": {
        "id": "4638707616191610881"
    }
}
```


1.56.6 Modify an LLM Provider

Request

Method	PATCH
Path	/api/v2/llm_provider/<id>
Body	LlmProviderModel

PATCH /api/v2/llm_provider/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"model":"llama3.1:70b","temperature":"0.1"}' \
  'https://10.33.3.191/api/v2/llm_provider/4638707616191610881'
```

Response

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

1.56.7 Delete an LLM Provider

Request

Method	DELETE
Path	/api/v2/llm_provider/<id>

DELETE /api/v2/llm_provider/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.33.3.191/api/v2/llm_provider/4638707616191610881'
```

Response

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

1.57 External Password Repository

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

1.57.1 Data Structures

Table 184: `PassvnModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Uniqueness is required.
`name`	string	yes	Case-insensitive. Uniqueness is required.
`url`	string	yes	
`type`	string {azure_key cyberark, laps, thycotic, vault}	yes	Immutable.
`login`	string	if `type` == `laps` || `thycotic`	
`secret`	string	if `type` == `azure_key_v` || `laps` || `thycotic` || `vault`	Protected.
`tls_certificate`	string		Format: `x509-certificate`.
`cyberark_application_id`	string	if `type` == `cyberark`	
`cyberark_safe`	string	if `type` == `cyberark`	
`thycotic_secret_fmt`	string	if `type` == `thycotic`	
`base_dn`	string	if `type` == `laps`	
`azure_tenant_uuid`	string	if `type` == `azure_key_v`	
`azure_client_uuid`	string	if `type` == `azure_key_v`	
`azure_secret_name_fmt`	string	if `type` == `azure_key_v`	Default: `%U`.
`identity_certificate`	string		Format: `x509-certificate`.
`identity_key`	string		Protected. Format: `private-key`.
`identity_key_passphrase`	string	if `identity_ke` is set	Passphrase to use to decrypt private key. Protected.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.57.2 Retrieve Available Attributes of the *PassvnModel*

Request

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

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

1.57.3 Create External Password Repository

Request

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

Example Request

POST /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"
    }
}
```

1.57.4 Get External Password Repositories List

Request

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

Example Request

GET /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"
    }
]
```


1.57.5 Get Information About External Password Repository by ID

Request

Method	GET
Path	/api/v2/passvn/<id>

Example Request

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

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"
    }
]
```


1.57.6 Delete an External Password Repository Definition

Request

Method	DELETE
Path	/api/v2/passvn/<id>

1.57.7 Changing External Password Repository Configuration

Request

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

Example Request

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

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

Response

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

1.58 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`.

1.58.1 Data Structures

Table 185: `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.

continues on next page

Table 185 – continued from previous page

Batch operation element	Possible values / Request variant	Description
	`params`	Include optional URL parameters.
	`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`.

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

1.59 Create Batch Operation

Request

Method	`POST`
Path	`/api/v2/batch`
Headers	`Content-Type: application/json`
Body	`BatchModel`

POST /api/v2/batch

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"
      }
    },
    "request1": {
      "method": "DELETE",
      "endpoint": "/user/{responses.request0.user[0].id}"
    },
```

(continues on next page)

(continued from previous page)

```
    "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,
```

(continues on next page)

(continued from previous page)

```
            "user_authentication_method": {
                "id": "8511803295730237489"
            }
        }
    }
}
```

1.60 Create 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,
```

(continues on next page)

(continued from previous page)

```
            "user": {
                "id": "8511803295730237446"
            }
        },
        "user_auth": {
            "result": "success",
            "status-code": 201,
            "user_authentication_method": {
                "id": "8511803295730237442"
            }
        }
    }
}
```

1.60.1 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,
            "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"
            }
        }
    }
}
```

1.61 Backup

Fudo allows configuring multiple backup target destinations, where data can be stored. Each backup target can have S3, Backblaze, FTP, or SFTP as a destination place.

1.61.1 Data Structures

Table 186: `BackupModel`

Attribute	Type	Required	Description
`id`	string		Unique and read-only object Identifier
`name`	string	yes	Unique, case insensitive object name
`type`	string {backblaze, ftp, s3, sftp}	yes	Immutable, case insensitive
`backblaze_buck`	string	If `type` == `backblaze`	Backblaze bucket name.
`backblaze_dire`	string	If `type` == `backblaze`	Directory within the Backblaze bucket.
`backblaze_keyi`	string	If `type` == `backblaze`	Backblaze key ID.

continues on next page

Table 186 – continued from previous page

Attribute	Type	Required	Description
backblaze_appl	string	If type == backblaze	Protected. Backblaze application key.
ftp_address	string	If type == ftp	FTP server address.
ftp_username	string	If type == ftp	FTP login username.
ftp_password	string	If type == ftp & ftp_usern provided	Protected. FTP password.
ftp_directory	string	If type == ftp	Target directory on the FTP server.
s3_bucket	string	If type == s3	S3 bucket name.
s3_directory	string	If type == s3	Directory within the S3 bucket.
s3_access_key_	string	If type == s3	AWS access key ID.
s3_secret_acce	string	If type == s3	Protected. AWS secret access key.
s3_endpoint	string	If type == s3	Custom S3 endpoint URL.
s3_region	string	If type == s3	AWS region name.
sftp_address	string	If type == sftp	SFTP server address.
sftp_port	number; default value 22	If type == sftp	SFTP server port.
sftp_username	string	If type == sftp	SFTP login username.
sftp_userkey	string	If type == sftp	Protected. User SSH private key.
sftp_userkey_p	string	If sftp_user provided	Protected. Passphrase to decrypt user SSH private key.
sftp_directory	string	If type == sftp	Directory on the SFTP server.
sftp_serverkey	string	If type == sftp	Protected. SFTP server SSH public key.
created_at	datetime		Read-only. Creation timestamp.
modified_at	datetime		Read-only. Modification timestamp.
session_replic	number		Read-only. Hidden. Expensive to use.
removed	boolean		Read-only.

1.61.2 Retrieve Available Attributes of the *BackupModel*

Request

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

GET /api/v2/objspec/backup

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/backup'
```

1.62 Create Backup Target

Request

Method	`POST`
Path	`/api/v2/backup`
Headers	`Content-Type: application/json`
Body	`BackupModel`

Example Request

POST /api/v2/backup

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/backup' \
  -d'{"name": "FTP_Backup","type": "ftp","ftp_address": "10.0.130.100"}'
```

Response

```
{
    "result": "success",
    "backup": {
        "id": "8016407336719482 90"
    }
}
```

1.63 Get Backup Definitions List

Request

Method	`GET`
Path	`/api/v2/backup`

Example Request

GET /api/v2/backup


```
"result": "success",
"backup": [
    {
        "id": "9124292845052624897",
        "name": "FTP_Backup",
        "type": "ftp",
        "path": "",
        "created_at": "2024-06-16 13:50:42.355762-07",
        "modified_at": "2024-06-16 14:29:47.217872-07"
    },
    {
        "id": "9124292845052624898",
        "name": "Backblaze_Backup",
        "type": "backblaze",
        "path": "myBucket\/",
        "created_at": "2024-06-16 14:29:47.226305-07",
        "modified_at": "2024-06-16 14:29:47.226305-07"
    }
]
```


1.64 Get a Backup Definition by ID

Request

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

GET /api/v2/backup/<id>

1.65 Assign Backup Definition to Session

Request

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

POST /api/v2/session/<session_id>/backup/<backup_id>

1.66 Delete Backup Definition

Request

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

DELETE /api/v2/backup/<id>

1.67 Upgrade

1.67.1 Data Structures

Table 187: `UpgradeModel`

Attribute	Type	Required	Description
`version`	string		The version provided by the upgrade package. Read-only.
`size`	number		Upgrade package size, in bytes. Read-only.
`upgrade_check_`	string {`never`, `running`, `success`, `failure`}	yes	Status of the upgrade check. Read-only.
`estimated_upgr`	number		Estimated upgrade time in seconds. Available after successful upgrade check. Read-only.
`has_upgrade_sn`	boolean	yes	Indicates whether an upgrade snapshot is available. Read-only.
`upgrade_runnin`	boolean	yes	True if an upgrade is in progress. Read-only.

1.67.2 Retrieve Available Attributes of the *UpgradeModel*

Request

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

GET /api/v2/objspec/upgrade_info

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/upgrade_info'
```

1.67.3 Upload the Upgrade File

Request

Method	`POST`
Path	`/api/v2/upgrade/upload`
Headers	`Content-Type: multipart/form-data` (set automatically by curl when using -F)
Body	File uploaded using the `file` form field

POST /api/v2/upgrade/upload

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -F 'file=@/path/to/fudo-5.6.0.upg' \
  'https://10.0.214.98/api/v2/upgrade/upload'
```

Response

```
```

1.67.4 Get Uploaded Upgrade Information

Request

Method	GET
Path	/api/v2/upgrade

GET /api/v2/upgrade

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/upgrade'
```

Response

```
{
    "upgrade": {
        "version": "5.6.3",
        "size": 857056256,
        "upgrade_check_status": "success",
        "estimated_upgrade_time": 300,
        "has_upgrade_snapshot": false,
        "upgrade_running": false
    },
    "result": "success"
}
```

1.67.5 Run the Upgrade Check

Request

Method	POST
Path	/api/v2/upgrade/check/run

POST /api/v2/upgrade/check/run

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/upgrade/check/run'
```

Response

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

1.67.6 Cancel the Upgrade Check

Request

Method	POST
Path	/api/v2/upgrade/check/cancel

POST /api/v2/upgrade/check/cancel

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/upgrade/check/cancel'
```

Response

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

1.67.7 Get the Upgrade Check Log

Request

Method	GET
Path	/api/v2/upgrade/check/log

GET /api/v2/upgrade/check/log

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/upgrade/check/log'
```

Response

```
Starting upgrade check.
waiting for server to start....2025-05-13 18:45:37.590 CEST (pid=97795) (user=)␣
```

(continues on next page)

(continued from previous page)

```
↪(app=) LOG:  redirecting log output to logging collector process
2025-05-13 18:45:37.590 CEST (pid=97795) (user=) (app=) HINT:  Future log␣
↪output will appear in directory "pg_log".
 done
server started
New upgrade script: UPG000754.
Upgrade UPG000754 started at 2025-05-13 09:45:42.
Upgrade UPG000754 completed successfully at 2025-05-13 09:45:43.
New upgrade script: UPG000756.
Upgrade UPG000756 started at 2025-05-13 09:45:43.
Upgrade UPG000756 completed successfully at 2025-05-13 09:45:43.
2025-05-13 18:45:37.590 CEST (pid=97795) (user=) (app=) LOG:  starting␣
↪PostgreSQL 16.2 on amd64-portbld-freebsd12.3, compiled by FreeBSD clang␣
↪version 10.0.1 (git@github.com:llvm/llvm-project.git llvmorg-10.0.1-0-
↪gef32c611aa2), 64-bit
2025-05-13 18:45:37.591 CEST (pid=97795) (user=) (app=) LOG:  listening on Unix␣
↪socket "/data/local/upgcheck/run/.s.PGSQL.5432"
2025-05-13 18:45:37.603 CEST (pid=97868) (user=) (app=) LOG:  database system␣
↪was interrupted; last known up at 2025-05-13 18:39:28 CEST
2025-05-13 18:45:37.652 CEST (pid=97868) (user=) (app=) LOG:  database system␣
↪was not properly shut down; automatic recovery in progress
2025-05-13 18:45:37.654 CEST (pid=97868) (user=) (app=) LOG:  redo starts at 0/
↪3B429E8
2025-05-13 18:45:37.663 CEST (pid=97868) (user=) (app=) LOG:  invalid record␣
↪length at 0/3BCE9B0: expected at least 24, got 0
2025-05-13 18:45:37.663 CEST (pid=97868) (user=) (app=) LOG:  redo done at 0/
↪3BCE978 system usage: CPU: user: 0.00 s, system: 0.00 s, elapsed: 0.00 s
2025-05-13 18:45:37.665 CEST (pid=97847) (user=) (app=) LOG:  checkpoint␣
↪starting: end-of-recovery immediate wait
2025-05-13 18:45:37.673 CEST (pid=97847) (user=) (app=) LOG:  checkpoint␣
↪complete: wrote 116 buffers (0.7%); 0 WAL file(s) added, 0 removed, 0␣
↪recycled; write=0.007 s, sync=0.001 s, total=0.008 s; sync files=72,␣
↪longest=0.001 s, average=0.001 s; distance=559 kB, estimate=559 kB; lsn=0/
↪3BCE9B0, redo lsn=0/3BCE9B0
2025-05-13 18:45:37.688 CEST (pid=97795) (user=) (app=) LOG:  database system␣
↪is ready to accept connections
Upgrade check finished successfully. Duration 1 seconds.
```

1.67.8 Run the Upgrade

Request

Method	`POST`
Path	`/api/v2/upgrade/run`

POST /api/v2/upgrade/run

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/upgrade/run'
```

Response

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

Note

After running the `upgrade/run` request, the operation may take some time to complete. Please wait patiently while the upgrade is being processed.

1.67.9 Delete Upgrade

Request

Method	`DELETE`
Path	`/api/v2/upgrade`

DELETE /api/v2/upgrade

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/upgrade'
```

Response

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

1.67.10 Delete Upgrade Snapshot

Request

Method	`DELETE`
Path	`/api/v2/upgrade/snapshot`

DELETE /api/v2/upgrade/snapshot

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/upgrade/snapshot'
```

Response

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

1.68 Hotfix

1.68.1 Upload the Hotfix File

Request

Method	`POST`
Path	`/api/v2/hotfix/upload`
Headers	`Content-Type: application/octet-stream`
Body	Raw hotfix file content sent as binary data
Authentication	Authenticated web session (`sessionid` cookie) with CSRF protection

POST /api/v2/hotfix/upload

Example Request

```
curl -sk -X POST 'https://10.31.118.184/api/v2/hotfix/upload' \
  -H 'Content-Type: application/octet-stream' \
  -H 'Origin: https://10.31.118.184' \
  -H 'Referer: https://10.31.118.184/settings/system/hotfix' \
  -H 'X-CSRFToken: <csrf_token>' \
  -H 'Cookie: sessionid=<session_id>; csrftoken=<csrf_token>' \
  --data-binary '@/path/to/hotfix_file.fshf'
```

Response

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

Note

This endpoint requires an authenticated web session and CSRF protection. Token-based authorization using the `Authorization` header is not sufficient.

1.68.2 Get Uploaded Hotfix Information

Request

Method	`GET`
Path	`/api/v2/hotfix`

GET /api/v2/hotfix

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/hotfix'
```

Response

```
{
    "result": "success",
    "hotfix": [
        {
            "name": "hotfix_name_5.6.3",
            "description": "Hotfix for ...",
            "installed": null
        }
    ]
}
```

1.68.3 Install the Hotfix

Request

Method	`POST`
Path	`/api/v2/hotfix/install/<name>`
Headers	`Authorization: <token>`
Body	Not required

POST /api/v2/hotfix/install/<name>

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.31.118.184/api/v2/hotfix/install/hotfix_name_5.6.3'
```

Response

```
{
    "result": "success",
    "output": "Running preinstall script.\nStopping pmonitord.\nWaiting for␣
↪PIDS: 49368.\nStopping fudod.\nWaiting for PIDS: 44506.\nRunning postinstall␣
↪script.\nStarting fudod.\nStarting pmonitord.\n"
}
```

Note

The `output` field contains the execution log of the hotfix installation process, including pre-installation and post-installation steps.

1.68.4 Delete Uploaded Hotfix File

Request

Method	`DELETE`
Path	`/api/v2/hotfix/<name>`

DELETE /api/v2/hotfix/<name>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/hotfix/hotfix_name_5.6.3'
```

Response

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

Note

The names of uploaded hotfixes can be retrieved using the `GET /api/v2/hotfix` endpoint.

1.69 License

1.69.1 Data Structures

Table 188: `LicenseModel`

Attribute	Type	Required	Description
`serial`	string		Read-only. License serial number.
`fuid`	string		Read-only. License fuid identifier.
`expiration_dat`	string	yes	Read-only. Specifies the license validity period. Format: `YYYY-MM-DD` / `unlimited`. Deprecated, use `psm_expiration_date` instead.
`expired`	boolean	yes	Read-only. License has expired? Deprecated, use `psm_expired` instead.
`psm_expiration`	string	yes	Read-only. Specifies the license validity period for the PSM module. Format: `YYYY-MM-DD` / `unlimited`.
`psm_expired`	boolean	yes	Read-only. License has expired for the PSM Module?
`vault_expirati`	string		Read-only. Specifies the license validity period for the Vault module. Format: `YYYY-MM-DD` / `unlimited`.
`vault_expired`	boolean		Read-only. License has expired for the Vault Module?
`support_expira`	string		Read-only. Specifies the license support end date. Format: YYYY-MM-DD.
`support_state`	string {active, expiring, expired, unknown}	yes	Read-only. Status of support based on support expiration date.
`support_expire`	number		Read-only. Number of days until customer support expires. 0 means today is last day.
`owner`	string	yes	Read-only. Specifies the name of the entity to which the license is issued.
`type`	string {commercial, test}	yes	Read-only. Specifies the type of license. The value can be set to `test` for test purposes or to `commercial` for commercial use.
`tier`	string {basic, full}	yes	Read-only. License tier.
`nodes`	string		Read-only. Limit how many nodes can be configured. Format: a positive integer or `unlimited`.
`servers`	string		Read-only. Limit how many servers can be configured. Format: a positive integer or `unlimited`.
`activeusers`	string		Read-only. The limit of active users. Format: a positive integer or `unlimited`. Deprecated, use `psm_activeusers` instead.
`psm_activeuser`	string		Read-only. The limit of active users is defined in the license for the PSM module. Number of users or `unlimited` for an infinite user limit.
`vault_activeus`	string		Read-only. The limit of active users is defined in the license for the Vault module. Number of users or `unlimited` for an infinite user limit.
`changers`	string		Read-only. The number of accounts and secrets that can have an assigned secret changer. For-

1.69.2 Retrieve Available Attributes of the *LicenseModel*

Request

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

GET /api/v2/objspec/license

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/license'
```

1.69.3 Data Structures

Table 189: `LicenseUploadModel`

Attribute	Type	Required	Description
`license`	string	yes	License file.

1.69.4 Retrieve Available Attributes of the *LicenseUploadModel*

Request

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

GET /api/v2/objspec/license_upload

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/license_upload'
```

1.69.5 Get License Information

Request

Method	`GET`
Path	`/api/v2/license`

GET /api/v2/license

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/license'
```

Response


```
{
    "license": {
        "serial": "80840259",
        "expiration_date": "2026-07-08",
        "expired": false,
        "psm_expiration_date": "2026-07-08",
        "psm_expired": false,
        "vault_expiration_date": "2026-09-08",
        "vault_expired": false,
        "support_expiration_date": "2026-07-08",
        "support_state": "expiring",
        "support_expires_in_days": 28,
        "owner": "Fudo Security",
        "type": "commercial",
        "tier": "full",
        "nodes": "3",
        "servers": "100",
        "activeusers": "50",
        "psm_activeusers": "50",
        "vault_activeusers": "99",
        "changers": "9",
        "servers_inuse": 2,
        "activeusers_inuse": 11,
        "psm_activeusers_inuse": 11,
        "vault_activeusers_inuse": 1,
        "changers_inuse": 0
    },
    "result"
         "success"
}
```


1.69.6 Upload the License

Request

Method	`POST`
Path	`/api/v2/license`
Headers	`Content-Type: Application/json`
Body	`LicenseUploadModel`

POST /api/v2/license

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/license' \
  -d '{
    "license": "serial=33333333
servers=5000
changers=400
expire=20271231
mode=host
procmaxocr=15
license type: commercial
type=test
owner=FudoSecurity
nodes=8
languages=en,pl
key=NTXXXXXXXXXXXXXXXXXXXXXXXXXXXX...<truncated>
signature=dTJOftdo2i4ykvXUYTDnijSy...<truncated>"
}'
```

Response

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

1.69.7 Delete Uploaded License File

Request

Method	DELETE
Path	/api/v2/license

DELETE /api/v2/license

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.31.135.179/api/v2/license'
```

Response

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

1.70 Exporting/Importing System Configuration

Warning

The endpoints described in this section belong to the `/internal` API group and may change without prior notice. These interfaces are intended for internal use and are not guaranteed to be stable between releases.

For more details refer to the *API BETA Endpoints* section.

1.70.1 Data Structures

Table 190: `ConfigurationModel`

Attribute	Type	Required	Description
`master_key`	string	yes	Base64 encode master key file content.
`configuration`	string	yes	Configuration file content.

1.70.2 Retrieve Available Attributes of the *ConfigurationModel*

Request

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

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

1.70.3 Exporting the Master Key

Note

Exporting the Master Key requires a certificate, which will be used to encrypt the exported key data.

Request

Method	`GET`
Path	`/api/v2/internal/masterkey/export`

GET /api/v2/internal/masterkey/export

```
curl -s -k -X GET \
        -H 'Authorization: <token>' \
        'https://10.0.214.98/api/v2/internal/masterkey/export' \
     -d '{
           "certificate": "-----BEGIN CERTIFICATE-----\nMIIC...snip...\n-----
```

(continues on next page)

(continued from previous page)

```
↪END CERTIFICATE-----\n"
        }'
```

1.70.4 Exporting System Configuration

Request

Method	GET
Path	/api/v2/internal/configuration/export

GET /api/v2/internal/configuration/export

The following example downloads the configuration to a file named `fudo_config.conf`.

Example Request

```
curl -s -k -X GET \
-H 'Authorization: <token>' \
'https://10.0.214.98/api/v2/internal/configuration/export' \
-o fudo_config.conf
```

1.70.5 Importing System Configuration

Request

Method	POST
Path	/api/v2/internal/configuration/import
Headers	Content-Type: Application/json
Body	ConfigurationModel

POST /api/v2/internal/configuration/import

Example Request

```
curl -s -k -X POST \
-H 'Authorization:<token>' \
'https://10.31.135.179/api/v2/internal/configuration/import' \
-H 'Content-Type: application/json' \
-d '{"master_key":"<base64 masterkey decrypted>","configuration": "<sql file␣
↪content>"}'
```

Response

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

1.71 Hardware Security Module NEW

Fudo Enterprise can keep the key that encrypts its master key (the KEK) inside a hardware security module instead of on disk. The module is reached through a PKCS#11 library supplied in an uploaded bundle; enrollment generates the KEK on the token and switches the system to HSM master-key mode.

1.71.1 Data Structures

Table 194: `HsmModel`

Attribute	Type	Required	Description
`enabled`	boolean		Read-only. Whether HSM master-key mode is active.
`module`	string		PKCS#11 module path relative to the uploaded bundle. Must not start with a slash.
`token_label`	string		PKCS#11 token label.
`key_label`	string		Read-only. Label of the KEK generated during enrollment.
`env`	object		Module environment. A map sent on `PATCH` replaces the whole map.
`pin`	string		Token PIN. Write-only and protected - never returned by `GET`. An empty string inherits the currently active PIN.
`test_only`	boolean		Dry run: validate the configuration without committing it. See the note below.

Table 195: `HsmStatusModel`

Attribute	Type	Required	Description
`enabled`	boolean		Read-only. Whether HSM master-key mode is active.
`healthy`	boolean		Read-only. The whole chain works: module loaded, token found, login accepted, exactly one KEK present.
`error`	string		Read-only. Diagnosis of the failing step. `null` when healthy.
`token_label`	string		Read-only. Token label reported by the HSM.
`token_manufactu`	string		Read-only. Token manufacturer.
`token_model`	string		Read-only. Token model.
`token_serial`	string		Read-only. Token serial number.
`firmware_versio`	string		Read-only. Token firmware version.
`pin_locked`	boolean		Read-only. Login is blocked until the PIN is reset.
`pin_expired`	boolean		Read-only. PIN is expired; cryptographic operations fail until it is changed.
`fingerprint`	string		Read-only. KEK fingerprint, comparable across cluster nodes.

Table 196: `HsmBundleModel`

Attribute	Type	Required	Description
`modules`	string-array		Read-only. PKCS#11 module (`.so`) paths in the active bundle.
`filename`	string		Read-only. Original upload filename of the active bundle.
`uploaded_at`	datetime		Read-only. RFC3339 time the active bundle was uploaded.

1.71.2 Retrieve Available Attributes

Request

Method	`GET`
Path	`/api/v2/objspec/hsm`, `/api/v2/objspec/hsm_status`, `/api/v2/objspec/hsm_bundle`

GET /api/v2/objspec/hsm

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.36.9.188/api/v2/objspec/hsm'
```

1.71.3 Get the HSM Configuration

Request

Method	`GET`
Path	`/api/v2/hsm`

GET /api/v2/hsm

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.36.9.188/api/v2/hsm'
```

Response

```
{
    "enabled": true,
    "module": "module.so",
    "token_label": "soft-hsm",
    "key_label": "fudo-kek-masterkey",
    "env": {
```

(continues on next page)

(continued from previous page)

```
        "PKCS11_PROXY_SOCKET": "tcp://10.0.100.37:2345"
    },
    "result": "success"
}
```

When HSM mode is off, the configuration is reported empty:

```
{
    "enabled": false,
    "module": null,
    "token_label": null,
    "key_label": null,
    "env": {},
    "result": "success"
}
```

1.71.4 Get the HSM Status

Request

Method	GET
Path	/api/v2/hsm/status

GET /api/v2/hsm/status

Runs the whole chain - load the module, find the token, log in, count the KEKs - and reports where it stops.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.36.9.188/api/v2/hsm/status'
```

Response

```
{
    "enabled": true,
    "healthy": true,
    "error": null,
    "token_label": "soft-hsm",
    "token_manufacturer": "SoftHSM project",
    "token_model": "SoftHSM v2",
    "token_serial": "bf5f6cb03dd72192",
    "firmware_version": "2.7",
    "pin_locked": false,
    "pin_expired": false,
    "fingerprint":
↪"61cf4f0c9721171647bc56af0f85dd4c851542339c12e3bb765408c70164f0b1",
```

(continues on next page)

(continued from previous page)

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

When the chain breaks, `healthy` is `false`, `error` carries the diagnosis and the token details are `null`:

```
{
    "enabled": true,
    "healthy": false,
    "error": "HSM unavailable: C_Initialize: Function::Initialize: PKCS11␣
↪error: Some problem has occurred with the token and/or slot.",
    "token_label": null,
    "token_manufacturer": null,
    "token_model": null,
    "token_serial": null,
    "firmware_version": null,
    "pin_locked": null,
    "pin_expired": null,
    "fingerprint": null,
    "result": "success"
}
```

Note

Compare `fingerprint` across cluster nodes to confirm they all reached the same KEK.

1.71.5 Test or Commit an HSM Configuration

Request

Method	`PATCH`
Path	`/api/v2/hsm`
Body	`HsmModel`

PATCH /api/v2/hsm

This endpoint both validates and enrolls, and it answers with an `HsmStatusModel` rather than a plain result:

- `test_only` set to `true` is a dry run. The configuration is exercised against the token and the outcome reported, but the live configuration is left untouched. The `enabled` field of the result describes the staged configuration, not the running one, so it reads `false`.
- `test_only` set to `false` commits: it enrolls the configuration, generates a KEK on the token, activates any bundle staged with `POST /api/v2/hsm/bundle` and switches Fudo Enterprise to HSM master-key mode.

Warning

Test the configuration with `test_only` set to `true` before committing it. A dry run is the only way to find a wrong token label or an unreachable module without changing the running system.

Example Request

Dry run:

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"module":"module.so","token_label":"soft-hsm","env":{"PKCS11_PROXY_SOCKET
↪":"tcp://10.0.100.37:2345"},"pin":"","test_only":true}' \
  'https://10.36.9.188/api/v2/hsm'
```

Response

```
{
    "enabled": false,
    "healthy": true,
    "error": null,
    "token_label": "soft-hsm",
    "token_manufacturer": "SoftHSM project",
    "token_model": "SoftHSM v2",
    "token_serial": "bf5f6cb03dd72192",
    "firmware_version": "2.7",
    "pin_locked": false,
    "pin_expired": false,
    "fingerprint":
↪"61cf4f0c9721171647bc56af0f85dd4c851542339c12e3bb765408c70164f0b1",
    "result": "success"
}
```

A dry run that cannot reach the token reports the reason and changes nothing:

```
{
    "enabled": false,
    "healthy": false,
    "error": "no token labelled 'does-not-exist'",
    "result": "success"
}
```

Example Request

Commit the configuration:

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{"module":"module.so","token_label":"soft-hsm","env":{"PKCS11_PROXY_SOCKET
↪":"tcp://10.0.100.37:2345"},"pin":"<token PIN>","test_only":false}' \
  'https://10.36.9.188/api/v2/hsm'
```

Response


```
{
    "enabled": true,
    "healthy": true,
    "error": null,
    "token_label": "soft-hsm",
    "token_manufacturer": "SoftHSM project",
    "token_model": "SoftHSM v2",
    "token_serial": "bf5f6cb03dd72192",
    "firmware_version": "2.7",
    "pin_locked": false,
    "pin_expired": false,
    "fingerprint": null,
    "result": "success"
}
```


Note

`fingerprint` is `null` in the enrollment response because the KEK is still being created. Read `GET /api/v2/hsm/status` afterwards to obtain it.

Sending `pin` as an empty string reuses the PIN already in effect, which is what you want when changing only the module path or the environment of a working configuration.

1.71.6 Get the Active Bundle

Request

Method	`GET`
Path	`/api/v2/hsm/bundle/active`

GET /api/v2/hsm/bundle/active

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.36.9.188/api/v2/hsm/bundle/active'
```

Response


```
{
    "modules": [
        "module.so"
    ],
    "filename": "libpkcs11-proxy.so",
    "uploaded_at": "2026-08-14T07:54:35.811133402+00:00",
    "result": "success"
}
```

1.71.7 Upload a PKCS#11 Bundle

Request

Method	`POST`
Path	`/api/v2/hsm/bundle`
Body	Raw file bytes

POST /api/v2/hsm/bundle

The bundle carries the vendor PKCS#11 library and whatever it needs alongside it. The file name is supplied in the `X-Fudo-Filename` header and the body is the raw file.

> **Warning**
>
> The upload only **stages** the bundle - `GET /api/v2/hsm/bundle/active` keeps reporting the previous one. The staged bundle becomes active when a configuration is committed with `PATCH /api/v2/hsm` and `test_only` set to `false`.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'X-Fudo-Filename: libpkcs11-proxy.so' \
  -H 'Content-Type: application/octet-stream' \
  --data-binary '@libpkcs11-proxy.so' \
  'https://10.36.9.188/api/v2/hsm/bundle'
```

Response

The response describes the staged bundle and, unlike other endpoints, carries no `result` field.

```
{
    "modules": [
        "module.so"
    ],
    "filename": "libpkcs11-proxy.so",
    "uploaded_at": "2026-08-18T15:55:14.422743725+00:00"
}
```

1.71.8 Rotate the Key Encryption Key

Request

Method	`POST`
Path	`/api/v2/hsm/rotate-kek`

POST /api/v2/hsm/rotate-kek

Generates a new KEK on the token and re-wraps the master key with it. The answer is an `HsmStatusModel` carrying the new fingerprint; `key_label` reported by `GET /api/v2/hsm` changes

as well.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.36.9.188/api/v2/hsm/rotate-kek'
```

Response


```
{
    "enabled": true,
    "healthy": true,
    "error": null,
    "token_label": "soft-hsm",
    "token_manufacturer": "SoftHSM project",
    "token_model": "SoftHSM v2",
    "token_serial": "bf5f6cb03dd72192",
    "firmware_version": "2.7",
    "pin_locked": false,
    "pin_expired": false,
    "fingerprint":
↪"e774d21cb5d1c478cf4d2cce5d0f1bea1fe1e5e3dca1b9afd1726e2fd82c8611",
    "result": "success"
}
```


Note

In this example the fingerprint moved from `61cf4f0c9721171647bc56af0f85dd4c851542339c12e3bb765408c7` to the value above, and `key_label` moved from `fudo-kek-masterkey` to `fudo-kek-d2b0e2e7c8b0d11a`. On a cluster, read the status on every node afterwards and confirm the fingerprints match again.

1.71.9 Disable HSM Master-Key Mode

Request

Method	`DELETE`
Path	`/api/v2/hsm`

DELETE /api/v2/hsm

Switches Fudo Enterprise back to keeping the master key without the module and clears the stored configuration - `module`, `token_label`, `key_label` and `env` are all reset.

Warning

The PIN is cleared together with the rest of the configuration. Turning HSM mode back on is a full enrollment: it needs the token PIN again and it generates a **new** KEK, so the fingerprint after re-enrollment differs from the one before.

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  'https://10.36.9.188/api/v2/hsm'
```

Response

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

1.72 Network

Fudo Enterprise allows retrieving network settings within its API.

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

1.72.1 Data Structures

Table 197: `NetworkModel`

Attribute	Type	Description
`hostname`	string	System hostname
`dns`	address	DNS address(es)
`search`	string	Domain search path
`management`	address	Admin Panel's address
`access_gateway`	address	Access Gateway's address
`labels`	string	Global configuration parameters
`interfaces`	object-array	Network interfaces configuration containing: • `name`, • `ether`, • `active`, • `use_dhcp`, • `routing_table`, • `inet`
`routing`	object	Routing configuration containing: • `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)

1.73 Get Network Settings

Request

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

GET /api/v2/network

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

1.74 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*.

1.74.1 Get Healthcheck Status

Request

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

Example Request

GET /api/v2/healthcheck`

Response - positive

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

Response - negative

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

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

1.75 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 and list 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.

1.75.1 Get Status Information

Request

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

Example Request

GET /api/v2/status`

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

1.76 IPMI

> **Note**
>
> This feature is available only if the device's IPMI port is use.

1.76.1 Data Structures

Table 198: `IPMIModel`

Attribute	Type	Required	Description
`host`	string	yes	Format: IPv4 address (e.g. `192.168.0.1`).
`mask`	number	yes	Value range: from `0` to `32`."
`gateway`	string	yes	Format: IPv4 address (e.g. `192.168.0.1`).

1.76.2 Retrieve Available Attributes of the *IPMIModel*

Request

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

GET /api/v2/objspec/ipmi

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/ipmi'
```

1.76.3 Get IPMI Configuration Setup

Request

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

GET /api/v2/network/ipmi

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/network/ipmi'
```

Response

```
{
    "ipmi": {
        "host": "192.168.1.100",
        "mask": 24,
        "gateway": "192.168.1.1"
    },
    "result": "success"
}
```

1.76.4 Get the Status of IPMI

Request

Method	`GET`
Path	`/network/ipmi/enabled`

GET /api/v2/network/ipmi/enabled

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/network/ipmi/enabled'
```

Response

```
{
    "ipmi_enabled": false,
    "result": "success"
}
```

1.76.5 Create IPMI Configuration

Request

Method	`POST`
Path	`/api/v2/network/ipmi`
Headers	`Content-Type: Application/json`
Body	`IPMIModel`

POST /api/v2/network/ipmi

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
      -H 'Content-Type: application/json' \
  'https://10.0.214.98/api/v2/network/ipmi' \
      -d'{"host": "192.168.1.100","mask": 24,"gateway": "192.168.1.1"}'
```

Response

```
{
    "ipmi": {
        "host": "192.168.1.100",
        "mask": 24,
        "gateway": "192.168.1.1"
    },
    "result": "success"
}
```

1.77 Disk Probe

Note

When the disk size changes in a virtual machine, the hypervisor typically notifies the guest system about this change, and the system automatically expands the data pool. However, some hypervisors don't provide this notification. The disk probe endpoint allows you to manually trigger a disk scan to detect such changes.

1.77.1 Trigger Disk Scan

Manually initiate a disk scan to detect changes in disk size that weren't automatically detected by the system.

Request

Method	`POST`
Path	`/api/v2/disk-probe`

POST /api/v2/disk-probe

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/disk-probe'
```

Success Response

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

1.78 Dashboard Storage

Note

Dashboard storage endpoints manage the user's dashboard configuration including widget layout, positioning, and settings. The dashboard is customizable per user and persists across sessions.

1.78.1 Data Structures

Widget Types

Available widget types:

- `CONCURRENT_SESSIONS` - Display current concurrent sessions count
- `ACTIVE_USERS` - Show number of active users
- `LICENSE` - License information display
- `NODE` - Node status and information
- `CONCURRENT_SESSIONS_CHART` - Chart showing concurrent sessions over time
- `LOGS` - Recent system logs display
- `SUSPICIOUS_SESSIONS` - ML-detected suspicious sessions counter
- `ACCOUNT_ALERTS` - Account-related alerts counter
- `SECRET_ALERTS` - Password Vault secret alerts counter

Table 199: `WidgetModel`

Attribute	Type	Required	Description
`type`	string	yes	Widget type from available types list.
`x`	number	yes	X position on dashboard grid.
`y`	number	yes	Y position on dashboard grid.
`cols`	number	yes	Width in grid columns.
`rows`	number	yes	Height in grid rows.
`minItemCols`	number		Minimum allowed width in columns.
`minItemRows`	number		Minimum allowed height in rows.
`maxItemCols`	number		Maximum allowed width in columns.
`maxItemRows`	number		Maximum allowed height in rows.
`config`	object	yes	Widget-specific configuration object.

Table 200: `DashboardStorageModel`

Attribut	Type	Required	Description
`value`	object	yes	Dashboard configuration containing widgets array.
`value` `widge`	array	yes	Array of WidgetModel objects defining dashboard layout.
`avai`	array		Read-only. List of widget types available for this user.

1.78.2 Get Dashboard Configuration

Retrieve the current user's dashboard configuration.

Request

Method	GET
Path	/api/v2/dashboard-storage/dashboard

GET /api/v2/dashboard-storage/dashboard

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/dashboard-storage/dashboard'
```

Response


```
{
    "available_widgets": [
        "CONCURRENT_SESSIONS",
        "ACTIVE_USERS",
        "LICENSE",
        "NODE",
        "CONCURRENT_SESSIONS_CHART",
        "LOGS",
        "SUSPICIOUS_SESSIONS",
        "ACCOUNT_ALERTS",
        "SECRET_ALERTS"
    ],
    "value": {
        "widgets": [
            {
                "cols": 3,
                "config": {
                    "fontSize": 48,
                    "link": "/sessions/",
                    "type": "CONCURRENT_SESSIONS"
                },
                "maxItemCols": 5,
                "maxItemRows": 4,
                "minItemCols": 2,
                "minItemRows": 2,
                "rows": 3,
                "type": "CONCURRENT_SESSIONS",
                "x": 0,
                "y": 0
            },
            {
                "cols": 3,
                "config": {
```


(continues on next page)

(continued from previous page)

```
                    "fontSize": 48,
                    "type": "ACTIVE_USERS"
                },
                "maxItemCols": 5,
                "maxItemRows": 4,
                "minItemCols": 2,
                "minItemRows": 2,
                "rows": 3,
                "type": "ACTIVE_USERS",
                "x": 3,
                "y": 0
            }
        ]
    },
    "result": "success"
}
```

1.78.3 Get Widget Defaults

Retrieve default configurations for all available widget types.

Request

Method	GET
Path	/api/v2/dashboard-storage/widget-defaults

GET /api/v2/dashboard-storage/widget-defaults

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.132/api/v2/dashboard-storage/widget-defaults'
```

Response

```
{
    "defaults": [
        {
            "cols": 3,
            "config": {
                "fontSize": 48,
                "link": "/sessions/",
                "type": "CONCURRENT_SESSIONS"
            },
            "maxItemCols": 5,
            "maxItemRows": 4,
            "minItemCols": 2,
            "minItemRows": 2,
            "rows": 3,
```

(continues on next page)

(continued from previous page)


```
            "type": "CONCURRENT_SESSIONS"
        },
        {
            "cols": 3,
            "config": {
                "fontSize": 48,
                "type": "ACTIVE_USERS"
            },
            "maxItemCols": 5,
            "maxItemRows": 4,
            "minItemCols": 2,
            "minItemRows": 2,
            "rows": 3,
            "type": "ACTIVE_USERS"
        },
        {
            "cols": 15,
            "config": {
                "filter": "all",
                "filterName": "all",
                "length": 20,
                "link": "/logs/",
                "showLabel": true,
                "theme": "dark",
                "type": "LOGS"
            },
            "minItemCols": 3,
            "minItemRows": 6,
            "rows": 7,
            "type": "LOGS"
        }
    ],
    "result": "success"
}
```


1.78.4 Update Dashboard Configuration

Modify the current user's dashboard layout and widget configuration.

Request

Method	`PATCH`
Path	`/api/v2/dashboard-storage/dashboard`
Headers	`Content-Type: application/json`
Body	`DashboardStorageModel`

PATCH /api/v2/dashboard-storage/dashboard

Warning

This endpoint replaces the entire dashboard configuration. Make sure to include all widgets you want to keep in the new configuration.

Example Request - Clear Dashboard

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "value": {
        "widgets": []
    }
  }' \
  'https://10.33.2.132/api/v2/dashboard-storage/dashboard'
```

Example Request - Custom Layout

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "value": {
        "widgets": [
            {
                "type": "CONCURRENT_SESSIONS",
                "x": 0,
                "y": 0,
                "cols": 6,
                "rows": 4,
                "config": {
                    "fontSize": 64,
                    "link": "/sessions/",
                    "type": "CONCURRENT_SESSIONS"
                }
            },
            {
                "type": "LOGS",
                "x": 6,
                "y": 0,
                "cols": 9,
                "rows": 8,
                "config": {
                    "filter": "all",
                    "length": 50,
                    "showLabel": true,
                    "theme": "light",
                    "type": "LOGS"
                }
```

(continues on next page)

(continued from previous page)

```
            }
        ]
    }
  }' \
  'https://10.33.2.132/api/v2/dashboard-storage/dashboard'
```

Success Response


```
{
    "available_widgets": [
        "CONCURRENT_SESSIONS",
        "ACTIVE_USERS",
        "LICENSE",
        "NODE",
        "CONCURRENT_SESSIONS_CHART",
        "LOGS",
        "SUSPICIOUS_SESSIONS",
        "ACCOUNT_ALERTS",
        "SECRET_ALERTS"
    ],
    "value": {
        "widgets": [
            {
                "type": "CONCURRENT_SESSIONS",
                "x": 0,
                "y": 0,
                "cols": 6,
                "rows": 4,
                "config": {
                    "fontSize": 64,
                    "link": "/sessions/",
                    "type": "CONCURRENT_SESSIONS"
                }
            },
            {
                "type": "LOGS",
                "x": 6,
                "y": 0,
                "cols": 9,
                "rows": 8,
                "config": {
                    "filter": "all",
                    "length": 50,
                    "showLabel": true,
                    "theme": "light",
                    "type": "LOGS"
                }
            }
        ]
```


(continues on next page)

(continued from previous page)

```
    },
    "result": "success"
}
```

1.79 Authentication Confirmation

1.79.1 Overview

Authentication confirmation endpoints provide mechanisms for confirming and invalidating user authentication methods in Fudo Enterprise. These endpoints support multiple authentication methods including password, challenge-response, and FIDO2.

1.79.2 Data Structures

Table 201: `ConfirmModel`

Attribute	Type	Required	Description
`method`	string {challenge, fido2, password}; Default value `password`	yes	Authentication method.
`assertion`	string	If `method` == `fido2`	FIDO2 assertion response (JSON).
`password`	string	If `method` == `challenge` | `password`	User password or challenge response.
`state`	string	If `method` == `challenge`	State for consecutive authentication steps.

1.79.3 Retrieve Available Attributes of the *ConfirmModel*

Request

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

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

1.79.4 Confirm Authentication Method

Request

Method	`POST`
Path	`/api/v2/profile/authentication/confirm`
Body	`ConfirmModel`

POST /api/v2/profile/authentication/confirm

Example Request - Password Method

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "method": "password",
    "password": "user_password"
  }' \
  'https://10.33.2.133/api/v2/profile/authentication/confirm'
```

Example Request - Multi-Factor Authentication (Challenge Method)

Step 1: Initial authentication with password

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "method": "password",
    "password": "user_password"
  }' \
  'https://10.33.2.133/api/v2/profile/authentication/confirm'
```

Challenge Response (when MFA is configured):

```
{
    "prompt": "One-time password (OATH): ",
    "userid": "5980780305148018689",
    "username": "admin",
    "user-domain": null,
    "methodid": "5980780305148018711",
    "result": "challenge",
    "state": "nIjT2r3nwg3fpPCs0ahFzwZNVrLYZq7HHG4G0bshukar"
}
```

Step 2: Complete authentication with OATH token

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "method": "challenge",
    "password": "579657",
    "state": "nIjT2r3nwg3fpPCs0ahFzwZNVrLYZq7HHG4G0bshukar"
```

(continues on next page)

(continued from previous page)

```
  }' \
  'https://10.33.2.133/api/v2/profile/authentication/confirm'
```

1.79.5 Invalidate Authentication

Request

Method	`POST`
Path	`/api/v2/profile/authentication/invalidate`
Body	`ConfirmModel`

POST /api/v2/profile/authentication/invalidate

Example Request - With Authentication Method

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "method": "password",
    "password": "user_password"
  }' \
  'https://10.33.2.133/api/v2/profile/authentication/invalidate'
```

Response

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

1.80 Profile Authentication Methods Management

1.80.1 Overview

Profile authentication methods endpoints allow users to manage their own authentication methods after successful reauthentication.

Note

These endpoints require an active API session and prior confirmation via the `/profile/authentication/confirm` endpoint which provides a temporary token.

1.80.2 Authentication Flow

1. **Reauthenticate** to obtain a confirmation token
2. **Use the token** in the `X-Auth-Confirm` header for all subsequent operations
3. **Token validity**: 10 minutes, extended with each use

1.80.3 Data Structures

Table 202: `AuthenticationMethodModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique authentication method identifier.
`type`	string {password, oath, extauth, sshkey, certificate, duo, sms, apikey, fido2}	yes	Immutable. Authentication method type.
`user_id`	string		Read-only. Protected. Uniqueness is required in the combination with `position`.
`description`	string		Optional description of the authentication method.
`position`	number		Uniqueness is required in the combination with `user_id`.
`external_sync`	boolean		Read-only.
`secret`	string	If `type` == `password` | `sshkey`	Protected. Authentication secret.
`external_authe`	string	If `type` == `oath` | `extauth`	Read-only; expensive to use. Type of the external authentication backing this method, for example `ad`. The portal uses it to decide whether a password change is offered.
`needs_change`	boolean		Read-only.
`apikey_device_`	string	If `type` == `apikey`	Read-only; expensive to use.
`apikey_device_`	string	If `type` == `apikey`	Read-only; expensive to use.
`apikey_device_`	string	If `type` == `apikey`	Read-only; expensive to use.
`apikey_key`	string	If `type` == `apikey`	Protected.
`apikey_hint`	string	If `type` == `apikey`	Read-only; expensive to use. First four and last four characters of the API key.
`apikey_expires`	datetime	If `type` == `apikey`	Expiration date and time for the API key. NULL means the key never expires.
`certificate_su`	string	If `type` == `certifica`	Read-only.

continues on next page

Table 202 – continued from previous page

Attribute	Type	Required	Description
duo_user_id	string	If type == duo	Read-only.
duo_username	string	If type == duo	Read-only.
oath_type	string {HOTP, TOTP}	If type == oath	Immutable. OATH type.
oath_initializ	boolean	If type == oath	Default value true.
oath_secret	string		Protected. Value-regexp: ^[A-Z2-7]+$
oath_tokenlen	number	If type == oath	Immutable. Value-range: [4, 16].
oath_timestep	number {30, 45, 60, 90, 120, 180, 300}	If type == oath & oath_type == TOTP	Immutable.
oath_counter	number	If type == oath	Read-only. Default value 0.
oath_timeshift	number	If type == oath & oath_type == TOTP	Read-only. Default value 0.
oath_reuse	boolean	If type == oath & oath_type == TOTP	Default value false. Allow reuse of TOTP tokens.
oath_url	string	If type == oath	Read-only. Protected.
oath_qrcode	string	If type == oath	Read-only. Protected.
sms_token	string	If type == sms	Protected.
sshkey_user_pr	boolean	If type == sshkey	Default value true.
sshkey_verific	boolean	If type == sshkey	Default value false.
sshkey_counter	number	If type == sshkey	
sshkey_publick	string	If type == sshkey	Read-only; expensive to use. User's SSH public key.

continues on next page

Table 202 – continued from previous page

Attribute	Type	Required	Description
`fido2_credenti`	string	If `type` == `fido2`	Read-only. Base64url-encoded FIDO2 credential ID.
`fido2_public_k`	string	If `type` == `fido2`	Read-only. Base64url-encoded COSE public key.
`fido2_counter`	number	If `type` == `fido2`	Read-only. Signature counter for clone detection.
`fido2_aaguid`	string	If `type` == `fido2`	Read-only. Authenticator Attestation GUID.
`fido2_transpor`	string	If `type` == `fido2`	Read-only. Supported transports: usb, nfc, ble, internal, hybrid, smart-card.
`created_at`	datetime		Read-only.
`modified_at`	datetime		Read-only.
`removed`	boolean		Read-only.

1.80.4 Retrieve Available Attributes of the *Authentication MethodModel*

Request

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

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

1.80.5 Step 1: Obtain Reauthentication Token

Before accessing authentication methods, you must reauthenticate and obtain a confirmation token.

Request

Method	`POST`
Path	`/api/v2/profile/authentication/confirm`
Body	`ConfirmModel`

Note

See section *Authentication Confirmation* for the list of available *ConfirmModel* attributes.

POST /api/v2/profile/authentication/confirm

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "method": "password",
    "password": "your_password"
  }' \
  'https://10.33.2.133/api/v2/profile/authentication/confirm'
```

Response

```
{
    "userid": "5980780305148018689",
    "username": "admin",
    "user-domain": null,
    "methodid": "5980780305148018690",
    "user-privs": ["account-create", "account-read", ...],
    "result": "success",
    "token": "22d05aff6c39f9de8bdba340c31873edaaa6390dcff30137e91bbe0f23161179"
}
```

Note

Save the `token` value for use in subsequent requests. The token is valid for 10 minutes and its validity is extended with each use.

1.80.6 Step 2: List User's Authentication Methods

Request

Method	`GET`
Path	`/api/v2/profile/authentication`

GET /api/v2/profile/authentication

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  -H 'X-Auth-Confirm:␣
↪22d05aff6c39f9de8bdba340c31873edaaa6390dcff30137e91bbe0f23161179' \
  'https://10.33.2.133/api/v2/profile/authentication'
```

Response

```
{
    "result": "success",
    "authentication_method": [
        {
```

(continues on next page)

(continued from previous page)


```
            "id": "5980780305148018689",
            "type": "password",
            "position": 0,
            "external_sync": false,
            "needs_change": false,
            "created_at": "2026-06-03 12:11:03.338262-07",
            "modified_at": "2026-06-03 12:11:15.629025-07"
        },
        {
            "id": "5980780305148018691",
            "type": "apikey",
            "position": 2,
            "external_sync": false,
            "needs_change": false,
            "created_at": "2026-06-03 12:11:16.0128-07",
            "modified_at": "2026-06-03 12:11:16.0128-07"
        },
        {
            "id": "5980780305148018698",
            "type": "oath",
            "position": 3,
            "external_sync": false,
            "needs_change": false,
            "oath_type": "TOTP",
            "oath_initialized": true,
            "oath_tokenlen": 6,
            "oath_timestep": 30,
            "oath_counter": 0,
            "oath_timeshift": 0,
            "oath_reuse": true,
            "created_at": "2026-06-05 00:37:05.628794-07",
            "modified_at": "2026-06-05 00:37:05.629827-07"
        }
    ]
}
```


1.80.7 Create Authentication Method

Request

Method	`POST`
Path	`/api/v2/profile/authentication`
Body	`AuthenticationMethodModel`

POST /api/v2/profile/authentication

Example Request - Create OATH/TOTP

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'X-Auth-Confirm:␣
↪22d05aff6c39f9de8bdba340c31873edaaa6390dcff30137e91bbe0f23161179' \
  -H 'Content-Type: application/json' \
  -d '{
    "type": "oath",
    "description": "Test OATH TOTP",
    "oath_type": "TOTP",
    "oath_initialized": true,
    "oath_tokenlen": 6,
    "oath_timestep": 30,
    "oath_reuse": false,
    "secret": "JBSWY3DPEHPK3PXP"
  }' \
  'https://10.33.2.133/api/v2/profile/authentication'
```

Response

```
{
    "result": "success",
    "authentication_method": {
        "id": "5980780305148018705",
        "oath_url": "otpauth://totp/admin?
↪secret=XWHOXB6YRLMBPMWM5MG4FUHIHVX3SYSI&issuer=Fudo%20Security",
        "oath_qrcode": "Qk1kbyUy..."
    }
}
```

Note

When creating an OATH method, the response includes `oath_url` for authenticator apps and `oath_qrcode` as a base64-encoded QR code image.

1.80.8 Get Authentication Method by ID

Request

Method	`GET`
Path	`/api/v2/profile/authentication/<id>`

GET /api/v2/profile/authentication/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  -H 'X-Auth-Confirm:␣
```

(continues on next page)

(continued from previous page)

```
↪22d05aff6c39f9de8bdba340c31873edaaa6390dcff30137e91bbe0f23161179' \
  'https://10.33.2.133/api/v2/profile/authentication/5980780305148018705'
```

Response


```
{
    "result": "success",
    "authentication_method": {
        "id": "5980780305148018705",
        "type": "oath",
        "description": "Test OATH TOTP",
        "position": 4,
        "external_sync": false,
        "needs_change": false,
        "oath_type": "TOTP",
        "oath_initialized": true,
        "oath_tokenlen": 6,
        "oath_timestep": 30,
        "oath_counter": 0,
        "oath_timeshift": 0,
        "oath_reuse": false,
        "created_at": "2026-06-08 06:32:32.470217-07",
        "modified_at": "2026-06-08 06:32:32.470217-07"
    }
}
```


1.80.9 Update Authentication Method

Request

Method	`PATCH`
Path	`/api/v2/profile/authentication/<id>`
Body	`AuthenticationMethodModel`

PATCH /api/v2/profile/authentication/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: <token>' \
  -H 'X-Auth-Confirm:␣
↪22d05aff6c39f9de8bdba340c31873edaaa6390dcff30137e91bbe0f23161179' \
  -H 'Content-Type: application/json' \
  -d '{
    "description": "Updated OATH Description",
    "oath_reuse": true
  }' \
  'https://10.33.2.133/api/v2/profile/authentication/5980780305148018705'
```

Response

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

1.80.10 Delete Authentication Method

Request

Method	DELETE
Path	/api/v2/profile/authentication/<id>

DELETE /api/v2/profile/authentication/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: <token>' \
  -H 'X-Auth-Confirm:␣
↪22d05aff6c39f9de8bdba340c31873edaaa6390dcff30137e91bbe0f23161179' \
  'https://10.33.2.133/api/v2/profile/authentication/5980780305148018705'
```

Response

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

1.80.11 Invalidate Reauthentication Token

Request

Method	POST
Path	/api/v2/profile/authentication/invalidate
Body	ConfirmModel

POST /api/v2/profile/authentication/invalidate

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{
    "method": "password",
    "password": "user_password"
  }' \
  'https://10.33.2.133/api/v2/profile/authentication/invalidate'
```

Response

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

1.81 UAG - Current User Identity

1.81.1 Data Structures

Table 203: `UserIdentityModel`

Attribute	Type	Required	Description
`username`	string	yes	Read-only. Logged user name.
`user_id`	string	yes	Read-only. Logged user ID.
`domain`	string		Read-only. Logged user domain.
`language`	string	yes	Read-only. Logged user language setting.
`help_url`	string	yes	Read-only. URL to the online help.
`license_tier`	string	yes	Read-only. Configured license tier. One of: `basic`, `full`.
`license_vault_cl`	boolean	yes	Read-only. The user can perform password vault checkout. User has an active Vault module, or there are available license slots.
`module_psm_enabl`	boolean	yes	Read-only. Whether the PSM (Resources) module is enabled for the logged user.
`module_vault_ena`	boolean	yes	Read-only. Whether the Password Vault module is enabled for the logged user.
`authentication_r`	object	yes	Read-only. Enabled or disabled state of each authentication method available for Access Gateway login: `password`, `oath`, `sshkey`, `fido2`.
`fido2_configure`	boolean	yes	Read-only. Whether a FIDO2 relying party ID is configured for the Access Gateway, making FIDO2 login usable.

1.81.2 Retrieve Available Attributes of the *UserIdentityModel*

Request

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

GET /api/v2/objspec/me

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/me'
```

1.81.3 Get Current User Identity

Request

Method	GET
Path	/api/v2/me

GET /api/v2/me

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/me'
```

Response

```
{
    "result": "success",
    "me": {
        "username": "admin",
        "user_id": "3260606130216239001",
        "domain": null,
        "language": "en",
        "help_url": "https://docs.fudosecurity.com/6.1/",
        "license_tier": "full",
        "license_vault_checkout_available": true
    }
}
```

1.82 UAG - Accounts List

1.82.1 Get Account List

Request

Method	GET
Path	/api/v2/account

GET /api/v2/account

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/account
```

Response


```
{
    "items": [
        {
            "id": "8169529724050079749",
            "name": "remoteapp-account",
            "type": "regular",
            "require_login": false,
            "blocked": false,
            "blocked_reason": null,
            "login_reason": false,
            "password_visible": false,
            "has_password_history": true,
            "has_remote_apps": true,
            "server": {
                "id": "8169529724050079749",
                "name": "remoteapp",
                "description": null,
                "address": "10.0.234.30",
                "port": 3389,
                "port_first": 3389,
                "port_last": 3389,
                "mask": 32,
                "dynamic": false
            },
            "pool": null,
            "listeners_info": {
                "external": false,
                "local": true,
                "otp_enabled": true,
                "play_enabled": false,
                "multiple_addresses": true,
                "webclient": {
                    "safe_id": "8169529724050079745",
                    "secproto": "tls"
                }
            },
            "session_id": null,
            "protocol": "rdp",
            "note_access_level": "none",
            "session_status": null,
            "session_reason": null,
            "timeout": null,
            "access_request": {
                "jit": "disabled",
                "connection_available": false
            },
            "otp_in_access_gateway": true,
            "rdp_remote_apps_only": false,
            "rdp_resolution": null
```


(continues on next page)

(continued from previous page)

```
        },
    ],
    "result": "success"
}
```

Note

- The `"password_visible": true` indicates that the **Reveal Password** option is enabled for the user and safe.
- The account ID is obtained: `"id": "8169529724050079749"`. This ID will be used for the checkout and checkin requests.
- When the checkout session is active then its ID is shown in the `session_id`. When checkout session for account and user is not active then `sessison_id` field is `null`.
- The `note_access_level` attribute indicates the user's access to account-related notes. This value is defined by the `note_access` setting on the associated Safe. For full details, refer to the section *Safes*.
- The `access_request.jit` attribute indicates whether an access request is required for this account right now. It replaces the former `access_request.enabled` boolean and takes one of the following values:
  - `disabled` - the safe does not use Just-in-Time access; connect directly.
  - `required` - an approved access request is needed before connecting.
  - `permitted_not_required` - the safe uses time-based Just-in-Time access and the current time falls inside the daily access policy window, so the user may connect directly, while access requests and their history remain available.

  The value of `permitted_not_required` changes over time as the daily access policy window opens and closes. For details on the safe-side configuration, refer to the `jit_mode` attribute in the *Safes* section.

1.83 UAG - Account Safe Listener

1.83.1 Data Structures

Table 205: `AccountSafeListenerModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique object identifier. Protected.
`access_denied`	object		Read-only. Expensive to use. Object of reasons why access to the object is denied for the API subject.

continues on next page

Table 205 – continued from previous page

Attribute	Type	Required	Description
account_id	string	yes	Read-only. Uniqueness is required in the combination of attribute account_id with attributes safe_id and listener_id.
safe_id	string	yes	Read-only. Uniqueness is required in the combination of attribute safe_id with attributes account_id and listener_id.
safe_name	string		Read-only.
listener_id	string		Read-only. Uniqueness is required in the combination of attribute listener_id with attributes account_id and safe_id.
listener_name	string		Read-only.
mode	string		Read-only. Mode of operation. One of: proxy, bastion, tunnel.
protocol	string		Read-only. Protocol used. One of: http, modbus, mysql, oracle, pgsql, tcp, tds, telnet, tn3270, tn5250, rdp, ssh, vnc.
external_address	string	If external_ is set	Read-only. Listener address to present in Access Gateway. Requires external_port.
external_port	number {from 1 to 65535}	If external_ is set	Read-only. Listener port to present in Access Gateway. Requires external_address.
otp_enabled	boolean		Read-only. Expensive to use. Does protocol support OTP authentication?
play_enabled	boolean		Read-only. Expensive to use. Does protocol allow click to play but additional authentication is required?
addresses	string[]		Read-only. Expensive to use. List of listener addresses.
listen_port	number {from 1 to 65535}		Read-only. Listener port.
tls_enabled	boolean		Read-only. TLS enabled.
ssh_public_key_1	string		Read-only. Expensive to use.
ssh_public_key_1	string	If protocol == ssh	Read-only. Expensive to use. SSH public key MD5 fingerprint.
ssh_public_key_1	string	If protocol == ssh	Read-only. Expensive to use. SSH public key SHA1 fingerprint.

continues on next page

Table 205 – continued from previous page

Attribute	Type	Required	Description
tls_certificate_	string	If protocol == http || rdp & tls_enabl == true	Read-only. Expensive to use. TLS certificate MD5 fingerprint.
tls_certificate_	string	If protocol == http || rdp & tls_enabl == true	Read-only. Expensive to use. TLS certificate SHA1 fingerprint.
rdp_public_key_1	string	If protocol == rdp & tls_enabl == false	Read-only. Expensive to use. RDP public key MD5 fingerprint.
rdp_public_key_1	string	If protocol == rdp & tls_enabl == false	Read-only. Expensive to use. RDP public key SHA1 fingerprint.

1.83.2 Retrieve Available Attributes of the *AccountSafeListenerModel*

Request

Method	GET
Path	/api/v2/objspec/account_safe_listener

GET /api/v2/objspec/account_safe_listener

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/account_safe_listener'
```

1.83.3 Get User Access Gateway / Safe / Listener Assignment

Request

Method	GET
Path	/api/v2/account_safe_listener

GET /api/v2/account_safe_listener

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/account_safe_listener
```

Response


```
{
    "result": "success",
    "account_safe_listener": [
        {
            "account_id": "8169529724050079750",
            "safe_id": "8169529724050079749",
            "safe_name": "Safe_2345",
            "listener_id": "8169529724050079746",
            "listener_name": "RDP:bastion",
            "mode": "bastion",
            "protocol": "rdp",
            "otp_enabled": true,
            "play_enabled": false,
            "addresses": [
                "10.31.116.195",
                "10.31.116.197",
                "10.31.116.196"
            ],
            "listen_port": 3389,
            "tls_enabled": true,
            "tls_certificate_fingerprint_md5":
↪"MD5:2f:6f:4c:3e:dd:bb:ba:06:83:92:2e:89:f5:98:39:2f",
            "tls_certificate_fingerprint_sha1":
↪"SHA1:2f:aa:62:aa:dd:2f:c8:10:7b:2f:4b:39:dd:43:4f:1a:8b:5a:dd:18"
        }
    ]
}
```


1.84 UAG - Account Access Request

Note

Access requests enable temporary, on-demand access to protected accounts or secrets. This mechanism is typically used in Just-in-Time (JIT) scenarios, where access must be explicitly approved before a connection can be established. Additionally, users with the *View on request* permission for a collection can request access to secrets within that collection.

The access approval process for accounts is configured per Safe. To enable voting for access requests, set the `required_votes` parameter when creating or updating a Safe.

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://<host>/api/v2/safe/<safe_id> \
  -d '{"required_votes": 1}'
```

For details, refer to the *Safe configuration* section.

1.84.1 Data Structures

Table 206: `AccessRequestModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique object identifier.
`user_id`	string	yes	Immutable. Requesting user.
`status`	string	yes	Read-only. Current request status. Expensive to use. One of: `expired`, `granted`, `pending`, `rejected`, `revoked`.
`operation`	string	yes	Immutable. Operation type. One of: `account_access`, `account_share`, `secret_view`, `secret_share`.
`type`	string	yes	Immutable. Access type. One of: `immediate`, `scheduled`, `preview`.
`immediate_interv`	number {from `1` to `24`}	If `type == immediate`	Read-only. Expensive to use. Requested duration in hours from the first session for immediate access.
`starts_at`	datetime	If `type == scheduled`	Scheduled start time.
`expires_at`	datetime	If `type == scheduled`	Scheduled expiration time.
`reason`	string	yes	The user's reason why access is being requested.
`account_id`	string		Read-only. Account identifier.
`account_name`	string		Read-only. Expensive to use. Account name.
`secret_id`	string		Read-only. Secret identifier.
`collection_id`	string		Read-only. Expensive to use. Collection identifier.
`secret_name`	string		Read-only. Expensive to use. Secret name.
`votes`	object-array		Read-only. Expensive to use. Vote history.
`required_votes`	number	yes	Read-only. Minimum number of votes required to grant access to the account.
`collected_votes`	number		Read-only. Expensive to use. Number of collected votes.
`archival`	boolean	yes	Read-only. Expensive to use. Is the request archival (i.e. expired, rejected or revoked)?

continues on next page

Table 206 – continued from previous page

Attribute	Type	Required	Description
`active`	boolean	yes	Read-only. Expensive to use. True when the access request is granted and within its validity period (starts_at <= now < expires_at). Indicates that the user can perform the associated operation.
`revoke_reason`	string		Read-only. The reason why the access request was revoked.
`created_at`	datetime		Read-only. Creation timestamp.
`modified_at`	datetime		Read-only. Modification timestamp.
`removed`	boolean		Read-only.

Table 207: `AccessRequestPostModel`

At-tribut	Type	Required	Description
`id`	string		Read-only. Unique object identifier.
`opera`	string	yes	Immutable. Operation type. One of: `account_access`, `secret_view`, `secret_share`.
`type`	string	yes	Immutable. Access type. One of: `immediate`, `scheduled`.
`immec`	number {from 1 to 24}	If `type` == `immediate`	Requested duration in hours.
`start`	datetime	If `type` == `scheduled`	Scheduled start time.
`expi1`	datetime	If `type` == `scheduled`	Scheduled expiration time.
`reasc`	string		The user's reason why access is being requested. Mutually exclusive with `reason_format_id`.
`reasc`	string		Identifier of the reason format used to compose the reason. Mutually exclusive with `reason`. Requires `operation` == `account_access`.
`reasc`	object-array	If `reason_format_ic` is set	Values for the fields of the chosen reason format, as `{field_id, value}` objects.
`accou`	string	If `operation` == `account_access`	Account identifier for account access requests.
`safe_`	string	If `operation` == `account_access`	Safe identifier for account access requests.
`secre`	string	If `operation` == `secret_view` || `secret_share`	Secret identifier for secret operations.

continues on next page

Table 207 – continued from previous page

Attribut	Type	Required	Description
reque_user	string	If `operation` == `secret_share`	User login for secret share requests.

Table 208: `AccessRequestRevokeModel`

Attribut	Type	Required	Description
`id`	string	yes	The access request id.
revok	string	yes	The user's reason why access is being revoked.

1.84.2 Retrieve Available Attributes of the *AccessRequestModel*

Request

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

1.84.3 Retrieve Available Attributes of the *AccessRequestPostModel*

Request

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

1.84.4 Retrieve Available Attributes of the *AccessRequestRevokeModel*

Request

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

1.84.5 Get Access Requests

Request

Method	`GET`
Path	`/api/v2/access_request`

GET /api/v2/access_request

Example Request

```
curl -s -k -X GET \
-H 'Authorization: sgfeea6jsaz4mum9su8w6' \
https://10.0.0.1/api/v2/access_request
```

Response


```
{
    "result": "success",
    "access_request": [
        {
            "id": "3260606130216239105",
            "user_id": "3260606130216239105",
            "status": "pending",
            "operation": "account_access",
            "type": "immediate",
            "immediate_interval": 2,
            "expires_at": "2026-04-23 05:35:11.209911-07",
            "reason": "Maintenance.",
            "account_id": "3260606130216239107",
            "account_name": "ad-user1-windows",
            "votes": [],
            "required_votes": 1,
            "collected_votes": 0,
            "archival": false,
            "active": false,
            "created_at": "2026-04-22 05:35:11.212162-07",
            "modified_at": "2026-04-22 05:35:11.217997-07"
        },
        {
            "id": "3260606130216239106",
            "user_id": "3260606130216239105",
            "status": "pending",
            "operation": "secret_view",
            "type": "immediate",
            "immediate_interval": 2,
            "expires_at": "2026-04-23 05:36:01.215024-07",
            "reason": "Maintenance.",
            "secret_id": "3260606130216239105",
            "collection_id": "3260606130216239105",
            "secret_name": "secret for: root-fudo-PV",
            "votes": [],
            "required_votes": 1,
            "collected_votes": 0,
            "archival": false,
            "active": false,
            "created_at": "2026-04-22 05:36:01.217266-07",
            "modified_at": "2026-04-22 05:36:01.217266-07"
        }
    ]
}
```

1.84.6 Create Access Request

Request

Method	`POST`
Path	`/api/v2/access_request`
Headers	`Content-Type: application/json`
Body	`AccessRequestPostModel`

POST /api/v2/access_request

Example Request (Account Access - Immediate)

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.137.67/api/v2/access_request \
  -d '{
        "operation": "account_access",
        "account_id": "3260606130216239107",
        "safe_id": "3260606130216239105",
        "type": "immediate",
        "immediate_interval": 2,
        "reason": "Maintenance."
      }'
```

Example Request (Account Access - Scheduled)

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.137.67/api/v2/access_request \
  -d '{
        "operation": "account_access",
        "account_id": "3260606130216239107",
        "safe_id": "3260606130216239105",
        "type": "scheduled",
        "reason": "Maintenance session",
        "starts_at": "2026-04-23T07:30:00-07:00",
        "expires_at": "2026-05-21T15:00:00-07:00"
      }'
```

Example Request (Secret View - Immediate)

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.137.67/api/v2/access_request \
  -d '{
        "operation": "secret_view",
        "secret_id": "3260606130216239105",
```

(continues on next page)

(continued from previous page)

```
        "type": "immediate",
        "immediate_interval": 2,
        "reason": "Maintenance."
      }'
```

Response

```
{
    "id": "3260606130216239112",
    "result": "success"
}
```

1.84.7 Revoke Access Request

Note

Only secret sharing access requests can be revoked from User Access Gateway.

Request

Method	`POST`
Path	`/api/v2/access_request/<id>/revoke`
Headers	`Content-Type: application/json`
Body	`AccessRequestRevokeModel`

POST /api/v2/access_request/<id>/revoke

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.137.67/api/v2/access_request/8169529724050079762/revoke \
  -d '{
        "revoke_reason": "No longer needed"
      }'
```

Response

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

1.85 UAG - Access Request Reason Formats NEW

A reason format defines the fields a user has to fill in when requesting access to an account. The endpoint returns every reason format defined by the administrator together with its fields, so that the User Access Gateway can render the request form.

Note

This endpoint does not have an object specification (`objspec`) - it returns a static structure described in the tables below.

1.85.1 Data Structures

Table 209: `ReasonFormatModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Reason format ID.
`name`	string		Read-only. Name of the reason format.
`description`	string		Read-only. Description of the reason format; `null` when not set.
`fields`	See the `ReasonFormatFieldM` table		Read-only. Fields of the reason format; an empty array when the format has no fields.

Table 210: `ReasonFormatFieldModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Reason format field ID.
`name`	string		Read-only. Name of the field. Unique within the reason format.
`type`	string {text, number, constant}		Read-only. Type of the field. `text` and `number` are filled in by the user; `constant` carries a fixed value defined by the administrator.
`value`	string		Read-only. Fixed constant value; `null` for the `text` and `number` types.

1.85.2 Get Access Request Reason Formats

Request

Method	`GET`
Path	`/api/v2/access_request_reason_format`

GET /api/v2/access_request_reason_format

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/access_request_reason_format'
```

Response

```
{
    "reason_formats": [
        {
            "id": "4638707616191610881",
            "name": "Incident handling",
            "description": "Reason format used for incident related requests.",
            "fields": [
                {
                    "id": "4638707616191610881",
                    "name": "Ticket number",
                    "type": "text",
                    "value": null
                },
                {
                    "id": "4638707616191610882",
                    "name": "Priority",
                    "type": "number",
                    "value": null
                },
                {
                    "id": "4638707616191610883",
                    "name": "Source system",
                    "type": "constant",
                    "value": "Service Desk"
                }
            ]
        }
    ],
    "result": "success"
}
```


1.86 UAG - Session Timeout Check

1.86.1 Get Session Timeout

Request

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

GET /api/v2/session/timeout

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/session/timeout
```

Response

```
{
    "timeout_uag": 15,
    "result": "success"
}
```

1.87 UAG - Live Sessions NEW

Running sessions of the signed-in user. The endpoints return only sessions that belong to the API subject and have not finished yet, together with the information the User Access Gateway needs to present them: the address the session was established on, the supervision requirements and whether the session may be shared with a share link.

1.87.1 Data Structures

Table 211: `SessionLiveModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique. Session ID.
`account_id`	string		Read-only. ID of the account used for the connection.
`webclient`	boolean		Read-only. Whether the session runs through the web client.
`listen_address`	string		Read-only. Listener bind address; `null` for web-client sessions.
`listen_port`	number		Read-only. Listener bind port; `null` for web-client sessions.
`status`	string {approved, disconnected, expired, rejected, terminated, waiting, waiting_supervision}		Read-only. Status of the session.
`allow_user_shar`	boolean		Read-only. Whether the Safe of the session allows the user to share the session with a share link. See the section *UAG - Session Sharing* ***NEW***.
`min_supervisors`	number		Read-only. Number of supervisors required to keep the session running.
`created_at`	datetime		Read-only. Timestamp of creation.

1.87.2 Retrieve Available Attributes of the *SessionLiveModel*

Request

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

GET /api/v2/objspec/session_live

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/objspec/session_live'
```

1.87.3 Get Live Sessions

Request

Method	GET
Path	/api/v2/session/live

GET /api/v2/session/live

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/session/live'
```

Response

```
{
    "result": "success",
    "session_live": [
        {
            "id": "4638707616191610882",
            "account_id": "4638707616191610884",
            "webclient": true,
            "status": "approved",
            "allow_user_sharing": true,
            "created_at": "2026-08-17 07:10:08.939173-07"
        },
        {
            "id": "4638707616191610891",
            "account_id": "4638707616191610884",
            "webclient": true,
            "status": "approved",
            "allow_user_sharing": true,
            "created_at": "2026-08-17 07:29:07.345671-07"
        }
    ]
}
```

1.87.4 Get a Single Live Session

Request

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

GET /api/v2/session/<id>/live

The response is an array, as for the whole listing. It is empty when the session does not exist, does not belong to the API subject or has already finished.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/session/4638707616191610882/live'
```

Response

```
{
    "result": "success",
    "session_live": [
        {
            "id": "4638707616191610882",
            "account_id": "4638707616191610884",
            "webclient": true,
            "status": "approved",
            "allow_user_sharing": true,
            "created_at": "2026-08-17 07:10:08.939173-07"
        }
    ]
}
```

1.88 UAG - Session Resolution NEW

The session player opened in the User Access Gateway does not know the ID of the session it has to play. Two endpoints resolve it:

- `POST /api/v2/session/resolve` - resolves the session the user has just connected to with a one-time password minted for the web client,
- `GET /api/v2/session_share/resolve` - resolves the session a share link points to and returns the playback context of that share.

1.88.1 Data Structures

Table 212: `SessionResolveModel`

Attribute	Type	Required	Description
`otp_id`	string	yes	ID of the OTP (from `POST /api/v2/secret/otp`) whose live session to resolve. See the section *UAG - OTP Generation*.

Table 213: `SessionShareResolveModel`

Attribute	Type	Required	Description
`session_id`	string		Read-only. ID of the shared session.
`protocol`	string {checkout, http, modbus, mysql, pgsql, rdp, ssh, tcp, tds, telnet, tn3270, tn5250, vnc}		Read-only. Protocol used for connection.
`live`	boolean		Read-only. `true` - the session is still running; `false` - the session has finished.
`started_at`	datetime		Read-only. Datetime of the session's start.
`finished_at`	datetime		Read-only. Datetime of the session's end; `null` for a running session.
`status`	string {approved, disconnected, expired, rejected, terminated, waiting, waiting_supervision}		Read-only. Status of the session.
`readonly`	boolean		Read-only. Whether the share allows the recipient to interact with the session.
`authenticated`	boolean		Read-only. Whether the share requires the recipient to be signed in.
`language`	string		Read-only. Interface language of the API subject.
`vhost`	string {mgmt, uag}		Read-only. Address the share was resolved on.
`width`	string		Read-only. Width of the recorded image; `null` for text protocols.
`height`	string		Read-only. Height of the recorded image; `null` for text protocols.

1.88.2 Retrieve Available Attributes of the *SessionResolveModel*

Request

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

GET /api/v2/objspec/session_resolve

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/objspec/session_resolve'
```

1.88.3 Resolve the Session of a One-Time Password

Request

Method	POST
Path	/api/v2/session/resolve
Headers	Content-Type: application/json
Body	SessionResolveModel

POST /api/v2/session/resolve

The one-time password must have been used already and the resolved session must belong to the API subject and still be running. The session row is created when the connection is established, so the web client repeats the request until the session becomes available.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.33.3.192/api/v2/session/resolve \
  -d '{"otp_id": "13"}'
```

Response

```
{
    "id": "4638707616191610891",
    "result": "success"
}
```

1.88.4 Resolve the Session of a Share Link

Request

Method	GET
Path	/api/v2/session_share/resolve
Headers	Session-Share-Key: <key>

GET /api/v2/session_share/resolve

The share key is passed in the `Session-Share-Key` header and it is the only authorization of this endpoint. The same endpoint is available in the management API; the `vhost` attribute reports which address the share was resolved on.

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Session-Share-Key:␣
↪rmNTote8QCxcK5rPRewpomwzl9GJaYDOFcpWd62Az2iPephvDCPDgD2gJgPzfkd7' \
  'https://10.33.3.192/api/v2/session_share/resolve'
```

Response

```
{
    "session_id": "4638707616191610882",
    "protocol": "ssh",
    "live": true,
    "started_at": "2026-08-17T14:10:08.938499Z",
    "finished_at": null,
    "status": "approved",
    "readonly": false,
    "authenticated": true,
    "language": "en",
    "vhost": "uag",
    "width": null,
    "height": null,
    "result": "success"
}
```


1.89 UAG - Shared Session Details NEW

Details of a session opened with a share link. The endpoint returns the reduced set of session attributes the player needs to play the recording - the attributes that identify the user, the account, the server or the Safe of the session are not exposed to the recipient of the link.

Note

The share key is passed in the `Session-Share-Key` header and it is the only authorization of this endpoint. The key must resolve to the session given in the path.

This endpoint has no object specification (`objspec`). The full session object of the management API is described in the section *Sessions*.

1.89.1 Data Structures

Table 214: `SharedSessionModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Session ID.
`started_at`	datetime		Read-only. Datetime of the session's start.
`finished_at`	datetime		Read-only. Datetime of the session's end; `null` for a running session.
`retention_locke`	boolean		Read-only. Indicates whether the session is protected against automatic deletion.
`protocol`	string {checkout, http, modbus, mysql, pgsql, rdp, ssh, tcp, tds, telnet, tn3270, tn5250, vnc}		Read-only. Protocol used for connection.

continues on next page

Table 214 – continued from previous page

Attribute	Type	Required	Description
subprotocol	string {checkout, http, http_rendered, modbus, mysql, pgsql, rdp, scp, sftp, ssh, ssh_command, tcp, tds, telnet, tn3270, tn5250, vnc, x11}		Read-only. Session subprotocol.
size	number		Read-only. Size of the recording in bytes.
bits_per_pixel	string		Read-only. Resolution options.
height	string		Read-only. Resolution options.
width	string		Read-only. Resolution options.
duration	number		Read-only. Session duration in seconds.
time_limit	number		Read-only. Time in seconds remaining until the session is terminated. Value is available only when terminate_at is defined. Value 0 means the session is finished or terminated.
created_at	datetime		Read-only. Timestamp of creation.
terminate_at	datetime		Read-only. Datetime of the session's termination.
websocket_url	string		Read-only. A part of the URL to the websocket that serves the data of this session.
type	string		Read-only. Session's type.
paused	boolean		Read-only. Indicates whether the session is paused.
local	boolean		Read-only. Indicates that the session is running or has a replica on the current cluster node.
timestamp_status	string {none, pending, completed}		Read-only. Status of the timestamping process.

1.89.2 Get Details of a Shared Session

Request

Method	GET
Path	/api/v2/session/<id>
Headers	Session-Share-Key: <key>

GET /api/v2/session/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Session-Share-Key:␣
↪rmNTote8QCxcK5rPRewpomwzl9GJaYD0FcpWd62Az2iPephvDCPDgD2gJgPzfkd7' \
  'https://10.33.3.192/api/v2/session/4638707616191610882'
```

Response


```
{
    "session": {
        "id": "4638707616191610882",
        "started_at": "2026-08-17T14:10:08.938499Z",
        "finished_at": null,
        "retention_locked": false,
        "protocol": "ssh",
        "subprotocol": "ssh",
        "size": 19456,
        "bits_per_pixel": null,
        "height": null,
        "width": null,
        "duration": null,
        "time_limit": null,
        "created_at": "2026-08-17T14:10:08.939173Z",
        "terminate_at": null,
        "websocket_url": "\/websocket\/4638707616191610882\/",
        "type": "session",
        "paused": false,
        "local": true,
        "timestamp_status": "none"
    },
    "result": "success"
}
```


1.90 UAG - Session Sharing NEW

A user may share their own running session with another user by creating a share link in the session player. The endpoints below list, create and revoke the share links the signed-in user created in the User Access Gateway.

Sharing is available only when it is enabled on the Safe of the session - the `allow_user_sharing` attribute described in the section *UAG - Live Sessions **NEW***.

Share links created in the User Access Gateway always use the same settings:

- the recipient may interact with the session (`readonly` is `false`),
- the recipient must be signed in and their identity is recorded in the access history (`authenticated` is `true`),
- the link is valid until the session ends (`valid_to` is `null`).

Shares created by an administrator in the management API are neither listed nor revocable here - see the section *Sharing Sessions*.

1.90.1 Data Structures

Table 215: `SessionShareModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique. Share ID.
`session_id`	string		Read-only. ID of the shared session.
`created_by`	string		Read-only. ID of the user who created the share.
`key`	string		Read-only. Share key - 64 alphanumeric characters.
`link`	string		Read-only. Expensive to use. Relative share link without host prefix.
`readonly`	boolean		Read-only. `true` - the recipient can only watch the session; `false` - the recipient can also interact with it.
`authenticated`	boolean		Read-only. `true` - the recipient must be signed in and their identity is recorded in the access history; `false` - anonymous access with the key only.
`valid_since`	datetime		Read-only. Start date and time of the share validity period.
`valid_to`	datetime		Read-only. End date and time of the share validity period; `null` - the share is valid until the session ends.
`created_at`	datetime		Read-only. Timestamp of creation.

1.90.2 Retrieve Available Attributes of the *SessionShareModel*

Request

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

GET /api/v2/objspec/session_share

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/objspec/session_share'
```

1.90.3 Get Session Share Links

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/share`

GET /api/v2/session/<session_id>/share

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/session/4638707616191610882/share'
```

Response

```
{
    "result": "success",
    "session_share": [
        {
            "id": "4638707616191610881",
            "session_id": "4638707616191610882",
            "created_by": "4638707616191610882",
            "key":
↪"rmNTote8QCxcK5rPRewpomwzl9GJaYD0FcpWd62Az2iPephvDCPDgD2gJgPzfkd7",
            "link": "\/play\/4638707616191610882
↪#key=rmNTote8QCxcK5rPRewpomwzl9GJaYD0FcpWd62Az2iPephvDCPDgD2gJgPzfkd7",
            "readonly": false,
            "authenticated": true,
            "valid_since": "2026-08-17 07:27:02.046789-07",
            "created_at": "2026-08-17 07:27:02.051077-07"
        }
    ]
}
```

1.90.4 Share a Session

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/share`

POST /api/v2/session/<session_id>/share

The request has no body - the share settings are fixed, as described above. The session must belong to the API subject, must still be running and its Safe must allow user sharing.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/session/4638707616191610882/share'
```

Response

```
{
    "id": "4638707616191610881",
    "key": "rmNTote8QCxcK5rPRewpomwzl9GJaYD0FcpWd62Az2iPephvDCPDgD2gJgPzfkd7",
    "link": "\/play\/4638707616191610882
```

(continues on next page)

(continued from previous page)

```
↪#key=rmNTote8QCxcK5rPRewpomwzl9GJaYDOFcpWd62Az2iPephvDCPDgD2gJgPzfkd7",
    "result": "success"
}
```

Note

The `link` attribute returns a path without the host prefix. Prepend the User Access Gateway address to obtain the link the recipient opens.

1.90.5 Revoke a Session Share Link

Request

Method	`DELETE`
Path	`/api/v2/session/<session_id>/share/<share_id>`

DELETE /api/v2/session/<session_id>/share/<share_id>

Revoking a share link also closes the connections that are still watching the session through it. The access history of the share is kept - see the section *UAG - Session Share Access* ***NEW***.

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/session/4638707616191610882/share/
↪4638707616191610881'
```

Response

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

1.91 UAG - Session Share Access NEW

Viewers that are currently connected to a session of the signed-in user through a share link. The listing lets the owner of the session see who is watching it and whether the viewer has already interacted with it.

Only open connections to sessions of the API subject are returned. Entries of viewers who have already disconnected are kept in the management API - see the section *Session Access History* ***NEW***.

1.91.1 Data Structures

Table 216: `SessionShareAccessModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique. Access entry ID.
`session_id`	string		Read-only. ID of the session that was accessed.
`session_share_ic`	string		Read-only. ID of the share link used to access the session.
`user_id`	string		Read-only. ID of the viewer; `null` for anonymous viewers.
`user_name`	string		Read-only. Name of the viewer; `null` for anonymous viewers.
`started_at`	datetime		Read-only. When the viewer started watching the session.
`joined_at`	datetime		Read-only. When the viewer first interacted with the session; `null` for view-only access.

1.91.2 Retrieve Available Attributes of the *SessionShareAccessModel*

Request

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

GET /api/v2/objspec/session_share_access

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/objspec/session_share_access'
```

1.91.3 Get Viewers Connected to a Session

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/access`

GET /api/v2/session/<session_id>/access

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/session/4638707616191610882/access'
```

Response

```
{
    "result": "success",
    "session_share_access": [
        {
            "id": "4638707616191610881",
            "session_id": "4638707616191610882",
            "session_share_id": "4638707616191610881",
            "user_id": "4638707616191610882",
            "user_name": "user_1",
            "started_at": "2026-08-17 07:28:42.592943-07"
        }
    ]
}
```


1.92 UAG - Session Comments NEW

Comments of a session shared with a share link. The endpoints are authorized with the share key only, so a recipient of the link can read the comments of the shared session and - when the share is not read-only - add new ones.

Note

The share key is passed in the `Session-Share-Key` header and it is the only authorization of these endpoints. The key must resolve to the session given in the path.

Comments added through a share link are append-only. Modifying and deleting comments is available in the management API only - see the section *Session Comment*.

The `modified_by` attribute is not returned to share link recipients. The author of a comment is

presented with the `modified_by_name` attribute.

1.92.1 Data Structures

Table 217: `SessionCommentModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique.
`parent_id`	string		Immutable. ID of the commented comment - used to reply to an existing comment. The parent comment must belong to the shared session.
`session_id`	string	yes	Immutable. ID of the commented session.
`text`	string	yes	Text content of the session comment.
`start_at`	datetime	yes	Value format: time. Expensive to use. Offset from the beginning of the session, in the `HH:MM:SS` format.

continues on next page

Table 217 – continued from previous page

Attribute	Type	Required	Description
`finish_at`	datetime	yes	Value format: time. Expensive to use. Offset from the beginning of the session, in the `HH:MM:SS` format.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`modified_by`	string		Read-only. ID of the author of the comment. Not returned to share link recipients.
`modified_by_name`	string		Read-only. Expensive to use. Name of the author of the comment.
`removed`	boolean		Read-only.

1.92.2 Retrieve Available Attributes of the *SessionCommentModel*

Request

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

GET /api/v2/objspec/session_comment

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.3.192/api/v2/objspec/session_comment'
```

1.92.3 Get Comments of a Shared Session

Request

Method	`GET`
Path	`/api/v2/session/<session_id>/comment`
Headers	`Session-Share-Key: <key>`

GET /api/v2/session/<session_id>/comment

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Session-Share-Key:␣
↪rmNTote8QCxcK5rPRewpomwzl9GJaYDOFcpWd62Az2iPephvDCPDgD2gJgPzfkd7' \
  'https://10.33.3.192/api/v2/session/4638707616191610882/comment'
```

Response

```
{
    "result": "success",
    "session_comment": [
        {
            "id": "4638707616191610881",
            "session_id": "4638707616191610882",
            "text": "Text content of the session comment.",
            "created_at": "2026-08-17 07:27:17.95841-07",
            "modified_at": "2026-08-17 07:27:17.95841-07",
            "modified_by_name": "user_1",
            "start_at": "00:01:00",
            "finish_at": "00:01:00"
        }
    ]
}
```


1.92.4 Add a Comment to a Shared Session

Request

Method	`POST`
Path	`/api/v2/session/<session_id>/comment`
Headers	`Content-Type: application/json`
Headers	`Session-Share-Key: <key>`
Body	`SessionCommentModel`

POST /api/v2/session/<session_id>/comment

The share must not be read-only. `start_at` and `finish_at` are given as an offset from the beginning of the session.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -H 'Session-Share-Key:␣
↪rmNTote8QCxcK5rPRewpomwzl9GJaYD0FcpWd62Az2iPephvDCPDgD2gJgPzfkd7' \
  https://10.33.3.192/api/v2/session/4638707616191610882/comment \
  -d '{"text": "Text content of the session comment.","start_at":"00:01:00",
↪"finish_at":"00:01:00"}'
```

Response


```
{
    "result": "success",
    "session_comment": {
        "id": "4638707616191610881"
    }
}
```

Example Request - a reply to an existing comment

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -H 'Session-Share-Key:␣
↪rmNTote8QCxcK5rPRewpomwzl9GJaYD0FcpWd62Az2iPephvDCPDgD2gJgPzfkd7' \
  https://10.33.3.192/api/v2/session/4638707616191610882/comment \
  -d '{"parent_id": "4638707616191610881","text": "Reply to the comment.",
↪"start_at":"00:01:00","finish_at":"00:01:00"}'
```

Response

```
{
    "result": "success",
    "session_comment": {
        "id": "4638707616191610882"
    }
}
```

1.93 UAG - Account Remote Applications

1.93.1 Data Structures

Table 218: `AccountRemoteAppModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique object identifier. Expensive to use.
`name`	string	yes	Read-only. Remote application name.
`account_id`	string	yes	Read-only. ID of the associated account. Expensive to use.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of last modification.
`removed`	boolean		Read-only.

1.93.2 Retrieve Available Attributes of the *AccountRemoteAppModel*

Request

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

GET /api/v2/objspec/remote_app

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/remote_app'
```

1.93.3 List Remote Applications Assigned to Account

Request

Method	GET
Path	/api/v2/account/<account_id>/remote_apps

GET /api/v2/account/<account_id>/remote_apps

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/account/8169529724050079749/remote_apps
```

Response

```
{
    "result": "success",
    "remote_app": [
        {
            "id": "8169529724050079745",
            "name": "firefox",
            "account_id": "8169529724050079749",
            "created_at": "2025-07-07 04:02:13.924887-07",
            "modified_at": "2025-07-07 04:02:13.924887-07"
        },
        {
            "id": "8169529724050079752",
            "name": "putty-constant-variables",
            "account_id": "8169529724050079749",
            "created_at": "2025-07-07 04:02:14.458032-07",
            "modified_at": "2025-07-07 04:02:14.458032-07"
        },
        {
            "id": "8169529724050079754",
            "name": "tightvnc",
            "account_id": "8169529724050079749",
            "created_at": "2025-07-07 04:02:14.52783-07",
            "modified_at": "2025-07-07 04:02:14.52783-07"
        }
    ]
}
```

1.94 UAG - Account Notes

Note

The `note_access_level` attribute indicates the user's access to account-related notes:

- `none` – no access,
- `read` – read-only access,
- `write` – full access (read and modify).

This value is defined by the `note_access` setting on the associated Safe.

To change it via API, use the following request:

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://<host>/api/v2/safe/<safe_id> \
  -d '{"note_access": "read"}'
```

For full details, refer to the section *Safes*.

1.94.1 Data Structures

Table 219: `AccountNoteModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Account Note ID.
`account_id`	string	yes	Immutable. Account ID.
`note`	string	yes	Text of the note.
`created_at`	datetime		Read-only. Timestamp of creation.
`modified_at`	datetime		Read-only. Timestamp of modification.
`removed`	boolean		Read-only.

1.94.2 Retrieve Available Attributes of the *AccountNoteModel*

Request

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

GET /api/v2/objspec/account_note

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/account_note'
```

1.94.3 Get Account Notes

Request

Method	GET
Path	/api/v2/account/<account_id>/note

GET /api/v2/account/<account_id>/note

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/account/8169529724050079749/note
```

Response

```
{
    "note": "Note content.",
    "result": "success"
}
```

1.94.4 Update Account Note

Request

Method	PATCH
Path	/api/v2/account/<account_id>/note
Headers	Content-Type: application/json
Body	AccountNoteModel

PATCH /api/v2/account/<account_id>/note

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.0.0.1/api/v2/account/8169529724050079749/note \
  -d '{"note": "Updated note."}'
```

Response

```
{
    "note": "Updated note.",
    "result": "success"
}
```

1.95 UAG - Account Hotseat Status

Note

- The `hotseat` check will return `true` (i.e., the account is considered in use) **only if** the `rdp_hotseat` option is enabled for the server associated with the account.
- This setting corresponds to the **"Inform about existing connection"** option in the server configuration UI.
- Only sessions that are **established via |product_name|** can be detected by this mechanism. Sessions opened outside of Fudo (e.g., direct RDP connections) will not trigger `hotseat: true`.

To enable it via API:

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://<host>/api/v2/server/<server_id> \
  -d '{"rdp_hotseat": true}'
```

Without this option, the endpoint will always return `hotseat: false`, even if a session is active.

1.95.1 Data Structures

Table 220: `AccountHotseatModel`

Attribute	Type	Required	Description
`account_id`	string	yes	ID of the account to check.
`server_id`	string	yes	ID of the server to check.
`server_address`	string	yes	Address of the server to check.
`server_port`	number	yes	Port of the server to check.

1.95.2 Retrieve Available Attributes of the *AccountHotseatModel*

Request

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

GET /api/v2/objspec/account_hotseat

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/account_hotseat'
```

1.95.3 Request Hotseat Status

Request

Method	`POST`
Path	`/api/v2/account/<account_id>/hotseat`
Headers	`Content-Type: application/json`
Body	`AccountHotseatModel`

POST /api/v2/account/<account_id>/hotseat

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{"server_address": "10.0.0.1", "server_port": 3389}' \
  https://10.0.0.1/api/v2/account/8169529724050079749/hotseat
```

Response

```
{
   "hotseat": true,
   "message": null,
   "result": "success"
}
```

1.96 UAG - Secret Checkout and Checkin

1.96.1 Data Structures

Checkout Object Specification

Table 221: `CheckoutModel`

Attribute	Type	Required	Description
`account_id`	string	yes	Account of which secret is retrieved.
`session_id`	string		When checkout session is ongoing, it can be reused.
`reason`	string		Reason to checkout secret. Required when login_reason is set in the safe.
`force`	boolean; default value `true`		Overrides exclusive checkout limit if configured.

1.96.2 Retrieve Available Attributes of the *CheckoutModel*

Request

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

GET /api/v2/objspec/checkout

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/checkout'
```

Checkin Object Specification

Table 222: `CheckinModel`

Attribute	Type	Required	Description
`session_id`	string	yes	Checkout session ID to stop.

1.96.3 Retrieve Available Attributes of the *CheckinModel*

Request

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

GET /api/v2/objspec/checkin

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/checkin'
```

1.96.4 Checkout Secret

Request

Method	`POST`
Path	`/api/v2/secret/checkout`
Headers	`Content-Type: application/json`
Body	`CheckoutModel`

POST /api/v2/secret/checkout

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.0.0.1/api/v2/secret/checkout \
  -d '{"account_id": "8169529724050079750", "reason": "emergency","force":false}
↪'
```

Note

- The `reason` field is optional and depends on the safe configuration. If not required, you can pass `"reason": null`.
- The `force` flag allows you to override exclusive checkout restrictions. If set to `false` and the password is already checked out, the system will wait until it is returned. To bypass this, set `force` to `true`.

Response

```
{
    "status": "approved",
    "session_id": "8169529724050079755",
    "timeout": null,
    "confirmation_timeout": null,
    "reason": null,
    "pwd": "password",
    "login": "Administrator",
    "domain": null,
    "result": "success"
}
```

Note

- In the following response, the password was revealed as `"pwd": "password"` and checkout session ID as `"session_id": "8169529724050079755"`.
- If there is a Password checkout time limit set for this specific account, the timeout will present the time (in seconds) after which the password is returned automatically (e.g., `"timeout": 1800`).
- If the **Require approval** option is enabled in the safe configuration, the `confirmation_timeout` specifies the timeframe (in minutes) within which authorized users can approve or reject the access request.

1.96.5 Repeat Checkout in the Same Session

Note

This scenario is used if the **Require approval** option is enabled in the safe configuration. After the administrator approves the access request, the request must be sent once more with the `session_id` number included to reveal the password.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
```

(continues on next page)

(continued from previous page)

```
  https://10.0.0.1/api/v2/secret/checkout \
  -d '{"account_id": "8169529724050079750", "reason": "emergency","force":false,
↪"session_id": "8169529724050079755"}'
```

Response

```
{
    "status": "approved",
    "session_id": "8169529724050079755",
    "timeout": null,
    "confirmation_timeout": null,
    "reason": null,
    "pwd": "password",
    "login": "Administrator",
    "domain": null,
    "result": "success"
}
```

1.96.6 Checkin Secret

To checkin the secret use `sesion_id` obtained in the checkout response.

Request

Method	`POST`
Path	`/api/v2/secret/checkin`
Headers	`Content-Type: application/json`
Body	`CheckinModel`

POST /api/v2/secret/checkin

Example Request

```
curl -s -k -X POST \
-H 'Authorization: sgfeea6jsaz4mum9su8w6' \
-H 'Content-Type: application/json' \
https://10.0.0.1/api/v2/secret/checkin \
-d '{"session_id": "8169529724050079755"}'
```

Response

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

1.97 UAG - Account Password History

1.97.1 List Password History Entries

Request

Method	GET
Path	/api/v2/account/<account_id>/secret_history

GET /api/v2/account/<account_id>/secret_history

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  "https://10.31.116.196/api/v2/account/8169529724050079750/secret_history?
↪filter=created_at.ge(2025-05-08T00:00:00Z),created_at.le(2025-07-08T23:59:59Z)
↪"
```

Response

```
{
    "items": [
        {
            "visible": true,
            "created_at": "2025-07-03T14:16:26.809242Z",
            "id": "4188347653454561300"
        },
        {
            "visible": true,
            "created_at": "2025-07-03T14:13:06.133029Z",
            "id": "4188347653454561299"
        },
        {
            "visible": true,
            "created_at": "2025-07-03T13:57:27.193281Z",
            "id": "4188347653454561282"
        }
    ],
    "result": "success"
}
```

1.97.2 Get Specific Historical Secret Value

Warning

This endpoint returns the historical password value in **plain text**. Access to this endpoint should be strictly controlled and limited to authorized users only.

Request

Method	GET

continues on next page

Table 224 – continued from previous page

Path	/api/v2/account/<account_id>/secret_history/<account_secret_id>

GET /api/v2/account/<account_id>/secret_history/<account_secret_id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  "https://10.31.116.196/api/v2/account/8169529724050079750/secret_history/
↪4188347653454561300"
```

Response

```
{
    "pwd": "Secret",
    "result": "success"
}
```

1.98 UAG - Secret Collections

Collections are containers for organizing secrets in a hierarchical structure within the Password Vault.

Note

Collections can only be created and managed in the Personal Vault. Organization Vault collections are managed by administrators through the main Fudo Enterprise system, not through the User Access Gateway.

1.98.1 Data Structures

Table 225: `CollectionModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Secret collection id. Unique.
`name`	string	yes	Collection name. Unique within parent collection. Case-insensitive.
`owner_id`	string		Write-only. Protected. Hidden. User ID of the personal vault owner.
`inherit_permiss:`	boolean		Read-only. Protected. Inherit permissions from parent collection.
`parent_id`	string		Parent collection id. Unique with name.
`subcollections_(`	number		Read-only. Expensive to use. Number of direct child collections.

continues on next page

Table 225 – continued from previous page

Attribute	Type	Required	Description
secrets_count	number		Read-only. Expensive to use. Number of descendant secrets.
path_to_root_ids	string-array		Read-only. Hidden. Expensive to use. Ordered list of ancestor collection IDs, starting with the root collection.
path_to_root_nar	string-array		Read-only. Hidden. Expensive to use. Ordered list of ancestor collection names, starting with the root collection.
access_policy	string		Read-only. Expensive to use. Access policy level. One of: view_on_request, view, edit_on_request, full_edit.
accessible_parer	string		Read-only. Hidden. Expensive to use. ID of the nearest ancestor collection that the user has direct access to view.
vault	string		Read-only. Hidden. Expensive to use. Vault type (organization, personal).
created_at	datetime		Read-only. Creation timestamp.
modified_at	datetime		Read-only. Modification timestamp.
removed	boolean		Read-only. Whether the collection has been removed.

1.98.2 Retrieve Available Attributes of the *CollectionModel*

Request

Method	GET
Path	/api/v2/objspec/collection

1.98.3 List Collections

Request

Method	GET
Path	/api/v2/collection

GET /api/v2/collection

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/collection'
```

Response

```
{
    "result": "success",
    "collection": [
        {
            "id": "3260606130216239105",
            "name": "Basic PV secrets",
            "subcollections_count": 0,
            "secrets_count": 4,
            "access_policy": "view_on_request",
            "created_at": "2026-04-17 06:34:37.877764-07",
            "modified_at": "2026-04-17 06:34:37.877764-07"
        },
        {
            "id": "3260606130216239118",
            "name": "Import Test Collection",
            "subcollections_count": 0,
            "secrets_count": 0,
            "access_policy": "full_edit",
            "created_at": "2026-04-22 06:00:55.155184-07",
            "modified_at": "2026-04-22 06:00:55.155184-07"
        }
    ]
}
```


1.98.4 Create Collection

Request

Method	`POST`
Path	`/api/v2/collection`
Headers	`Content-Type: application/json`
Body	`CollectionModel`

POST /api/v2/collection

Example Request

```
curl -s -k -X POST \
    -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
    -H 'Content-Type: application/json' \
    https://10.0.214.98/api/v2/collection \
    -d '{"name": "API Documentation Test"}'
```

Response


```
{
    "result": "success",
    "collection": {
        "id": "3260606130216239116"
```


(continues on next page)

(continued from previous page)

```
    }
}
```

1.98.5 Get Collection by ID

Request

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

GET /api/v2/collection/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/collection/3260606130216239109'
```

Response

```
{
    "result": "success",
    "collection": {
        "id": "3260606130216239105",
        "name": "Basic PV secrets",
        "subcollections_count": 0,
        "secrets_count": 4,
        "access_policy": "view_on_request",
        "created_at": "2026-04-17 06:34:37.877764-07",
        "modified_at": "2026-04-17 06:34:37.877764-07"
    }
}
```

1.98.6 Update Collection

Request

Method	`PATCH`
Path	`/api/v2/collection/<id>`
Headers	`Content-Type: application/json`
Body	`CollectionModel` (partial)

PATCH /api/v2/collection/<id>

Example Request

```
curl -s -k -X PATCH \
    -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
    -H 'Content-Type: application/json' \
```

(continues on next page)

(continued from previous page)

```
    https://10.0.214.98/api/v2/collection/3260606130216239109 \
    -d '{"name": "Updated Payment Collection"}'
```

Response

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

1.98.7 Delete Collection

Request

Method	DELETE
Path	/api/v2/collection/<id>

DELETE /api/v2/collection/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/collection/3260606130216239109'
```

Response

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

1.98.8 Import Secrets to Collection from CSV

This endpoint imports secrets from a CSV file into a collection. The CSV file must be constructed according to the following rules:

- The first row is a *header row* containing names corresponding to the API fields names (refer to *API Documentation:* Secrets).
- The *header row* must include all fields that are required when manually creating a secret of specific type. Other fields are optional and can be left empty.
- A comma (,) has to be used as a field separator.

Example CSV file:

```
name,type,login,domain,secret,uri
login,login,admin,portal.example.com,SuperSecure123!,https://portal.example.com/
↪login
login2,login,db_admin,db.example.com,DbPassword2024,https://db.example.com/admin
note,note,,,Quarterly meeting notes: Q4 targets discussed.,
api_key,apikey,aws_service_account,api.aws.amazon.com,AKIAIOSFODNN7EXAMPLE,
```

(continues on next page)

(continued from previous page)

```
↪https://api.aws.amazon.com
cert,certificate,,,,
ssh_key,sshkey,,,,
```

Note

SSH private keys and certificates are typically stored in multi-line PEM format. When importing them from a CSV file, enclose the entire value in double quotes ("") so it is treated as a single CSV field.

Example CSV for a certificate secret:

```
name,type,login,domain,certificate,secret
"secret-1","certificate","","","-----BEGIN CERTIFICATE-----
MIID...EXAMPLE...DATA
-----END CERTIFICATE-----","-----BEGIN PRIVATE KEY-----
MIIE...EXAMPLE...DATA
-----END PRIVATE KEY-----"
```

Request

Method	`POST`
Path	`/api/v2/collection/<id>/secret_import`
Headers	`Content-Type: multipart/form-data`
Body	`CSV file upload`

POST /api/v2/collection/<id>/secret_import

Example Request

```
curl -s -k -X POST \
    -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
    -F 'file=@secrets.csv' \
    'https://10.0.214.98/api/v2/collection/3260606130216239120/secret_import'
```

Response

```
{
    "result": "success",
    "imported_count": 5,
    "failed_count": 0,
    "skipped_count": 1
}
```

Note

The CSV file should have a header row with column names. Required columns: `name`, `type`.

1.99 UAG - Secret Management

Note

Secrets are encrypted data items stored in collections within the Password Vault.

Secret types supported:

- **login** - Username/password credentials
- **sshkey** - SSH private/public key pairs
- **note** - Secure text notes
- **apikey** - API tokens and keys
- **certificate** - X.509 certificates with private keys

1.99.1 Data Structures

Table 226: `SecretModel`

Attribute	Type	Required	Description
`id`	string		Read-only. Unique secret identifier.
`name`	string	yes	Secret name. Case-insensitive. Uniqueness is not required - a collection can hold several secrets with the same name.
`collection_id`	string	yes	Parent collection identifier.
`owner_id`	string		Read-only. Expensive to use. User ID of the personal vault owner.
`collection_name`	string		Read-only. Hidden. Expensive to use. Collection name.
`type`	string	yes	Immutable. Secret type. One of: `login`, `sshkey`, `note`, `apikey`, `certificate`.
`description`	string		Not encrypted secret description.
`login`	string	If `type == login || sshkey || apikey`	Username for authentication.
`domain`	string	If `type == login || sshkey || apikey`	Domain for the credential.
`certificate`	string	If `type == certifica`	X.509 certificate.
`x509_pubkey_fin`	string		Read-only. Expensive to use. Public key SHA256 fingerprint from certificate.

continues on next page

Table 226 – continued from previous page

Attribute	Type	Required	Description
secret	string		Protected. Encrypted secret value (password, private key, etc).
secret_passphra	string	If type == certifica || sshkey	Protected. Passphrase to decrypt private key.
has_secret	boolean		Read-only. Expensive to use. Whether secret value is set.
ssh_public_key	string		Read-only. Expensive to use. SSH public key from private key.
ssh_fingerprint_	string		Read-only. Expensive to use. SSH key SHA256 fingerprint.
access_policy	string		Read-only. Expensive to use. Access policy level.
checkout_mode	string		Read-only. Expensive to use. Checkout mode (simple, exclusive).
my_checkout_id	string		Read-only. Expensive to use. Current user's checkout ID if checked out.
my_checkout_exp	datetime		Read-only. Expensive to use. Managed secret access expiration time if user has active checkout.
key_pubkey_finge	string		Read-only. Expensive to use. TLS key SHA256 fingerprint derived from private key.
path_to_root_ids	string-array		Read-only. Hidden. Expensive to use. Ordered list of ancestor collection IDs, starting with the root collection.
path_to_root_nar	string-array		Read-only. Hidden. Expensive to use. Ordered list of ancestor collection names, starting with the root collection.
policy_compliant	boolean		Read-only. Hidden. Expensive to use. Indicates whether the secret conforms to global vault configuration requirements.
compromised	boolean		Read-only. Hidden. Expensive to use. Indicates whether the secret is known to be compromised.
policy_compliant	boolean	If type == login	Read-only. Hidden. Protected. Partial policy compliance check.
vault	string		Read-only. Hidden. Expensive to use. Vault type (organization, personal).
shared_with	string-array		Read-only. Hidden. Expensive to use. List of users you tried to share the secret with.

continues on next page

Table 226 – continued from previous page

Attribute	Type	Required	Description
checked_out_by_(	boolean		Read-only. Hidden. Expensive to use. Indicates whether another user currently has an active checkout of the secret.
created_at	datetime		Read-only. Creation timestamp.
modified_at	datetime		Read-only. Modification timestamp.
removed	boolean		Read-only. Soft deletion flag.

1.99.2 Retrieve Available Attributes of the *SecretModel*

Request

Method	GET
Path	/api/v2/objspec/secret

GET /api/v2/objspec/secret

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/secret'
```

1.99.3 List Secrets

Retrieve a list of secrets accessible to the user.

Request

Method	GET
Path	/api/v2/secret

GET /api/v2/secret

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/secret
```

Response

```
{
    "result": "success",
    "secret": [
        {
            "id": "3260606130216239105",
            "name": "secret for: root-fudo-PV",
```

(continues on next page)

(continued from previous page)


```
            "collection_id": "3260606130216239105",
            "type": "login",
            "login": "root",
            "has_secret": true,
            "access_policy": "view_on_request",
            "checkout_mode": "simple",
            "created_at": "2026-04-17 06:34:37.912715-07",
            "modified_at": "2026-04-17 06:34:37.91632-07"
        },
        {
            "id": "3260606130216239106",
            "name": "secret for: user01-macOS-PV",
            "collection_id": "3260606130216239105",
            "type": "login",
            "login": "user01",
            "has_secret": true,
            "access_policy": "view_on_request",
            "checkout_mode": "simple",
            "created_at": "2026-04-17 06:34:41.255687-07",
            "modified_at": "2026-04-17 06:34:41.257013-07"
        }
    ]
}
```


1.99.4 Get Secret by ID

Retrieve details of a specific secret.

Request

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

GET /api/v2/secret/<id>

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/secret/3260606130216239105
```

Response


```
{
    "result": "success",
    "secret": {
        "id": "3260606130216239105",
        "name": "secret for: root-fudo-PV",
        "collection_id": "3260606130216239105",
        "type": "login",
```


(continues on next page)

(continued from previous page)


```
        "login": "root",
        "has_secret": true,
        "access_policy": "view_on_request",
        "checkout_mode": "simple",
        "created_at": "2026-04-17 06:34:37.912715-07",
        "modified_at": "2026-04-17 06:34:37.91632-07"
    }
}
```


1.99.5 Create Secret

Create a new secret in a collection.

Request

Method	`POST`
Path	`/api/v2/secret`
Headers	`Content-Type: application/json`
Body	`SecretModel`

POST /api/v2/secret

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{
    "name": "Staging Database",
    "collection_id": "3260606130216239119",
    "type": "login",
    "description": "Staging environment database",
    "login": "staging_user",
    "domain": "staging.example.com",
    "secret": "StrongPassword123!"
  }' \
  'https://10.0.214.98/api/v2/secret'
```

Response


```
{
    "result": "success",
    "secret": {
        "id": "3260606130216239109"
    }
}
```

1.99.6 Update Secret

Update properties of an existing secret.

Request

Method	PATCH
Path	/api/v2/secret/<id>
Headers	Content-Type: application/json
Body	Partial SecretModel

PATCH /api/v2/secret/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{
    "description": "Updated description"
  }' \
  'https://10.0.214.98/api/v2/secret/3260606130216239109'
```

Response

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

1.99.7 Delete Secret

Permanently delete a secret from the collection.

Request

Method	DELETE
Path	/api/v2/secret/<id>

DELETE /api/v2/secret/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/secret/3260606130216239109'
```

Response

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

1.100 Secret History

Table 227: `SecretHistoryModel`

Attribut	Type	Required	Description
`id`	string	yes	Read-only. Secret history identifier.
`secre`	string	yes	Secret identifier.
`curre`	boolean	yes	Read-only. Whether it's the current version of secret.
`state`	string	yes	Read-only. Secret secret changer state. One of: `pending`, `confirmed`, `rejected`.
`creat`	datetime		Read-only. Creation timestamp.
`modif`	datetime		Read-only. Modification timestamp.
`remov`	boolean		Read-only.

1.100.1 Retrieve Available Attributes of the *SecretHistoryModel*

Request

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

GET /api/v2/objspec/secret_history

1.100.2 Get Secret History

Retrieve history of all secrets accessible to the user.

Request

Method	`GET`
Path	`/api/v2/secret/history`

GET /api/v2/secret/history

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/secret/history
```

Response

```
{
    "result": "success",
    "secret_history": [
        {
            "id": "3260606130216239105",
            "secret_id": "3260606130216239105",
```

(continues on next page)

(continued from previous page)


```
            "current": true,
            "state": "confirmed",
            "created_at": "2026-04-17 06:34:37.915698-07",
            "modified_at": "2026-04-17 06:34:37.915698-07"
        },
        {
            "id": "3260606130216239106",
            "secret_id": "3260606130216239106",
            "current": true,
            "state": "confirmed",
            "created_at": "2026-04-17 06:34:41.256853-07",
            "modified_at": "2026-04-17 06:34:41.256853-07"
        }
    ]
}
```


1.101 Shared Secrets

Table 228: `SecretSharedModel`

Attribut	Type	Required	Description
`id`	string		Read-only. Secret identifier.
`name`	string		Read-only. Secret name.
`colle`	string		Read-only. Parent collection identifier.
`colle`	string		Read-only. Hidden. Expensive to use. Collection name.
`type`	string		Read-only. Secret type.
`desci`	string		Read-only. Not encrypted secret description.
`logir`	string		Read-only. Username.
`domai`	string		Read-only. Domain.
`certi`	string		Read-only. X.509 certificate.
`secre`	string		Read-only. Protected. Encrypted secret.
`secre`	string		Read-only. Protected. Passphrase.
`has_s`	boolean		Read-only. Expensive to use. Whether secret is set.
`valic`	datetime		Read-only. Expensive to use. Expiration time of granted access.
`creat`	datetime		Read-only.
`modif`	datetime		Read-only.
`remov`	boolean		Read-only.

1.101.1 Retrieve Available Attributes of the *SecretSharedModel*

Request

Method	GET
Path	/api/v2/objspec/secret_shared

GET /api/v2/objspec/secret_shared

1.101.2 Get Shared Secrets

Retrieve secrets shared with the user through access requests.

Request

Method	GET
Path	/api/v2/secret/shared

GET /api/v2/secret/shared

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/secret/shared
```

Response

```
{
    "result": "success",
    "secret_shared": []
}
```

1.102 Secret URI Management

Table 229: SecretUriModel

Attribut	Type	Required	Description
id	string		Read-only. Unique secret URI identifier.
secre	string	yes	Immutable. Secret identifier.
secre	string		Read-only. Hidden. Expensive to use. Secret name.
uri	string	yes	URL/connection string assigned to the secret.
colle	string		Read-only. Hidden. Expensive to use. Collection identifier.
host	string		Read-only. Hidden. Host extracted from the provided uri.
port	number		Read-only. Hidden. Port extracted from the provided uri.
logir	string		Read-only. Hidden. Expensive to use.

continues on next page

Table 229 – continued from previous page

Attribut	Type	Required	Description
domai	string		Read-only. Hidden. Expensive to use.
vault	string		Read-only. Hidden. Expensive to use. Vault type (organization, personal).
creat	datetime		Read-only.
modif	datetime		Read-only.
remov	boolean		Read-only.

1.102.1 Retrieve Available Attributes of the *SecretUriModel*

Request

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

GET /api/v2/objspec/secret_uri

1.102.2 List All Secret URIs

Retrieve all URIs associated with secrets.

Request

Method	`GET`
Path	`/api/v2/secret/uri`

GET /api/v2/secret/uri

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  https://10.0.0.1/api/v2/secret/uri
```

Response

```
{
    "result": "success",
    "secret_uri": []
}
```

1.102.3 Get Secret URIs

Retrieve URIs associated with a specific secret.

Request

Method	`GET`
Path	`/api/v2/secret/<secret_id>/uri`

GET /api/v2/secret/<secret_id>/uri

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.0.1/api/v2/secret/3260606130216239110/uri'
```

Response

```
{
    "result": "success",
    "secret_uri": [
        {
            "id": "3260606130216239105",
            "secret_id": "3260606130216239110",
            "uri": "https://example.com/api",
            "created_at": "2026-04-22 08:53:41.4058-07",
            "modified_at": "2026-04-22 08:53:41.4058-07"
        }
    ]
}
```

1.102.4 Add URI to Secret

Associate a URI with a secret.

Request

Method	`POST`
Path	`/api/v2/secret/<secret_id>/uri`
Headers	`Content-Type: application/json`
Body	`SecretUriModel`

POST /api/v2/secret/<secret_id>/uri

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{"uri": "https://example.com/api"}' \
  'https://10.0.214.98/api/v2/secret/3260606130216239110/uri'
```

Response

```
{
    "result": "success",
    "secret_uri": {
        "id": "3260606130216239105"
    }
}
```

1.102.5 Update Secret URI

Update an existing URI associated with a secret.

Request

Method	PATCH
Path	/api/v2/secret/<secret_id>/uri/<id>
Headers	Content-Type: application/json
Body	Partial SecretUriModel

PATCH /api/v2/secret/<secret_id>/uri/<id>

Example Request

```
curl -s -k -X PATCH \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{"uri": "https://new-api.example.com/v2"}' \
  'https://10.0.214.98/api/v2/secret/3260606130216239110/uri/3260606130216239105
↪'
```

Response

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

1.102.6 Delete Secret URI

Remove a URI association from a secret.

Request

Method	DELETE
Path	/api/v2/secret/<secret_id>/uri/<id>

DELETE /api/v2/secret/<secret_id>/uri/<id>

Example Request

```
curl -s -k -X DELETE \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/secret/3260606130216239110/uri/3260606130216239105
↪'
```

Response

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

1.103 UAG - Secret Checkout/Checkin

Note

The checkout/checkin mechanism provides controlled access to secret values with audit trails.

When a secret is checked out, it becomes temporarily unavailable to other users until it is checked back in. This ensures exclusive access during sensitive operations.

Access to secrets may require approval through access requests, depending on the secret's `access_policy` setting:

- `full_edit` - Full access without approval
- `view_on_request` - Requires access request approval before checkout
- `none` - No access allowed

1.103.1 Data Structures

Table 230: `SecretCheckoutModel`

Attribute	Type	Required	Description
`secret_id`	string	yes	Secret identifier. Protected.

Table 231: `SecretCheckinModel`

Attribut	Type	Required	Description
`secre`	string	yes	Secret identifier. Protected.

1.103.2 Retrieve Available Attributes of the *SecretCheckoutModel*

Request

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

GET /api/v2/objspec/secret_checkout

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/secret_checkout'
```

1.103.3 Retrieve Available Attributes of the *SecretCheckinModel*

Request

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

GET /api/v2/objspec/secret_checkin

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/secret_checkin'
```

1.103.4 Checkout Secret

Checkout a secret to gain exclusive access to its value. The secret must be checked back in after use.

Note

If the secret's `access_policy` is set to `view_on_request`, an approved access request is required before checkout.

Request

Method	`POST`
Path	`/api/v2/secret/<secret_id>/checkout`
Headers	`Content-Type: application/json`
Body	`Empty or SecretCheckoutModel`

POST /api/v2/secret/<secret_id>/checkout

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.116.196/api/v2/secret/3260606130216239105/checkout \
  -d '{}'
```

Response

```
{
    "secret_access_id": "1",
    "checkout_type": "simple",
    "expires_at": null,
    "result": "success"
}
```

Note

After successful checkout, the secret will have a `my_checkout_id` field when queried via GET /secret/<secret_id>.

1.103.5 Checkin Secret

Return a previously checked out secret, making it available for other users.

Request

Method	`POST`
Path	`/api/v2/secret/<secret_id>/checkin`
Headers	`Content-Type: application/json`
Body	`Empty or SecretCheckinModel`

POST /api/v2/secret/<secret_id>/checkin

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.31.116.196/api/v2/secret/3260606130216239105/checkin \
  -d '{}'
```

Response

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

1.104 UAG - Secret Lookup

Note

Secret Lookup allows retrieving the plaintext value of a previously checked out secret from the Password Vault.

1.104.1 Data Structures

Table 232: `SecretLookupModel`

Attribute	Type	Required	Description
`secret_id`	string	yes	Protected. ID of a checked out secret.
`secret`	string		Read-only. Secret in plaintext (password, private key, etc).

1.104.2 Retrieve Available Attributes of the *SecretLookupModel*

Request

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

GET /api/v2/objspec/secret_lookup

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.33.2.133/api/v2/objspec/secret_lookup'
```

Response

```
{
    "result": "success",
    "secret_lookup": {
        "secret_id": {
            "type": "string",
            "description": "Id of a checked out secret.",
            "id": true,
            "required": true,
            "protected": true
        },
        "secret": {
            "type": "string",
            "readonly": true,
            "allow-empty": true,
            "description": "Secret in plaintext (password, private key, etc).",
            "filterable": true
        }
    }
}
```

1.104.3 Lookup Secret Value

Retrieve the plaintext value of a previously checked out secret.

Note

Prerequisites:

- The secret must be checked out first using `/api/v2/secret/<secret_id>/checkout`
- User must have active checkout session for this secret
- Checkout must not be expired

Request

Method	POST
Path	/api/v2/secret/<secret_id>/lookup
Headers	Content-Type: application/json
Body	Empty {} or omitted

POST /api/v2/secret/<secret_id>/lookup

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{}' \
  'https://10.33.2.133/api/v2/secret/3260606130216239105/lookup'
```

Success Response

```
{
    "result": "success",
    "secret": "MySecretPassword123!"
}
```

Error Response - Secret Not Checked Out

```
{
    "result": "failure",
    "message": "Secret is not checked out or checkout has expired"
}
```

Error Response - Insufficient Permissions

```
{
    "result": "failure",
    "message": "Insufficient permissions to access this secret"
}
```

1.104.4 Usage Example with Full Workflow

```
# Step 1: Checkout the secret
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{"secret_id": "3260606130216239105"}' \
  'https://10.33.2.133/api/v2/secret/3260606130216239105/checkout'

# Response: {"result": "success", "checkout_id": "3260606130216239201"}

# Step 2: Lookup the secret value
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
```

(continues on next page)

(continued from previous page)

```
  -H 'Content-Type: application/json' \
  -d '{}' \
  'https://10.33.2.133/api/v2/secret/3260606130216239105/lookup'

# Response: {"result": "success", "secret": "MySecretPassword123!"}

# Step 3: Checkin when done (optional but recommended)
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  -d '{"secret_id": "3260606130216239105"}' \
  'https://10.33.2.133/api/v2/secret/3260606130216239105/checkin'

# Response: {"result": "success"}
```

1.105 UAG - Secret History Reveal

Note

Secret History Reveal allows viewing historical values of secrets from the Password Vault. This is useful for auditing secret changes and retrieving previous secrets if needed.

1.105.1 Data Structures

Table 233: `SecretHistoryRevealModel`

Attribute	Type	Required	Description
`id`	string	yes	Protected. Secret history ID.
`secret`	string	yes	Read-only. Historical secret value in plaintext (password, private key, etc).

1.105.2 Retrieve Available Attributes of the *SecretHistoryRevealModel*

Request

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

GET /api/v2/objspec/secret_history_reveal

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.133/api/v2/objspec/secret_history_reveal'
```

1.105.3 Reveal Historical Secret Value

Retrieve the plaintext value of a specific historical version of a secret.

Warning

- This endpoint only works for historical versions (`current: false`)
- For current version (`current: true`), use checkout and lookup endpoints
- Accessing historical secret values requires special permissions
- The operation is audited in the system logs

Request

Method	`POST`
Path	`/api/v2/secret/history/<id>`
Headers	`Content-Type: application/json`
Body	`Empty {}`

POST /api/v2/secret/history/<id>

Note

`<id>` - Secret history ID obtained from `/api/v2/secret/history` endpoint.

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{}' \
  'https://10.33.2.133/api/v2/secret/history/5980780305148018689'
```

Success Response (Historical Version)

```
{
    "result": "success",
    "secret": "<historical password>"
}
```

Error Response - Current Version

```
# When trying to reveal current version (current: true)
{
    "result": "failure",
    "message": "Use checkout to reveal current secret."
}
```

Error Response - History Not Found

```
{
    "result": "failure",
    "message": "Secret history entry not found"
}
```

Error Response - Insufficient Permissions

```
{
    "result": "failure",
    "message": "Insufficient permissions to reveal historical secret values"
}
```

1.105.4 Complete Workflow Example

This example shows how to retrieve and reveal historical password values using real data:

```
# Step 1: Get secret history list
curl -s -k -X GET \
  -H 'Authorization: <token>' \
  'https://10.33.2.133/api/v2/secret/history'

# Response:
{
    "result": "success",
    "secret_history": [
        {
            "id": "5980780305148018689",
            "secret_id": "5980780305148018690",
            "current": false,
            "state": "confirmed",
            "created_at": "2026-06-05 10:21:47.992825-07",
            "modified_at": "2026-06-05 10:21:47.992825-07"
        },
        {
            "id": "5980780305148018690",
            "secret_id": "5980780305148018690",
            "current": true,
            "state": "confirmed",
            "created_at": "2026-06-09 02:41:45.662429-07",
            "modified_at": "2026-06-09 02:41:45.662429-07"
        }
    ]
}

# Step 2: Reveal historical value (current: false)
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{}' \
  'https://10.33.2.133/api/v2/secret/history/5980780305148018689'
```

(continues on next page)

(continued from previous page)

```
# Response: Success - returns old password
{
    "result": "success",
    "secret": "<password value>"
}

# Step 3: Try to reveal current value (current: true) - will fail
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{}' \
  'https://10.33.2.133/api/v2/secret/history/5980780305148018690'

# Response: Error - must use checkout for current version
{
    "result": "failure",
    "message": "Use checkout to reveal current secret."
}

# Step 4: For current version, use checkout and lookup instead
# First checkout:
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{}' \
  'https://10.33.2.133/api/v2/secret/5980780305148018690/checkout'

# Then lookup:
curl -s -k -X POST \
  -H 'Authorization: <token>' \
  -H 'Content-Type: application/json' \
  -d '{}' \
  'https://10.33.2.133/api/v2/secret/5980780305148018690/lookup'
```

1.105.5 Related Endpoints

- `GET /api/v2/secret/history` - List all secret history entries
- `GET /api/v2/secret/<id>` - Get current secret metadata (without revealing the value)
- `POST /api/v2/secret/<id>/checkout` - Checkout current secret for use
- `POST /api/v2/secret/<id>/lookup` - Reveal current checked-out secret value

1.106 UAG - Change Password NEW

1.106.1 Data Structures

Table 234: `ChangePasswordModel`

Attribute	Type	Required	Description
`state`	string		Change password state.
`password`	string	yes	Old or new password depending on state or prompt.
`method_id`	string		ID of the authentication method whose password is changed. See the section *Profile Authentication Methods Management*.

1.106.2 Retrieve Available Attributes of the *ChangePasswordModel*

Request

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

GET /api/v2/objspec/change_password

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/change_password'
```

1.106.3 Change Password

Request

Method	`POST`
Path	`/api/v2/change-password`
Headers	`Content-Type: application/json`
Body	`ChangePasswordModel`

POST /api/v2/change-password

Example Request

```
curl -s -k -X POST \
-H 'Authorization: sgfeea6jsaz4mum9su8w6' \
-H 'Content-Type: application/json' \
https://10.0.0.1/api/v2/change-password \
-d '{"password": "new-password"}'
```

Response

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

1.107 UAG - Change Language

1.107.1 Data Structures

Table 235: `ChangeLanguageModel`

Attribute	Type	Required	Description
`lang`	string	yes	Language code. Possible values: `en`, `pl`, `ru`, `ua`, `kk`.

1.107.2 Retrieve Available Attributes of the *ChangeLanguageModel*

Request

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

GET /api/v2/objspec/change_language

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/change_language'
```

1.107.3 Change Language

Request

Method	`POST`
Path	`/api/v2/change_language`
Headers	`Content-Type: application/json`
Body	`ChangeLanguageModel`

POST /api/v2/change_language

Example Request

```
curl -s -k -X POST \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  -H 'Content-Type: application/json' \
  https://10.0.0.1/api/v2/change_language \
  -d '{"lang": "pl"}'
```

Response

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

1.108 UAG - OTP Generation

1.108.1 Data Structures

Table 236: `OtpModel`

Attribute	Type	Required	Description
`account_id`	string	yes	The account to generate a one-time password.
`safe_id`	string	yes	Safe identifier.
`listener_id`	string	If `webclient == false`	Required if webclient is false.
`server_id`	string		Server identifier.
`server_address`	string		Valid IPv4 or IPv6 or hostname.
`server_port`	number		Value-format: port. Default port for given protocol is used if not passed.
`account_login`	string		Login for the account.
`webclient`	boolean; default value `false`		Whether the OTP is for a Webclient.

1.108.2 Retrieve Available Attributes of the *OtpModel*

Request

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

GET /api/v2/objspec/otp

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/otp'
```

1.108.3 Generate OTP

Request

Method	`POST`
Path	`/api/v2/secret/otp`
Headers	`Content-Type: application/json`
Body	`OtpModel`

POST /api/v2/secret/otp

Example Request

```
curl -s -k -X POST \
    -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
    -H 'Content-Type: application/json' \
    https://10.0.0.1/api/v2/secret/otp \
    -d '{"account_id": "8169529724050079750", "safe_id": "8169529724050079749",
↪"webclient":true,"server_address":"10.0.136.1","port":3389}'
```

Response

```
{
    "otp": "80434736YPxLckb4Wy_9f8Vuv7Z3OGv_",
    "result": "success"
}
```

1.109 UAG - Generating RDP Configuration

1.109.1 Data Structures

Table 237: `RdpConfigModel`

Attribute	Type	Required	Description
`host`	string	yes	Destination host.
`port`	number	yes	Connection port.
`otp`	string	yes	One-time password for RDP connection.
`app`	string		RemoteApp name (if applicable).
`suffix`	string		Optional suffix for session URL.
`safe_id`	string		Identifier of the Safe.
`server_id`	string		Identifier of the Server.
`listener_id`	string		Identifier of the Listener.

1.109.2 Retrieve Available Attributes of the *RdpConfigModel*

Request

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

GET /api/v2/objspec/rdp_config

Example Request

```
curl -s -k -X GET \
  -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
  'https://10.0.214.98/api/v2/objspec/rdp_config'
```

1.109.3 Generate RDP Configuration

Request

Method	`POST`
Path	`/api/v2/safe/rdp_config`
Headers	`Content-Type: application/json`
Body	`RdpConfigModel`

POST /api/v2/safe/rdp_config

Example Request

```
curl -s -k -X POST \
    -H 'Authorization: sgfeea6jsaz4mum9su8w6' \
    -H 'Content-Type: application/json' \
    https://10.0.0.1/api/v2/safe/rdp_config \
    -d '{
      "host": "10.31.116.195",
      "port": 3389,
      "otp": "80434736wemPxwmZnKsC8wQxjbUZ3axv",
      "app": "8169529724050079745",
      "suffix": "remoteapp-account",
      "safe_id": "8169529724050079745"
    }'
```

Note

The one-time password (`otp`) required in this request can be generated using the `POST /api/v2/secret/otp` endpoint. For more information, refer to the *UAG - OTP Generation* section.

Response

```
full address:s:10.31.116.195:3389
username:s:80434736wemPxwmZnKsC8wQxjbUZ3axv
prompt for credentials:i:1
password:s:
remoteapplicationmode:i:1
remoteapplicationprogram:s:remoteapp:8169529724050079745%
```