HTTPS API

Created by: Zsolt Démi, Software Development Manager
August 19, 2025

Content

BASIS OF OPERATION OF API

Basic Operation

The API can be used via HTTPS requests. Each function is available through a separate HTTPS URL — hereafter referred to as an ***endpoint***. Endpoints that retrieve information are of the HTTP GET type, while control and configuration endpoints that modify settings use the HTTP POST type.

To use the API, an API key is required. The API key is unique for each user and must be sent in the request header under the field API key.

The API server does not maintain a session, so each query and control operation must include the device ID and the device authentication credentials.

Different types of devices may have distinct endpoints for the same function. Therefore, the documentation specifies the supported device types for each endpoint.

Data Format

The API server always expects the input parameters of requests in JSON format, and responses are also always returned in JSON format. Therefore, even for queries, the required information must be included in the body of the request in JSON format.

Example:

```
{
   "hwid": “901F1232670F",
   "password": “9999",
   "type":"pager7"
}
```

Possible Responses

All API requests can basically result in two types of outcomes. If the request is successful, the result field of the JSON response will contain the value OK.

Example:

{ “result”:”OK”,

… }

If the result value is OK, then in addition to the result field, the response will always include a data JSON object. This data JSON contains the queried data and a status value. The status value must be 0 in case of success.

If the request fails, the JSON result field will contain the word ERROR and an additional error code in the error field.

Example:

{ "result": "ERROR",
"error": "authenticationError.accessDenied" }

Possible Error Codes

invalidCommmand : Invalid command – the device does not accept such a command.

invalidParameters : The specified parameters are incorrect. Only the values specified in the documentation are allowed to used for parameters.

crcError : The checksum is incorrect. An error occurred in the server–device communication; the command must be repeated.

commandError.communicationError : An error occurred in the server–device communication; the command must be repeated.

invalidPassword : Invalid password.

partitionAlwaysArmed : The state of the partition cannot be changed because this partition is always armed.

activeZoneDetected : The state of the partition cannot be changed because there is an active zone.

authenticationError.accessDenied : Authentication failed. The device ID – password pair is incorrect.

authenticationFailed : Authentication failed. The device ID – password pair is incorrect.
authenticationError.notAvailable : The device is not available, so authentication fails.

otherCommandInProgress: Another command is in progress, so this command failed. The command must be repeated.

ENDPOINTS

Pager7 / Smart Module BASE, Pager8

GET DEVICE STATUS

SUPPORTED DEVICE TYPE
Pager7 / Smart Module BASE
Pager8

Information about the device status can be obtained using this endpoint. If the response to the request is successful, the response includes the device's alarm memory, the status of its partitions, the state of the relay outputs, the values detected on the inputs, the power supply voltage, the GSM signal strength, and the values of the device registers (in the case of Pager8).

The parameters of the request are as follows:

hwid : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

password : The login password used on the device.

type : Can be either Pager7 or Pager8. The type of the target device must be specified in this field.

Endpoint	https://api.tell.hu/api/state
Request type	GET
Request body (sample)	
	{
	"hwid": "901F1232670F",
	"password": "9999",
	"type":"pager7"
	}
Response (sample)	
	{
	"result": "OK",

```
  "data": {
    "alarm": false,
    "alarmTime": null,
    "alarmEvent": null,
    "alarmEventParam1": null,
    "alarmEventParam2": null,
    "configReload": [],
    "partitions": {
      "1": true,
      "2": false
    },
    "relays": {
      "1": false
    },
    "inputs": {
      "1": 1,
      "2": 2700,
      "3": 1,
      "4": 1,
      "5": 0,
      "6": 0
    },
    "gsmSignalStrength": -52,
    "voltage": 20.8,
    "time": 1689934303,
    "registers": {}
  }
}
```

RELAY ON

SUPPORTED DEVICE TYPE
Pager7 / Smart Module BASE
Pager8

This command allows switching on the specified relay output of the device.

The parameters of the request are as follows:

hwid : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

password : The login password used on the device.

type : Can be either Pager7 or Pager8. The type of the target device must be specified in this field.

slot : The index of the relay to be controlled. This may vary depending on the device design — the Pager7 product comes in two versions: one with a single output and one with two outputs. The Pager8 product has 4 outputs. Accordingly, the index can be 1, 2, 3, or 4.

Endpoint	https://api.tell.hu/relay/close
Request type	GET
Request body (sample)	
	{
	"hwid": “901F1232670F",
	"password": “9999",
	“type":"pager7",
	“slot”:1
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0
	}
	}

RELAY OFF

SUPPORTED DEVICE TYPE
Pager7 / Smart Module BASE
Pager8

This command allows switching off the specified relay output of the device.

The parameters of the request are as follows:

hwid : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

password : The login password used on the device.

type : Can be either Pager7 or Pager8. The type of the target device must be specified in this field.

slot : The index of the relay to be controlled. This may vary depending on the device design — the Pager7 product comes in two versions: one with a single output and one with two outputs. The Pager8 product has 4 outputs. Accordingly, the index can be 1, 2, 3, or 4.

Endpoint	https://api.tell.hu/relay/open
Request type	GET
Request body (sample)	
	{
	"hwid": “901F1232670F",
	"password": “9999",
	“type”:"pager7",
	“slot”:1
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0
	}
	}

PARTITION ARMING

SUPPORTED DEVICE TYPE
Pager7 / Smart Module BASE
Pager8

This command is used to arm the partitions of the device.

The parameters of the request are as follows:

hwid : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

password : The login password used on the device.

type : Can be either Pager7 or Pager8. The type of the target device must be specified in this field.

slot : The index of the partition to be armed. The Pager7 and Pager8 products have two partitions, so the slot index can be 1 or 2.

Endpoint	https://api.tell.hu/partition/arm
Request type	GET
Request body (sample)	
	{
	"hwid": “901F1232670F",
	"password": “9999",
	“type":"pager7",
	“slot”:1
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0
	}
	}

PARTITION DISARMING

SUPPORTED DEVICE TYPE
Pager7 / Smart Module BASE
Pager8

This command is used to disarm the partitions of the device.

The parameters of the request are as follows:

hwid : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

password : The login password used on the device.

type : Can be either Pager7 or Pager8. The type of the target device must be specified in this field.

slot : The index of the partition to be armed. The Pager7 and Pager8 products have two partitions, so the slot index can be 1 or 2.

Endpoint	https://api.tell.hu/partition/disarm
Request type	GET
Request body (sample)	
	{
	"hwid": “901F1232670F",
	"password": “9999",
	“type":"pager7",
	“slot”:1
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0
	}
	}

RESTART PAGER DEVICE

SUPPORTED DEVICE TYPE
Pager7 / Smart Module BASE
Pager8

This command is used to restart (reboot) the device.

The parameters of the request are as follows:

hwid: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

password : The login password used on the device.

type : Can be either Pager7 or Pager8. The type of the target device must be specified in this field.

Endpoint	https://api.tell.hu/api/reboot
Request type	GET
Request body (sample)	
	{
	"hwid": “901F1232670F",
	"password": “9999",
	“type":"pager7"
	}
Response (sample)	
	{
	"result": "OK"
	}

GET FIRMWARE VERSION FROM DEVICE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin privileges to get the current firmware version of the device directly from the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin is being used.

uid: The user's unique identifier within the device (get first using the *getusers* request).

Endpoint	https://api.tell.hu/gc/getversionstatus
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	”uid”: ”a the user's unique identifier”
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	“fwVersion”: “10.01.3.8331”
	}
	}

GET FIRMWARE VERSION FROM SERVER

SUPPORTED DEVICE TYPE

Gate Control PRO

This command is used to query the firmware version number of the device from the server.

The parameters of the request are as follows:

hwid : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

appId : The application identifier. For Gate Control PRO devices, all software that uses the device via the API must be registered as a mobile application. A mobile application or the programming software of the device can be used for this purpose. The reason for this is that the Gate Control PRO device must store all control operations and associate them with a user in order to identify who initiated the action.

Response:

The response contains a JSON object named data. The version field of this object contains the firmware version number of the device.

Endpoint	https://api.tell.hu/gc/getdeviceversion
Request type	GET
Request body (sample)	
	{
	"hwid": “11:22:33:44:55:D1”,
	"appId": “9999439fe62ea874a3aa”
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0,
	"version": "9.00.2.8221"
	}
	}

GET THE DEVICE CONTROL MODE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command is used to get the control mode of the device.

The parameters of the request are as follows:

hwid : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

appId : The application identifier. For Gate Control PRO devices, all software that uses the device via the API must be registered as a mobile application. A mobile application or the programming software of the device can be used for this purpose. The reason for this is that the Gate Control PRO device must store all control operations and associate them with a user in order to identify who initiated the action.

Response:

The response contains a JSON object named data. The mode field of this object contains the device control mode. The mode can take values from 1 to 5, depending on the control mode. In this example, the device is in control mode 1.

Endpoint	https://api.tell.hu/gc/getoperationmode
Request type	GET
Request body (sample)	
	{
	"hwid": “11:22:33:44:55:D1”,
	"appId": “9999439fe62ea874a3aa”
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0,
	"mode": 1
	}
	}

GET SUPPORTED USER CAPACITY

SUPPORTED DEVICE TYPE

Gate Control PRO

This command is used to get the maximum number of users supported by the device.

The parameters of the request are as follows:

hwid: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

appId: The application identifier. For Gate Control PRO devices, all software that uses the device via the API must be registered as a mobile application. A mobile application or the programming software of the device can be used for this purpose. The reason for this is that the Gate Control PRO device must store all control operations and associate them with a user in order to identify who initiated the action.

Response:

The response contains a JSON object named data. The maxUsers field of this object contains the maximum number of users supported. In this response, the value is 1000, meaning the device is capable of managing up to 1000 users.

Endpoint	https://api.tell.hu/gc/getmaxusers
Request type	GET
Request body (sample)	
	{
	"hwid": “11:22:33:44:55:D1”,
	"appId": “9999439fe62ea874a3aa”
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0,
	"maxUsers": 1000
	}
	}

GATE OPENING COMMAND

SUPPORTED DEVICE TYPE

Gate Control PRO

This command can be used to trigger a gate opening on the device. The gate index to be opened can be specified using the data key.

The parameters of the request are as follows:

hwid: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

appId: The application identifier. For Gate Control PRO devices, all software that uses the device via the API must be registered as a mobile application. A mobile application or the programming software of the device can be used for this purpose. The reason for this is that the Gate Control PRO device must store all control operations and associate them with a user in order to identify who initiated the action.

data: The gate index must be specified in this parameter. If the value of data is 1, the gate opening command applies to output 1 of the device. If the value of data is 2, the gate opening command applies to output 2 of the device. **IMPORTANT:** The control mode of the device determines how the outputs operate. Therefore, in some cases, controlling output 2 may not be applicable.

Endpoint	https://api.tell.hu/gc/open
Request type	GET
Request body (sample)	
	{
	"hwid": “11:22:33:44:55:D1”,
	"appId": “9999439fe62ea874a3aa”,
	“data”: 1
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0
	}
	}

API USER REGISTRATION

SUPPORTED DEVICE TYPE

Gate Control PRO

This command enables the addition of a new user to a device that will be controlled via the API. It is required to access all other endpoints without the need for the API user to perform registration through the mobile application.

The parameters of the request are as follows:

hwid: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

password: The registration password belonging to the QR code of the device (default password: 1234).
This is used to register the Gate Control PRO device in the mobile app, i.e. to add mobile devices to the Gate Control PRO device.

Endpoint	https://api.tell.hu/gc/addappid
Request type	GET
Request body (sample)	
	{
	"hwid": “11:22:33:44:55:D1”,
	"password": “9876”
	}
Response (sample)	
	{
	"result": "OK",
	"data": {
	"status": 0,
	“appId”: “40-character-long identifier”
	}
	}

SUPERADMIN REGISTRATION

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows adding a new superadmin user to the device to be controlled via the API. This is required in order to access functions through the API that are only available to users with superadmin privileges.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

name: The username of the user to be registered (max. 40 characters).

phnr: The phone number of the user to be registered.

hwName: A custom name can be assigned to the device (appId) to be automatically created for the given user, which the user can then use to send requests. Any chosen string-type value can be used in this key (max. 40 characters).

Endpoint	https://api.tell.hu/gc/registrationrequest
Request type	POST
Request body (sample)	{
	“name”: “Elek”,
	"hwId": “11:22:33:44:55:D1”,
	"phnr": “0611234567”,
	“hwName”: “Device name”
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	“appId”: “40-character-long identifier”,
	“uid”: “The user's identifier within the device”
	}
	}

EDIT SUPERADMIN

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows modifying the data of a superadmin user.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

appId: The appId that identifies the application/project in which the superadmin is being used.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

name: The username of the user to be edited (get first using the *getusers* request).

phnr: The phone number of the user to be edited.

uid: The internal user identifier within the device (get first using the *getusers* request).

Endpoint	https://api.tell.hu/gc/editsuperadmin
Request type	POST
Request body (sample)	{
	“name”: “Elek”,
	"hwId": “11:22:33:44:55:D1”,
	"phnr": “0611234567”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“uid”: “The user's identifier within the device”
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	}
	}

GET GROUP RULES

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows listing the group rules of the device using a superadmin or admin user privilege.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

Endpoint	https://api.tell.hu/gc/getgroups
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	“groups”: [
	{
	“index”: 1,
	“uid”: “identifier of the group rule”,
	“name”: “group rule name”,
	“type”: true / false, // Allow/Deny

	“schemes”: [“plan identifier1”], // List of access templates (period / weekly plans) associated with the group rule (string array-bin UIDs)
	“startDate”: “2025.03.29. 00:00:00”,
	“endDate”: “2026.03.29. 00:00:00”,
	“ut”: “U | M | A | C | B” // The rule applies to: U = Registered users with User role M = Registered users with Administrator role A = Registered users with Superadmin role C = All registered users B = Everyone N = Incoming calls from unregistered phone number with presented caller ID X = Incoming calls from private phone numbers (with hidden caller ID)
	}
	]
	}
	}

ADD GROUP RULE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows adding a group rule to the device using superadmin or admin user privileges.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: Group rule name (max. 30 characters).

type: Rule type: Allow/Deny. This is a boolean variable, its value is either true=Allow or false=Deny.

startDate and ***endDate:*** Validity period of the group rule.
Both dates must be in the format: **YYYY.MM.DD HH:MM:SS.**

schem or ***schemes:*** Array of access templates (period / weekly plans) identifiers to which the group rule should apply (get first using the *getschemas* request).

ut: The rule applies to:

- **U =** Registered users with User role
- **M =** Registered users with Administrator role
- **A =** Registered users with Superadmin role
- **C =** All registered users
- **B =** Everyone
- **N =** Incoming calls from unregistered phone number with presented caller ID
- **X =** Incoming calls from private phone numbers (with hidden caller ID)

Endpoint	https://api.tell.hu/gc/addgroup
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “group rule name”,
	“type”: true / false, // Allow/Deny
	“startDate”: “2025.03.29. 00:00:00”,
	“endDate”: “2026.03.29. 00:00:00”,
	“schem”: [“plan identifier1”, “plan identifier2”],
	“ut”: “U | M | A | C | B” // The rule applies to: U = Registered users with User role M = Registered users with Administrator role A = Registered users with Superadmin role C = All registered users B = Everyone N = Incoming calls from unregistered phone number with presented caller ID X = Incoming calls from private phone numbers (with hidden caller ID)
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

EDIT GROUP RULE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to edit a group rule.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: Group rule name (max. 30 characters).

type: Rule type: Allow/Deny. This is a boolean variable, its value is either **true**=Allow or **false**=Deny.

startDate and ***endDate:*** Validity period of the group rule.
Both dates must be in the format: **YYYY.MM.DD HH:MM:SS.**

schem or ***schemes:*** Array of access templates (period / weekly plans) identifiers to which the group rule should apply (get first using the *getschemas* request).

uid: The internal identifier of the group rule to be edited within the device (get first using the *getschemas* request).

ut: The rule applies to:

- **U =** Registered users with **User** role
- **M =** Registered users with **Administrator** role
- **A =** Registered users with **Superadmin** role
- **C =** All registered users
- **B =** Everyone
- **N =** Incoming calls from unregistered phone number with presented caller ID
- **X =** Incoming calls from private phone numbers (with hidden caller ID)

Endpoint	https://api.tell.hu/gc/editgroup
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “group rule name”,
	“type”: true / false, // Allow/Deny
	“startDate”: “2025.03.29. 00:00:00”,
	“endDate”: “2026.03.29. 00:00:00”,
	“schem”: [“plan identifier1”, “plan identifier2”],
	“uid”: “unique identifier of the group rule”,
	“ut”: “U | M | A | C | B” // The rule applies to: U = Registered users with User role M = Registered users with Administrator role A = Registered users with Superadmin role C = All registered users B = Everyone N = Incoming calls from unregistered phone number with presented caller ID X = Incoming calls from private phone numbers (with hidden caller ID)
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

DELETE GROUP RULE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to delete a group rule.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

uid: The internal identifier of the group rule to be edited within the device (get first using the *getgroups* request).

Endpoint	https://api.tell.hu/gc/deletegroup
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “group rule name”,
	“uid”: “unique identifier of the group rule”
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

GET ACCESS TEMPLATES

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to list the device's access templates.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

Endpoint	https://api.tell.hu/gc/getschemas
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	“schemas”: [
	{
	“uid”: “access template identifier”,
	“name”: “access template name”,
	“days”: [// The scheme is valid on these days and at these times.

	{
	“day”: “mon | tue | wed, etc.”,
	“fromTime”: “00:00”,
	“toTime”: “23:59”
	}
	]
	}
	]
	}

ADD ACCESS TEMPLATE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to add an access template in the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: Name of the access template to be added (max. 16 characters).

days: List of the days on which the access template is valid. This is an array containing the following data:

day: A string representing the three-letter English abbreviation of the day of the week. Example: mon, tue

fromTime: Time in 24-hour format indicating the start time for that day.
Example: 12:01 (valid range: 00:00–23:59)

toTime: Time in 24-hour format indicating the start time for that day.
Example: 23:59 (valid range: 00:00–23:59)

Endpoint	https://api.tell.hu/gc/addschema
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “access template name”,
	“days”: [
	{
	“day”: “mon | tue | wed, etc.”,

	“fromTime”: “00:00”,
	“toTime”: “23:59”
	}
	]
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

EDIT ACCESS TEMPLATE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to edit an existing access template on the device.

The parameters of the request are as follows:

hwId : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: The name of the access template (get first using the *getschemas* request).

uid: The unique identifier of the access template (get first using the *getschemas* request).

days: A list of days and time intervals during which the access template is valid. This is an array containing the following data:

day: A string representing the three-letter English abbreviation of the day of the week. Example: mon, tue

fromTime: Time in 24-hour format indicating the start time for that day.
Example: 12:01 (valid range: 00:00–23:59)

toTime: Time in 24-hour format indicating the start time for that day.
Example: 23:59 (valid range: 00:00–23:59)

Endpoint	https://api.tell.hu/gc/editschema
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “access template name”,
	“uid”: “access template identifier”,

	“days”: [
	{
	“day”: “mon | tue | wed, etc.”,
	“fromTime”: “00:00”,
	“toTime”: “23:59”
	}
	]
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

DELETE ACCESS TEMPLATE

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to delete an existing access template from the device.

The parameters of the request are as follows:

hwId : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

uid: The unique identifier of the access template (get first using the *getschemas* request).

Endpoint	https://api.tell.hu/gc/deleteschema
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“uid”: “access template identifier”
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

GET USERS

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to list the users added in the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

startNumber: The starting index used for pagination. 0 refers to the first item.

count: Number of items to be returned.

Endpoint	https://api.tell.hu/gc/getusers
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“startNumber”: 0,
	“count”: 1
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	“users”: [
	{

	“uid”: “user identifier”,
	“name”: “user’s username”,
	“fname”: “user’s full name or comment”,
	“phoneNumber”: “user's phone number”,
	“index”: 0, //user sequence number
	“inserter”: “name of the person who added the user”,
	“schemes”: [”identifier1”, ”identifier2”], // Identifiers of the access templates assigned to the user.
	“role”: “U | M | A”, // Access level: U = User M = Administrator A = Superadministrator
	“call”: true / false, // Acknowledge control via phone call.
	“Sms”: true / false, // Acknowledge control via SMS.
	“out1”: true / false, // Is the user authorized to control output 1?
	“out2”: true / false, // Is the user authorized to control output 2?
	“accepter”: “name of the authorizing person”,
	“specificRuleType”: “A | D | ””, // Custom rule: A = The user is allowed D = The user is blocked "" = (Empty string) No custom rule applies
	“specificRuleFromDate”: “2025.03.29. 00:00:00”, // The custom rule is valid from this date
	“specificRuleToDate”: “2025.03.29. 23:59:59”, // The custom rule is valid until this dat
	“go1”: true / false, // Can the user control output 1 during a call?
	“go2”: true / false, // Can the user control output 2 during a call?
	“doorBell”: true / false, // Should the user receive notification on doorbell?

	“cam1”: true / false, // Camera 1 enabled?
	“cam2”: true / false, // Camera 2 enabled?
	“pushE”: true / false, // Push notification about technical error.
	“pushD”: true / false, // Push notification about limit switch error.
	“smsD”: true / false, // SMS notification about limit switch error.
	“approved”: true / false // Is the user enabled?
	}
	]
	}

ADD USER

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to add a new user to the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: The user's username (max. 40 characters).

fname: The user's full name or a comment (max. 40 characters).

phoneNumber: The user's phone number.

go1: Can the user control output 1 during a call? (true / false)

go2: Can the user control output 2 during a call? (true / false)

pushD: Push notification about terminal error. (true / false)

smsD: SMS notification about terminal error. (true / false)

inserter: The name of the user who is adding this user.

role: Role / access level.
"U | M | A"
Access level:
U = User
M = Administrator
A = Superadministrator

schemes: Array of access templates identifiers (uid) to be assigned to the user. Get the access templates first using the *getschemas* request. The answer will include the identifiers.

call: Acknowledge control via phone call. (true / false)

out1: Is the user authorized to control output 1? (true / false)

out2: Is the user authorized to control output 2? (true / false)

sms: Acknowledge control via SMS. (true / false)

specificRuleType: Custom rule.
“A | D | (empty string)”,
Custom rule:
A = The user is allowed
D = The user is blocked
"" = (Empty string) No custom rule applies

doorBell: Should the user receive a notification when the doorbell rings? (true / false)

cam1: Camera 1 enabled. (true / false)

cam2: Camera 2 enabled. (true / false)

pushE: Push notification about technical error. (true / false)

Endpoint	https://api.tell.hu/gc/adduser
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “user’s username”,
	“fname”: “user’s full name or comment”,
	“phoneNumber”: “user’s phone number”,
	“schemes”: [“identifier1”,”identifier2”],
	“go1”: true / false,
	“go2”: true / false,
	“pushD”: true / false,
	“smsD”: true / false,
	“inserter”: “name of the person who added the user”,
	“role”: “U | M | A” Access level: U = User M = Administrator A = Superadministrator
	“call”: true / false,
	“out1”: true / false,
	“out2”: true / false,

	“sms”: true / false,
	“specificRuleType”: “A | D | (empty string)”, Custom rule: A = The user is allowed D = The user is blocked "" = (Empty string) No custom rule applies
	“doorBell”: true / false,
	“cam1”: true / false,
	“cam2”: true / false,
	“pushE”: true / false
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

EDIT USER

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to edit an existing user added in the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

uid: The user's unique identifier within the device (get first using the *getusers* request).

name: The user's username (get first using the *getusers* request).

fname: The user's full name or a comment (max. 40 characters).

phoneNumber: The user's phone number.

go1: Can the user control output 1 during a call? (true / false)

go2: Can the user control output 2 during a call? (true / false)

pushD: Push notification about terminal error. (true / false)

smsD: SMS notification about terminal error. (true / false)

inserter: The name of the user who is adding this user.

role: Role / access level.
"U | M | A"
Access level:
U = User
M = Administrator
A = Superadministrator

schemes: Array of access templates identifiers (uid) to be assigned to the user. Get the access templates first using the *getschemas* request. The answer will include the identifiers.

call: Acknowledge control via phone call. (true / false)

out1: Is the user authorized to control output 1? (true / false)

out2: Is the user authorized to control output 2? (true / false)

sms: Acknowledge control via SMS. (true / false)

specificRuleType: Custom rule.
“A | D | (empty string)”,
Custom rule:
A = The user is allowed
D = The user is blocked
"" = (Empty string) No custom rule applies

doorBell: Should the user receive a notification when the doorbell rings? (true / false)

cam1: Camera 1 enabled. (true / false)

cam2: Camera 2 enabled. (true / false)

pushE: Push notification about technical error. (true / false)

Endpoint	https://api.tell.hu/gc/edituser
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	”uid”: ”the user's unique identifier”,
	“name”: “user’s username”,
	“fname”: “user’s full name or comment”,
	“phoneNumber”: “user’s phone number”,
	“schemes”: [“identifier1”,”identifier2”],
	“go1”: true / false,
	“go2”: true / false,
	“pushD”: true / false,
	“smsD”: true / false,
	“inserter”: “name of the person who added the user”,
	“role”: “U | M | A” Access level: U = User M = Administrator A = Superadministrator
	“call”: true / false,
	“out1”: true / false,
	“out2”: true / false,

	“sms”: true / false,
	“specificRuleType”: “A | D | ’”, Custom rule: A = The user is allowed D = The user is blocked "" = (Empty string) No custom rule applies
	“doorBell”: true / false,
	“cam1”: true / false,
	“cam2”: true / false,
	“pushE”: true / false
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

DELETE USER

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to delete an existing user from the device.

The parameters of the request are as follows:

hwId : The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

uid: The user's unique identifier on the device (get first using the *getusers* request).

Endpoint	https://api.tell.hu/gc/deleteuser
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“uid”: “a the user's unique identifier”
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

GET SCHEDULED CONTROLS

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to list the scheduled control plans added in the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

Endpoint	https://api.tell.hu/gc/getschedules
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	“schedules”: [
	{
	“index”: 1, // the index of the scheduled task
	“name”: “name of the scheduled task”,
	“days”: [// the days on which the scheduled task is active.
	{

	“day”: “mon | tue | wed, etc.”,
	“fromTime”: “00:00”,
	“toTime”: “23:59”
	}
	],
	”outs”: [// Outputs to which the task applies.
	{
	”index”: 1, // output index
	”on”: true/false // turned on/off
	}
	]
	}

ADD SCHEDULED CONTROL

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to add a scheduled control plan to the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: The name of the scheduled control plan (max. 16 characters).

days: This is an array that defines when the scheduled task should be active. Each element must contain the following data:

day: A string representing the three-letter English abbreviation of the day of the week. Example: mon, tue

fromTime: Time in 24-hour format indicating the start time for that day.
Example: 12:01 (valid range: 00:00–23:59)

toTime: Time in 24-hour format indicating the start time for that day.
Example: 23:59 (valid range: 00:00–23:59).

outs: Outputs. The outputs to which the schedule should apply. This is an array where each element must contain the following data:

index: The index number of the output.

on: Can have a value of true or false. Output on or off.

Endpoint	https://api.tell.hu/gc/addschedule
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “name of the scheduled task”,

	“days”: [
	{
	“day”: “mon | tue | wed, etc.”,
	“fromTime”: “00:00”,
	“toTime”: “23:59”
	}
	],
	”outs”: [
	{
	”index”: 1, // index
	”on”: true/false // turned on
	}
	]
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

EDIT SCHEDULED CONTROL

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to edit an existing scheduled control plan added in the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: The name of the scheduled control plan (get first using the *getschedules* request).

days: This is an array that defines when the scheduled task should be active. Each element must contain the following data:

day: A string representing the three-letter English abbreviation of the day of the week. Example: mon, tue

fromTime: Time in 24-hour format indicating the start time for that day.
Example: 12:01 (valid range: 00:00–23:59)

toTime: Time in 24-hour format indicating the start time for that day.
Example: 23:59 (valid range: 00:00–23:59).

outs: Outputs. The outputs to which the schedule should apply. This is an array where each element must contain the following data:

index: The index number of the output.

on: Can have a value of true or false. Output on or off.

Endpoint	https://api.tell.hu/gc/editschedule
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,

	“name”: “name of the scheduled task”,
	“days”: [
	{
	“day”: “mon | tue | wed, etc.”,
	“fromTime”: “00:00”,
	“toTime”: “23:59”
	}
	],
	”outs”: [
	{
	”index”: 1, // index
	”on”: true/false // turned on
	}
	]
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

DELETE SCHEDULED CONTROL

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to delete an existing scheduled control plan from the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

name: The name of the scheduled control task to be deleted (get first using the *getschedules* request).

Endpoint	https://api.tell.hu/gc/deleteschedule
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	“name”: “name of the scheduled task”
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

GET HOLIDAYS

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to list the holidays registered on the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

Endpoint	https://api.tell.hu/gc/getholidays
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”
	}
Response (sample)	{
	"data": {
	"result": “OK”,
	“holidays”: [
	{
	”index”: 1, // index
	”date”: ”2025.07.10”
	}
	]
	}

ADD HOLIDAYS

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to add a holiday to the device. The device can store a maximum of 120 holidays.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

date: The date to be added. Format: YYYY.MM.DD
Example: 2025.07.10.

Endpoint	https://api.tell.hu/gc/addholiday
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	”date”: ”2025.07.10”
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

DELETE HOLIDAYS

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to delete an existing holiday from the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

date: The date to be deleted. Format: YYYY.MM.DD
Example: 2025.07.10.

Endpoint	https://api.tell.hu/gc/deleteholiday
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	”date”: ”2025.07.10”
	}
Response (sample)	{
	"data": {
	"result": “OK”
	}
	}

GET EVENT LOGS

SUPPORTED DEVICE TYPE

Gate Control PRO

This command allows a user with superadmin or admin privileges to read the event logs from the device.

The parameters of the request are as follows:

hwId: The hardware identifier of the device. It can be found on the device box or copied from the programming software.

hwName: A custom name can be assigned to the device or project used to send requests. Any chosen string-type value can be used in this key (max. 40 characters). The value of this parameter is necessary for logging.

appId: The appId that identifies the application/project in which the superadmin/admin is being used.

count: Number of entries to read.

startNumber: Get entries starting from this index.

startDate: Get log entries from this date and time. Format: YYYY.MM.DD. HH:MM:SS
(Example: 2025.07.10. 00:00:00)

endDate: Get log entries up to this date and time. Format: YYYY.MM.DD. HH:MM:SS
(Example: 2025.07.11. 23:59:59)

Endpoint	https://api.tell.hu/gc/geteventlogs
Request type	POST
Request body (sample)	{
	"hwId": “11:22:33:44:55:D1”,
	“hwName”: “Device name”,
	“appId”: “40-character-long identifier”,
	”count”: 1,
	”startNumber”: 0,
	”startDate”: ”2025.07.10. 00:00:00”,
	”endDate”: ”2025.07.11. 23:59:59”
	}

Response (sample)	{
	”data”: {
	”statusCode”: 200,
	”result”: ”OK”,
	”size”: 100,
	”eventLogs”: [
	{
	”index”: 0, // index
	”type”: ”event type”,
	”uname”: ”name of the user who triggered the event”,
	”eid”: ”event identifier”,
	”dtime”: ”2025.07.10. 13:23:59”,
	”res”: ”event details”,
	”share”: 1
	}
	]
	}