HTTP API manual for 2N devices

v.3.3

www.2n.com

Content:

1. Introduction

HTTP API is an application interface designed for control of selected **2N devices** functions via the **HTTP**. It enables **2N devices** to be integrated easily with third party products, such as home automation, security and monitoring systems, etc.

HTTP API provides the following services:

- **System API** – provides device configuration changes, status info and upgrade.
- **Switch API** – provides switch status control and monitoring, e.g. door lock opening, etc.
- **I/O API** – provides device logic input/output control and monitoring.
- **Audio API** – provides audio playback control and microphone monitoring.
- **Camera API** – provides camera image control and monitoring.
- **Display API** – provides display control and user information display.
- **E-mail API** – provides sending of user e-mails.
- **Phone/Call API** – provides incoming/outgoing call control and monitoring.
- **Logging API** – provides reading of event records.

Set the transport protocol (**HTTP** or **HTTPS**) and way of authentication (**None**, **Basic** or **Digest**) for each function. Create up to five user accounts (with own username and password) in the **HTTP API** configuration for detailed access control of services and functions.

Use the configuration web interface on the **Services / HTTP API** tab to configure your **HTTP API**. Enable and configure all the available services and set the user account parameters.

Refer to https://ip_device_address/apitest for a special tool integrated in the device HTTP server for HTTP API demonstration and testing.

Caution

Warning
In order to ensure the full functionality and guaranteed performance, we strongly recommend that the topicality of the product / device version in use be verified as early as in the installation process. The customer hereby acknowledges that the product / device can achieve the guaranteed performance and full functionality pursuant to the manufacturer's instructions only if the latest product / device version is used after having been tested for full interoperability and not having been determined by the manufacturer as incompatible with certain versions of other products, and only in conformity with the manufacturer's instructions, guidelines or recommendations and in conjunction with suitable products and devices of other suppliers. The latest versions are available at https://www.2n.com/cs_CZ/ or can be updated via the configuration interface if the devices are adequately technically equipped. Should the customer use a product / device version other than the latest one or a version determined by the manufacturer as incompatible with certain versions of other products, or should the customer use the product / device in contradiction to the manufacturer's instructions, guidelines or recommendations or in conjunction with unsuitable products / devices of other suppliers, the customer is aware of and agrees with all functionality limitations of such a product / device if any as well as with all consequences incurred as a result thereof. Using a product / device version other than the latest one or a version determined by the manufacturer as incompatible with certain versions of other products, or using the product / device in contradiction to the manufacturer's instructions, guidelines or recommendations or in conjunction with unsuitable products / devices of other suppliers, the customer agrees that the 2N TELEKOMUNIKACE a.s. company shall not be held liable for any functionality limitation of such a product or any damage, loss or injury related to this potential functionality limitation.

1.1 HTTP API Release Notes

1.1 HTTP API Release Notes

Version	Changes
2.50	• Expansion of the **api/mobilekey/config** function **GET** response by the **pairingKey** object and detailed **keys** object description. • Change of the **keys** object in **GET** response to replace **key** parameter with **publicKey** and add optional parameters **type** and **ctime**.

Version	Changes
2.49	• Change of the **api/accesspoint/grantaccess** function behavior to activate the configured Door Switch instead of always triggering Switch 1.
2.47	• Expansion of the **api/display/image** function by the **displayLayer** parameter for **FlexiLayout** layer specification. • Change of the **api/phone/status** function to always return **sipNumber** parameter. • Change of the **api/lpr/licenseplate** function to support **plateText** parameter up to 12 characters with optional trimming to 10 characters.
2.45	• Change of the **api/dir/create** function to make JSON parameter parsing order-independent.
2.44	• HTTP API and Automation support for **2N LiftIP 2.0.** • Addition of the **api/system/timezone** function. • Addition of the **api/system/timezone/caps** function. • Expansion of the **api/system/time** function of the **PUT** method for time configuration.
2.42	• Addition of the **api/cert/ca** function. • Addition of the **api/cert/user** function.
2.40	• The **api/lpr/licenseplate** function has been extended to include parameters **lprID** and **lprDir**.
2.39	• New event **DtmfSent**.
2.38	• Expansion of the **MotionDetection** event by the **ID** parameter, which specifies the motion detection profile number on the web interface.
2.37	• Addition of the **api/accesspoint/grantaccess** function. • Addition of the **ApiAccessRequested** event generated whenever the **api/accesspoint/grantaccess** request is sent with the result "success" : true.

Version	Changes
2.36	• Expansion of the **api/switch/status** function by the **holdTimeout** parameter. • Expansion of the **api/switch/ctrl** function by the **timeout** parameter. • Addition of the **api/phone/calllog** function for call log download and deletion of selected / all records.
2.35	• Addition of the **api/system/time** function for device time retrieval. • Addition of the **api/system/time/set** function for device time setting. • Addition of the **users** parameter to **api/call/dial** for making calls to one or more users.
2.34	• Addition of the **api/lift/grantaccess** function for enabling lift floors based on authorization in another device.
	• Addition of the **/api/pcap/live**, **api/pcap/live/stop** and **api/pcap/stats** functions for incoming / outgoing packet capture control.
2.32	• Addition of the **/api/lpr/licenseplate** function for access control based on license plate recognition. • Addition of the **api/lpr/image** function for retrieving images received from license plate recognition.
2.31	• Addition of the **/api/mobilekey/config** for reading and writing location IDs and encryption keys for Bluetooth Authentication.
2.30	• Removal of the **apbBroken** parameter from the **AccessTaken** event. • Addition of the **apbBroken** parameter to the **UserAuthenticated** event.
2.29	• Addition of the new function for **api system caps**. • New event **CapabilitiesChanged**.
2.28	• Unchanged.

Version	Changes
2.27	• New events: **LiftStatusChanged, LiftConfigChanged, LiftFloorEnabled.** • Addition of the new functions for **api holidays, api config holidays, api dir template, api dir create, api dir update, api dir delete, api dir get, api dir query**.
2.26	• New events: **DtmfEntered**, **AccessTaken**, **ApLockStateChanged**, **RexActivated**.
2.25	• Unchanged.
2.24	• Change of user addition to the directory due to deletion of positions.
2.23	• Addition of the **switchDisabled** parametr to **UserRejected** event.
2.22	• New events: **CardHeld**, **PairingStateChanged**, **SwitchesBlocked**, **FingerEntered**, **MobKeyEntered**, **DoorStateChanged**, **UserRejected**, **DisplayTouched**.
2.21	• The **api/display/image** (**display**, **blob-image**, **blob-video**, **duration**, **repeat** parameters) function extended for **2N® IP Verso** • New events: **UserAuthenticated**, **SilentAlarm**, **AccessLimited** • Addition of the **timeSpan** parameter to the **/api/email/send** function
2.15	• New events: **TamperSwitchActivated**, **UnauthorizedDoorOpen**, **DoorOpenTooLong** and **LoginBlocked** • Addition of the **tzShift** event that gives the difference between the local time and Coordinated Universal Time (UTC) • The **email/send** function extended with a resolution setting option for the images to be sent

Version	Changes
2.14	• Addition of the **api/pcap**, **api/pcap/restart** and **api/pcap/stop** functions for network traffic download and control • Addition of the **audio/test** function for automatic audio test launch • Addition of the **email/send** function • Addition of the **response** parameter to the **/api/io/ctrl** and **/api/switch/ctrl** functions • The **/call/hangup** function extended with a **reason** parameter specifying the call end reason • New events: **MotionDetected, NoiseDetected** and **SwitchStateChanged** • The **CallStateChanged** event extended with a **reason** parameter specifying the call end reason
2.13	• First document version

2. HTTP API Description

All **HTTP API** commands are sent via **HTTP/HTTPS** to the intercom address with absolute path completed with the **/api** prefix. Which protocol you choose depends on the current intercom settings in the **Services / HTTP API** section. The **HTTP API** functions are assigned to services with defined security levels including the **TLS** connection request (i.e. **HTTPS**).

Example: *Switch 1 activation* http://10.0.23.193/api/switch/ctrl?switch=1&action=on

The absolute path includes the function group name (system, firmware, config, switch, etc.) and the function name (caps, status, ctrl, etc.).
To be accepted by the intercom, a request has to include the method and absolute path specification followed by the Host header.

Example:

```
GET /api/system/info HTTP/1.1
Host: 10.0.23.193
Intercom HTTP Server reply:
HTTP/1.1 200 OK
Server: HIP2.10.0.19.2
Content-Type: application/json
Content-Length: 253
{
  "success" : true,
  "result" : {
    "variant" : "2N IP Vario",
    "serialNumber" : "08-1860-0035",
    "hwVersion" : "535v1",
    "swVersion" : "2.10.0.19.2",
    "buildType" : "beta",
    "deviceName" : "2N IP Vario"
  }
}
```

This chapter also includes:

2.1 HTTP Methods

2N IP intercom applies the following four HTTP methods:

- **GET** – requests intercom content download or general command execution
- **POST** – requests intercom content download or general command execution
- **PUT** – requests intercom content upload
- **DELETE** – requests intercom content removal

The **GET** and **POST** methods are equivalent from the viewpoint of **HTTP API** but use different parameter transfers (refer to the next subsection). The **PUT** and **DELETE** methods are used for handling of such extensive objects as configuration, firmware, images and sound files.

2.2 Request Parameters

Practically all the **HTTP API** functions can have parameters. The parameters (switch, action, width, height, blob-image, etc.) are included in the description of the selected **HTTP API** function. The parameters can be transferred in three ways or their combinations:

1. in the request path (uri query, **GET**, **POST**, **PUT** and **DELETE** methods);
2. in the message content (application/x-www-form-urlencoded, **POST** and **PUT** methods);
3. in the message content (multipart/form-data, **POST** and **PUT** methods) – **RFC-1867**.

If the transfer methods are combined, a parameter may occur more times in the request. In that case, the last incidence is preferred.

There are two types of the **HTTP API** parameters:

1. Simple value parameters (switch, action, etc.) can be transferred using any of the above listed methods and do not contain the blob- prefix.
2. Large data parameters (configuration, firmware, images, etc.) always start with blob- and can only be transferred via the last-named method (multipart/form-data).

2.3 Replies to Requests

Replies to requests are mostly in the **JSON** format. Binary data download (user sounds, images, etc.) and intercom configuration requests are in **XML**. The Content-Type header specifies the response format. Three basic reply types are defined for **JSON**.

Positive Reply without Parameters

This reply is sent in case a request has been executed successfully for functions that do not return any parameters. This reply is always combined with the **HTTP** status code **200 OK**.

```
{
  "success" : true,
}
```

Positive Reply with Parameters

This reply is sent in case a request has been executed successfully for functions that return supplementary parameters. The **result** item includes other reply parameters related to the function. This reply is always combined with the **HTTP** status code **200 OK**.

```
{
  "success" : true,
  "result" : {
    ...
  }
}
```

Negative Reply at Request Error

This reply is sent in case an error occurs during request processing. The reply specifies the error code (**code**), text description (**description**) and error details if necessary (**param**). The reply can be combined with the **HTTP** status code **200 OK** or **401 Authorisation Required**.

```
{
  "success" : false,
  "error" : {
    "code" : 12,
    "param" : "port",
    "description" : "invalid parameter value"
  }
}
```

The table below includes a list of available error codes.

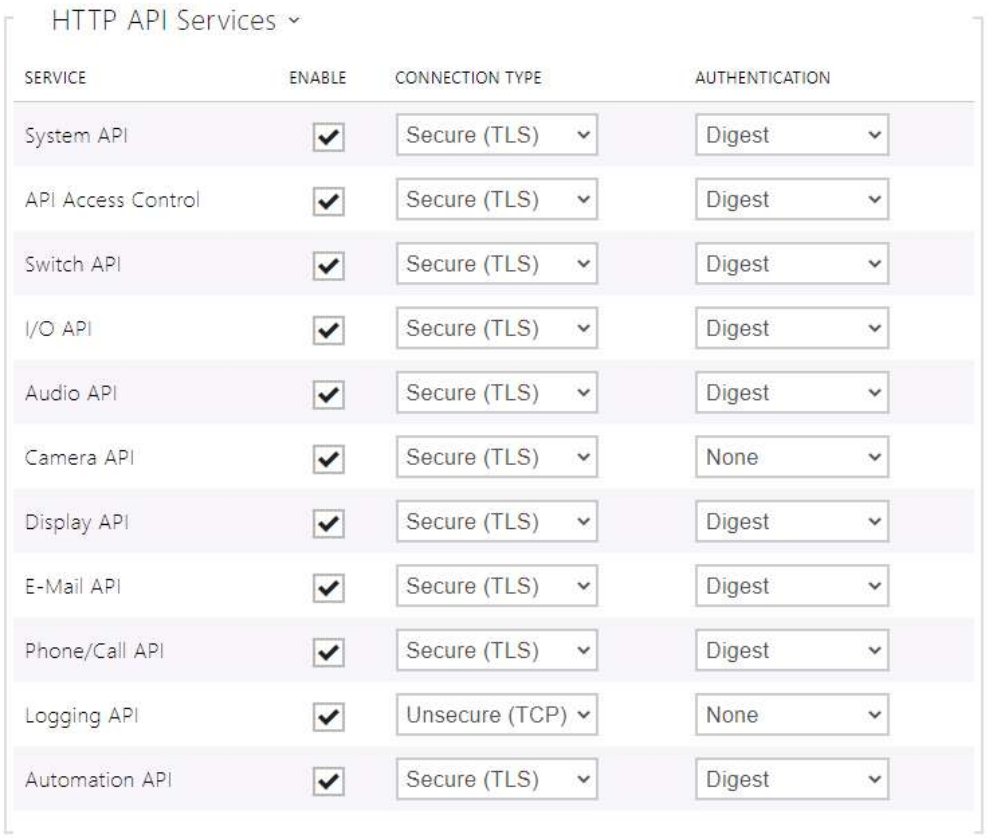
Code	Description	
1	function is not supported	The requested function is unavailable in this model.
2	invalid request path	The absolute path specified in the **HTTP** request does not match any of the **HTTP API** functions.

Code	Description	
3	invalid request method	The **HTTP** method used is invalid for the selected function.
4	function is disabled	The function (service) is disabled. Enable the function on the **Services** / **HTTP API** configuration interface page.
7	invalid connection type	**HTTPS** connection is required.
8	invalid authentication method	The authentication method used is invalid for the selected service. This error happens when the Digest method is only enabled for the service but the client tries to authenticate via the Basic method.
9	authorisation required	User authorisation is required for the service access. This error is sent together with the **HTTP** status code Authorisation Required.
10	insufficient user privileges	The user to be authenticated has insufficient privileges for the function.
11	missing mandatory parameter	The request lacks a mandatory parameter. Refer to **param** for the parameter name.
12	invalid parameter value	A parameter value is invalid. Refer to **param** for the parameter name.
13	parameter data too big	The parameter data exceed the acceptable limit. Refer to **param** for the parameter name.
14	unspecified processing error	An unspecified error occurred during request processing.

Code	Description	
15	no data available	The required data are not available on the server.
17	parameter shouldn't be present	Parameter collision (it is impossible to write a specified parameter combination).
18	request is rejected	The request cannot be processed now and was rejected by the device.
19	file version is lower than minimum	The submitted file version is lower than required.

3. HTTP API Services Security

Set the security level for each **HTTP API** service via the **2N IP intercom** configuration web interface on the **Services / HTTP API** tab: disable/enable a service and select the required communication protocol and user authentication method.



Set the required transport protocol for each service separately:

- **HTTP** – send requests via **HTTP** or **HTTPS**. Both the protocols are enabled and the security level is defined by the protocol used.
- **HTTPS** – send requests via **HTTPS**. Any requests sent via the unsecured **HTTP** are rejected by the intercom. **HTTPS** secures that no unauthorised person may read the contents of sent/received messages.

Set authentication methods for the requests to be sent to the intercom for each service. If the required authentication is not executed, the request will be rejected. Requests are authenticated via a standard authentication protocol described in **RFC-2617**. The following three authentication methods are available:

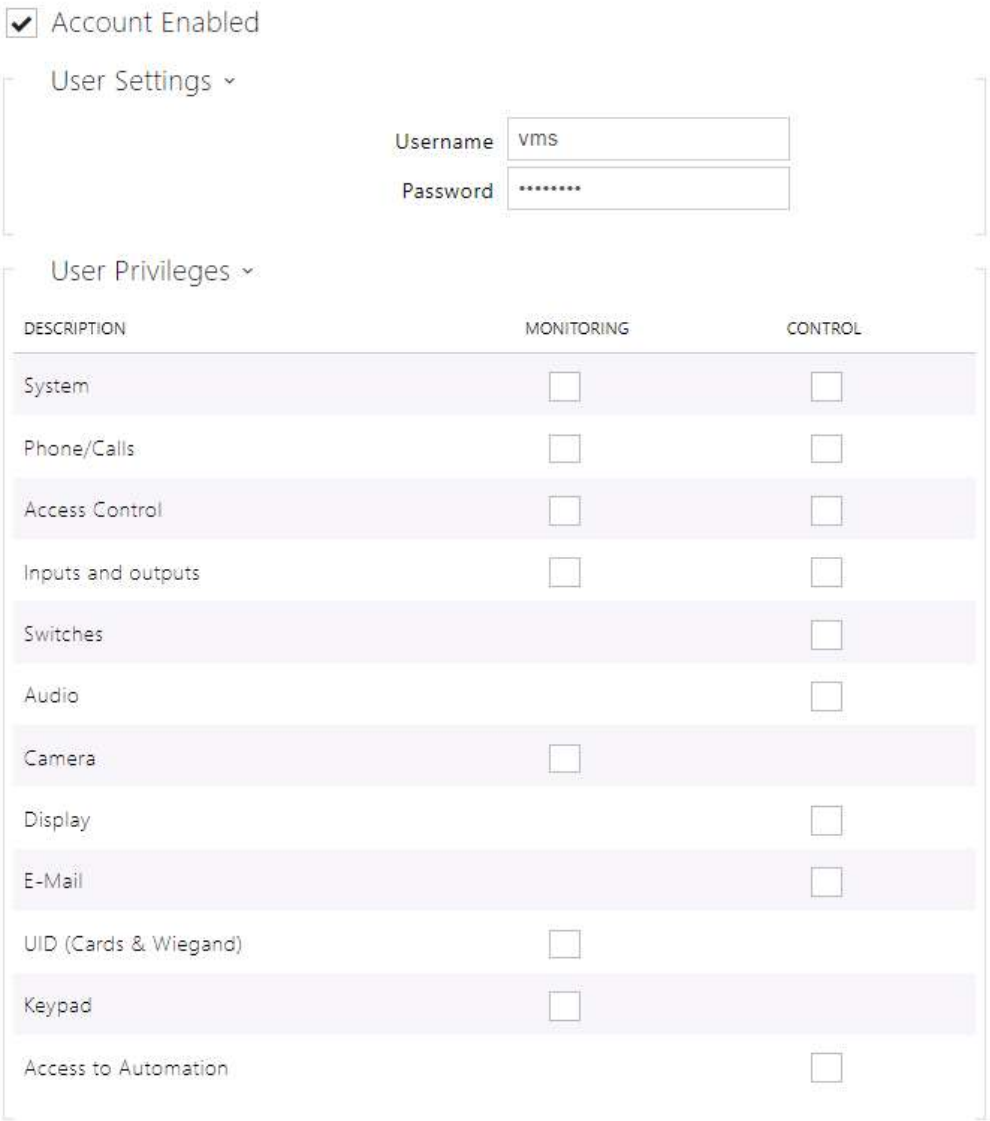
- **None** – no authentication is required. In this case, this service is completely unsecure in the **LAN**.
- **Basic** – Basic authentication is required according to **RFC-2617**. In this case, the service is protected with a password transmitted in an open format. Thus, we recommend you to combine this option with **HTTPS** where possible.

- **Digest** – Digest authentication is required according to **RFC-2617**. This is the default and most secure option of the three above listed methods.

We recommend you to use the **HTTPS + Digest** combination for all the services to achieve the highest security and avoid misuse. If the other party does not support this combination, the selected service can be granted a dispensation and assigned a lower security level.

4. User Accounts

With **2N IP intercom** you can administer up to five user accounts for access to the **HTTP API** services. The user account contains the user's name, password and **HTTP API** access privileges.



Use the table above to control the user account privileges to the **HTTP API** services.

5. Overview of HTTP API Functions

The table below provides a list of all available **HTTP API** functions including:

- the **HTTP** request absolute path;
- the supported **HTTP** methods;
- the service in which the function is included;
- the required user privileges (if authentication is used);
- the use of the selected function is not subject to license in versions FW 2.35 and higher (i.e. the function is avalaible without entering the license key)

Absolute path	Method	Service	Privileges
/api/automation/trigger	GET	Automation	Access to Automation
/api/accesspoint/blocking/ctrl	GET/POST	Access Control	Access Control – Control
/api/accesspoint/blocking/status	GET/POST	Access Control	Access Control – Monitoring
/api/accesspoint/grantaccess	GET/POST	Access Control	Access Control – Control
/api/audio/test	GET/POST	Audio	Audio – Control
/api/call/answer	GET/POST	Phone/Call	Phone/Calls – Control
/api/call/dial	GET/POST	Phone/Call	Phone/Calls – Control
/api/call/hangup	GET/POST	Phone/Call	Phone/Calls – Control
/api/call/status	GET/POST	Phone/Call	Phone/Calls – Monitoring
/api/camera/caps	GET/POST	Camera	Camera – Monitoring
/api/camera/snapshot	GET/POST	Camera	Camera – Monitoring
/api/config	GET/POST/PUT	System	System – Control
/api/config/factoryreset	GET/POST	System	System – Control
/api/config/holidays	GET/PUT	System	System – Control
/api/dir/create	PUT	System	System – Control

Absolute path	Method	Service	Privileges
/api/dir/delete	PUT	System	System – Control
/api/dir/get	POST	System	System – Control
/api/dir/query	POST	System	System – Control
/api/dir/template	GET/POST	System	System – Control
/api/dir/update	PUT	System	System – Control
/api/display/caps	GET/POST	Display	Display – Control
/api/display/image	PUT/DELETE	Display	Display – Control
/api/email/send	GET/POST	E-mail	E-mail – Control
/api/firmware	PUT	System	System – Control
/api/firmware/apply	GET/POST	System	System – Control
/api/firmware/reject	GET/POST	System	System – Control
/api/holidays	GET/PUT	System	System – Control
/api/io/caps	GET/POST	I/O	Inputs and outputs – Monitoring
/api/io/ctrl	GET/POST	I/O	Inputs and outputs – Monitoring
/api/io/status	GET/POST	I/O	Inputs and outputs – Monitoring
/api/lift/grantaccess	GET/POST	Access Control	Access Control – Control
/api/log/caps	GET/POST	Logging	–
/api/log/pull	GET/POST	Logging	–
/api/log/subscribe	GET/POST	Logging	*
/api/log/unsubscribe	GET/POST	Logging	*

Absolute path	Method	Service	Privileges
/api/lpr/image	GET/POST	Access Control	Access Control – Monitoring
/api/lpr/licenseplate	POST	Access Control	Access Control – Control
/api/mobilekey/config	GET/PUT	Access Control	Access Control – Monitoring
/api/pcap	GET/POST	System	System – Control
/api/pcap/live	GET/POST	System	System – Control
/api/pcap/live/stats	GET/POST	System	System – Control
/api/pcap/live/stop	GET/POST	System	System – Control
/api/pcap/restart	GET/POST	System	System – Control
/api/pcap/stop	GET/POST	System	System – Control
/api/phone/calllog	DELETE	Phone/Call	Phone/Calls – Control
/api/phone/calllog	GET/POST	Phone/Call	Phone/Calls – Monitoring
/api/phone/status	GET/POST	Phone/Call	Phone/Calls – Monitoring
/api/switch/caps	GET/POST	Switch	Switches – Monitoring
/api/switch/ctrl	GET/POST	Switch	Switches – Control
/api/switch/status	GET/POST	Switch	Switches – Monitoring
/api/system/caps	GET	System	System – Monitoring
/api/system/info	GET/POST	System	–
/api/system/restart	GET/POST	System	System – Control
/api/system/status	GET/POST	System	System – Control

Absolute path	Method	Service	Privileges
/api/system/time	GET/POST/PUT	System	System – Monitoring/ Control
/api/system/time/set	GET/POST	System	System – Control
/api/system/timezone	GET/PUT	System	System – Monitoring/ Control
/api/system/timezone/ caps	GET	System	System – Monitoring
/api/system/ca	GET/PUT/DELETE	System	System – Control
/api/system/user	GET/PUT/DELETE	System	System – Control

This section also includes:

5.1 api system

The following subsections detail the HTTP functions available for the **api/system** service.

5.1.1 api system info

The **/api/system/info** function provides basic information on the device: type, serial number, firmware version, etc. The function is available in all device types regardless of the set access rights.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes the following information on the device:

Parameter	Description
devType	Internal device identifier
variant	Model name (version)
variantId	Internal numerical identifier of the product
customerId	Internal numerical identifier
serialNumber	Serial number
macAddr	Network identifier of the device
hwVersion	Hardware version
swVersion	Firmware version
buildType	Firmware build type (alpha, beta, or empty value for official versions)
firmwarePackage	FW package indication
deviceName	Device name set in the configuration interface on the **Services / Web Server** tab

Caution

- For versions 2.33.2 and higher, the "buildType" key value range is changed; the value will include the "release" string for the official version. For versions 2.32.1 and lower, the "buildType" value range is empty for the official version.

Example:

```
GET /api/system/info
{
  "success" : true,
  "result" : {
    "devType" : "2-14-0-0",
    "variant" : "2N IP Verso",
    "variantId" : 14,
    "customerId" : 0,
    "serialNumber" : "00-0000-0005",
    "macAddr" : "FC-1E-B3-00-00-05",
    "hwVersion" : "570v1",
    "swVersion" : "2.35.0.45.0",
    "buildType" : "dev",
    "firmwarePackage" : "verso",
    "deviceName" : "2N IP Verso"
  }
}
```

5.1.2 api system status

The **/api/system/status** function returns the current intercom status.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes the current device status.

Parameter	Description
systemTime	Device real time in seconds since 00:00 1.1.1970 (unix time)
upTime	Device operation time since the last restart in seconds

Example:

```
GET /api/system/status
{
  "success" : true,
  "result" : {
    "systemTime" : 1418225091,
    "upTime" : 190524
  }
}
```

5.1.3 api system restart

The **/api/system/restart** restarts the intercom.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/system/restart
{
  "success" : true
}
```

5.1.4 api system caps

The **/api/system/caps** function is used for sending information to **2N® Access Commander** on a change in the list of available functions of the device.

The function is part of the **System API** service and the user has to be assigned the **System** privilege for authentication if required.

The **GET** method can be used for this function.

The reply is in the **application/json** format and includes a set of device info.

```
{   "success":true,
    "result":{
     "options":{
         "codecG722":"active,licensed",
         "codecG729":"active",
         "codecL16":"active",
         "audioLoopTest":"active,licensed",
         "noiseDetection":"active,licensed",
         "userSounds":"active,licensed",
         "adaptiveVolume":"active",
         "antiHowling":"active",
         "keyBeep":"active",
         "camera":"active",
         "video":"active",
         "cameraPtz":"active,licensed",
         "motionDetection":"active,licensed",
         "encH264":"active",
         "encH263":"active",
         "encMpeg4":"active",
         "encJpeg":"active",
         "decH264":"active",
         "phone":"active",
         "phoneVideo":"active",
         "phoneVideoOut":"active",
         "sips":"active,licensed",
         "srtp":"active,licensed",
         "callAnswerMode":"active",
         "doorOpenCallback":"active",
         "rtspServer":"active,licensed",
         "rtspClient":"active,licensed",
         "audioMulticast":"active",
         "smtpClient":"active,licensed",
         "ftpClient":"active,licensed",
         "onvif":"active,licensed",
         "snmp":"active,licensed",
         "tr069":"active,licensed",
         "knocker":"active",
         "my2n":"active",
         "informacast":"active,licensed",
         "autoProv":"active,licensed",
         "httpApi":"active,licensed",
         "eap":"active,licensed",
         "eapMd5":"active,licensed",
         "eapTls":"active,licensed",
         "vpn":"active",
         "userVpn":"active",
         "rioManager":"active,licensed",
         "siteChannel":"active",
         "localCalls":"active",
         "switches":"active",
         "advancedSwitches":"active,licensed",
         "switchUserCodes":"active",
```

```
            "securedInput":"active",
            "rexInput":"active",
            "tamperInput":"active",
            "doorSensor":"active",
            "keypad":"active",
            "buttons":"active",
            "liftControl":"active,licensed",
            "limitFailedAccess":"active,licensed",
            "silentAlarm":"active,licensed",
            "scrambleKeypad":"active,licensed",
            "tamperBlockSwitch":"active,licensed",
            "antiPassback":"active,licensed",
            "dir":"active",
            "dirDeputy":"active",
            "dirPhoto":"active",
            "automation":"active,licensed",
            "licDownload":"active",
            "profiles":"active",
            "licensing":"active",
            "Ac2n":"active",
            "doorControl":"active",
            "nfc":"active,licensed",
            "vbus":"active",
            "vbusExtenders":"active",
            "cardReader":"active",
            "fpReader":"active",
            "bleReader":"active",
            "wiegand":"active",
            "powerManager":"active",
            "audioInput":"active",
            "lightSensor":"active",
            "irLed":"active",
            "backlight":"active",
            "backlightDayNight":"active",
            "display":"active"
        }

    }


}
```


5.1.5 api system time

The **/api/system/time** function is used for device time retrieval or setting.

You can use the **GET** method for data retrieval and the **PUT** method for configuration upload.

GET method

The function is part of the **System** service and the user has to be assigned the **System (Monitoring)** privilege for authentication if required.

No parameters are defined for the **GET** method.

The response is in the **application/json** format and includes the device real time in seconds from 00:00 1.1.1970 (unix time).

Example:

```
GET /api/system/time
{
  "success" : true,
  "result" : {
    "utcTime" : 1639472172,
    "source" : "My2N",
    "automatic" : true,
  }
}
```

PUT method

Caution

- We recommend that this endpoint is used for time setting only in case the ***Use time from Internet*** parameter is disabled. If it is enabled, the time value is overwritten with a value from the NTP server or the My2N time service.

The function is part of the **System** service and the user has to be assigned the **System (Control)** privilege for authentication if required.

Request parameters for **PUT**:

Parameter	Description
automatic	automatic time retrieval from NTP server If true is completed, no more parameters are entered.
utcTime	number = unix time, min BuildTime, max 2147483647
server	NTP Server Address (IPv4 address or domain)

The reply is in the **application/json** format.

```
PUT /api/system/time?automatic=0&server=pool.ntp.org&utcTime=1700829813{ "success" :
true, }
```

5.1.6 api system timezone

The **/api/system/timezone** function is used for obtaining information on the device time zone or for time zone setting.

You can use the **GET** method for data retrieval and the **PUT** method for configuration upload.

GET method

The function is part of the **System** service and the user has to be assigned the **System (Monitoring)** privilege for authentication if required.

No parameters are defined for the **GET** method.

The response is in the **application/json** format and includes information on whether the zone has been set automatically and what time zone has been set. In case the time zone has been set manually, the custom parameter shows the zone creating rule.

Example:

```
GET /api/system/timezone
{
    "success": true,
    "result": {
        "automatic": true,
        "zone": "America/Los Angeles"
    }
}
nebo
{
    "success": true,
    "result": {
        "automatic": false
        "zone": "custom",
        "custom": "UTC-08:00"
    }
}
```

PUT method

The function is part of the **System** service and the user has to be assigned the **System (Control)** privilege for authentication if required.

Request parameters for **PUT**:

Parametr	Popis
automatic	0 or 1 If true (1) is completed, no more parameters are entered.
zone	Define the zone: enter either the zone name or "custom" for manual setting. Refer to the zone name list on the 5.1.7 api system timezone caps endpoint.
custom	Define the zone by writing *UTC−08:00, UTC+03:00*, etc. Available for zone="custom" only.

Example:

```
PUT /api/system/timezone?automatic=0&zone=custom&custom=UTC-08:00
{
  "success" : true
}
```

5.1.7 api system timezone caps

The **api/system/timezone/caps** returns a list of available time zones.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The response is in the **application/json.**

```
GET /api/system/timezone/caps
{
  "success": true,
  "result": {
    "timezones": [
      "Africa/Abidjan",
      "Africa/Accra",
      "Africa/Bissau",
      "Africa/Monrovia",
      "Africa/Sao_Tome",
      "America/Danmarkshavn",
      "Antarctica/Troll",
      "Atlantic/Canary",
      "Atlantic/Faroe",
      "Atlantic/Madeira",
      "Atlantic/Reykjavik",
      "Etc/GMT",
      "Etc/UCT",
```

```
      "Etc/UTC",
      "Europe/Lisbon",
      "Europe/London",
        ...

    ]
  }
}
```

5.2 api firmware

The following subsections detail the HTTP functions available for the **api/firmware** service.

5.2.1 api firmware

The **api/firmware** function uploads the firmware file for upgrade/downgrade.

Methods

- PUT

Services and Privileges

- Services: System API
- Privileges: System Control

Request PUT

The request contains a file in **multipart/form-data**.

Table 1. Request Parameters

Parameter	Mandatory	Expected Values	Default Value	Description
blob-fw	Yes	Valid firmware binary file	-	Firmware file

Example of a PUT Request

```
http://192.168.1.1/api/firmware
```

Response to PUT

The response is in the **application/json** format. The response contains the **success** and **result** keys. The **result** value contains various keys described in the table below.

Table 2. Response JSON Keys

Key	Typical Returned Values	Description
fileId	Random identifier (8 HEX characters)	Contains a random identifier of the uploaded firmware file. The identifier must be used to confirm the uploaded firmware using **api/firmware/apply** or to reject the uploaded firmware using **api/firmware/reject**.
version	String with version identification major.minor.patch.build.id	Contains version identification of the uploaded firmware file.
downgrade	`true` or `false`	This flag is `true` if the uploaded firmware has a lower version than the current firmware in the device.
note	String with escaped characters	Contains an upgrade message for the uploaded firmware (e.g. warning about major changes).

Example of a Response to PUT


```
{ "success" : true, "result" : { "fileId" : "7d6adf16", "version" : "2.32.4.41.2",
"downgrade" : false, "note" : "EN:\r\nVER=2.20.0\r\nSome changes associated with the
downgrade to a lower version result in a loss of original settings in a certain part
of configuration.\r\n\r\n* All the cards installed in the **Directory \/ Access
cards** menu are moved to the **Directory \/ Users** menu as new users upon firmware
upgrade. Each user is automatically named as !Visitor #n, where n gives the user
number in the list. This change is irreversible upon downgrade.\r\n* Service cards
are now available in the **Hardware \/ Card reader** menu.\r\n* All the user
access ... ... ... \u043F\u0440\u043E\u0444\u0438\u043B\u0435\u043C
\u043F\u043E\u043B\u044C\u0437\u043E\u0432\u0430\u0442\u0435\u043B\u044F.
\r\n\r\n" } }
```


The following specific error codes may be returned:

- `Error code 12`
  - param = "blob-fw"
  - description = "invalid parameter value"
  - The uploaded firmware file does not match the requirements (invalid file, firmware for a different device…)
- `Error code 19`
  - description = "file version is lower than the required minimum"
  - The uploaded firmware file has a lower version than the minimum version allowed for the device.

> **Note**
>
> The device does not reply to requests to upload another firmware version when the previous firmware file is present. Use **api/firmware/reject** to reject the previous firmware first and then upload another firmware version. The uploaded firmware file is automatically rejected in 5 minutes if not applied.

5.2.2 api firmware apply

The **api/firmware/apply** function confirms the uploaded firmware file and performs device upgrade/downgrade.

Methods

- GET
- POST

Services and Privileges

- Services: System API
- Privileges: System Control

Request GET or POST

The request contains a file in **URL**.

Table 1. Request Parameters

Parameter	Mandatory	Expected Values	Default Value	Description
fileid	Yes	Firmware file identifier	-	This parameter has to correspond to the identifier of the currently uploaded firmware file.

Example of a GET or POST Request

```
http://192.168.1.1/api/firmware/apply?fileid=7d6adf16
```

Response to GET or POST

The response is in the **application/json** format. The response contains **success**. If success is `true`, the firmware is applied and the device is upgraded/downgraded.

Example of a Response to GET or POST

```
{ "success" : true }
```

The following specific error codes may be returned:

- `Error code 12`
  - parameter = "fileid"
  - description = "invalid parameter"

    - The file identifier is invalid (e.g. contains non-HEX characters).
- `Error code 14`
    - description = "new firmware not found"
    - There is no firmware file uploaded with such a fileid.

5.2.3 api firmware reject

The **api/firmware/reject** function rejects the uploaded firmware file.

Methods

- GET
- POST

Services and Privileges

- Services: System API
- Privileges: System Control

Request PUT

The request contains a file in **URL**.

Table 1. Request Parameters

Parameter	Mandatory	Expected Values	Default Value	Description
fileId	Yes	Firmware file identifier	-	This parameter has to correspond to the identifier of the currently uploaded firmware file.

Example of a GET or POST Request

```
http://192.168.1.1/api/firmware/reject?fileId=7d6adf16
```

Response to GET or POST

The response is in the **application/json** format. The response contains **success**. If success is `true`, the firmware is rejected and it is possible to upload a new firmware file using **api/firmware**.

Example of a Response to GET or POST

```
{ "success" : true }
```

The following specific error codes may be returned:

- `Error code 12`
  - parameter = "fileId"
  - description = "invalid parameter"
  - The file identifier is invalid (e.g. contains non-HEX characters).
- `Error code 14`
  - description = "new firmware not found"
  - There is no firmware file uploaded with such fileId.

Note

- The device does not reply to the **api/firmware** requests to upload another firmware version when the previous firmware file is present. Use **api/firmware/reject** to reject the previous firmware first and then upload another firmware version. The uploaded firmware file is automatically rejected in 5 minutes if not applied.

5.3 api config

The following subsections detail the HTTP functions available for the **api/config** service.

5.3.1 api config

The **/api/config** function helps you upload or download device configuration.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required. The function is available with the Enhanced Integration licence key only.

Use the **GET** or **POST** method for configuration download and **PUT** method for configuration upload.

Request parameters for **PUT**:

Parameter	Description
blob-cfg	Mandatory parameter including device configuration (XML)

No parameters are defined for the GET/POST methods.

For configuration download, the reply is in the **application/xml** format and contains a complete device configuration file.

The **/api/config** function using the **PUT** method uploads configuration with a delay of approx. 15 s; do not reset or switch off the intercom during this interval.

Example:

```
GET /api/config
<?xml version="1.0" encoding="UTF-8"?>
<!--
        Product name: 2N IP Vario
       Serial number: 08-1860-0035
    Software version: 2.10.0.19.2
    Hardware version: 535v1
  Bootloader version: 2.10.0.19.1
             Display: No
         Card reader: No
-->
<DeviceDatabase Version="4">
<Network>
    <DhcpEnabled>1</DhcpEnabled>
    ...
    ...
```

For configuration upload, the reply is in the **application/json** format and includes no other parameters.

Example:

```
PUT /api/config
{
  "success" : true
}
```

Caution

- User positions are cancelled in the directory in version 2.24. Thus, download the current configuration, make the required changes and then upload the configuration to update the directory.
- Should you fail to keep the instructions above, data may get lost.

5.3.2 api config factoryreset

The **/api/config/factoryreset** function resets the factory default values for all the intercom parameters. This function is equivalent to the function of the same name in the System / Maintenance / Default setting section of the configuration web interface.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Table 1. Request JSON Keys

Key Name	Mandatory	Expected values	Default value	Description
section	No	`network`	N/A	This parameter resets the default values for all network settings too (including certificates). If the parameter is not specified, the default values for all configuration settings are reset except for network settings.

The reply is in the **application/json** format and includes no parameters.

The **/api/config/factoryreset** function resets the intercom factory values with a delay of approx. 15 s; do not reset or switch off the intercom during this interval.

Example:

```
GET /api/config/factoryreset
{
  "success" : true
}
```

5.3.3 api config holidays

The **/api/config/holidays** function can be used to get/set the bank holidays list.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET** or **PUT** method can be used for this function.

No parameters are defined for the **GET** method.

Request parameters for **PUT** method:

Parameter	Description
blob-json	Mandatory parameter containing definition of bank holidays (JSON)

The reply of the **GET** method is in the **application/json** format and contains an array of bank holidays. The dates are formatted as DD/MM[/YYYY], where the year is specified only if the holiday is valid for the particular year only.

GET /api/config/holidays

```
{ "success" : true, "result" : { "dates": [ "01\/01", "24\/12", "01\/04\/2018" ] } }
```

The **PUT** method JSON format is the same format as a result of the **GET** method.

```
{ "dates": [ "01\/01", "24\/12", "01\/04\/2018" ] }
```

The reply of the **PUT** method is in the **application/json** format and contains no other parameters.

PUT /api/config/holidays

```
{ "success": true
}
```

5.4 api switch

The following subsections detail the HTTP functions available for the **api/switch** service.

5.4.1 api switch caps

The **/api/switch/caps** function returns the current switch settings and control options. Define the switch in the optional **switch** parameter. If the **switch** parameter is not included, settings of all the switches are returned.

The function is part of the **Switch** service and the user must be assigned the **Switch Monitoring** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
switch	Optional switch identifier (typically, 1 to 4)

The reply is in the **application/json** format and includes a switch list (**switches**) including current settings. If the **switch** parameter is used, the **switches** field includes just one item.

Parameter	Description
switch	Switch Id (1 to 4)
enabled	Switch control enabled in the configuration web interface
mode	Selected switch mode (**monostable**, **bistable**)
switchOnDuration	Switch activation time in seconds (for monostable mode only)
type	Switch type (**normal**, **security**)

Example:

```
GET /api/switch/caps
{
  "success" : true,
  "result" : {
    "switches" : [
      {
        "switch" : 1,
        "enabled" : true,
        "mode" : "monostable",
        "switchOnDuration" : 5,
        "type" : "normal"
      },
      {
        "switch" : 2,
        "enabled" : true,
        "mode" : "monostable",
        "switchOnDuration" : 5,
        "type" : "normal"
      },
      {
        "switch" : 3,
        "enabled" : false
      },
      {
        "switch" : 4,
        "enabled" : false
      }
    ]
  }
}
```

5.4.2 api switch status

The **api/switch/status** function returns the current switch statuses.

Service and Privileges Groups

- Service group is Switch.
- Privileges group is Switch Control.

Methods

- GET
- POST

Request

The request contains parameters in the URL (or in the **application/x-www-form-urlencoded** format when POST is used).

Table 1. Request Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
switch	No	Integer defining a switch (typically 1 to 4)	–	Defines which switch status will be returned. **api/switch/caps** can be used for obtaining the number of switches of a particular device. The status of switches is returned if this parameter is omitted.

Example of a Request

```
URL: https://192.168.1.1/api/switch/status?switch=1
```

Response

The success response is in the **application/json** format. It contains two JSON keys `success` and `result`, which contains the key `switches` (status information on individual switches are in an Array of one to four elements).

Table 2. Response switches JSON Keys

Key	Typical Returned Values	Description
switch	Integer (typically 1 to 4)	Defines to which switch the status is related.
active	`true` or `false`	Defines the current state of the switch (`true` – the switch is activated, `false` – the switch is deactivated).

Key	Typical Returned Values	Description
locked	`true` or `false`	Defines whether the switch is locked or not (`true` – the switch is locked in deactivated position and cannot be operated, `false` – the switch is unlocked and can be operated normally). Locking has the priority over holding the switch - i.e. when the switch is simultaneously locked and held, it is deactivated and cannot be operated.
held	`true` or `false`	Defines whether the switch is held or not (`true` – the switch is held in activated position and cannot be operated, `false` – the switch is released and can be operated normally). Locking has the priority over holding the switch – i.e. when the switch is simultaneously locked and held, it is deactivated and cannot be operated.

Example of a Response


```
{ "success": true, "result": { "switches": [ { "switch": 1, "active": true, "locked":
false, "held": true }, { "switch": 2, "active": true, "locked": false, "held": false
}, { "switch": 3, "active": false, "locked": true, "held": true }, { "switch": 4,
"active": false, "locked": true, "held": false } ] } }
```


There may occur various errors (e.g. missing mandatory parameter). Errors are returned in .json with a response code 200.

5.4.3 api switch ctrl

The **/api/switch/ctrl** is used for control of switches.

Service and Privileges Groups

- Service group is Switch.
- Privileges group is Switch Access Control.

Methods

- GET
- POST

Request

The request contains parameters in the URL (or in the **application/x-www-form-urlencoded** format when POST is used).

Table 1. Request Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
switch	Yes	Integer defining a switch (typically 1 to 4)	–	Defines which switch will be controlled. **api/switch/caps** can be used for obtaining the number of switches of a particular device.
action	Yes	String defining the command	–	Defines which command will be applied to the switch. The available commands are: • `on` - activate switch • `off` - deactivate switch • `trigger` - activate monostable switch, toggle the state of bistable switch • `lock` - lock switch (locked switch is deactivated and cannot be operated) • `unlock` - unlock switch (allow normal operation) • `hold` - hold switch activated (held switch is activated and cannot be operated), if the switch is locked and held together it is deactivated • `release` - release the switch from being held (allow normal operation)

Parameter Name	Mandatory	Expected Values	Default Value	Description
response	No	String defining a text that is to be returned instead of standard JSON response	–	The device will return the text specified in this parameter instead of a standard JSON response.
timeout	No (used when `action=hold`)	Range of 1–86 400 seconds	–	Defines the timeout in seconds after which the switch releases again automatically after receiving the `hold` command.
message	No	String (up to 63 characters)		Adds supplementary information to be displayed in the event log.

Example of a Request

```
URL: https://192.168.1.1/api/switch/ctrl?switch=4&action=trigger&response=TEST
```

Response

The success response is in the **application/json** format (unless a custom text response is defined in the `response` parameter).

Table 2. Response JSON Keys

Key	Typical Returned Values	Description
success	`true` or `false`	When a command was performed successfully, the success value is `true`, and it is `false` when the requested switch state could not be reached (e.g. the switch is locked and the requested state is activated switch).

Example of a Response

```
{ "success": true }
```

Additional error information is contained in the response when the success is `false`. Error code 14 "action failed" is returned when the requested result could not be achieved (e.g. when the switch is locked and `action=on` is requested). A command to change the operation type (i.e. held, locked) will always succeed since the operation can be changed all the time except when the switch is disabled (a device will return error 14 to all commands when the switch is disabled).

5.5 api io

The following subsections detail the HTTP functions available for the **api/io** service.

5.5.1 api io caps

The **/api/io/caps** function returns a list of available hardware inputs and outputs (ports) of the device. Define the input/output in the optional **port** parameter. If the **port** parameter is not included, settings of all the inputs and outputs are returned.

The function is part of the **I/O** service and the user must be assigned the **I/O Monitoring** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
Port	Optional input/output identifier

The reply is in the **application/json** format and includes a port list (**ports**) including current settings. If the **port** parameter is used, the **ports** field includes just one item.

Parameter	Description
port	Input/output identifier
type	Type (**input** – for digital inputs, **output** – for digital outputs)

Example:

```
GET /api/io/caps
{
  "success" : true,
  "result" : {
    "ports" : [
      {
        "port" : "relay1",
        "type" : "output"
      },
      {
        "port" : "relay2",
        "type" : "output"
      }
   ]
  }
}
```

5.5.2 api io status

The **/api/io/status** function returns the current statuses of logic inputs and outputs (ports) of the device. Define the input/output in the optional **port** parameter. If the **port** parameter is not included, statuses of all the inputs and outputs are returned.

The function is part of the **I/O** service and the user must be assigned the **I/O Monitoring** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
port	Optional input/output identifier. Use also **/api/io/caps** to get identifiers of the available inputs and outputs.

The reply is in the **application/json** format and includes a port list (**ports**) including current settings (**state**). If the **port** parameter is used, the **ports** field includes just one item.

Example:

```
GET /api/io/status
{
  "success" : true,
  "result" : {
    "ports" : [
      {
        "port" : "relay1",
        "state" : 0
      },
      {
        "port" : "relay2",
        "state" : 0
      }
    ]
  }
}
```

5.5.3 api io ctrl

The **/api/io/ctrl** function controls the statuses of the device logic outputs. The function has two mandatory parameters: **port**, which determines the output to be controlled, and **action**, defining the action to be executed over the output (activation, deactivation).

The function is part of the **I/O** service and the user must be assigned the **I/O Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
port	Mandatory I/O identifier. Use also **/api/io/caps** to get the identifiers of the available inputs and outputs.
action	Mandatory action defining parameter (**on** – activate output, log. 1, **off** – deactivate output, log. 0)
response	Optional parameter modifying the intercom response to include the text defined here instead of the JSON message.

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/io/ctrl?port=relay1&action=on
{
  "success" : true
}
```

If the response parameter is used, the reply does not include the json messages; the server returns a text/plain reply with the specified text (which can be empty).

Example:

```
GET /api/io/ctrl?port=relay1&action=on&response=text
text
```

```
GET /api/io/ctrl?port=relay1&action=on&response=
```

5.5.4 api io doorbell

The **/api/io/doorbell** function activates the logical activation of the doorbell in the answering units.

The function is part of the **I/O** service and, where authentication is used, the user has to be assigned the **Entries and Exits – Control** privilege.

Methods:

- POST

The function has no parameters.

The reply is in the **application/json** format and includes no parameters.

Example:

```
POST /api/io/doorbell
{
  "success" : true
}
```

5.6 api phone

The following subsections detail the HTTP functions available for the **api/phone** service.

5.6.1 api phone status

The **/api/phone/status** functions helps you get the current statuses of the device SIP accounts.

The function is part of the **Phone/Call** service and the user must be assigned the **Phone/Call Monitoring** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
account	Optional SIP account identifier (1 or 2 or 3 or 4). If the parameter is not included, the function returns statuses of all the SIP accounts.

The reply is in the **application/json** format and includes a list of device SIP accounts (**accounts**) including current statuses. If the **account** parameter is used, the **accounts** field includes just one item.

Parameter	Description
account	Unique SIP account identifier (1 or 2 or 3 or 4)
enabled	SIP account enabled
sipNumber	SIP account telephone number
registrationEnabled	SIP account registration enabled
registered	Account registration with SIP Registrar

Example:


```
{
  "success" : true,
  "result" : {
    "accounts" : [
      {
        "account" : 1,
        "accountType" : "general",
        "enabled" : false,
        "sipNumber" : "",
        "registrationEnabled" : false,
        "registered" : false
      },
```

```
      {
        "account" : 2,
        "accountType" : "general",
        "enabled" : true,
        "sipNumber" : "1784973567",
        "registrationEnabled" : true,
        "registered" : true,
        "registerTime" : 1721138562
      },
      {
        "account" : 3,
        "accountType" : "local",
        "enabled" : true,
        "sipNumber" : "2NIPStyle-5034500194"
      },
      {
        "account" : 4,
        "accountType" : "msteams",
        "enabled" : true,
        "sipNumber" : "+1784973567",
        "registrationEnabled" : true,
        "registered" : true,
        "registerTime" : 1721138562
      }
    ]
  }
}
```


5.6.2 api phone calllog

The **/api/phone/calllog** helps you download or delete all or selected call records.

The function is part of the **Phone/Call API** function and the user has to be assigned the **Phone/Call Access Monitoring** privilege for authentication if required.

The call log provides the following information:

- Call type
  - Incoming call (connected or declined)
  - Missed call (unanswered incoming call)
  - Completed elsewhere (incoming call answered via another device)
  - Outgoing call (regardless of the result)
  - Doorbell button
- Contact type (icon contact setting)
- Called / calling user ID
- Call date and time

GET or POST Method

The function has no parameters.

The response is in the **application/json** format and includes the current device states:

Parameter	Description
id	Unique record identification.
callType	Call type specification. • incoming • outgoing • missed • voicemail • completedElsewhere • doorbell button
devType	Internal device identifier.
name	Phone book user name specification.
date	Call record date.
duration	Call duration in seconds.

The records are arranged from the newest to the oldest one according to the absolute call record time.

Caution

- The field is empty if no logs are available.

Example:

```
{
  "success" : true,
  "result" : {
    "callLog" : [
      {
        "id" : ID,
        "callType" : "incoming",
        "devType" : "2-14-0-0",
        "name" : "Franta Vomáčka",
        "date" : "2027-11-06T12:23:52Z",
        "duration": 1514
      },
      {
        "id" : ID,
        "callType" : "incoming",
        "devType" : "4-13-1-2",
        "name" : "Pepa Vonášek",
        "date" : "2027-12-06T12:23:52Z",
        "duration": 15
      },
      ...
    ]
  }
}
```

Door bell

```
{
  "success" : true,
  "result" : {
    "callLog" : [
      {
        "id" : ID,
        "callType" : "doorbell",
        "date" : "2027-11-06T12:23:52Z"
      },
      ...
    ]
  }
}
```

DELETE Method

The function is part of the **Phone/Call API** function and the user has to be assigned the **Phone/Call Access Control** privilege for authentication if required.

Request parameters:

Parameter	Description
id	Unique identifier of the record to be deleted.

Example:

```
{
  "success" : false,
  "error" : {
    "code" : 12,
    "param" : "id",
    "description" : "record not found"
  }
}
```

5.6.3 api phone config

The **/api/phone/config** function is used for monitoring and checking the SIP account settings.

The **GET** method can be used for downloading and the **PUT** method for uploading the configuration in this function.

The function is part of the **Phone/Call** service and, if authentication is required, the user has to be assigned the **Phone/Calls – Monitoring** privilege for the **GET** method and **Phone/Calls – Management** for the **PUT** method.

GET Method

Request parameters:

Parameter	Description
account	Optional parameter defining the SIP account identifier (1 or 2). If the parameter is not included, the function returns the states of all the SIP accounts.

The response is in the **application/json** format for the **GET** method and provides a list of the device SIP accounts (**accounts**) including their current states. In case the account is specified using the **account** parameter, the response only provides information on the given account.

Caution

- For security reasons, the device does not return the password if the **GET** method is used.

Example:

```
GET /api/phone/config
{
    "success": true,
    "result": {
        "accounts": [
            {
                "account": 1,
                "enabled": false,
                "displayName": "",
                "sipNumber": "",
                "domain": "",
                "domainPort": "",
                "authId": "",
                "proxyAddress": "",
                "proxyPort": "",
                "registrationEnabled": false,
                "registrarAddress": "",
                "registrarPort": "",
                "answerMode": "1"
            },
            {
                "account": 2,
                "enabled": false,
                "displayName": "",
                "sipNumber": "",
                "domain": "",
                "domainPort": "",
                "authId": "",
                "proxyAddress": "",
                "proxyPort": "",
                "registrationEnabled": false,
                "registrarAddress": "",
                "registrarPort": "",
                "answerMode": "1"
            }
        ]
    }
}
```

PUT Method

Request parameters:

Parameter	Description
blob-json	Mandatory parameter containing the SIP account configurations (in the JSON format).

The **blob-json** parameter is mandatory for the **PUT** method and can include all the **accounts** parameters from the file obtained using the **GET** method. In addition to the mandatory **account** parameter, one more parameter must be included at least. The other parameters are optional. It is possible to specify the **password** parameter and enter the password in the open form for each account in the JSON file uploaded. This parameter is not part of the response to the **GET** method for security reasons. The response is in the **application/json** format. Should an error occur during verification, the whole process fails and none of the parameters will be used.

Example:

```
PUT /api/phone/config
{
    "success": true,
}
```

The database parameters correspond to the JSON file parameters as follows:

Database parameter	JSON parameter	Additional info
Phone.Sip	**account**	Numbering starts from 1, not from 0.
Phone.Sip.Enabled	**enabled**	
Phone.Sip.User.DisplayName	**displayName**	
Phone.Sip.User.Id	**sipNumber**	
Phone.Sip.User.AuthId	**authId**	If the parameter is empty, the Phone.Sip.User.Id parameter is used instead.
Phone.Sip.User.PasswordString	**password**	In open form – can be uploaded into the device only using the PUT method, cannot be obtained using the GET method.

Database parameter	JSON parameter	Additional info
Phone.Sip.Client.Domain	**domain**	
Phone.Sip.Client.Port	**domainPort**	
Phone.Sip.Proxy.Address	**proxyAddress**	
Phone.Sip.Proxy.Port	**proxyPort**	
Phone.Sip.Registrar.Enabled	**registrationEnabled**	
Phone.Sip.Registrar.Address	**registrarAddress**	
Phone.Sip.Registrar.Port	**registrarPort**	
Phone.Sip.Misc.AnswerMode	**answerMode**	

5.7 api call

The following subsections detail the HTTP functions available for the **api/call** service.

5.7.1 api call status

The **/api/call/status** function helps you get the current states of active telephone calls. The function returns a list of active calls including parameters.

The function is part of the **Phone/Call** service and the user must be assigned the **Phone/Call Monitoring** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
session	Optional call identifier. If the parameter is not included, the function returns statuses of all the active calls.

The reply is in the **application/json** format and includes a list of active calls (**sessions**) including their current states. If the **session** parameter is used, the **sessions** field includes just one item. If there is no active call, the **sessions** field is empty.

Parameter	Description
session	Call identifier
direction	Call direction (**incoming**, **outgoing**)
state	Call state (**connecting**, **ringing**, **connected**)
calls	Individual Call Routing of Ongoing Call. For example, calling a phone number in a group with a contact representative creates two simultaneous calls to two different destinations (**peer**).

Example:

```
GET /api/call/status
[
  {
    "calls": [
      {
        "id": 6,
        "peer": "sip:10.0.29.27",
        "state": "ringing"
      },
      {
        "id": 7,
        "peer": "sip:10.0.29.31",
        "state": "ringing"
      }
    ],
    "direction": "outgoing",
    "session": 4,
    "state": "ringing"
  }
]
```

5.7.2 api call dial

The **/api/call/dial** function helps you initiate a new outgoing call to a selected phone number or sip uri using the *number* parameter or one or more users using the *users* parameter. The command may include just one of the mentioned parameters, otherwise it will be returned with an error reponse.

The function is part of the **Phone/Call** service and the user must be assigned the **Phone/Call Control** privilege for authentication if required.

The **/api/call/dial** function allows you to initiate a new outgoing call to a selected phone number or sip uri using the *number* parameter, or to one or more users using the *users* parameter. The command may contain just one of the listed parameters, otherwise an error message is returned.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
number	Mandatory parameter specifying the destination phone number or sip uri
users	List of comma-separated user uuids (unique IDs).

The reply is in the **application/json** format and includes information on the outgoing call created.

Parameter	Description
session	Call identifier, used, for example, for call monitoring with **/api/call/status** or call termination with **/api/call/hangup**

Example:

```
GET /api/call/dial?number=sip:1234@10.0.23.194
{
  "success" : true,
  "result" : {
    "session" : 2
  }
}
```

5.7.3 api call answer

The **/api/call/answer** function helps you answer an active incoming call (in the **ringing** state).

The function is part of the **Phone/Call** service and the user must be assigned the **Phone/Call Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
session	Active incoming call identifier

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/call/answer?session=3
{
  "success" : true
}
```

5.7.4 api call hangup

The **/api/call/hangup** helps you hang up an active incoming or outgoing call.

The function is part of the **Phone/Call** service and the user must be assigned the **Phone/Call Control** privilege for authentication if required. The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
session	Active incoming/outgoing call identifier
reason	End call reason: **normal** – normal call end (default value) **rejected** – call rejection signalling **busy** – station busy signalling

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/call/hangup?session=4
{
  "success" : true
}
```

5.8 api camera

The following subsections detail the HTTP functions available for the **api/camera** service.

5.8.1 api camera caps

The **/api/camera/caps** function returns a list of available video sources and resolution options for JPEG snapshots to be downloaded via the **/api/camera/snapshot** function.

The function is part of the **Camera** service and the user must be assigned the **Camera Monitoring** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes a list of supported resolutions of JPEG snapshots (**jpegResolution**) and a list of available video sources (**sources**), which can be used in the **/api/camera/snapshot** parameters.

Parameter	Description
width, height	Snapshot resolution in pixels
source	Video source identifier

Example:

```
GET /api/camera/caps
{
  "success" : true,
  "result" : {
    "jpegResolution" : [
      {
        "width" : 160,
        "height" : 120
      },
      {
        "width" : 176,
        "height" : 144
      },
      {
        "width" : 320,
        "height" : 240
      },
      {
        "width" : 352,
        "height" : 272
      },
      {
        "width" : 352,
        "height" : 288
      },
      {
        "width" : 640,
        "height" : 480
      }
    ],
    "sources" : [
      {
        "source" : "internal"
      },
      {
        "source" : "external"
      }
    ]
  }
}
```

5.8.2 api camera snapshot

The **/api/camera/snapshot** function helps you download images from an internal or external IP camera connected to the intercom. Specify the video source, resolution and other parameters.

The function is part of the **Camera** service and the user must be assigned the **Camera Monitoring** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
width	Mandatory parameter specifying the horizontal resolution of the JPEG image in pixels. The snapshot resolution must comply with one of the supported options (see **api/camera/caps**). If an unsupported value is entered, the request will not be executed.
height	Mandatory parameter specifying the vertical resolution of the JPEG image in pixels. The snapshot height and width must comply with one of the supported options (see **api/camera/caps**). If an unsupported value is entered, the request will not be executed.
source	Optional parameter defining the video source (**internal** – internal camera, **external** – external IP camera). If the parameter is not included, the default video source included in the Hardware > Camera > Common settings section of the configuration web interface is selected.
fps	Optional parameter defining the frame rate. If the parameter is set to **≥** 1, the intercom sends images at the set frame rate using the **http server push** method.
time	Optional parameter defining the snapshot time in the intercom memory. The time values must be within the intercom memory range: <-30, 0> seconds. When this parameter is used together with the **fps** parameter, the **fps** parameter is ignored and function returns only a single frame of the maximum resolution of 1280×960 px (width×height). When this parameter is used, the function returns snapshots of the maximum resolution of 1280×960 px (width×height). Higher **width** and **height** requests will be ignored.

The reply is in the **image/jpeg** or **multipart/x-mixed-replace** (pro fps **≥** 1) format. If the request parameters are wrong, the function returns information in the **application/json** format.

Example:

```
 GET /api/camera/snapshot?width=640&height=480&source=internal

 # following command returns a frame which was captured 5 seconds before the command
was executed
 GET /api/camera/snapshot?width=1280&height=960&source=internal&time=-5
```

5.9 api display

The following subsections detail the HTTP functions available for the **api/display** service.

5.9.1 api display caps

The **/api/display/caps** function returns a list of device displays including their properties. Use the function for display detection and resolution.

The function is part of the **Display** service and the user must be assigned the **Display Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes a list of available displays (**displays**).

Parameter	Description
display	Display identifier
resolution	Display resolution in pixels

Example:

```
GET /api/display/caps
{
  "success" : true,
  "result" : {
    "displays" : [
      {
        "display" : "internal",
        "resolution" : {
          "width" : 320,
          "height" : 240
        }
      }
    ]
  }
}
```

5.9.2 api display image

1) 2N IP Style

The **/api/display/image** function helps you modify the content to be displayed: upload a GIF / JPEG image to or delete an earlier uploaded image from the display. Progressive JPEG images are not supported.

The function is part of the **Display** service and the user must be assigned the **Display Control** privilege for authentication if required.

The **PUT** or **DELETE** method can be used for this function: **PUT** helps upload an image to the display, **DELETE** helps delete an uploaded image from the display.

PUT method

Request parameters:

Parameter	Description
blob-image	Mandatory parameter containing a JPEG / BMP / PNG image with 1280 x 800 display resolution (refer to **/api/display/caps**). The parameter is applied only if the **PUT** method is used. Progressive JPEG images are not supported.
duration	Optional parameter. Image display time. The parameter is set in milliseconds.

Parameter	Description
displayLayer	Optional parameter defining which FlexiLayout layer will be replaced by the image. Valid values: • top (default value) – Showcase mode (former behaviour) • popup – Information messages / pop-up messages in Custom GUI • main – content of the operational layer for standard pages created in Custom GUI • default – Custom GUI home page displayed after waking up from Sleep Mode/ Preview Mode

There are two ways how to display an image: as a notification or as an overlay. Notifications are displayed for a predefined period of time and automatically disappear after the timeout. Overlays keep displayed until replaced with another image or removed by the user. If the HTTP request does not include an optional parameter **duration**, the image is displayed in the overlay mode, i.e. uploaded for an indefinite period of time. If an optional parameter **duration** is included, the image is displayed in the notification mode, which ends when a preset timeout expires. Touch the display to end the notification earlier.

When uploaded for the first time, the image is transferred from the main unit to the display via an internal bus (which may take some time). Several images may be stored in the display memory and if the same images are sent to the device in the future, they are no longer transferred via the internal bus. They are immediately displayed from the memory instead.

The reply is in the **application/json** format and includes no parameters.

Image parameters:

Model	Image size	Supported formats
2N IP Style	1280 x 800 pixels	Normal JPEG (recommended), PNG

Note

- The supported JPEG format is JPEG Baseline (non-progressive encoding).

Example:

```
PUT api/display/image&duration=30000&displayLayer=popup  {
  "success" : true
}
```

DELETE method

Parameter	Description
display	Mandatory display identifier. Find the value in Hardware/Extending modules/ Module name or using **/api/display/caps**.
displayLayer	Optional parameter defining on which display the image should be deleted. Valid values: • top (default value) – Showcase mode (former behaviour) • popup – Information messages / pop-up messages in Custom GUI • main – content of the operational layer for standard pages created in Custom GUI • default – Custom GUI home page displayed after waking up from Sleep Mode/ Preview Mode • all – all of the abovementioned values

Example:

```
DELETE api/display/image
{
  "success" : true
}
```

2) 2N IP Verso

The **/api/display/image** function helps you modify the content to be displayed: upload a GIF / JPEG / BMP image to or delete an earlier uploaded image from the display. Progressive JPEG images are not supported.

The function is part of the **Display** service and the user must be assigned the **Display Control** privilege for authentication if required.

The **PUT** or **DELETE** method can be used for this function: **PUT** helps upload an image to the display, **DELETE** helps delete an uploaded image from the display.

PUT method

Request parameters:

Parameter	Description
display	Mandatory display identifier. Find the value in Hardware/Extending modules/Module name or using **/api/display/caps**.
blob-image	Mandatory parameter containing a JPEG / BMP / PNG image with 320 x 214 display resolution (refer to **/api/display/caps**). The parameter is applied only if the **PUT** method is used. The request may contain just one parameter: blob-image or blob-video. Progressive JPEG images are not supported.
blob-video	Mandatory parameter containing an MPEG4 / H264 video of the maximum duration of 60 s, maximum of 15 fps and resolution of 320 x 214 pixels. The request may contain just one parameter: blob-image or blob-video.
duration	Optional parameter. Image display / video playing time. The parameter is set in milliseconds.
repeat	Optional parameter. Video playing repetition count. The parameter applies to video only.

There are two ways how to display an image: as a notification or overlay. Notifications are displayed for a predefined period of time and automatically disappear after the timeout. Overlays keep displayed until replaced with another image or removed by the user.

If the HTTP request does not include any of the above mentioned optional parameters, the overlay mode is used, i.e. the image is displayed for an indefinite period of time. If both the optional parameters are included, the notification is terminated by the event that is generated earlier. Touch the display to end the notification earlier.

When uploaded for the first time, the image is transferred from the main unit to the display via an internal bus (which may take some time). Several images may be stored in the display memory and if the same images are sent to the device in the future, they are no longer transferred via the internal bus. They are immediately displayed from the memory instead.

The reply is in the **application/json** format and includes no parameters.

Image parameters:

Model	Image size	Supported formats
2N IP Verso	320 x 214 pixels	Normal JPEG (recommended), BMP, PNG

Note

- The supported JPEG format is JPEG Baseline (non-progressive encoding).

Example:

```
  api/display/image?display=ext1&duration=30000
{
  "success" : true
}
```

Video parameters:

Model	Video size	Supported formats
2N IP Verso	214 x 240 pixels	MPEG4 / H264: Baseline profile, up to 5.2 level

Example:

```
  api/display/image?display=ext1&repeat=5
 {
  "success" : true
}
```

DELETE method

Parameter	Description
display	Mandatory display identifier. Find the value in Hardware/Extending modules/ Module name or using **/api/display/caps**.

Example:

```
DELETE /api/display/image?display=ext1
{
  "success" : true
}
```

3) 2N IP Vario

The **/api/display/image** function helps you modify the content to be displayed: upload a GIF / JPEG / BMP image to or delete an earlier uploaded image from the display.

The function is part of the **Display** service and the user must be assigned the **Display Control** privilege for authentication if required.

The **PUT** or **DELETE** method can be used for this function: **PUT** helps upload an image to the display, **DELETE** helps delete an uploaded image from the display.

Request parameters:

Parameter	Description
display	Mandatory display identifier (**internal**).
blob-image	Mandatory parameter including an image in the supported format with display resolution (see **/api/display/caps**). The parameter is applied only if the **PUT** method is used.

The reply is in the **application/json** format and includes no parameters.

Image parameters:

Model	Image size	Supported formats
2N IP Vario	320 x 240 pixels	JPEG (recommended), GIF, BMP

Caution

The supported JPEG format is JPEG Baseline (non-progressive encoding).

Example:

```
DELETE /api/display/image?display=internal
{
  "success" : true
}
```

- 5.9.2.1 api display image examples

5.9.2.1 api display image examples

The below-mentioned examples help sending data from the control application to the **2N® IP Verso** and **2N® IP Vario** displays.

An image can be displayed either as a notification or overlay. **2N® IP Verso** can display images in either way, **2N® IP Vario** can only display notifications. Notifications are displayed for a pre-defined time and disappear automatically after this timeout. Overlays keep displayed until replaced with another image or removed by the user.

The *__duration__* parameter gives the image/video display time in ms.
The *__repeat__* parameter specifies the count of video repetitions and is ignored for images.

If the HTTP request does not include any of the above-mentioned parameters, the overlay mode is used, i.e. the image is displayed for an indefinite period of time. If both the parameters are included, the display is terminated by the event that happens first.

Image Loading to 2N® IP Verso/2N® IP Vario Display

Note

Each model supports a different image resolution.

Model	Image size	Supported formats
2N® IP Verso	214 x 240 pixels	JPEG (recommended), BMP, PNG
2N® IP Vario	320 x 240 pixels	JPEG (recommended), GIF, BMP

Request URL: https://10.27.24.15/api/display/image?display=ext1

- Request method: PUT
- Remote address: 10.27.24.15:443
- Status code: 200 OK
- Version: HTTP/1.1

Response headers (95 B)

- Server: HIP2.22.0.31.1
- Content-Type: application/json
- Content-Length: 24

Request headers (494 B)

- Host: 10.27.24.15
- User-Agent: Mozilla/5.0 (Windows NT 6.1; W…) Gecko/20100101 Firefox/56.0
- Accept: */*
- Accept-Language: cs,en-US;q=0.7,en;q=0.3
- Accept-Encoding: gzip, deflate, br
- Referer: https://10.27.24.15/apitest.html
- Content-Length: 1325
- Content-Type: multipart/form-data; boundary=…----------258852674219952
- Cookie: _ga=GA1.1.375392382.1496656977…id=GA1.1.638680516.1507547865
- Connection: keep-alive

Query string

- display: ext1

Request payload

----------------------------258852674219952

Content-Disposition: form-data; name="blob-image"; filename="picture.png"

Content-Type: image/png


```
‰PNG
IHDR   Ö   đ   ót
R   sRGB ®Îé   gAMA  ±Źüa       pHYs  Ă ĂÇo¨d  üIDATx^íŘŃqŰ8@ŃÔ•,\OŞq3)Ć»Ž4Y,$Ť'Ô
Í¬ÎůÔČ\ƒ˘ž}
@J,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$
HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$Hë:    ľž}űííýţáIžy/ţ@,ŚIP,±×L�‘ ±Ó\–őŰ^b;    Žkż˙řůëÓ©í–
f)ËýBÎLđçŹđ÷mŢł.jËb¶v?˜m|;éJđBÎKđ0‹›a÷ŕţ/›dY¸Z$Á9+Áá[śCC/Ău
´)éż6ĆŃŘĚ8[\quŽNđ%ÁŘ©żoŚÂ˘ŚÍöu6–×mcšŤ%x!§żŽlĚ¶˙°¦I¸Ë5céw¬“`ě©    •}
š%¸Íı7še`»Îľ"Á9;ÁáÚ˜%¸ÍbwúHI_^Č“ś–ŕq|7Ëí–ŕ‹:+Áť ďĎÁŮög±;ő ţ?8)ÁÍŻâř‹    ÝćfřKŘ_'Á
Ř÷x9FÇYL¦Ó«ÝĚĆÇ÷â©ž�ŕâ|Z?ž–ŰśĹlşşââ(\M†KJđBÎú–848µ|x~–Á=r«ƒ%Śť•ŕĽŚ·÷Ĺd±˙ÇY<>ÝŘů‘x|
5žęĽ?Ń¸ďöWŢR‰fâ#ß”`ĚÜŻJ,ń’    îĂ4^1Áá]Y,µ–Jpőš0
Ě˝R,;ú!
Ř
{
Ą
Wo
ĚŔ
kxÉ×®D,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$H
L,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$H
L,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$H
L,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$H
L,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,Ä$HL,¤>>
ţ+uKéż<:–    IEND®B`,
```


----------------------------258852674219952--

Video Loading to 2N® IP Verso Display

Info

Model	Video size	Supported formats
2N® IP Verso	214 x 240 pixels	MPEG4 / H264: Baseline profile, level up to 5.2

Request URL: https://10.27.24.15/api/display/image?display=ext1&duration=20&repeat=3

- Request method: PUT
- Remote address: 10.27.24.15:443
- Status code: 200 OK
- Version: HTTP/1.1

Response headers (95 B)

- Server: HIP2.22.0.31.1
- Content-Type: application/json
- Content-Length: 24

Request headers (516 B)

- Host: 10.27.24.15
- User-Agent: Mozilla/5.0 (Windows NT 6.1; W…) Gecko/20100101 Firefox/56.0
- Accept: */*
- Accept-Language: cs,en-US;q=0.7,en;q=0.3
- Accept-Encoding: gzip, deflate, br
- Referer: https://10.27.24.15/apitest.html
- Content-Length: 943815
- Content-Type: multipart/form-data; boundary=----------------------------14948718218673
- Cookie: _ga=GA1.1.375392382.1496656977…id=GA1.1.638680516.1507547865
- Connection: keep-alive

Query string

- display – ext1
- duration – 20
- repeat – 3

Request payload

----------------------------14948718218673

Content-Disposition: form-data; name="blob-video"; filename="2N_intro.mp4"

Content-Type: video/mp4

```
ftypmp42  isomiso2avc1mp41   free O!mdat  ·¨łÜEé˝ćŮH·–,Ř Ů#îďx264 - core 148 r2708
86b7198 - H.264/MPEG-4 AVC codec - Copyleft 2003-2016 - http://www.videolan.org/
x264.html - options: cabac=0 ref=2 deblock=0:0:0 analyse=0x1:0x111 me=hex subme=6
psy=1 psy_rd=1.00:0.00 mixed_ref=1 me_range=16 chroma_me=1 trellis=1 8x8dct=0 cqm=0
deadzone=21,11 fast_pskip=1 chroma_qp_offset=-2 threads=6 lookahead_threads=1
sliced_threads=0 nr=0 decimate=1 interlaced=0 bluray_compat=0 constrained_intra=0
bframes=0 weightp=0 keyint=150 keyint_min=15 scenecut=40 intra_refresh=0
rc_lookahead=30 rc=crf mbtree=1 crf=22.0 qcomp=0.60 qpmin=0 qpmax=69 qpstep=4
vbv_maxrate=20000 vbv_bufsize=25000 crf_max=0.0 nal_hrd=none filler=0 ip_ratio=1.40
aq=1:1.00 €  őeˆ„    ®C‡Ü!q@ CzˇNbyRćŞŇÔ~ˆ$]´í·ŢFb0~ůh˙M=>?
„´mÍßŹ˙âµWjŻ«¸ĄzŹ”Ä˙OŹ”#ŚĎŢŢÜ~éÂ6ŰËÓăďŞ üP•?´n?é¦žš{–ü7ŢĘ«“b»ž¶Ť˜G
LZ¨˙.˜üß˙ÓřŹđý×\Ů’žjo¸…z˝x˙Ők&+ý˙ťřG˙kü¸3 ˆŔ|p«^ů˙¸˝UzÔż¨˙XąłÉž¤ŔŁŞ˙€pŔ!>lÍ�ŹůMfÓoďľ_„0„)
ćÎlŕő,ňË˙ţź?_?Ăţ|Ź˙ř{>˙řÎl&/Íźţ÷ďť~»ŔżT<vW
Íź/}ţ Ď    e‡ŕ•ť¶ß¨Őy9čšziý–$
‰˙ů
_Á
ż
+
˙ř
{]
Ď
]u×]wÜ
Ŕ
"ý
ż9˙ĎČ§ű˙ü$lŮ7ęzë®şë®şë®úë®şë®şë®şë®şë®şë®ż˙ŐxxCîş‰®şë®şë®:O˙äőy˙ŻŽŠů{�Osóţ«ă‘u]u×S·,
\7ťĽ·p°Ó–X    ]`ű§ÄńęĽƒđÜřţš§/Źó˙ Gíż...
```

----------14948718218673--

5.9.3 api display language

The `GET /api/display/language` returns language of the current end-user session, default end-user language, supported languages by the device, and languages configured for selection on display.

The function is part of the **Display** service and the user must be assigned the **Display Monitoring** privilege for authentication if required.

The **GET** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes:

Parameter	Description
sessionCurrently	Currently selected language for the session (Sentrio Cabin only)
default	Language selected in the configuration of the device as default
supported	All languages supported by the device display, contains system languages (fixed) and custom (configurable texts by user)
enabled[]	languages configured for the menu on the display (can be selected by the the end-user when interacting with the device), the list is ordered in the order the device presents these options to the end user (Sentrio Cabin only)

Example:

```
GET /api/display/language
{
    "session": "en",
    "default": "en",
    "supported": {
        "system": [
            "en",
            "cs",
            "nl"
        ],
        "custom": "en"
    },
    "enabled": [
        "en",
        "cx-en",
        "nl"
    ]
}
```

5.9.4 api display text

The `PUT /api/display/text` function helps you show a message on the device display.

The function is part of the **Display API** service and the user has to be assigned the **Display (Control)** privilege for authentication if required.

Methods:
GET – sets the message on the display.
DELETE – removes the message from the display.

GET method

Two input formats are available in JSON:

1. Message with translations (`message[]`)
2. Freetext (`text`)

A combination of the two formats is not supported.

Parameters:

Parameter	Type	Mandatory	Description
`uid`	string	No	Message identifier for a third party system. Max. length: 40 characters.
`response`	bootlean	No	Defines whether or not the messages requires a response. Derfault: `false`.
`timeout`	number	No	Display timeout (in seconds). Default: `3600`. Max. values: • `response=true`: `3600` • `response=false`: `1209600`
`icon`	string	No	Message icon. Valid values: `"none"`, `"operator"`, `"technician"`.

Format of the message with translations, `message[]`key parameters:

Parameter	Type	Mandatory	Description
`language`	string	Yes	Language code (ISO 639).
`text`	string	Yes	Message text in the selected language.

Freetext format:

Parameter	Type	Mandatory	Description
`text`	string	Yes	Message text. Max. length: 1024 characters.

Example of request

```
{
    "uid": "user_defined_string",
    "message": [
        {
            "language": "en",
            "text": "Hello, how can I help you?"
        },
        {
            "language": "cs",
            "text": "Dobrý den, jak Vám mohu pomoci?"
        }
    ],
    "response": true,
    "timeout": 3600,
    "icon": "operator"
}
```

Response

```
{
    "success": true,
    "result": {
        "response": "",
        "uid": "user_defined_string"
    }
}
```

DELETE method

The request does not contain any parameters.

```
DELETE /api/display/text
{
    "success": true,
    "result": {
        "uid": "user_defined_string"
    }
}
```

5.10 api log

The following subsections detail the HTTP functions available for the **api/log** service.

- 5.10.1 api log caps

5.10.1 api log caps

The **/api/log/caps** function returns a list of supported event types that are recorded in the device. This list is a subset of the full event type list below:

Event type	Description	Parameters	
		Permanent	Conditioned
AccessBlocked	Signals blocking of user authentication, zone code, REX exit button and license plate based access on an access point.	"ap, state"	
AccessLimited	An event occuring whenever 5 unsuccessful user authentication attempts are made (card, code, fingerprint). The access module is blocked for 30 seconds even in case the subsequent authentication is correct. Signals user rejection.	"ap, type, state"	
AccessTaken	When applying the card in the Antipassback area.	"ap, session"	
ApiAccessRequested	An event whenever a request was sent to /api/accesspoint/grantaccess with the result "success" : true.	"ap, valid"	"session, uuid"
AudioLoopTest	Signals performance and result of an automatic audio loop test.	"result"	
CallSessionStateChanged	An event describing the direction, status of the call, address, created session number and how many calls were generated.	"session, state"	"originator, info"
CallStateChanged	Indicates call direction (incoming, outgoing) and SIP/opponent identification at a call state change (ringing, connected, terminated).	"direction, state, peer, session, call"	"reason, device, sipAccount, sipCallId "

Event type	Description	Parameters	
		Permanent	Conditioned
CapabilitiesChanged	Signals a change in available functions.		
CardHeld	Signals RFID card tapping and holding for more than 4 s.	"reader, uid, valid"	"ap, session, direction, uuid"
CardEntered	Signals tapping of an RFID card on the card reader.	"reader, uid, valid"	"ap, session, direction, uuid"
CodeEntered	Signals entering of a user code via the numeric keypad.	"code, valid "	"ap, session, direction, input, type, uuid, reason"
ConfigurationChanged	Signals a device configuration change.		
DeviceState	Signals a system event generated at device state changes.	"state"	
DisplayTouched	Signals display touch.	"x, y, dx, dy"	
DirectoryChanged	Change in the directory.	"series"	"timestamp"
DirectorySaved	Saved change in the directory.	"series"	"timestamp"
DoorOpenTooLong	Signals excessively long door opening or door closing failure within the timeout.	"state"	
DoorStateChanged	Signals a door state change.	"state"	

Event type	Description	Parameters	
		Permanent	Conditioned
DtmfEntered	DTMF code received in call or off call locally.	"code, call, valid"	"type, uuid"
DtmfPressed	DTMF code pressed in call or off call locally.	"code, call valid"	
DtmfSent	DTMF code sent in call or off call locally.	"code"	"call"
ExternalCameraStateChanged	Signals an external camera state change.	"state"	"id, reason"
ErrorStateChanged	Signals a LiftIP 2.0 error state change.		"in, state, reason"
FingerEntered	Signals that a finger has been swiped across the biometric reader.	"valid"	"ap, session, direction, uuid"
FingerEnrollState	Placing a finger on the reader to record the user's fingerprint.	"session, state"	
HardwareChanged	Signals a connection change of the extending modules.	"reason, class, id"	"info, config, state, categories"
CheckingCall	Displays details of an accomplished checking call.		"action"
InputChanged	Signals a logic input state change.	"port, state"	
KeyPressed	Signals a quick dial/numerical keypad button press, display touch or Bluetooth autentication key press.	"key"	

Event type	Description	Parameters	
		Permanent	Conditioned
KeyReleased	Signals a quick dial/numerical keypad button release.	"key"	
LicensePlateRecognized	Signals car license plate recognition for valid access.	"ap, licensePlate, valid"	"session, uuid"
LiftConfigChanged	Signals an elevator control setting change.	"hash"	
LiftErrorStateChanged	Signals a LiftIP 2.0 error state change.		"in, state, reason"
LiftFloorsEnabled	Floor access by an elevator.	"floors"	"uuid, session"
LiftStatusChanged	Lift Control module connection/ disconnection detection.	"module, ready"	
LoginBlocked	Signals temporary blocking of login to the web interface.	"address"	
MobKeyEntered	Signals Bluetooth reader authentication.	"action, authid, valid"	"ap, session, direction, uuid"
MotionDetected	Signals motion detection via a camera.	ID = corresponds to the motion detection profile number in the web interface "state"	

Event type	Description	Parameters	
		Permanent	Conditioned
NoiseDetected	Signals increased noise level detection.	only for models equipped with a microphone or microphone input "state"	
OutputChanged	Signals a logic output state change.	"port, state"	
PairingStateChanged	Signals pairing with a Bluetooth interface.	"state, authId, pending_blocked"	
RescueStateChanged	Signals a rescue state change.		"state, reason"
RegistrationStateChanged	Signals a SIP server registration state change.	"sipAccount, state"	"reason"
RexActivated	Signals REX departure button activation.	"ap, session, valid"	"reason"
SilentAlarm	Signals silent alarm activation.	"ap, session, name"	"uuid"
SwitchesBlocked	Signals lock blocking by tamper switch activation.	"state"	

Event type	Description	Parameters	
		Permanent	Conditioned
SwitchOperationChanged	Change in the operation of the switch (signals the state of locking or holding the switch, starting and restarting the timer or ending it - transition to permanent holding).	"switch"	"enabled, locked, held, hold_timeout, originator"
SwitchStateChanged	Signals a switch 1–4 state change.	"switch, state"	"ap, session, originator, call, peer, device"
TamperSwitchActivated	Signals tamper switch activation.	"state"	
UnauthorizedDoorOpen	Signals unauthorized door opening.	only for models equipped with digital inputs "state"	
UserActionActivated	Signals a change of the input configured as User Action Trigger.	"id, state"	
UserAuthenticated	Signals user authentication and subsequent door opening.	"ap, session, name"	"uuid, apbBroken"
UserRejected	Signals user authentication rejection.	"ap, session, name"	"uuid, reason"
VirtualInput	Changing the virtual input.	"port, state"	

Event type	Description	Parameters	
		Permanent	Conditioned
VirtualOutput	Changing the virtual output.	"port, state"	
WaveKeyActivated	Bluetooth authentication activated.	"type"	

The function is part of the **Logging** service and requires no special user privileges.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format:

Parameter	Type	Description
events	array	Array of strings including a list of supported event types

Example:

```
GET /api/log/caps
{
  "success" : true,
  "result" : {
    "events" : [
      "KeyPressed",
      "KeyReleased",
      "InputChanged",
      "OutputChanged",
      "CardEntered",
      "CallStateChanged",
      "AudioLoopTest",
      "CodeEntered",
      "DeviceState",
      "RegistrationStateChanged"
    ]
  }
}
```

5.10.2 api log subscribe

The **/api/log/subscribe** function helps you create a subscription channel and returns a unique identifier to be used for subsequent dialling of the **/api/log/pull** or **/api/log/unsubscribe** function.

Each subscription channel contains an event queue of its own. All the new events that match the channel filter (**filter** parameter) are added to the channel queue and read using the **/api/log/pull** function.

At the same time, the device keeps the event history queue (last 10000 events) in its internal memory. The event history queue is empty by default.

Use the **include** parameter to specify whether the channel queue shall be empty after restart (storing of events occurring after the channel is opened), or be filled with all or some events from the event history records.

Use the **duration** parameter to define the channel duration if it is not accessed via **/api/log/pull**. The channel will be closed automatically when the defined timeout passes as if the **/api/log/unsubscribe** function were used.

The function is part of the **Logging** service and requires some user privileges for authentication. Unprivileged user events shall not be included in the channel queue.

Table of events:

Event type	Required user privileges
TamperSwitchActivated	None
UnauthorizedDoorOpen	None
DoorOpenTooLong	None
LoginBlocked	None
SilentAlarm	None
DoorStateChanged	None
DeviceState	None
AudioLoopTest	None
MotionDetected	None
NoiseDetected	None
HardwareChanged	None

Event type	Required user privileges
FingerEnrollState	None
LiftStatusChanged	None
LiftFloorsEnabled	None
LiftConfigChanged	None
CapabilitiesChanged	None
ConfigurationChanged	None
ExtCameraStateChanged	None
RescueStateChanged	None
ErrorStateChanged	None
LiftCheckingCall	None
DtmfSent	None
RexActivated	None
AccessBlocked	None
AccessTaken	None
AccessLimited	None
DisplayTouched	None
DtmfPressed	None
SwitchesBlocked	None
InputChanged	I/O monitoring
OutputChanged	I/O monitoring
VirtualInputChanged	I/O monitoring
VirtualOutputChanged	I/O monitoring

Event type	Required user privileges
SwitchStateChanged	I/O monitoring
SwitchOperationChanged	I/O monitoring
UserActionActivated	I/O monitoring
CardEntered	UID monitoring (cards/Wiegand)
CardHeld	UID monitoring (cards/Wiegand)
DtmfEntered	UID monitoring (cards/Wiegand)
PairingStateChanged	UID monitoring (cards/Wiegand)
MobKeyEntered	UID monitoring (cards/Wiegand)
WaveKeyEntered	UID monitoring (cards/Wiegand)
FingerEntered	UID monitoring (cards/Wiegand)
UserAuthenticated	UID monitoring (cards/Wiegand)
UserRejected	UID monitoring (cards/Wiegand)
CallStateChanged	Call/phone monitoring
CallSessionStateChanged	Call/phone monitoring
RegistrationStateChanged	Call/phone monitoring
DirectoryChanged	System monitoring
DirectorySaved	System monitoring
ApiAccessRequested	Access Control Monitoring
LicensePlateRecognized	Access Control Monitoring
KeyPressed	Keypad monitoring
KeyReleased	Keypad monitoring

Event type	Required user privileges
CodeEntered	Keypad monitoring

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Type	Mandatory	Default value	Description
include	string	No	new	Define the events to be added to the channel event queue: **new** – only new events occurring after channel creation **all** – all events recorded so far including those occurring after channel creation **−t** – all events recorded in the last **t** seconds including those occurring after channel creation (−10, e.g.)
filter	list	No	no filter	List of required event types separated with commas. The parameter is optional and, if not included, all the event types of the device are transmitted via the channel that are not hidden by default. It is necessary to request the hidden events in this parameter to get them. Events hidden by default: • **FingerEnrollState** • **DirectorySaved** • **DirectoryChanged** • **HardwareChanged** • **DisplayTouched** • **PairingStateChanged** • **LiftConfigChanged** • **CapabilitiesChanged** • **ConfigurationChanged** • **ExtCameraStateChanged**

Parameter	Type	Mandatory	Default value	Description
duration	uint32	No	90	Define a timeout in seconds after which the channel shall be closed automatically if no **/api/log/pull** reading operations are in progress. Every channel reading automatically extends the channel duration by the value included here. The maximum value is 3600 s.

The reply is in the **application/json** format and includes an identifier created by subscription.

Parameter	Type	Description
id	uint32	Unique identifier created by subscription

Example:

```
GET /api/log/subscribe?filter=KeyPressed,InputChanged
{
  "success" : true,
  "result" : {
    "id" : 2121013117
  }
}
```

5.10.3 api log unsubscribe

The **/api/log/unsubscribe** function helps you close the subscription channel with the given identifier. When the function has been executed, the given identifier cannot be used, i.e. all subsequent **/api/log/pull** or **/api/log/unsubscribe** calls with the same identifier will end up with an error.

The function is part of the **Logging** service and requires no special user privileges.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Type	Mandatory	Default value	Description
id	uint32	Yes	–	Identifier of the existing channel obtained by preceding dialling of **/api/log/subscribe**

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/log/unsubscribe?id=21458715
{
  "success" : true,
}
```

5.10.4 api log pull

The **/api/log/pull** helps you read items from the channel queue (subscription) and returns a list of events unread so far or an empty list if no new event is available. Larger amounts of events are pulled in batches of 128 events.

Use the **timeout** parameter to define the maximum time for the intercom to generate the reply. If there is one item at least in the queue, the reply is generated immediately. In case the channel

queue is empty, the intercom puts off the reply until a new event arises or the defined timeout elapses.

The function is part of the **Logging** service and requires no special user privileges. Reading events is conditioned by the privilege allowing the user to monitor such events, refer to 5.10.2 api log subscribe for the event table.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Type	Mandatory	Default value	Description
id	uint32	Yes	–	Identifier of the existing channel created by preceding dialling of **/api/log/subscribe**
timeout	uint32	No	0	Define the reply delay (in seconds) if the channel queue is empty. The default value 0 means that the intercom shall reply without delay.

The reply is in the **application/json** format and includes a list of events.

Parameter	Type	Description
events	array	Event object array. If no event occurs during the timeout, the array is empty.

Example:

```
GET /api/log/pull
{

  "success" : true,
  "result" : {
    "events" : [
      {
        "id" : 1,
        "tzShift" : 0,
        "utcTime" : 1437987102,
        "upTime" : 8,
        "event" : "DeviceState",
        "params" : {
          "state" : "startup"
        }
      },
      {
        "id" : 3,
        "tzShift" : 0,
        "utcTime" : 1437987105,
        "upTime" : 11,
        "event" : "RegistrationStateChanged",
        "params" : {
          "sipAccount" : 1,
          "state" : "registered"
        }
      }
    ]
  }
}
```

Events

Each event in the **events** field includes the following common information:

Parameter	Type	Description
id	uint32	Internal event record ID (32bit number, 1 after intercom restart incremented with every new event)
utcTime	uint32	Absolute event rise time (Unix Time, UTC)
upTime	uint32	Relative event rise time (seconds after intercom restart)
tzShift	int32	Difference between the local time and Coordinated Universal Time (UTC) in minutes. Add this value to utcTime to obtain the local time of event generation according to the device time zone: localTime = utcTime + tzShift * 60
event	string	Event type (KeyPressed, InputChanged, ...)
params	object	Specific event parameters

DeviceState

Signals the device state changes.

Event parameters:

Parameter	Type	Description
state	string	Signalled device state: **startup** – generated one-time after device start (always the first event ever)

Example:

```
{
  "id" : 1,
  "tzShift" : 0,
  "utcTime" : 1437987102,
  "upTime" : 8,
  "event" : "DeviceState",
  "params" : {
    "state" : "startup"
  }
}
```

AudioLoopTest

Signals performance and result of an automatic audio loop test. The event is signalled whenever the automatic test has been performed (either scheduled or manually started).

Parameter	Type	Description
result	string	Result of an accomplished text: **passed** – the test was carried out successfully, no problem has been detected. **failed** – the test was carried out, a loudspeaker/ microphone problem has been detected.

Example:


```
 {
  "id" : 26,
  "tzShift" : 0,
  "utcTime" : 1438073190,
  "upTime" : 9724,
  "event" : "AudioLoopTest",
  "params" : {
    "result" : "passed"
  }
}
```

MotionDetected

Signals motion detection via a camera. The event is available in camera-equipped models only. The event is generated only if the function is enabled in the intercom camera configuration.

Event parameters:

Parameter	Type	Description
state	string	Motion detector state: **in** – signals the beginning of the interval in which motion was detected. **out** – signals the end of the interval in which motion was detected.

Example:

```
{
  "id" : 2,
  "tzShift" : 0,
  "utcTime" : 1441357589,
  "upTime" : 1,
  "event" : "MotionDetected",
  "params" : {
    "state" : "in"
  }
}
```

NoiseDetected

Signals an increased noise level detected via an integrated or external microphone. The event is generated only if this function is enabled in the intercom configuration.

Event parameters:

Parameter	Type	Description
state	string	Noise detector state: **in** – signals the beginning of the interval in which noise was detected. **out** – signals the end of the interval in which noise was detected.

Example:

```
{
  "id" : 2,
  "tzShift" : 0,
  "utcTime" : 1441357589,
  "upTime" : 1,
  "event" : "NoiseDetected",
  "params" : {
    "state" : "in"
  }
}
```

KeyPressed and KeyReleased

Signals pressing **(KeyPressed)** or releasing **(KeyReleased)** of speed dial or numeric keypad buttons.

Event parameters:

Parameter	Type	Description
key	string	Pressed/released button code: **0** to **9** – numeric keypad buttons **%1**–**%150** – speed dialling buttons ***** – button with a * or phone symbol **#** – button with a # or key symbol

Example:

```
{
  "id" : 4,
  "tzShift" : 0,
  "utcTime" : 1437987888,
  "upTime" : 794,
  "event" : "KeyPressed",
  "params" : {
    "key" : "5"
  }
}
```

CodeEntered

Signals entering of a user code via the numeric keypad. The event is generated in numeric keypad equipped devices only.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit
session	string	Informs how many times the code has been entered.
direction	string	Code direction: **in** – arrival **out** – departure **any** – passage *Note: Set the card reader direction using the intercom configuration interface.*
code	string	User code, 1234, e.g. The code includes 2 digits at least and **00** cannot be used.
type	string	
uuid	string	User's unique ID
valid	boolean	Code validity (i.e. if the code is defined as a valid user code or universal switch code in the intercom configuration): **false** – invalid code **true** – valid code

Example:


```
{
  "id" : 128,
  "tzShift" : 0,
  "utcTime" : 1548078453,
  "upTime" : 1061,
  "event" : "CodeEntered",
  "params" : {
    "ap" : 0,
    "session" : 8,
    "direction" : "in",
    "code" : "1234",
    "type" : "user",
    "uuid" : "54877b0e-4cc3-c645-9530-6c7850f47a9c",
    "valid" : true
  }
}
```

CardEntered

Signals tapping an RFID card on the card reader. The event is generated in RFID card reader equipped devices only.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit
session		Informs how many times the card has been applied.
direction	string	RFID direction: **in** – arrival **out** – departure **any** – passage *Note: Set the card reader direction using the intercom configuration interface.*
reader	string	RFID card reader/Wiegand module name, or one of the following non-modular intercom model values: **internal** – internal card reader (**2N IP intercoms**) **external** – external card reader connected via the Wiegand interface *Note: Set the card reader name using the intercom configuration interface.*
uid	string	Unique identifier of the applied card (hexadecimal format, 6 - 16 characters depending on the card type)
uuid	string	User's unique ID

Parameter	Type	Description
valid	boolean	Validity of the applied RFID card (if the card uid is assigned to one of the intercom users listed in the phonebook) **false** – invalid card **true** – valid card

Example:


```
{
  "id" : 60,
  "tzShift" : 0,
  "utcTime" : 1548078014,
  "upTime" : 622,
  "event" : "CardEntered",
  "params" : {
    "ap" : 0,
    "session" : 5,
    "direction" : "in",
    "reader" : "ext2",
    "uid" : "4BD9E903",
    "uuid" : "54877b0e-4cc3-c645-9530-6c7850f47a9c",
    "valid" : true
  }
}
```

InputChanged and OutputChanged

Signals a state change of the logic input **(InputChanged)** or output **(OutputChanged).** Use the **/api/io/caps** function to get the list of available inputs and outputs.

Event parameters:

Parameter	Type	Description
port	string	I/O port name
state	boolean	Current I/O port logic state: **false** – inactive, log. 0 **true** – active, log. 1

Example:


```
{
  "id" : 2,
  "tzShift" : 0,
  "utcTime" : 1437987103,
  "upTime" : 9,
  "event" : "OutputChanged",
    "params" : {
    "port" : "led_secured",
    "state" : false
  }
}
```

SwitchStateChanged

Signals a switch state change (refer to the intercom configuration in Hardware | Switches).

Event parameters:

Parameter	Type	Description
switch	uint32	Switch number 1...4
state	boolean	Current logic state of the switch: **false** – inactive, log.0 **true** – active, log.1
originator	string	Informs how the switch was activated. **profile** – by transition to the preset active time profile. **api** – by http api (api/switch/ctrl). **ap** – by user authentication at the access point. The event is then completed with app and session. **rex** – by pressing the exit button (that opens the door for a defined period of time for the person to leave the room). **idt** – by http api (api/switch/ctrl) if special authentication for 2N® Indoor Touch 2.0, 1.0 was used. **dtmf** – by dtmf code in the call. **auth** – authorization by a user / universal / zone code. **uni** – universal code authorization. **zone** – zone code authorization. **automation** – by an automation action.

Example:


```
{
  "id" : 2,
  "tzShift" : 0,
  "utcTime" : 1437987103,
  "upTime" : 9,
  "event" : "SwitchStateChanged",
    "params" : {
        "switch" : 1,
        "state" : true
  }
}
```

CallStateChanged

Signals a setup/end/change of the active call state.

Event parameters:

Parameter	Type	Description
direction	string	Call direction: **incoming** – incoming call **outgoing** – outgoing call
state	string	Current call state: **connecting** – call setup in progress (outgoing calls only) **ringing** – ringing **connected** – call connected **terminated** – call terminated
peer	string	SIP URI of the calling (incoming calls) or called (outgoing calls) subscriber
session	uint32	Unique call identifier. Can also be used in the **/api/call/answer**, **/api/call/hangup** and **/api/call/status** functions.
call	uint32	TBD

Example:


```
 {
  "id" : 5,
  "tzShift" : 0,
  "utcTime" : 1438064126,
  "upTime" : 660,
  "event" : "CallStateChanged",
  "params" : {
    "direction" : "incoming",
    "state" : "ringing",
    "peer" : "sip:2229@10.0.97.150:5062;user=phone",
    "session" : 1,
    "call" : 1
  }
}
```

RegistrationStateChanged

Signals a change of the SIP account registration state.

Event parameters:

Parameter	Type	Description
sipAccount	uint32	SIP account number showing a state change: **1** – SIP account 1 **2** – SIP account 2
state	string	New SIP account registration state: **registered** – account successfully registered **unregistered** – account unregistered **registering** – registration in progress **unregistering** – unregistration in progress

Example:

```
{
  "id" : 3,
  "tzShift" : 0,
  "utcTime" : 1437987105,
  "upTime" : 11,
  "event" : "RegistrationStateChanged",
  "params" : {
    "sipAccount" : 1,
    "state" : "registered"
  }
}
```

TamperSwitchActivated

Signals tamper switch activation - device cover opening. Make sure that the tamper switch function is configured in the Digital Inputs | Tamper Switch menu.

Event parameters:

Parameter	Type	Description
state	string	Tamper switch state: **in** – signals tamper switch activation (i.e. device cover open). **out** – signals tamper switch deactivation (device cover closed).

Example:


```
{
  "id" : 54,
  "tzShift" : 0,
  "utcTime" : 1441357589,
  "upTime" : 158,
  "event" : "TamperSwitchActivated",
  "params" : {
    "state" : "in"
  }
}
```

UnauthorizedDoorOpen

Signals unauthorized door opening. Make sure that a door-open switch is connected to one of the digital inputs and the function is configured in the Digital Inputs | Door State menu.

Event parameters:

Parameter	Type	Description
state	string	Unauthorized door opening state: **in** – signals the beginning of the unauthorized opening state. **out** – signals the end of the unauthorized door opening state.

Example:

```
{
  "id" : 80,
  "tzShift" : 0,
  "utcTime" : 1441367842,
  "upTime" : 231,
  "event" : "UnauthorizedDoorOpen",
  "params" : {
    "state" : "in"
  }
}
```

DoorOpenTooLong

Signals an excessively long door opening or failure to close the door within a timeout. Make sure that a door-open switch is connected to one of the digital inputs and the function is configured in the Digital Inputs | Door State menu.

Event parameters:

Parameter	Type	Description
state	string	DoorOpenToo Long state: **in** – signals the beginning of the DoorOpenTooLong state. **out** – signals the end of the DoorOpenTooLong state.

Example:

```
{
  "id" : 96,
  "tzShift" : 0,
  "utcTime" : 1441369745,
  "upTime" : 275,
  "event" : "DoorOpenTooLong",
  "params" : {
    "state" : "out"
  }
}
```

LoginBlocked

Signals a temporary blocking of the web interface access due to repeated entering of an invalid login name or password.

Event parameters:

Parameter	Type	Description
address	string	IP address from which invalid data were entered repeatedly.

Example:

```
{
  "id" : 5,
  "tzShift" : 0,
  "utcTime" : 1441369745,
  "upTime" : 275,
  "event" : "LoginBlocked",
  "params" : {
    "address" : "10.0.23.32"
  }
}
```

UserAuthenticated

Signals user authentication and subsequent door opening.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit
session	string	Informs how many times the user has been authenticated.
name	string	Specifies the name of the phone book user.
uuid	string	User's unique ID
apbBroken	string	Tapped card validity in Anti-passback. **false** – inactive soft APB **true** – active and broken soft ABP

Example:


```
{
  "success" : true,
  "result" : {
    "events" : [
      {
        "id" : 65,
        "tzShift" : 0,
        "utcTime" : 1593606655,
        "upTime" : 7951,
        "event" : "UserAuthenticated",
        "params" : {
          "ap" : 0,
          "session" : 6,
          "name" : "Alice Gruberov\u00E1",
          "uuid" : "8fa29ebc-2fe8-4a8c-9a3b-d8b0351fb6f8",
          "apbBroken" : true
        }
      }
    ]
  }
}
```

CardHeld

Signals that an RFID card has been tapped on the reader for more than 4 s.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit
session	string	Informs how many times the card has been applied.
direction	string	RFID direction: **in** – arrival **out** – departure **any** – passage *Note: Set the card reader direction using the intercom configuration interface.*
reader	string	Identification of the reader that read the card.
uid	string	User uid for devices connected to the Access Commander only. Devices disconnected from the Access Commander do not send this parameter.
valid	string	true, false

Example:


```
{
  "id" : 9,
  "tzShift" : 0,
  "utcTime" : 1516893493,
  "upTime" : 354,
  "event" : "CardHeld",
  "params" : {
    "ap" : 1,
    "session" : 4,
    "direction" : "out",
    "reader" : "ext2",
    "uid" : "3F00F318E7",
    "valid" : true
   }
}
```

SilentAlarm

Signals silent alarm activation.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit.
session	string	Informs how many silent alarms have been activated.
name	string	Specifies the phonebook username.

Example:

```
{
  "id" : 200,
  "tzShift" : 0,
  "utcTime" : 1548079445,
  "upTime" : 2053,
  "event" : "SilentAlarm",
  "params" : {
    "ap" : 0,
    "session" : 17,
    "name" : "Joseph",
    "uuid" : "54877b0e-4cc3-c645-9530-6c7850f47a9c"
  }
}
```

AccessLimited

Signals rejection of the set user.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit.
type	string	card, code, finger
state	string	State, available values: in = active, out = inactive.

Example:

```
{
    "id" : 408,
    "tzShift" : 0,
    "utcTime" : 1517302112,
    "upTime" : 408951,
    "event" : "AccessLimited",
    "params" : {
      "ap" : 0,
      "type" : "card",
      "state" : "in"
    }
}
```

PairingStateChanged

Signals pairing with a Bluetooth interface.

Event parameters:

Parameter	Type	Description
state	string	pending / inactive / pending_blocked / expired / paired
authId	string	Authorisation ID

Example:


```
{
  "id" : 197,
  "tzShift" : 0,
  "utcTime" : 1516894499,
  "upTime" : 1360,
  "event" : "PairingStateChanged",
  "params" : {
    "state" : "pending",
    "authId" : "F2CAE955C9B4E81CD00E3A096E52543B"
  }
}
```

SwitchesBlocked

Signals lock blocking by the tamper switch. If the function is enabled, all the switches get blocked for 30 minutes whenever the tamper is activated. Blocking is active even after the device restart

Event parameters:

Parameter	Type	Description
state	string	in, out

Example:


```
{
  "id" : 205,
  "tzShift" : 0, "utcTime" : 1516894667,
  "upTime" : 1528,
  "event" : "SwitchesBlocked",
  "params" : {
    "state" : "in"
  }
}
```

FingerEntered

Signals that a finger has been tapped on the biometric reader.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit.
session	string	Informs how many times the finger has been enrolled.
direction	string	Fingerprint reader passage direction: **"in"** – entry **"out"** – exit **"any"** – any direction *Note: Set the reader passage direction via the intercom configuration interface.*
uuid	string	User's unique ID
valid	string	Fingerprint validity (if available as a valid user fingerprint in the configuration) **false** – invalid fingerprint **true** – valid fingerprint

Example: Reading of a user's fingerprint

```
{
  "id" : 1368,
  "tzShift" : 0,
  "utcTime" : 1548145535,
  "upTime" : 62598,
  "event" : "FingerEntered",
  "params" : {
    "ap" : 0,
    "session" : 1,
    "direction" : "in",
    "valid" : false
  }
}
```

Unsuccessful specification: Reading of an unset user's fingerprint

```
{
    "id" : 14,
    "tzShift" : 0,
    "utcTime" : 1511859513,
    "upTime" : 65887,
    "event" : "FingerEntered",
    "params" : {
        "session" : 3,
        "valid" : false
    }
}
```

MobKeyEntered

Signals Bluetooth reader authentication.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit.
session	string	Informs how many times the WaveKey authorisation has been applied.
direction	string	Passage direction: **"in"** – entry **"out"** – exit **"any"** – any direction *Note: Set the reader passage direction via the intercom configuration interface.*
authid	string	WaveKey ID.
uuid	string	User's unique ID
valid	string	WaveKey validity (if available as a valid user WaveKey in the configuration) **false** – invalid WaveKey **true** – valid WaveKey

Example:


```
{
  "id" : 161,
  "tzShift" : 0,
  "utcTime" : 1548079174,
  "upTime" : 1782,
  "event" : "MobKeyEntered",
  "params" : {
    "ap" : 0,
    "session" : 9,
    "direction" : "in",
    "authid" : "48c48155eed7ea1dbb0b4d534b7459b9",
    "uuid" : "54877b0e-4cc3-c645-9530-6c7850f47a9c",
    "valid" : true
  }
}
```

DoorStateChanged

Signals a door state change.

Event parameters:

Parameter	Type	Description
state	string	opened, closed

Example:

```
{
        "id" : 240,
        "tzShift" : 0,
        "utcTime" : 1516895295,
        "upTime" : 2156,
        "event" : "DoorStateChanged",
        "params" : {
          "state" : "opened"
        }
}
```

UserRejected

Signals user authentication rejection.

Event parameters:

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit.
session	string	Informs how many times the authorisation has been rejected.
name	string	User name
uuid	string	User's unique ID
reason	string	accessBlocked, switchLocked, invalidTime, invalidProfile, invalidSequence, invalidCredential, authInterrupted, timeout, switchDisabled

Example:


```
{
  "id" : 173,
  "tzShift" : 0,
  "utcTime" : 1548079274,
  "upTime" : 1882,
  "event" : "UserRejected",
  "params" : {
    "ap" : 0,
    "session" : 10,
    "name" : "Joseph",
    "uuid" : "54877b0e-4cc3-c645-9530-6c7850f47a9c",
    "reason" : "invalidCredential"
  }
}
```

DisplayTouched

Signals display touch.

Event parameters:

Parameter	Type	Description
x	string	Display touch point coordinate. The maximum value depends of the display resolution.
y	string	Display touch point coordinate.
dx	string	Coordinate change due to movement on the display; negative values are possible. The maximum value depends of the display resolution.
dy	string	Coordinate change due to movement on the display.

Example:


```
{
    "id" : 337,
    "tzShift" : 0,
    "utcTime" : 1517301424,
    "upTime" : 408263,
    "event" : "DisplayTouched",
    "params" : {
      "x" : 89,
      "y" : 100,
      "dx" : 0,
      "dy" : 0
    }
}
```

DtmfEntered

Signals a DTMF code in the call.


```
{
    "id" : 86,
    "tzShift" : 0,
    "utcTime" : 1558522871,
    "upTime" : 3531,
    "event" : "DtmfEntered",
    "params" : {
      "code" : "00",
      "type" : "uni",
      "call" : 3,
      "valid" : true
 }
}
```


Parameter	Type	Description
code	string	Display the code characters entered.
type	string	The code type used. **uni** – universal switch code **user** – user code
call	string	Call ID.
valid	string	Code validity (i.e. the valid universal switch code or valid user code). **false** – invalid code **true** – valid code

AccessTaken

Signals that a card has been tapped in the Anti-passback area.

```
{
  "success" : true,
  "result" : {
    "events" : [

    ]
  }
}
```

ApLockStateChanged

Signals an emergency lockdown state change (on/off).

```
{
    "id" : 35,
    "tzShift" : 0,
    "utcTime" : 1558522465,
    "upTime" : 3125,
    "event" : "ApLockStateChanged",
    "params" : {
      "ap" : 0,
      "state" : "in"
    }
}
```

Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit.
state	string	Status change state. **"in"** – beginning of the emergency lockdown interval **"out"** – end of the emergency lockdown interval

RexActivated

Signals the input activation set for the REX button.


```
{
    "id" : 29,
    "tzShift" : 0,
    "utcTime" : 1558522162,
    "upTime" : 2822,
    "event" : "RexActivated",
    "params" : {
      "ap" : 1,
      "session" : 1
    }
}
```


Parameter	Type	Description
ap	string	Access Point, available states: 0 = entry, 1 = exit.
session	string	Display how many times the REX button has been activated.

LiftStatusChanged

Signals the Lift Control module connection/disconection.


```
  {
        "id" : 2871,
        "tzShift" : 0,
        "utcTime" : 1561540370,
        "upTime" : 73822,
        "event" : "LiftStatusChanged",
        "params" : {
          "module" : 0,
          "ready" : true
        }

},
```


Parameter	Type	Description
module	string	Display the ID module.
ready	string	

LiftFloorsEnabled

Signals permanent access to a floor or permanent user access.

```
 {
       "id" : 2850,
       "tzShift" : 0,
       "utcTime" : 1561540011,
       "upTime" : 73463,
       "event" : "LiftFloorsEnabled",
       "params" : {
         "type" : "user"
         "floors" : [
           0, 1, 2, 3, 4
         ],
         "uuid" : "621a5a49-1f8b-d34c-9a8b-881055864deb",
       }
     },
```

```
{
       "id" : 2855,
       "tzShift" : 0,
       "utcTime" : 1561540016,
       "upTime" : 73468,
       "event" : "LiftFloorsEnabled",
       "params" : {
         "type" : "public"
         "floors" : [
           1, 4
         ],
       }
     },
```

Parameter	Type	Description
type	string	Provides information on the access type. **public** – change of public access **user** – user authentication
floors	string	Provides information on the accessible floors.

LifConfigChanged

Signals a change in the lift control configuration.

```
{
        "id" : 2860,
        "tzShift" : 0,
        "utcTime" : 1561540163,
        "upTime" : 73615,
        "event" : "LiftConfigChanged",
        "params" : {
          "hash" : 11
        }
      },
```

Parametr	Typ	Popis
hash	string	Unique configuration code.

CapabilitiesChanged
Signals a change in available functions.


```
{
  "success":true,
  "result":{
   "events":[
     {
      "id":21,
      "tzShift":0,
      "utcTime":1585037151,
      "upTime":256,
      "event":"CapabilitiesChanged",
      "params":{

      }

     }


   ]

  }

}
```

Parameter	Type	Description
id	string	Event sequence number.
tzShift	uint32	Difference between the local time and UTC in minutes. Add this value to utcTime to get the local time of event generation according to the time zone setting in the device: localTime = utcTime + tzShift * 60
utcTime	uint32	Absolute event generation time (Unix Time, UTC – Coordinated Universal Time).
upTime	uint32	Relative event generation time (seconds after the intercom restart).
event	string	CapabilitiesChanged event type.
params	object	Specific parameters of the event.

5.11 api audio

The following subsections detail the HTTP functions available for the **api/audio** service.

5.11.1 api audio test

The **/api/audio/test** function launches an automatic test of the intecom built-in microphone and speaker. The test result is logged as an **AudioLoopTest** event.

The function is part of the **Audio** service and the user must be assigned the **Audio Control** privilege for authetication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/audio/test
{
  "success" : true
}
```

5.12 api email

The following subsections detail the HTTP functions available for the **api/email** service.

5.12.1 api email send

The **/api/email/send** function sends an e-mail to the required address. Make sure that the SMTP service is configured correctly for the device (i.e. correct SMTP server address, login data etc.).

The function is part of the **Email** service and the user must be assigned the **Email Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

Request parameters:

Parameter	Description
to	Mandatory parameter specifying the delivery address.
subject	Mandatory parameter specifying the subject of the message.
body	Optional parameter specifying the contents of the message (including html marks if necessary). If not completed, the message will be delivered without any contents.
pictureCount	Optional parameter specifying the count of camera images to be enclosed. If not completed, no images are enclosed. Parameter values: [0, 5].
timeSpan	Optional parameter specifying the timespan in seconds of the snapshots enclosed to the email. Default value: 0.

Parameter	Description
width	Optional parameters specifying the resolution of camera images to be enclosed. The image height and width must comply with one of the supported options (see **api/camera/caps**).
height	

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/email/send?to=somebody@email.com&subject=Hello&body=Hello
{
  "success" : true
}
```

5.13 api pcap

The following subsections detail the HTTP functions available for the **api/pcap** service.

5.13.1 api pcap

The **/api/pcap** function helps download the network interface traffic records (pcap file). You can also use the **/api/pcap/restart** a **/api/pcap/stop** functions for network traffic control.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and the downloaded file can be opened directly in Wireshark, for example.

Example:

```
GET /api/pcap
```

5.13.2 api pcap restart

The **/api/pcap/restart** function deletes all records and restarts the network interface traffic recording.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/pcap/restart
{
  "success" : true
}
```

5.13.3 api pcap stop

The **/api/pcap/stop** function stops the network interface traffic recording.

The function is part of the **System** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET** or **POST** method can be used for this function.

The function has no parameters.

The reply is in the **application/json** format and includes no parameters.

Example:

```
GET /api/pcap/restart
{
  "success" : true
}
```

5.13.4 api pcap live

The **api/pcap/live** function is used for starting of the chunked packet capture.

Service and Privileges Groups

- Service group is System.
- Privileges group is System Control.

Methods

- GET
- POST

Request

The request contains parameters in the URL (or in the **application/x-www-form-urlencoded** format when POST is used).

Table 1. Request Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
duration	No	Integer defining duration of download in seconds	indefinitely	Defines the duration of the packet capture. If the parameter is omitted or 0, the duration is infinite (i.e. until it is stopped by **api/pcap/live/stop** or the download is severed by the target device).

Example of a Request

```
URL: https://192.168.1.1/api/pcap/live?duration=10
```

Response

The device starts streaming chunked data upon a successful request.

Example of Using Python to Download the Packet Capture

```
command = requests.post( "https://" + address + "/api/pcap/live?duration=120",
verify=False, stream=True, auth=HTTPBasicAuth("admin", "pass") ) with
open("trace.pcap", 'wb') as f: for chunk in command.iter_content(chunk_size=None):
f.write(chunk)
```

If a packet capture is already running, another packet capture cannot be started.

5.13.5 api pcap live stop

The **api/pcap/live/stop** function is used for stopping of the chunked packet capture.

Service and Privileges Groups

- Service group is System
- Privileges group is System Control

Methods

- GET
- POST

Request

The request does not have any parameters.

Example of a Request

```
URL: https://192.168.1.1/api/pcap/live/stop
```

Response

The device stops streaming chunked data upon a successful request. The request can help stop a capture without a set duration or stop a capture with a duration value prematurely.

The device replies with **`success`** : **`true`** even if there is no running capture. There are no specific error codes for this endpoint.

5.13.6 api pcap live stats

The **api/pcap/live/stats** function is used for getting of status of the chunked packet capture.

Service and Privileges Groups

- Service group is System.
- Privileges group is System Control.

Methods

- GET
- POST

Request

The request does not have any parameters.

Example of a Request

```
URL: https://192.168.1.1/api/pcap/live/stats
```

Response

The response is in the **application/json** format. The response contains the **success** and **result** keys. The **result** value contains detailed information on the packet capture status.

Table 1. Response JSON Keys

Key	Typical Returned Values	Description
running	`true` or `false`	Indicates whether the chunked packet capture is currently running or not.
bytesSent	Integer	Contains the number of bytes sent in the currently running open packet capture. If the packet capture is not running, the value is 0.
packetsSent	Integer	Contains the number of packets sent in the currently running open packet capture. If the packet capture is not running, the value is 0.

Example of a Response

```
{ "success": true, "result": { "running": true, "bytesSent": 11261, "packetsSent": 90
} }
```

5.14 api dir

The following subsections detail the HTTP functions available for the **api/dir** service.

5.14.1 api dir template

The **/api/dir/template** function retrieves the template of an entry in the directory.

Methods

- GET
- POST

Request

Table 1. Request Parameters

Key Name	Mandatory	Expected Values	Default Value	Description
N/A	-	-	-	-

Example of a Request

```
https://192.168.1.1/api/dir/template
```

Response

The response is in the **application/json** format. The **result** object contains the keys **series** and **users**.

Go to the topic **api/dir/query** to get more information on the use of the key **series**.

The key **users** contains an array with one object (entry template) that contains all available keys of an entry in the directory with their default values for a particular device.

Tip

- You can get better acquainted with the structure of the JSON response in the example at the end of this topic.

Note

- Available keys depend on the model, type and hardware configuration of a device (e.g. key photo is only applicable for devices that have a display and store images in their directories).

Table 2. Response JSON Keys in the **users** Array

Key	Typical Returned Values	Description
uuid	Empty	Unique User Identifier. When a new entry in the directory is created by **api/dir/create**, uuid can be either provided as a parameter of the request or automatically generated by the device. The format of uuid is "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX", where X can be any hexadecimal digit. All zeroes are reserved for an empty uuid.
deleted	`false`	Indication of whether an entry in the directory has been deleted or not. Deleted entries remain in the directory until the maximum number of entries is reached. Stored deleted entries preserve uuid only for logging reasons. Two valid values: `false`, `true`.
owner	Empty	Indication of whether an entry in the directory is remotely managed by 2N® My2N, 2N® Access Commander or another remote management system. This value is intended for internal 2N® TELEKOMUNIKACE a.s. usage, alternatively it can be used for deleting a group of users (see **api/dir/delete**).
name	Empty	Name of an entry in the directory (a user or device name). A string of up to 63 characters is expected. The name can be left empty (the entry is in such a case identified by its uuid in logs, emails, etc.).

Key	Typical Returned Values	Description
photo	Empty	Image of an entry in the directory (e.g. user's photo, company logo). Saved as base64 encoded jpeg with the following syntax: **EXAMPLE:** ***_DATA_IN_BASE64***
email	Empty	Email address of an entry in the directory. The expected format is namestructure@domainhierarchy.top. It is possible to enter multiple addresses separated with commas (saved as one string).
treepath	/	Definition of positions of an entry in the directory on the display. • The default position is in the root folder. This position is achieved by simply entering only one slash. **EXAMPLE: /** shows the entry in a root folder • An entry may be positioned on a display several times - the positions are separated with a semi-colon (**;**). **EXAMPLE: */Folder1/;/Folder2/*** shows the entry both in Folder1 and Folder2 • An entry may be assigned a calling group that also serves as an alternative name in an individual position on the display by omitting the slash at the end of the position definition. **EXAMPLE: */Folder1/Calling Group*** shows the entry in Folder1 under the name "Calling Group" • An entry may be prioritized (i.e. a prioritized entry is shown above unprioritized entries) individually in each position by adding **:1** at the end of the position definition. **EXAMPLE: */Folder1/:1;Folder2/Calling Group:1*** shows the entry prioritized in Folder1 under its name and the entry prioritized in Folder2 as "Calling Group". • Multiple entries may be assigned to one calling group (selecting this calling group on a display results in a group call to all the entries under the calling group). **EXAMPLE:** *Entry1:* ***/Calling Group*** *Entry2:* ***/Calling Group*** shows both entries in the root folder as one row named "Calling Group" (both entries are called when this row is selected)

Key	Typical Returned Values	Description
virtNumber	Empty	Virtual number of an entry in the directory. Virtual numbers may be dialed using a dialpad (if configured). The maximum length is 7 characters. The first and the last character may be chosen from the range of A to Z or 0 to 9. The rest of the characters may be between 0 to 9.
deputy	Empty	Uuid of a deputy entry that is called when the original callee is unavailable or not answering. When the deputy is not set the deputy uuid, it remains empty.
buttons	Empty	Buttons assigned to this entry in the directory. An array of integers (assigned according to the button position starting from 1) separated by a comma.

Key	Typical Returned Values	Description

callPos	Array	Calling information of an entry. Entered as an array of up to three objects, i.e. up to three sets of calling information can be entered. Each of these three objects can contain the following keys:
		• peer - a phone number of an entry in the directory
		• profiles - time profiles if this phone number is valid (a number is not dialed when invalid)
		  • P=X,..,Y
		  where X,..,Y stands for a comma-separated array of predefined time profiles from 0 (time profile 1) to 19 (time profile 20)
		  EXAMPLE: *P=1,3,5* means that the predefined profiles 2, 4 and 6 define the validity period of the phone number
		  • D=A,..,B@H:MM-H:MM
		  where A,..,B stands for a comma-separated array of days of week (0 to 6 from Sunday to Saturday, 7 is Holiday), H stands for hour of the day (from 0 to 23), MM stands for minutes (from 00 to 59) - two values defining an interval. Several definitions may be combined separated with a semi-colon.
		  EXAMPLE: *D=7@0:15-13:15;D=5,7@13:15-15:15;D=7@15:15-23:30* means that the phone number is valid on Holiday from 0:15 to 13:15, on Friday and Holiday from 13:15 to 15:15 and on Holiday from 15:15 to 23:30.
		  EXAMPLE: *D=5,7* means that the phone number is valid on Friday and Holiday for the whole day.
		• grouped - defines whether the number is dialed in a group call together with the previous number (the third number is dialed with a deputy). Can be `true` or `false`.
		• ipEye - defines the IP address of the PC on which the 2N® IP Eye application is running (used for receiving video if the telephone does not have a display).

Key	Typical Returned Values	Description

access	JSON Object	Access Control information of an entry in the directory. Contains the following keys:
		• validFrom - definition of the start of the validity term for the credentials of an entry in the directory. Entered in the Unix Time format. If left empty, the validity period starts at the beginning of the time (i.e. 00:00:00 UTC Jan 1st 1970).
		• validTo - definition of the end of the validity term for the credentials of an entry in the directory. Entered in the Unix Time format. If left empty, the validity period ends at the end of the time (i.e. 03:14:07 UTC Jan 19th 2038).
		• accessPoints - contains an array of access points (two access points, entry and exit). Each array item is represented as a JSON object with the following keys:
		  • enabled - defines whether it is generally possible to use this access point (i.e. if it is possible to authenticate at that particular access point). Two valid values: `true`, `false`.
		  • profiles - defines whether it is currently possible to use this access point (i.e. if it is possible at the moment to authenticate at that particular access point). The syntax of the profile definition is the same as in callPos.
		• pairingExpired - defines whether the Bluetooth pairing of an entry in the directory has expired or not. Two valid values: `true`, `false`.
		• virtCard - defines the virtual card of an entry in the directory that is relayed to Wiegand and other 3rd party systems if there is a successful authentication of the entry in the directory. 6 to 32 hexadecimal characters are expected.
		• card - defines up to two cards of an entry in the directory that are used for authentication. The card numbers are written as an array of strings. 6 to 32 hexadecimal characters are expected.
		• mobkey - defines the Bluetooth authentication ID of an entry in the directory. 32 hexadecimal characters are expected.

Key	Typical Returned Values	Description
		• fpt - fingerprint templates of an entry in the directory. An encoded fingerprint is expected (for the details contact the Technical Support staff). • pin - defines the pin of an entry in the directory. 2 to 15 digits are expected. • apbException - defines whether an entry in the directory has an exception from the anti-passback policy (e.g. if so, its credentials can be used multiple times for entry without any exit). Two valid values: `true`, `false`. • code - defines up to three individual codes for switches. The individual switch codes are written in an array of strings (2 to 15 digits). The first position in the array defines an individual code for the first switch. Input an empty string to skip a code for the particular switch. • liftFloors - defines the configuration of accessible lift floors upon authentication. The following formatting is expected: F=P,..,R@PROFILE1_DEFINITION| F=X,..,Z@PROFILE2_DEFINITION where P,..,R and X,..,Z are arrays of comma-separated floors (0 to 63). io_1_1 is entered as 0, io_1_5 is entered as 4, io_2_2 is entered as 9 and so on. The arrays of floors active in certain profiles are separated by |. Predefined profiles or ad hoc definition of a new profile can be used (see the syntax definition in callPos/profiles). The profile definition part can be omitted if no profile is applied. ***EXAMPLE: F=2,4*** defines floors without any time profile (user can access them any time). ***EXAMPLE: F=5@P=0,7*** defines that the sixth floor (F=5) is accessible the whole day on Mondays and Holidays. ***EXAMPLE: F=0@P=7,13|F=0@D=5@9:15-11:45;D=4@11:45-13:30*** defines that the first floor (F=0) is accessible in predefined profiles 8 and 14 (P=7,13) and in the time profile defined by the definition string.

Key	Typical Returned Values	Description
		• licensePlates - defines a set of license plates configured to the user (used for opening upon license plate recognition). Individual licensePlates are separated by a comma. Whitespaces are ignored. A maximum of 255 characters is allowed (including whitespaces). The array is limited to 20 license plates and each license plate may have a maximum of 10 non-whitespace characters.
timestamp	0	A timestamp of performed changes in the directory. Timestamps are automatically generated by the directory in an ascending order. Go to the topic **api/dir/query** to get more information on the use of the timestamp.

Example of a Response


```
{
    "success": true,
    "result": {
        "series": "5247939846841727056",
        "users": [
            {
                "uuid": "",
                "deleted": false,
                "owner": "",
                "name": "",
                "photo": "",
                "email": "",
                "treepath": "\/",
                "virtNumber": "",
                "deputy": "",
                "buttons": "",
                "callPos": [
                    {
                        "peer": "",
                        "profiles": "",
                        "grouped": false,
                        "ipEye": ""
                    },
                    {
                        "peer": "",
                        "profiles": "",
                        "grouped": false,
                        "ipEye": ""
                    },
                    {
                        "peer": "",
                        "profiles": "",
                        "grouped": false,
                        "ipEye": ""
                    }
                ],
                "access": {
                    "validFrom": "0",
                    "validTo": "0",
                    "accessPoints": [
                        {
                            "enabled": true,
                            "profiles": ""
                        },
                        {
                            "enabled": true,
                            "profiles": ""
                        }
                    ],
```

```
                    "pairingExpired": false,
                    "virtCard": "",
                    "card": [
                        "",
                        ""
                    ],
                    "mobkey": "",
                    "fpt": "",
                    "pin": "",
                    "apbException": false,
                    "code": [
                        "",
                        "",
                        "",
                        ""
                    ],
                    "licensePlates": "",
                    "liftFloors": ""
                },
                "timestamp": 0
            }
        ]
    }
}
```


5.14.2 api dir create

The **/api/dir/create** function creates (or overwrites) an array of entries in the directory and sets their selected fields.

Service and Privileges Groups

- Service group is System.
- Privileges group is System Control.

Methods

- PUT

Request

The request contains the **query** parameter and parameters in the **application/json** format.

Key Name	Type	Mandatory	Expected Values	Default Value	Description
force	query	No	`1 (True)` `0 (False)`	`0`	This key selects whether the entry in the directory identified by uuid (see below) is overwritten by the new set of data. When the value for this key is set to `True`, a new dataset overwrites the existing data and the remaining fields are reset to their default values. When it is set to `False` or omitted and there is an existing entry in the directory with the specified uuid, the device replies with error code `EDIR_UUID_ALREADY_EXISTS` and changes to the configuration are not processed. This key does not affect a creation of a new entry in the directory in any way.
.users	application/json	No	array of JSON objects defining parameters of an entry in the directory	-	Go to the topic **api/dir/template** to get an overview of all available keys in the JSON definition of an entry in the directory. It is possible to submit empty objects in the array. The device creates an empty entry in the directory for each empty object (it is only assigned a uuid). If an object in the array contains the key uuid, an entry with the specified uuid is created or modified, or the device replies with an error code. If an object in the array does not contain uuid, the device creates a new entry and assign it a new uuid. The entry parameters are set to the values according to the keys defined in the JSON structure of a request. Study the example below. If this key is omitted or if its value is an empty array, the device response contains only the key **series** (no new entries in the directory are created).

Example of Request

Request 1: Creation of new directory

```
URL: https://192.168.1.1/api/dir/create?force=1
JSON:
{
  "users": [
    {
      "uuid": "01234567-89AB-CDEF-0123-456789ABCDEF",
      "name": "Julius Thompson",
      "email": "Julius@snlsa.com",
      "access": {
        "pin": "1234"
      }
    },
    {
      "name": "Carlos Inpiers",
      "owner": "My2N",
      "email": "Carlos_Inpieros@emailos.cz"
    },
    {
      "uuid": "01234567-89AB-CDEF-0123-456789ABCDEF",
      "name": "Fridrich Dairy",
      "email": "mycountry",
      "access": {
        "pin": "5678"
      },
      "test": "something",
      "albert": "einstein"
    },
    {},
    {}
  ]
}
```

1. First Entry: If there is no entry in the directory with uuid 01234567-89AB-CDEF-0123-456789ABCDEF, the device creates an entry in the directory with this uuid and set its parameters name, email and access to the specified values. If there is an entry in the directory with uuid 01234567-89AB-CDEF-0123-456789ABCDEF, the device overwrites its parameters name, email and access to the specified values and sets all of its other parameters to their default values (because the key force is set to True).
2. The device creates a second entry, assigns it a random uuid, sets its name, owner and email to the specified values and leaves the rest of its parameters at default values.
3. The third entry does not overwrite the existing entry with the same uuid because there are several errors (wrong email format, two non-existent fields referenced by **test** and **albert**).
4. Furthermore, two new empty entries are created (because there are two empty objects in the array). Each is assigned a random uuid, the rest of their parameters are set to default values.

Request 2: Creation of 3 new users

```
URL: https://192.168.1.1/api/dir/create
JSON:
{
   "users":[
      {
         "name":"user1",
         "email":"user1gmail.com",
         "callPos":[
            {
               "peer":"2246",
               "profiles":"",
               "grouped":false
            }
         ]
      },
      {
         "name":"user2",
         "email":"user2@gmail.com",
         "callPos":[
            {
               "peer":"2246",
               "profiles":"",
               "grouped":false
            }
         ]
      },
      {
         "name":"user3",
         "email":"user3@gmail.com",
         "callPos":[
            {
               "peer":"234324234",
               "profiles":"",
               "grouped":false
            }
         ]
      }
   ]
}
```

The request tries to create three new entries in the directory and assign them random uuid identifiers, names, e-mails and call information (CallPos), leaving default values for the remaining parameters.

Response

The response is in the **application/json** format. The **result** object contains the keys **series** and **users**.

Go to the topic **api/dir/query** to get more information on the use of the key **series**.

The key **users** contains an array of objects that contain keys and values of the result of the request (see the table below).

Tip

- You can get better acquainted with the structure of the JSON response in the example at the end of this topic.

Table 2. Response JSON Keys in the **users** Array

Key	Typical Returned Values	Description
uuid	uuid	Unique User Identifier of a created, modified or unchanged entry.
timestamp	integer	A timestamp of performed changes in the directory. Go to the topic **api/dir/query** to get more information on the use of the timestamp. Timestamp is present only when a change in the directory was successful.

Key	Typical Returned Values	Description
errors	array of error objects	An error object containing an array of all errors that occured. **errors** object is present only when a change in the directory failed. It contains an error code in the value of the key **code** showing a reason for the failure of a change in the directory. It may contain a further specification of the error reason in the value of the key **field** for error codes `EDIR_FIELD_NAME_UNKNOWN` and `EDIR_FIELD_VALUE_ERROR` showing which key or value violates the validation rules. The following error codes may be returned in a response: • `EDIR_UUID_DOES_NOT_EXIST` – user with given uuid does not exist. • `EDIR_UUID_IS_MISSING` – mandatory parameter uuid is missing. • `EDIR_UUID_INVALID_FORMAT` - uuid is not in the valid format which is "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX", where X can be any hexadecimal digit. All zeroes are reserved as an empty uuid. • `EDIR_UUID_ALREADY_EXISTS` - an entry with the specified uuid exists in the directory and the key **force** is set to false or omitted. Therefore the requested modification cannot be performed. • `EDIR_FIELD_NAME_UNKNOWN` - unknown key. The list of available keys for a particular device can be obtained using the **/api/dir/template** function. • `EDIR_FIELD_NOT_AVAILABLE` – the set key is invalid for the given device model. The list of available keys for a particular device can be obtained using the **/api/dir/template** function. • `EDIR_FIELD_VALUE_ERROR` - the specified value does not fit validation criteria (the value is not valid). • `EDIRLIM_USER` - the directory is full. • `EDIRLIM_PHOTO` - the limit of photo storage has been reached. New entries can be created without photos. • `EDIRLIM_FPT` - the limit of fingerprint templates storage has been reached. New entries can be created without fingerprint templates. • `EINCONSISTENT` - there is an inconsistency in the values of the keys **validFrom** and **validTo** (**validFrom** has to be lower than **validTo**).

Examples of Response

Response to Request 1: Creation of new directory


```
{
  "success": true,
  "result": {
    "series": "6423407687606431951",
    "users": [
      {
        "uuid": "01234567-89AB-CDEF-0123-456789ABCDEF",
        "timestamp": 34
      },
      {
        "uuid": "044197A7-54AD-7577-6EEA-787A6097263E",
        "timestamp": 35
      },
      {
        "errors": [
          {
            "code": "EDIR_FIELD_VALUE_ERROR",
            "field": "email"
          },
          {
            "code": "EDIR_FIELD_NAME_UNKNOWN",
            "field": "test"
          },
          {
            "code": "EDIR_FIELD_NAME_UNKNOWN",
            "field": "albert"
          }
        ]
      },
      {
        "uuid": "41970B83-21C8-45DD-8FFC-787A6097263E",
        "timestamp": 36
      },
      {
        "uuid": "0447BBA7-6E7c-420C-A654-466D43D6A067",
        "timestamp": 37
      }
    ]
  }
}
```


1. The first entry is created with the specified uuid and fields (unspecified fields are set to their default values). The entry gets created regardless whether there is an already existing entry with the same uuid because the key **force** in the request is set to `true`. The timestamp of the change is returned.

2. The second entry is created, assigned a random uuid and its specified fields are filled (unspecified fields are set to their default values). The timestamp of the change is returned.
3. The third object in the request contained an invalid email address format. Furthermore, non-existent fields were referenced by the keys **test** and **albert**.
4. The fourth and fifth entries where created successfully with randomly assigned uuids and all fields set to default values. The timestamp in the device updated twice to reflect that. The timestamps of the changes are returned.

Response to Request 2: Creation of 3 new users


```
{
   "success":true,
   "result":{
      "series":"20680937807286928 47",
      "users":[
         {
            "uuid":"01234567-89AB-CDEF-0123-456789ABCDCC",
            "errors":[
               {
                  "code":"EDIR_FIELD_VALUE_ERROR",
                  "field":"email"
               }
            ]
         },
         {
            "uuid":"01234567-89AB-CDEF-0123-456789ABCDCB",
            "timestamp":15207
         },
         {
            "uuid":"01234567-89AB-CDEF-0123-456789ABCDCA",
            "timestamp":15208
         }
      ]
   }
}
```


The e-mail of the user1 entry was invalid, so the entry was not created. The other two users were created successfully.

5.14.3 api dir update

The **/api/dir/update** function updates an array of entries in the directory and sets their selected fields.

Methods

- PUT

Request

The request contains parameters in the **application/json** format. Go to the topic **api/dir/template** to get more information on various parameters of an entry in the directory and their representation.

Table 1. Request JSON Keys

Key Name	Mandatory	Expected Values	Default Value	Description
users	Yes	array of JSON objects defining parameters of an entry in the directory	-	The array has to contain at least one object with the key **uuid**, which defines the entry to be updated. Go to the topic **api/dir/template** to get an overview of all available keys in the JSON definition of an entry in the directory.

Example of Request

```
URL: https://192.168.1.1/api/dir/update JSON { "users": [ { "uuid": "01234567-89AB-CDEF-0123-456789ABCDEF", "name": "ABCD", "email": "abcd@def.cz", "access": { "pin": "1234" } }, { "uuid": "76543210-68FF-18CA-3210-FEDCBA987654", "name": "ABCD2", "owner": "My2N", "email": "abcd2@def.cz" }, { "uuid": "01234567-89A-CDEF-0123-456789ABCDEF", "name": "ABCD3", "owner": "My2N", "email": "abcd3@def.cz" }, { "uuid": "01234567-89AB-CDEF-0123-456789ABCDEF", "name": "ABCD4", "owner": "My2N", "email": "abcd4@def.cz", "albert": "einstein" }, { "uuid": "01234567-89AB-CDEF-0123-456789ABCDEF", "name": "ABCD4", "owner": "My2N", "email": "abcd4@def.cz", "access.pin": "hello" } ] }
```

If there is no entry in the directory with uuid 01234567-89AB-CDEF-0123-456789ABCDEF, the device will respond with an error code (see below). Similarly for the second uuid 76543210-68FF-18CA-3210-FEDCBA987654.

If the entry with uuid 01234567-89AB-CDEF-0123-456789ABCDEF is present, it will update its parameters according to the specified values for various keys. Similarly for the second uuid 76543210-68FF-18CA-3210-FEDCBA987654.

The third entry will not be updated (uuid has a wrong format).

The fourth entry will not be updated (unknow field name).

The fifth entry will not be updated (wrong format of access pin).

Response

The response is in the **application/json** format. The **result** object contains the keys **series** and **users**.

Go to the topic **api/dir/query** to get more information on the use of the key **series**.

The key **users** contains an array of objects that contain keys and values of the result of the request (see the table below).

Tip

- You can get better acquainted with the structure of the JSON response in the example at the end of this topic.

Table 2. Response JSON Keys in the **users** Array

Key	Typical Returned Values	Description
uuid	uuid	Unique User Identifier of a modified or unchanged entry.
timestamp	integer	A timestamp of performed changes in the directory. Go to the topic **api/dir/query** to get more information on the use of the timestamp. The timestamp is present only when a change in the directory was successful.

Key	Typical Returned Values	Description
errors	array of error objects	An error object containing array of all errors that occured. **errors** key is present only when a change in the directory failed. It contains an error code in the key **code** showing a reason for the failure of a change in the directory. It may contain a further specification of the error reason in the key **field** for error codes `EDIR_FIELD_NAME_UNKNOWN` and `EDIR_FIELD_VALUE_ERROR` showing which key or value violates the validation rules. The following error codes may be returned in a response: • `EDIR_UUID_DOES_NOT_EXIST` - entry with the given uuid does not exist (i.e. cannot be updated). • `EDIR_UUID_IS_MISSING` - the mandatory key **uuid** is missing. • `EDIR_UUID_INVALID_FORMAT` - uuid is not in the valid format which is "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX", where X can be any hexadecimal digit. All zeroes are reserved as an empty uuid. • `EDIR_FIELD_NAME_UNKNOWN` - unknown key. The list of available keys for a particular device can be obtained using the **/api/dir/template** function. • `EDIR_FIELD_VALUE_ERROR` - a specified value does not fit the validation criteria (the value is not valid). • `EDIRLIM_PHOTO` - the limit of the photo storage has been reached. Photos cannot be added. • `EDIRLIM_FPT` - the limit of the fingerprint template storage has been reached. Fingerprint templates cannot be added. • `EINCONSISTENT` - there is an inconsistency in the values of the keys **validFrom** and **validTo** (**validFrom** has to be lower than **validTo**).

Example of Response


```
{ "success": true, "result": { "series": "6423407687606431951", "users": [ { "uuid":
"01234567-89AB-CDEF-0123-456789ABCDEF", "timestamp": 39 }, { "uuid":
"76543210-68FF-18CA-3210-FEDCBA987654", "errors": [ { "code":
"EDIR_UUID_DOES_NOT_EXIST" } ] }, { "uuid": "01234567-89A-CDEF-0123-456789ABCDEF",
"errors": [ { "code": "EDIR_UUID_INVALID_FORMAT" } ] }, { "uuid": "01234567-89AB-
CDEF-0123-456789ABCDEF", "errors": [ { "code": "EDIR_FIELD_NAME_UNKNOWN", "field":
"albert" } ] }, { "uuid": "01234567-89AB-CDEF-0123-456789ABCDEF", "errors": [ {
"code": "EDIR_FIELD_VALUE_ERROR", "field": "access.pin" } ] } ] } }
```


The first entry in the directory is updated successfully, its **uuid** and **timestamp** of the change are returned.

The second entry does not exist (no entry with such **uuid**).

The third object has a wrong format of **uuid**.

An unknown key **albert** has been passed in the fourth object.

An invalid value of PIN has been passed in the fifth object.

5.14.4 api dir delete

The **/api/dir/delete** function deletes an array of entries in the directory.

Methods

- PUT

Request

The request contains parameters in the **application/json** format.

Table 1. Request JSON Keys

Key Name	Mandatory	Expected Values	Default Value	Description
owner	Yes if users is omitted	a string	-	All entries in the directory with the specified owner are deleted
users	Yes if owner is omitted	array of JSON objects defining uuids	-	The array has to contain at least one object with the key **uuid**, which defines the entry that is to be deleted.

Example of Request

```
URL: https://192.168.1.1/api/dir/delete JSON (owner specified) { "owner": "My2N" }
JSON (uuid specified) { "users": [ { "uuid": "01234567-89AB-
CDEF-0123-456789ABCDEF" }, { "uuid": "76543210-68FF-18CA-3210-FEDCBA987654" },
{ "uuid": "76543210-68FF-18-3210-FEDCBA987654" } ] }
```

If there is no entry in the directory with the specified owner, an empty array is returned.

If there is no entry in the directory with uuid 01234567-89AB-CDEF-0123-456789ABCDEF, the device will respond with an error code (see below). Similarly for the second uuid 76543210-68FF-18CA-3210-FEDCBA987654.

If the entry with uuid 01234567-89AB-CDEF-0123-456789ABCDEF is present, it will be deleted. Similarly for the second uuid 76543210-68FF-18CA-3210-FEDCBA987654.

The third uuid has a wrong format and an error is returned.

Response

The response is in the **application/json** format. The **result** object contains the keys **series** and **users**.

Go to the topic **api/dir/query** to get more information on the use of the key **series**.

The key **users** contains an array of objects that contain keys **uuid** and **timestamp**.

- You can get better acquainted with the structure of the JSON response in the example at the end of this topic.

Table 2. Response JSON Keys in the **users** Array

Key	Typical Returned Values	Description
uuid	uuid	Unique User Identifier of a deleted or unchanged entry.
timestamp	integer	A timestamp of performed changes in the directory. Go to the topic **api/dir/query** to get more information on the use of the timestamp. The timestamp is present only when a change in the directory was successful.

Key	Typical Returned Values	Description
errors	array of error objects	An error object containing an array of all errors that occured. **errors** object is present only when a change in the directory failed. It contains an error code in the key **code** showing a reason for the failure of a change in the directory. The following error codes may be returned in a response: • `EDIR_UUID_DOES_NOT_EXIST` - entry with the given uuid does not exist (i.e. cannot be deleted). • `EDIR_UUID_INVALID_FORMAT` - uuid is not in the valid format, which is "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX", where X can be any hexadecimal digit. All zeroes are reserved as an empty uuid.

Example of Response

```
{ "success": true, "result": { "series": "6423407687606431951", "users": [ { "uuid":
"01234567-89AB-CDEF-0123-456789ABCDEF", "timestamp": 39 }, { "uuid":
"76543210-68FF-18CA-3210-FEDCBA987654", "errors": [ { "code":
"EDIR_UUID_DOES_NOT_EXIST" } ] }, { "uuid": "76543210-68FF-18-3210-FEDCBA987654",
"errors": [ { "code": "EDIR_UUID_INVALID_FORMAT" } ] } ] } }
```

The first entry in the directory is deleted successfully, its **uuid** and **timestamp** of the change are returned.

The second entry does not exist (no entry with such **uuid**).

The third object has a wrong format of **uuid**.

5.14.5 api dir get

The **/api/dir/get** function retrieves an array of entries in the directory and their specified fields.

Methods

- POST

Request
The request contains parameters in the **application/json** format. Go to the topic **api/dir/template** to get more information on various parameters of an entry in the directory and their object representation.

Table 1. Request JSON Keys

Key Name	Mandatory	Expected Values	Default Value	Description
fields	No	array of strings	all fields with non-default values	Specify the names of the required fields in the response, if the key is not specified, all fields with non-default values are returned, if an empty array is submitted, all available fields are returned. Go to the topic **api/dir/template** to get an overview of all available keys in the JSON definition of an entry in the directory. Unknown field names are ignored.
users	No	array of JSON objects defining uuids	-	The array has to contain at least one object with the key **uuid**, which defines the entry whose fields are to be returned. If the key is missing or an empty array is submitted, an empty array is returned.

Example of Request

```
URL: https://192.168.1.1/api/dir/get JSON { "fields": [ "name", "email",
"callPos.peer", "callPos[1].grouped" ], "users": [ { "uuid": "01234567-89AB-
CDEF-0123-456789ABCDEF" }, { "uuid": "76543210-68FF-18CA-3210-FEDCBA987654" },
{ "uuid": "76543210-68FF-18-3210-FEDCBA987654" } ] }
```

If there is no entry in the directory with uuid 01234567-89AB-CDEF-0123-456789ABCDEF, the device will respond with an error code (see below). Similarly for the second uuid 76543210-68FF-18CA-3210-FEDCBA987654.

If the entry with uuid 01234567-89AB-CDEF-0123-456789ABCDEF is present, its specified fields (in the example name, email, phone numbers of all calling destinations and for the second

calling destination also grouped) will be returned. Similarly for the second uuid 76543210-68FF-18CA-3210-FEDCBA987654.

The uuid 76543210-68FF-18-3210-FEDCBA987654 is in a wrong format.

Response
The response is in the **application/json** format. The **result** object contains the keys **series** and **users**.

Go to the topic **api/dir/query** to get more information on the use of the object **series**.

The key **users** contains array of objects that contain keys and values of the result of the request (see the table below).

Tip

- You can get better acquinted with the structure of the JSON response in the example at the end of this topic.

Table 2. Response JSON Keys in the **users** array

Key Name	Typical Returned Values	Description
uuid	uuid	Unique User Identifier of a found entry.
Various keys	various	Specified fields of an entry in the directory that are returned. See the **api/dir/template**.
timestamp	integer	A timestamp of the last performed changes for each returned entry in the directory. Go to the topic **api/dir/query** to get more information on the use of the timestamp. The timestamp is present only when an entry in the directory is returned.

Key Name	Typical Returned Values	Description
errors	array of error objects	An error object containing an array of all errors that occured. **errors** object is present only when a change in the directory failed. It contains an error code in the key **code** showing a reason for the failure of a change in the directory. The following error codes may be returned in a response: • `EDIR_UUID_DOES_NOT_EXIST` - entry with the given uuid does not exist (i.e. cannot be updated). • `EDIR_UUID_INVALID_FORMAT` - uuid is not in the valid format which is "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX", where X can be any hexadecimal digit. All zeroes are reserved as an empty uuid.

Example of Response


```
{ "success": true, "result": { "series": "6423407687606431951", "users": [ { "uuid":
"01234567-89AB-CDEF-0123-456789ABCDEF", "name": "ABCD", "email": "abcd@abcd.cz",
"callPos": [ { "peer": "" }, { "peer": "", "grouped": "false" }, { "peer": "" } ],
"timestamp": 39 }, { "uuid": "76543210-68FF-18CA-3210-FEDCBA987654", "errors": [ {
"code": "EDIR_UUID_DOES_NOT_EXIST" } ] }, { "uuid": "76543210-68FF-18-3210-
FEDCBA987654", "errors": [ { "code": "EDIR_UUID_INVALID_FORMAT" } ] } ] } }
```


The first entry in the directory is returned successfully, its **uuid** and **timestamp** are returned.

The second entry does not exist (no entry with such **uuid**).

The third object has a wrong format of **uuid**.

5.14.6 api dir query

The **/api/dir/query** function retrieves an array of entries in the directory defined by timestamp iterator and their specified fields.

Methods

- POST

Request

The request contains parameters in the **application/json** format. Go to the topic **api/dir/template** to get more information on various parameters of an entry in the directory and their object representation.

Table 1. Request JSON Keys

Key Name	Mandatory	Expected Values	Default Value	Description
series	No	string	current device series	The string represent a number of the timestamps series in the device. If the key is not submitted, the current device series is considered. If the specified series differs from the current device series, the device will return its series, the highest timestamp value and invalid timestamp.
fields	No	array of strings	all fields with non-default values	Specify the names of the required fields in the response, if the key is not specified, all fields with non-default values are returned, if an empty array is submitted, all available fields are returned. Go to the topic **api/dir/template** to get an overview of all available keys in the JSON definition of an entry in the directory. Unknown field names are ignored.
iterator	No	JSON object	{"timestamp": 0}	The key defines the iterator for the query (timestamp iterator is supported). The timestamp iterator has an integer value. When specified, only newer entries are returned. The last timestamp is always returned by any of **api/dir/create**, **api/dir/update** or **api/dir/delete** and can be used as "the last known" change. If the timestamp iterator value is zero, all directory entries are returned. If the timestamp iterator value is higher or equal than the current timestamp value in the device, the device will return its series and the highest timestamp value.

Example of Request

```
URL: https://192.168.1.1/api/dir/query JSON { "series": "2229480630597592840",
"fields": [ "name", "email", "callPos.peer", "callPos[1].grouped" ], "iterator":
{ "timestamp": 6 } }
```

If the series is inconsistent with the current series in the device, the device returns its current series, the maximum value of the timestamp and invalid timestamp.

If the specified timestamp is lower than the current maximum timestamp, all the higher timestamps are returned.

The device is capable of handling of up to 10000 unique user identifiers. Once the number of uuids gets higher, the device returns key **invalid**, which indicates that there is an unknown history of the directory (there were entries in the directory that were deleted and the device no longer stores them).

If the specified timestamp is lower than the invalid timestamp, the device returns its current series, the maximum value of the timestamp and invalid timestamp.

Response

The response is in the **application/json** format. The **result** object contains the keys **series** and **users**.

The key **users** contains array of objects that contain keys and values of the result of the request (see the table below).

> **Tip**
>
> - You can get better acquainted with the structure of the JSON response in the example at the end of this topic.

Table 2. Response JSON Keys in the **users** array

Key Name	Typical Returned Values	Description
uuid	uuid	Unique User Identifier of a found entry.

Key Name	Typical Returned Values	Description
Various keys	various	Specified fields of an entry in the directory that are returned. See the **api/dir/template**.
timestamp	integer	A timestamp of the last performed changes for each returned entry in the directory. The timestamp is present only when an entry in the directory is returned.

Example of Response


```
{ "success": true, "result": { "series": "2229480630597592840", "users": [ { "uuid":
"01234567-89AB-CDEF-0123-456789ABCDEF", "name": "ABCD", "email": "abcd@abcd.cz",
"callPos": [ { "peer": "" }, { "peer": "", "grouped": "false" }, { "peer": "" } ],
"timestamp": 7 }, { "uuid": "A6543210-68FF-18CA-3210-FEDCBA987654", "name": "DEFG",
"email": "defgd@defg.cz", "callPos": [ { "peer": "" }, { "peer": "", "grouped":
"false" }, { "peer": "" } ], "timestamp": 9 }, { "uuid":
"044197A7-54AD-7577-6EEA-787A6097263E", "name": "HIJK", "email": "hijk@hijk.cz",
"callPos": [ { "peer": "" }, { "peer": "", "grouped": "false" }, { "peer": "" } ],
"timestamp": 10 } ] } }
```


Three entries in the directory that have timestamp higher than 6 are returned (in this case the maximum timestamp in the directory is 10).

5.15 api mobilekey

The following subsections detail the HTTP functions available for the **api/mobilekey** service.

5.15.1 api mobilekey config

The **api/mobilekey/config** function is used for reading and writing of location IDs and encryption keys for Bluetooth Authentication.

Service and Privileges Groups

- Service group is API Access Control.
- Privileges group is Access Control.

Methods

- **GET** – read location IDs and encryption keys
- **PUT** – write location IDs or encryption keys

GET Request

There are no parameters used for **GET** request.

The response to a **GET** request is in the ***application/json*** format. The **result** object contains keys ***location, keys*** *and* ***pairingKey***.

Table 1. Response to GET Request JSON Keys

Key	Typical Returned Values	Description
location	String	***location*** is the location ID of a 2N device. The details are described in the Request section.
keys	Array of objects containing encryption keys	***keys*** contains encryption keys that are used for secure communication between a 2N device and a device used for authentication via Bluetooth. The array length is always 4 (empty objects are returned for missing keys). The objects in the array have the following keys: • ***type*** – algorithm type can be: ecc, rsa, unknown. This key is optional • ***publicKey*** – Base64 encoded DER encoded public key. This key is mandatory • ***ctime*** – creation time represented as Unix time 32 bit unsigned integer. This key is optional and is present only when the key has a known creation time.
pairingKey	Object containing encryption key or absent	***pairingKey*** is exported if pairing key data are present at the 2NOS device. It is exported at the same format as the other keys in the keys section. This key is optional.

```
{
   "success":true,
```

```
   "result":{
      "location":"54-1046-0745",
      "keys":[
         {
            "type":"rsa",
            "publicKey":"MIICXAIBAAKBgQhBqr5YI= (...)",
            "ctime":1608047754
         },
         {
            "type":"rsa",
            "publicKey":"MIICXQIBAAKBgQCfyMHsTjP (...)",
            "ctime":1608046389
         },
         {
            "type":"rsa",
            "publicKey":"MIICXQIBAAKBUNQNqodNo (...)"
         },
         {

         }
      ]
   }
}
```


PUT Request

The **PUT** request contains parameters in the ***application/json*** format.

Table 2. PUT Request JSON Keys

Key Name	Mandatory	Expected Values	Default Value	Description
location	No	String of maximum length of 127 characters	–	***location*** defines the specific device location for the purpose of Bluetooth authentication. Any string that defines the location uniquely is accepted. The location is broadcast by the 2N devices and serves for selecting relevant authentication parameters by the Bluetooth authentication device.

Key Name	Mandatory	Expected Values	Default Value	Description
key	No		–	***key*** helps upload data for the primary encryption key. The array contains encryption keys that are used for secure communication between a 2N device and a device used for authentication via Bluetooth. The objects in the array have the following keys: • ***type*** – algorithm type "ecc" ("rsa" only if the Compatible mode is active) • ***key*** – encryption key data (DER format encoded in Base64), use 1024 bit encryption keys, this key is mandatory, • ***ctime*** – creation time represented as Unix time 32 bit unsigned integer, this key is optional.
keys	No	Array of objects containing encryption keys	–	***keys*** contains encryption keys that are used for secure communication between a 2N device and a device used for authentication via Bluetooth. The objects in the array have the following keys: • ***type*** – algorithm type, RSA is currently supported, this key is optional, • ***key*** – encryption key data (DER format encoded in Base64), use 1024 bit encryption keys, this key is mandatory, • ***ctime*** – creation time represented as Unix time 32 bit unsigned integer, this key is optional.

The 2N devices allow up to four encryption keys to be used at one time. The first encryption key in the array is considered to be the primary encryption key and the other encryption keys are secondary. If a Bluetooth device authenticates itself with any secondary encryption key the 2N device will prompt the Bluetooth device to replace its encryption key with the primary encryption key. Because of this the newest encryption key should always be added to the beginning of the array.

If an array **keys** of a length shorter than 4 is submitted, the missing encryption keys are deleted (replaced with an empty object).

The key ***location*** is by default the serial number of a 2N device. Change it accordingly to add several devices to one location.

The key ***type*** is not mandatory. If the algorithm is omitted, the 2N device automatically assumes that RSA (***rsa***) is used. If the Compatibility mode is inactive, then **type** of the first item in **keys** must be ECC, the other keys can be ECC or RSA.

The key ***ctime*** is not mandatory. If the creation time is omitted or invalid, the 2N device will display Jan 1st 1970 00:00:00 in the configuration web and will not return ***ctime*** for this encryption key.

Response

Example of PUT Request – upload of 2 encryption keys

```
URL: https://192.168.1.1/api/mobilekey/config
{
   "location":"LocationUniqueID",
   "keys":[
      {
         "type":"rsa",              // compatibility mode is active (rsa supported)
         "key":"MIICXAIBAqr5YI (...)",
         "ctime":1608047606
      },
      {
         "type":"rsa",
         "key":"MIICXQInJSGse (...)",
         "ctime":1608044538
      }
   ]
}
```

Example of PUT Request – upload of primary encryption key

```
URL: https://192.168.1.1/api/mobilekey/config
{
  "location": "00-0001-0014",
  "key": {
    "key": "MIIQInJSdfsed...",
    "type": "ecc",
    "ctime": 1733159857
  }
}
```

The response to a **PUT** request does not contain any details. E.g., if there is an invalid encryption key value, the key will not be written without any notification.

5.15.2 api mobilekey compatibility

The **api/mobilekey/compatibility** function is used for reading and writing of location IDs and encryption keys for Bluetooth Authentication (WaveKey).

Service and Privileges Groups

- Service group is API Access Control.
- Privileges group is Access Control (Control).

Methods

- **GET** – returns the WaveKey compatibility mode activation state
- **PUT** – sets the WaveKey compatibility mode activation

GET request

There are no parameters used for **GET** request.

GET /api/mobilekey/compatibility
Example of Response to GET Request:
{ "success": true, "result": { "compatibilityMode": false } }

PUT request

The **PUT** request contains parameters in the ***application/json*** format.

Table1. PUT Request JSON Keys

Key Name	Mandatory	Expected Values	Description
compatibilityMode	Yes	`true / false`	**Compatibility Mode** ensures the WaveKey function for those users who cannot update to My2N 3.5.0 (Android) or 3.7.0 (iOS) and higher. Once the Compatibility mode is deactivated, the primary key has to be generated again.

Example of PUT Request:

```
PUT /api/mobilekey/compatibility
Content-Type: application/json

{
  "compatibilityMode": false
}
```

Example of Response to PUT Request:

```
{
  "success" : true
}
```

5.16 api lpr

The following subsections detail the HTTP functions available for the **api/lpr** service.

- 5.16.1 api lpr licenseplate
- 5.16.2 api lpr image

5.16.1 api lpr licenseplate

The **api/lpr/licenseplate** function is used for access control by license plate recognition.

Service and Privileges Groups

- Service group is API Access Control.
- Privileges group is Access Control.

Methods

- POST

Request

The request contains parameters in the **application/json** format.

Table 1. Request JSON Keys

Key Name	Mandatory	Expected Values	Default Value	Description
lprUuid	Yes	uuid string	–	Uuid of the licence plate recognition event generated by the License Plate Recognition system.
lprID	Yes	ID number	–	Internally unique identifier designating one license plate in one recorded car arrival. One and the same license plate can be recognized multiple times within one arrival. In case the camera obtains more details from another recognition, the plateText will be specified while the lprID will remain the same. Each recognition event generates a lprUuid of its own.
accessPoint	Yes	0 or 1	-	Indicates whether a vehicle with the detected license plate is entering (0) or exiting (1) – this is important for Access Rules that are applied to the event in the 2N device.
plateText	Yes	license plate string (range of 1–12 characters)	–	Text of the recognized license plate that is used to identify a user in the 2N device directory.

Key Name	Mandatory	Expected Values	Default Value	Description
lprDir	No	0 to 3	–	Defines the detected car/license plate motion direction according to the camera direction setting. Options: • 0 = unknown • 1 = Undefined (In or Out) • 2 = in • 3 = out
plateImage	No	image encoded in base64	No image	The image in which the license plate was recognized. The size of the image data is limited to 256 kB.

Example of Request

```
URL:
https://192.168.1.1/api/lpr/licenseplate

JSON:
{
    "lprUuid": "bc4baad9-d2cd-4706-986f-b942963bfa9f",
    "lprID": 143289,
    "accessPoint": 0,
    "plateText": "ABC123456",
    "plateImage": "/9j/4AAQSkZJRgABAQEASABIAAD//gATQ3JlYXRlZCB3aXRoIEdJTVD/
4gKwSUNDX1BST0ZJTEUAAQEAAAKgbGNtcwQwAABtbnRyUkdCIFhZWiAH5AAMABIACgAHAA5hY3NwTVNGVAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA9tYAAQAAAADTLWxjbXMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA1kZXNjAAABIAAAAEBjcHJ0AAABYAAAADZ3dHB0AAABmAAAABRja
GFkAAABrAAAACxyWFlaAAAB2AAAABRiWFlaAAAB7AAAABRnWFlaAAACAAAAABRyVFJDAAACFAAAACBnVFJD
AAACFAAAACBiVFJDAAACFAAAACBjaHJtAAACNAAAACRkbW5kAAACWAAAACRkbWRkAAACfAAAACRtbHVjAAA
AAAAAAAEAAAAMZW5VUwAAACQAAAAcAEcASQBNAFAAIABiAHUAaQBsAHQALQBpAG4AIABzAFIARwBCbWx1Yw
AAAAAAAAABAAAADGVuVVMAAAAaAAAAHABQAHUAYgBsAGkAYwAgAEQAbwBtAGEAaQBuAABYWVogAAAAAAAA9
tYAAQAAAADTLXNmMzIAAAAAAAEMQgAABd7///MlAAAHkwAA/ZD///uh///
9ogAAA9wAAMBuWFlaIAAAAAAAAG+gAAA49QAAA5BYWVogAAAAAAAAJJ8AAA+EAAC2xFhZWiAAAAAAAABilw
AAt4cAABjZcGFyYQAAAAAAwAAAAJmZgAA8qcAAA1ZAAAT0AAACltjaHJtAAAAAAADAAAAAKPXAABUfAAAT
M0AAJmaAAAmZwAAD1xtbHVjAAAAAAAAAAEAAAAMZW5VUwAAAAgAAAAcAEcASQBNAFBtbHVjAAAAAAAAAAEA
AAAMZW5VUwAAAAgAAAAcAHMAUgBHAEL/
2wBDAAMCAgMCAgMDAwMEAwMEBQgFBQQEBQoHBwYIDAoMDAsKCwsNDhIQDQ4RDgsLEBYQERMUFRUVDA8XGBY
UGBIUFRT/
2wBDAQMEBAUEBQkFBQkUDQsNFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UFBQUFBT/wgARCABMAIADAREAAhEBAxEB/8QAGwAAAgMBAQEAAAAAAAAAAAAAAAcFBggDBAL/
xAAaAQACAwEBAAAAAAAAAAAAAAAABQMEBgIB/
9oADAMBAAIQAxAAAAHUx4kXairWqwAAAAAAAAAFlrWHgkcKhqtzRps56eO5KPsAD5CGnh689S0Unk75j5I
```

```
/rz2Wilh5odHZvQxU0KGfJNf4/WS0Unk65An4Js6aJDfaF5qKmPP3zGezycd3xsbH6vFe1x7yRO+/
ghnyS207dds1/
J3x35707l9HUrlS+0LufdAk0VnXyfbqlkzXbFx+rxXtce8kTvv4IZ8kutG601bK60bluqWoCxBmnS55/
IHeetAjbalp8niGfJdi4/
V4r2uPeSJ338EM+SbLxmup1yosGi6j3acZNCBrTJajPWgR3Cpaa6lplnU5rYmP1eK9rj3kid9/
BDPkm0MXr1g0XVW1VAAqVurorOvs9aBH9nut8lp1C3VsddfxbtMg8kTv2cdIHQImqpa3ijcAAAWzJdZK1lZ
M10NPA7Ujmdrzr5hQWjRa9kLtsKWmRddlouaEAAAAAAAAAACRil1vktRa6tnh75FSxgAAAAAAAAASkUno8
9/8QAKhAAAQMDAwIGAgMAAAAAAAAABQADBAIGBwEVFzE2EhMWMzQ1EBEUMDL/
2gAIAQEAAQUCrr0bpL5Kpad5KKLkoouSii5KKLkoouSii5KKLkoouSii5KKLkoouSiiE5L8bjblLzeSCVUU
WmY7smvZCK2QitjIqoMQbpTbdb1eyEVIgSomi001q1rDz2qFjUlXIg5S6q0ILMIBKPDoT3qkSvVIlRpTM1n
IwtmEQx2MaYDVOU06vx25TJ4btBeD824Poli738pdVHusrFYlSnZshNMuP1Y/
GyRwnKP8Aqw+17vrqruSy5tU63MlRvKNQfnXB9EsXe/
lLqgNpzT+kTGMalRLMDxE2y1GomXMLgK67h9QkLD7Xu7uTGMnxQMnRvFBgfOuD6JYu9/
KXVWw1Szb1w37SGnTMglpKlk5c782H2vd3cmNJPlmL4jfybaH/AD7g+iWLvfyl1Vua/
sBc1jTSpjjYquNiq42Ko7bkq3tbD7Xu7uS0JWkO45UaiZGiY1ajTbiq0pArF3v5Rbq1bVtX04FjcnQ1ydDX
J0NcnQ1d9ys3HVbt9Rgog1PpKFdNf1qLyVWyxydDVy3s+dZWLqNfMuELQeGERkkVI/
sgj5BORbQOkAMTzDcijYhq2IatiGrYhq2IatiGrYhq2IatiGrYhq2IatiGpmO1GpX/
xAAsEQABAwAJAgcBAQEAAAAAAAABAAIDBAUQERMVM1FSEkIhMTJBcYGRIhQw/9oACAEDAQE/
AVLWAaboxeswl2CzCXYLMJdgswl2CzCXYLMJdgswl2CzCXYLMJdgswl2CzCXYLMJdgswl2CzCXYLMJdgoqwBN0gQN6p8nTH0j
3sa1zvSFgy8T+LBl4n8WDLxP4sGTifywAu8AsGXifOje3xcLPNYUg82myr5C5hYfZVl22UZgZE25OljYbn
OX+iLkF/
oi5BBwcLwqwjDXBw91QWBsXVvYQCLip48KQtUWo1TaTviyre76VZdtgpUzRcHJ7y89TrA0u9IVCjdHH/
SrLtVD0Gqma7lRXl8LSVWLbpA5Retqm0nfFlW930qy7bIKK+fx9k2rmD1FNosLe1eSfPGz1OVKnx3eHkFQ9
Bqpeu5Vc69haqxb/AcotRqm0nfFlW930qy7bKOLom/Cnpohd0AJ9Pld5eCdK9/
qNtD0Gql67lVzv7LVS29ULlFqNU2k74sq3u+lWXbZBpN+FSKG+WTraVl8u4WXy7hZfLuFNR3QXdXuqHoNVL
13KiO6ZmpwDhcUygNa/
qvU+k74sq3u+lWI8Gmyj03Cb0OHgsxj2KzGPYrMY9isxj2KpdIbPd0+ygprIowwhTyCWQvC8lHWFwukCzGP
YqkUwzDpb4CyrR6ipohMzpKkidEbnD/rHG6U3NCghELOmwi/
zWFHxWFHxWFHxWFHxWFHxWFHxWFHxWFHxWFHxWFHxWFHxWFHxQAHlZ//
xAAvEQABAwEFBgYDAQEBAAAAAAABAAIDBAUQERVREhMxUoGRITIzQUJxFDTwIiMw/9oACAECAQE/
AeKhs0uGMhwWWxalZbFqVlsWpWpWpWpWpWpWpWpWpWxalZbFqVlsWpWpUtm4DGIojDwMkLjDTwIiojx/
kLj7XOc7ZHoxK38XMO6bIojDwMkLjDTwIiojx/
lON4mjPgHC60ow14ePdWX8+l1W8vmdimwSvGLWr8abkK/
Gm5CnNLDg4KzHPYWn2VoSF0ux7C4EtOIVPJvog9Qqn9Vn2LrU4M6qy/
n0udSQuO0WpjAwbLeFxcG4EtOUnkNCqBSN3PYR1E/
AG5ql8jlT+qz7F1qcGdVZfz6XVb9mzEhoxK38XMO6bIojDwMkLjDTwIiojx/
n0uqPWf9mzEhoxK38XMO6bIojDwMkLjDTwIiojx/
n0uqPWf9mzEhoxK38XMO6bIojDwMkLjDTwIiojx/
1D5AqeRwmf8AaP2LrU4M6qy/n0udSQuO0WpjAwbLeFxcG4EtOUnkNCqBSN3PYR1E/
Vd5F9kYqV1C3xipXULfGKldQt8YqV1C3xipXULfGKldQt8YqV1C3xipXULfGKld/
5L1lls3S0ANY5hNbEoyfNbEoyfNbEoUikZkRTOrJXkBsVM15BFKrHMJrYlFX5Z1lNLgKN6iYVWCM5KZERSq
krRUS9MShrXgFRQ8y5oub8T7b0orYIhOgjhlnVVhWn5xppxOUVLCkZQY1oygxrQjrDgvNryEC1SGJhoUDwh
FtImlM/
zhJyyivvkvG0Ii0pFFJEXyrBNOgjjZJRRLPEzKp4oFxfNypEv0g9sXR9Xc7q3roeiH1i5vxPtvAy1OEDYJZ
EaJgSDffPhHTwkS571loCcLQKVh1JlsmlcctCBctKRc34n2xKe/
wB5YnrSqtDpEqRlaMagqr5Fhp7M6180X+Il+kHti6Pq7ndW9dD0Q+sXN+J9t5XGrLTCLThXPpH4mccc8jY2
d8YJMXF0u8btijYA0Cf2pRIXhZ1q0n5QW0vyhHAFQYbSy2i8vniU9/vL0kTkvXCDiH1p0ScxnBxQ60/
aJfpB7Yuj6u53VvXQ9EPrFzfifbeVxqy0wi04Vz6R+JnHHPI2Nnfv/
eWJ/pIfZzONV9qL/
```

```
MTVOUKH1LEt0g9sXR9Xc7q3roeiH1i5vxPtvXO6AOyHpuXdZsO0wOKqKmCmiMZLa67oxktrrujGS2uu6GUm
SbLha04Na8n8xKe/wB5Yn+kiSNVoKlYX2pSHWHEq24KgXmht4p0jbA7Vjg6KvtrF0VX/
HPsvXQ9EPrFznPyopp2brySr7PhDA+KqLQhjmj/AFpHNH+tI5o/8o5o/
wDKJVWmja4K1W35aboZlHJd1wgrxhpTCtYmZoBUBdKqIsVTAsC3Oy/
DEKU4UFoq+yOZv9aR4O234PLVwpWqleugdOLQEr1w5LEtk/
GA9BQrMy0rZpp5F839VGZZonXF0ZoFitp1eM4Wlb1l1sXB0GlYyfK7EYyfK7EYyfK7EYyfK7EYyfK7EYyfK
7EYyfK7EYyfK7EYyfK7EYyfK7EYyfK7EYyfK7EYsstg0OgBpe//
xAAnEAABAgQGAgMBAQAAAAAAAAABABEhMVHwEEFhkaHBcYEwsdHxIP/
aAAgBAQABPyEF8SSYAVUJJrxHiCLex8tGjRo0aNGjRo0aIIaYXG8jct4PpDxGOuAMiET+TgzZJG5wZ6pfHs
FdHSvLpWt0o4OCEA4whgccD0r66QSZ4AEO4wGQEhgBMowFgWAJklsDHBKjk/
8AYHfE7RpIQR4nhSl9t7BjlOePtBGNBY7AmHJmyiQAmIsgNiUDFaQYTW6yOATjiYsax9BCvFGKiwVxnBJuB
DJCSOgIzAsNd38tgmOSZYGA5GUkcLNkctOUapzIMGCJOHLHMQDhkUEIWOoB4S4UYqLBXGcJDkELE5gM0ykn
RDykRr9PGDhUnQAJDa4cXctJA9sy1PQXLTstAhnJGaNKNqmHR5bdRiosFcZxBiENUHclVCZPwgDEmeicwc6
x3ciZL6XYG0seWnZaBGJz/oG4KHanb/Q/DqxUYqLBXGcRQLwuKjphJoAMhPL/
ABPnyykoTf5Du4FC5adtoE+bs3mDkhMRjAqDFBs+FpgXAP4IjDBncxhYKqEAjs6l4+2BDxRhYpGYV89q+e1
/e/a/v/
tNk6DgjQZDHTeRx3N5WcELYgiCIQFwRkj64Qfkln7Vw9ogf7pdyc00wiU3AoAjzoSpH7HtEfZBkGpZj5cue
gw1E5BNjGt5FpoJYFxnyobFX90r+6V/dK/ulf3Sv7pX90r+6V/dK/ulf3Sv7pafpg7DD//
aAAwDAQACAAMAAAAQ5222222dFT9dTNQqNhSVn9+sNdo2ZCesNp6Jf3+sNzOtfOesNwSWfGJsVSW3WR3rWt
ttttt9iSSSSSSU/8QAJxEAAQIEBAcBAQAAAAAAAAAAAQARMWGx0RAhkfFBUXGBocHw4TD/
2gAIAQMBAT8QJADlGnWDD98LaDdbQbraDdbQbraDdbQbraDdbQbraDdbQboKYTENEAARBGGTMvHH
1gVYhMg63pZbkst6WTMdZbA4y5ktyWQFyBMEYAEmEURCQAJG2HRQdCoO/
1g1WIBPUhMiAzK3YLdgntuJIHzFz9muhwRm7wWTgI6A4KEHgIdDmvIFV5qmEX1xUHf6wGWwGQyFkTkcnA2x
CZB0agWJLt2C9vpVlSiJcMGoFGShpkicCIof1eUKrzVMIvrioO/
1gGblzH1zUYz0yuoeB651QABgGTmwCOHHSKGEyl1WVKpKBZjZg1H4UA8cC2o/F5AqvNUwi+uKg7/
WAAxyURK5I7CDzWRN6BdP7575aQxrKlUlAmOeD6H9Rhhwz0LryBVeaphF9cVB3+sPDURwFnzfk3IrfDZb4b
LfDZZ2g5oS7DmqypVJQJ/
EsDlqLsiuEckFOkAuze0TFmphF9cUc8OCRq1sCAdBA8V8wuvmF18wuvmF1ksRmjNrIzIkPBuZPNAEYGyBJO
E2OSOI49l8wum5VDgSVl7R12jyKyvqHp/
XNuP0UJjmYkzwADA6lNApTQKU0ClNApTQKU0ClNApTQKU0ClNApTQKU0CAsDYf/
8QAJxEAAQICCgMBAQAAAAAAAAAAAQAR0fEQITFBUWFxobHwgZHB4TD/
2gAIAQIBAT8QAJMEAaYLfc1PBBTwQU8EFPBBTwQU8EFPBBTwQU8EFPBBTwQU8EEcjnIxRDIGIQyrO5s+0BW
AGZZSZFSZFSZFAxYepGh8LDNSZFFGCWRBoJADlEgSJzEaNcZqJrs80P1sJA0CeEIxZSxSxFhgOBRR3qNoXq
2R6ZsKtQ7oAmwIaOxCdK0ivUVFbc8LqMRR0NF2eaCd0TWazFA4mCgWyAzqQ0SdgxPkqz0vXE4IQbF31BQYG
v2HQ7wB5E1tzwuoxFHQ0XZ5oO22AfcFYkNa4K2CGlXCIOTlMTjG+weynQj1hguJwW3+lFxUN6P6jjGh/R/
VsjwuoxFHQ0XZ5oMccWxZATUHJza2SrcTqMGViY0H2nicFs/
pWSx5H4hnG9x7EVsjwuoxFHQ0XZ5o3jlH7O6xsXxClgipYIqWCKqkIqW5+TguJwWz+lHAAcgP6L8K2JBceE
BAAkM7/
P1A7GDmjoaIIvZY+njQUOi3ArvGC7xgusYLrGCCsDUsyeKGnALWvcAEQxyEQCGKCdmDcbvK7xgviQigDXlf
xBdYLxiEJuBuNf6lrAdsREdQsAyoKubFTJFTJFTJFTJFTJFTJFTJFTJFTJFTJFTJFTJFTJFTJFHnSTnR//
xAAkEAEAAQMEAgIDAQAAAAAAAABEQAhMRBBUYFhoSBxMJHxsf/
aAAgBAQABPxAvDyhiVLYAvNJ7hnAN3C8mTj8vnz58+fKctkm85Z5Cj5UduBYqUGRhsipogkzZlc
gm+lqVYS8wHt3uUyDBXqiuwBWht3UyOOBKXQF7B5SAnGxQxORKQBCKrY0YHfM5keB1fQ0DBP
gQxORiQcAULChPSAnBIjfZK/jq/
n6kgwAoGEk3GyUe9dkpQGETcssrR6KISwQ2FZyt8EYTYon6GmuNqg7/
VgRJ1+1XuoKZAASIIAMzlNHPYwFDwu+yKFxWCL4bDo+C72tSoAM8q0Rkd69iV/
et3wGJPPQ0AVC+OQH2VALyIviwDfMmYi0/
BQbv25MCRwi2InfRd7GqYDYMDAnx6VM6aFCqgdmHNEQRAApKMhKCTEULN5LyMdqGrxgLwXMnZ+nROGk4Sra
SZUFElukB8DBh4kHcnG3o3HEs80g20tA0SmwTqpYMLE4EMW2o/
4k4UYR2aHLyzhYSR5IJ4NEgtSnXdIiACDAyErpZAE8WZKDr/AEqKgE4iMnhFI2W9LL4JIH1fMdw/
lYQIX4dIuVCg674kgSWwA+pyumSPjX0J+UGDBgwYMDBgwYMiFYNegNP/9k=
}
```

Response

The response is in the **application/json** format.

Table 2. Response JSON Keys

Key	Typical Returned Values	Description
success	`true`, `false`	The value is `true` when the request is processed successfully. When there is an error, the value is `false` and additional information is available in the `error` key.

Example of Response

```
{
    "success": true
}
```

There may occur various errors (e.g. missing mandatory parameter). When Error code 13 (parameter data are too big) is returned, the request was not processed and it is necessary to send the request again with a smaller image or without an image.

Subsequently received duplicate valid requests are ignored (the last ten successful requests are held in the memory). It is possible to attempt at resending a request when there is no reply from a 2N device without the risk of a duplicate barrier opening or duplicate event logging.

5.16.2 api lpr image

The **api/lpr/image** function is used for getting images received from the license plate recognition.

Service and Privileges Groups

- Service group is API Access Control.
- Privileges group is Access Control.

Methods

- GET
- POST

Request

The request contains parameters in the URL.

Table 1. Request Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
plateText	Yes	String with license plate text	-	Text of a recognized license plate that is used to identify which image should be returned (up to five images are stored). If two or more images belong to the same license plate text, the newest one is returned.

Example of Request

```
URL: https://192.168.1.1/api/lpr/image?plateText=ABC123456
```

Response

The success response is in the **image/jpeg** format.

There may occur various errors (e.g. missing a mandatory parameter). Errors are returned in json with a response code 200. If there is no image associated to the submitted plate text, error 15 "no data available" is returned.

5.17 api accesspoint blocking

The following subsections detail the HTTP functions available for the **api/accesspoint/blocking** service.

5.17.1 api accesspoint blocking ctrl

The **api/accesspoint/blocking/ctrl** function controls blocking of access on individual access points.

Service and Privileges Groups

- Service group is API Access Control.
- Privileges group is Access Control.

Methods

- POST

Request

The request contains parameters in the URL.

Table 1. Request URL Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
id	Yes	Integer (0, 1)	-	Specifies the identifier of the access point that is to be controlled (0 for Entry and 1 for Exit).
action	Yes	String (on, off)	-	Specifies whether the blocking for the corresponding access point should be switched on or switched off.

Example of Request

```
URL:
https://192.168.1.1/api/accesspoint/blocking/ctrl?id=0&action=on
```

Response
The response is in the **application/json** format.

Table 2. Response JSON Keys.

Key	Typical Returned Values	Description
success	`true`, `false`	The value is `true` when the request is processed successfully (i.e. the access blocking is in the desired state regardless of a change).

Example of a Response

```
{
    "success": true
}
```

There may occur various errors (e.g. missing mandatory parameter). When Error code 18 (access point disabled) is returned, the request was not processed because the specified access point was disabled at the time.

5.17.2 api accesspoint blocking status

The **api/accesspoint/blocking/status** function returns the status of access blocking for individual access points.

Service and Privileges Groups
- Service group is API Access Control.
- Privileges group is Access Control.

Methods
- GET

- POST

Request
The request contains parameters in the URL.

Table 1. Request URL Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
id	No	Integer (0, 1)	All	Specifies for which access point the status should be returned. If this parameter is omitted, the access blocking status is returned for all the access points.

Example of Request

```
URL: https://192.168.1.1/api/accesspoint/blocking/status?id=0
```

Response

The response is in the **application/json** format. The value of the `result` key contains one key `accessPoints`, which contains an array with an object for each access point (the array has a length of 1 if an access point was specified in the request). The objects in the array contain the following keys.

Table 2. Response JSON Keys

Key	Typical Returned Values	Description
id	Integer (0, 1)	Identifies the access point (0 for Entry, 1 for Exit).
blocked	Boolean (`true`, `false`)	Contains the current status of access point blocking (`true` when the access point is blocked, `false` when the access point is not blocked).

Example of Response


```
{ "success": true, "result": { "accessPoints": [ { "id": 0, "blocked": true }, { "id":
 1, "blocked": false } ] } }
```


There may occur various errors (e.g. insufficient privileges).

5.17.3 api accesspoint grantaccess

The **api/accesspoint/grantaccess** function helps grant remote access permission to a user (employee/user or user assigned to a general group. e.g. visitor). The remote access permission can also be granted via a specific account that clearly identifies the access granting user.

Service and Privileges Groups

- Service group is API Access Control.
- Privileges group is Access Control.

Methods

- GET
- POST

Request

The request contains parameters in the URL format.

Table 1. URL Request Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
id	Yes	Integer (0, 1)	–	Identifies the access point to be checked (0 for Arrival and 1 for Departure).
user	Yes	uuid	–	Identifies the user that initiates door opening (and whose access settings are to be considered).

Response

The response is in the **application/json** format.

Table 2. JSON Response Keys

Key	Typical Returned Values	Description
success	`true`, `false`	The value is `true` if the request has been processed successfully (i.e. access blocking is in the requested state regardless of the change).
reason	`invalidAp`, `invalidCredential`, `accessBlocked`	The key is displayed in case the response is accessGranted:false. If the access is successful the key is not displayed.

Example of Response

```
{
  "success" : true,
  "result" : {
    "accessGranted" : false,
    "reason" : "invalidAp"
  }
}
```

There may occur various errors (e.g. missing mandatory parameter). Error code 18 (access point disallowed) means that the request has not been processed because the access point was not allowed at the time of processing.

5.18 api lift

The following subsections detail the HTTP functions available for the **api/lift** service.

- 5.18.1 api lift grantaccess

5.18.1 api lift grantaccess

The api/lift/grantaccess function is used for enabling lift floors based on authorization in another device.

Service and Privileges Groups

- Service group is API Access Control.
- Privileges group is Access Control (Control).

Methods

- GET
- POST

Request

The request contains parameters in the URL (or in the application/x-www-form-urlencoded format when POST is used).

Table 1. Request JSON Keys

Key Name	Mandatory	Expected Values	Default Values	Description
uuid	Yes	uuid	-	Uuid of a user which is to be granted access to their floors (according to the Access Rights configuration).
duration	NO	1 .. 600	duration configured in the target device	Defines the floor activation time. The default duration configured in the ***Switch-On Duration*** parameter is used if the duration parameter is omitted.

Example of Request

```
URL:
https://192.168.1.1/api/lift/grantaccess?user=09ebfd7d-24e4-4d58-ad02-804ad69938a6&duration=180
```

Response

The response is in the **application/json** format.

Table 2. Response JSON Keys

Key	Typical Returned Values	Description
success	`true, false`	The value is `true` when the request is processed successfully. If there is an error, the value is `false` and additional information is available in the `error` key.

Example of Response

```
{
    "success": true
}
```

There may occur various errors (e.g. missing mandatory parameter). When Error code 12, param: user (User not found), is returned, the request was not processed because there is no such uuid in the target device directory. If the submitted uuid is missing or has a wrong format, the device will reply with error code 11 (missing mandatory parameter) or error code 12 (invalid parameter value) respectively.

When floors are activated while being active, the longer duration will be applied (remaining time vs new request duration).

This API endpoint can be used for lift floor control in parallel with the standard Access Control from another device (e.g. send the lift floor activating request from an intercom to the Access Unit that is in the lift and interfaces directly with the relay boards).

5.19 api automation

The following subsections detail the HTTP functions available for the **api/automation** service.

5.19.1 api automation trigger

Service and Privileges Groups

- The service group is *Automation API*.
- The privileges group is *Access to Automation*.

Methods

- GET
- POST

Request
The request contains parameters in the URL.

Table 1. Request URL Parameters

Parameter Name	Mandatory	Expected Values	Default Value	Description
triggerId	Yes	String (user defined in the Automation	-	Identifies which HttpTrigger block will activate

Example of Request

```
URL:
https://192.168.1.1/api/automation/trigger?triggerId=triggerName
```

Response
The response is in the application/json format.

Table 2. Response JSON Keys.

Key	Typical Returned Values	Description
success	true, false	The value is true when the request is processed successfully (i.e. the access blocking is in the desired state regardless of a change).

Example of a Response

```
{
    "success": true
}
```

There may occur various errors (e.g. missing mandatory parameter). When the specified trigger ID is not found (i.e., there is no block with such Name), an error code 12 is returned with Description "HttpTrigger not found.".

5.20 api cert

The following subsections detail the HTTP functions available for the **api/cert** service.

5.20.1 api cert ca

The **/api/cert/ca** function helps you administer the CA certificates.

The function is part of the **System API** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET**, **PUT** or **DELETE** method can be used for this function. The GET method returns information about one or more CA certificates on the device. The **PUT** method uploads the given CA certificates to the device. The **DELETE** method deletes a single CA certificate from the device.

GET method

Request parameters for **GET**:

Parameter	Description
id	An optional *string* value identifying a CA certificate. The **id** value is user defined id, internal id or certificate fingerprint (hash). If **id** is not completed, the reply includes a long list of all user certificates in the device.

The reply is in the **application/json** format and can include the following parameters:

Parameter	Description
fingerprint	A *fingerprint* (hash) of the certificate.
subjet, issuer	A *dictionary* which splits information for the Subject or the Issuer: Common Name (CN), Organization (O), Organization Unit (OU), Location (L), State (S), Country (C).
id	A *string* value of the previously specified certificate identification.
startDate	A *date* identifying when this certificate started to be valid.
endDate	A *date* identifying when this certificate will cease to be valid.
protected	A *boolean* value indicating whether the certificate is protected and therefore cannot be deleted from the device. Internal certificates with **id** starting with "#" are protected and cannot be deleted.

Parameter	Description
systemUseOnly	A *boolean* value indicating whether the certificate should be selectable by the user as a certificate for any service. If it is `true`, the certificate is not shown in the selection list.

Example 1: List of all the certificates in the device

```
GET /api/cert/ca                                    //request
{                                                   //response
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint" : "4deea7060d80babf1643b4e0f0104c82995075b7",
        "subject" : {
          "CN" : "Thawte RSA CA 2018",
          "O" : "DigiCert Inc",
          "OU" : "www.digicert.com",
          "C" : "US"
        },
        "issuer" : {
          "CN" : "DigiCert Global Root CA",
          "O" : "DigiCert Inc",
          "OU" : "www.digicert.com",
          "C" : "US"
        },
        "startDate" : "2017-11-06T12:23:52Z",
        "endDate" : "2027-11-06T12:23:52Z",
        "allowRemove" : true
      },
      {
        "fingerprint" : "a8985d3a65e5e5c4b2d7d66d40c6dd2fb19c5436",
        "subject" : {
          "CN" : "DigiCert Global Root CA",
          "O" : "DigiCert Inc",
          "OU" : "www.digicert.com",
          "C" : "US"
        },
        "issuer" : {
          "CN" : "DigiCert Global Root CA",
          "O" : "DigiCert Inc",
          "OU" : "www.digicert.com",
          "C" : "US"
        },
        "startDate" : "2006-11-10T00:00:00Z",
```

```
        "endDate" : "2031-11-10T00:00:00Z",
        "protected" : false,
        "id" : "#my2n-utility",
        "systemUseOnly" : true
      }
    ]
  }
}
```

Example 2: Get one certificate identified by **id**

```
GET /api/cert/ca?id=#my2n-utility          //request
{                                          //response
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint" : "a8985d3a65e5e5c5b2d7d66d40c6dd2fb19c5436",
        ...
        "id" : "#my2n-utility",
        ...
      }
    ]
  }
}
```

PUT method

If one and the same certificate is already on the device, it is overwritten. It is possible to upload multiple certificates in one PEM formatted file. It can contain any blocks, only certificates are processed. If any of the included certificates fails to load, none are saved and the error code is returned.

Request parameters for **PUT**:

Parameter	Description
blob-cert	A mandatory *blob-cert* contains the certificate in the DER or PEM format.

Parameter	Description
id	An optional *string* of a unique user defined identification of a certificate. The user defined id starts with the '@' character. It must consist of 1-40 characters of the following set: `[a-z][A-Z][0-9]`, _ and -. If a new certificate with the same **id** is uploaded, the original certificate is overwritten. The **id** must not be specified when uploading multiple certificates in one file.

The reply is in the **application/json** format and includes:

Parameter	Description
fingerprint	A *fingerprint* (hash) of a certificate.
replaced	A *fingerprint* of a replaced certificate.

Example

```
PUT /api/cert/ca                                  //request
{                                                 // response
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint": "9623fa25e414aa930ed22348a22d04a4c4fda26b"
      },
      {
        "fingerprint": "9623fa25e414aa930ed22348a22d04a4c4fda26b"
        "replaced": "9623fa25e414aa930ed22348a22d04a4c4fda26c"
      }
    ]
  }
}
----
{                                                 //response
  "success" : false,
  "error" : {
    "code" : 12,
    "param" : "blob-cert",
    "description" : "invalid certificate",
    "data" : "invalid_cert"
  }
}
```

DELETE method

Request parameters for **DELETE**:

Parameter	Description
id	A mandatory *string* value identifying a CA certificate. The **id** value is user defined id, internal id or certificate fingerprint (hash). Internal certificates with **id** starting with "#" are protected and cannot be deleted.

The reply is in the **application/json** format.

Example:

```
DELETE /api/cert/ca?
fingerprint=a163b11215a30f08603fd85c314327e275772b00                    //request
{
  "success" : true
/response
}
-----
{
//response
  "success" : false,
  "error" : {
    "code" : 12,
    "param" : "id",
    "description" : "certificate not found",
    "data": "cert_not_found"
  }
}
```

5.20.2 api cert user

Funkce **/api/cert/user** function helps you administer the user certificates.

The function is part of the **System API** service and the user must be assigned the **System Control** privilege for authentication if required.

The **GET**, **PUT** or **DELETE** method can be used for this function. The GET method returns information about one or more user certificates on the device. The **PUT** method uploads the given user certificate to the device. The **DELETE** method deletes a single user certificate from the device.

GET method

Request parameters for **GET**:

Parameter	Description
id	An optional *string* value identifying an user certificate. The **id** value is user defined id, internal id or certificate fingerprint (hash). If **id** is not completed, the reply includes a long list of all user certificates in the device.

The reply is in the **application/json** format and can include the following parameters:

Parameter	Description
fingerprint	A *fingerprint* (hash) of the certificate.
subjet, issuer	A *dictionary* which splits information for the Subject or the Issuer: Common Name (CN), Organization (O), Organization Unit (OU), Location (L), State (S), Country (C).
id	A *string* value of the previously specified certificate identification.
startDate	A *date* identifying when this certificate started to be valid.
endDate	A *date* identifying when this certificate will cease to be valid.
protected	A *boolean* value indicating whether the certificate is protected and therefore cannot be deleted from the device. Internal certificates with **id** starting with "#" are protected and cannot be deleted.
systemUseOnly	A *boolean* value indicating whether the certificate should be selectable by the user as a certificate for any service. If it is `true`, the certificate is not shown in the selection list.

Example: Get information of one certificate identified by **id** (fingerprint)

```
GET /api/cert/user?id=a164b11215a30f08603fd85c314327e274772b00  //request
{                                                               //response
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint" : "a164b11215a30f08603fd85c314327e274772b00",
        "subject" : {
```

```
          "CN" : "00-0001-0205",
          "O" : "2N TELEKOMUNIKACE a.s.",
          "S" : "Czech Republic",
          "C" : "CZ"
        },
        "issuer" : {
          "CN" : "My2N Device Utility Certificate Authority",
          "O" : "2N TELEKOMUNIKACE a.s.",
          "S" : "Czech Republic",
          "C" : "CZ"
        },
        "startDate" : "2021-11-08T07:50:36Z",
        "endDate" : "2022-02-06T07:50:36Z",
        "protected" : false,
        "id" : "#my2n-utility",
        "systemUseOnly" : true
      }
    ]
  }
}
```


PUT method

If the same certificate is already on the device, it is overwritten.

Request parameters for **PUT**:

Parameter	Description
blob-cert	A mandatory *blob-cert* contains the certificate in DER or PEM format.
blob-pk	A mandatory *blob-pk* contains the private key in DER or PEM format.
password	An optional *password* contains the password for the private key.
id	An optional *string* of an unique user defined identification of a certificate. The user defined id starts with the '@' character. It must consist of 1-40 characters of the set: `[a-z][A-Z][0-9]`, _ and -. If a new certificate with the same **id** is uploaded, the original certificate is overwritten.

The reply is in the **application/json** format and includes:

Parameter	Description
fingerprint	A *fingerprint* (hash) of a certificate.

Parameter	Description
replaced	A *fingerprint* of a replaced certificate.

Example

```
PUT /api/cert/user                                  //request
{                                                   //response
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint": "9623fa25e414aa930ed22348a22d04a4c4fda26b"
      }
    ]
  }
}
```

DELETE method

Request parameters for **DELETE**:

Parameter	Description
id	A mandatory *string* value identifying a CA certificate. The **id** value is user defined id, internal id or certificate fingerprint (hash). Internal certificates with **id** starting with "#" are protected and cannot be deleted.

The reply is in the **application/json** format.

Example

```
DELETE /api/cert/user?
fingerprint=4deea7060d80bacf1643b4e0f0104c82995075b7      //request
{                                                                    //
response
  "success" : true
}
```

5.20.3 api cert csr

The **/api/cert/csr** function helps you administer the certificate signing requests (CSR) and work with them in the device.

The function is part of the **System API** system and requires the user to have the **System – Control** privilege for authentication if required.

The **POST**, **GET**, **PUT** and **DELETE** methods can be used for this function.
The **POST** method helps create a new CSR.
The **GET** method retrieves information on the CSRs stored in the device.
The **PUT** method uploads the certificate corresponding to the given CSR to the device.
The **DELETE** method deletes the CSR from the device.

POST Method

Request parameters for **POST**:

Parameter	Description
commmonName	A mandatory parameter (*string*) containing a fully qualified domain name (FQDN) of the device (*e.g. verso01.internal*, verso01.example.com).
sanMdns	An optional parameter (*number*, {0,1}) defining whether or not SAN with the mDNS name will be included in the CSR (*<hostname>.local*). The default value is *1* (added).
sanIp	An optional parameter (*number*, {0,1}) defining whether or not SAN with the current IPv4 address will be included in the CSR (*<hostname>.local*). The default value is *1* (added).
algorithm	An optional parameter (string) defining the cryptographic algorithm for key generation. Applicable values: *P-256, P-384, RSA-2048, RSA-3072. P-256* is the default value. Note: *RSA-3072* is unavailable on the TI-ARM legacy platform.
id	An optional parameter (*string*) defining the unique identifier of the certificate. If this parameter is unset, the certificate is only identified by fingerprint. • It must start with @ and contain 1–40 characters [a–z] [A–Z][0–9], „_“ a „-“.
country	An optional parameter (*string*) defining the country (ISO 3166 Alpha-2, 2 uppercase letters, *CZ,* e.g.).
state	An optional parameter (*string*) defining the state/ province/region. Length: 1–128 characters. The \ character is not allowed.

Parameter	Description
locality	An optional parameter (*string*) defining the city/location. Length: 1–128 characters. The \ character is not allowed.
organization	An optional parameter (*string*) defining the organization. Length: 1–64 characters. The \ character is not allowed.
organizationalUnit	An optional parameter (*string*) defining the organizational unit. Length: 1–64 characters. The \ character is not allowed.
email	An optional parameter (*string*) containing the e-mail address (e.g. user@example.com). It has to have a valid format and length of 1–254 characters.

Output parameters:

In the case of success, a PEM file containing the **CSR** generated is returned.

In the case of error, a reply in the **application/json** format is returned including the error description.

Example 1: CSR generation based on input parameters

```
POST /api/cert/csr commonName=2nipverso-0000010016.internal&algorithm=P-256&id=%40tes
t&country=CZ&state=Hlavn%C3%AD+m%C4%9Bsto&locality=Praha&organization=2N&organization
alUnit=2N+OS&email=2nos%40example.com // request

-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAVwCAQAwgZwxJjAkBgNVBAMMHTJuaXB2ZXJzby0wMDAwMDEwMDE2Lmlu
dGVybmFsMQswCQYDVQQGEwJDWjEXMBUGA1UECAwOSGxhdm7DrSBtxJtzdG8xDjAM
BgNVBAcMBVByYWhhMQswCQYDVQQKDAIyTjEOMAwGA1UECwwFMk4gT1MxHzAdBgkq
hkiG9w0BCQEWEDJub3NAZXhhbXBsZS5jb20wWTATBgcqhkjOPQIBBggqhkjOPQMB
BwNCAASlQVzGnOuQVl/6jVP3fI1Udy0nBFU5ll1iuWj1k+e6aUIXUhob6Ak+YYY2
W71VQYUOQKksZ4vmAO/ACzo+jJMGoF0wWwYJKoZIhvcNAQkOMU4wTDBKBgNVHREE
QzBBgh0ybmlwdmVyc28tMDAwMDAxMDAxNi5pbnRlcm5hbIIaMm5pcHZlcnNvLTAw
MDAwMTAwMTYubG9jYWyHBKwRAAMwCgYIKoZIzj0EAwIDSAAwRQIgDSeN22+Hl2eU
6Chm7kHYXE34AXpN7Lt3oVjDnWc4aMoCIQCVFCllfhIKtaa9/f0Qn0E7aX05VvJM
7cUMFqPyvTICMA==
-----END CERTIFICATE REQUEST----- // successful reply

{
  "success" : false,
  "error" : {
    "code" : 12,
    "param" : "locality",
    "description" : "invalid parameter value"
  }
} // error
```

GET Method

Request parameters for **GET**:

Parameter	Description
id	An optional parameter (*string*) identifying the CSR. The *id* parameter can contain a user defined ID or fingerprint (hash) of the CSR for which information is to be retrieved. If *id* is unset, the reply includes a full list of all the CSR certificates in the device. • The user defined *id* starts with @ and must be followed by 1 to 40 characters of the following set: [a–z], [A–Z], [0–9], „_“ a „-“. • Fingerprint is a hexadecimal value representing hash CSR.

The reply is in the **application/json** format and can include the following parameters:

Parameter	Description
fingerprint	CSR fingerprint.
subject	A structure (dictionary) containing information on the subject (Subject Distinguished Name). DN is split into RDN items (if set): Common Name (CN), Organization (O), Organizational Unit (OU), Location (L), State (S), Country (C).
id	A string representing the internal CSR ID. The value is user defined. The CSR does not need to have an ID – it can only be identified using its fingerprint. In that case, it is not included in the reply.

Example 1: Display of all CSRs in the device

```
GET /api/cert/csr // request

{
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint" : "1b59cd8563e37f19f1b579b16943204cfe057c00",
        "subject" : {
          "CN" : "2nipverso.internal",
          "O" : "2N",
          "OU" : "2N OS"
        }
      },
      {
        "fingerprint" : "7900d3488bdbdae0560d64cfc1d3961e87205d5a",
        "subject" : {
          "CN" : "myverso.internal",
          "O" : "2N",
          "OU" : "2N OS App",
          "L" : "Praha",
          "S" : "Praha",
          "C" : "CZ"
        },
        "id" : "@myid"
      }
    ]
  }
} // reply
```

Example 2: Obtaining one CSR identified with an internal ID

```
GET /api/cert/csr?id=@myid // request

{
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint" : "7900d3488bdbdae0560d64cfc1d3961e87205d5a",
        "subject" : {
          "CN" : "myverso.internal",
          "O" : "2N",
          "OU" : "2N OS App",
          "L" : "Praha",
          "S" : "Praha",
          "C" : "CZ"
        },
        "id" : "@myid"
      }
    ]
  }
} // reply
```

PUT Method

Request parameters for **PUT**:

Parameter	Description
id	A mandatory parameter (string) identifying the CSR. The *id* parameter can contain a user defined CSR ID or fingerprint (hash). • The user defined *id* starts with @ and must be followed by 1 to 40 characters of the following set: [a–z], [A–Z], [0–9], „_“ a „-“. • Fingerprint is a hexadecimal value representing hash CSR.
blob-cert	A mandatory parameter containing a certificate in the PEM format. The certificate must match the private key of the given CSR.

The reply is in the **application/json** format and can include the following parameters:

Parameter	Description
certificates[]	An array with a list of certificates.

Parameter	Description
certificates[].fingerprint	Certificate fingerprint.
certificates[].replaced	Fingerprint of the replaced CSR. It is included only if *id* was set as fingerprint.

Example 1: Certificate upload to the device. The certificate matches the CSR private key.

```
PUT /api/cert/csr?id=9623fa25e414aa930ed22348a22d04a4c4fda26c // request

{
  "success" : true,
  "result" : {
    "certificates" : [
      {
        "fingerprint": "9623fa25e414aa930ed22348a22d04a4c4fda26b"
        "replaced": "9623fa25e414aa930ed22348a22d04a4c4fda26c"
      }
    ]
  }
} // reply

{
  "success" : false,
  "error" : {
    "code" : 12,
    "param" : "blob-cert",
    "description" : "private key mismatch",
    "data" : "pk_mismatch"
  }
} // reply
```

DELETE Method

Request parameters for **DELETE**:

Parameter	Description
id	A mandatory parameter (*string*) identifying the CSR. The *id* parameter can contain a user defined CSR ID, internal ID or fingerprint (hash). • It starts with @ and must be followed by 1 to 40 characters of the following set: [a–z], [A–Z], [0–9], „_“ a „-“. • A hexadecimal value representing hash CSR.

Example 1: Deleting CSR according to its fingerprint (success/error examples)

```
DELETE /api/cert/csr?id=4deea7060d80babf1643b4e0f0104c82995075b7 // request

{
  "success" : true
} // reply

{
  "success" : false,
  "error" : {
    "code" : 12,
    "param" : "id",
    "description" : "certificate not found",
    "data": "cert_not_found"
  }
} // reply
```