Application Note 001it-2023

# Gateway http: porta IoT

## Configurazione API http per l'integrazione con le serrature elettroniche **dormakaba** e descrizione del caso d'uso di sblocco di un Cilindro Elettronico o Maniglia Elettronica.


## Autore

Rita Petrongari

## Revisore

Alfredo Montini



Il documento è indirizzato agli installatori/sviluppatori che devono integrare dispositivi domotici e di sicurezza di terze parti con la centrale lares 4.0, utilizzando il gateway http: **porta IoT** per la loro gestione. In particolare questo documento descrive l'integrazione di prodotti elettronici per porte **dormakaba,** attraverso la configurazione di API http e il caso d'uso di sblocco di un cilindro elettronico/maniglia elettronica.

## Sommario

## Introduzione

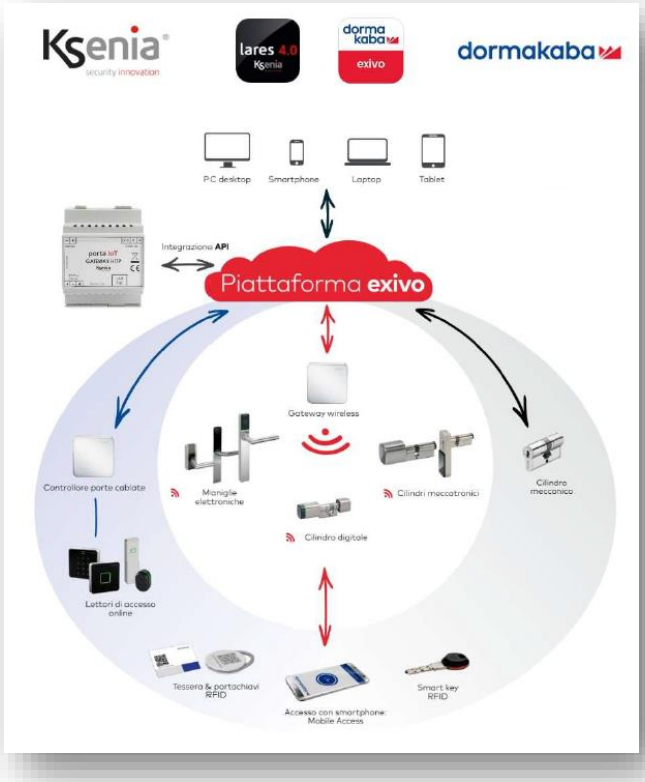
**In generale**, l'integrazione tra la centrale lares 4.0 e i prodotti di terze parti è di tipo API http con metodi GET – PUT – POST – DELETE e body message di tipo json.

**Questo documento** fornisce le seguenti informazioni:

1) modalità di acquisizione dei dati per la connessione Ksenia/ dormakaba: autenticazione, chiavi ID, stringhe URL, ecc.
2) configurazione passo-passo, lato Ksenia e lato dormakaba, per permettere lo sblocco delle serrature elettroniche dormakaba (Cilindro o Maniglia) direttamente dalla piattaforma lares 4.0, grazie al gateway HTTP **porta IoT**, mediante **metodo POST.**

## Architettura della soluzione

La soluzione descritta permette di sbloccare/aprire dalla centrale lares 4.0 mediante il Gateway http **porta IoT**, la serratura di una porta in cui siano stati installati cilindro o serratura elettronici di marca **dormakaba**, presenti su Piattaforma Exivo. Lato Ksenia, lo sblocco può avvenire da **App lares 4.0** (sia da locale che da remoto), mediante inserimento di un codice PIN oppure mediante lettura chiavette Tag su tastiere **ergo-X** o lettori **volo/volo-in** di Ksenia.



dormakaba è azienda leader per le soluzioni di accesso e sicurezza che comprendono, tra l'altro, maniglie elettroniche facilmente montabili su serrature e porte esistenti oppure cilindri elettronici che vanno a sostituire i cilindri meccanici esistenti.

Link utili per approfondire il tema relativo ai prodotti **dormakaba**:
https://www.dormakaba.com/it-it
https://www.dormakaba.com/it-it/offerta/prodotti

## Limitazioni

La soluzione descritta nel presente documento prevede la comunicazione diretta tra il gateway http di Ksenia (**porta IoT**) con il cloud **Exivo** di **dormakaba** attraverso la rete Internet. Questo significa che un'eventuale perdita della connessione di rete verso il cloud impedisce il normale funzionamento e quindi rende impossibile l'apertura del cilindro elettronico/maniglia elettronica dalle interfacce della lares 4.0.

Al fine di aumentare la disponibilità e affidabilità della soluzione, si consiglia di prevedere un collegamento di backup alla rete Internet (fornito ad esempio dall'infrastruttura di rete presente nell'impianto).

## Compatibilità

**Ksenia** : la funzionalità di sblocco serrature elettroniche è compatibile a partire dalla versione 1.107.27 firmware e dalla versione 1.41.0 software della centrale lares 4.0.

**dormakaba**: rivolgersi ai propri referenti dormakaba per le considerazioni ottimali necessarie per il proprio sito di controllo accessi.

# Brevi cenni sulla configurazione del dispositivo Gateway porta IoT di Ksenia

I requisiti per la configurazione del Servizio Gateway http sono i seguenti:

1. la centrale lares 4.0 deve essere registrata sul cloud di Ksenia SecureWeb;
2. il programma di configurazione Installer deve essere avviato da Ksenia SecureWeb;
3. attivare il servizio Gateway http sul dispositivo porta IoT.

Dal programma di configurazione Installer occorre configurare il dispositivo IP, i dispositivi collegati e le API http/s in uscita e in ingresso. I passi principali sono descritti nel seguito mentre per la compilazione dei campi è possibile consultare l'help online contestuale:

1. nel menu <**Dispositivi IP->Gateway**> configurare il gateway porta IoT e i parametri di rete richiesti;
2. nel menu <**Servizi->Gateway HTTP**> attivare il servizio Gateway http* per il porta IoT.
   (*Il servizio attivato è legato al MAC Address del dispositivo porta IoT e non è trasferibile ad altro dispositivo);
3. nel menu <**Servizi -> Gateway http**> configurare i dati generali del gateway:
   - Abilita HTTPS = questa voce abilita la connessione sicura, se abilitata il protocollo https deve essere gestito anche dal dispositivo che si deve integrare;
   - Tipo di autenticazione = genera un token random per autenticarsi con il dispositivo da integrare. Alcuni dispositivi forniscono un proprio codice di autenticazione che deve essere riportato nell'URL delle API in uscita (*come nel caso del Philips Hue, descritto nel seguito*).
4. nel menu <**Servizi->Gateway HTTP**> configurare le API in uscita (ossia come mandare le richieste): aggiungere i dispositivi da connettere alla centrale lares 4.0 e le azioni (con metodo GET-PUT-POST-DELETE) da inviare a ciascun dispositivo connesso, come richiesto dallo stesso;
5. nei menu <**Partizioni**>, <**Uscite**>, <**Zone**> e <**Scenari**> configurare le API in ingresso (ossia come processare le richieste) che consentono al dispositivo connesso di effettuare una serie di azioni come sintetizzato nella tabella di seguito.

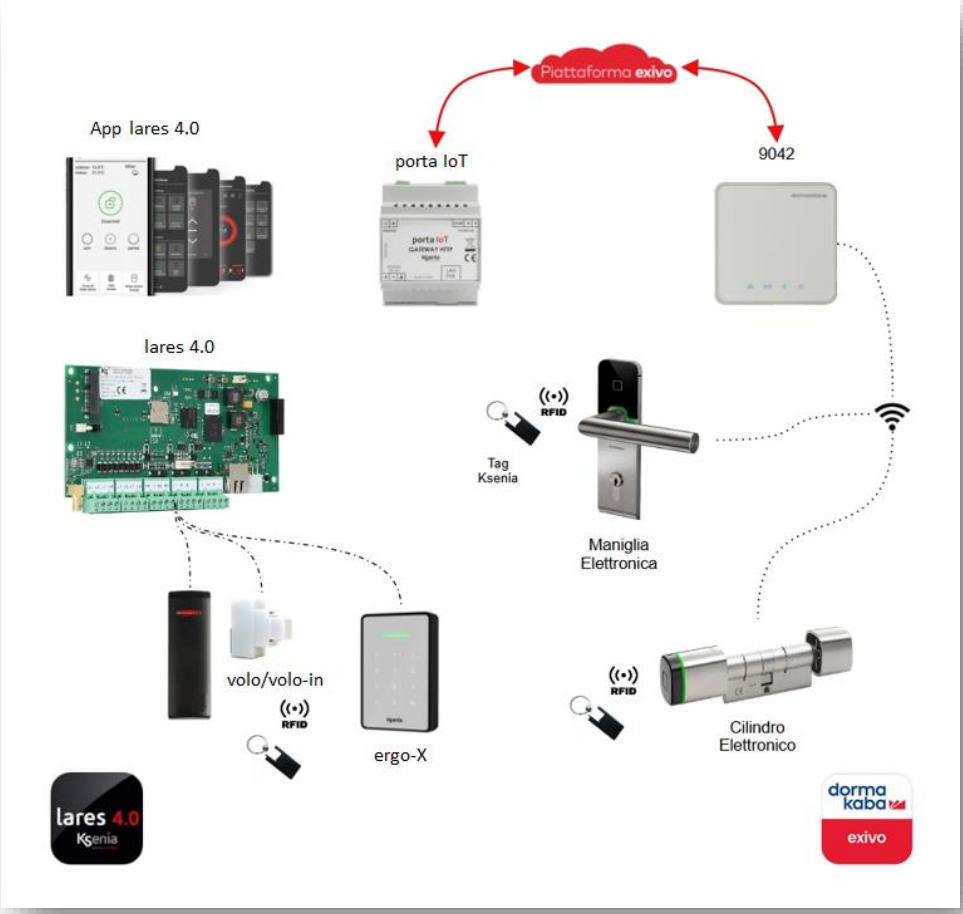
| | Metodi | Partizioni | Zone | Uscite | Scenari |
|---|---|---|---|---|---|
| Lettura stato | GET */Legge i dati* | X | X | X | X |
| Modifica stato | GET */Legge i dati*<br>PUT */Aggiorna i dati* | -<br>X | X<br>X | X<br>X | -<br>- |
| Escludi/Includi | GET */Legge i dati*<br>PUT */Aggiorna i dati* | -<br>- | X<br>X | -<br>- | -<br>- |
| Esecuzione scenario | GET */Legge i dati*<br>POST */Inserisce i dati* | -<br>- | -<br>- | -<br>- | X<br>X |

## Porte in ascolto lato porta IoT

| Listening port | Descrizione |
|---|---|
| 8080 | Connessione in http |
| 8443 | Connessione in HTTPS |
| 69 | Porta della scheda madre della lares 4.0 |

## Integrazione passo-passo (esempio)

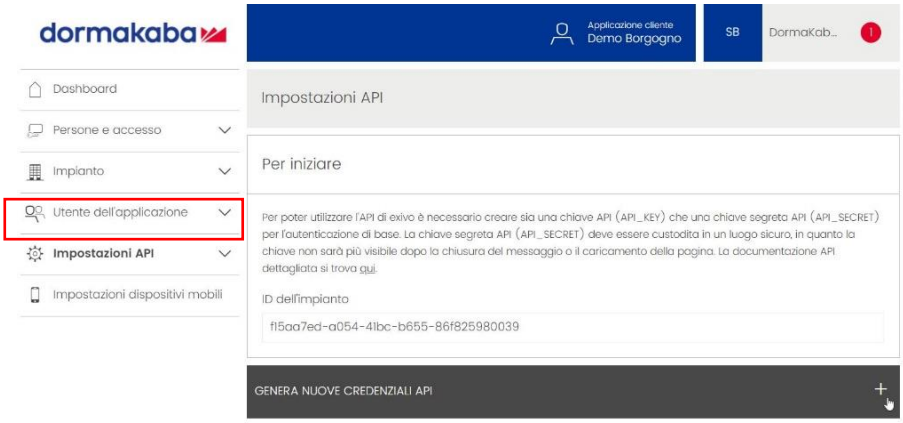
Si assume una adeguata conoscenza della centrale lares 4.0 e del cloud di Ksenia SecureWeb e dei prodotti dormakaba su piattaforma Exivo, è necessaria anche la registrazione al cloud Exivo.



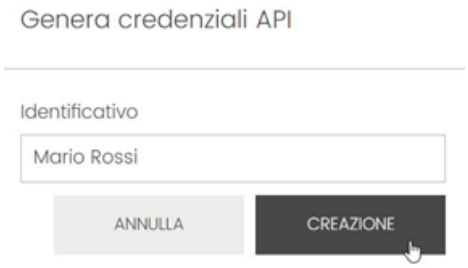
## Configurazione lato dormakaba

a. Generare nuove credenziali API

1) Collegarsi al portale cloud di Exivo : https://customer.exivo.io/login
Dalla home page aprire il menu <**Impostazioni API**> e generare nuove credenziali API cliccando su <+>.

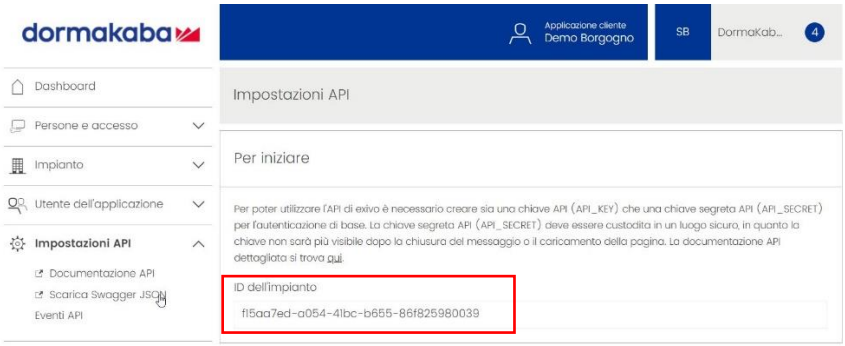



2) Scegliere un nome utente che identificherà le credenziali API e cliccare su “CREAZIONE” per confermare.




3) Salvare in un luogo sicuro la **chiave segreta API (API_SECRET) prima di chiudere la finestra** premendo la <X>.
La c**hiave API(API_KEY)** che identifica l’utente autorizzato sarà sempre visibile.

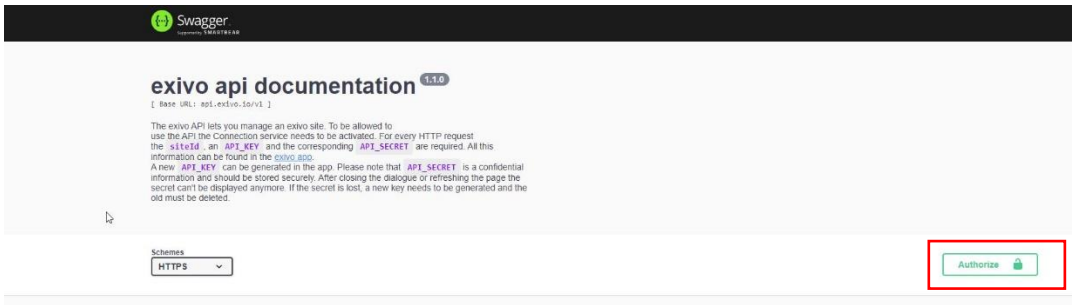
4) Prendere nota del “**ID dell’impianto**” che identificherà in modo univoco il vostro impianto e poi selezionare il menu “**Documentazione API**” per accedere al servizio API Swagger di Exivo.




b. Avviare il Servizio API Swagger di Exivo per acquisire le chiavi ID del cilindro elettronico e la stringa “Request URL”; utilizzare le credenziali API appena generate.

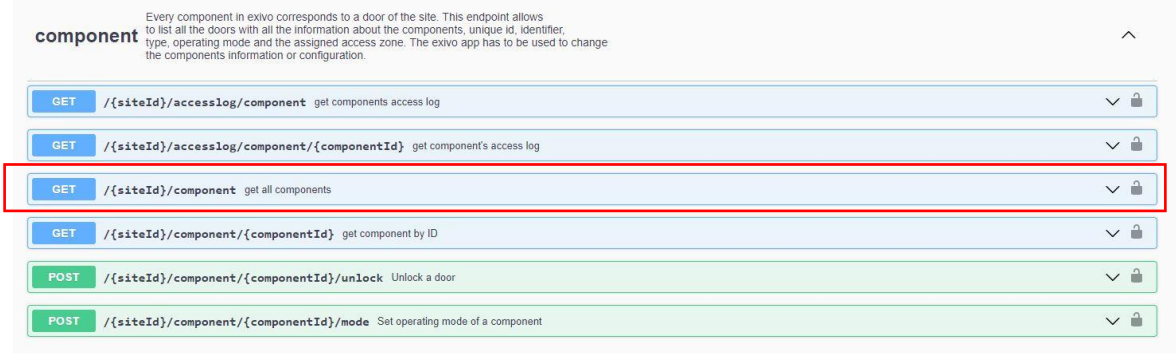
1) Dal menu “Documentazione API” (descritto al passo precedente) si accede al servizio API Swagger di Exivo che permette di ottenere i dati necessari da inserire successivamente nella programmazione del Gateway porta IoT, lato Ksenia.

   Cliccare su <**Authorize**>

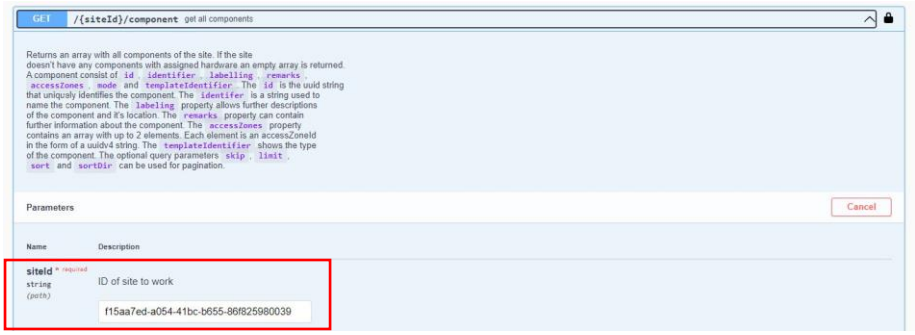



2) Inserire la **chiave API_KEY** (come Username) e la **password API_SECRET** (come Password), create in precedenza per “Mario Rossi”, quindi cliccare su <**Authorize**>

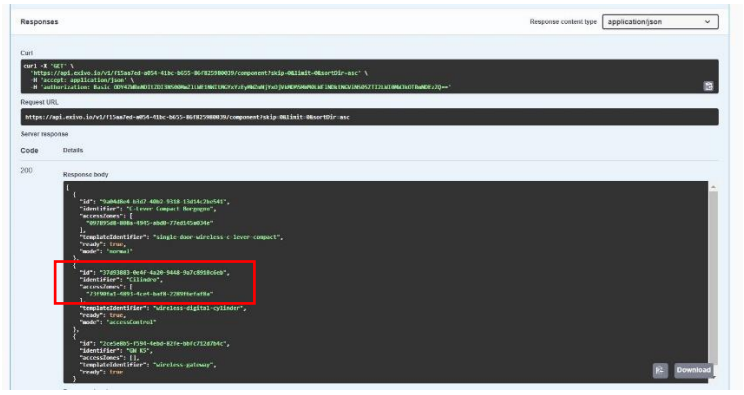
3) Cliccare sulla funzione **GET all components** per conoscere l'ID del Cilindro elettronico in quanto ogni elemento fisico e non fisico è identificato con una chiave ID.




4) Inserire la chiave "**ID dell'impianto**", di cui avete preso nota precedentemente, nel campo "**ID of site work**" e cliccare su "**EXECUTE**".

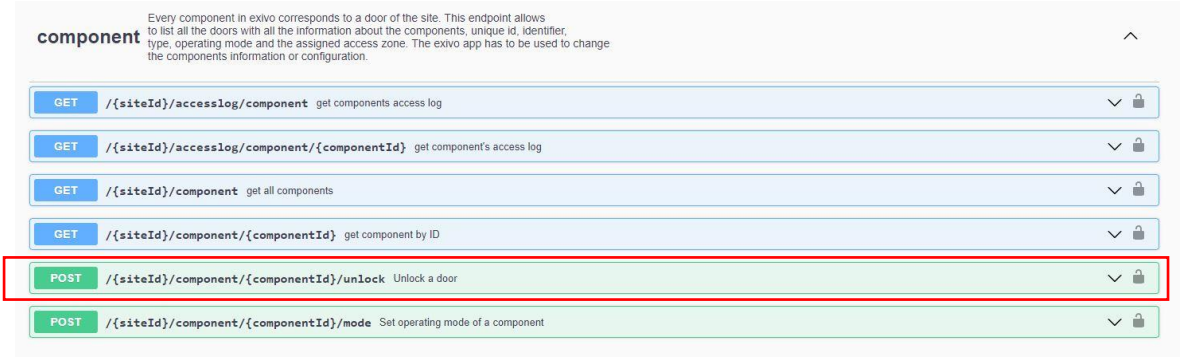



5) La funzione GET all components visualizzerà gli **ID** di tutti i componenti fisici, **prendere nota dell'ID del vostro Cilindro Elettronico**.

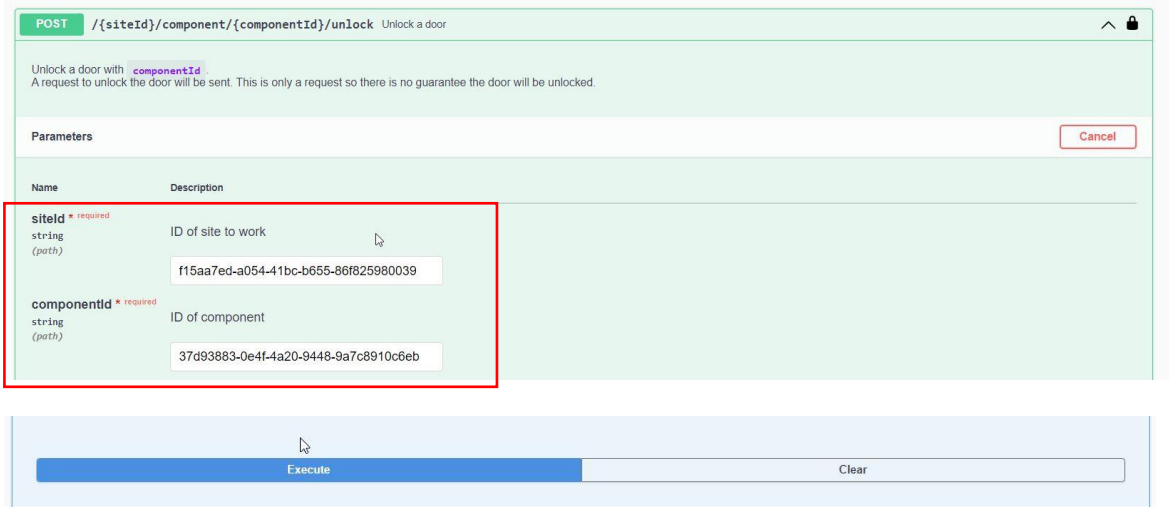


```
"id": "37d93883-0e4f-4a20-9448-9a7c8910c6eb",
"identifier": "Cilindro",
"accessZones": [
  "73f90fa1-4893-4ce4-baf8-2289f6efaf8a"
],
"templateIdentifier": "wireless-digital-cylinder",
"ready": true,
"mode": "accessControl"
```


6) Per ottenere la stringa di comando **POST** di sblocco del Cilindro Elettronico, da inserire in fase di programmazione del Gateway porta IoT nella sezione "Azioni", cliccare sulla funzione **"POST Unlock a door"**.




7) Inserire l'**ID dell'impianto** (Site ID) nel campo "**ID of site to work**" e l'**ID del Cilindro Elettronico**, nel campo "**ID of components**", di cui avete preso nota precedentemente, cliccare su "**Execute**".

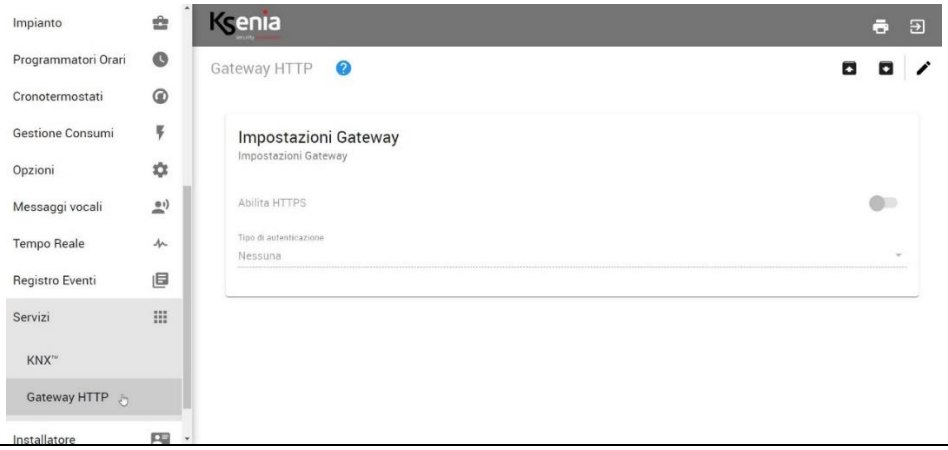



8) In tal modo viene visualizzata la struttura "Curl" e la **stringa "Request URL"** che dovrà essere copiata, salvata e inserita come descritto di seguito nel paragrafo "**Configurazione lato Ksenia**".

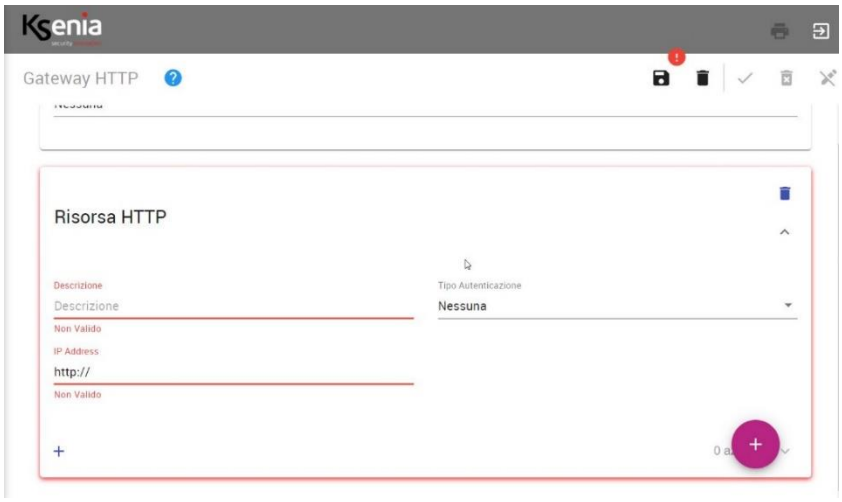
## Configurazione lato Ksenia

a. Configurare la Risorsa Http del cilindro elettronico dormakaba, nei servizi del Gateway http

1) Dall'interfaccia webserver della centrale, aprire il menu <Servizi -> Gateway http>.




2) Aggiungere la Risorsa http, che equivale al servizio Exivo, cliccando sul **<+>**:




Inserire nei campi i seguenti valori:

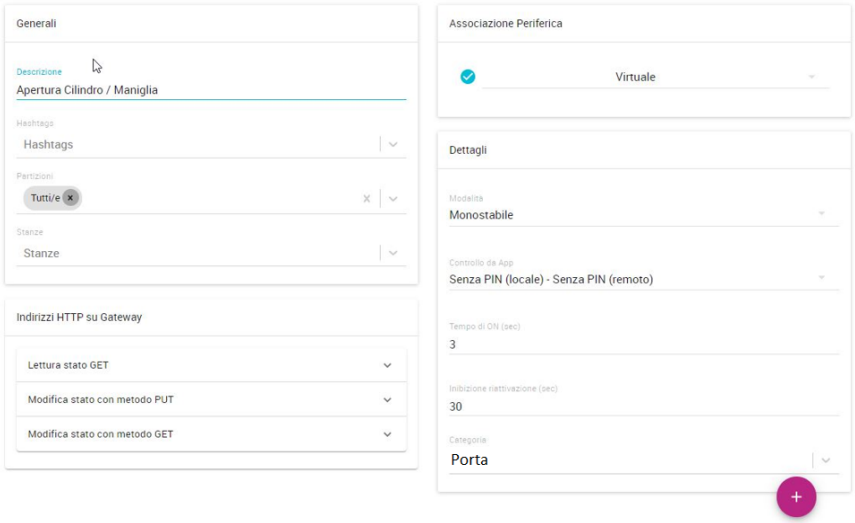
- Descrizione = *es. Exivo cloud*
  (*"Abilita http" deve essere abilitato, quindi inserisci i seguenti dati*):
- Tipo autenticazione = **Basic**
  Username = inserire la **Chiave API(API_KEY)**
  Password = inserire la **Chiave segreta API (API_SECRET)**

- IP address = **https://api.exivo.io** (URL per raggiungere il servizio API di Exivo)


3) Aggiungi l'azione per comandare l'apertura del cilindro/maniglia con metodo POST, cliccando sul **<+>**:
   - Descrizione = *es. Cilindro / Maniglia apertura*
   - Metodo = **POST** + stringa di comando **"Request URL"** ottenuta dal servizio API Swagger di Exivo (es.: /v1/f15aa7ed-a054-41bc-b655-86f825980039/component/37d93883-0e4f-4a20-9448-9a7c8910c6eb/unlock)

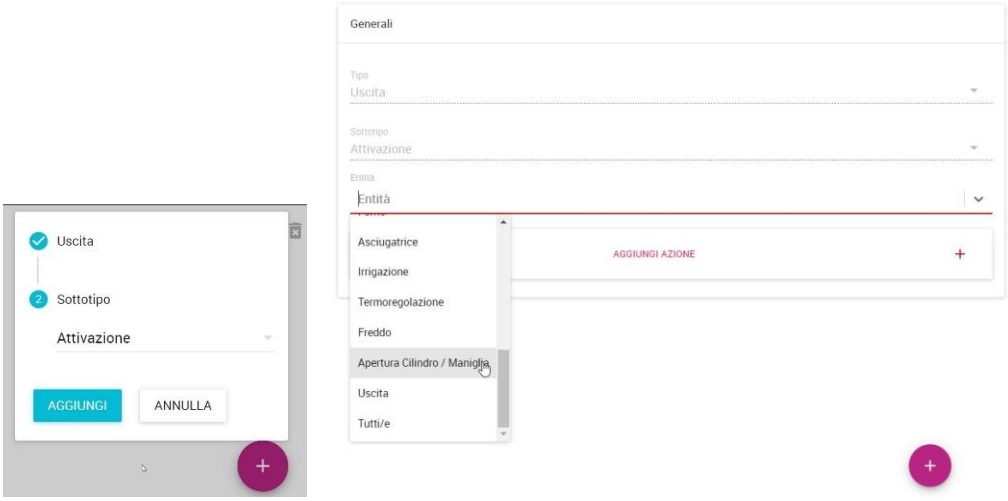

b. Configurare un'uscita virtuale e assegnarle la categoria PORTA

1) Aprire il menu <Impianto->Uscite>.
   Descrizione = es.: "*Apertura Cilindro / Maniglia*"
   Tipo = virtuale
   Modalità = monostabile
   Controllo da APP = senza PIN
   Categoria = PORTA.




c. Creare scenario per **Attivazione** cilindro da **APP lares 4.0** oppure da **Tempo Reale**.

1) Aprire il menu <Impianto -> Scenari -> Eventi> ed aggiungere un evento:
Tipo: Uscita
Sottotipo: Attivazione
Entità: *Apertura Cilindro / Maniglia*
**ed aggiungere l'azione di tipo Gateway - Azione http – *Cilindro / Maniglia apertura*.**




d. Creare scenario **Riconosciuto codice** PIN da **tastiera ergo-X**.

1) Aprire il menu <Impianto -> Scenari -> Eventi> ed aggiungere un evento:
Tipo: Tastiera
Sottotipo: Riconosciuto codice
Entità: *ergo-X*
**ed aggiungere l'azione di tipo Gateway - Azione http – *Cilindro / Maniglia apertura***



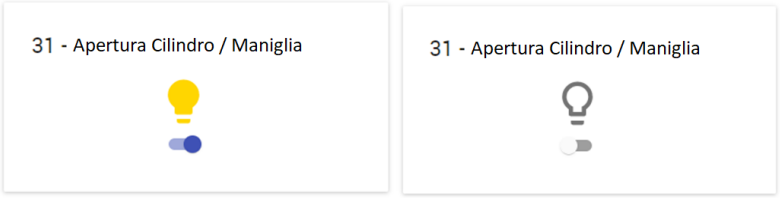
e. Creare scenario per **Riconosciuta chiave** TAG Ksenia da lettore **volo**.

1) Aprire il menu <Impianto -> Scenari -> Eventi> ed aggiungere un evento:
Tipo: Lettore
Sottotipo: Riconosciuta chiave
Entità: *volo*
**ed aggiungere l'azione di tipo Gateway - Azione http – *Cilindro / Maniglia apertura***



f. Attivazione/Sblocco cilindro dal menu "Tempo reale->Uscite", cliccare su "*Apertura Cilindro / Maniglia*" e verificare l'apertura della porta.

Solo un click per aprire la porta:

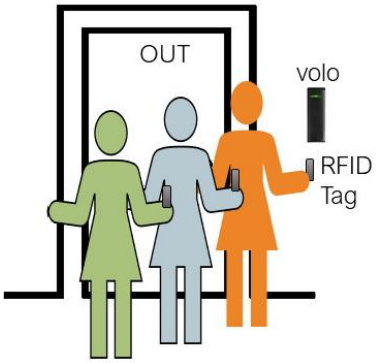



g. Attivazione/Sblocco cilindro da App lares 4.0, toccare l'icona *Apertura Cilindro / Maniglia* e verificare l'apertura della porta.

Toccare l'icona *Apertura Cilindro/Maniglia* per aprire:


h. Attivazione/Sblocco cilindro da Tag e verificare l'apertura della porta.

Passare la chiave Tag sul lettore configurato (volo).




i. Attivazione/Sblocco cilindro da Codice PIN e verificare l'apertura della porta.

Digitare il codice PIN sulla tastiera configurata (ergo-X).