Application Note 006it rev.3

GATEWAY HTTP E ZONE IP

API http/s per la piattaforma IoT lares 4.0

Il documento è indirizzato agli installatori che vogliono integrare un dispositivo IP (principalmente telecamere IP) con la piattaforma IoT lares 4.0.

Sommario

Zone IP 3
Gateway http/s 6
Endpoints http/s 8
Diagnostica della zona IP 12
Sicurezza della connessione 12
Azioni http/s 13
Porte in ascolto 16

Zone IP

In tutte le centrali antintrusione le “zone”, o ingressi, rappresentano il trigger che fa scattare la logica di funzionamento di una centrale: se il sistema è inserito e una zona si porta in una condizione di allarme, il sistema stesso si porta in ALLARME e viene eseguita tutta la sequenza di azioni che è stata programmata, ad esempio viene fatta suonare la sirena e avvisati i proprietari dell’area protetta per mezzo, ad esempio, di una telefonata o notifica PUSH.

Quando il sistema non è inserito, la condizione di allarme potrebbe essere ignorata oppure gestita ad esempio per commutare un’uscita (come accendere una luce quando qualcuno passa sotto un sensore).

Normalmente le zone sono di due tipi:

- Filari o bus, quando sono connesse tramite cavo a sensori (universali o su BUS, oppure contatti magnetici): quando il sensore rileva una violazione della zona che protegge, chiude o apre il contatto (oppure invia una segnalazione su BUS);
- Wireless quando il sensore o il contatto magnetico comunicano via radio: se il sensore rileva una violazione della zona che protegge, invia una segnalazione in centrale.

La funzionalità “Zone IP” introduce un terzo tipo di zona:

- Il dispositivo o sensore è collegato in rete IP alla centrale, normalmente sulla stessa LAN, e segnala le variazioni di stato inviando una richiesta http secondo il formato accettato dalla centrale stessa.

In questo modo, **qualunque dispositivo IP in grado di essere programmato per inviare la richiesta prevista dalla centrale, può essere utilizzato per commutare lo stato di una zona.**

Principalmente questi dispositivi sono telecamere IP dotate di video analisi a bordo oppure un NVR[1] evoluto: quando la video analisi della telecamera viene verificata essa invia la richiesta http alla centrale che la elabora di conseguenza. In questo modo ogni telecamera IP con video analisi può essere gestita come un vero e proprio sensore dalle centrali lares 4.0.

Nel caso di una zona IP:

- La centrale lares 4.0 ha il ruolo di SERVER http;
- Il dispositivo IP ha il ruolo di CLIENT http;
- La richiesta http deve essere inviata verso uno specifico URL[2] gestito dal server http (chiamato anche “endpoint http”);
- I metodi http supportati dal server sono:
  - GET
  - POST
- La centrale lares 4.0 mette a disposizione due URL:

[1] NVR = Network Video Recorder

[2] URL = Uniform Resource Locator

- Uno per mandare in ALLARME la zona
- Uno per il RIPRISTINO della zona

- Tutte le zone previste dal taglio di centrale possono essere configurate come zone IP.

Il SERVER http in esecuzione sulla centrale lares 4.0 per gestire le richieste http, è in ascolto sulla porta **tcp/69** (non è la porta standard per le richieste http perché quella standard, la tcp/80, è usata per la connessione al web server di configurazione quando la centrale è impostata per la connessione http).

Il formato e il metodo http dei due URL accettati dalle centrali lares 4.0 sono descritti nella Tabella 1.

URL	METODI	AZIONE
http://<ip_centrale>:69/ZONES/<numero_zona>/ALARM	GET POST	Porta lo stato della zona in ALLARME
http://<ip_centrale>:69/ZONES/<numero_zona>/RESTORE	GET POST	Porta lo stato della zona a RIPOSO

Tabella 1 - URL previsti per le zone IP sulle centrali lares 4.0

Dove:

- <ip_centrale> = indirizzo IP della centrale lares 4.0
- <numero_zona> = ID della zona

La singola zona IP può essere configurata in due modi:

- Con AUTO RIPRISTINO
  In questo caso, dopo 3 secondi dalla ricezione della richiesta di ALARM la zona torna a RIPOSO automaticamente.
- Senza AUTO RIPRISTINO
  In questo caso, la zona IP torna nello stato di RIPOSO solo quando la centrale riceve la richiesta di RESTORE.

È necessario quindi programmare sul dispositivo IP, uno o entrambi gli URL della Tabella 1, in funzione del fatto che la zona sia stata configurata con auto ripristino o meno, specificando il numero della zona corretto.

Ad ogni richiesta la centrale lares 4.0 risponde come specificato nella Tabella 2.

URL	RISPOSTA (codice risposta http)
http://<ip_centrale>:69/ZONES/<zona_corretta>/ALARM	200 (OK)
http://<ip_centrale>:69/ZONES/<zona_non_IP>/ALARM	404 (Not found)
http://<ip_centrale>:69/ZONES/<zona_non_programmata>/ALARM	404 (Not found)

Tabella 2 - Codici di risposta http alle richieste per zone IP

Le stesse risposte sono inviate in caso di richiesta per RESTORE.

Qualunque contenuto nel body della richiesta GET o POST viene ignorato.

Nella Figura 1 un esempio di richiesta http GET corretta che porta in allarme la zona di ID 15 di una centrale di indirizzo IP 192.168.1.128 (in rosso la richiesta del client, in blu la risposta del server).

Figura 1 - Richiesta http corretta per la zona IP di ID=15

Nella Figura 2 la stessa richiesta verso la stessa centrale ma per la zona di ID 14 che non è programmata come zona IP (stessa situazione se la zona non fosse presente in programmazione).

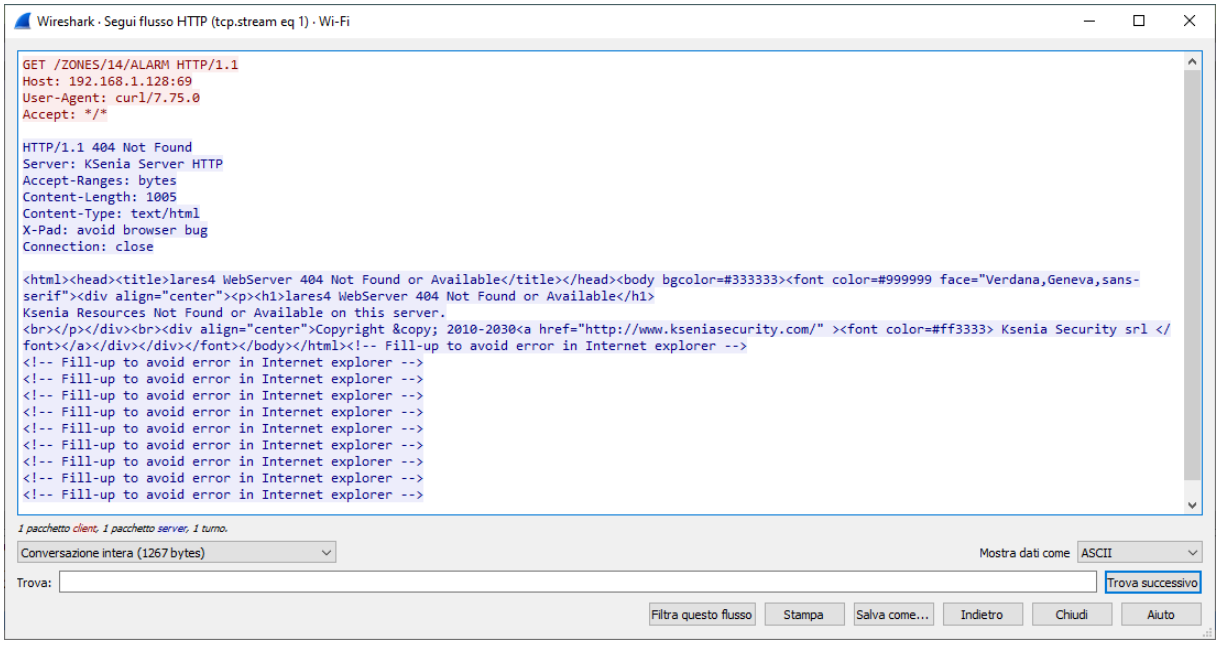

Figura 2 - Richiesta http errata per la zona IP di ID=14

Gateway http/s

La funzionalità “Zone IP” permette di utilizzare un dispositivo IP di terze parti, principalmente telecamere IP in grado di essere programmate per inviare richieste http, solo per modificare lo stato di una zona. Presenta quindi i seguenti limiti:

- A differenza di un normale sensore, il dispositivo IP che controlla la zona non è supervisionato, cioè la centrale non ne conosce il suo stato operativo (funziona oppure non funziona) quindi una zona potrebbe non cambiare stato perché semplicemente il dispositivo IP che dovrebbe comandarla non comunica più in rete (disconnesso) oppure è guasto.
- La richiesta non è cifrata (protocollo http invece che https).
- La centrale non è in grado di discriminare la sorgente della richiesta http arrivata.

Per ovviare a queste limitazioni ed estendere l’integrazione con le altre funzionalità delle centrali lares 4.0 è stato introdotto un servizio che si chiama “gateway http/s” molto più performante e sicuro che richiede però un hardware dedicato su cui essere in esecuzione: questo servizio è compreso nella periferica IP chiamata *porta IoT* oppure può essere attivato sulla periferica *porta 4.0*.

Nel seguito del documento, per semplicità, si farà riferimento sempre alla periferica *porta IoT*.

La centrale lares 4.0 e la periferica *porta IoT* devono comunicare tra loro in modo da scambiarsi le informazioni trasportate dalle richieste http/s da e verso i dispositivi di terze parti: questa comunicazione bidirezionale avviene attraverso il protocollo proprietario.

Con la presenza del *porta IoT* l’architettura della soluzione diventa:

- Il *porta IoT* ha il doppio ruolo di server HTTP/S per le richieste che riceve dai dispositivi di terze parti e di CLIENT per le richieste che invia verso i dispositivi di terze parti;
- La centrale lares 4.0 e il *porta IoT* comunicano tra loro in modo bidirezionale per mezzo di un protocollo proprietario Ksenia (descritto nell’apposito capitolo);
- L’unico indirizzo IP esposto (quello che mette a disposizione gli endpoint http/s) deve essere quello del *porta IoT*;
- Il SERVER http/s in esecuzione sul *porta IoT* può essere configurato in http o in https (scegliendo una delle due modalità tutte le richieste saranno elaborate solo se del tipo selezionato);
- Le richieste verso dispositivi di terze parti possono essere eseguite in http o in https;
- La funzionalità “zone IP” continua ad essere disponibile sulla centrale lares 4.0 per cui quando si configura una zona è possibile scegliere tra due tipi:
    - IP = quando la zona IP è gestita dal web server sulla centrale lares 4.0
    - IP (gateway http) = quando la zona IP è gestita dal web server sul *porta IoT*

  Ne consegue che nei due casi cambia l’indirizzo IP da indicare nell’URL.

L’architettura del sistema con il *porta IoT* dove è in esecuzione il servizio gateway http/s diventa quella descritta nella Figura 3.

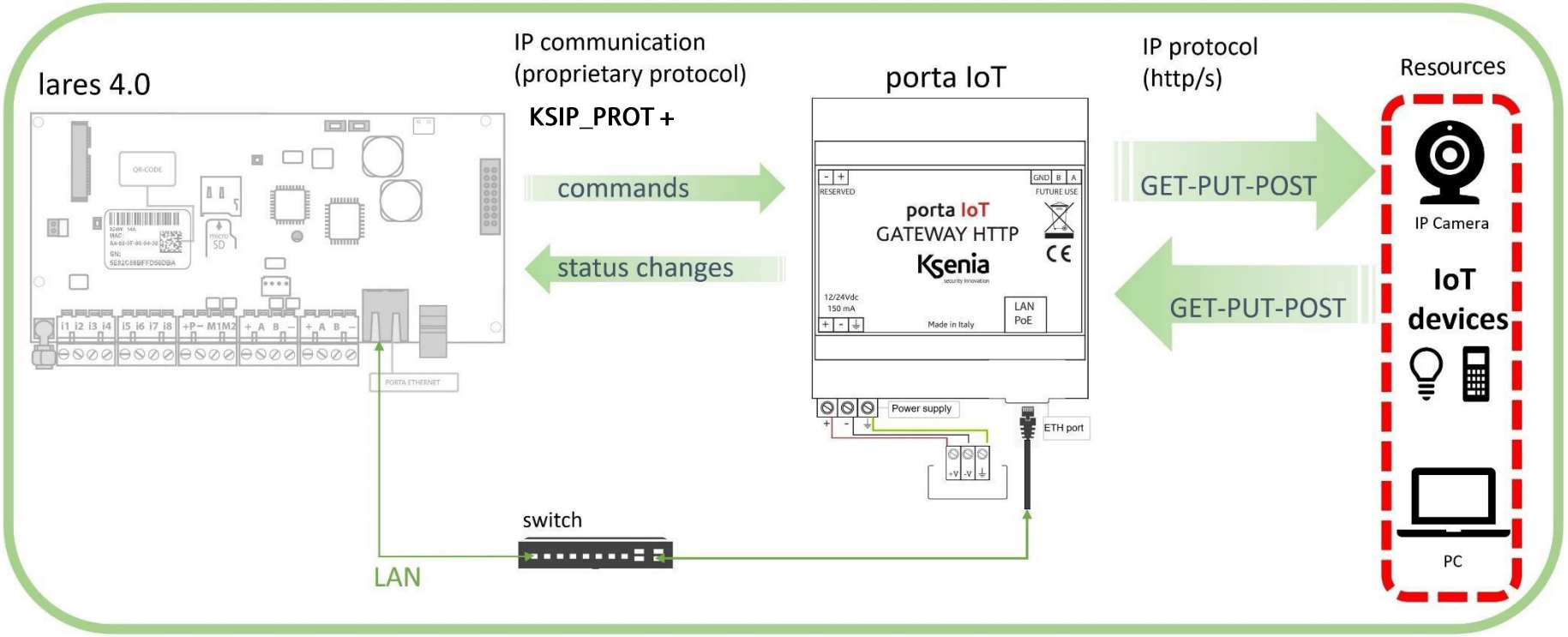

Figura 3 - Architettura lares 4.0 e porta IoT.

Endpoints http/s

Gli endpoints messi a disposizione dal servizio gateway http rappresentano gli URL delle richieste gestiste e delle relative risposte.

Il gateway http permette di gestire le entità della centrale lares 4.0 descritte nella Tabella 3: per semplicità si presuppone che il server sia configurato in https, l'indirizzo IP della centrale è 192.168.1.1 e l'entità che si desidera gestire, indipendentemente dalla sua tipologia, è sempre quella di ID=1.

Entità	Metodo http	Funzione	Formato

ZONE	GET	Lettura stato	URL = https://192.168.1.1:8443/zones/1
			risposta 200 OK con BODY:
			{
			"id": "1",
			"status": "STATUS_VALUE",
			"bypass": "BYPASS_VALUE"
			}
			dove:
			STATUS_VALUE = rest | alarm | mask | tamper
			BYPASS_VALUE = on | off
			Oppure 404 se zona non è IP o non programmata

	PUT	Modifica stato	URL = https://192.168.1.1:8443/zones/1 con
			BODY:
			{
			"status": "STATUS_VALUE"
			}
			dove:
			STATUS_VALUE = rest | alarm | mask
			Risposta: 200 o 404

	GET	Modifica stato	URL = http://192.168.1.1:8443/zones/1/params?status=STATUS_VALUE dove: STATUS_VALUE = rest | alarm | mask Risposta: 200 o 404
	POST	Modifica stato	URL = https://192.168.1.1:8443/zones/1/alarm (porta lo stato della zona in ALLARME) Risposta: 200 (OK) o 404 (se la zona non è programmata come zona IP) URL = https://192.168.1.1:8443/zones/1/restore (porta lo stato della zona a RIPOSO) Risposta: 200 (OK) o 404 (se la zona non è programmata come zona IP)

	PUT	Esclusione/ inclusione	URL = https://192.168.1.1:8443/zones/1 con BODY:
			{
			"bypass": "BYPASS_VALUE"
			}
			dove:
			BYPASS_VALUE = on | off
			Risposta: 200 o 404

	GET	Esclusione/ inclusione	URL = http://192.168.1.1:8443/zones/1/params?bypass=BYPASS_VALUE dove: BYPASS_VALUE = on | off Risposta: 200 o 404

USCITE	GET	Lettura stato	URL = https://192.168.1.1:8443/outputs/1
			risposta 200 OK con BODY:
			{
			"id": "1",
			"status": "STATUS_VALUE"
			}
			dove:
			STATUS_VALUE = on | off
			Oppure 404 se l'uscita non è programmata

	PUT	Modifica stato	URL = https://192.168.1.1:8443/outputs/1
			con BODY:
			{
			"status": "STATUS_VALUE"
			}
			dove:
			STATUS_VALUE = on | off | tgl
			Risposta: 200 o 404

	GET	Modifica stato	URL = http://192.168.1.1:8443/outputs/1/params?status=STATUS_VALUE dove: STATUS_VALUE = on | off | tgl Risposta: 200 o 404

PARTIZIONI	GET	Lettura stato	URL = https://192.168.1.1:8443/partitions/1 risposta 200 OK con BODY:
			{
			"id": "1",
			"arm": "ARM_VALUE",
			"status": "STATUS_VALUE"
			}
			dove:
			ARM_VALUE = disarm | delayed | immediate | entry_time | exit_time
			STATUS_VALUE = rest | alarm | alarm_memory | tamper | tamper_memory
			Oppure 404 se la partizione non è programmata

	PUT	Modifica stato	URL = https://192.168.1.1:8443/partitions/1 con BODY: { "mode": "MODE_VALUE"
			} dove: MODE_VALUE = disarm | delayed_arm | instant_arm Risposta: 200 o 404
SCENARI	POST	Esecuzione scenario	URL = https://192.168.1.1:8443/scenarios/1/execute Risposta 200 o 404 se lo scenario non è programmato
	GET	Esecuzione scenario	URL = https://192.168.1.1:8443/scenarios/1/execute Risposta 200 o 404 se lo scenario non è programmato

Tabella 3 – Endpoint del gateway http e relative risposte

Tutti gli endpoints sono descritti nell'interfaccia di configurazione della centrale lares 4.0 dove, risorse per risorsa, è possibile copiare gli URL per usarli nella configurazione del dispositivo di terze parti.

La Figura 4, a titolo di esempio, riporta questa sezione dell'interfaccia di configurazione per la zona di ID=14.

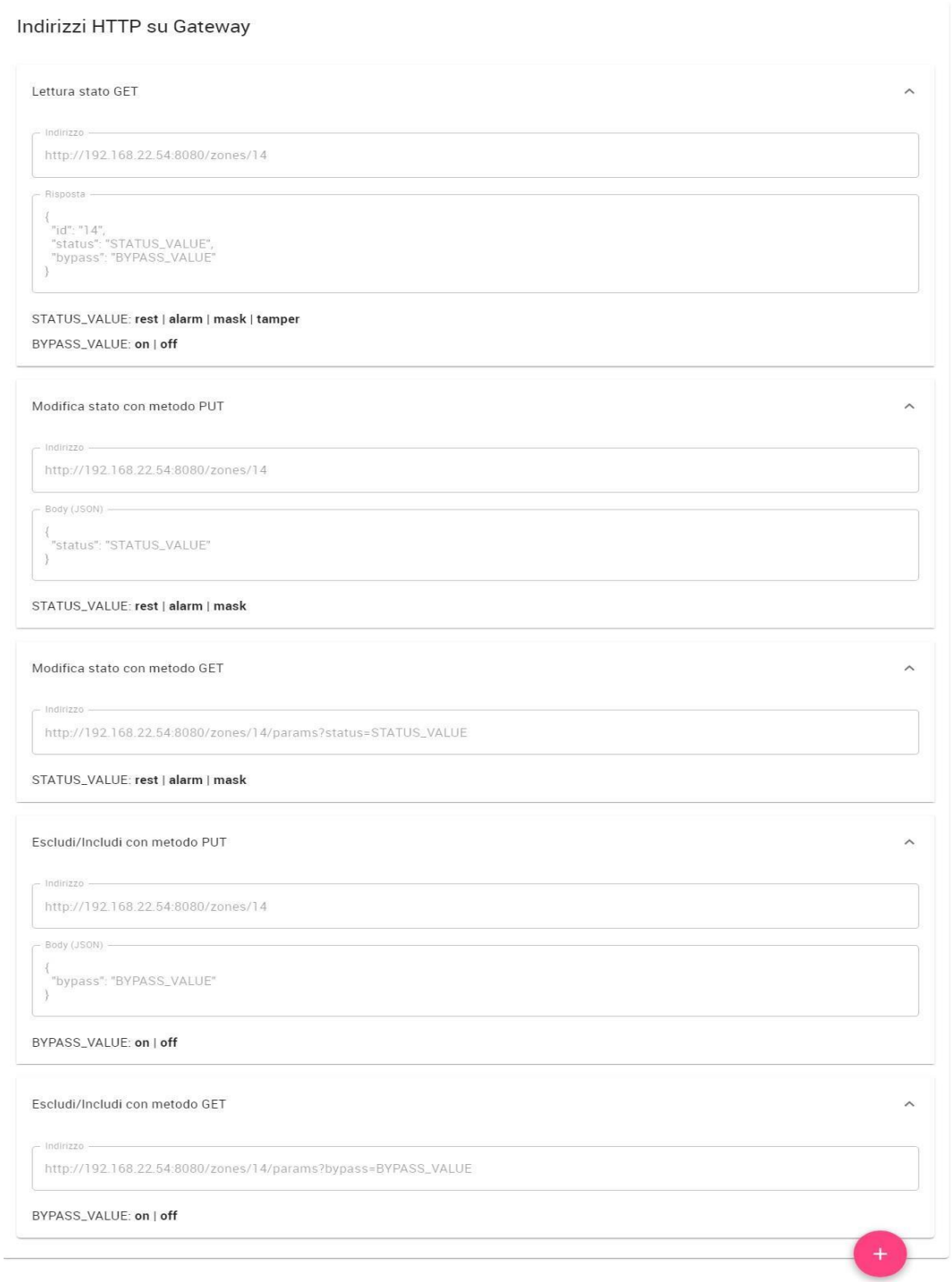

Figura 4 - Endpoints disponibili per ogni zona

Diagnostica della zona IP

Una delle funzionalità che introduce il gateway http, è la possibilità di diagnosticare lo stato di funzionamento del dispositivo IP di terze parti che dovrebbe inviare le richieste http relative ad una determinata zona.

Questa funzione consiste in:

- Configurare l'indirizzo IP del dispositivo che è programmato per inviare richieste http/s verso una determinata zona;
- Configurare il tempo, espresso in minuti, dopo il quale la zona viene considerata in scomparsa se il dispositivo NON risponde ai ping ICMP inviati dal gateway http.

Inserendo l'indirizzo IP si fa in modo che quella determinata zona possa essere "comandata" solo dalle richieste che arrivano dal dispositivo avente l'indirizzo IP configurato.

Sicurezza della connessione

Con il servizio gateway, a differenza della funzionalità "zone IP", è possibile autenticare i dispositivi di terze parti che possono inviare richieste al sistema.

L'autenticazione avviene per mezzo di un TOKEN da inserire nell'header http in un apposito campo che deve chiamarsi X-Auth-Token: questo TOKEN è una chiave esadecimale a 128 bit generata in modo random dalla centrale e che deve essere copiata nella configurazione del dispositivo di terze parti che dovrà inserirla nel campo X-Auth-Token di ogni richiesta.

Qui di seguito un esempio di una richiesta all'URL /ZONES/7/ALARM (allarme per la zona di ID=7) dove è stato inserito il campo X-Auth-Token: solo se il suo valore è uguale a quello presente in configurazione della centrale la richiesta viene elaborata.

```
GET /ZONES/7/ALARM http/1.1
Host: 192.168.22.54:8080

User-Agent: curl/7.75.0
Accept: */*

X-Auth-Token : 12d86348-bc39-4b8a-9fdf-745fca8cd10a

[Full request URI: http://192.168.22.54:8080/ZONES/7/ALARM]
```

Ovviamente, il massimo della sicurezza si ottiene configurando:

- Endpoint in HTTPS (tutte le richieste in ingresso sono cifrate)
- Autenticazione con TOKEN abilitata

- Per le zone, configurazione della supervisione specificando l'indirizzo IP del dispositivo da supervisionare.

Azioni http/s

Mentre gli endpoints http/s gestiscono le richieste in ingresso, le azioni sono le richieste che partono dalla centrale verso i dispositivi di terze parti a seguito di un evento che si verifica in centrale: gli eventi possono essere di qualsiasi tipo, come il cambio di stato di una partizione o di una zona ma anche il riconosciuto codice di un utente, e si configurano dall'interfaccia web di configurazione come se fossero dei normali scenari.

Per inviare una richiesta verso un dispositivo IP di terze parti deve essere configurata prima la RESOURCE, cioè le informazioni di contatto del dispositivo.

Una RESOURCE consiste in:

- Descrizione: campo che identifica il tipo di dispositivo con cui la centrale si interfaccia
- Indirizzo IP: indirizzo IP a cui risponde il dispositivo di terze parti; va specificato se la richiesta deve usare il protocollo http o https.
- Tipo di autenticazione: indica il tipo di autenticazione http richiesta dal dispositivo di terze parti. Può essere NESSUNA, BASIC o DIGEST. Negli ultimi due casi vanno specificati username e password per autenticarsi.

Una volta definita una RESOURCE vanno aggiunte le ACTIONs cioè gli URL verso cui inviare le richieste: ciascuna ACTION corrisponde a un singolo messaggio tra quelli accettati dal dispositivo di terze parti con il quale ci si interfaccia. Il formato di tale messaggio dipende dal dispositivo stesso e generalmente è riportato nella documentazione oppure si può personalizzare nell'interfaccia di configurazione del dispositivo stesso.

Nella definizione della ACTION è possibile scegliere il metodo http della richiesta tra GET, PUT, POST e DELETE e l'eventuale campo BODY della richiesta.

La Figura 5 mostra l'interfaccia di configurazione web di una centrale lares 4.0 dove si possono notare:

- La scelta del protocollo https per gli endpoints messi a disposizione dal servizio;
- L'abilitazione dell'autenticazione http attraverso il TOKEN e il TOKEN stesso generato dalla centrale;
- La configurazione di una RESOURCE con la relativa descrizione, l'indirizzo IP (in questo caso il dispositivo richiede una connessione https e per comodità è stato riportato insieme all'indirizzo anche la parte comune degli URL delle singole ACTIONs), l'autenticazione verso il dispositivo di tipo BASIC e i relativi username e password.

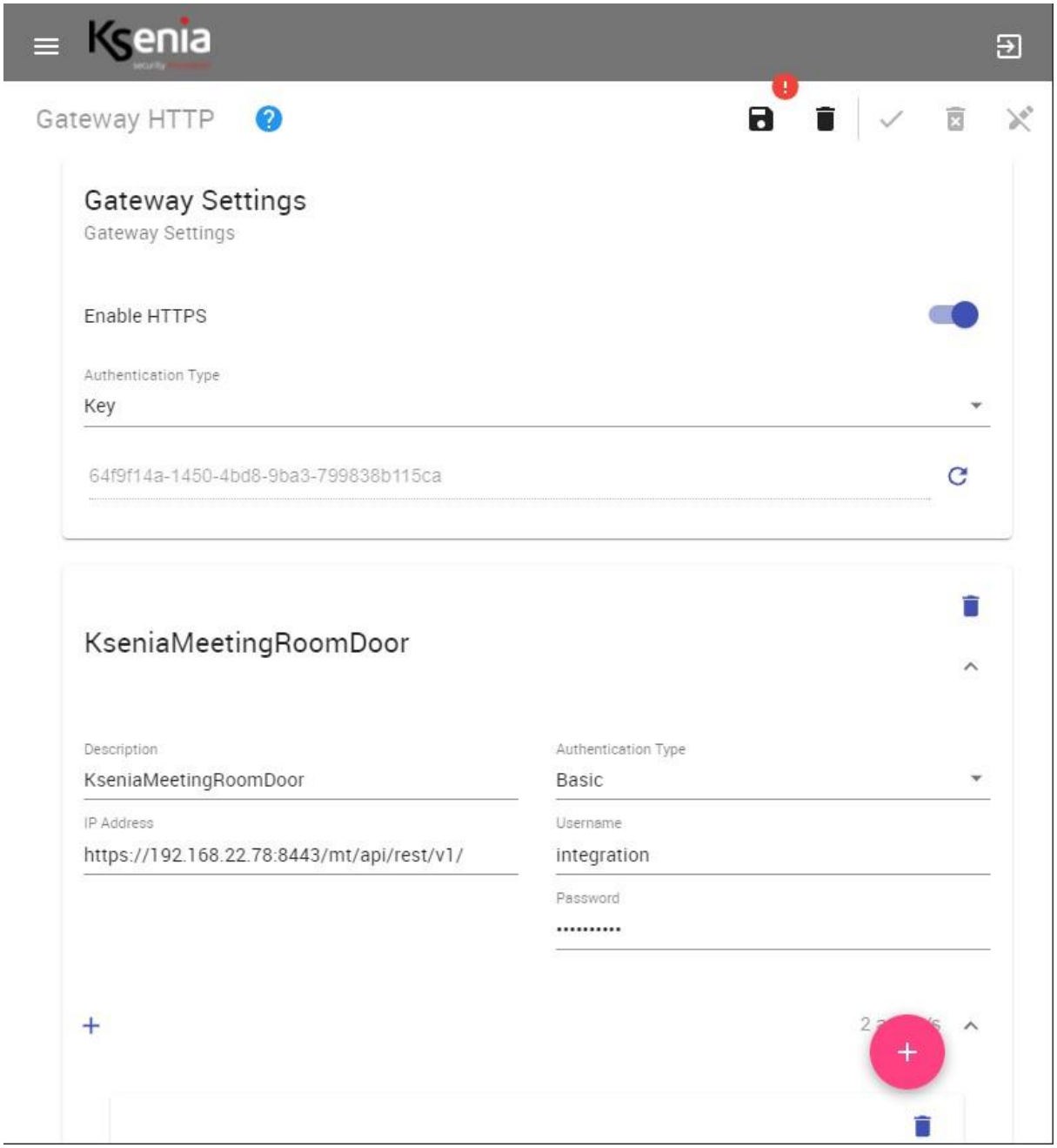

Figura 5 - Configurazione gateway http e risorsa

Una volta definita la RESOURCE, l'interfaccia permette di aggiungere le vari ACTIONs per quel dispositivo: come ultimo passo della configurazione, queste ultime andranno associate agli eventi della centrale nella relativa pagina di configurazione di quest'ultimi.

La Figura 6 mostra la configurazione di due ACTIONs per la stessa RESOURCE: per entrambe il dispositivo prevede una richiesta di tipo PUT (sugli URL /alarm e /bookmark) che devono prevedere

nel body un JSON predefinito. L'interfaccia di configurazione della centrale lares 4.0 permette di inserire qualunque testo garantendo la massima flessibilità.

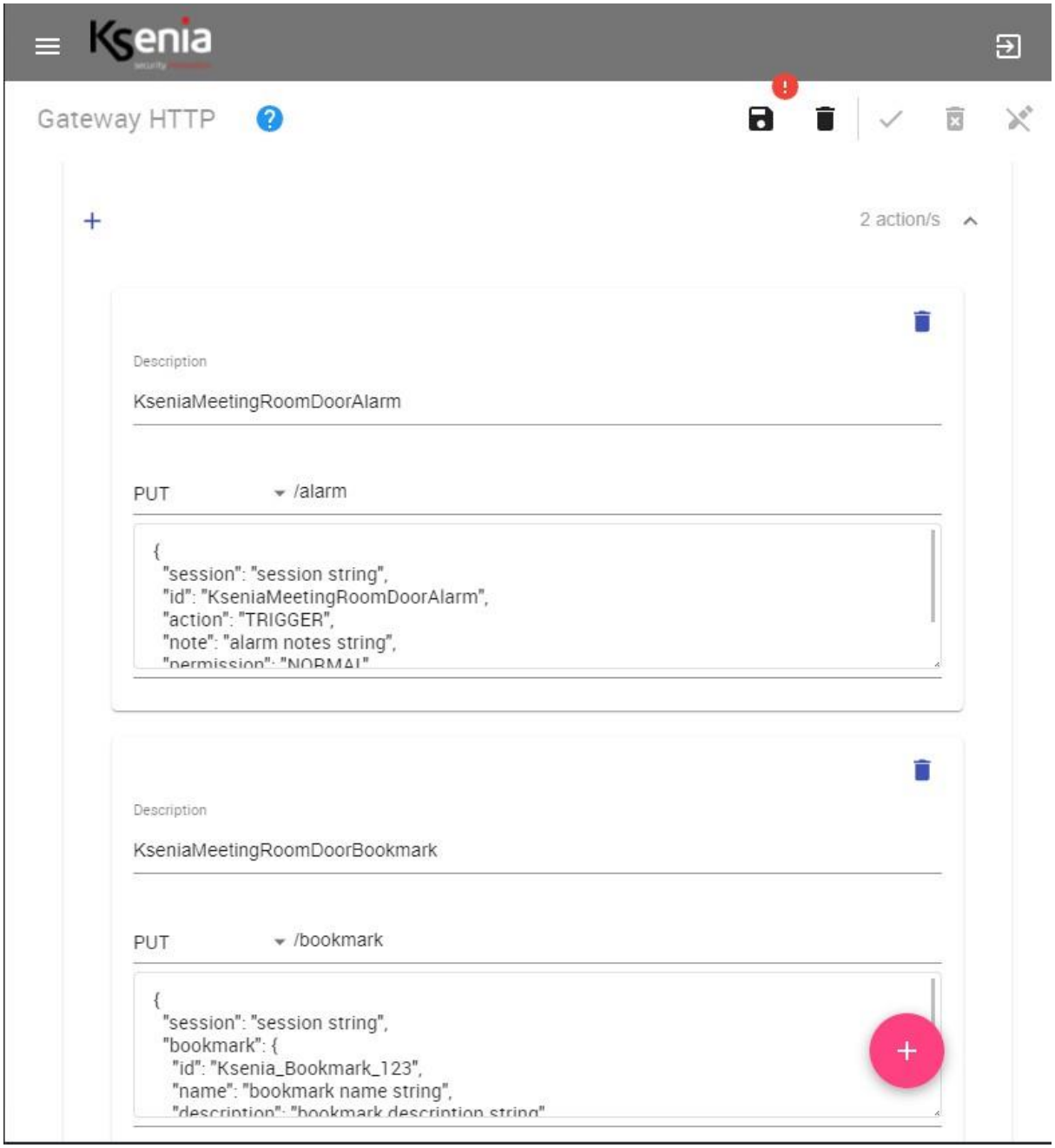

Figura 6 - ACTIONS per una specifica RESOURCE

Porte in ascolto

La Tabella 4 riporta tutte le porte TCP e UDP utilizzate dalla centrale lares 4.0 e dalla periferica *porta IoT*. Tra di esse sono specificate anche le porte utilizzate per mettere in comunicazione bidirezionale la centrale e il *porta IoT* attraverso due protocolli che saranno descritti nei rispettivi paragrafi.

lares 4.0	porta IoT	Funzionalità
tcp/69	-	SERVER http per zone IP in centrale
tcp/80	tcp/8080	SERVER http per configurazione su lares 4.0 e per gateway http su porta IoT
tcp/443	tcp/8443	SERVER https per configurazione su lares 4.0 e per gateway https su porta IoT
udp/4998	-	SERVER per protocollo proprietario KSIP_PROT
-	udp/4996	CLIENT per il protocollo proprietario KSIP_PROT
udp/5683	udp/5683	CLIENT/SERVER per protocollo CoAP

Tabella 4 - Porte TCP e UDP utilizzate