

**UTILIZZO E CONFIGURAZIONE API HTTP CON SCHEDA PRIMELAN.  
VERSIONE DOCUMENTO: 1.00 DEL 22/04/2022**

Questa documentazione ha lo scopo di descrivere il funzionamento e la configurazione delle API https che rendono la centrale Prime (equipaggiata con scheda PrimeLan 3.10) compatibile con tutti i dispositivi ed applicazioni di terze parti che sfruttano tale protocollo.

**DESCRIZIONE DELLE FUNZIONALITÀ**

Dalla sua versione 3.10 la scheda PrimeLan può comunicare con dispositivi di terze parti tramite un protocollo https.

Tale caratteristica consente a qualsiasi dispositivo supporti tale funzionalità di:

1. Visualizzare la versione delle API
2. Effettuare un test di connessione verso la centrale
3. Conoscere lo stato di ogni zona di centrale
4. Conoscere lo stato delle uscite
5. Conoscere lo stato delle aree
6. Conoscere la lista degli scenari
7. Ottenere il log eventi di centrale
8. Visualizzare lo stato del dispositivo GSM/3G/4G collegato in centrale
9. Visualizzare i guasti di sistema
10. Visualizzare l'elenco delle zone "aperte" di una data area
11. Visualizzare l'elenco delle zone "aperte" di un dato scenario
12. Attivare/disattivare uscite
13. Escludere/includere zone\*
14. Inserire/disinserire aree\*
15. Applicare scenari di inserimento
16. Cancellare memorie di allarme

\* Funzioni che per motivi di sicurezza devono essere abilitate esplicitamente

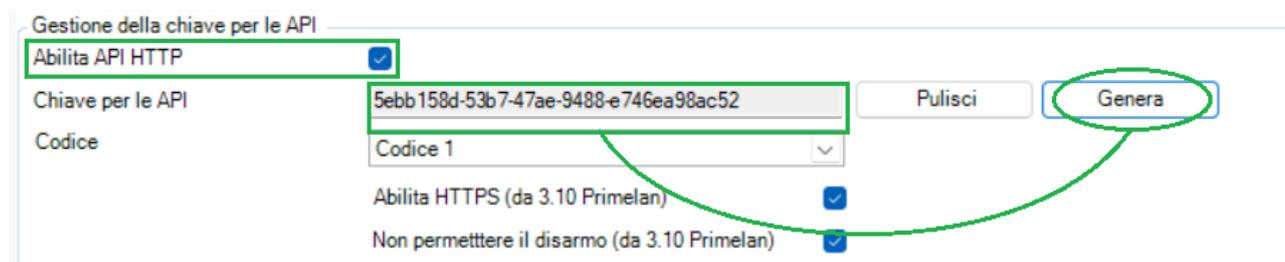
Una applicazione tipica di tali funzionalità è quella che consente ad una telecamera IP di attivare uscite di centrale o generare eventi a seguito di una specifica rilevazione.

L'utilizzo di questo protocollo può essere utilizzato anche da un generico software di supervisione per monitorare lo stato dell'impianto.

## CONFIGURAZIONE SISTEMA E LISTA COMANDI

Per poter sfruttare questa funzionalità è necessario che sulla centrale Prime sia connessa una scheda di rete PrimeLan con versione FW 3.10 o successiva.

Una volta configurati i parametri di rete, tramite il software PrimeStudio aprire la pagina di configurazione della PrimeLan, abilitare le API HTTP e cliccare sul pulsante “Genera” per ottenere una “Apikey”.



Una volta effettuata questa breve configurazione sarà possibile inviare alla centrale il comando http per effettuare l’operazione richiesta.

La formattazione del comando deve seguire il seguente schema:

[https://ip\\_centrale/cgi-bin/api.cgi?apikey=apikey\\_generata&cmd=](https://ip_centrale/cgi-bin/api.cgi?apikey=apikey_generata&cmd=)

[http://ip\\_centrale/cgi-bin/api.cgi?apikey=apikey\\_generata&cmd=](http://ip_centrale/cgi-bin/api.cgi?apikey=apikey_generata&cmd=) (nel caso di HTTPS disabilitato)

**N.B.** Per motivi di sicurezza, Inim consiglia sempre l'utilizzo della connessione con crittografia SSL (https) abilitata. Qualora fosse necessario disattivare tale crittografia, è consigliabile generare una nuova APIKEY ogni 90 giorni.

dove:

- “**ip\_centrale**” deve essere sostituito con l’indirizzo IP della centrale (o del gateway in caso di connessioni p2p da remoto)
- “**apikey\_generata**” deve essere sostituito con la chiave API che appare sul software PrimeStudio al momento della pressione del tasto “Genera” nella fase di abilitazione delle API http.

A questa stringa che può essere considerata “fissa” devono seguire i vari comandi con i rispettivi parametri che consentono di operare in centrale.

Elenchiamo di seguito la sintassi dei vari comandi.

**1)VISUALIZZARE LA VERSIONE DELLE API**

Comando da inviare in centrale	
<b>Comando</b>	“version”
<b>Parametri</b>	

Esempio: <https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=version>

Risposta dalla centrale	
<b>Parametro</b>	<b>Valori</b>
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	Version: X: //versione delle API

**2)EFFETTUARE UN TEST DI CONNESSIONE VERSO LA CENTRALE**

Comando da inviare in centrale	
<b>Comando</b>	“ping”
<b>Parametri</b>	

Esempio: <https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=ping>

Risposta dalla centrale	
<b>Parametro</b>	<b>Valori</b>
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	pong: //comunicazione avvenuta con successo

### 3) CONOSCERE LO STATO DELLE ZONE DI CENTRALE

Comando da inviare in centrale	
Comando	“get_zones_status”
Parametri	

Esempio: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_zones\\_status](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_zones_status)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"lb": // nome della zona "tl": // terminale della zona "st": // stato della zona {0 = guasto, 1 = pronta, 2 = allarme, 3 = corto circuito} "mm": // memoria allarmi di zona {0 = non presente, 1 = presente} "by": // esclusione di zona: {0 = esclusa, 1 = non esclusa} "id": // id della zona  N.B. Tali info vengono elencate per ogni zona di centrale

### 4) CONOSCERE LO STATO DELLE USCITE

Comando da inviare in centrale	
Comando	“get_outputs_status”
Parametri	

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_outputs\\_status](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_outputs_status)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione

	5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	<p>"lb": // nome dell'uscita            "tl": // id del terminale di uscita            "st": // stato dell'uscita {0 = off, 1 = on, 0-100: solo se dimming}            "t": // tipologia di uscita {0 = normale/ibrida, 1 = dimming, 2 = DAC, 3 = 0-10V }            "id": // id uscita</p> <p>Se l'uscita è di tipo dimming vengono aggiunti i seguenti parametri:</p> <ul style="list-style-type: none"> <li>• v: voltaggio;</li> <li>• p: potenza</li> <li>• c: <math>\cos(\phi)</math> sfasamento</li> </ul> <p>N.B. Tali info vengono elencate per ogni uscita di centrale</p>

## 5) CONOSCERE LO STATO DELLE AREE

Comando da inviare in centrale	
Comando	"get_partitions_status"
Parametri	

Es: [https://192.168.1.980/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_partitions\\_status](https://192.168.1.980/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_partitions_status)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	<p>"lb": // nome area            "am": // modalità di inserimento {1 = totale, 2 = parziale, 3 = istantanea, 4 = disinserita}            "st": // stato area {0 = allarme, 1 = pronta, 2 = sabotaggio}            "mm": // memoria di allarme {0 = non presente, 1 = presente}            "id": // id dell'area</p> <p>N.B. Tali info vengono elencate per ogni area di centrale</p>

## 6) CONOSCERE LA LISTA DEGLI SCENARI

Comando da inviare in centrale	
Comando	"get_scenarios_status"
Parametri	

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_scenarios\\_status](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_scenarios_status)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"lb": //nome scenario "st": // stato dello scenario {0 = non attivo, 1 = attivo} "id": // id scenario  N.B. Tali info vengono elencate per ogni scenario di centrale

## 7) OTTENERE IL LOG EVENTI DI CENTRALE

Comando da inviare in centrale	
Comando	"get_log_elements"
Parametri	"p1": //numero da 1 a 4000 che indica il numero di eventi che si vogliono ottenere

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_log\\_elements&p1=4000](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_log_elements&p1=4000)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato

Data	"id": // id dell'evento "dt": // data e ora dell'evento "ty": // tipologia evento "ag": // agente dell'evento (chi ha generato l'evento) "lo": // luogo dell'evento "v": // <i>uso futuro</i>
------	--

## 8) VISUALIZZARE LO STATO DEL NEXUS

Comando da inviare in centrale	
Comando	"get_gsm_status"
Parametri	

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_gsm\\_status](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_gsm_status)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"vcc": // tensione di alimentazione "fwv": // versione del firmware "gop": // operatore telefonico "gpw": // campo "cre": // credito

## 9)VISUALIZZARE I GUASTI DI SISTEMA

Comando da inviare in centrale	
Comando	“get_faults_status”
Parametri	

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_faults\\_status](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_faults_status)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	<pre> "vcc": // tensione di alimentazione "fau": // bitmap dei guasti: { //byte 0 byte s_disponibile_1 :1; /* byte s_disponibile_2 :1; /* byte s_low_battery :1; /* byte s_guasto_rete :1; /* byte s_no_linetel :1; /* byte s_jam_radio :1; /* byte s_low_bat_wls :1; /* byte s_ev_scomparsa_wls :1; /*  //byte 1 byte s_guasto_gsm :1; /* byte s_sensore_sporco :1; /* byte s_zone_guasto :1; /* byte s_sirene :1; /* byte s_alimentatore :1; /* byte s_tastiera_radio :1; /* byte s_scomp_sab :1; /* byte s_scomp_internet :1; /* }           </pre>

### 10) VISUALIZZARE LE ZONE APERTE DI UNA SPECIFICA AREA

Comando da inviare in centrale	
<b>Comando</b>	“get_partitions_nrz”
<b>Parametri</b>	“p1”: // ID area
	“p2”: // tipo di inserimento area {1 = totale, 2 = parziale, 3 = istantaneo}

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_partitions\\_nrz&p1=2&p2=1](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_partitions_nrz&p1=2&p2=1)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"id": // id della zona "lb": // nome della zona

### 11) VISUALIZZARE LE ZONE APERTE DI UNO SPECIFICO SCENARIO DI INSERIMENTO

Comando da inviare in centrale	
<b>Comando</b>	“get_scenarios_nrz”
<b>Parametri</b>	“p1”: // ID scenario

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get\\_scenarios\\_nrz&p1=3](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=get_scenarios_nrz&p1=3)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"id": // id della zona "lb": // nome della zona

**12) ATTIVARE/DISATTIVARE USCITE**

<b>Comando da inviare in centrale</b>	
<b>Comando</b>	“set_outputs_mode”
<b>Parametri</b>	<p>“p1”: // ID dell’uscita</p> <p>Valori possibili per il parametro p1:</p> <ul style="list-style-type: none"> <li>• Da 0 a 9 terminali presenti in centrale</li> <li>• Da 10 a 509 Numerazione lineare terminali su moduli di espansione: 10 = Modulo di espansione 1 terminale 1 509 = Modulo di espansione 100 terminale 5</li> <li>• Da 510 a 569 Numerazione lineare terminali su tastiere 510 = Tastiera 1 terminale 1 569 = Tastiera 30 terminale 2</li> <li>• Da 585 a 704 Moduli domotici 585 = Modulo domotico 1 terminale 1 704 = Modulo domotico 30 terminale 4 (Relè SW2)</li> <li>• Da 705 a 764 terminali su nuovi lettori 705 = Terminale lettore 1 (solo Nby/K) 764 = Terminale lettore 60</li> <li>• Da 955 a 974 terminali su stazioni di alimentazione ISOPOWER gestite dalla versione 3.10 di Prime 955 = Stazione di alimentazione 1 Terminale 1 974 = Stazione di alimentazione 10 Terminale 2</li> <li>• Da 985 a 999 terminali virtuali 985 = Terminale virtuale 1 999 = Terminale virtuale 15</li> </ul>
	“p2”: // valore dell’uscita {0: off, 1 = on, 1÷100 valore dimming}

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set\\_outputs\\_mode&p1=15&p2=0](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set_outputs_mode&p1=15&p2=0)

<b>Risposta dalla centrale</b>	
<b>Parametro</b>	<b>Valori</b>
<b>Status</b>	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell’autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
<b>Data</b>	"Data": "OK" //se la modifica è andata a buon fine

### 13) ESCLUDERE/INCLUDERE ZONE

Comando da inviare in centrale	
<b>Comando</b>	“set_zones_mode”
<b>Parametri</b>	<p>“p1”: // ID della zona</p> <p>Valori possibili per il parametro p1:</p> <ul style="list-style-type: none"> <li>• Da 0 a 9 terminali presenti in centrale</li> <li>• Da 10 a 509 Numerazione lineare terminali su moduli di espansione: 10 = Modulo di espansione 1 terminale 1 509 = Modulo di espansione 100 terminale 5</li> <li>• Da 510 a 569 Numerazione lineare terminali su tastiere 510 = Tastiera 1 terminale 1 569 = Tastiera 30 terminale 2</li> <li>• Da 585 a 704 Moduli domotici 585 = Modulo domotico 1 terminale 1 704 = Modulo domotico 30 terminale 4 (Relè SW2)</li> <li>• Da 705 a 764 terminali su nuovi lettori 705 = Terminale lettore 1 (solo Nby/K) 764 = Terminale lettore 60</li> <li>• Da 985 a 999 terminali virtuali 985 = Terminale virtuale 1 999 = Terminale virtuale 15</li> </ul> <p><b>Inclusione/esclusione delle zone doppie</b> Per gestire l'esclusione/inclusione delle zone doppie bisogna aggiungere al parametro p1 il numero 1005, quindi ad esempio se si desidera escludere la zona 10 doppia di centrale, il parametro p1 sarà: <math>1005 + 9 = 1014</math></p>
	“p2”: // stato dell'esclusione {0 = inclusa, 1 = esclusa}

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set\\_zones\\_mode&p1=122&p2=1](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set_zones_mode&p1=122&p2=1)

Risposta dalla centrale	
Parametro	Valori
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell'autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione

	5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"Data": "OK" //se la modifica è andata a buon fine

## 14)INSERIRE/DISINSERIRE AREE

Comando da inviare in centrale	
<b>Comando</b>	“set_partitions_mode”
<b>Parametri</b>	“p1”: // ID dell’area
	“p2”: // modalità di inserimento { 1= totale, 2= parziale, 3= istantanea, 4= disinserita, 5= cancella memoria allarme }
	La modalità di armamento 4(disinserita) è soggetta all’abilitazione del flag “Non autorizzare alle API il bypass/disarmaneto delle zone” sul software Prime/STUDIO

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set\\_partitions\\_mode&p1=4&p2=1](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set_partitions_mode&p1=4&p2=1)

Risposta dalla centrale	
<b>Parametro</b>	<b>Valori</b>
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell’autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"Data": "OK" //se la modifica è andata a buon fine

## 15)APPLICARE SCENARI DI INSERIMENTO

Comando da inviare in centrale	
<b>Comando</b>	“set_scenarios_mode”
<b>Parametri</b>	“p1”: // ID dello scenario da attivare

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set\\_scenarios\\_mode&p1=3](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set_scenarios_mode&p1=3)

Risposta dalla centrale	
<b>Parametro</b>	<b>Valori</b>
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell’autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"Data": "OK" //se la modifica è andata a buon fine

## 16) CANCELLARE LE MEMORIE DI ALLARME

Comando da inviare in centrale	
<b>Comando</b>	“set_partitions_mode”
<b>Parametri</b>	“p1”: // ID dell’area
	“p2”: // inserendo il valore 5 al parametro si avrà la cancellazione delle memorie di area

Es: [https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set\\_partitions\\_mode&p1=4&p2=5](https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&cmd=set_partitions_mode&p1=4&p2=5)

Risposta dalla centrale	
<b>Parametro</b>	<b>Valori</b>
Status	0 - SUCCESS: comando ok 1 - ERROR_PARAM: errore nei parametri 2 - ERROR_APIKEY: errore nell’autenticazione 3 - ERROR_COMMAND: errore comando 4 - ERROR_EXECUTION: errore di comunicazione 5 - ERROR_PROTOCOL: HTTPS richiesto 6 - ERROR_AUTHORIZATION: non autorizzato
Data	"Data": "OK" //se la modifica è andata a buon fine

## ESEMPIO DI PROGRAMMAZIONE DI TELECAMERA IP

Uno degli utilizzi più frequenti di queste API, riguarda la programmazione di telecamere IP che possono generare eventi in centrale o attivare direttamente delle uscite.

Di seguito viene mostrato un esempio di tale configurazione.  
La telecamera in oggetto è la Hikvision modello DS-2CD2126G2-I.

Dopo aver configurato la centrale e la PrimeLan con l'attivazione delle API e la generazione dell'APIKEY, possiamo procedere come segue:

- Accedere alla pagina web della telecamera.
- Portarsi nella sezione "Configurazioni".

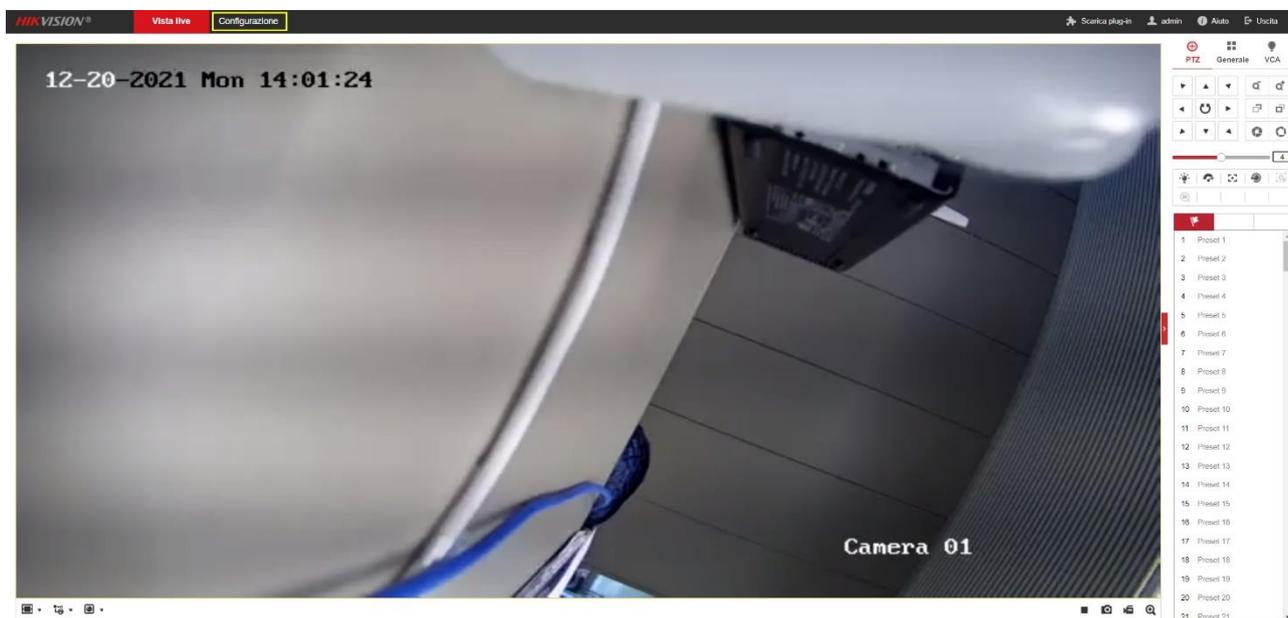


Figura 1:View Camera

- Passare al pannello “Rete”

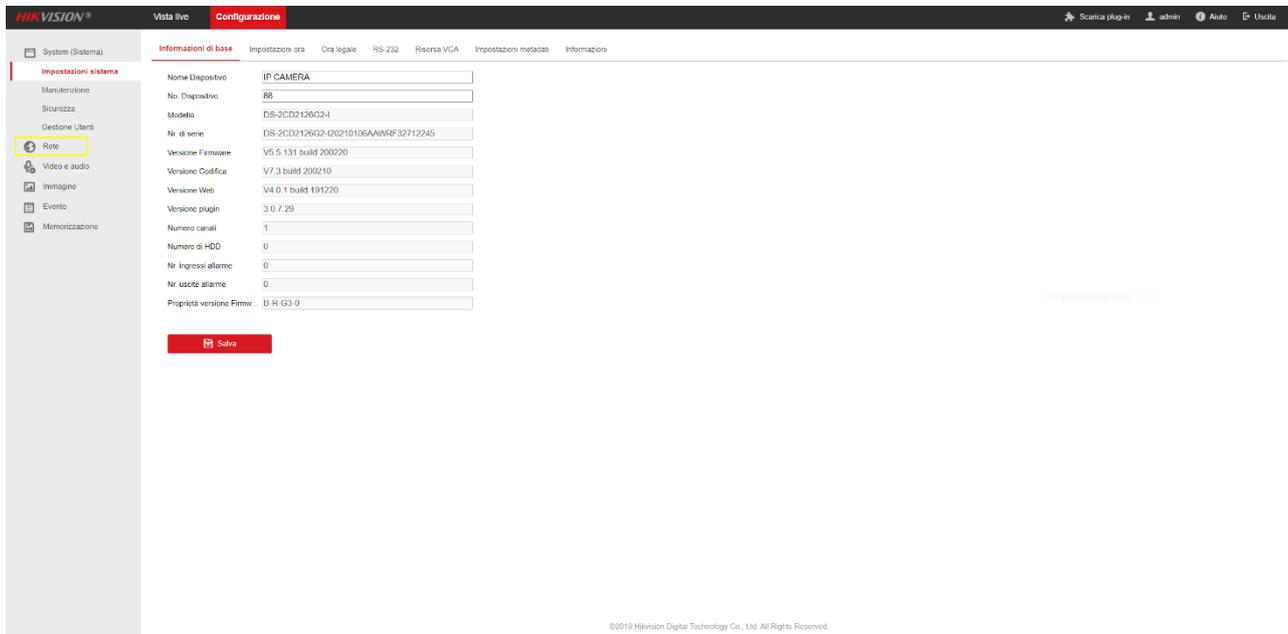


Figura 2: Rete

- Passare alla sezione “Security Control Panel Configuration”

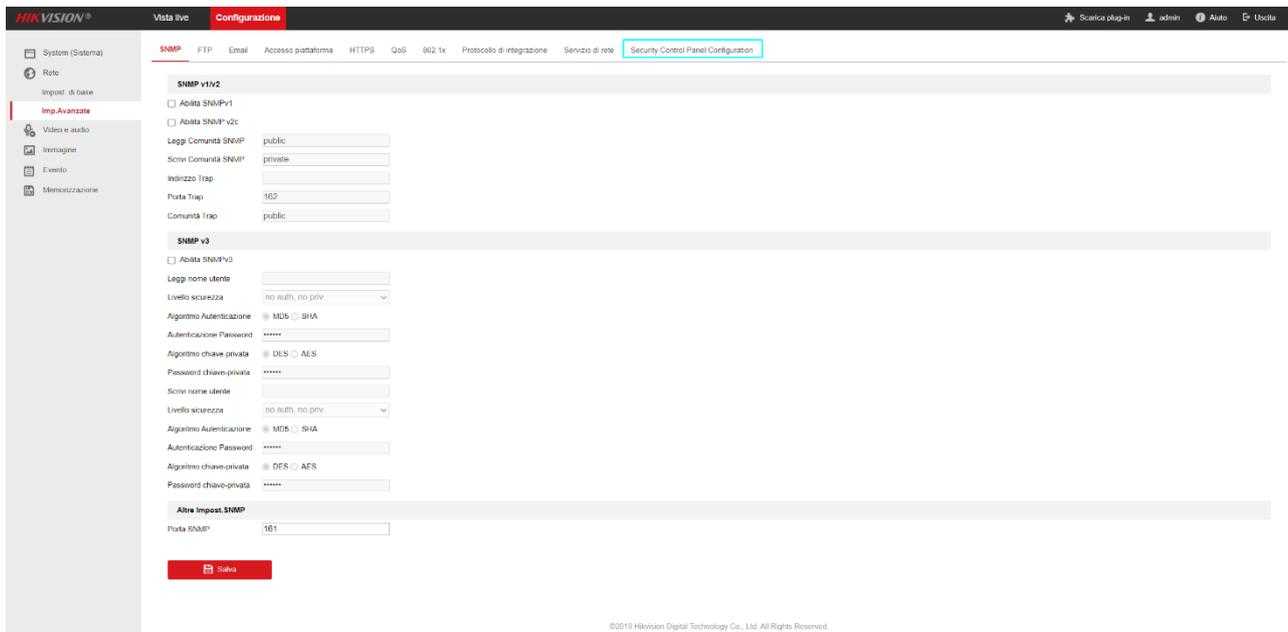


Figura 3:Rete Avanzata

- Nella sezione “Security Control Panel Configuration” troviamo una tabella da poter configurare i comandi da inviare in centrale.

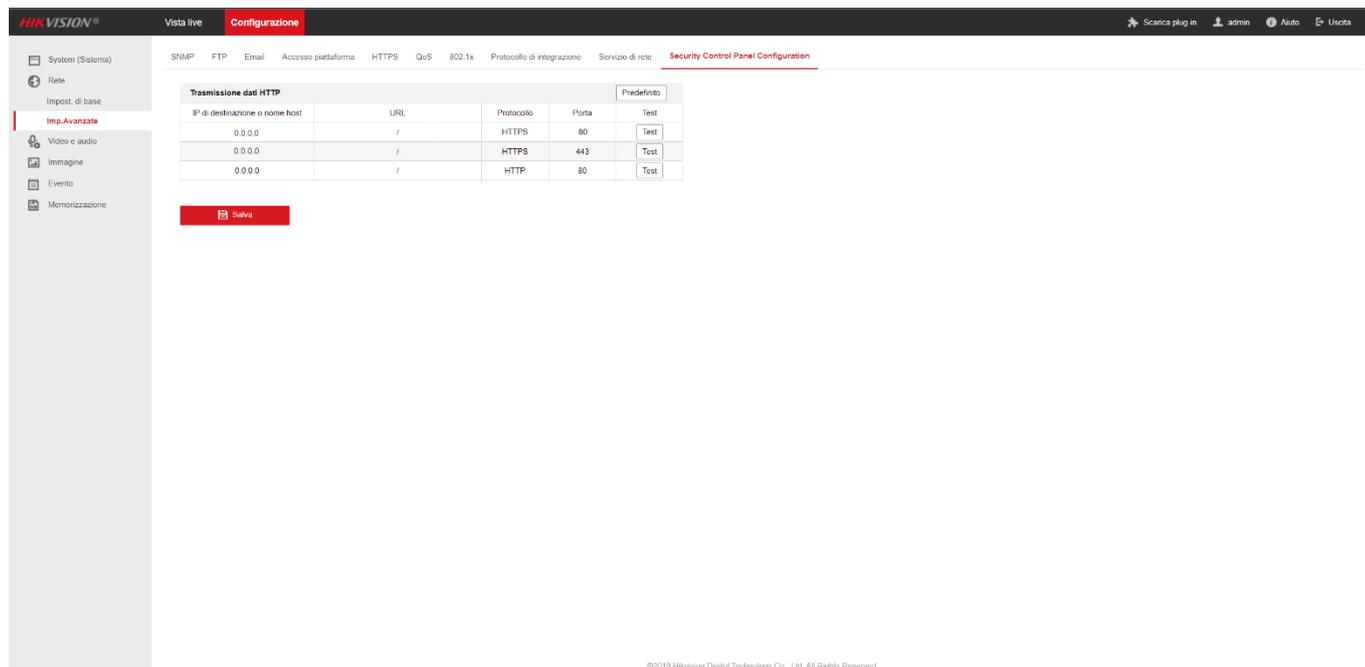


Figura 4: Configurazione Stringa HTTPS

Seguendo le tabelle dei comandi descritte nei capitoli precedenti, se volessimo attivare un'uscita di centrale dovremmo compilare una delle righe di questa tabella in questo modo:

IP di destinazione	URL	Protocollo	Porta
192.168.1.98	<code>https://192.168.1.98/cgi-bin/api.cgi?apikey=5ebb158d-53b7-47ae-9488-e746ea98ac52&amp;cmd=set_outputs_mode&amp;p1=1&amp;p2=1</code>	HTTPS	443

In questo specifico esempio, nel momento in cui la telecamera dovesse inviare questa stringa in centrale, si avrà l'attivazione dell'uscita con ID=1

Questo modello di telecamera permette di configurare un massimo di 3 IP di destinazioni diversi o di abilitare 3 comandi differenti.

Questi comandi vengono inviati per eventi che possono essere programmati sulla telecamera stessa. Un esempio può riguardare la programmazione una zona di rilevazione: L'attraversamento di tale zona da parte di una persona può scatenare l'evento che tramite le API descritte può attivare un'uscita di centrale.