

AIBOX-PRO - Device Management Portal (DMP) guide

(A partire dalla versione firmware 104210)

(La funzione **6. Accesso Remoto** non è disponibile per gli ZN-AIBOX-STD)

1. Descrizione

Il **Device Management Portal (DMP)** è una piattaforma web che consente la gestione centralizzata dei dispositivi AIBOX.

Il portale permette di:

- Creare accessi con differenti autorizzazioni: utenti e partner.
- Accedere alla pagina web dei dispositivi AIBOX-PRO.
- Eseguire aggiornamenti firmware senza accesso al dispositivo.
- Gestire database dei dispositivi senza accesso al dispositivo.
- Configurare azioni automatiche su eventi di sistema: inaccessibilità.

L'utilizzo del DMP è particolarmente indicato per installazioni distribuite su più siti geografici e per attività di supporto tecnico remoto.

2. Utenti e partner

L'organizzazione prevede la creazione di **partner** ed **utenti**, tramite i quali si possono aggiungere e gestire i singoli AIBOX.

Gli **utenti** sono creati dai partner, e si distinguono in due ruoli:

- **USER**, con accesso più limitato: può aggiungere ed accedere agli AIBOX.
- **ADMIN**, con privilegi estesi: può visualizzare e creare altri utenti, aggiungere e modificare AIBOX, visualizzare le informazioni sul proprio partner, può limitare la visualizzazione a determinati AIBOX per ogni utente USER con lo stesso codice partner (vedi punto **8. Gestione utenti**).

Es.1:

- *Azienda1* e *Azienda2* chiedono l'accesso al DMP come partner.
- Gli utenti di *Azienda1* non vedranno gli AIBOX né gli utenti di *Azienda2* e viceversa.
- *Azienda1* e *Azienda2* non potranno creare nuovi partner, ma potranno creare degli utenti (USER e ADMIN) che potranno accedere e visualizzare tutti i loro dispositivi.

Es. 2:

- Un **partner** ha creato diversi utenti, tra cui **Milano1**.
- **Milano1** aggiunge un dispositivo.
- Esso sarà visibile ed accessibile **da tutti gli utenti del partner**.

Dal punto di vista operativo degli **utenti**:

1. Il **nome utente** può essere modificato dagli ADMIN.
2. La **password** è gestita solo dal singolo utente (ADMIN o USER).
3. Gli **ADMIN** possono creare nuovi utenti (sia USER che ADMIN).
4. Sia USER che ADMIN sono autorizzati ad aggiungere nuovi dispositivi AIBOX.

3. Registrazione dispositivi

Al primo avvio di AIBOX, verrà richiesto l'inserimento del **Partner Code** e del **Passcode**, che dovranno essere richiesti a **CBC**.

Con questi codici AIBOX, verrà registrato nel Device Management Portal.

Per poter registrare ed usare il dispositivo nel portale, AIBOX necessita di una connessione internet.

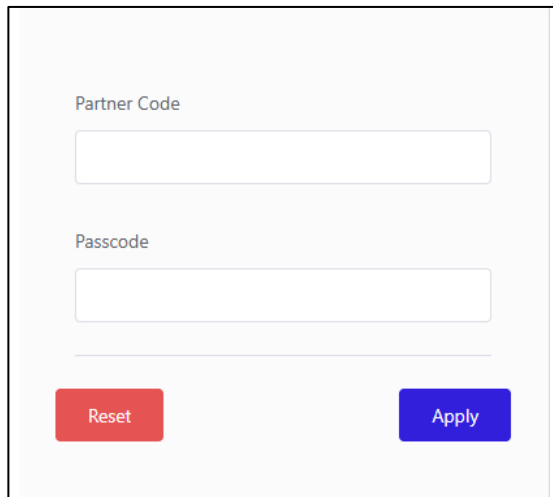
Nel caso in cui il dispositivo sia protetto da un firewall, è necessario abilitare le seguenti eccezioni, autorizzando i relativi elementi:

- Porta **443** per **api.ailn.io**
- Porta **48883** per **br2.mq.noif-fnc.ailn.io**
- **Tutte le porte** per **api.eu1.p.ailn.io**

Se non si è inserito il codice durante l'installazione di AIBOX o se si è aggiornato il firmware di un dispositivo già in funzione, si può accedere alla pagina del dispositivo AIBOX scrivendo l'indirizzo IP nel seguente modo:

<https://192.168.X.X:8443/#pages/cpcode>

Apparirà la pagina seguente relativa l'inserimento di Partner Code e Passcode.



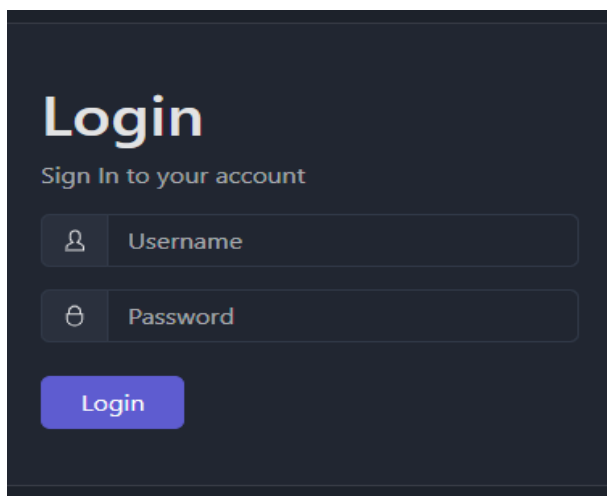
The screenshot shows a web form for registration. It has two input fields: 'Partner Code' and 'Passcode'. Below the 'Passcode' field is a horizontal line. At the bottom of the form are two buttons: a red 'Reset' button on the left and a blue 'Apply' button on the right.

4. Accesso al DMP

La gestione dei dispositivi rappresenta una delle funzionalità principali del DMP. Dopo aver effettuato l'accesso al portale tramite il seguente link,

<https://device.portal.ailn.io/#/pages/login>

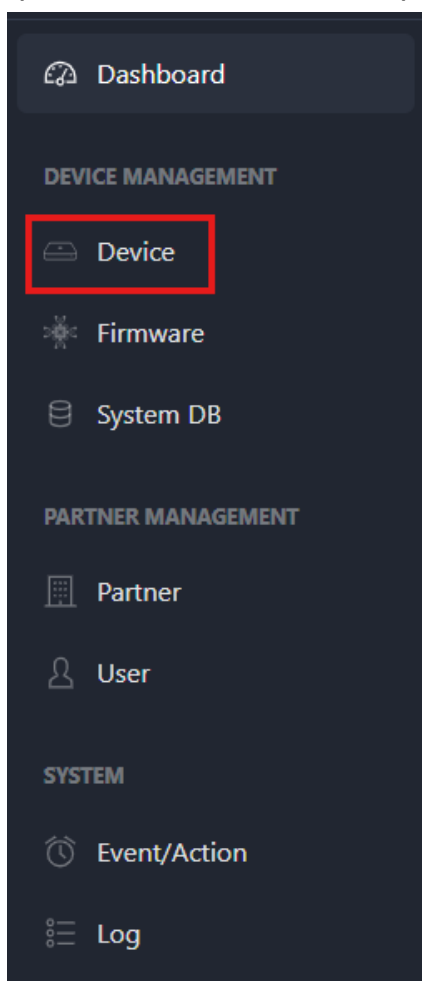
sarà possibile accedere tramite le credenziali rilasciate precedentemente assieme al Partner Code ed il Passcode.



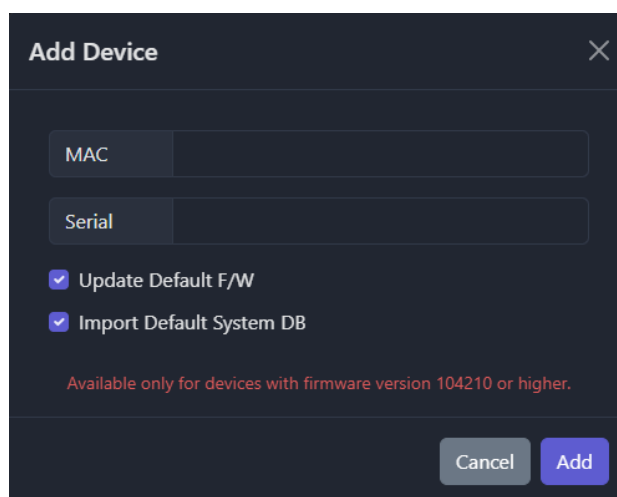
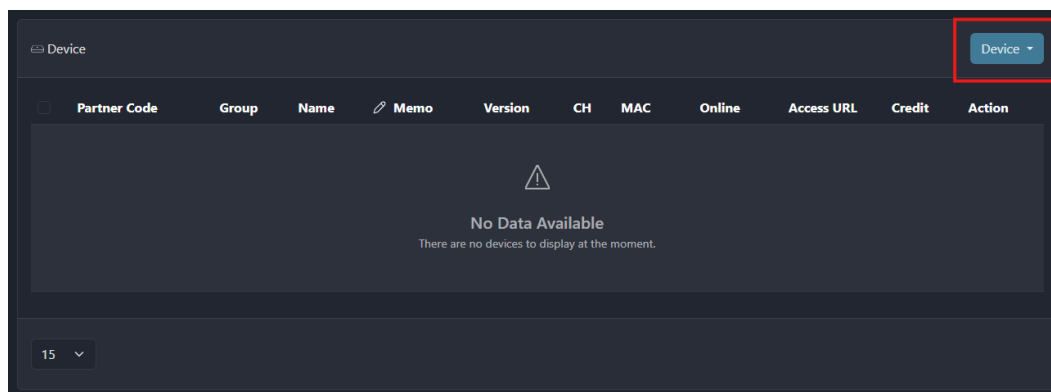
A dark-themed login interface. At the top, the word "Login" is displayed in a large, white, sans-serif font. Below it, the text "Sign In to your account" is in a smaller, lighter font. There are two input fields: the first is labeled "Username" with a person icon, and the second is labeled "Password" with a lock icon. Both fields have a light gray border. Below the fields is a blue button with the text "Login" in white.

5. Registrazione degli AIBOX.

Per aggiungere un dispositivo, premere **Device** nel menu principale.



Per aggiungere il proprio dispositivo, premere il tasto **Device** sulla destra.
ZN-AIBOX2



Durante l'aggiunta del dispositivo, il portale consente di selezionare se effettuare l'aggiornamento del **firmware (FW)** ad una versione di default e l'importazione del **database (DB)**.

6. Accesso remoto

Dal punto di vista operativo, ogni dispositivo dispone di un **menu azione** (accessibile tramite  a fine riga).

Descrizione delle azioni:

 Update	...
 System DB Import	...
 System DB Export	...
 Reboot	...
 Group Setting	...
 Open Remote Access	
 Close Remote Access	
 Delete	

- **Update:** aggiornare il firmware.
- **System DB:** importare o esportare la configurazione.
- **Reboot:** riavviare il dispositivo.
- **Group Setting:** aggiungere o togliere da uno o più gruppi.
Nota: I **gruppi**, consentono di filtrare la visualizzazione degli AIBOX o procedere con l'aggiornamento contemporaneo.
- **Remote Access:** abilitare o disabilitare il link alla pagina web.
Nota: Se disabilitato, si impedisce qualsiasi accesso remoto.

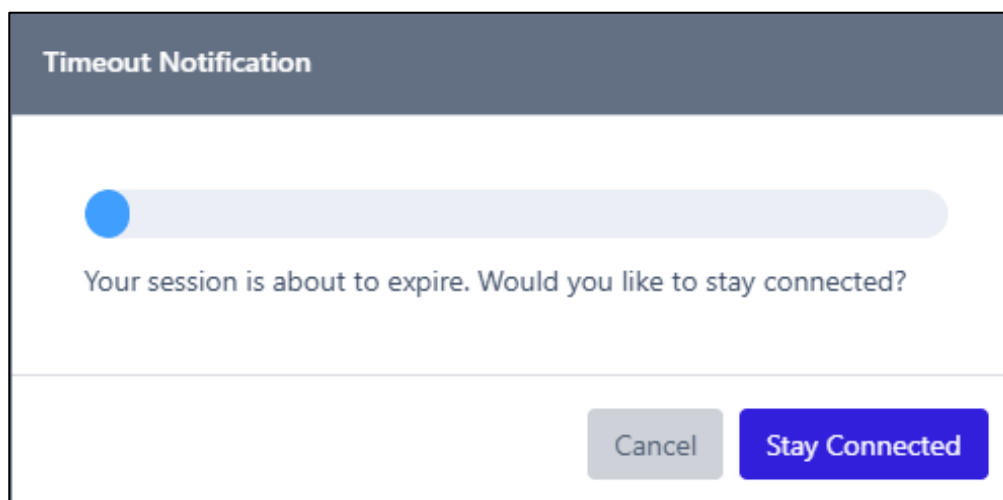
Il **Remote Access** è necessario alla creazione del link per l'accesso remoto all'AIBOX. Una volta abilitato, compariranno due pulsanti sotto la voce **Access URL**, che permetteranno di:

- Copiare il link e condividerlo.
- Premere il link per accedere al dispositivo.

Alla prima installazione saranno disponibili per ogni AIBOX, **432 crediti** che garantiscono l'accesso per **72 ore**.

Ad ogni primo accesso, verranno detratti 3 crediti, l'equivalente di trenta minuti.

Dopo la creazione del link, è possibile accedere all'AIBOX più volte entro 30 minuti, superati i quali, se la pagina web di AIBOX sarà aperta, apparirà un avviso pop-up per avvisare del tempo rimanente e si potrà decidere se chiudere la pagina web o rimanere connessi utilizzando ulteriori crediti.



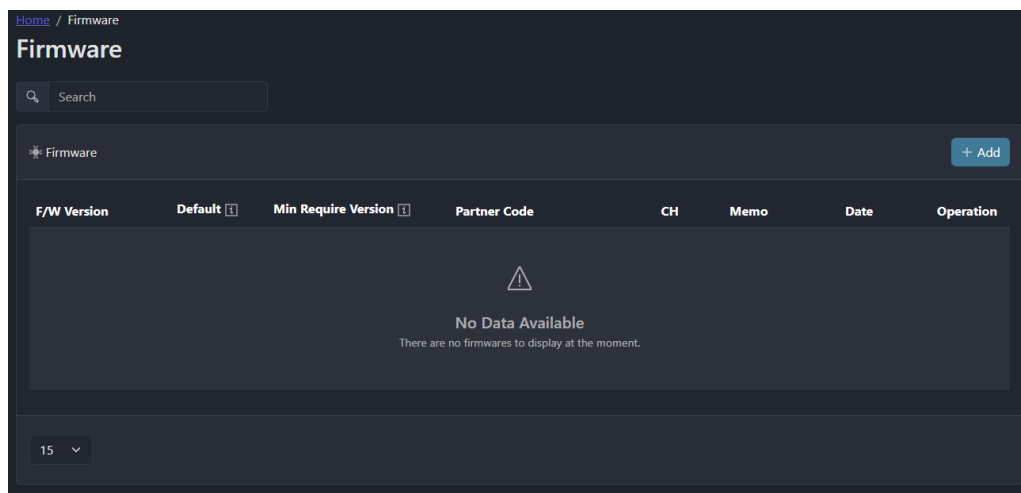
NOTA: All'esaurimento dei crediti è possibile acquistarne di nuovi. I crediti verranno trasferiti al proprio codice Partner dopo l'acquisto ma non sarà possibile trasferirli al singolo dispositivo.

Quando un dispositivo termina i propri crediti, questi verranno automaticamente detratti dal saldo del partner a cui è associato nel momento in cui verrà richiamato il link per la connessione remota.

7. Gestione Firmware

Il portale consente anche una gestione centralizzata dei firmware. È possibile caricare sul portale nuovi firmware direttamente dal proprio PC.

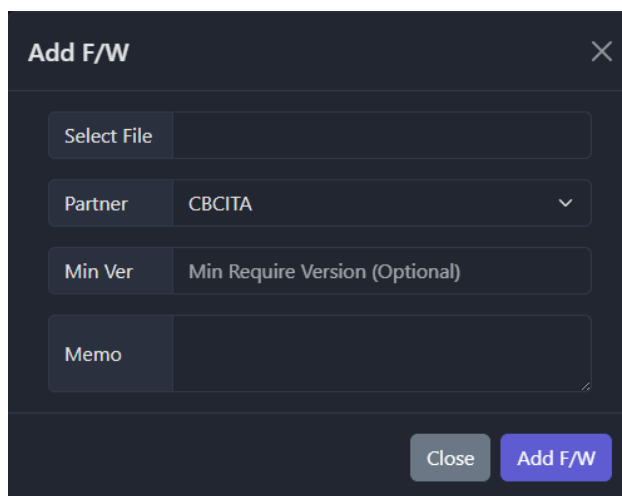
Dal menu principale, premere su **Firmware**.



Premere il pulsante **Add** sulla destra.

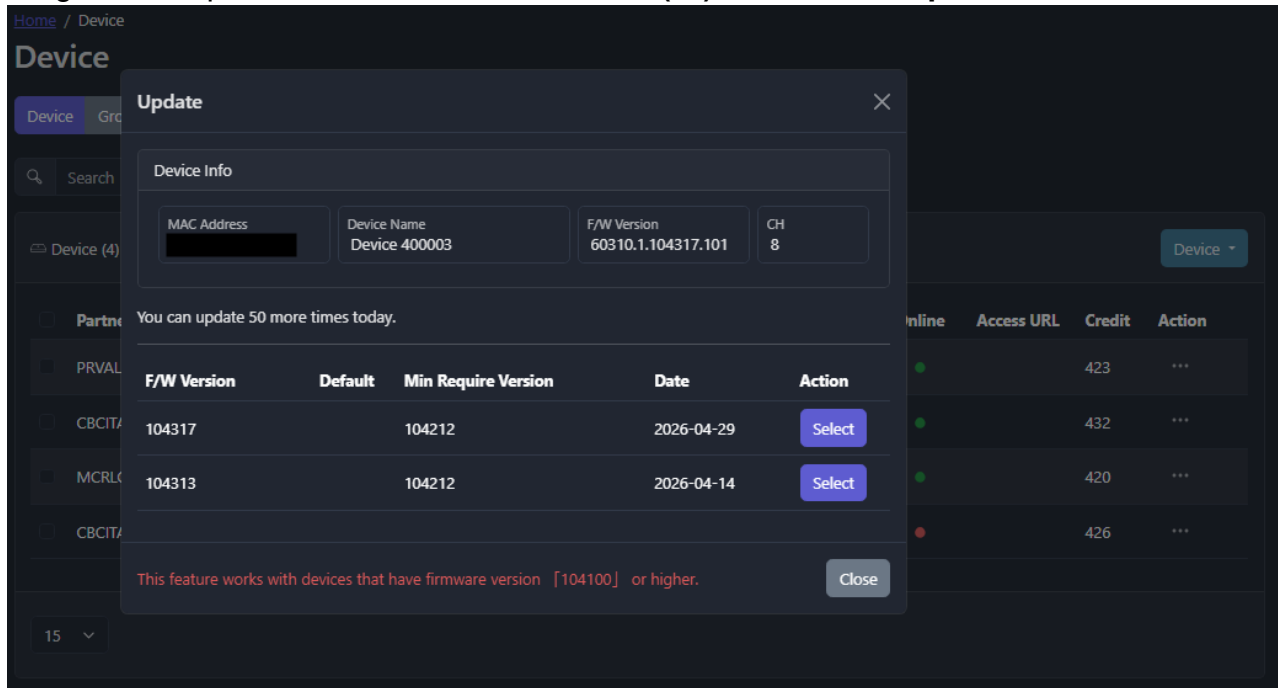
Selezionare il file dal proprio computer tramite **Select File**.

Min Ver, dà la possibilità di impostare una versione minima richiesta. Questo significa che un firmware specifico non può essere installato su dispositivi che soddisfano un minimo requisito di versione (es. scrivere: "104212").



NOTA: Nella sezione Firmware del menu principale, è possibile scaricare una copia del firmware caricato.

Per procedere all'aggiornamento del firmware, dal menu principale premere **Device**, scegliere il dispositivo e tramite **menu azione (...)**, selezionare **Update**:



Selezionare la versione FW desiderata premendo su **Select**.

8. Gestione utenti

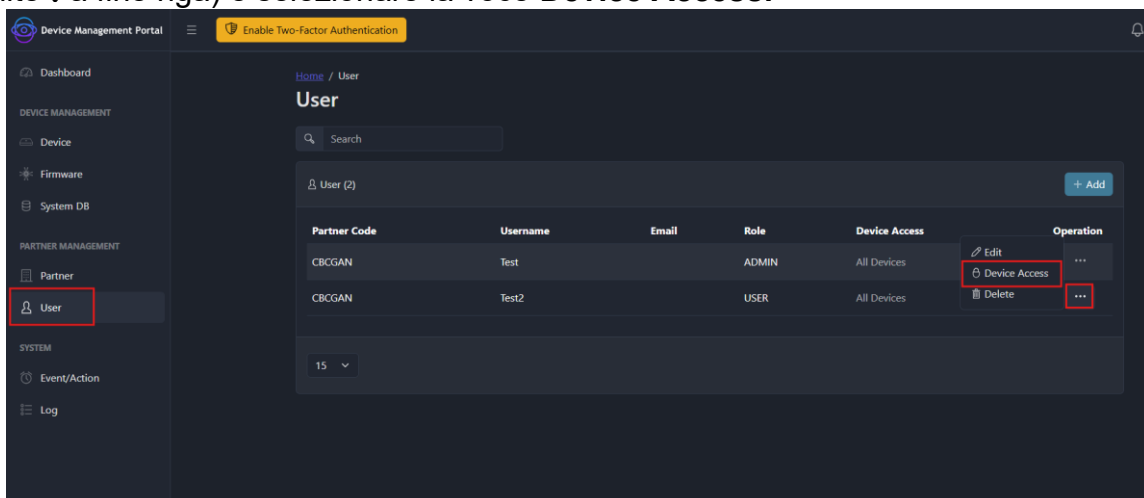
Tramite questo menu, l'utente ADMIN potrà:

- aggiungere altri utenti ADMIN
- aggiungere utenti USER

Per ogni utente USER, potrà limitare la visione a specifici dispositivi (gruppi) o tutti i dispositivi.

Per modificare questa impostazione, recarsi nel menu **User**.

Successivamente, nella riga dello USER scelto, premere sul menu opzione (accessibile tramite : a fine riga) e selezionare la voce **Device Access**.

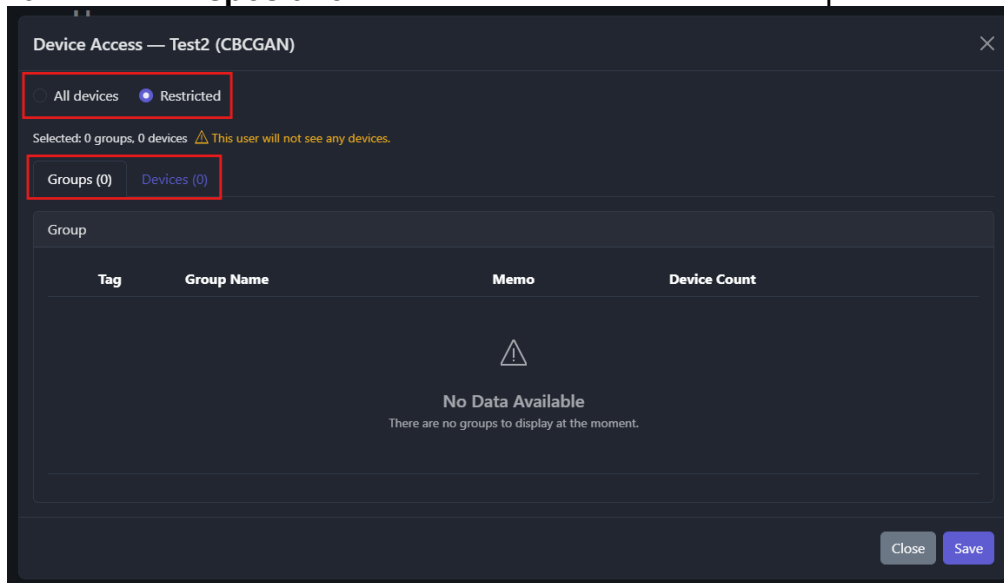


Nel menu comparso, selezionare quali dispositivi saranno visualizzabili all'utente:

- **All devices:** permette di visualizzare tutti i dispositivi del Partner.
- **Restricted:** permette di visualizzare dispositivi specifici.

I dispositivi sono selezionabili:

- tramite **Gruppi**: selezionare gruppi di dispositivi già creati.
- tramite **Dispositivo**: selezionare individualmente i dispositivi.



Successivamente, premere **Save** per confermare.

NOTA: una volta limitata la visione dei dispositivi ad un utente, quest'ultimo non potrà più inserire AIBOX sul portale.

9. Eventi e azioni automatiche

Tramite il menu principale, **Event/Action**, il portale offre anche funzionalità di automazione tramite la configurazione di **eventi e azioni**. È possibile creare regole che si attivano in funzione dello stato del dispositivo, in particolare quando un dispositivo:

- diventa **Online**
- diventa **Offline**

Queste regole possono essere applicate sia a singoli dispositivi sia a gruppi, rendendo la gestione molto flessibile.

Una volta definito l'evento, è possibile configurare diverse tipologie di azione:

- **Email:** Il server di inoltro e-mail è gestito internamente ed è una nuova funzionalità **BETA**. Nel prossimo aggiornamento del portale, sarà richiesto l'utilizzo del proprio SMTP di posta. Per gli utenti che già utilizzano la funzione, verrà mantenuto il servizio **BETA**. In questa fase è sufficiente definire l'azione; non è necessario configurare manualmente il server di posta. L'email arriverà da un server mailer-xx@ailn.io; il nome del mittente lo decide il partner, mentre xx sarà un numero definito dal server.

- **HTTP:**
Richiede l'impostazione di:
 - Indirizzo del server di destinazione
 - Contenuto del messaggio
- **Sentinel:** Utilizzabile per integrazioni con sistemi esterni di monitoraggio o sicurezza.

10.FAQ

1. Le funzionalità di accesso remoto sono basate su servizi cloud?

Il server di gestione di AIBOX è realizzato e gestito su GCP (Google Cloud Platform). Sfruttiamo l'infrastruttura di livello enterprise di GCP per garantire elevata disponibilità e sicurezza per i nostri servizi di gestione remota.

La disponibilità del servizio è progettata per operare con un uptime di circa il 99,98% in condizioni operative normali. Attualmente, il servizio di accesso remoto non è configurato con un'architettura di ridondanza/failover separata.

2. Quando si avvia l'accesso remoto, da quale direzione parte la comunicazione?

(Dispositivo → Server Esterno o Server Esterno → Dispositivo).

Tutte le sessioni di accesso remoto vengono avviate tramite una connessione in uscita (Dispositivo → Server esterno). Poiché il dispositivo stabilisce prima la connessione con il nostro server di gestione, non è necessario aprire porte in entrata, proteggendo di fatto il dispositivo da accessi esterni non autorizzati.

Per quanto riguarda le connessioni in uscita, se il firewall è restrittivo (ad esempio, controlla anche il traffico HTTPS e altri tipi di traffico), è necessario aprire porte in uscita specifiche.

Direction	Domain / IP Address	Port	비고
Outbound	*.mtnl.noif-fnc.aaln.io	822 and 8082	

3. Esistono situazioni in cui è necessaria la configurazione del router?

(come il port forwarding o UPnP)

In ambienti di rete standard, non sono necessarie configurazioni complesse del router, come il port forwarding o l'UPnP. L'AIBOX è progettato per funzionare senza problemi anche dietro un NAT (router/gateway) purché disponga di una connessione Internet attiva per raggiungere i nostri server.

Nota: in ambienti con rigide policy di firewall aziendali, potrebbe essere necessario inserire nella whitelist specifiche porte in uscita.

4. Quali protocolli di comunicazione vengono utilizzati durante l'accesso remoto?

La comunicazione successiva all'autenticazione del dispositivo utilizza protocolli crittografati sicuri come HTTPS, Secure WebSocket (WSS) e Secure MQTT (MQTTS). Utilizziamo il protocollo SSH (Secure Shell) per la trasmissione sicura dei dati e la gestione remota; internamente, viene impiegato come parte di un meccanismo di tunneling SSH per trasportare in modo sicuro le comunicazioni di accesso remoto basate su HTTPS tra il dispositivo e l'infrastruttura di accesso remoto. Per garantire l'integrità e la riservatezza dei dati, tutte le comunicazioni sono crittografate utilizzando TLS 1.3.

5. Come viene eseguita l'autenticazione del dispositivo?

(ad esempio, indirizzo MAC, certificati univoci, ecc.)

L'autenticazione è rigorosamente controllata tramite certificati RSA univoci rilasciati a ciascun dispositivo al momento della produzione. Solo i dispositivi dotati di un certificato valido, rilasciato in fabbrica, possono autenticarsi e stabilire una connessione con il server di gestione, prevenendo così la falsificazione dell'hardware o l'accesso non autorizzato.

Attualmente, il certificato del dispositivo non richiede una data di scadenza per il rinnovo.