

**ANALISI VIDEO INTELLIGENT DEEP LEARNING**

## Integrazioni centrali aylook

*Versione 1.8 06/07/2025*

*Seguici su*    

## INDICE

Introduzione .....	3
<b>Centrali integrate con aylook</b> .....	3
Centrale Tecnoalarm .....	4
<b>Abilitazione Integrazione</b> .....	5
<b>Verifica Abilitazione Tecno Out</b> .....	6
<b>Gestione Zone Virtuali Ev10-50</b> .....	6
Azioni su Aylook.....	7
<b>Inserimento su aylook</b> .....	8
Centrale Tecnofire .....	9
<b>Abilitazione Integrazione</b> .....	9
<b>Inserimento su aylook</b> .....	11
Centrale Satel.....	12
<b>Inserimento su aylook</b> .....	12
<b>Importazione Nomi oggetti tramite file XML</b> .....	13
Centrale Ksenia .....	15
<b>Inserimento su aylook</b> .....	15
Centrale Inim .....	16
<b>Prime</b> .....	16
<b>Abilitazione Integrazione</b> .....	16
<b>Inserimento su aylook</b> .....	18
<b>Smartliving</b> .....	19
<b>Inserimento su aylook</b> .....	19
Centrale AVS.....	20
<b>Inserimento su aylook</b> .....	20
Centrale Elmo.....	21
<b>Inserimento su aylook</b> .....	21
Centrale Risco.....	22
<b>Risco Prosys+</b> .....	22
<b>Risco ProSys 16/40/128</b> .....	22
<b>Inserimento su aylook</b> .....	23
Centrale UTC.....	24
<b>Abilitazione integrazione</b> .....	24
<b>Inserimento su aylook</b> .....	29

## Introduzione

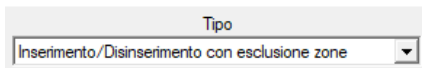
Aylook può essere dotato di un applicativo software che consente l'integrazione con i modelli più importanti e diffusi di centrali d'allarme dotate di scheda LAN. L'integrazione completa tra telecamere, sensori ed aree sorvegliate permette di supervisionare l'impianto con pochi click: chiunque può interagire con il sistema di sicurezza e capire in pochi secondi lo stato dell'impianto.

## Centrali integrate con aylook

Su aylook è possibile integrare le seguenti centrali:

- **AVS:** AVS Ultra, AVS Xtream 6, AVS Xtream 6 B, AVS Xtream 32, AVS Xtream 32 B, AVS Xtream 64, AVS Xtream 64 B e AVS Xtream 640;
- **Elmo:** serie ETR, PREGIO, VILLEGGIO e TITANIA;
- **Inim:** Inim SmartLiving 5-15, Inim SmartLiving 10-50, Inim SmartLiving 10-100, Inim Prime, Hesa Quaranta Q15, Hesa Quaranta Q50 e Hesa Quaranta Q100;
- **Ksenia:** Ksenia Lares 16-IP, Ksenia Lares 48-IP, Ksenia Lares 128-IP e Ksenia Lares 4.0;
- **Risco:** Risco Prosys 16, Risco Prosys 40, Risco Prosys 128, Risco Prosys Plus e Risco LightSys (con ethernet modello Dual Socket);
- **Satel:** Satel Integra 64, Satel Integra 64 Plus, Satel Integra 128, Satel Integra 128 Plus, Satel Integra 128 WRL e Satel Integra 256;
- **Tecnoalarm:** Tecnoalarm TP8-88, Tecnoalarm TP8-88 PLUS, Tecnoalarm TP 20 - 440, Tecnoalarm EV10-50 e Tecnoalarm EV12-150;
- **UTC:** UTC serie Master;

## Centrale Tecnoalarm

Modello integrato	Tecnoalarm TP8-88, TP8-88 PLUS, TP20-440, EV10-50 <sub>1</sub> EV12-150 <sub>2</sub>
Gestione Sensori	Gestito Stato di Allarme, Memoria Allarme, Manomissione ed Esclusione Gestite Zone Virtuali su Ev10-50/12-150 (con licenza Zone IP)
Gestione Programmi	Gestito Inserimento/Disinserimento <sub>3</sub> Gestito Reset Memoria Allarmi <sub>4</sub> Gestito Arma con Esclusione Zone <sub>5</sub>
Gestione Uscite	Gestite uscite di tipo Telecomando (16 su 8-88,32 su 440, 36 su Ev10-50 e 72 su EV12-150) <sub>6</sub>
Importazione Nomi	Su TP8-88P/TP20-440 con almeno FW 1.9.00 e Tecno Out 3.5.00 e su Ev10-50/12-150. Va premuto il pulsante Sincronizza Nomi da Setup Centrale
Utilizzo Multi PIN	Supportato <sub>7</sub>
Abilitazione Integrazione	Licenza Tecno-Out
Modulo da installare sulla centrale	Modulo di rete ESP-LAN su 8-88 e 20-440
Porta Integrazione Default	10005
Configurazione Particolare	-
Note	<p>Gli attributi/permessi descritti nella seguente lista valgono per le centrali TP8-88 con Release 2.4.08 e EV10-50/12-150 con release 2.0.</p> <p>La funzione "Arma Centrale" arma tutti i programmi (anche quelli non utilizzati).</p> <p>Non si possono escludere le zone a centrale armata.</p> <p>Solo utenti con attributo "Privilegiato" attivo possono escludere le zone.</p> <p>Non è possibile utilizzare il Tecno Out e il Supervisor Tecnoalarm contemporaneamente.</p> <p>1.Ev10-50 Integrata solo in Aylook 9.</p> <p>2.Ev12-150 integrata solo in Aylook 9 dalla versione 9.1.14.</p> <p>3.Permesso solo agli utenti con attributo contenente l'operazione. Permessi solo ai Programmi di pertinenza. In caso di anomalie l'operazione è permessa (forzata) solo a utenti con attributo "Bypass allarmi generali" attivo.</p> <p>4.Dalla versione 8.1.11 con ASC e App Aylook 2.1.2. Solo su Centrale. Tutti gli utenti possono azzerare le memorie di propria pertinenza.</p> <p>Solo dopo il tempo di allarme.</p> <p>5.Dalla versione 8.1.12 con ASC e App Aylook 2.1.2. Esclude le zone durante l'inserimento solo a utenti con attributo "Esclusione zone disabilitato" disattivo.</p> <p></p> <p>6.Solo utenti con attributo "Disabilitazione accesso telecomandi" disattivo.</p> <p>7.Sulla centrale tutti gli eventi di gestione centrale verranno visualizzati nello Storico Eventi come azioni eseguite tramite il Tecno Out.</p>

## Abilitazione Integrazione

Richiedere al distributore Tecnoalarm il codice per l'abilitazione del protocollo TECNO\_OUT, tale codice andrà inserito tramite tastierino in centrale (seguire guida ufficiale Tecnoalarm).

Abilitare il protocollo TECNO\_OUT in modalità SERVER porta di default (**10005**) e inserire una **Passphrase** di 16 caratteri (es 1234567890qwerty, utilizzare solo lettere e cifre). Tecno Out è garantita dall'utilizzo di una chiave di crittografia AES 128bit.

Inserendo l'IP di Aylook nella White List, la connessione tramite il protocollo Tecno Out sarà esclusivamente tra questi due device.

Se viene indicata una porta differente la stessa andrà specificata durante l'inserimento della centrale nel formato x.x.x.x:p su Aylook (es 192.168.5.168:10010), in questo caso su centrale è stata specificata la porta 10010 al posto di 10005). L'immagine sotto è uno screenshot della configurazione di una tp888Plus aperta su Centro.

Le operazioni indicate vanno eseguite in prima configurazione.

La centrale TecnoAlarm TP8-88/20-440 accetta una sola connessione in ingresso su ogni porta del Tecno-Out configurata.

La centrale TecnoAlarm Ev10-50 accetta due connessioni in ingresso su ogni porta del Tecno-Out configurata.

## Verifica Abilitazione Tecno Out



Da Centro clicca sul tasto "Info", si visualizza la finestra "Informazioni dispositivo".

**Attenzione:** la finestra viene visualizzata solo se si è collegati alla centrale. La finestra fornisce informazioni relative alla centrale, alle

L'abilitazione TECNO OUT è confermata solo se è presente la spunta su "Protocollo TECNO OUT" sotto il menu "Opzioni":

Informazioni dispositivo	
Tipo dispositivo	Tp888E
Versione hardware	0F
Versione firmware	0.7.4
Lingua firmware	ITALIA
Versione vocabolario	2
Lingua vocabolario	ITALIA
Serial number SN	3019991
Identificativo ID	225
NET info	
Mobile network info	TECNOCELL BUS
Tecnosalarm Connect Service info	
Opzioni	
Vocale	<input checked="" type="checkbox"/>
Programmazione avanzata	<input type="checkbox"/>
Protocollo TECNO OUT	<input checked="" type="checkbox"/>
Accesso	
Accesso remoto	<input checked="" type="checkbox"/>
Restrizioni SW	Visualizza + Operazioni + Modifica parametri
Restrizioni APP	Visualizza + Operazioni + Modifica parametri
Accesso installatore da tastiera	<input checked="" type="checkbox"/>
OK	

## Gestione Zone Virtuali Ev10-50

Per la Ev10-50 è necessario avere l'abilitazione Zone IP per gestire le Zone Virtuali su aylook:

Opzioni	
Vocale	<input checked="" type="checkbox"/>
Programmazione avanzata	<input checked="" type="checkbox"/>
Protocollo TECNO OUT	<input checked="" type="checkbox"/>
Zone IP	<input checked="" type="checkbox"/>
Programmazione avanzata con varchi	<input type="checkbox"/>

La Zona Virtuale deve essere opportunamente configurata come in questo esempio.

Scegliere il Protocollo IP corretto (Supervisor-TecnoOut) ed il canale utilizzato (Extra1). Mettere le 4 spunte in basso su Auto-Ripristino al fine di rimettere a riposo in modo automatico dopo 10secondi la zona in seguito al rispettivo evento.

Zona
6 V-Tlc Strada
Zona virtuale
Copia

Descrizione  
V-Tlc Strada

Configurazione zona

Tipo
ISTANTANEA
Cicli
1 CICLO
Numero attivazioni
0  
in minuti
0

Virtuale

Protocollo IP  
Supervisor-TecnoOut
Canale  
Extra 1

Zona contemporanea
Contemporaneita' non attiva
Tempo contemporaneita' [sec]
5
primo allarme in AND , successivi OR

Abitazione
Auto-ripristino

Allarme
☒
☒

Tamper
☒
☒

Mask
☒
☒

Fail
☒
☒

## Azioni su Aylook

Per mandare in allarme una zona virtuale, vanno utilizzate le azioni di aylook. Nella sezione Allora, Centrale, troveremo le seguenti voci dedicate.

attiva allarme sulla zona virtuale

ripristina allarme sulla zona virtuale

attiva manomissione sulla zona virtuale

ripristina manomissione sulla zona virtuale

resetta la zona virtuale

Non è necessario creare anche l'azione di ripristino allarme/manomissione se è stata messa la spunta su Auto-Ripristino nella configurazione della Zona Virtuale su Centro.

Ecco un esempio di azione dove viene mandata in allarme una zona virtuale in seguito alla rilevazione di una persona su una telecamera mentre una partizione è inserita:

rileva movimento la telecamera Strada nell'area Tutte le aree con classe Tutte le classi ...  
la partizione 6-Perimetrale V1 è armata

attiva allarme sulla zona virtuale null V-Tlc Strada  
genera allarme con oggetto Predefinito con suono Nessun suono per 1 ogni 5 sec.

Anteklab srl: Via Manzoni 49, 46047 Porto Mantovano (MN) - Tel: 0376397765 - aylook@antek.it

P a g . 7 | 29

## Inserimento su aylook

Per inserire la centrale su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **Password:** Passphrase precedentemente configurata a bordo centrale;
- **PIN:** Un codice PIN valido abilitato a tutte le funzioni.

**NUOVA CENTRALE ANTI-INTRUSIONE**

Nome:

Modello:

Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

Password/Passphrase:

PIN:

**SALVA**



## Centrale Tecnofire

Modello integrato	Tecnofire TFA1, TFA2, TFA4, TSA1, TSM1
Gestione Sensori	Sì (Allarme, Memoria Allarme, Manomissione)
Gestione Zone	Visualizzazione Stato (Armata, Disarmata, Allarme) <sub>1</sub>
Gestione Moduli	Visualizzazione Uscite <sub>2</sub>
Cancellazione memoria allarme	Non supportata
Importazione Nomi	Sì
Utilizzo Multi PIN	Supportato <sub>3</sub>
Abilitazione Integrazione	Licenza Tecno-Out
Modulo da installare sulla centrale	Modulo di rete TFNET
Porta Integrazione Default	10005
Configurazione Particolare	-
Note	<p>Non è possibile utilizzare il Tecno Out e il Supervisor Tecnofire contemporaneamente.</p> <p>1.Non è possibile escludere le zone. Non è gestita la zona 0 di default.</p> <p>2.Gli ingressi dei moduli sono visualizzati come sensori su aylook.</p> <p>Su aylook l'uscita è accesa quando il modulo è incluso e spento quando è escluso.</p> <p>3.Sulla centrale tutte gli eventi di gestione centrale verranno visualizzati nello Storico Eventi come azioni eseguite tramite il Tecno Out.</p>

## Abilitazione Integrazione

Richiedere al distributore Tecnofire il codice per l'abilitazione del protocollo TECNO\_OUT, tale codice andrà inserito tramite tastierino in centrale (seguire guida ufficiale Tecnofire).

Abilitare il protocollo TECNO\_OUT in modalità SERVER porta di default (**10005**) dal menu "Ethernet" del dispositivo TFNET. Inserendo l'IP di Aylook nella White List, la connessione tramite il protocollo Tecno Out sarà esclusivamente tra questi due device.

Inserire una **Passphrase** di 16 caratteri (es 1234567890qwerty, utilizzare solo lettere e cifre) nella riga "TECNO OUT" sotto il menu "Sicurezza" del dispositivo TFNET. Tecno Out è garantita dall'utilizzo di una chiave di crittografia AES 128bit.

Dispositivo 4 [TFNET]

SNTP		EMAIL		Modbus		IHD	
Comunicatori	Codici di rapporto	Codici di rapporto zone	Temporizzazioni	Ethernet	Sicurezza	Opzioni	DDNS
<p>Output connection</p> <p>Passphrase</p> <p>A <input type="text"/></p> <p>B <input type="text"/></p> <p>C <input type="text"/></p> <p>D <input type="text"/></p> <p>E <input type="text"/></p> <p>F <input type="text"/></p> <p>G <input type="text"/></p> <p>H <input type="text"/></p>							
SERVICE				<input type="text"/>			
SERVER 1				<input type="text"/>			
SERVER 2				<input type="text"/>			
TECNO OUT				<input type="text" value="1234567890qwerty"/>			

OK Annulla ?

Dispositivo 4 [TFNET]

SNTP		EMAIL		Modbus		IHD	
Comunicatori	Codici di rapporto	Codici di rapporto zone	Temporizzazioni	Ethernet	Sicurezza	Opzioni	DDNS
IP address		<input type="text" value="192-168-1-112"/>		<input checked="" type="checkbox"/> Controllo linea Ethernet			
Subnet mask		<input type="text" value="255-255-255-0"/>					
Gateway		<input type="text" value="192-168-1-1"/>					
DNS		<input type="text" value="8-8-8-8"/>					
<input checked="" type="checkbox"/> SERVER 1 Port <input type="text" value="10001"/> White list <input type="text"/> <input type="text"/> <input type="text"/>		<input checked="" type="checkbox"/> SERVER 2 Port <input type="text" value="10002"/> White list <input type="text"/> <input type="text"/> <input type="text"/>		<input checked="" type="checkbox"/> TECNOSERVER TECNOALARM Port <input type="text" value="21001"/>			
<input checked="" type="checkbox"/> SERVICE TECNOALARM Port <input type="text" value="21001"/>							
<input checked="" type="checkbox"/> TECNO OUT SERVER <input type="text" value="SERVER"/> Port <input type="text" value="11111"/> White list <input type="text" value="0-0-0-0"/> <input type="text" value="0-0-0-0"/> <input type="text" value="0-0-0-0"/>		<input type="checkbox"/> MODBUS SERVER <input type="text" value="SERVER"/> Port <input type="text" value="0"/> White list <input type="text" value="0-0-0-0"/> <input type="text" value="0-0-0-0"/> <input type="text" value="0-0-0-0"/>					

OK Annulla ?

## Inserimento su aylook

Per inserire la centrale su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **Password:** Passphrase precedentemente configurata a bordo centrale;
- **PIN:** codice PIN inserito nel Setup della centrale.

NUOVA CENTRALE ANTI-INTRUSIONE

Nome: Tecnofire

Modello: Tecnofire TFA1-298

Tipo connessione: ☒ IP ☐ Seriale

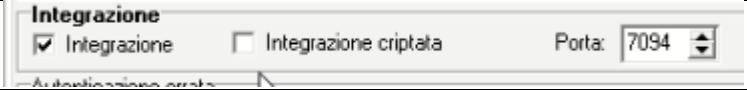
Indirizzo IP: 192.168.5.45

Password/Passphrase: .....

PIN: .....

SALVA

## Centrale Satel

Modello integrato	Satel Integra 64, 64+, 128, 128+, 128 WRL e 256 Plus
Gestione Sensori	Si (Allarme, Memoria Allarme, Manomissione)
Gestione Aree	Si (Armata, Disarmata, Memoria Allarme) Supportato l'inserimento di tipo 1, 2 e 3
Gestione Uscite	Si (Monostabili e Bistabili)
Cancellazione memoria allarme	Si
Importazione Nomi	Si (è necessario avviarla manualmente, sincronizzazione lenta) <i>Dalla 9.1.11 l'importazione dei nomi avviene tramite importazione file XML descritta in questo manuale</i>
Utilizzo Multi PIN	Funziona con tutti i PIN di centrale
Abilitazione Integrazione	
Modulo da installare sulla centrale	ETHM-1
Porta Integrazione Default	7094
Configurazione Particolare	Integrazione criptata deve essere disabilitata
Note	Il PIN errato non viene segnalato (verrà quindi visualizzata sempre la spunta verde) 1. L'inserimento totale è di tipo 1, quindi con esclusione delle zone. Tipo 2 con esclusione delle zone interne e Tipo 3 con esclusione delle zone interne senza ritardo

### Inserimento su aylook

Per inserire la centrale su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale.
- **File Mappatura:** File XML per importare il file dei nomi degli oggetti

NUOVA CENTRALE ANTI-INTRUSIONE

Nome:

Modello:

Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

File mappatura:

SALVA

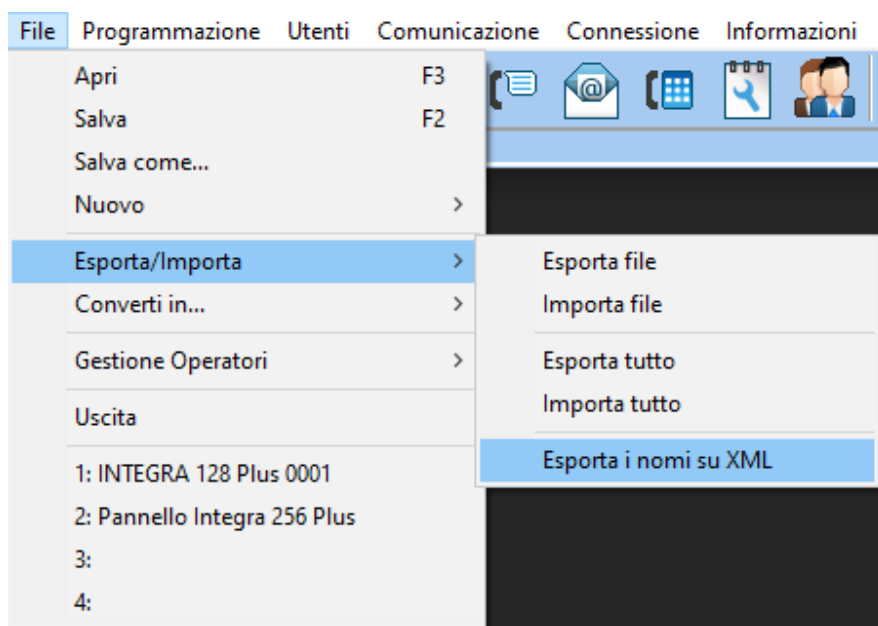
## Importazione Nomi oggetti tramite file XML

Dalla versione 9.1.11 di aylook è stata implementata l'importazione dei nomi degli oggetti di centrale tramite il file XML generato dal software DLOADX. Questo permette di cambiare i nomi molto più velocemente rispetto al comando manuale Sincronizza Nomi.

Per scaricare il file è necessario collegarsi alla centrale con il software proprietario DLOADX.

Premere su File, Esporta/Importa, Esporta i nomi su XML.

Salvare il file sul proprio PC.



Adesso è necessario importare il file su aylook pertanto collegarsi su aylook e dal menu Centrale, una volta aggiunta la centrale Satel con gli altri dati, premere su Importa file in File Mappatura e selezionare il file appena scaricato.

**NUOVA CENTRALE ANTI-INTRUSIONE**

Nome:

Modello:

Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

File mappatura:  ...

SALVA

Una volta caricato comparirà nella schermata. Premere Salva per salvare:

**NUOVA CENTRALE ANTI-INTRUSIONE**

Nome:

Modello:

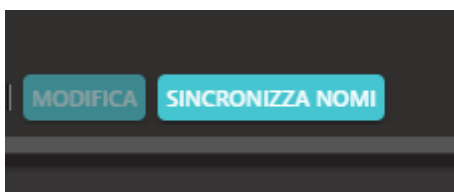
Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

File mappatura:

**SALVA**

Per importare i nomi, Premere su Sincronizza Nomi e nell'arco di 10secondi circa tutti i nomi verranno aggiornati.



Qualora si volesse aggiornare nuovamente la lista, va rifatta la stessa procedura.

## Centrale Ksenia

Modello integrato	Ksenia Lares 16-IP/ 48-IP/ 128-IP e Lares 4.0
Gestione Sensori	Si (Allarme, Memoria Allarme, Manomissione) e zone virtuali <sub>1</sub>
Gestione Aree	Si (Armata, Disarmata, Memoria Allarme)
Gestione Uscite	Si, comprese uscite virtuali (timer software) <sub>2</sub>
Cancellazione memoria allarme	Si (solo completa da centrale)
Importazione Nomi	Si
Utilizzo Multi PIN	Supportato
Abilitazione Integrazione	Non prevista.
Modulo da installare sulla centrale	Non previsto.
Porta Integrazione Default	TCP 80 (solo per Lares 4.0)
Configurazione Particolare	-
Note	<ol style="list-style-type: none"> <li>1. Il numero di zone supportate si ottiene sommando tutte le zone configurabili in centrale (zone fisiche e zone virtuali), il numero massimo di zone è 16, 40, 96, 140, 644 a seconda del modello utilizzato.</li> <li>2. Il numero di uscite supportate si ottiene sommando tutte le uscite configurabili in centrale (uscite fisiche ed uscite virtuali), il numero massimo di uscite è 16, 18, 40, 140 e 644 a seconda del modello utilizzato.</li> </ol>

## Inserimento su aylook

Per inserire la centrale Ksenia Lares occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **Utente:** numero dell'utente formato da 4 cifre (non richiesto dalla Lares 4.0);
- **Password:** password dell'utente (non richiesto dalla Lares 4.0);
- **PIN:** PIN inserito nel Setup della centrale.

NUOVA CENTRALE ANTI-INTRUSIONE

Nome:

Modello:

Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

PIN:

SALVA

## Centrale Inim

### Prime

<b>Modello integrato</b>	<b>Inim Prime</b>
<b>Gestione Sensori</b>	Sì (Allarme, Memoria Allarme, Manomissione) Gestite le zone doppie ed i terminali virtuali
<b>Gestione Aree</b>	Sì (Armata, Disarmata, Memoria Allarme)
<b>Gestione Scenari</b>	Non supportata
<b>Gestione Uscite</b>	Sì
<b>Cancellazione memoria allarme</b>	Sì
<b>Importazione Nomi</b>	Sì
<b>Utilizzo Multi PIN</b>	Non supportato. Usare il PIN inserito in Setup
<b>Abilitazione Integrazione</b>	Abilitare la chiave API nel Setup Prime LAN
<b>Modulo da installare sulla centrale</b>	Scheda di rete INIM PRIME LAN
<b>Porta Integrazione Default</b>	80
<b>Configurazione Particolare</b>	-
<b>Note</b>	Supporta solo la configurazione dei terminali standard.

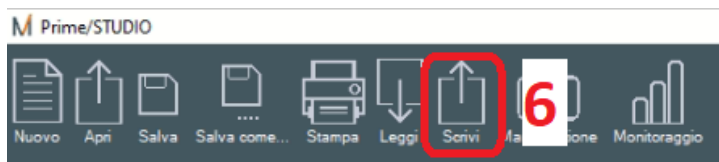
### Abilitazione Integrazione

Per integrare la Inim Prime è obbligatorio avere installata la scheda aggiuntiva Prime LAN.

Una volta installato il modulo dovete Abilitare le API HTTPS mettendo la spunta sulla casella **"Abilita API http"** (1). Successivamente occorre premere il pulsante **"Genera"** (2) per creare la chiave API e selezionare il **"Codice"** (3) al quale associare questa chiave API.

Togliere la spunta da "Permetti solo connessioni via HTTPS" e "Non permettere il disarmo".

Per salvare la configurazione dovete scrivere la programmazione della scheda con il pulsante **"Scrivi"** (4) e poi successivamente scrivere anche la programmazione completa della centrale con il pulsante **"Scrivi"** (6):





**5** **4** d e-mail Configurazione parametri e-mail Mappe grafiche Gestione Telecamere ONVIF Programmazione KNX

Parametri e-mail

Oggetto

Mittente (nome@dominio.it)

Mail Server  Porta

Account (seleziona)  Preconfigura Metodo SSL NO SSL

Richiesta autenticazione NO AUTHENTICATION  Timeout (s)

Nome utente

Password  Mostra

Gestione della chiave per le API

Abilita API HTTP/HTTPS **1** ☒

Chiave per le API  Pulisci **2** Genera

Codice **3**

Permetti solo connessioni via HTTPS (da 3.10 Primelan) ☐ Non permettere il disarmo (da 3.10 Primelan) ☐

Abilitazione HTTPS

Abilita HTTPS (da 3.10 di PrimeLan) ☐

Destinatari

Id.	Nome	Indirizzo
1		
2		
3		
4		

Configurazione PrimeLAN

NOTA BENE: Se scrivete solo la programmazione della centrale e non della scheda, non salverà i dati.

Per verificare se i dati sono stati correttamente salvati potete leggere la programmazione della scheda con il pulsante di lettura **"Leggi"** (5).

## Inserimento su aylook

Per inserire la centrale Inim Prime occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **Utente:** numero dell'utente formato da 4 cifre;
- **Password:** password di installatore (di default è "pass");
- **PIN:** PIN dell'utente amministratore a bordo centrale;
- **API Key:** chiave API da generare a bordo centrale.

Sulla Inim Prime è possibile creare delle zone virtuali che possono essere pilotate da uscite virtuali attraverso le azioni di Aylook. In questo modo è possibile mandare la centrale/area in allarme quando scatta l'analisi video.

## Smartliving

Modello integrato	Inim SmartLiving 10-15/10-50/10-100
Gestione Sensori	Sì (Allarme, Memoria Allarme, Manomissione) Sono gestite le zone doppie <sup>1</sup>
Gestione Aree	Sì (Armata, Disarmata, Memoria Allarme) e Inserimento Parziale
Gestione Scenari	Non supportata
Gestione Uscite	Sì <sup>2</sup>
Cancellazione memoria allarme	Sì
Importazione Nomi	Non supportata
Utilizzo Multi PIN	Sì, con tutti i PIN utente
Abilitazione Integrazione	Non prevista
Modulo da installare sulla centrale	Scheda di rete INIM LAN SI
Porta Integrazione Default	5004
Configurazione Particolare	-
Note	<p>Supporta solo la configurazione dei terminali standard  Non sono gestite le zone sismiche  Non sono gestiti terminali delle tastiere  Non sono gestiti i terminali virtuali  Non sono supportati i terminali impostati come Ingresso-Uscita</p> <ol style="list-style-type: none"> <li>1. Le zone doppie seguono la stessa numerazione delle zone normali incrementate di 100 nel setup di aylook</li> <li>2. l'utente deve avere il permesso per pilotarle mettendo la spunta sulle uscite da Utenti, Codici, Abilitazione Uscite  La numerazione delle zone-uscite segue il numero dei terminali quindi se il terminale 4 è impostato come zona allora deve essere tolta la spunta dall'uscita 4 dal setup aylook</li> </ol>

## Inserimento su aylook

Per inserire la centrale Inim SmartLiving su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale.

NUOVA CENTRALE ANTI-INTRUSIONE

Nome:

Modello:

Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

SALVA

## Centrale AVS

Modello integrato	AVS XTREAM 640/64/32/6 e AVS Ultra
Gestione Sensori	Si (Allarme, Memoria Allarme, Manomissione)
Gestione Aree	Si (Armata, Disarmata, Memoria Allarmi)
Gestione Uscite	Si <sup>1</sup>
Cancellazione memoria allarme	Non supportata.
Importazione Nomi	Non è supportata l'importazione nomi oggetti di centrale.
Utilizzo Multi PIN	Non supportato. Usare il PIN inserito in Setup.
Abilitazione Integrazione	Non prevista.
Modulo da installare sulla centrale	Modulo EWEB PLUS o XWEB
Porta Integrazione Default	Porta TCP 2101
Configurazione Particolare	-
Note	<p><sup>1</sup>Le uscite possono essere gestite solo se impostate come uscite utente;</p> <p>La centrale supporta fino a 4 collegamenti differenti contemporaneamente, per ogni collegamento però deve necessariamente essere utilizzato un PIN diverso.</p> <p>Dalla versione 9.1.11 è supportata la memoria allarmi dei settori.</p> <p>Nelle versioni precedenti, non essendo supportata la memoria allarme dei settori sarà necessario creare delle azioni con le zone interessate.</p>

## Inserimento su aylook

Per inserire la centrale su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **PIN:** codice PIN da usare sul tastierino di aylook per usare la centrale.

NUOVA CENTRALE ANTI-INTRUSIONE

Nome:

Modello:


Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

PIN:

SALVA

## Centrale Elmo

Modello integrato	Elmo Proxima, ViDomo, Pregio, Titania e ETR
Gestione Sensori	Si (Allarme, Memoria Allarme) <sup>1</sup>
Gestione Settori	Si (Armata, Disarmata)
Gestione Uscite	Si <sup>2</sup>
Cancellazione memoria allarme	Non supportata.
Importazione Nomi	Supporta importazione nomi oggetti (è necessario avviarla manualmente, sincronizzazione lenta).
Utilizzo Multi PIN	Non supportato. Usare il PIN inserito in Setup.
Abilitazione Integrazione	Non prevista.
Modulo da installare sulla centrale	Non previsto.
Porta Integrazione Default	10000 (su ETR 10001) <sup>3</sup>
Configurazione Particolare	-
Note	<p>Non essendo supportata la memoria allarme dei settori, la centrale non va mai in allarme.</p> <p>È necessario creare delle azioni con le zone interessate.</p> <p>L'utente deve avere abilitata la Piccola Manutenzione.</p> <p>1. Non è supportata la manomissione delle zone.</p> <p>Non sono supportati i sensori collegati a ripetitori seriali RPX485.</p> <p>2. Le uscite devono essere impostate su Controllo Manuale</p> <p>3. La porta va abilitata dal menu Opzioni/Parametri di rete</p> 

## Inserimento su aylook

Per inserire la centrale su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **Utente:** numero dell'utente formato da 3 o 4 cifre;
- **Password:** PIN dell'utente utilizzato;
- **PIN:** codice PIN da usare sul tastierino di aylook per comandare la centrale.

NUOVA CENTRALE ANTI-INTRUSIONE

Nome: 
Modello:

Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

Utente:

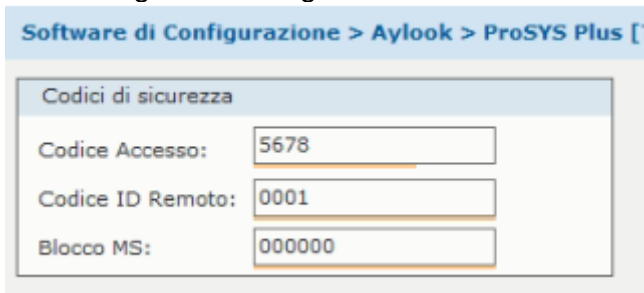
Password/Passphrase:

PIN:

SALVA

## Centrale Risco

### Risco Prosys+

<b>Modello integrato</b>	<b>Risco ProSys+, LightSys e LightSys+</b>
<b>Gestione Sensori</b>	Si (Allarme, Memoria Allarme, Manomissione)
<b>Gestione Aree</b>	Si (Armata, Disarmata, Memoria Allarme)
<b>Gestione Uscite</b>	Si (Configurate come Codice Utente)
<b>Cancellazione memoria allarme</b>	Non supportata.
<b>Importazione Nomi</b>	Non supportata.
<b>Utilizzo Multi PIN</b>	Non supportato. Usare il PIN inserito in Setup.
<b>Abilitazione Integrazione</b>	Non prevista.
<b>Modulo da installare sulla centrale</b>	Scheda di rete IP Dual Socket (per continuare a usare il cloud).
<b>Porta Integrazione Default</b>	TCP 1000
<b>Configurazione Particolare</b>	Supporta solo la seguente configurazione di sicurezza di base 
<b>Note</b>	Non si possono escludere le zone a centrale armata

### Risco ProSys 16/40/128

<b>Modello integrato</b>	<b>Risco ProSys 16/40/128</b>
<b>Gestione Sensori</b>	Si (Allarme, Memoria Allarme, Manomissione)
<b>Gestione Aree</b>	Si (Armata, Disarmata, Memoria Allarme)
<b>Gestione Uscite</b>	Si
<b>Cancellazione memoria allarme</b>	Non supportata.
<b>Importazione Nomi</b>	Non supportata.
<b>Utilizzo Multi PIN</b>	Non supportato. Usare il PIN inserito in Setup.
<b>Abilitazione Integrazione</b>	Non prevista.
<b>Modulo da installare sulla centrale</b>	Scheda di rete IP Dual Socket (per continuare a usare il cloud)
<b>Porta Integrazione Default</b>	1000
<b>Configurazione Particolare</b>	-
<b>Note</b>	-

## Inserimento su aylook

Per inserire la centrale su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **PIN:** codice PIN da usare sul tastierino di aylook per usare la centrale.

NUOVA CENTRALE ANTI-INTRUSIONE

Nome:

Modello:

Tipo connessione:
 ☒ IP
 ☐ Seriale

Indirizzo IP:

PIN:

SALVA

## Centrale UTC

Modello integrato	UTC Master
Gestione Sensori	Si (Allarme, Memoria Allarme, Manomissione)
Gestione Aree	Si (Armata, Disarmata, Memoria Allarme)
Gestione Uscite	Si
Cancellazione memoria allarme	Non supportata.
Importazione Nomi	Non supportata.
Utilizzo Multi PIN	Non supportato. Usare il PIN inserito in Setup.
Abilitazione Integrazione	Abilitazione sulla scheda di rete come da manuale.
Modulo da installare sulla centrale	Scheda di rete
Porta Integrazione Default	UDP 3001
Configurazione Particolare	-
Note	Supportata solo la configurazione di Security con tutti valori a 0.

## Abilitazione integrazione

Collegarsi alla centrale UTC via browser (consigliato Internet Explorer) e controllare che tutti i seguenti campi siano configurati correttamente come nelle seguenti schermate:

Schermata IP centrale (deve essere nella stessa classe di Aylook):



<b>User Authentication</b>	
<a href="#">Home</a>	
<a href="#">Login</a>	
<a href="#">Logout</a>	
<a href="#">Change user details</a>	
<b>Network Setup</b>	
<a href="#">Static address parameters</a>	
<a href="#">Central station parameters</a>	
<a href="#">Network Receiver</a>	
<a href="#">Email/TFTP parameters</a>	
<a href="#">Network Probing</a>	



### Setup the Universal Interface Network Parameters

Enter IP address:	192	168	5	80
Enter netmask:	255	255	255	0
Enter gateway address:	192	168	5	254



Spostarsi nel menù "Central Station Parameters" e aggiungere nella lista l'IP di Aylook per permettere la comunicazione sulla porta 3001 UDP:



**User Authentication**

- Home
- Login
- Logout
- Change user details

**Network Setup**

- Static address parameters
- Central station parameters**
- Network Receiver
- Email/TFTP parameters
- Network Probing

**Panel Setup**

- SecureStream: Event ACK interval
- SecureStream: Heartbeat interval
- Panel physical address
- Panel security password
- Twofish Encryption key

**Firewall Setup**

- Show all rules
- Add a new rule
- Delete a rule

**Utilities**

- Enable/Disable web interface
- Auto enroll
- Restart communications
- Local event log
- Printer event log
- CPU load
- System uptime
- Flash ROM version
- Restore factory defaults
- Reboot CPU
- Upload ROM image



### Setup the Central Station Network Parameters

#### Alarm Reporting Central Stations

Station	IP Address	Protocol	Port	Event Type	Encryption
1	0 0 0 0	TCP	0	None	None
2	0 0 0 0	TCP	0	None	None
3	0 0 0 0	TCP	0	None	None

#### Management Central Stations

Station	IP Address	Protocol	Port	Event Type	Encryption
4	192 168 5 125	UDP	3001	Computer	None
5	0 0 0 0	UDP	0	Computer	None
6	192 168 5 16	UDP	3001	Computer	None
7	0 0 0 0	UDP	0	Computer	None
8	0 0 0 0	UDP	0	Computer	None
9	0 0 0 0	UDP	0	Computer	None
10	0 0 0 0	UDP	0	Computer	None
11	0 0 0 0	UDP	0	Computer	None
12	0 0 0 0	UDP	0	Computer	None
13	0 0 0 0	UDP	0	Computer	None
14	0 0 0 0	UDP	0	Computer	None
15	0 0 0 0	UDP	0	Computer	None

Submit Reset all

Nel Menù "Network Receiver" assicurarsi di avere questi valori impostati:



**User Authentication**

- Home
- Login
- Logout
- Change user details

**Network Setup**

- Static address parameters
- Central station parameters
- Network Receiver**
- Email/TFTP parameters
- Network Probing



### Setup the Network Receiver parameters

Receiver number:	1
Line number:	1
Heartbeat interval(sec):	150
Receiver version:	<input type="radio"/> V1.9.0 and lower <input checked="" type="radio"/> V1.9.1 - V1.9.3 <input type="radio"/> V1.9.4 and higher

Submit Reset

Nel Menù "Network Probing" assicurarsi di avere questi valori impostati:



## Setup Network Probing

### User Authentication

[Home](#)

[Login](#)

[Logout](#)

[Change user details](#)

### Network Setup

[Static address parameters](#)

[Central station parameters](#)

[Network Receiver](#)

[Email/TFTP parameters](#)

[Network Probing](#)

Network Probing: ☒ off ☐ on

Submit

Reset

Nel Menù "SecureStream: Event ACK Interval" assicurarsi di aver impostato il Timeout a 0:



## Setup the Event Acknowledge Timeout

### User Authentication

[Home](#)

[Login](#)

[Logout](#)

[Change user details](#)

### Network Setup

[Static address parameters](#)

[Central station parameters](#)

[Network Receiver](#)

[Email/TFTP parameters](#)

[Network Probing](#)

### Panel Setup

[SecureStream: Event ACK interval](#)

[SecureStream: Heartbeat interval](#)

[Panel physical address](#)

[Panel security password](#)

[Twofish Encryption key](#)

Timeout (sec): 0

Submit

Reset

Nel Menù "SecureStream: Heartbeat interval" assicurarsi di aver impostato il Timeout a 5:



#### User Authentication

[Home](#)  
[Login](#)  
[Logout](#)  
[Change user details](#)

#### Network Setup

[Static address parameters](#)  
[Central station parameters](#)  
[Network Receiver](#)  
[Email/TFTP parameters](#)  
[Network Probing](#)

#### Panel Setup

[SecureStream: Event ACK interval](#)  
[SecureStream: Heartbeat interval](#)  
[Panel physical address](#)  
[Panel security password](#)  
[Twofish Encryption key](#)



#### Setup the Heartbeat Timeout

Heartbeat timeout:  ☒ seconds ☐ minutes

Impostare dal menù "Panel Physical Address" l'address sul valore 1:



#### User Authentication

[Home](#)  
[Login](#)  
[Logout](#)  
[Change user details](#)

#### Network Setup

[Static address parameters](#)  
[Central station parameters](#)  
[Network Receiver](#)  
[Email/TFTP parameters](#)  
[Network Probing](#)

#### Panel Setup

[SecureStream: Event ACK interval](#)  
[SecureStream: Heartbeat interval](#)  
[Panel physical address](#)  
[Panel security password](#)  
[Twofish Encryption key](#)



#### Setup the Panel Physical Address (Computer Address)

Panel address:

La "Security Password" di default è a zero ma può essere sostituita con altri valori:



<b>User Authentication</b>
<a href="#">Home</a>
<a href="#">Login</a>
<a href="#">Logout</a>
<a href="#">Change user details</a>
<b>Network Setup</b>
<a href="#">Static address parameters</a>
<a href="#">Central station parameters</a>
<a href="#">Network Receiver</a>
<a href="#">Email/TFTP parameters</a>
<a href="#">Network Probing</a>
<b>Panel Setup</b>
<a href="#">SecureStream: Event ACK interval</a>
<a href="#">SecureStream: Heartbeat interval</a>
<a href="#">Panel physical address</a>
<a href="#">Panel security password</a>
<a href="#">Twofish Encryption key</a>



#### Setup the Panel Security Password

Security password:	00	00	00	00	00
--------------------	----	----	----	----	----

Submit Reset

Il campo "Twofish Encryption Key" dovrebbe essere disattivato o compilato in questo modo:



<b>User Authentication</b>
<a href="#">Home</a>
<a href="#">Login</a>
<a href="#">Logout</a>
<a href="#">Change user details</a>
<b>Network Setup</b>
<a href="#">Static address parameters</a>
<a href="#">Central station parameters</a>
<a href="#">Network Receiver</a>
<a href="#">Email/TFTP parameters</a>
<a href="#">Network Probing</a>
<b>Panel Setup</b>
<a href="#">SecureStream: Event ACK interval</a>
<a href="#">SecureStream: Heartbeat interval</a>
<a href="#">Panel physical address</a>
<a href="#">Panel security password</a>
<a href="#">Twofish Encryption key</a>



#### Setup the Encryption Key

000	000	000	000	000	000	000	000	000	000	000	000	000	000	000	000	000	000
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

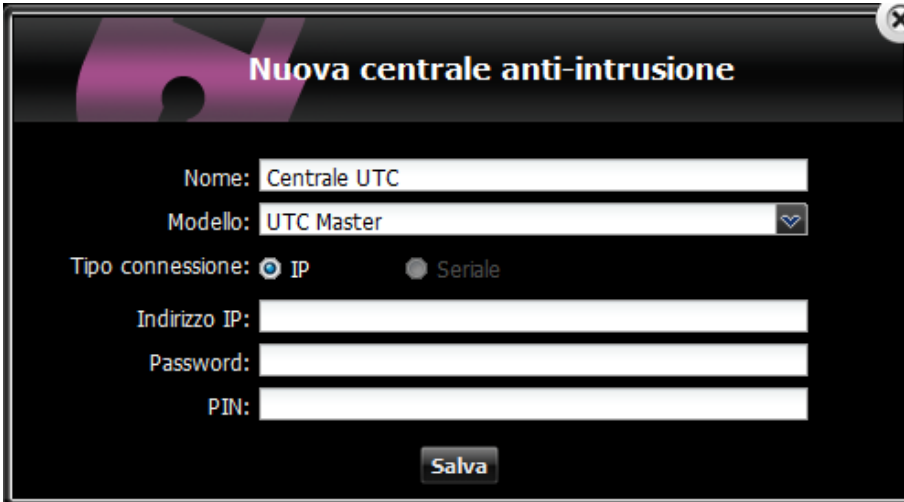
Submit Reset all

**Nota Bene:** Riavviare l'unità di rete prima di aggiungere la centrale su Aylook.

## Inserimento su aylook

Per inserire la centrale su aylook occorre compilare i seguenti campi di inserimento:

- **Nome:** nome con il quale verrà visualizzata la centrale;
- **Modello:** modello della centrale;
- **Indirizzo IP:** indirizzo IP della centrale;
- **Password:** Security Password;
- **PIN:** codice PIN inserito nel Setup della centrale.



**Nuova centrale anti-intrusione**

Nome:

Modello:

Tipo connessione: ☒ IP ☐ Seriale

Indirizzo IP:

Password:

PIN:

**Salva**