

CENTRALE SANS FIL AVEC RÉSEAU IP ET 4G**Réf. 1051/018****MANUEL D'INSTALLATION**

TABLE DES MATIÈRES

1	INTRODUCTION	3
2	DESCRIPTION DE LA CENTRALE	4
2.1	IDENTIFICATION DES PARTIES	4
2.2	Logement de la carte SIM GSM	5
2.3	Alimentation	6
2.4	Branchements filaires de la centrale	7
3	INSTALLATION	8
3.1	Pré-requis de base	8
3.2	Phases de montage de la centrale	8
4	DESCRIPTION ET UTILISATION DES CODES D'ACCES	10
4.1	Codes utilisateur	10
4.2	Code Master	10
4.3	Code Installateur	10
4.4	Code Coercition	10
5	PROGRAMMATION DE LA CENTRALE ZENO	11
5.1	PRÉDISPOSITION DU RÉSEAU LOCAL (LAN) Et INTERNET (WAN)	11
5.2	Installation du logiciel Finder	13
5.3	CONFIGURER LES RÉGLAGES DE RÉSEAU DE LA CENTRALE	14
6	ACCÈS AU PANNEAU DE CONTRÔLE DE LA CENTRALE	15
7	GESTION DES DISPOSITIFS	17
7.1	Apprentissage	17
7.2	Walk Test	19
7.3	Modifier d'un dispositif	20
7.3.1	Liste des attributs des détecteurs	22
7.3.2	Liste des attributs des détecteurs	23
7.3.3	Liste des attributs de la télécommande 1051/035	24
7.3.4	Liste des attributs du clavier 1051/025	25
7.3.5	Liste des attributs de la caméra 1051/004	25
7.4	Élimination d'un dispositif	26
7.5	Fonction « Désactiver » dispositif	26
7.6	Identification d'un dispositif	26
7.7	Demande d'informations photos/vidéos	27
7.8	Programmation de la sirène	27
8	REGLAGES DU SYSTEME	28
8.1	Info	28
8.2	Réglages	29
8.3	Paramètres système	31
8.4	Visualisation utilisateurs	33
8.5	Réglages de réseau	34
8.6	Réglage GSM	35
8.7	Rapports	36
8.8	Chargement	39
8.9	Capture événements	40
9	HISTORIQUE	41
10	RAPPORT EVENEMENTS	42
11	FIRMWARE	43
12	CARACTÉRISTIQUES TECHNIQUES DE LA CENTRALE	44
13	OUTILS DE GESTION À DISTANCE	45

1 INTRODUCTION

Le présent manuel décrit l'installation et la programmation du système anti-intrusion sans fil **URMET ZENO**, conçu pour tous les environnements résidentiels prévoyant le contrôle vidéo des alarmes. Basé sur la connectivité 4G/IP, ce système offre à l'utilisateur la possibilité d'une gestion à distance à travers le portail utilisateur et l'application **MyZeno** pour smartphone et il met à disposition des outils fiables de contrôle et de production de rapports.

Le système **ZENO** est intégralement bidirectionnel et il garantit un flux de communication continu entre la centrale et les dispositifs qui en font partie. L'exactitude des données transmises fait l'objet d'un monitoring constant.

Caractéristiques du système :

- CONFORME AUX CERTIFICATIONS EN 50131 DEGRÉ 2, CLASSE II
- DOUBLE COMMUNICATION BIDIRECTIONNELLE : RF 868 MHz et ZigBee 2,4 GHz
- COMMUNICATEUR 4G/IP INTÉGRÉ
- SUPERVISION
- APPLICATION GESTION GRATUITE

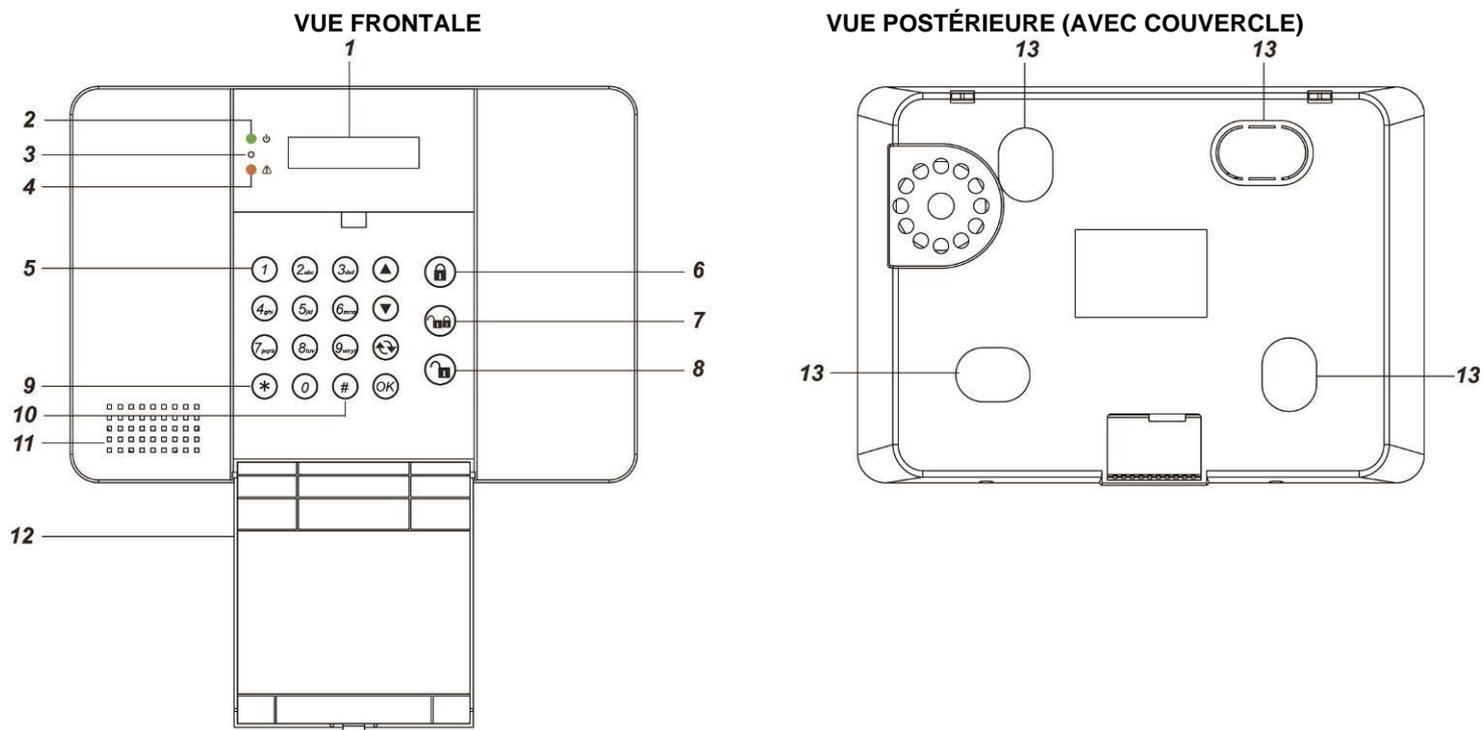
L'application **MyZeno** est gratuite et est téléchargeable sur Google Play (pour Android) et App Store (pour iOS).

L'application et le portail permettent les opérations suivantes:

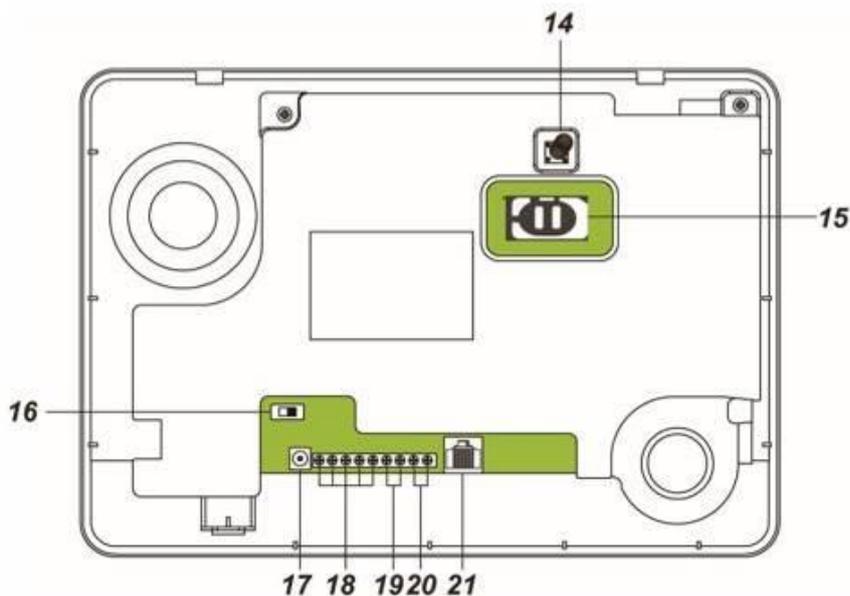
- activer, désactiver et partialiser l'installation
- visualiser l'état des dispositifs présents dans le système
- signaler des états d'alarme au moyen de dispositifs locaux (sirène interne et externe), d'appels vocaux, SMS, notifications Push, mails et protocoles numériques
- visualiser les images relatives à un événement d'alarme ou sur demande
- réaliser la fonction d'écoute environnementale bidirectionnelle
- visualiser l'historique des événements
- modifier le mot de passe
- gérer les notifications Push et les informations de base du système

Pour plus d'informations sur l'utilisation du portail et de l'application **MyZeno** sur téléphones iPhone et Android, se reporter au manuel correspondant disponible sur le site www.urmet.com, dans la section *Téléchargement / Documentation*.

2 DESCRIPTION DE LA CENTRALE



VISION POSTÉRIEURE (INTERNE)



2.1 IDENTIFICATION DES PARTIES

- 1. Écran LCD à rétroéclairage**
- 2. Voyant d'alimentation (vert)**
 VOYANT ALLUMÉ - Système correctement alimenté
 VOYANT ÉTEINT - Absence d'alimentation électrique sur secteur, batterie de secours complètement déchargée ou interrupteur sur OFF
 VOYANT CLIGNOTANT - Absence d'alimentation électrique sur secteur, système alimenté uniquement par la batterie de secours
- 3. Micro**
- 4. Voyant d'état de fonctionnement (jaune)**
 VOYANT ALLUMÉ - Système en condition d'anomalie
 VOYANT ÉTEINT - Système en état de fonctionnement normal

5. **Clavier**
 - ▲ : pour déplacer le curseur sur l'écran vers le haut
 - ▼ : pour déplacer le curseur sur l'écran vers le bas
 - ↺ : pour quitter la visualisation présente et revenir à la précédente
 - OK : confirmer une sélection ou une donnée
6. **Touche d'activation totale du système**
7. **Touche d'activation partielle du système**
8. **Touche de désactivation du système**
9. * : en appuyant sur cette touche pendant 3 secondes, l'on accède au menu Installateur
10. # : en appuyant sur cette touche pendant 3 secondes, l'on accède au menu Utilisateur
11. **Sirène interne et haut-parleur**
12. **Couvercle de fermeture du clavier**
13. **Prédispositions pour fixation murale**
14. **Dispositif anti-effraction (Tamper). Il détecte une effraction comme ouverture de l'habillage ou arrachage du mur.**
15. **Logement pour carte SIM téléphonique**
16. **Interrupteur d'activation batterie de secours rechargeable**
17. **Connecteur d'alimentation à jack (actuellement non utilisé)**
18. **Borniers filaires pour la connexion d'actionneurs et dispositif anti-effraction (Tamper) externes**
19. **Borniers pour utilisations futures**
20. **Borniers pour utilisations futures**
21. **Port Ethernet de programmation locale**

2.2 LOGEMENT DE LA CARTE SIM GSM

La centrale **Urmet ZENO** 1051/018 exploite la connectivité **4G/IP** intégrée pour contrôler les états du système et des dispositifs. Pour exploiter les fonctions 4G/IP, il est nécessaire de loger une carte SIM active pour l'utilisation de la phonie et de la transmission de données sur la centrale.

En l'absence de cette carte SIM, la centrale signale dans tous les cas une série d'anomalies causées par l'absence de connexion à Internet. La centrale Zeno a en effet été conçue pour fonctionner en toute circonstance avec le communicateur téléphonique GSM actif et l'absence de carte SIM est toujours signalée.

La carte SIM GSM doit être mise en place dans le logement prévu à cet effet au dos de la Centrale :



LOGEMENT CARTE SIM

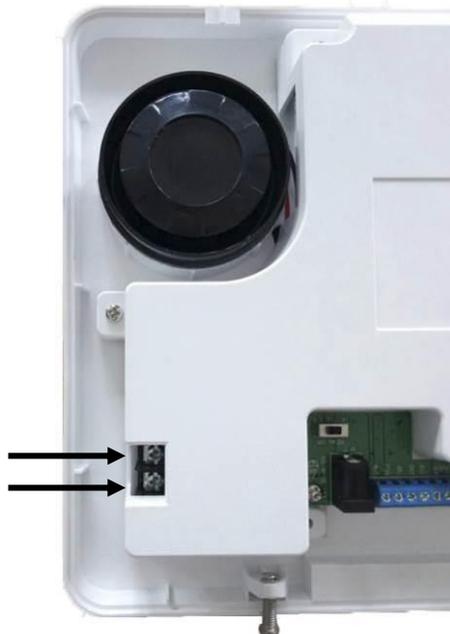
- Débloquer l'accès en faisant coulisser le porte-carte vers la gauche
- Soulever le porte-carte et mettre en place délicatement la carte SIM avec les contacts orientés vers le bas.
- Abaisser le porte-carte et bloquer l'accès en le faisant coulisser vers la droite.

<NOTE>

Désactiver le code PIN de la carte SIM avant de mettre en place cette dernière dans la centrale à moins qu'il n'ait déjà été désactivé (utiliser des cartes SIM spéciales pour ce type d'application).

2.3 ALIMENTATION

La centrale **Urmet ZENO** 1051/018 est alimentée sur secteur (230 Vca). Brancher le câble fourni à cet effet aux deux bornes sur le côté de la centrale, comme indiqué sur la figure ci-dessous.



Après avoir branché le câble au secteur d'alimentation électrique et avoir alimenté la centrale, placer sur la position **ON** l'interrupteur de la batterie.



Batterie rechargeable

La centrale renferme une batterie rechargeable qui fait office de batterie de secours en l'absence d'alimentation.

Pendant le fonctionnement normal, l'alimentation sur secteur est utilisée pour alimenter la centrale et simultanément pour charger la batterie. 72 heures environ sont nécessaires pour obtenir la pleine charge de la batterie.

La position par défaut de l'interrupteur de la batterie est la position **OFF**. Dans cette condition, la batterie n'est pas chargée quand la centrale est branchée au secteur d'alimentation électrique et elle ne peut pas être utilisée comme batterie de secours en cas de coupure d'alimentation. Il est par conséquent nécessaire de placer l'interrupteur sur **ON** après avoir alimenté la centrale.

<NOTE>

- Si l'alimentation est absente et que la batterie est presque déchargée, l'état de batterie déchargée est signalé, sur l'écran et par communication à distance, et la sirène interne est désactivée pour économiser l'énergie.
- L'autonomie de la centrale alimentée uniquement sur batterie est 15 heures environ, en fonction de son

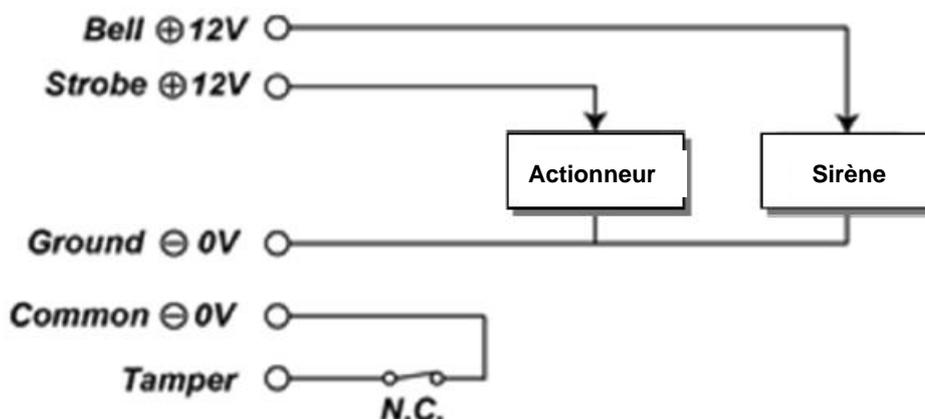
comportement pendant l'absence d'alimentation sur secteur.

- Quand la centrale fonctionne uniquement sur batterie, elle utilise une modalité de fonctionnement à basse consommation et elle limite les interactions avec les connexions à distance : elle continue à envoyer les notifications des événements mais elle ne peut recevoir de commandes à distance en cas de demande de connexion à distance à travers l'application.

2.4 BRANCHEMENTS FILAIRES DE LA CENTRALE

La centrale 1051/018 dispose des branchements filaires suivants :

BORNES	DESCRIPTION
BELL	Positif pour sirènes NON auto-alimentées à 12 Vcc : présent en condition d'alarme (12 Vcc, MAX. 0,4 A)
STB	Positif pour actionneurs à 12 Vcc (Strobe) : présent en condition d'alarme (12 Vcc, MAX. 0,4 A)
GND / COM	Masse alimentations
TMP	Entrée ligne de garde 24 h externe pour détection anti-effraction tamper (normalement fermée) <i>NB : pour effacer les notifications d'effraction sur ce type d'entrée, il est nécessaire d'éliminer la présence du circuit ouvert avant de désactiver la détection (voir menu correspondant : « Tamper externe »)</i>



3 INSTALLATION

3.1 PRE-REQUIS DE BASE

La façon la plus simple de connaître les fonctions du système et de le rendre opérationnel rapidement est de programmer tous les dispositifs et les accessoires et de les positionner et de les monter.

La centrale est conçue pour un montage mural. Pour garantir une bonne installation, il est recommandé de tenir compte des recommandations suivantes :

- La centrale nécessite une connexion Ethernet et il est recommandé de la doter d'une carte SIM.
- La centrale doit être installée dans une position dissimulée, non visible de l'extérieur.
- Éviter de monter la centrale à proximité de grands objets métalliques qui pourraient avoir un effet sur le niveau des signaux radio.
- La centrale doit être protégée à l'aide de détecteur de telle sorte qu'aucun intrus ne puisse s'en approcher sans avoir auparavant déclenché une alarme.

3.2 PHASES DE MONTAGE DE LA CENTRALE

Étape 1. Desserrer les 2 vis sur la partie basse de la centrale (**Figure 1**) et décrocher la base du corps supérieur de la centrale.

ATTENTION : pour ouvrir l'habillage de la centrale, avant de faire pivoter le couvercle pour le décrocher de la base, le faire glisser pour en décrocher les dents de fixation à la base.

Étape 2. La base présente 4 zones pré-découpées qui permettent de réaliser les trous de montage mural, 2 zones pré-découpées sur les côtés et 1 trou sur la partie inférieure pour le passage des câbles (**Figure 2**).

Figure 1

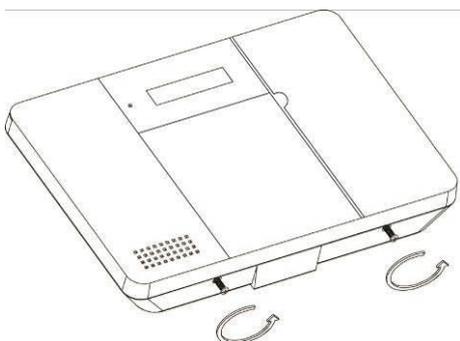
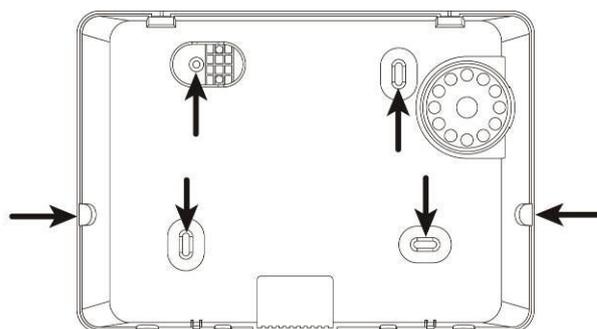


Figure 2



Étape 3. Utiliser la base comme gabarit pour marquer la position des trous de montage mural (**Figure 3**). En utilisant les chevilles fournies à cet effet, fixer la base au mur (**Figures 4 et 5**).

Figure 3

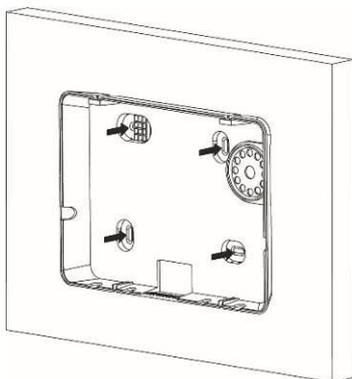


Figure 4

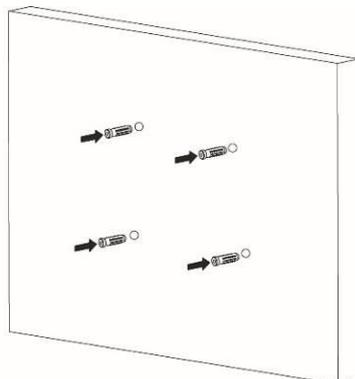
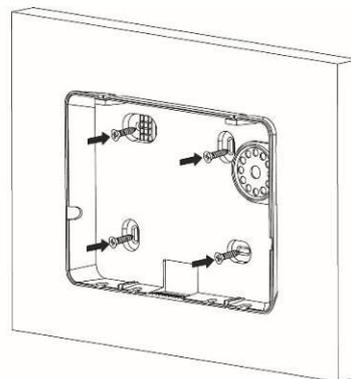


Figure 5



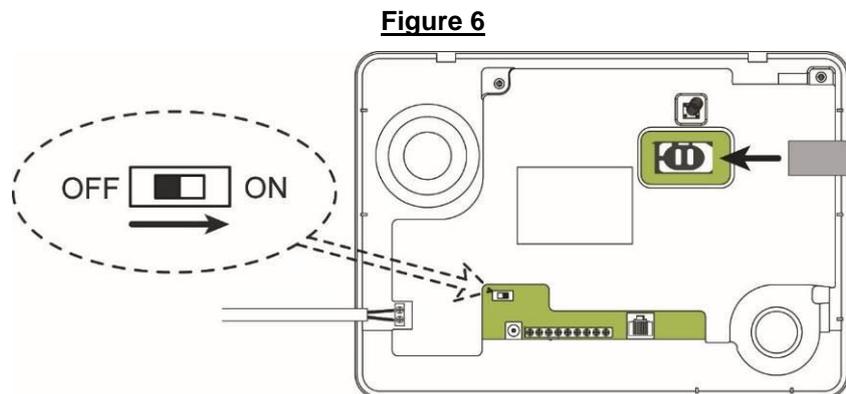
Étape 4. Au besoin, brancher les actionneurs et le dispositif anti-effraction externes.

Étape 5. Mettre en place une carte SIM dans le logement prévu à cet effet. Avant de mettre place la carte SIM, s'assurer que le code PIN de la carte a été activé.

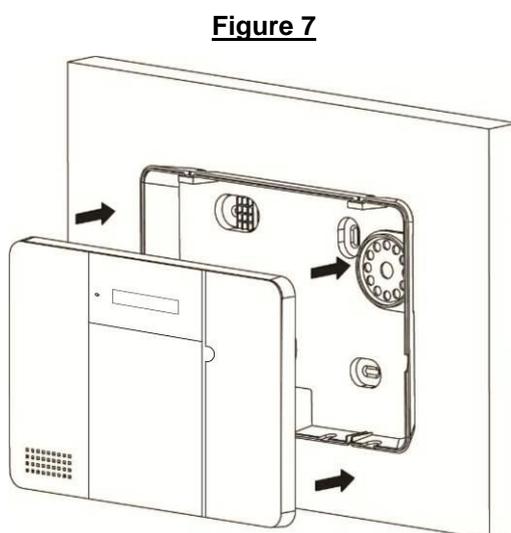
NB : un certain temps peut s'avérer nécessaire à l'enregistrement de la carte SIM sur le réseau mobile ; aussi, après l'allumage de la centrale attendre quelques minutes avant de l'utiliser.

Étape 6. Alimenter la centrale (**Figure 6**).

Étape 7. Uniquement après avoir allumé la centrale, placer l'interrupteur de la batterie sur **ON**.



Étape 8. Accrocher le corps supérieur de la centrale à la base et le fixer à l'aide des vis prévues à cet effet (**Figure 7**).



Étape 9. L'installation de la centrale est à ce stade terminée et le voyant vert de l'alimentation doit être allumé.

PRÉ-REQUIS DU SYSTÈME

Pour installer le système, l'ordinateur au moyen duquel la programmation est effectuée doit avoir les caractéristiques suivantes :

- Logiciel d'exploitation Microsoft Windows 98, ME, NT4.0, 2000, XP, Vista (7, 8 ou 10).
- Microsoft Internet Explorer 5.x ou suivant ou Google Chrome (conseillé).
- Processeur : Intel Pentium II 266 MHz ou supérieur
- Mémoire : 64 Mo ou plus
- Résolution VGA : 800 x 600 ou supérieure

4 DESCRIPTION ET UTILISATION DES CODES D'ACCES

Pour fournir la sécurité maximale pendant l'utilisation du système, la Centrale du système ZENO 1051/018 offre différents niveaux d'autorisation pour les différentes situations de fonctionnement.

4.1 CODES UTILISATEUR

Les codes Utilisateur servent à effectuer les opérations d'activation et de désactivation du système ou bien sont utilisés comme codes de premier niveau pour accéder aux différents menus de la centrale.

Dans la Centrale, il est possible de mémoriser jusqu'à 20 codes PIN Utilisateur, chacun d'eux étant associable à un nom qui est ensuite visualisé dans l'historique des événements de la centrale. Les noms peuvent être créés lors de la première programmation du système ou dans un deuxième temps quand il est nécessaire de les modifier, de les éliminer ou de les ajouter.

- Le **Code PIN Utilisateur 1**, qui ne peut pas être éliminé mais qui peut être modifié, est réglé par défaut sur la valeur **1234**.
- En revanche, les Codes PIN Utilisateur 2-20 ne sont pas pré-réglés et ils doivent être saisis par l'utilisateur.
- Le Code PIN Utilisateur représente le premier niveau de mot de passe. L'écran visualise le message **Saisir code** dès que l'on commence à saisir son propre Code PIN Utilisateur.

4.2 CODE MAITRE

Le code Master, qui s'affiche après avoir appuyé pendant 3 sec. sur la touche # et saisi le Code PIN Utilisateur, permet d'accéder au menu de Programmation Utilisateur qui contient les configurations qui peuvent être exécutées par l'utilisateur.

- Le **Code Master** est réglé par défaut sur la valeur **1111**.

4.3 CODE INSTALLATEUR

Le code Installateur, qui s'affiche après avoir appuyé pendant 3 sec. la touche * et saisi le Code PIN Utilisateur, permet d'accéder au menu Installateur pour la configuration de tous les paramètres de la centrale.

- Le **Code Installateur** réglé par défaut sur la valeur **7982**.

4.4 CODE CONTRAINTE

Le code Contrainte peut être utilisé pour générer une Alarme Panique silencieuse quand l'utilisateur est contraint de désactiver le système sous la menace. Une demande de secours est générée, via SMS et Notifications, sans être découvert.

- Le code de Coercition n'a pas de valeurs par défaut et doit être programmé pour être utilisé.

Attention. Il est recommandé de conserver les codes en lieu sûr.

5 PROGRAMMATION DE LA CENTRALE ZENO

La Centrale peut être programmée dans deux modalités différentes :

1. en utilisant un PC, pour sa configuration complète, et la connexion à Internet
2. à l'aide du clavier tactile et de l'écran de la centrale, pour son utilisation de base

Il est recommandé d'effectuer la première installation avec un PC et d'utiliser la deuxième modalité, avec clavier et écran, pour les interventions rapides d'entretien.

Les pages suivantes décrivent la première modalité, la deuxième est quant à elle décrite dans le *Manuel d'utilisation et de programmation de la Centrale*.

5.1 PRÉDISPOSITION DU RÉSEAU LOCAL (LAN) ET INTERNET (WAN)

Pré-requis de connexion à Internet.

Pour garantir le parfait fonctionnement du système Zeno, la centrale doit être connectée à un routeur ADSL et/ou au réseau de téléphonie mobile 4G/3G/GPRS à l'aide d'une carte SIM activée pour le trafic de données à installer dans la centrale. Pour garantir le plus haut degré de sécurité et les prestations maximales, il est recommandé de prévoir les deux connexions :

- ☞ le réseau ADSL garantit les meilleures performances d'accès à distance et de chargement de vidéos et photos
- ☞ la double connexion garantit le parfait fonctionnement de toutes les fonctions du système en cas d'interruption d'une des deux connexions

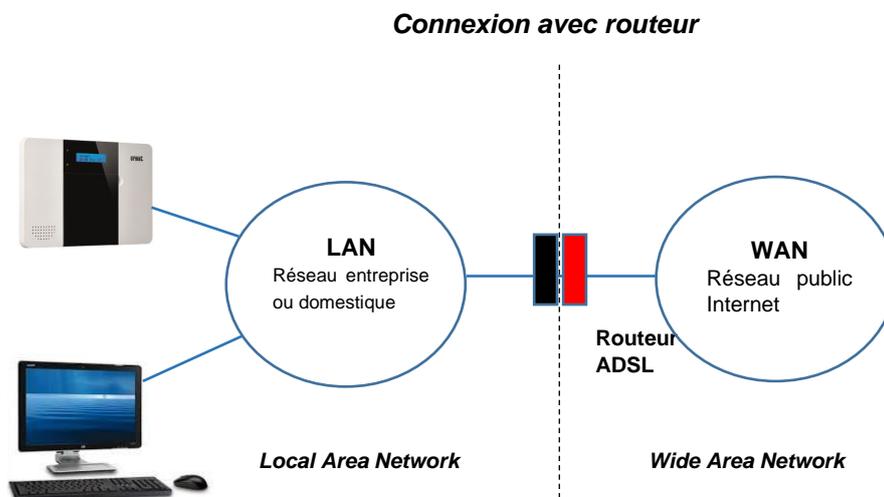
Pour garantir le bon fonctionnement, sur le routeur, ne sont nécessaires ni la fonction de Port Forwarding ni le service DDNS (Dynamic Domain Name System). Il est en revanche recommandé d'activer le service DHCP sur le routeur.

Connexion de la centrale à un PC pour la mise en service

La mise en service de la centrale doit être effectuée à l'aide d'un PC.

La connexion peut être réalisée de deux manières :

- ☞ à travers le routeur ADSL utilisé pour la connexion de la centrale au réseau Internet, en utilisant le câble Ethernet fourni à cet effet (méthode conseillée) ;
- ☞ par connexion directe au PC en utilisant le câble Ethernet fourni à cet effet.



Pour se connecter à sa propre centrale, utiliser un PC connecté au routeur.

La centrale est déjà configurée pour la plupart des configurations de réseau possibles. Les paramètres par défaut sont les suivants :

- IP = **192.168.1.130**
- DNS = 8.8.8.8 ; DNS2 = 8.8.4.4
- Passerelle = 192.168.1.1
- Masque de réseau = 255.255.255.0
- DHCP = OFF

Si le routeur utilisé est doté de serveur DHCP, il est conseillé d'activer l'adressage DHCP sur la centrale également, à l'aide du programme Finder, comme indiqué dans le paragraphe suivant.

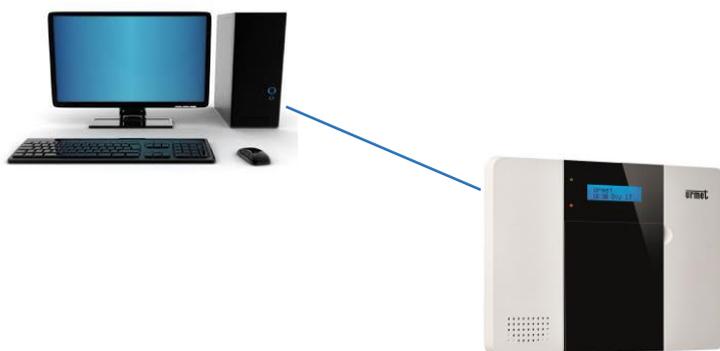
Si le routeur n'est pas doté de serveur DHCP, il est nécessaire de configurer une adresse statique de la même famille que le réseau LAN utilisé.

ATTENTION ! Si le routeur n'est pas doté de serveur DHCP et que, sur la centrale, l'adressage DHCP est activé, celle-ci n'est pas joignable.

<NOTE>

Dans le cas où sur le réseau local, existerait déjà un dispositif avec adresse statique IP 192.168.1.130, il est nécessaire de le débrancher temporairement (si possible) ou bien d'utiliser la connexion directe ci-après et de configurer une adresse IP différente sur la centrale ou l'adressage DHCP.

Connexion directe :



Pour pouvoir configurer la centrale avec la connexion directe à un PC, procéder d'une des manières suivantes :

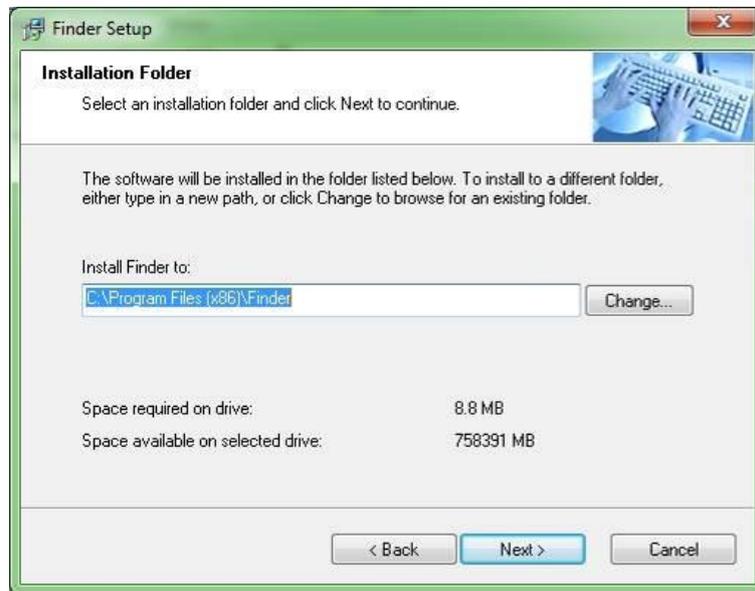
1. Configurer le PC avec une adresse IP de la même famille que la centrale : utiliser une adresse 192.168.1.xxx (avec xxx différent de 130) et un masque de réseau 255.255.255.0
2. Ou bien, à l'aide du programme Finder (voir plus bas), configurer la centrale avec une adresse IP de la même famille que le PC. Par exemple, si le PC a une adresse appartenant à la famille 192.168.0.xxx, configurer la centrale avec une adresse appartenant à la même famille, mais différente de celle du PC et un masque de réseau 255.255.255.0.

5.2 INSTALLATION DU LOGICIEL FINDER

CETTE INSTALLATION EST NÉCESSAIRE UNIQUEMENT À LA PREMIER UTILISATION

Afin de programmer et de contrôler la centrale, un logiciel spécial est fourni, « **Finder** » (qui fonctionne sous Microsoft Windows 7 ou supérieur), qui permet d'identifier et de localiser la centrale sur le réseau local (LAN). Pour installer le logiciel « **Finder** » :

- Phase 1.** Se connecter au site Internet www.urmet.com et accéder aux ressources de la centrale **Zeno 1051/018**, dans la section *Produits-Anti-effraction*. En fin de manuel, figure le Code QR du lien.
- Phase 2.** Télécharger et lancer le programme **Finder**.
- Phase 3.** Double-cliquer sur l'icône pour lancer l'installation de l'application. En cas de blocage du PC dû à la présence de protections ou d'un pare-feu, permettre au système d'installer l'application conformément aux modalités prévues par le logiciel d'exploitation utilisé.



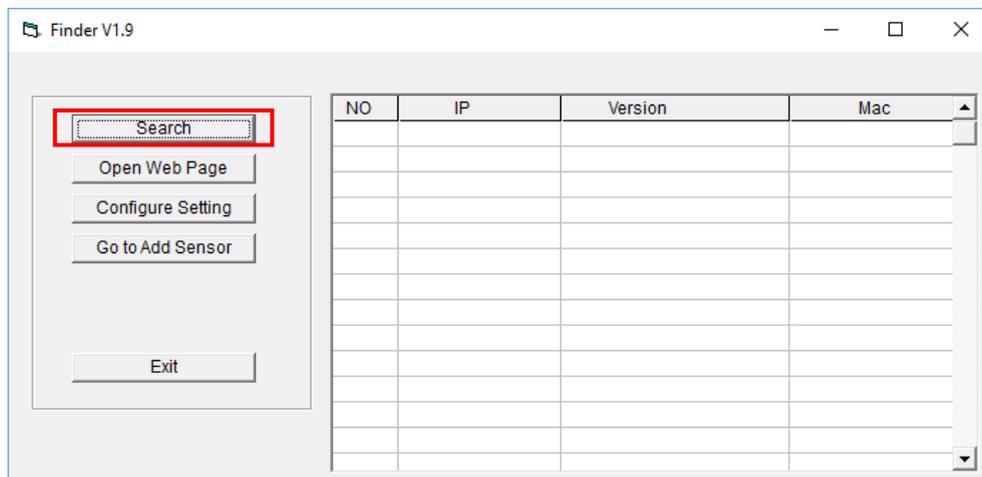
Phase 4. Cliquer sur « **Change** » pour sélectionner le dossier du fichier ; s'il n'est pas nécessaire de modifier le parcours, cliquer sur « **Next** » pour continuer.

Phase 5. Cliquer sur « **Next** » pour lancer l'installation. Au terme de l'installation, cliquer sur « **Finish** ».



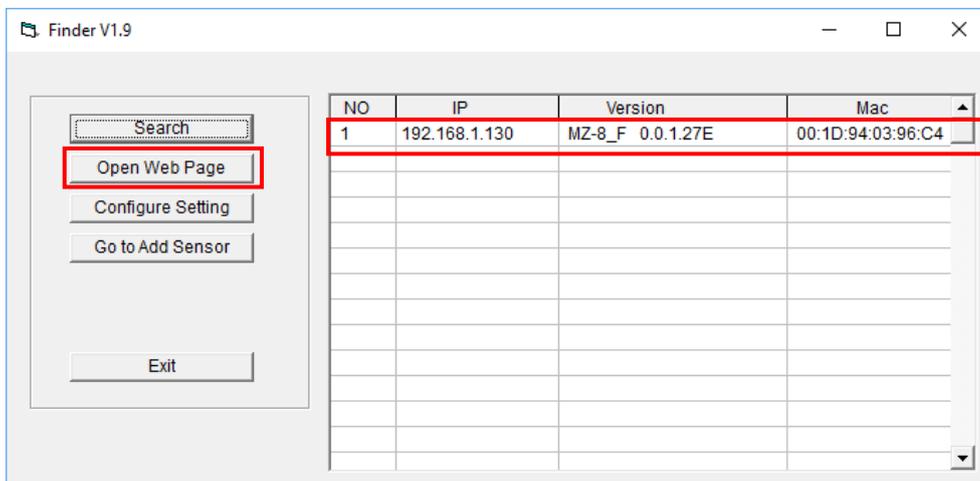
Phase 6. Sur le bureau, une nouvelle icône s'affiche : [Finder.exe](#)

Phase 7. Double-cliquer sur « **Finder.exe** » pour lancer l'installation. La fenêtre suivante s'affiche :



Phase 8. Cliquer sur « **Search** » : le programme lance la recherche des adresses IP connues sur le réseau local.

Phase 9. Identifier l'adresse IP de la centrale dans la liste. S'affichent également l'adresse MAC et la version firmware du produit.

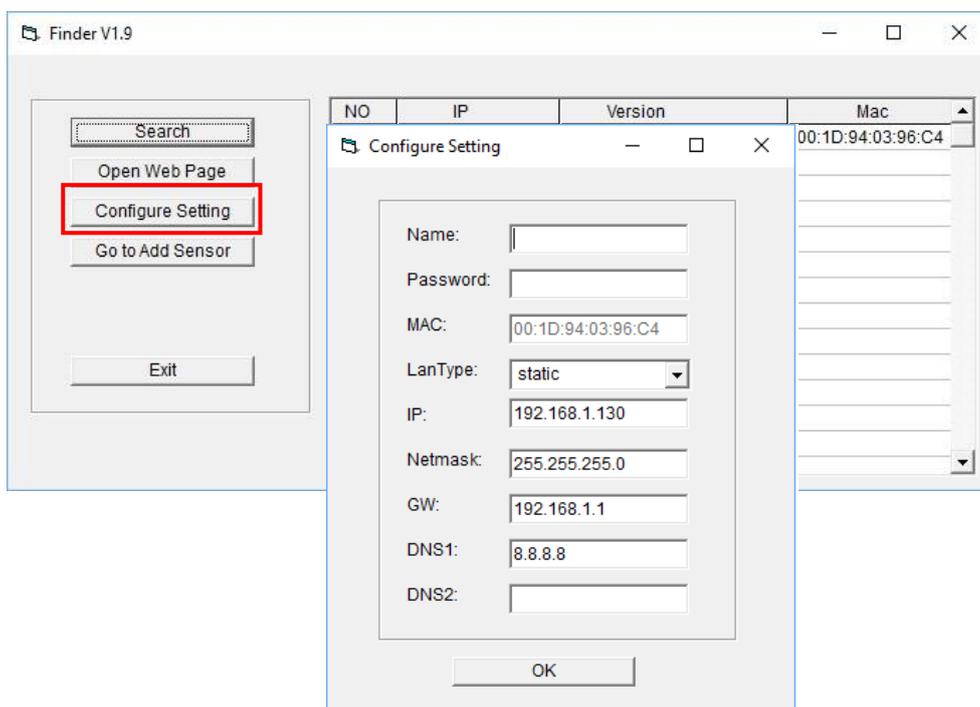


Phase 10. Une fois la centrale identifiée, la sélectionner et cliquer sur « **Open Web Page** » pour se connecter au panneau de contrôle local de la centrale **Zeno**. Les données d'accès sont ensuite demandées (voir chapitre 4).

5.3 CONFIGURER LES RÉGLAGES DE RÉSEAU DE LA CENTRALE

Cette fonction sert uniquement dans le cas où l'on souhaiterait configurer manuellement les réglages de réseau.

Phase 1. Sélectionner la centrale puis cliquer sur **Configure Setting** ; ensuite, s'affiche la fenêtre suivante :



Phase 2. Saisir le nom utilisateur et le mot de passe pour la configuration des réglages.

Nom Utilisateur (prédéfini): **admin**

Mot de passe (prédéfini) : **cX+HsA*7F1**

ATTENTION ! Pour se conformer à certaines dispositions anti-piratage, la Centrale Zeno adopte le mécanisme suivant de génération du mot de passe. Après la saisie du mot de passe prédéfini **cX+HsA*7F1**, le système demande, au premier accès, de le modifier en saisissant son propre mot de passe. Si tel n'est pas le cas en l'espace d'une heure, le système empêche l'accès et il est alors nécessaire de couper l'alimentation de la centrale et de la rétablir pour effectuer l'opération complète.

NB : après une réinitialisation des données par défaut, la centrale adopte à nouveau le mot de passe prédéfini.

Phase 3. Sélection de **DHCP** ou **Static** comme LAN Type. En sélectionnant **Static**, il est ensuite possible de saisir manuellement les informations de réseau restantes. En sélectionnant **DHCP**, il n'est ensuite plus possible de modifier les autres informations de réseau.

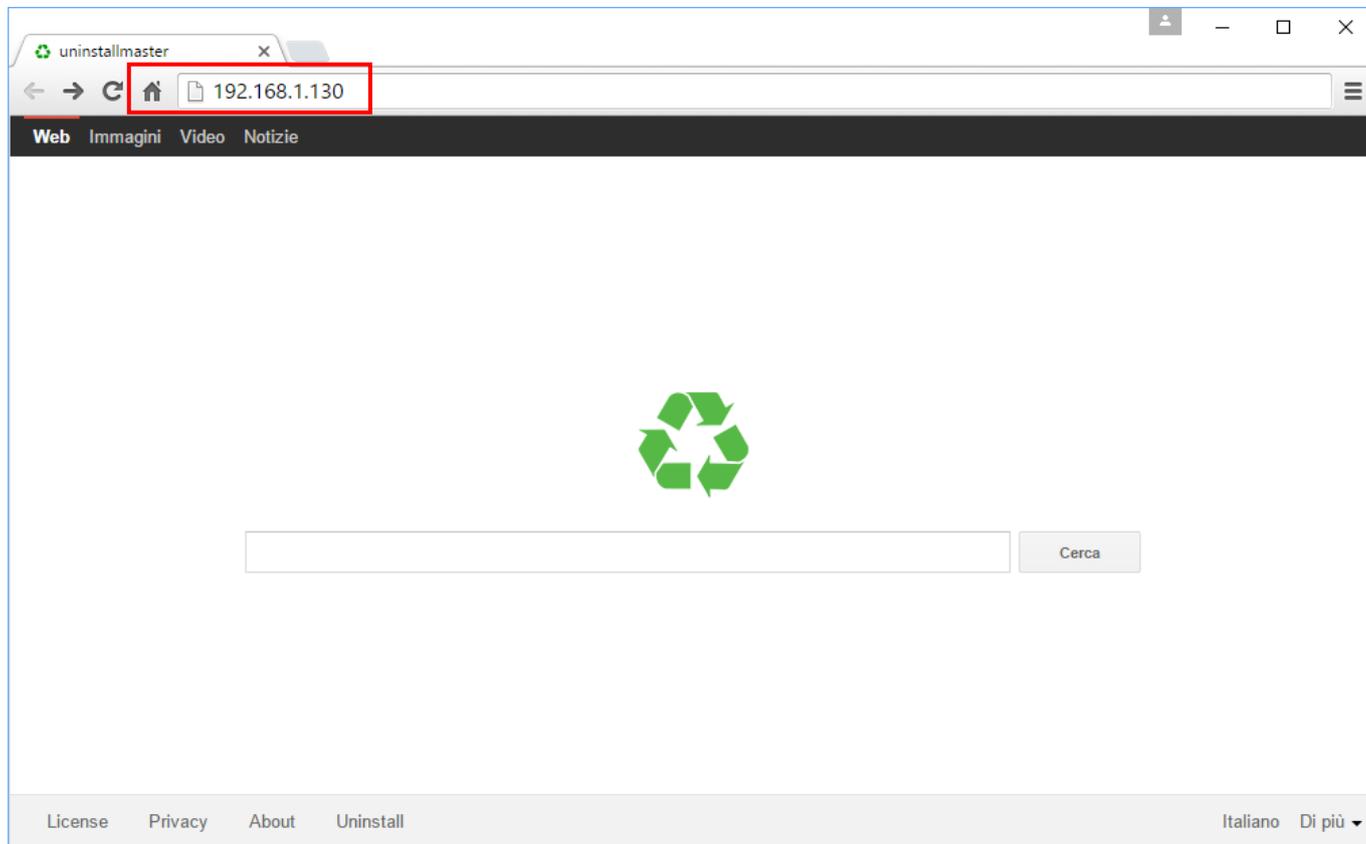
Phase 4. Après avoir saisi un nouveau réglage, cliquer sur **OK** pour confirmer. Si le nom utilisateur et le mot de passe sont corrects, une fenêtre affiche le message suivant : **Status: Configure success!** (État: configuration réussie!)

<NOTE> L'option « Go to add sensor » n'est pas disponible sur la présente version.

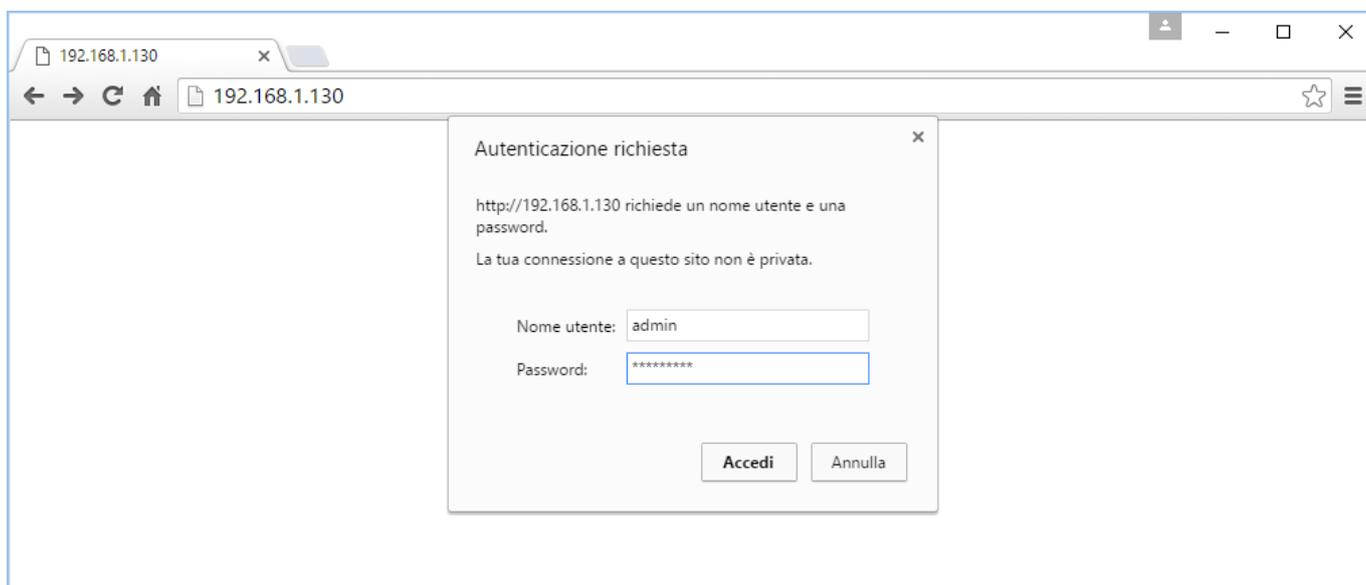
6 ACCÈS AU PANNEAU DE CONTRÔLE DE LA CENTRALE

Phase 1. Sélectionner la centrale dans le logiciel Finder et cliquer sur « Open Web Page » pour se connecter au panneau de contrôle.

Différemment, utiliser un navigateur et saisir, dans le champ des adresses, l'adresse IP de la centrale indiquée par le logiciel Finder.



Phase 2. Dans la fenêtre de demande des données d'accès, saisir le nom utilisateur et le mot de passe puis appuyer sur « **Accéder** ».



Nom Utilisateur par défaut : **admin** Mot de passe par défaut : **cX+HsA*7F1**

Phase 3. La page ci-dessous visualise l'accès au panneau de contrôle local avec les informations correspondantes relatives à la centrale.



The screenshot shows a web interface with a navigation menu at the top. The menu items are: Bienvenue (highlighted with a red box), Contrôles, Centrale, Dispositifs, Paramètres, Utilisateur, Historique, Capture événements, Rapport événements, GSM, Réseau, Rapport, and Uploader. Below the menu, there are two more items: Firmware and Déconnexion. The main content area displays the following information:

Bienvenue dans la centrale !

Version Firmware: ML-8TP_F 1.0.3.4D
Version ZigBee : 3.4.2.6.2
Version GSM : 1575B11SIM5320E
Adresse MAC : 00:1D:94:06:44:B4

7 GESTION DES DISPOSITIFS

Dans le présent chapitre, sont décrites les modalités pour apprendre, modifier, éliminer et contrôler les différents dispositifs qui peuvent constituer le système **Zeno**. Il est possible d'acquérir jusqu'à **50** dispositifs, un total de **6** détecteurs maximum avec appareil-photo et un total de **4** caméras IP 1051/004.

L'image ci-dessous montre une page de gestion sans dispositifs configurés :

Configuration dispositifs

Adresse	Type	Nom	Attribut	Conditions	Batterie	Autoprotection	Exclure	RSSI	État	
<input type="checkbox"/> 1	Contact magnétique	21 17/19	Instantanée A							Modifier
<input type="checkbox"/> 2	Télécommande		A PANIQUE							Modifier
<input type="checkbox"/> 3	Clavier		A PANIQUE							Modifier

Surveillance

Programmation sirène

Mode apprentissage

Dispositif: Code: Nom:

Les pages de configuration des dispositifs sur le panneau de contrôle sont les suivantes :

1. page PROGRAMMATION SIRÈNE → pour programmer une sirène externe
2. page APPRENTISSAGE → pour apprendre un dispositif à l'intérieur de la centrale
3. page WALK TEST → pour effectuer un test de portée d'un dispositif
4. fonction AJOUTER DISPOSITIF RF → non disponible
5. page MODIFIER → pour programmer les dispositifs et associer les attributs
6. fonction ÉLIMINER → pour éliminer un dispositif précédemment acquis
7. fonction DÉACTIVER → pour désactiver temporairement un dispositif
8. fonction IDENTIFICATION → pour vérifier le signal d'un dispositif
9. page SURVEILLANCE : demande IMAGE/VIDÉO → pour obtenir manuellement une image ou une vidéo
10. page CONTRÔLE ACTIONNEURS → pour le contrôle d'actionneurs et volets roulants

7.1 APPRENTISSAGE

Phase 1. Alors que la centrale est **Désactivée**, appuyer sur la touche « **Début Apprentissage** », sur la page des dispositifs. La centrale accède à la phase d'apprentissage et un timeout de 20 minutes s'active pour effectuer l'apprentissage des dispositifs. Au terme de cette durée, la centrale quitte automatiquement la modalité d'apprentissage.

Phase 2. Appuyer sur le bouton d'apprentissage du dispositif. Pour certains dispositifs (voir le manuel des instructions de chaque produit), maintenir enfoncé le bouton d'apprentissage pendant 10 secondes environ pour transmettre un code d'apprentissage (pour plus de détails, consulter le manuel du dispositif).

Phase 3. Si la centrale reçoit le code d'apprentissage, elle émet 2 bips brefs ; cliquer sur le bouton « **Mettre à jour** » pour visualiser les informations du dispositif sur la page. En revanche, si la centrale émet 1 bip long, cela indique que le dispositif a déjà été acquis par la centrale.

Bienvenue Contrôles Centrale Dispositifs Paramètres Utilisateur Historique Capture événements Rapport événements GSM Réseau Rapport Uploader
Firmware Firmware/RF Déconnexion

Centrale en mode Apprentissage

Apprentissage dispositif

Appuyer sur "Arrêt" au terme d'un apprentissage ou d'un Test

Mettre à jour Arrêt

#	Dispositif	Type	RSSI
		Élément non trouvé	
#	ID	Type	
		Élément non trouvé	

Début test

<NOTE>

- Si la centrale émet 2 bips brefs pendant l'apprentissage des dispositifs mais ne visualise pas les informations du dispositif lorsque la page est rafraîchie, cela indique que la centrale a reçu le code de supervision du dispositif au lieu du code d'apprentissage. Répéter la procédure d'apprentissage.

Bienvenue Contrôles Centrale Dispositifs Paramètres Utilisateur Historique Capture événements Rapport événements GSM Réseau Rapport Uploader
Firmware Firmware/RF Déconnexion

Apprentissage dispositif

Appuyer sur "Arrêt" au terme d'un apprentissage ou d'un Test

Mettre à jour Arrêt

#	Dispositif	Type	RSSI
		Élément non trouvé	
#	ID	Type	
<input checked="" type="checkbox"/> 9	RF:00557f10	Contact magnétique	

Ajouter Tout ajouter

Début test

Phase 4. Cliquer sur la case du dispositif et sélectionner « **Ajouter** » pour inclure le dispositif à la centrale.

Phase 5. La centrale affiche le message « Mise à jour effectuée ». Le dispositif est acquis par le système.

<Note>

La centrale est en mesure d'effectuer le test de Supervision sur les dispositifs uniquement si, en phase d'apprentissage, sur la page « Paramètres Centrale », le test de Supervision a été précédemment activé. En revanche, si les dispositifs sont appris avec le test de Supervision désactivé, il n'est pas possible de l'activer ensuite mais il est nécessaire d'éliminer et de réapprendre les dispositifs que l'on souhaite soumettre au test de Supervision.

Bienvenue Contrôles Centrale Dispositifs Paramètres Utilisateur Historique Capture événements Rapport événements GSM Réseau Rapport Uploader
Firmware Firmware/RF Déconnexion

Mise à jour effectuée

Apprentissage dispositif

Appuyer sur "Arrêt" au terme d'un apprentissage ou d'un Test

Mettre à jour Arrêt

#	Dispositif	Type	RSSI
3	Dispositif 4	Contact magnétique	0
#	ID	Type	
		Élément non trouvé	

Début test

Phase 6. Suivre la procédure de la Phase 2 à la Phase 5 pour acquérir d'autres dispositifs. Pour quitter la modalité d'apprentissage de la centrale et en rétablir le fonctionnement normal, cliquer sur le bouton « **Fin** ». Ensuite, s'affiche la page de l'apprentissage et du Walk test.

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)
[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Centrale en mode Standard

Apprentissage dispositif

[Début apprentissage](#)
[Début test](#)

Phase 7. En cliquant à nouveau sur le menu « Dispositifs », tous les dispositifs précédemment acquis s'affichent.

Exemple de dispositifs présents dans la centrale après avoir effectué l'apprentissage :

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)
[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Configuration dispositifs

Adresse	Type	Nom	Attribut	Conditions	Batterie	Autoprotection	Exclure	RSSI	État	
<input type="checkbox"/> 1	Contact magnétique	21 17/19	Instantanée A							Modifier
<input type="checkbox"/> 2	Télécommande		A PANIQ SILENC							Modifier
<input type="checkbox"/> 3	Clavier		A PANIQUE							Modifier
<input type="checkbox"/> 4	Contact magnétique		Commun Retardé 1							Modifier

[Supprimer](#) [Exclure](#) [Rétablir](#) [Identifier](#) [Vérifier version](#)

Surveillance

SIGNIFICATION DES COLONNES :

Adresse : numéro d'ajout du dispositif

Type : type de dispositif

Nom : nom qui peut être attribué au dispositif au sein du système

Attribut : établit les modalités de fonctionnement du dispositif

Conditions : état de service du dispositif (il est par exemple indiqué s'il est Hors-service)

Batterie : état de la batterie (il est indiqué si la charge de la batterie est basse)

Tamper : état d'effraction (tamper) du dispositif

Désactiver : affiche l'état de désactivation permanente ou temporaire du dispositif

RSSI : niveau du signal radio, mesuré de 1 à 9 ; avec un niveau inférieur à 3, la communication est encore assurée mais il est recommandé de rechercher une position garantissant une meilleure portée

État : information sur l'état du dispositif

7.2 WALK TEST

Le Walk Test doit être utilisé pour s'assurer de la présence des dispositifs, pour contrôler leur portée radio et pour s'assurer du bon déclenchement des alarmes.

<NOTE>

Pour les tests de couverture des détecteurs, faire référence aux manuels des instructions correspondants.

Phase 1. Appuyer sur le bouton « **Début Walk Test** » au bas de la page des dispositifs (il est prévu que le test soit automatiquement quitté au bout de 20 minutes).

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)
[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Centrale en mode Test

Test

Appuyer sur "Arrêt" au terme d'un apprentissage ou d'un Test

#	Dispositif	Type	RSSI
Élément non trouvé			

Phase 2. Appuyer sur le bouton d'apprentissage du dispositif pour transmettre un code de test (pour plus de détails, consulter le manuel du dispositif) ou générer une alarme

Phase 3. Si la centrale reçoit le code de test, elle émet 1 bip prolongé ; cliquer sur le bouton « **Mettre à jour** » pour visualiser les informations sur la page et contrôler le niveau de portée du dispositif (colonne RSSI).

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)
[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Test

Appuyer sur "Arrêt" au terme d'un apprentissage ou d'un Test

#	Dispositif	Type	RSSI
1	Dispositif 4	Contact magnétique	9

Phase 4. Pour arrêter le Walk Test et rétablir le fonctionnement normal de la centrale, cliquer sur le bouton « Fin ».

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)
[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Centrale en mode Standard

Test

NOTE : la valeur du signal radio (RSSI) de la caméra IP 1051/004 est sans importance puisque la connexion à la caméra est de type IP.

7.3 MODIFIER D'UN DISPOSITIF

Après avoir acquis un dispositif dans le système, sur la page « Dispositifs », il est possible de procéder à la modification de ses réglages.

Phase 1. Cliquer sur la **Modifier** à hauteur du dispositif à programmer.

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)
[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Configuration dispositifs

Adresse	Type	Nom	Attribut	Conditions	Batterie	Autoprotection	Exclure	RSSI	État
<input type="checkbox"/> 1	Contact magnétique	2I 17/19	Instantanée A						Modifier
<input type="checkbox"/> 2	Télécommande		A PANIQ SILENC						Modifier
<input type="checkbox"/> 3	Clavier		A PANIQUE						Modifier

Phase 2. La page ci-dessous s'affiche pour modifier les réglages du dispositif. Cliquer sur le bouton **Sauvegarder** après avoir saisi les réglages ou les informations voulues.

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#)

[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Modifier le dispositif

Type: Contact magnétique
 ID: RF:00557f10
 ID2:
 Nom:
 Tag:
 Dispositif: 4 ▾
 Attribut: Commun Retardé 1 ▾
 Attribut: EXCL. PERMAN.
 Attribut: HABIL. RAPPORT
 Attribut: Normalement ouvert
 Carillon : Habilité

SIGNIFICATION DES CHAMPS

Nom : saisir un nom pour le dispositif. 27 caractères maximum sont admis.

Tag : non disponible. Pour utilisations futures.

Dispositif : en principe, il n'est pas nécessaire de modifier le numéro du dispositif ; le modifier uniquement pour des besoins particuliers.

Attribut : le réglage de l'attribut détermine les modalités de déclenchement d'une alarme dans les différents états du système. Sur la page suivante, les différents attributs qui peuvent être associés à un dispositif sont présentés. Le tableau qui suit décrit l'utilisation et les comportements du système pour chaque attribut.

Désactivation permanente (exclusion) : cette option désactive (exclut) le dispositif sélectionné tant que la fonction n'est pas désélectionnée. Les signaux de batterie déchargée et d'effraction envoyés par le dispositif sont néanmoins envoyés. Pour éliminer complètement les notifications, il est nécessaire d'éliminer le dispositif.

ATTENTION ! La désactivation permanente ne désactive pas les sirènes dont seul l'envoi des rapports de notifications d'anomalies relatives aux sirènes est exclu.

Pour la fonction de « Désactivation temporaire » du dispositif, consulter le paragraphe 7.5. **Fonction « Désactiver » dispositif.**

Activation rapport : cette fonction est utilisée uniquement pour les télécommandes et pour les contacts de porte utilisés pour activer le système. Si la fonction est sélectionnée, la centrale envoie un rapport quand le système est activé/désactivé avec les télécommandes ou avec le contact de porte.

Normalement ouvert : cette fonction est utilisée uniquement pour les contacts de porte utilisés pour activer le système. Si l'option est sélectionnée, le contact de porte est au repos quand il est ouvert. Quand le contact de porte se ferme, le système est totalement activé.

Si la fonction **Normalement ouvert** n'est pas sélectionnée, le contact de porte est au repos quand il est fermé. Quand le contact de porte s'ouvre, le système est totalement activé.

Sonnette : quand la fonction est active, la centrale émet un son de Sonnette (« ding-dong ») pour informer l'utilisateur de la détection d'un mouvement ou de l'ouverture d'un contact en état de désactivation. Si la fonction est désactivée, aucun son n'est émis. Pour plus d'informations, consulter le paragraphe 8.3 **Paramètres système.**

Alarmes volets roulants : pour éviter le déclenchement d'alarmes multiples, une fois une alarme volet roulant déclenchée, l'alarme suivante ne peut être déclenchée que 30 secondes plus tard.

7.3.1 Liste des attributs des détecteurs

The image shows a configuration window for a detector. A dropdown menu is open, displaying the following list of options:

- Commun Instantané (selected)
- Commun Parcours
- Total Instantané
- Total / Parcours
- Intérieur retardé
- Commun Retardé 1
- Commun retardé 2
- Partiel retardé
- Commun instantané silencieux
- Commun externe silencieux
- 24h/24h
- Incendie
- Médecin/Urgence
- Inondation
- Clé marche-arrêt
- Panique silencieuse
- Panique avec sirène
- Temporisée A
- Temporisée B
- Temporisée C

Below the dropdown menu, the following attributes are visible:

- Attribut: EXCL.PERMAN.
- Attribut: HABIL. RAPPORT
- Attribut: Normalement ouvert
- Carillon : Habilité

A **Sauvegarder** button is located at the bottom of the configuration area.

7.3.2 Liste des attributs des détecteurs

Le tableau qui suit décrit l'utilisation et les comportements du système en cas d'alarme pour chaque attribut attribué aux détecteurs.

SI L'ATTRIBUT DÉTECTEUR EST :	L'ALARME SE DÉCLENCHE :
COMMUN INSTANTANÉ	<ul style="list-style-type: none"> si le système est en activation totale OU partielle A/B/C <p><i>UTILISATION TYPE : protection d'un accès qui doit transmettre une notification d'alarme immédiate, y compris pendant les temps d'entrée et de sortie. Par exemple pour la protection d'une fenêtre à l'arrière d'une maison avec jardin.</i></p>
COMMUN PARCOURS	<ul style="list-style-type: none"> si le système est en activation totale ou partielle A/B/C mais non pas pendant les temps d'entrée et de sortie <p><i>UTILISATION TYPE : protection de la zone où un clavier de commande est installé (généralement près de la porte d'accès).</i></p>
COMMUN RETARDÉ	<ul style="list-style-type: none"> si le système est activé totalement mais au terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) si le système est activé partiellement A/B/C mais terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) <p><i>UTILISATION TYPE : sur une installation avec partialisations et zones communes, pour la protection d'une zone commune y compris quand une seule partialisation a été activée (par exemple : l'accès au garage ou à une entrée principale).</i></p>
TOTAL INSTANTANÉ SILENCIEUX	<ul style="list-style-type: none"> si le système est en activation totale OU partielle A/B/C pendant les temps de sortie pendant les temps d'entrée <p><i>UTILISATION TYPE : identique à « Commun instantané » mais utilisé quand on entend éviter les alarmes sonores et lumineuses des sirènes. Des notifications et des appels vocaux sont envoyés.</i></p>
24H	<ul style="list-style-type: none"> si système est désactivé si le système est en activation totale OU partielle A/B/C pendant les temps d'entrée et de sortie <p><i>UTILISATION TYPE : pour la protection d'un objet de valeur (tableau par exemple)</i></p>
ACTIVER/DÉSACTIVER	Voir détails en fin de tableau.
INSTANTANÉ A	<ul style="list-style-type: none"> si le système est en activation totale ou partielle A, AB, AC <p><i>UTILISATION TYPE : alarmes instantanées associées à la partialisation A</i></p>
INSTANTANÉ B	<ul style="list-style-type: none"> si le système est en activation totale ou partielle B, AB, BC <p><i>UTILISATION TYPE : alarmes instantanées associées à la partialisation B</i></p>
INSTANTANÉ C	<ul style="list-style-type: none"> si le système est en activation totale ou partielle C, AC, BC <p><i>UTILISATION TYPE : alarmes instantanées associées à la partialisation C</i></p>
RETARDÉ A	<ul style="list-style-type: none"> si le système est activé totalement mais au terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) si le système est activé partiellement A, AB, AC mais terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) <p><i>UTILISATION TYPE : maison à 3 accès distincts, chacun desquels étant associé à une partialisation.</i></p>
RETARDÉ B	<ul style="list-style-type: none"> si le système est activé totalement mais au terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) si le système est activé B, AB, BC mais terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) <p><i>UTILISATION TYPE : maison à 3 accès distincts, chacun desquels étant associé à une partialisation.</i></p>
RETARDÉ C	<ul style="list-style-type: none"> si le système est activé totalement mais au terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) si le système est activé partiellement C, AC, BC mais terme du temps réglé sur « Temps ENTRÉE 1 » + 30 sec. (si l'extension du temps entrée = ON) <p><i>UTILISATION TYPE : maison à 3 accès distincts, chacun desquels étant associé à une partialisation.</i></p>

Activer/Désactiver : attribut à associer uniquement aux contacts magnétiques 1051/203, pour lesquels il est possible de configurer la fonction suivante. Ne pas l'associer aux autres modèles de contacts.

Activation/désactivation du système via entrée filaire : il est possible d'activer/désactiver le système via une connexion filaire (par exemple une clé mécanique à haute sécurité) en mesure de fournir un contact libre NF ou NO à brancher aux entrées filaires du 1051/203.

- Ouverture du contact filaire : le système s'active totalement.
- Fermeture du contact filaire : le système se désactive totalement.

<NOTE>

- ☞ Pour utiliser cette fonction, il est recommandé de désactiver la détection d'ouverture du Contact magnétique 1051/203 (voir le manuel du produit pour les détails).
- ☞ L'activation totale du système intervient directement, sans tenir compte des éventuelles anomalies présentes sur le système et sans utiliser le temps de sortie.
- ☞ Cette fonction ne doit pas être utilisée sur les Contacts magnétiques 1051/201 et 1051/202.

Activer/Désactiver : attribut associable aux seuls contacts magnétiques pour lesquels il est possible de configurer la modalité « Normalement ouvert » ou « Normalement fermé » (décrite en détails au paragraphe 7.3 Modification d'un dispositif).

UTILISATION TYPE : activation/désactivation du système à l'aide d'une clé mécanique.

ATTENTION ! L'activation totale du système au moyen de cet attribut associé à un contact magnétique intervient directement sans tenir compte des éventuelles anomalies présentes sur le système et sans activer le temps de sortie.

7.3.3 Liste des attributs de la télécommande 1051/035

Modifier le dispositif		Modifier le dispositif	
Type:	Télécommande	Type:	Télécommande
ID:	RF:03ba0400	ID:	RF:03ba0400
ID2:		ID2:	
Nom:	<input type="text"/>	Nom:	<input type="text"/>
Tag:	<input type="text"/>	Tag:	<input type="text"/>
Dispositif:	2 ▾	Dispositif:	2 ▾
Attribut:	<input type="checkbox"/> EXCL. PERMAN.	Attribut:	<input type="checkbox"/> EXCL. PERMAN.
Attribut:	<input checked="" type="checkbox"/> HABIL. RAPPORT	Attribut:	<input checked="" type="checkbox"/> HABIL. RAPPORT
Attribut:	Partiel A ▾	Attribut:	Partiel A ▾
Attribut:	Partiel A Partiel B Partiel C Partiel A+B Partiel A+C Partiel B+C	Attribut:	Panique silencieuse ▾
Activation scène:	Partiel A Partiel B Partiel C Partiel A+B Partiel A+C Partiel B+C	Activation scène:	Panique silencieuse Panique avec sirène Enclenchement scène

La télécommande peut prendre les attributs suivants :

ATTRIBUT DE PARTIALISATION DE ZONES

Partiel A ou B ou C ou A+B ou A+C ou B+C : associe la touche  de la télécommande à l'activation des partialisations A ou B ou C ou des zones doubles AB ou AC ou BC.

ATTRIBUT DE DÉCLENCHEMENT D'ALARME PANIQUE OU COMMANDE SCÉNARIOS

Panique silencieuse / Panique avec sirènes : active la touche  de la télécommande pour la fonction de Panique silencieuse, pour déclencher une alarme sans activer les sirènes en cas d'activation sous la menace ou pour la fonction Panique avec sirènes, pour faire retentir les sirènes en cas d'agression ou de demande de secours.

La fonction d'activation scénario n'est pour l'instant pas disponible.

La télécommande est également un dispositif à communication bidirectionnelle : quand sa commande est reconnue par la centrale, la reconnaissance est confirmée par le clignotement rapide du voyant (clignotement vert). En cas d'échec de

la reconnaissance, le voyant clignote lentement trois fois (clignotement rouge). Dans ce dernier cas, en contrôler la programmation et la portée.

Si l'on souhaite activer l'antivol avec la télécommande, y compris en présence d'anomalies sur le système, il est nécessaire d'appuyer deux fois sur la touche dédiée. Le début du décompte effectué par la centrale, si prévu, confirme l'activation du système. Faire attention au signal sonore du décompte pour être certain d'avoir activé le système et, éventuellement, régler le volume sur la page « Paramètres système » / « Réglage son ».

7.3.4 Liste des attributs du clavier 1051/025

The image shows two screenshots of the 'Modifier le dispositif' (Modify device) interface for a keypad. Both screenshots show the following fields: Type: Clavier, ID: RF:00180170, ID2: (empty), Nom: (empty), Tag: (empty), Dispositif: 3 (dropdown), and Attribut: EXCL.PERMAN. The left screenshot shows the 'Attribut' dropdown menu open, listing options: Partiel A, Partiel B, Partiel C, Partiel A+B, Partiel A+C, and Partiel B+C. The right screenshot shows the 'Attribut' dropdown menu open, listing options: Partiel A, Panique avec sirène, Panique silencieuse, and Panique avec sirène (highlighted).

Le clavier, programmé à cet effet, peut prendre attributs suivants :

ATTRIBUT DE PARTIALISATION DE ZONES

Partiel A ou B ou C ou A+B ou A+C ou B+C : associe la touche  du clavier l'activation des partialisations A ou B ou C ou des zones doubles AB ou AC ou BC.

ATTRIBUT DE DÉCLENCHEMENT D'ALARME PANIQUE

Panique silencieuse / Panique avec sirènes : active la pression simultanée sur les **touches 1 et 3** pour la fonction de Panique silencieuse, pour déclencher une alarme sans activer les sirènes en cas d'activation sous la menace ou pour la fonction Panique avec sirènes, pour faire retentir les sirènes en cas d'agression.

7.3.5 Liste des attributs de la caméra 1051/004

Pour la caméra IP, il est possible de configurer les paramètres indiqués sur la figure suivante à l'aide du menu **Modifier** :

 EXCL.PERMAN., Carillon: Habilité, Déclenchement par zone: Tous (dropdown), Déclenchement par zone: Déshabilité (dropdown), Déclenchement par zone: Déshabilité (dropdown), Déclenchement par zone: Déshabilité (dropdown), and a 'Sauvegarder' button."/>

The image shows a screenshot of the 'Modifier le dispositif' (Modify device) interface for an IP camera. The fields are: Type: IP caméra, ID: XF:b0c5ca3007d8, ID2: (empty), Nom: IP Cam Egon, Tag: (empty), Dispositif: 4 (dropdown), Attribut: 24h/24h (dropdown), Attribut: EXCL.PERMAN., Carillon: Habilité, Déclenchement par zone: Tous (dropdown), Déclenchement par zone: Déshabilité (dropdown), Déclenchement par zone: Déshabilité (dropdown), Déclenchement par zone: Déshabilité (dropdown), and a 'Sauvegarder' button.

Nom : saisir un nom pour le dispositif. 27 caractères maximum sont admis.

Tag : non disponible. Pour utilisations futures.

Dispositif : en principe, il n'est pas nécessaire de modifier le numéro du dispositif ; le modifier uniquement pour des besoins particuliers.

Attribut : le réglage de l'attribut détermine dans quels états la caméra peut être visualisée à distance.

Les attributs utilisables sont les suivants :

- **24h/24h** : la caméra peut être visualisée en toute circonstance.
- **COMMUN INSTANTANÉ** : la vision est possible uniquement dans l'état de système entièrement ou partiellement activé A, B ou C.
- **TOTAL INSTANTANÉ** : la vision est possible uniquement dans l'état de système entièrement activé.
- **INSTANTANÉ A/B/C** : la vision est possible uniquement dans l'état de système partiellement activé A/B/C.

Désactivation permanente (exclusion) : cette option désactive (exclut) la transmission des vidéos associés à l'alarme de la caméra sélectionnée tant que la fonction n'est pas désélectionnée. La possibilité de visualiser la caméra en temps réel n'est pas désactivée.

Sonnette : option NON DISPONIBLE.

Trigger dispositif : par l'intermédiaire de ces 4 options, il est possible d'associer l'enregistrement d'une vidéo à une alarme déclenchée par 4 détecteurs différents ou de tout détecteur de l'installation (option Tous). Sélectionner le numéro du détecteur à associer (il figure dans le tableau des dispositifs) ou bien sélectionner Tous. Outre les détecteurs, il est possible d'associer une télécommande : dans ce cas, la vidéo est envoyée en cas d'alarme Panique.

Le menu **Vue** permet d'accéder à la visualisation de la caméra en temps réel. Cette fonction peut être utilisée pour positionner correctement la caméra.

Le menu **Réglages** permet d'accéder à l'interface complète de programmation de la caméra. Faire référence au manuel complet de la caméra IP 1051/004 pour son utilisation.

7.4 ÉLIMINATION D'UN DISPOSITIF

Pour éliminer un dispositif de la centrale, sélectionner, sur la page **Configuration des dispositifs**, la case correspondante et cliquer sur **Éliminer** : le dispositif sélectionné est ensuite éliminé. Avant d'éliminer le dispositif, un pop-up s'affiche pour demander de confirmer l'élimination du dispositif.

ATTENTION ! Par souci de sécurité, la fonction « Éliminer » ne désactive pas les sirènes même si elle les exclut de la liste des dispositifs et des rapports de notification des anomalies.

Pour désactiver les sirènes, il est nécessaire d'en couper l'alimentation ou de procéder à une réinitialisation des réglages par défaut (voir manuel du dispositif).

<NOTE> Si un dispositif reste déconnecté de la centrale, sa consommation est supérieure.

Pour éliminer les dispositifs 1051/104, 1051/106 et 1051/003, il n'est pas nécessaire d'exécuter la commande d'éliminer mais il suffit de rétablir les valeurs par défaut.

7.5 FONCTION « DESACTIVER » DISPOSITIF

Les dispositifs peuvent être simultanément exclus en sélectionnant, sur la page de Gestion des dispositifs, la case correspondante et en cliquant sur « **Désactiver** ». La première intrusion est ignorée par le système pendant la première activation ; toutes les intrusions suivantes déclenchent en revanche l'alarme. Pendant cette période, le dispositif signale néanmoins les situations de batterie déchargée et d'effraction.

Cette fonction peut être utilisée pour éviter les alarmes d'effraction accidentelles lors du changement des batteries d'un dispositif ou quand ce dernier est placé dans une autre position.

ATTENTION ! La désactivation temporaire ne désactive pas les télécommandes, le clavier, les sirènes ni la caméra IP. Pour les claviers et les sirènes, la désactivation temporaire empêche uniquement l'envoi des rapports de notifications d'anomalies.

7.6 IDENTIFICATION D'UN DISPOSITIF

La fonction d'identification, sur la page de gestion des dispositifs, est disponible pour les seuls dispositifs 1051/104, 1051/106, 1051/003 et elle peut être utilisée pour identifier ces dispositifs à l'issue de l'apprentissage.

La fonction d'identification NE DOIT PAS être utilisée dans la minute qui suit la pression sur le bouton du dispositif ni dans les 3 minutes qui suivent l'apprentissage du dispositif. Différemment, le dispositif pourrait ne pas recevoir correctement les signaux provenant de la centrale.

Phase 1. Sélectionner la case correspondant au numéro du dispositif et cliquer sur « Identifier » sous la liste.

Phase 2. Si le dispositif reçoit correctement le signal, le voyant correspondant clignote 10 fois comme signe de confirmation.

Si le voyant du dispositif ne clignote pas, cela indique que le dispositif ne reçoit pas le signal de la centrale.

7.7 DEMANDE D'INFORMATIONS PHOTOS/VIDEOS

Dans la section Surveillance de gestion dispositifs, sélectionner la case correspondant au numéro du dispositif et cliquer sur « **Demande image** » pour contrôler manuellement le détecteur doté de caméra et acquérir une image. Le détecteur doté de caméra acquiert 1 image qui peut être visionnée sur le panneau de contrôle « **Capture événements** ». En cliquant sur « **Demande image sans flash** », une photo sans allumage du flash est demandée.

Dans le cas où la caméra IP serait sélectionnée, les vidéos enregistrées sont visibles sur le portail, sur l'appli et sur l'interface locale de programmation de la caméra quelques instants plus tard. Mais elles ne sont pas visibles sur la page « **Capture événements** ».

7.8 PROGRAMMATION DE LA SIRENE

Cette section traite de la programmation de la sirène externe.

Home. Ne pas utiliser. Pour utilisations futures.

Tamper Sirène : cette option sert à activer/désactiver la protection anti-effraction de la sirène. Sélectionner ON/OFF et cliquer sur la touche « **Tamper Sirène** » pour confirmer le choix.

Son confirmation : cette option permet de décider de faire émettre un bip par la sirène quand le système est activé ou désactivé. Sélectionner ON/OFF et cliquer sur la touche « **Son confirmation** » pour confirmer le réglage.

Son entrée : cette option permet de décider de faire émettre un bip par la sirène pendant le décompte du temps d'entrée. Sélectionner ON/OFF et cliquer sur la touche « **Son entrée** » pour Entrée le réglage.

Test : cette option permet d'effectuer un test de la sirène intégrée à la centrale et de toutes les sirènes externes acquises. Sélectionner « ON » et cliquer sur la touche « **Test** ». Toutes les sirènes du système d'alarme sont et restent activées tant qu'elles ne sont pas éteintes en sélectionnant « OFF » et en cliquant à nouveau sur « Test ».

<NOTE>

Les modifications du réglage de la sirène sont effectuées simultanément sur toutes celles présentes sur le système mais NON PAS sur celle présente sur la centrale.

- ☞ Pour éviter une alarme indésirable d'effraction lors du changement des batteries de la sirène ou d'installation dans une autre position, il est tout d'abord nécessaire de désactiver le Tamper de la sirène, en sélectionnant « Tamper Sirène OFF » sur la page de modification.
- ☞ En cas d'oubli de la réactivation du Tamper, au bout de une heure la sirène est à nouveau active.

8 REGLAGES DU SYSTEME

Ce chapitre traite des pages de configuration de base du système. En particulier :

1. page INFO → état du système et présence d'anomalies
2. page RÉGLAGES → données de fonctionnement de la centrale
3. page PARAMÈTRES → comportements de la centrale à travers alarmes, retards, avis, etc.
4. page UTILISATEUR → liste des utilisateurs autorisés
5. page RÉSEAU → réglage réseau LAN
6. page GSM → réglage réseau 4G/3G/GPRS
7. page RAPPORTS → modalités d'envoi des rapports
8. page CHARGEMENT → réglages pour l'envoi d'images et de vidéos

Il est recommandé de procéder à la configuration du système en respectant la séquence des images du présent chapitre.

8.1 INFO

Cette page permet de visualiser l'état du système et les éventuelles anomalies présentes.

Bienvenue **Contrôles** Centrale Dispositifs Paramètres Utilisateur Historique Capture événements Rapport événements GSM Réseau Rapport Uploader Firmware

Firmware/RF Déconnexion

Informations et défauts système

État système :OFF

Defaut		
<input type="checkbox"/> SIM absente		
<input type="checkbox"/> Pas de signal GSM		

Effacer

État système : état d'activation du système.

Anomalie. Dans cette section, figurent les anomalies éventuellement présentes sur le système.

Touche Effacer. Dès l'instant où le système demande une double confirmation en présence d'anomalies pour l'activation du système, cette page permet de décider d'ignorer ou non celles sélectionnées et d'activer le système directement sans que la double confirmation ne soit nécessaire (code saisi à nouveau ou commande d'activation forcée sur les claviers ou touche d'activation nouvellement enfoncée sur la télécommande).

8.2 REGLAGES

Cette page permet de configurer certains réglages généraux du système.

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)

[Firmware](#) [Firmware/RF](#) [Déconnexion](#)

Paramètres système

Mot clé utilisateur :

Mot clé installateur :

Durée de coupure du secteur :

Détection perturbation :

Test périodique : Intervalle : Décalage:

Ecoute télésurveilleur :

Durée écoute:

Mains Libres :

Rappel :

Num. préféré Mains Libres:

Autoprotection externe:

Alerte température haute:

Alerte température basse:

Résolution image alarme caméra IR:

Ign. défaut IP/GSM:

Activation rapide:

Activation rapide:

Message vocal:

Fuseau horaire :

Date & Heure : / / :

Maintenir les configurations réseau Maintenir les configurations dispositif

[Sauvegarde & Rétablissement](#)

Mot de passe utilisateur : non utilisé.

Mot de passe installateur : non utilisé.

Temps absence alimentation secteur : dans ce champ, indiquer le temps d'attente pour la centrale avant de générer une notification suite à la détection de l'absence d'alimentation électrique. Le réglage par défaut est de **8 minutes**.

Activation Jamming : dans ce champ, indiquer si la centrale doit relever les interférences de radiofréquence et générer une notification le cas échéant. Le réglage par défaut est **ON**. Si la centrale relève une interférence radio en mesure d'aveugler les communications avec les dispositifs pendant plus de 30 secondes, elle signale l'événement à travers les rapports prévus à cet effet. L'alarme s'affiche si l'interférence dure plus de 30 secondes.

Test périodique : cette fonction permet de configurer les tests périodiques de la centrale, tests internes et tests de rapport. La Période d'Offset permet d'établir au bout de combien de temps le premier rapport est envoyé à compter de l'allumage de la centrale. Il est recommandé de ne pas modifier les paramètres par défaut (intervalle 24 h - période offset 1 h).

Contrôle Environnement : menu à utiliser en cas de connexion numérique à une centrale de surveillance. Non prévu pour le fonctionnement normal. Contacter l'Assistance technique Urmet pour plus d'informations sur son utilisation.

Durée contrôle environnement : ce menu établit le temps d'ouverture du canal phonique bidirectionnel de la centrale à l'utilisateur en cas d'appel Mains libres ou en cas d'ouverture d'un canal phonique pendant un appel suite à une alarme.

Mains libres : ce menu permet d'activer la fonction Mains libres grâce à laquelle, en cas d'appel Mains libres ou suite à une alarme, l'utilisateur peut ouvrir un canal phonique (pour le temps voir le paramètre réglé dans Durée Contrôle) avec la centrale pour écouter l'espace ambiant et communiquer avec d'éventuelles personnes à proximité de la centrale.

Timer rappel : non utilisé.

Numéro mains libres : numéro à appeler, avec l'indicatif 0039 de l'Italie en appel mains libres.

Tamper externe : ce menu permet d'activer/désactiver un dispositif anti-effraction (Tamper) connecté sur le bornier de la centrale.

Image alarme appareil-photo IR : cette fonction permet de modifier le réglage de capture des images d'alarme des détecteurs dotés d'appareil-photo. Les options disponibles sont les suivantes :

- ☞ **640 x 480 x 3** : le détecteur doté d'appareil-photo capture 3 images à une résolution de 640 x 480 quand il détecte une intrusion.
- ☞ **320 x 240 x 6** : le détecteur doté d'appareil-photo capture 6 images à une résolution de 320 x 240 quand il détecte une intrusion.
- ☞ **320 x 240 x 3** : le détecteur doté d'appareil-photo capture 3 images à une résolution de 320 x 240 quand il détecte une intrusion (**réglage par défaut**).

Ignorer panne IP/GSM : permet d'ignorer ou non les événements d'erreur relatifs à la fonction Ethernet ou GSM. Les événements d'erreur ignorés sont visualisés sur le panneau de contrôle local.

- ☞ **Désactivé** : en sélectionnant Désactivé, aucun événement n'est ignoré.
- ☞ **IP** : en sélectionnant IP, les événements relatifs à la fonction Ethernet sont ignorés.
- ☞ **GSM** : en sélectionnant GSM, les événements relatifs à la transmission de données GPRS sont ignorés.
- ☞ **IP+GSM** : en sélectionnant IP+GSM, tous les événements relatifs à la connexion Internet sont ignorés.

Le réglage par défaut est **Désactivé**.

Après avoir effectué les réglages précédents, appuyer sur le bouton « **Sauvegarder** » pour confirmer les modifications.

Fuseau horaire : permet de régler le fuseau horaire local.

Date et Heure : permet de régler la date et l'heure courantes.

Après avoir réglé fuseau horaire et date/heure, appuyer sur le bouton « **Réglage heure** » pour confirmer les modifications.

Redémarrer Centrale : appuyer sur ce bouton pour redémarrer la centrale sans modifier aucun paramètre.

Réinitialisation : appuyer sur cette touche pour effacer toutes les informations et les réglages mémorisés dans la centrale et rétablir les valeurs par défaut.

Il est néanmoins possible de :

- ne pas modifier les paramètres de réseau en sélectionnant l'option « Maintenir réglages de réseau »
- ne pas perdre la configuration des dispositifs déjà acquis en sélectionnant l'option « Maintenir réglages dispositif »

Pour effectuer la réinitialisation, procéder comme suit :

- couper l'alimentation sur secteur et placer l'interrupteur de la batterie en **OFF**.
- rétablir l'alimentation sur secteur et dès que deux signaux sonores d'avertissement sont émis, appuyer sur la touche ▲. L'écran affiche une indication alphanumérique et la version du firmware ;
- appuyer successivement sur les touches suivantes : ▼▲▼▲▼▲▼ OK. L'écran affiche : *FACTORY RESET*
- appuyer à nouveau sur la touche OK ;

il est ensuite possible de relâcher le bouton et de replacer l'interrupteur de la batterie sur **ON**.

ATTENTION ! Après avoir effectué la réinitialisation (depuis le panneau de contrôle ou le clavier menu LCD), la centrale n'est plus en mesure de gérer le chargement ni les rapports puis l'adresse du serveur est elle aussi effacée. Il est indispensable de la rétablir pour réactiver cette fonction. A cet effet, utiliser la procédure d'Envoi configuration du portail (voir le guide correspondant disponible sur le site ; pour accéder utiliser le lien fourni en fin de manuel).

Backup and Restore

Actuellement cette fonction n'est pas active.

8.3 PARAMETRES SYSTEME

Cette page permet de régler certains paramètres de la centrale.

The screenshot shows the 'Paramètres de centrale' page with the following settings:

- Dernière sortie : OFF
- Activation forcée : Désactiver
- Alarme Autoprotection : Si activation totale
- Extension Temporisation Rapport : ON
- Temporisation entrée 1 : Activation Totale: 10 Sec, Activation Partielle: 10 Sec
- Temporisation entrée 2 : Activation Totale: 10 Sec, Activation Partielle: 10 Sec
- Temporisation sortie : Activation Totale: 10 Sec, Activation Partielle: 10 Sec
- Temps d'alarme : 3 Min
- Test Supervision : Désactivé
- Configuration sons : Carillon: Faible, Entrée totale: Faible, Entrée partielle: Faible, Sortie totale: Faible, Sortie partielle: Faible, Avertissement défauts: Faible, Sirène interne: OFF

Dernière sortie :

- ☞ **Dernière sortie On** : si le système est en état d'activation totale et qu'un contact magnétique a été réglé avec l'attribut **Commun retardé 1 / parcours totale**, le système s'active automatiquement une fois le contact magnétique fermé, même si le temps de retard pour la sortie n'est pas encore écoulé. Pour la liste complète des attributs des dispositifs, voir le tableau du paragraphe 5.3.
- ☞ **Dernière sortie Off** : la fonction ci-dessus n'est pas active.
- ☞ Le réglage par défaut est **Dernière sortie Off**.

Activer avec anomalies :

- ☞ **Confirmer** : avec ce réglage, si l'on tente de procéder à l'activation en présence d'une anomalie, une double confirmation est demandée pour l'activation du système (code saisi deux fois ou commande d'activation forcée sur les claviers ou touche d'activation nouvellement enfoncée sur la télécommande) ; réglage par défaut.
- ☞ **Activation directe** : avec ce réglage, l'activation du système en présence d'une anomalie intervient directement sans que la double confirmation ne soit nécessaire.
- ☞ Le réglage par défaut est **Confirmer**.

Alarme Tamper :

- ☞ **Total**. Les alarmes anti-effraction (Alarmes Tamper) sont générées uniquement en activation totale (l'événement d'effraction est dans tous les cas signalé également en activation partielle ou en désactivation).
- ☞ **Toujours**. L'alarme anti-effraction est générée dans tout état du système.
- ☞ Le réglage par défaut est **Total**.

Extension temps entrée :

- ☞ **Off**. Avec ce réglage, si le décompte du retard entrée 1 et 2 est lancé et que la centrale n'est pas désactivée avant le terme du décompte, la centrale signale une alarme anti-intrusion aussitôt après la fin du décompte.
 - ☞ **On**. Avec ce réglage, si le décompte du retard entrée 1 et 2 est lancé et que la centrale n'est pas désactivée avant le terme du décompte, la centrale attend encore 30 secondes après la fin du décompte avant de signaler une alarme anti-intrusion.
- Le réglage par défaut est **On**.

<NOTE>

Pendant les 30 secondes du temps d'extension le bip est exclu.

Retard entrée 1 : établit le temps dont dispose l'utilisateur pour désactiver le système quand des alarmes sont générées par les détecteurs qui prévoient les retards d'entrée 1. Programmable pour chaque état d'activation totale ou partielle (pour plus d'information, consulter le paragraphe **7.3 Modification des réglages du dispositif**).

Le réglage par défaut est de **20 secondes**.

Retard entrée 2 : établit le temps dont dispose l'utilisateur pour désactiver le système quand des alarmes sont générées par les détecteurs qui prévoient les retards d'entrée 2. Programmable pour chaque état d'activation totale ou partielle (pour plus d'information, consulter le paragraphe **7.3 Modification des réglages du dispositif**).

Le réglage par défaut est de **20 secondes**.

Retard sortie : établit le temps nécessaire à l'activation du système pour chaque état d'activation totale et partielle.

Le réglage par défaut est de **30 secondes**.

Temps activation alarme : quand une alarme se déclenche, la sirène de la centrale et la sirène externe émettent une alarme en fonction du réglage de la durée de l'alarme définie dans ce champ.

Le réglage par défaut est de **3 minutes**.

<NOTE>

Vérifier dans le même temps la configuration de Durée Alarme de la sirène externe. Si des durées différentes ont été programmées sur le panneau de contrôle local et sur la sirène, la durée la plus courte prévaut.

Test supervision : permet de régler le timer de supervision pour les dispositifs accessoires. Si aucun signal de supervision n'est reçu avant l'écoulement de la durée programmée pour un dispositif donné, la centrale déclenche une alarme de supervision qui est ensuite notifiée à l'utilisateur.

Le réglage par défaut est désactivé.

ATTENTION. Pour utiliser la modalité de Supervision et l'alarme correspondante en cas de non-réception du signal d'un dispositif par la centrale, le dispositif doit être appris alors que le Test Supervision est activé.

Réglage son :

- ☞ **Sonnette** : si ce son est activé, la centrale émet le son d'une sonnette, quand une alarme se déclenche sur un détecteur à fonction Sonnette, alors que le système en état de désactivation (pour plus d'information, consulter le paragraphe **7.3 Modification des réglages du dispositif**).
- ☞ **Entrée totale** : si ce son est activé, la centrale en état d'activation totale émet des bips pendant le temps d'entrée
- ☞ **Entrée partielle** : si ce son est activé, la centrale en état d'activation partielle émet des bips pendant le temps d'entrée.
- ☞ **Sortie totale** : si ce son est activé, la centrale émet des bips pendant le temps de sortie pour l'activation totale.
- ☞ **Sortie partielle** : si ce son est activé, la centrale émet des bips pendant le temps de sortie pour l'activation partielle.
- ☞ **Son alerte** : si ce son est activé, la centrale émet des bips toutes les 30 secondes si une anomalie est présente sur le système.
- ☞ **Sirène interne** : activée, la sirène intégrée à la centrale est activée et émet un son d'alarme quand une alarme se déclenche.

8.4 VISUALISATION UTILISATEURS

Cette page affiche le nom des utilisateurs autorisés à utiliser le système (enregistrés à travers l'application ou à travers le portail). Cette page permet uniquement de visualiser les utilisateurs mais pas d'en enregistrer de nouveaux. La centrale **Zeno** permet de créer ou de modifier les codes des utilisateurs uniquement à l'aide du Menu utilisateur visualisable sur l'écran.

[Bienvenue](#) [Contrôles](#) [Centrale](#) [Dispositifs](#) [Paramètres](#) [Utilisateur](#) [Historique](#) [Capture événements](#) [Rapport événements](#) [GSM](#) [Réseau](#) [Rapport](#) [Uploader](#)
[Firmware](#) [Déconnexion](#)

Affichage utilisateurs

Adresse	Code	Nom	Archivé
1		<input type="text" value="user"/>	<input checked="" type="checkbox"/>
2		<input type="text" value="Luca"/>	<input checked="" type="checkbox"/>
3		<input type="text" value="io"/>	<input checked="" type="checkbox"/>
4		<input type="text" value="tu"/>	<input checked="" type="checkbox"/>
5		<input type="text" value="lei"/>	<input checked="" type="checkbox"/>
6		<input type="text"/>	<input type="checkbox"/>
7		<input type="text"/>	<input type="checkbox"/>
8		<input type="text"/>	<input type="checkbox"/>
9		<input type="text"/>	<input type="checkbox"/>
10		<input type="text"/>	<input type="checkbox"/>
11		<input type="text"/>	<input type="checkbox"/>
12		<input type="text"/>	<input type="checkbox"/>
13		<input type="text"/>	<input type="checkbox"/>
14		<input type="text"/>	<input type="checkbox"/>
15		<input type="text"/>	<input type="checkbox"/>
16		<input type="text"/>	<input type="checkbox"/>
17		<input type="text"/>	<input type="checkbox"/>
18		<input type="text"/>	<input type="checkbox"/>
19		<input type="text"/>	<input type="checkbox"/>
20		<input type="text"/>	<input type="checkbox"/>

Pour des raisons de sécurité, les codes personnels des utilisateurs ne sont pas visualisés. Le code par défaut pour l'utilisateur 1 est **1234**.

Le champ « **Mémorisé** » est utilisé pour établir si les opérations d'activation et de désactivation de l'utilisateur doivent ou non figurer dans la liste des événements. Le signe de coche active l'enregistrement des événements.

8.5 REGLAGES DE RESEAU

Cette page permet de configurer les réglages du réseau.

The screenshot shows a web interface with a navigation bar at the top containing tabs: Bienvenue, Contrôles, Centrale, Dispositifs, Paramètres, Utilisateur, Historique, Capture événements, Rapport événements, GSM, Réseau (highlighted in red), Rapport, and Uploader. Below the navigation bar are links for Firmware and Déconnexion.

Configuration réseau

DHCP : ON (dropdown)
Adresse IP : 192.168.0.111
Masque sous-réseau : 255.255.255.0
Passerelle : 192.168.2.1
DNS : 8.8.8.8

SNTP : pool.ntp.org (text input) Intervalle: 8 Heures (dropdown)

RESERVE : (empty text input) De: (empty text input)
Sauvegarder (button)

Utilisateur Web : admin (text input)
Nouveau mot de passe : (empty text input)
Répéter mot de passe : (empty text input)
Modifier mot de passe (button)

XMPP : xmpp://testv2.elkron.com:5222 (text input)
Domaine : elkron-home-portal (text input)
Administration : security_admin (text input)

État: Connecté
Reconnexion (button)

DHCP :

- ☞ **On.** Si DHCP est réglé sur On, la centrale obtient automatiquement du serveur DHCP de réseau l'adresse IP. Aussi, aucun réglage n'est nécessaire.
- ☞ **Off.** Si DHCP est réglé sur Off, il est nécessaire de saisir manuellement les informations pour l'adresse IP, le masque de sous-réseau, la passerelle et le DNS. Veiller à s'assurer de disposer de toutes les données nécessaires à l'environnement de réseau. Pour plus d'informations, s'adresser à l'administrateur du réseau local.

SNTP : le réglage SNTP permet d'indiquer les paramètres de synchronisation et de mise à jour automatique de l'horloge de la centrale. Il est recommandé de ne pas modifier ces paramètres.

Après avoir effectué les réglages précédents, appuyer sur le bouton « **Sauvegarder** » pour mettre à jour les réglages.

Réglage du compte de l'administrateur

Dans cette section, il est possible d'indiquer le nom utilisateur et le mot de passe pour accéder au panneau de contrôle de la centrale.

- ☞ **Utilisateur Web :** nom utilisateur à utiliser pour accéder au panneau de contrôle local. Le nom prédéfini est « **admin** ». Pour modifier le nom utilisateur, saisir un nouveau nom dans le champ. Le nombre maximal de caractères est de 20.
- ☞ **Nouveau mot de passe :** pour modifier le mot de passe, en saisir un nouveau dans ce champ. Le nombre maximal de caractères est de 20.
- ☞ **Répéter mot de passe :** saisir à nouveau le mot de passe dans ce champ.

<NOTE>

Il est recommandé de modifier le mot de passe pas défaut en fin d'installation.

XMPP, Domaine et Administration : ces réglages établissent les modalités de connexion au serveur de système pour le contrôle à distance.

ATTENTION ! Ces paramètres ne doivent en aucun cas être modifiés !

En cas d'intervention d'entretien ou en cas de modification accidentelle de ces paramètres, rétablir :

- **XMPP :** xmpp://www.myzeno.urmet.com:5222

État : état de connexion au serveur de système.

<NOTE>

- Dans le cas où s'afficherait « déconnecté », cela indique l'absence de connexion avec le serveur de système. Appuyer sur le bouton « Reconnecter » pour tenter d'établir la connexion.
- En cas de déconnexion IP Ethernet, le système fonctionne en 4G/3G/GPRS (si une carte SIM activée pour la transmission de données est présente). Au rétablissement de la connexion IP Ethernet, par mesure de sécurité, le système attend quelques minutes avant de rétablir la connexion IP Ethernet.

8.6 REGLAGE GSM

Cette page permet de contrôler l'état du GSM et de configurer les réglages du réseau 4G/3G/GPRS.

The screenshot shows a web interface for GSM configuration. At the top, there is a navigation menu with buttons for 'Bienvenue', 'Contrôles', 'Centrale', 'Dispositifs', 'Paramètres', 'Utilisateur', 'Historique', 'Capture événements', 'Rapport événements', 'GSM', 'Réseau', 'Rapport', 'Uploader', and 'Firmware'. Below the menu, there is a 'Déconnexion' button. The main heading is 'Programmation GSM'. The status is 'État: SIM absente' and the IMEI is '861311003973764'. There are input fields for 'GPRS APN' (ibox.tim.it), 'Utilisateur', and 'Mot de passe'. There are also input fields for 'MMS APN' (mms), 'Utilisateur', and 'Mot de passe'. Below these, there are input fields for 'URL', 'Adresse Proxy', and 'Port' (80). There is a 'Sauvegarder' button and a 'RAZ GSM' button.

État : dans ce champ, s'affiche l'état du module 4G/3G/GPRS (présence carte SIM et couverture du champ).

IMEI : dans ce champ, s'affiche le code IMEI du module 4G/3G/GPRS.

GPRS : afin de pouvoir utiliser la connexion 4G/3G/GPRS comme connexion de back-up, il est nécessaire de programmer cette section pour garantir les communications avec les dispositifs à distance.

☞ **Nom APN (point d'accès).** Le nom d'un point d'accès pour le 4G/3G/GPRS. Le nom APN doit être demandé au fournisseur du service de téléphonie. APN des principaux opérateurs :

- **TIM :** ibox.tim.it
- **Vodafone :** mobile.vodafone.it ; web.omnitel.it ; m2m.vodafone.bis
- **Wind :** internet.wind ; internet.wind.biz
- **Fastweb :** apn.fastweb.it

Une fois réglé le nom APN, le système peut se connecter à Internet.

☞ **User (GPRS).** Le nom d'accès à indiquer avant d'accéder aux fonctions GPRS. Cette information, si nécessaire, doit être demandée au fournisseur du service de téléphonie.

☞ **Mot de passe GPRS.** Le mot de passe de l'utilisateur à indiquer avant d'accéder aux fonctions GPRS. Cette information, si nécessaire, doit être demandée au fournisseur du service de téléphonie.

MMS : actuellement, la possibilité d'utiliser les messages MMS n'est pas activée.

Après avoir saisi toutes les informations, cliquer sur le bouton « **Sauvegarder** » pour mettre à jour les réglages.

Réinitialisation GSM. Ce bouton permet de réinitialiser le module 4G/3G/GPRS présent dans la centrale.

<NOTE>

1. Éliminer la demande du code PIN de la carte SIM (utiliser un téléphone portable).
2. Utiliser une carte SIM activée pour données et phonie, en en vérifiant la date d'échéance.
3. Dès l'instant où il s'agit d'une installation de sécurité, pour la carte SIM, il est recommandé de recourir à un type de contrat d'abonnement n'exposant pas au risque d'épuisement du crédit
4. En cas d'utilisation de cartes SIM prépayées, à intervalles, s'assurer que le crédit est suffisant pour garantir le fonctionnement du module GSM.
5. Il est recommandé d'activer une carte SIM prépayée ou sous contrat prévoyant un trafic de données non inférieur à 100 Mo/mois. Les consommations moyennes pour les connexions ADSL et 4G/3G/GPRS sont les suivantes :

- 50 Mo/mois pour une connexion au serveur « Always ON » (24 heures sur 24 tous les jours du mois)
- 25 Ko pour chaque photo à la résolution maximale

URMET décline toute responsabilité en cas d'indisponibilité, temporaire ou permanente, du réseau de téléphonie mobile GSM pouvant compromettre l'envoi des informations programmées.

8.7 RAPPORTS

Cette page permet de régler la destination des rapports. Jusqu'à 8 destinations sont disponibles pour la transmission des informations.

Bienvenue Contrôles Centrale Dispositifs Paramètres Utilisateur Historique Capture événements Rapport événements **GSM** Réseau Rapport Uploader
Firmware Déconnexion

Configuration rapport

Adresse	Configuration	Groupe	Filtres
1	<input type="text" value="ip://127037490356@testv2.elkron.com:8765/CID"/>	1 ▼	Tous les événements ▼
2	<input type="text"/>	2 ▼	Tous les événements ▼
3	<input type="text"/>	3 ▼	Tous les événements ▼
4	<input type="text"/>	4 ▼	Tous les événements ▼
5	<input type="text"/>	5 ▼	Tous les événements ▼
6	<input type="text"/>	6 ▼	Tous les événements ▼
7	<input type="text"/>	7 ▼	Tous les événements ▼
8	<input type="text"/>	8 ▼	Tous les événements ▼

IP (Ethernet ou GPRS) au format CID, ex. : ip://account@server.porta/CID
 IP (Ethernet ou GPRS) au format SIA, ex. : ip://account@server.port/SIA
 IP (Ethernet ou GPRS) au format CID_SIA (DC 09), ex. : ip://account@xxx.xxx.xxx.xxx:port/CID_SIA
 SMS au format texte, ex. : sms://telefono/TEXT
 GSM (CID), ex. : gsm://account@telefono
 CSD, ex. : csd://account@telefono
 Appel vocal, ex. : voix://telephone

Sauvegarder Test

Type de rapport :

La centrale ZENO supporte les types de rapport suivants :

☞ Rapport IP/GPRS au format CID/SIA DC09 :

Format de destination du rapport : ip://account@xxx.xxx.xxx.xxx:port/CID_SIA

Par exemple : ip://account@59.124.123.22:8765/CID_SIA

ip://	6543	59.124.123.23	:8765	/CID_SIA
Type de rapport	Comptes	Adresse IP du serveur	Numéro de port	Format du rapport

☞ Rapport IP/GPRS au format CID :

Format de destination du rapport : ip://Account@Server IP:Port/CID

Par exemple : ip://6543@59.124.123.22:8765/CID

ip://	6543	@59.124.123.23	:8765	/CID
Type de rapport	Compte (4-8 chiffres)	Adresse IP du serveur	Numéro de port	Format du rapport

☞ Rapport IP/GPRS au format SIA :

Format de destination du rapport : ip://Account@Server IP:Port/SIA

Par exemple : ip://6543@59.124.123.22:8765/SIA

ip://	6543	@59.124.123.23	:8765	/SIA
Type de rapport	Compte (4-8 chiffres)	Adresse IP du serveur	Numéro de port	Format du rapport

rapport	chiffres)	serveur	port	rapport
---------	-----------	---------	------	---------

☞ **Rapport SMS au format CID (uniquement si la centrale dispose d'une carte SIM) :**

Format de destination du rapport : sms://Account@numéro de portable/CID

Par exemple : sms://1234@0926064587/CID

sms://	1234	0926064587	/CID
Type de rapport	Compte (4-8 chiffres)	Numéro de portable	Format du rapport

☞ **Rapport SMS au format Texte (uniquement si la centrale dispose d'une carte SIM) :**

Format de destination du rapport : sms://nombre portable/TEXT

Par exemple : sms://00393476064587/TEXT

sms://	00393476064587	/TEXT
Type de rapport	Numéro de portable	Format du rapport

☞ **Rapport numérique GSM au format CID (uniquement si la centrale dispose d'une carte SIM) :**

Format de destination du rapport : gsm:// Account@Numéro tél.

Par exemple : gsm://1234@1234567890

gsm://	1234	@1234567890
Type de rapport	Compte (4-8 chiffres)	Numéro de téléphone

☞ **Rapport numérique GSM au format CSD :**

Format de destination du rapport : csd:// Account@Numéro tél.

Par exemple : csd://1234@1234567890

csd://	1234	@1234567890
Type de rapport	Compte (4-8 chiffres)	Numéro de téléphone

☞ **Rapport appel mains libres :**

Format de destination du rapport : voix://Numéro tél.

Par exemple : voix://00391234567890

voix://	0039	1234567890
Type de rapport	Indicatif international	Numéro de téléphone

<NOTE>

- L'adresse 1 est configurée automatiquement à la première connexion au serveur.

ATTENTION ! Les paramètres de toute la ligne ne doivent en aucun cas être modifiés ! C'est pourquoi la première ligne n'est pas modifiable.

- Le type de rapport doit être indiqué en minuscules.
- L'envoi des mails peut être réglé uniquement sur le portail.
- L'envoi des SMS doit être configuré sur le panneau de contrôle et prévoit 2 cas :

1. Si dans le réglage des rapports, ils sont classés comme Groupe 1, ils ne sont envoyés que si la connexion IP fait défaut.
2. Si dans le réglage des rapports, ils sont classés comme Groupe autre que le Groupe 1, ils sont toujours envoyés. S'il est nécessaire d'envoyer des SMS à des numéros différents, sélectionner des Groupes différents.

Groupe :

Il est possible d'attribuer les destinations des rapports à des groupes différents. Les groupes de rapport fonctionnent sur la base des règles suivantes :

- ☞ La priorité d'envoi des rapports est définie par le numéro attribué au Groupe. Le Groupe 1 a la priorité sur les numéros suivants. De Groupe 1 → Groupe 2 → Groupe 3 →....., etc.
- ☞ Si plusieurs destinations de rapports sont attribuées à un groupe, quand un rapport est envoyé avec succès à une des destinations, le système arrête l'envoi du rapport aux destinations restantes du groupe et passe au rapport du groupe suivant.
- ☞ Si la centrale ne parvient pas à envoyer le rapport à la première destination d'un groupe, elle passe à la destination suivante. Si elle ne parvient à envoyer le rapport à aucune destination du groupe, la centrale effectue 2 autres tentatives avant de passer au groupe suivant.
- ☞ Si elle ne parvient à envoyer le rapport à aucun groupe, la centrale recommence à envoyer le rapport en commençant par le Groupe 1 jusqu'à ce que au moins un groupe reçoive le rapport.
- ☞ Pour les rapports « **VOCAUX** », si l'appel n'aboutit pas, la centrale compose à nouveau chaque numéro de téléphone 3 fois, jusqu'à un maximum de 9 tentatives.

Exemple : pour recevoir les appels vocaux et les SMS en cas d'alarme, utiliser deux groupes distincts, un pour chaque type de notification. En revanche, pour recevoir un seul type de notification, utiliser un seul groupe dans lequel doivent être indiqués dans l'ordre voulu appels vocaux et SMS. Dans ce dernier cas, le SMS est reçu uniquement si les appels vocaux n'aboutissent pas.

<NOTE>

Pendant les appels VOCAUX, il est possible d'interrompre le cycle d'appels à l'aide de la touche « 1 » ou « 9 » (pour plus de détails, voir le manuel d'utilisation et de programmation de la centrale Zeno).

EXEMPLES

Exemple	Configuration	Comportement
A	1) Notification IP -> Groupe 1 2) Envoi SMS -> Groupe 1	La centrale envoie uniquement une notification sur smartphone si elle est correctement reçue. Elle envoie en revanche le message SMS si la notification n'est pas reçue (par exemple, pour cause d'absence de réseau de données sur la centrale ou le smartphone).
B	1) Notification IP -> Groupe 1 2) Envoi Appel -> Groupe 2	La centrale envoie dans tous les cas notification et appel téléphonique.
C	1) Notification IP -> Groupe 1 2) Envoi Appel -> Groupe 2 3) Envoi SMS -> Groupe 2	La centrale envoie dans tous les cas notification et appel téléphonique. Si l'appel téléphonique n'aboutit pas, elle envoie également le message SMS.
D	1) Notification IP -> Groupe 1 2) Envoi SMS -> Groupe 2 3) Envoi appel téléphonique -> Groupe 2	La centrale envoie dans tous les cas notification et message SMS. Si le message SMS n'aboutit pas, elle envoie également un appel téléphonique.

Filtres :

En sélectionnant le filtre, il est possible de définir des notifications d'événements différentes :

- ☞ Tous les événements : la centrale signale aux destinataires du rapport les événements relatifs à des alarmes et des états du système.
- ☞ Événements d'état : la centrale signale aux destinataires du rapport les seuls événements relatifs à l'activation et à la désactivation du système et les états des Tamper. Il est déconseillé d'utiliser ce filtre, surtout sur l'adresse 1 parce qu'il bloque la notification des alarmes aux dispositifs à distance.

☞ Événements d'alarme : La centrale signale aux destinataires du rapport les seuls événements relatifs aux alarmes.

Rapport d'essai : cliquer sur « Test » pour envoyer un message d'essai ; il est envoyé au premier destinataire de la liste avec la valeur de Groupe la plus basse. Pour pouvoir envoyer le message d'essai à chaque destinataire, il suffit par conséquent de modifier temporairement la valeur des Groupes pour chaque destinataire.

<NOTE>

La destination d'envoi du rapport relatif aux caméras IP 1051/004 doit être programmée sur l'interface locale de la caméra (faire référence au manuel correspondant).

8.8 CHARGEMENT

Cette page permet de régler la destination d'envoi des images/vidéos acquises par les détecteurs dotés d'appareil-photos ou de caméras.

Adresse	Configuration
1	xhttp://testv2.elkron.com:8090/up-post.js
2	
3	
4	
5	
Prefix	127037490356

IP (Ethernet ou GPRS) avec protocole HTTP, ex: http://server:porta/path
IP (Ethernet ou GPRS) avec protocole FTP, ex: ftp://utente:password@server:porta/path
E-mail, ex: mailto: user@example.com
MMS, ex: mms: téléphone

Sauvegarder

Adresse 1 : adresse configurée automatiquement à la première connexion au serveur.

ATTENTION ! Ce paramètre ne doit en aucun cas être modifié !

En cas d'intervention d'entretien ou en cas de modification accidentelle de ce paramètre, rétablir :

Adresse 1 : <http://www.myzeno.urmet.com:8080/up-post.php>

Adresses 2~5 : indiquer adresses FTP.

☞ Format FTP : [ftp://user:password@IP address:port/folder](#)

Accès : identifiant d'accès de la centrale

ATTENTION : ce paramètre ne doit jamais être modifié !

En cas d'intervention d'entretien ou en cas de modification accidentelle de ce paramètre, il est nécessaire d'utiliser la procédure d'envoi de la configuration sur le portail (voir le guide dédié).

<NOTE>

La destination d'envoi d'images/vidéos acquis par les caméras IP 1051/004 doit être programmée sur l'interface locale de la caméra (faire référence au manuel correspondant).

8.9 CAPTURE EVENEMENTS

Cette page montre les images acquises par les détecteurs dotés d'appareil-photo. Seules les images des 10 derniers événements sont mémorisées. Cliquer sur l'image ou sur le Téléchargement de la vidéo pour visualiser le fichier.

Bienvenue	Contrôles	Centrale	Dispositifs	Paramètres	Utilisateur	Historique	Capture événements	Rapport événements	GSM	Réseau	Rapport	Uploader
Firmware	Déconnexion											
<h3>Image/vidéo événement</h3>												
Date et heure	Dispositif	Type	État									
2020-04-07 09:22:42	Dispositif 20	Image alarme 127037490356_Z20_2020-04-07_092242 	Disponible									
2020-03-28 12:38:35	Dispositif 13 (IR VIDEO CAM)	Demande vidéo 127037490356_Z13_2020-03-28_123835 Chargement	Disponible									
2020-03-28 12:32:59	Dispositif 20	Demande image 127037490356_Z20_2020-03-28_123259 	Disponible									

Date et heure : date et heure d'acquisition de l'image/vidéo.

Dispositif : numéro d'identification du détecteur qui a fourni l'image.

Type : image.

Image d'alarme : dans l'état actif ou partialisé, le détecteur doté d'appareil-photo trois ou six images en fonction du paramètre présent dans la page des Réglages.

Image demandée : il est possible de demander manuellement au détecteur d'acquérir une image.

État : l'état de l'événement acquis peut prendre les valeurs suivantes.

- **En attente fichier média** : le détecteur doté d'appareil-photo ou de caméra a acquis l'image/la vidéo et l'enverra à la centrale dès que le fichier sera prêt. Pour les images/vidéos d'alarme, si la centrale est désactivée dans cet état, l'image et la vidéo sont éliminées et ne sont pas envoyées.
- **En attente de capture** : le détecteur doté d'appareil-photo ou de caméra est en cours d'envoi de l'image/vidéo acquis à la centrale. Pour les images/vidéos d'alarme, si la centrale est désactivée dans cet état, l'image et la vidéo sont éliminées et ne sont pas envoyées.
- **Chargé** : le détecteur doté d'appareil-photo ou de caméra a terminé l'envoi de l'image/vidéo à la centrale. La centrale charge ensuite l'image/vidéo sur la destination programmée.
- **Disponible** : la centrale a terminé le chargement de l'image/vidéo.
- **Erreur** : le détecteur doté d'appareil-photo ou de caméra n'est pas parvenu à envoyer l'image/vidéo à la centrale. S'assurer que l'appareil-photo/caméra n'est pas défectueuse ou que sa batterie n'est pas déchargée (photos et films consomment une grande quantité d'énergie) puis effectuer un Walk Test pour contrôler l'intensité du signal.
- **Timeout** : le détecteur doté d'appareil-photo ou de caméra n'a pas répondu à la demande de la centrale. S'assurer que l'appareil-photo/caméra n'est pas défectueuse ou que sa batterie n'est pas déchargée (photos et films consomment une grande quantité d'énergie) puis effectuer un Walk Test pour contrôler l'intensité du signal.

<NOTE>

☞ Si l'alarme d'un détecteur doté d'appareil-photo ou de caméra est générée alors que le système est actif, ne pas désactiver le système d'alarme avant que l'état « Chargé » ou « Disponible » ne soit visualisé. Dans le cas contraire, l'image/vidéo est éliminée et n'est pas envoyée à la centrale ni au serveur du système.

☞ Les vidéos enregistrées par la caméra IP 1051/004 ne sont pas disponibles sur cette page.

9 HISTORIQUE

Cette page enregistre l'historique des événements de la centrale. L'historique mémorise 250 événements qui incluent :

- ✓ Tous les événements d'alarme
- ✓ Tous les événements d'anomalie
- ✓ Tous les événements d'activation et de désactivation depuis la télécommande ou le clavier avec l'information correspondante relative à l'utilisateur
- ✓ Tous les événements d'activation et de désactivation à distance

Bienvenue	Contrôles	Centrale	Dispositifs	Paramètres	Utilisateur	Historique	Capture événements	Rapport événements	GSM	Réseau	Rapport	Uploader
Firmware	Déconnexion											

Historique événements

Date et heure	Dispositif	Utilisateur	Événement
2020-05-21 13:43:58	Dispositif 20		Autoprotection rétablie
2020-05-21 12:04:27	Dispositif 30 (TVCC SIRENA)		Autoprotection
2020-05-21 11:37:19	Dispositif 20		Autoprotection
2020-05-21 11:17:28			Login Installateur
2020-05-21 11:16:47			Pas de signal GSM
2020-05-21 11:16:09			Allumé
2020-05-21 11:11:03			Autoprotection centrale OK
2020-05-21 11:10:58			Autoprotection centrale
2020-05-20 09:41:34		Utilisateur 1 (user)	Changement d'état distant : OFF
2020-05-20 09:41:25	Dispositif 13 (IR VIDEO CAM)		Début entrée 1

Date et heure : la date et l'heure auxquelles l'événement s'est produit..

Dispositif : dispositif qui a provoqué l'événement

Utilisateur : utilisateur qui a effectué l'action relative à l'événement.

Événement : description de l'événement.

<NOTE>

Les événements relatifs à la caméra IP 1051/004 ne sont pas disponibles sur cette page.

10 RAPPORT EVENEMENTS

Sur cette page, figurent tous les événements qui se sont succédés pendant le fonctionnement normal de la centrale et qui ont été envoyés au serveur du système :

Bienvenue	Contrôles	Centrale	Dispositifs	Paramètres	Utilisateur	Historique	Capture événements	Rapport événements	GSM	Réseau	Rapport	Uploader
Firmware	Déconnexion											

Rapport événements

Date et heure	Événement	CID événement	Groupe	Dispositif / Utilisateur	État
2020-05-21 13:43:58	Autoprotection rétablie	3383	1	20	Exécuté
2020-05-21 12:16:08	Test périodique	1602	0	0	Exécuté
2020-05-21 12:04:27	Autoprotection	1383	1	30	Exécuté
2020-05-21 11:37:19	Autoprotection	1383	1	20	Exécuté
2020-05-21 11:11:03	Autoprotection centrale rétablie	3137	0	0	Exécuté
2020-05-21 11:10:58	Autoprotection centrale	1137	0	0	Exécuté
2020-05-20 13:40:11	Test périodique	1602	0	0	Exécuté
2020-05-20 09:41:34	Désactivé à distance	1401	1	1	Exécuté
2020-05-20 09:30:00	Partiel A+B	3712	1	12	Exécuté
2020-05-20 09:29:45	Batterie chargée	3384	1	12	Exécuté
2020-05-20 09:25:55	Batterie faible	1384	1	12	Exécuté
2020-05-19 13:40:08	Test périodique	1602	0	0	Exécuté
2020-05-18 13:40:06	Test périodique	1602	0	0	Exécuté

La centrale enregistre un total de 250 événements signalés avec les informations suivantes :

Date et heure : date et heure de l'événement.

Événement : description de l'événement

Format du code CID Événements :

Le code CID Événements est enregistré dans un format de 4 chiffres constitué de « **Préfixe + Code événement** »

- ✓ Préfixe : « **1** » représente les événements en cours. « **3** » représente le reset des événements.
- ✓ Code événement : Code CID Événement de 3 chiffres.

Par exemple : « **1302** » signifie « Batterie déchargée » et « **3302** » signifie « Reset de batterie déchargée ».

Groupe : paramètre à ne pas prendre en compte. Pour utilisations futures.

Dispositif/utilisateur : pour activation/désactivation, utilisé avec le nom de l'utilisateur. Pour l'alarme, le numéro du dispositif s'affiche.

État : visualise la confirmation de la transmission de l'événement

<NOTE>

Les événements relatifs à la caméra IP 1051/004 ne sont pas disponibles sur cette page.

11 FIRMWARE

Cette page permet de mettre à jour le firmware de la centrale.

The screenshot shows a web interface with a top navigation bar containing the following items: Bienvenue, Contrôles, Centrale, Dispositifs, Paramètres, Utilisateur, Historique, Capture événements, Rapport événements, GSM, Réseau, Rapport, Uploader, and Firmware (highlighted with a red box). Below the navigation bar is a 'Déconnexion' link. The main content area is titled 'Mettre à jour Firmware'. Underneath the title, there is a file selection area with the text 'Fichier : Scegli file Nessun file selezionato' and a 'Sauvegarder' button (highlighted with a red box).

Phase 1. Sélectionner le fichier du firmware dans l'ordinateur.

Phase 2. Cliquer sur « **Sauver** » pour charger le fichier du firmware sur la centrale.

Phase 3. Le chargement s'effectue en quelques minutes seulement : NE PAS éteindre la centrale pendant l'opération. Pendant la phase de mise à jour, sur la centrale, les 3 voyants s'allument simultanément et au terme de la mise à jour, la centrale émet 2 bips sonores et retourne dans l'état initial.

Phase 4. Une fois l'opération terminée, cliquer sur le bouton « Accès » et s'assurer de la présence de la nouvelle version FW.

12 CARACTÉRISTIQUES TECHNIQUES DE LA CENTRALE

Performances principales :

- Communications bidirectionnelles en radiofréquence avec tous les dispositifs
- Connexion en radiofréquence jusqu'à 50 dispositifs
- Connexion jusqu'à 6 détecteurs IR dotés d'appareil-photo pour le contrôle vidéo des alarmes
- Connexion jusqu'à 4 caméras IP
- Gestion de 3 zones de partialisation + total
- 20 utilisateurs configurables maximum (codes et télécommandes)
- 20 codes d'activation/désactivation/partialisation configurables maximum
- Capacité de mémorisation : jusqu'à 200 événements
- Enregistrement de 3 ou 6 photos pour chaque alarme. Enregistrement de 30 secondes de vidéo dans le cas de la caméra IP, avec possibilité d'obtenir également l'enregistrement vidéo avant de l'événement d'alarme.
- Activations/désactivations depuis télécommandes, claviers, PC, smartphone ; contacts configurés pour les activations et désactivations.
- Envoi alarmes/images sur serveur HTTP/FTP, mails, appels téléphoniques et SMS (uniquement si la centrale dispose d'une carte SIM), notifications Push, protocoles CID et SIA.
- Écoute environnement.
- Écoute environnement avec caméra IP.
- Transmission alarmes via :
 - DTMF CID sur GSM (DC05) (uniquement si la centrale dispose d'une carte SIM)
 - CID/ SIA sur TCP/IP (DC09), sur Ethernet ou 4G (uniquement si la centrale dispose d'une carte SIM)
 - SMS sur GSM (uniquement si la centrale dispose d'une carte SIM)
 - Vidéos et images sur E-mail/ FTP sur Ethernet ou 4G (uniquement si la centrale dispose d'une carte SIM)
- Contrôle à distance via portail WEB ou APP (iOS et Android).
- Mesure présence signaux sans fil et 4G.
- Supervision de tous les dispositifs, sauf télécommande.
- Détection interférences en radiofréquence (anti-Jamming).
- Sirène intégrée.
- Conforme aux certifications EN 50131 Degré 2, Classe II.

Caractéristiques :

- GSM quad band 900/1800/850/1900 MHz
- Connexion sans fil en :
 - 4G
 - ZigBee HA 1.2
 - 868 MHz bande étroite
- Connexion sur réseau Ethernet 10/100 Mbit
- Alimentation interne de 12 V 1 A
- Consommation maximale : 41 mA à 230 Vca
- Batterie interne backup rechargeable : 7,2 V Ni-Mh, 1100 mAH
- Autonomie de la batterie de backup : 15 heures (moyenne), en fonction du comportement effectif
- Niveau sonore de la sirène interne : 95 dB à 1 m
- Température de fonctionnement : de -10°C à +45°C
- Dimensions : 260 x 176 x 30 mm
- Poids : 600 g

13 OUTILS DE GESTION À DISTANCE

Le système **Urmet Zeno** peut être géré à distance via smartphone et PC. Urmet met à disposition une application dédiée et un portail internet multi-navigateur, accessibles à l'aide de données confidentielles choisies par l'utilisateur.

Le **portail** est accessible à l'adresse suivante : <https://www.myzeno.urmet.com/home/>. La première chose à effectuer est de s'enregistrer comme Nouvel Utilisateur (une procédure guidée indique les opérations à effectuer). Après s'être enregistré, sur le portail, il est possible d'effectuer les opérations suivantes :

- Activer/partialiser/désactiver l'installation
- Visualiser l'état des dispositifs présents dans le système
- Visualiser les 200 derniers événements
- Configurer de nouveaux utilisateurs et de nouveaux codes ; visualiser ceux déjà présents en qualité de maître
- Visualiser les informations de base du système
- Configurer certains paramètres des dispositifs (entre autres l'exclusion des détecteurs en mode permanent)
- Modifier le mot de passe principal
- Configurer l'e-mail et les notifications push d'envoi des rapports
- Générer le code pour l'accès à l'installateur
- Visualiser les images filmées par les caméras IP 1051/004 en temps réel.

Le manuel d'utilisation du portail est disponible sur le site Urmet, dans la section *Produits-Anti-intrusion*. Pour y accéder, il est possible d'utiliser le lien suivant.

L'application **MyZeno** peut être installée sur le smartphone en se connectant à l'**App Store** (pour iPhone) ou à **Google Play** (pour Android). L'application permet de :

- Activer/partialiser/désactiver l'installation
- Visualiser l'état des dispositifs présents dans le système
- Visualiser les 200 derniers événements
- Visualiser les informations de base du système
- Modifier le mot de passe principal
- Configurer l'e-mail et les notifications push d'envoi des rapports
- Configurer des notifications pour les applications et les e-mails
- Effectuer l'enregistrement de la centrale et de l'utilisateur associé.
- Générer le code pour l'accès à l'installateur
- Visualiser les images filmées par les caméras IP en temps réel.

<NOTES IMPORTANTES>

- L'utilisateur doit prévoir une connexion à Internet via modem ADSL ou SIM de données compatible avec les dispositifs du système et avoir souscrit un abonnement à Internet.
- L'accès au portail et à l'application et la réception de notifications impliquent que la centrale Zeno soit constamment connectée à Internet.
- L'installation et la configuration des appareils de télécommunication qui permettent d'accéder à Internet sont de l'entière responsabilité de l'utilisateur.
- Urmet met en garde l'utilisateur contre le risque potentiel d'interruption de la connexion à Internet, qui pourrait compromettre, en tout ou partie, l'accès et le fonctionnement du portail et de l'application et la réception de notifications et de mails.
- Urmet décline toute responsabilité en cas de mauvais fonctionnement ou d'impossibilité d'accès au portail et à l'application et de réception de notifications et de mails à cause d'une interruption de la connexion à Internet de l'utilisateur.
- La connexion de plus d'une session à la fois n'est pas admise, que ce soit depuis l'application ou depuis le portail. Une connexion exclut l'autre.
- Pendant les phases d'installation puis d'entretien à travers le panneau de contrôle local, il est déconseillé d'utiliser simultanément l'application et le portail pour d'éventuels tests de système ou pour interagir avec le système. Au terme des opérations d'installation et d'entretien, débrancher le PC local.
- En l'absence de réception des mails, contrôler le contenu des dossiers de spam/mails indésirables.
- Pour des raisons de sécurité, le portail et l'application sont sujet à une durée maximale de chaque session.
- Pour le portail et l'application, il est recommandé d'utiliser un mot de passe d'au moins 8 caractères.
- Une tentative d'effraction alors que le système est actif est enregistrée dans l'historique de l'application et du portail comme effraction tamper et comme alarme d'intrusion.

Les éventuelles mises à jour de la documentation et aux ressources et approfondissements sont disponibles sur le site www.urmet.fr :

Dans cette section, on peut trouver :

- Le manuel complet de programmation et d'utilisation de la centrale
- La guide d'utilisation du portail et de l'appli **MyZeno**
- Le logiciel **FINDER** pour la configuration initiale de la centrale

DÉCLARATION DE CONFORMITÉ UE SIMPLIFIÉE

Le fabricant, URMET S.p.A., déclare que le type d'appareil radio :

CENTRALE SANS FIL AVEC RÉSEAU IP ET 4G Réf. 1051/018 est conforme à la Directive 2014/53/UE.

Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante :

www.urmet.com

LES BONS GESTES DE MISE AU REBUT DE CE PRODUIT (Déchets d'équipements électriques et électroniques)

 Ce symbole apposé sur le produit, ses accessoires ou sa documentation indique que ni le produit, ni ses accessoires électroniques usagés (chargeur, casque audio, câble USB, etc.), ne peuvent être jetés avec les autres déchets ménagers.

 La mise au rebut incontrôlée des déchets présentant des risques environnementaux et de santé publique, veuillez séparer vos produits et accessoires usagés des autres déchets. Vous favoriserez ainsi le recyclage de la matière qui les compose dans le cadre d'un développement durable.

DS1051-028

URMET S.p.A.
10154 TURIN (ITALIE)
VIA BOLOGNA 188/C
Tél. +39 011.24.00.000

urmet



Service technique Service clients TÉL.
0112339810
<http://www.urmet.com>
e-mail : info@urmet.com
Fabriqué à Taiwan selon les
spécifications Urmet