Control Panel

B6512

fr Guide de présentation

Table des matières

1 Logiciel de paramétrage à distance (RPS, Remote Programming Software)

Le logiciel Remote Programming Software (RPS) est un utilitaire de gestion des comptes et de paramétrage de centrale destiné aux systèmes d'exploitation Microsoft Windows. Les opérateurs peuvent effectuer des tâches de programmation, de stockage de compte, de commande à distance et de diagnostics pour différentes centrales.

Assistance

Accédez à nos **services d'assistance** à l'adresse www.boschsecurity.com/xc/en/support/.
Bosch Security and Safety Systems propose une assistance dans les domaines suivants :

- Applications & Outils
- Building Information Modeling
- Garantie
- Dépannage
- Réparation & Échange
- Sécurité des produits

Bosch Building Technologies Academy

Visitez le site Web Bosch Building Technologies Academy et accédez à des **cours de formation, des didacticiels vidéo** et des **documents** : www.boschsecurity.com/xc/en/support/training/

2 Utilisez les logiciels les plus récents

Avant d'utiliser l'appareil pour la première fois, assurez-vous d'installer la dernière version applicable de votre logiciel. Pour une fonctionnalité, une compatibilité, des performances et une sécurité cohérentes, mettez régulièrement à jour le logiciel tout au long de la durée de vie de l'appareil. Suivez les instructions de la documentation produit relative aux mises à jour logicielles.

Les liens suivants fournissent plus de précisions :

– Informations générales : https://www.boschsecurity.com/xc/en/support/product-security/
– Avis de sécurité (liste des vulnérabilités identifiées et des solutions proposées) : https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch n'assume aucune responsabilité en cas de dommages provoqués par l'utilisation de ses produits avec des composants logiciels obsolètes.

3 Paramètres de conformité

3.1 Vérification SIA CP-01

Valeur par défaut : Non
Choix :
– Oui : RPS examine les paramètres pour vérifier la conformité SIA CP-01 des paramètres de compte de centrale.
– Non : RPS n'examine pas la conformité des paramètres.
RPS vérifie la conformité SIA CP-01 des paramètres suivants :
Type de contrainte, page 84
Sirène d'alarme, page 146
Durée de la temporisation de sortie, page 104
Durée intrusion, page 111
Avertissement de temporisation de sortie, page 118
Avertissement de temporisation d'entrée, page 118
Temporisation d'entrée, page 227
Longueur du code, page 89
Avertissement à distance, page 90
Nombre de points inhibables, page 90
Rapports d'annulation, page 85
Règle de présence de deux personnes ?, page 108 ?
Contrainte en avance ?, page 109 ?
Tout activé Instantané, page 181
Partielle Instantané, page 182
Fonction de saisie de code, page 125
Emplacement dans le menu RPS
Vérification de la conformité > Vérification SIA CP-01

3.2 Conformité ULC

Valeur par défaut : Non
Choix :
– Oui. Ajuster le fonctionnement de centrale pour la conformité ULC (UL Canada).
– Non : Ne pas ajuster pour la conformité ULC.
Si ce paramètre est défini sur Oui, la centrale est configurée pour ignorer l'entrée de tous les détecteurs pendant au moins 120 secondes au démarrage du système.
Lorsque le traitement du détecteur est démarré, la centrale signale un événement unique avant de signaler des événements de point. En outre, aucun événement lié à l'alimentation n'est signalé à moins qu'il ne soit déterminé que le défaut ne sera pas restauré dans un délai de 120 secondes.
Emplacement dans le menu RPS
Paramètres de conformité > Conformité ULC

3.2.1 Conformité CAN/ULC-S304

CAN/ULC-S304, CENTRE DE RÉCEPTION DES SIGNAUX ET UNITÉS DE CONTRÔLE D'ALARME SUR SITE
Cette norme couvre les exigences en matière de construction et de performances pour les unités de contrôle et accessoires des systèmes d'alarme intrusion, y compris les unités de contrôle et accessoires sur site protégé pour les connexions locales ou les connexions de

centre de réception de signal, et pour le matériel de réception d'alarme de centre de réception de signal, y compris le matériel d'enregistrement. Ce matériel est conçu pour une utilisation sur site, dans des coffres-forts et des chambres fortes.

Exigences de paramétrage de centrale
La définition du paramètre Compatible ULC sur Oui est la première exigence de paramétrage de centrale pour la conformité avec la norme CAN ULC-S304.

3.2.2 CAN/ULC-S559, paramétrage requis

CAN/ULC-S559, Normes pour l'équipement des systèmes et des centrales de réception d'alarme incendie
La norme CAN/ULC-S559 couvre les exigences relatives aux systèmes et centres de réception d'alarme incendie, notamment le matériel de transmission et de réception, le matériel de centre de réception incendie propriétaire et les accessoires d'unité de contrôle. Les systèmes de centre de réception de signal incendie incluent l'unité et le récepteur de site protégé pour les applications en intérieur et en extérieur ordinaires (non dangereuses). Les méthodes de paramétrage, le test, le service et autres logiciels conçus pour une utilisation avec le matériel des systèmes et centrales de réception d'alarme incendie sont inclus dans l'évaluation du matériel. Les unités de réception des signaux utilisées dans les centres de réception d'alarme incendie, les centres satellites, les centres de traitement du signal et les centres de relais sont également couverts par les exigences de cette norme.

PARAMÈTRES DE CONFORMITÉ > Compatible ULC
Définissez le paramètre PARAMÈTRES DE CONFORMITÉ > Compatible ULC sur Oui.

PARAMÈTRES LIÉS À LA CENTRALE > Routage des rapports
Dans la colonne Groupe destinataire 4 :
- Définissez Rapports incendie, Rapports gaz, Rapports cambriolage, Rapports urgence personnelle, Rapports utilisateur et Rapports tests sur Non.
- Définissez les rapports de sortie, les rapports de fonctions automatiques, les rapports RPS, les rapports de points, les rapports de changement d'utilisateur et les rapports d'accès sur Non.
- Vérifiez que rapport des diagnostiques est défini sur la fonction customiser. Les étapes suivantes permettent de configurer les paramètres personnalisés.

PARAMÈTRES LIÉS À LA CENTRALE > Routage des rapports > Rapports d'incendie > Annulation incendie
Définissez le paramètre PARAMÈTRES LIÉS À LA CENTRALE > Routage des rapports > Rapports d'incendie > Annulation incendie pour chaque groupe destinataire (1 à 4) sur Non.

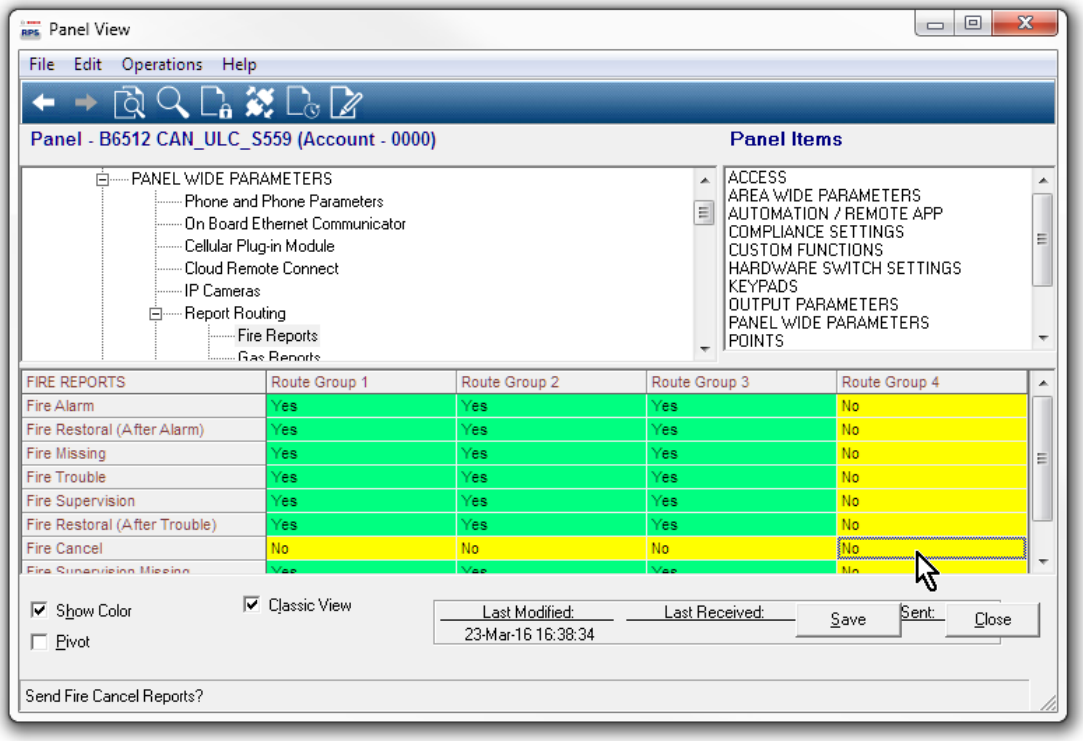


Figure 3.1: Annulation incendie

PARAMÈTRES LIÉS À LA CENTRALE > Routage des rapports > Rapports diagnostiques
Dans la colonne Route Groupe 4, définir SDI2 Défaillance de l'appareil sur Oui. Définissez les autres rapports sur No.

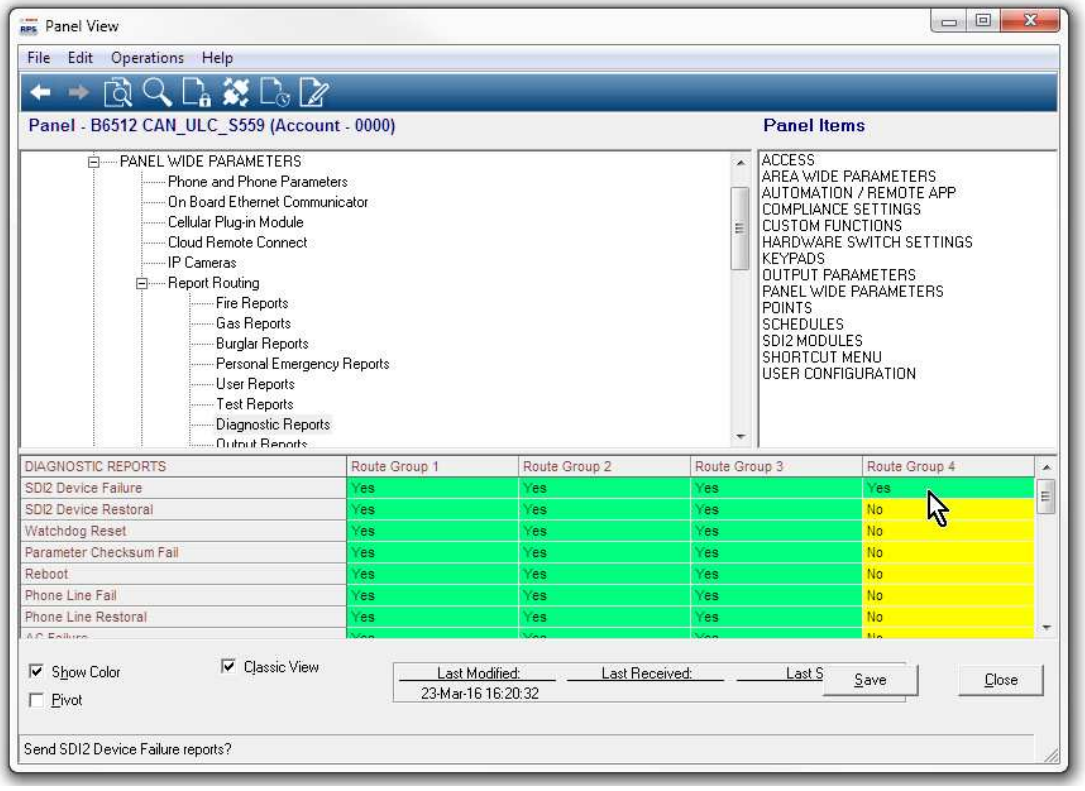


Figure 3.2: Défaillance de dispositif SDI2

PARAMÈTRES LIES DE LA CENTRALE> Communicateur> Dispositif de destination principal

Dans la colonne Route Groupe 4, Définissez la destination principale sur le périphérique de destination utilisée (par exemple, IP embarqué, destination 4).

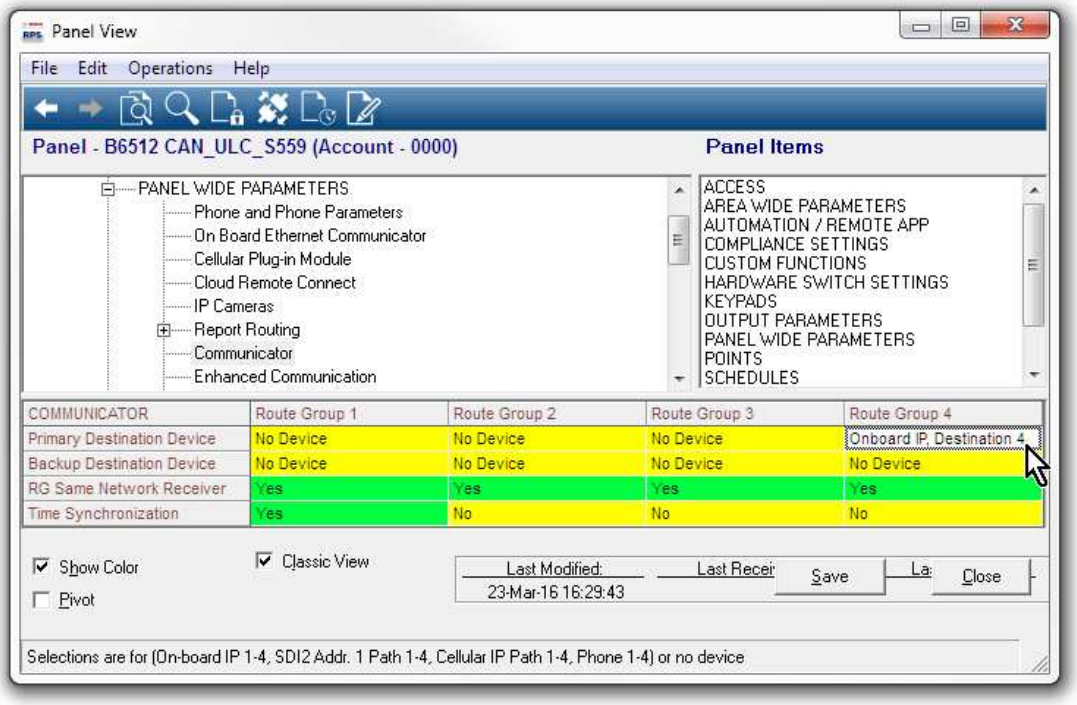


Figure 3.3: Dispositif destinataire principal

PARAMÈTRES LIES DU PANNEAU> Communication améliorée> Destination 4

Dans la colonne Destination 4, définissez Network Address sur 0.1.1.1 (cette adresse est intentionnellement une adresse fictive sur le réseau). Définissez Cadence d'interrogation sur 0 et En attente d'accusé de réception (secondes) sur 5.

POINTS > Profils de point (Indices de point)

Configurez les profils de point 1, 4 et 6 comme suit.

Il est important de configurer les paramètres dans l'ordre.

Profil de point 1

Définissez Alarme abandons sur No. sur No.

Définissez le texte du profil du point (première langue) sur la centrale incendie défaut

Définissez le type de point / la réponse / le style de circuit> Type de point sur le point de feu.

Définissez le type de point / la réponse / le style de circuit> le type de circuit sur une seule EOL (1KΩ) ou une seule OEL (2KΩ).

Définissez Réponse sur 3.

Profil de point 4

Définissez le texte du profil du point (première langue) sur l'alarme de la centrale d'incendie.

Définissez le type de point / la réponse / le style de circuit> Type de point sur le point de feu.

Définissez Point Type / Réponse / Circuit Style > Circuit Style sur Simple EOL (1KΩ), Simple EOL (2KΩ) ou Double EOL.

Si vous définissez Point Type / Réponse / Circuit Style > Circuit Style sur Simple EOL (1KΩ) ou Simple EOL (2KΩ), définissez Réponse sur 1.

Si vous définissez Type de point / Réponse / Circuit Style > Circuit Style sur Double EOL, définissez Réponse sur 0.

Profil de point 6

Définissez le texte du profil du point (première langue) sur la surveillance de la centrale d'incendie.

Définissez le type de point / la réponse / le style de circuit> Type de point sur le point de feu.

Définissez Point Type / Réponse / Circuit Style > Circuit Style sur Simple EOL (1KΩ), Simple EOL (2KΩ) ou Double EOL.

Si vous définissez Point Type / Réponse / Circuit Style > Circuit Style sur Simple EOL (1KΩ) ou Simple EOL (2KΩ), définissez Réponse sur 9.

Si vous définissez Type de point / Réponse / Circuit Style > Circuit Style sur Double EOL, définissez Réponse sur 2.

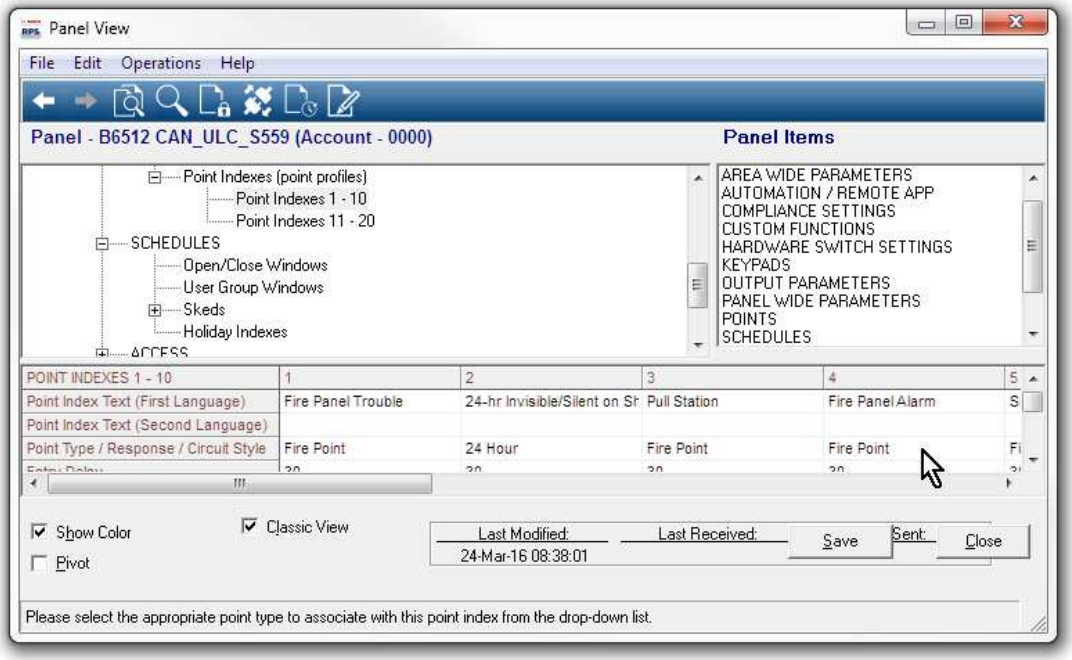


Figure 3.4: Profils de point

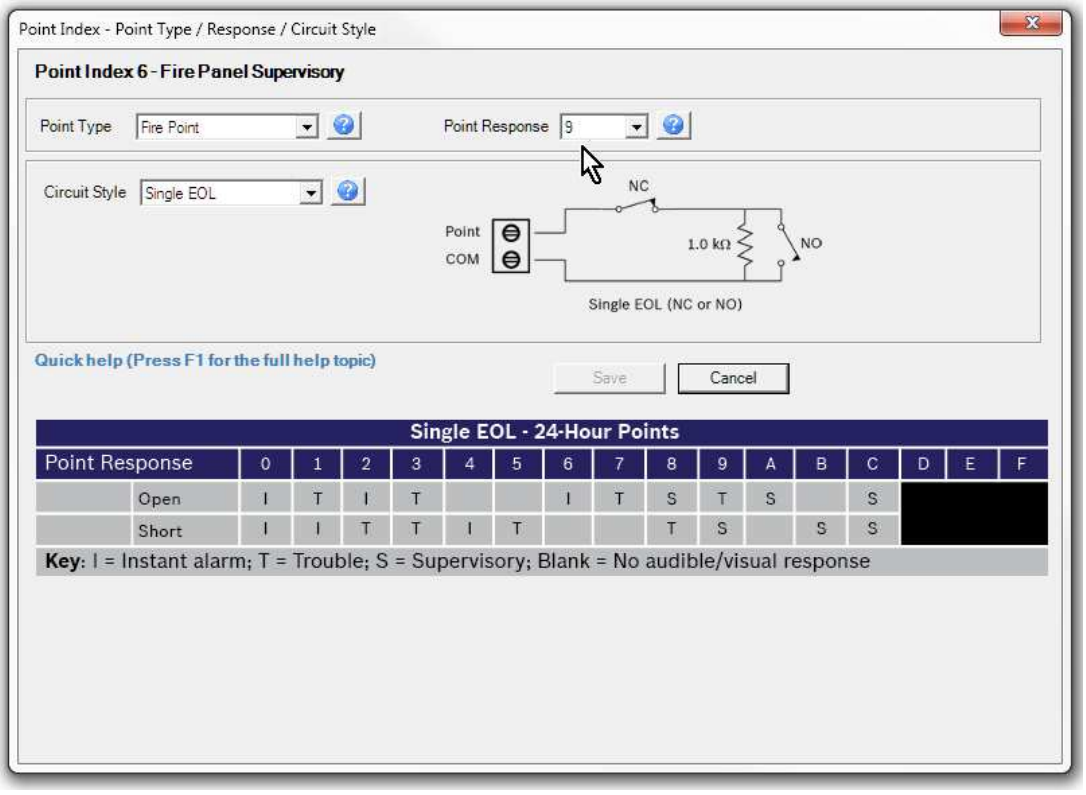


Figure 3.5: Réponse du type de point et type de circuit

POINTS> Affectations de points

Définissez les paramètres POINTS> Affectations de points, texte et profil, pour les points 1, 2 et 3 intégrés comme suit.

Point 1

Définissez Point de missions> de Texte Alarme centrale incendie.
Définissez Point d'affectation> profile 4 de Texte Alarme centrale incendie.

Point 2

Définissez Point d'affectations> de Texte Alarme centrale incendie.
Définissez Point de affectations> Profile sur 1 - Centrale d'incendie en défaut

Point 3

Définissez les affectations de points> Texte sur Surveillance du panneau d'incendie sur Supervision Centrale Incendie.
Définissez affectations de points > Profil sur 6 - Supervision de centrale.

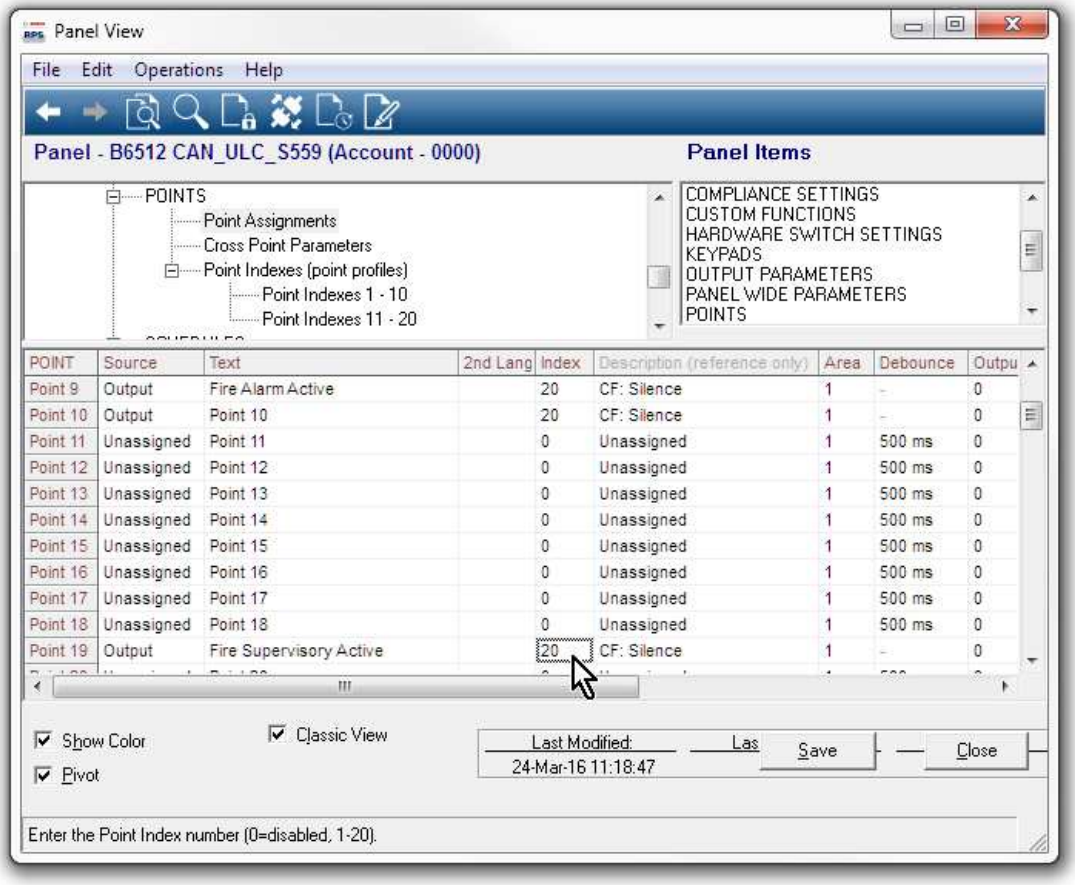


Figure 3.6: Supervision de centrale

3.2.3 CAN/ULC-S559, paramétrage recommandé

Rendre silencieux les événements d'alarme incendie, de défaut et de supervision sur la centrale

Lorsque les centrales sont configurées comme décrit ci-dessous, elles rendent automatiquement silencieux les pavés numériques connectés à la centrale en ce qui concerne les événements d'alarme incendie, de défaut et de supervision de la centrale d'alarme incendie.

FONCTIONS CUSTOMISER > fonction customiser 128

Définissez fonction customiser 128 > fonction customiser Textesur Silence.
Définissez fonction customiser 128 > Fonction 1 sur Défaut Silence (définissez Paramètre 1 sur Partition 1).
Définissez fonction customiser 128 > Fonction 2 sur AlarmeSilence (définissez Paramètre 1 sur Partition 1).

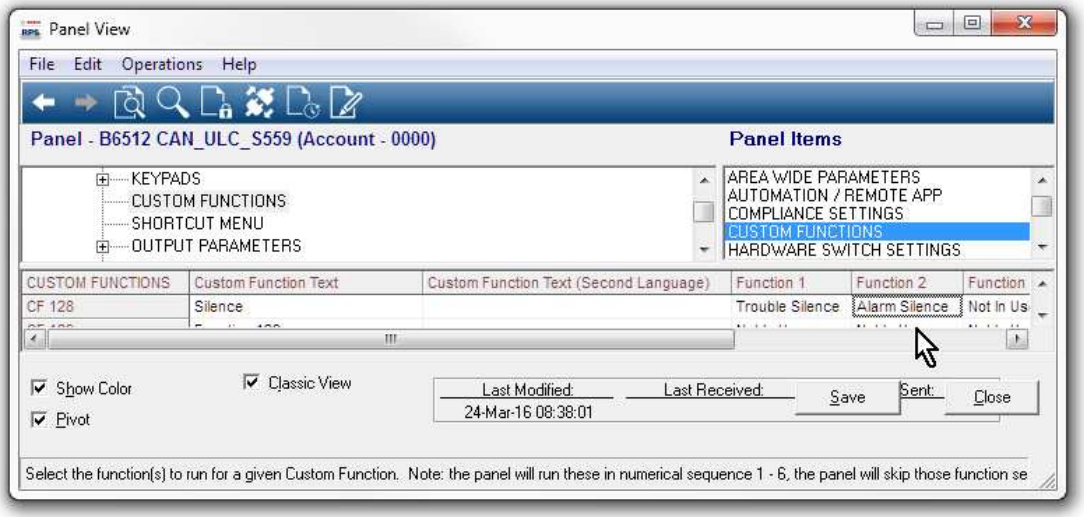


Figure 3.7: Fonction personnalisée 128

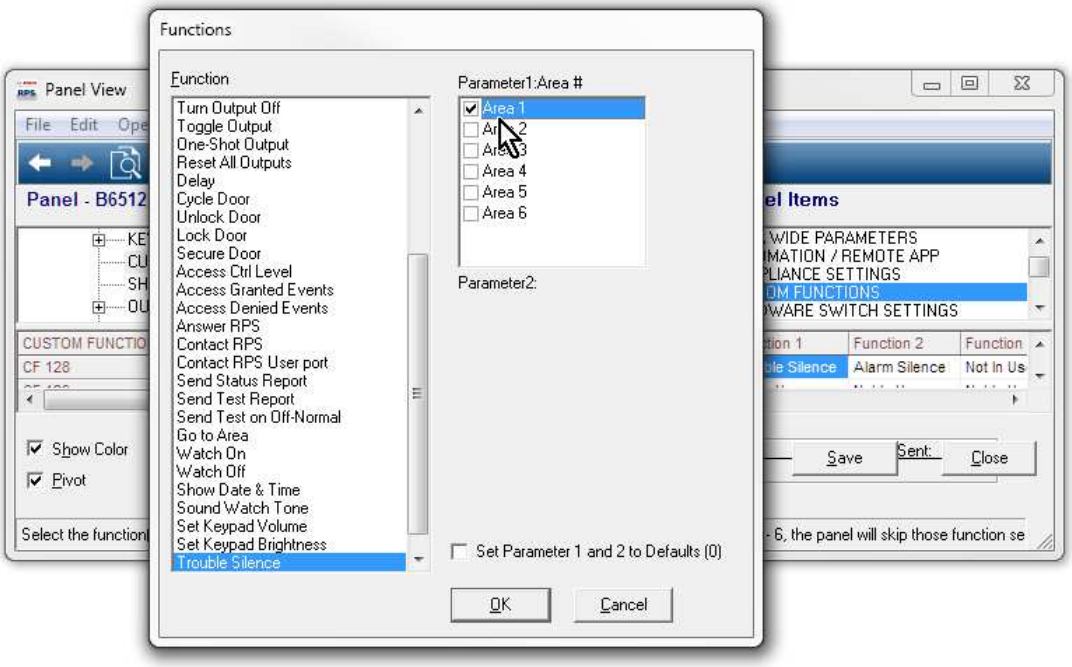


Figure 3.8: Sélection de la zone 1

sortie Paramètres> sorties liées de la centrale

Pour les sorties virtuelles :

Définissez sortie liées à la centrale > Résumé incendie sur 9.

Définissez Sortie liées à la centrale > Résumé incendie Défaut sur 10.

Définissez Sortie liées à la centrale > Résumé supervision incendie sur 19.

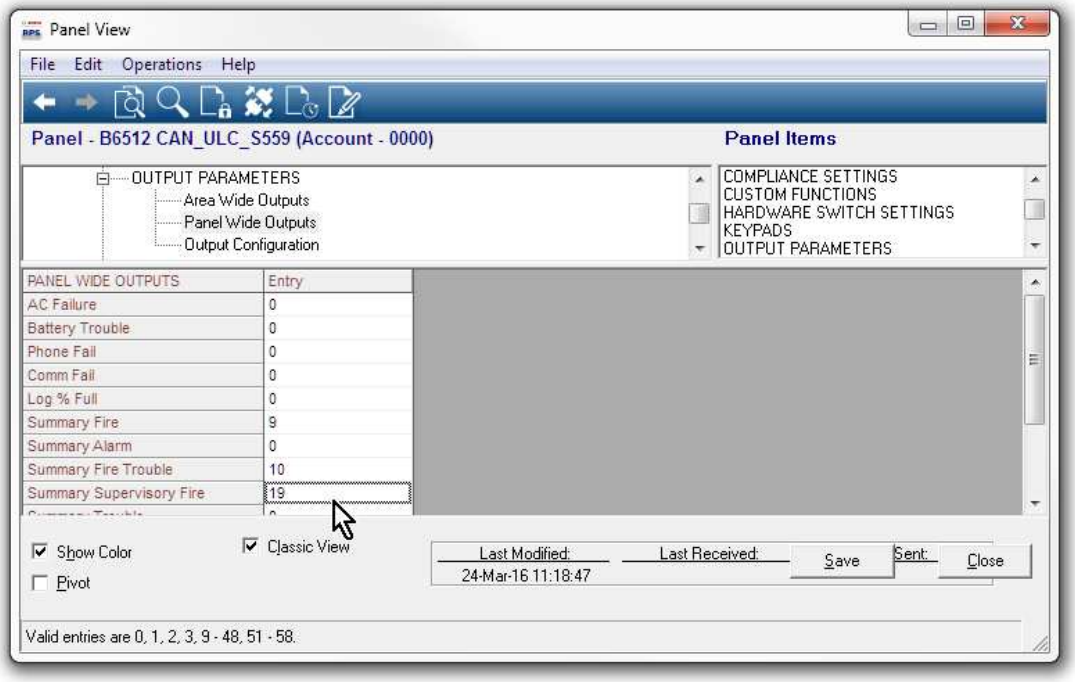


Figure 3.9: Sorties liées de la centrale

POINTS > Profils de point (Indices de point)

Configurez le profil point 20 comme suit.

Il est important de configurer les paramètres dans l'ordre.

Profil de point 20

Définissez Texte profile de point(Première langue) sur CF: Silence.

Définissez Type de point / Réponse / Style de circuit > Type de point sur fonction customiser.

Laissez Type de point / Réponse / Style circuit >Style circuit défini sur la valeur par défaut Simple EOL (1KΩ).

Laissez Type de point / Réponse / Style circuit > Réponse défini sur la valeur par défaut 7.

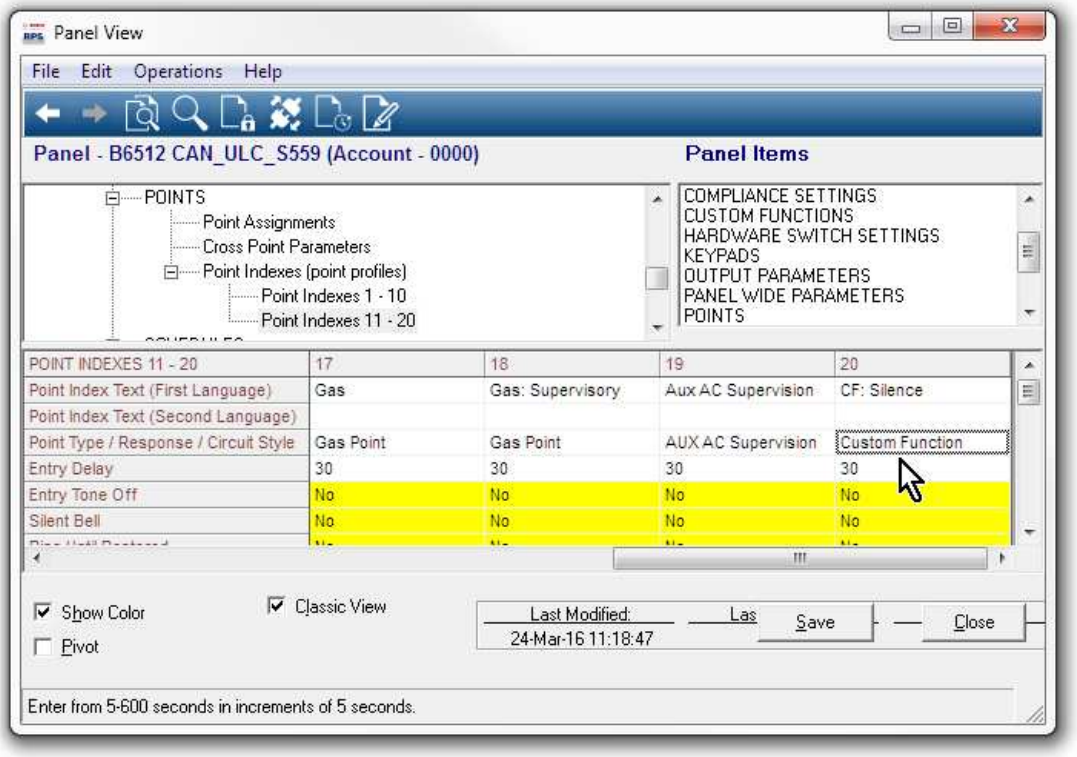


Figure 3.10: Profil de point 20

POINTS> Affectations de points

Définissez les paramètres POINTS > Points Liés, Source, Texte et Profile, pour les points 9, 10 et 19 comme suit.

Point 9

Définissez Points Liés > Source sur Sorties.
Définissez Points Liés > Textesur Fire AlarmeActive.
Définissez Points Liés > Profile sur 20 - CF: Silence

Point 10

Définissez Points Liés > Source sur Sorties.
Définissez Points Liés > Texte sur Défaut Incendie actif
Définissez Points Liés > Profile sur 20 - CF: Silence

Point 19

Définissez Points Liés > Source sur Sorties.
Définissez Points Liés > Texte sur Défaut supervision Incendie actif
Définissez Points Liés > Profile sur 20 - CF: Silence

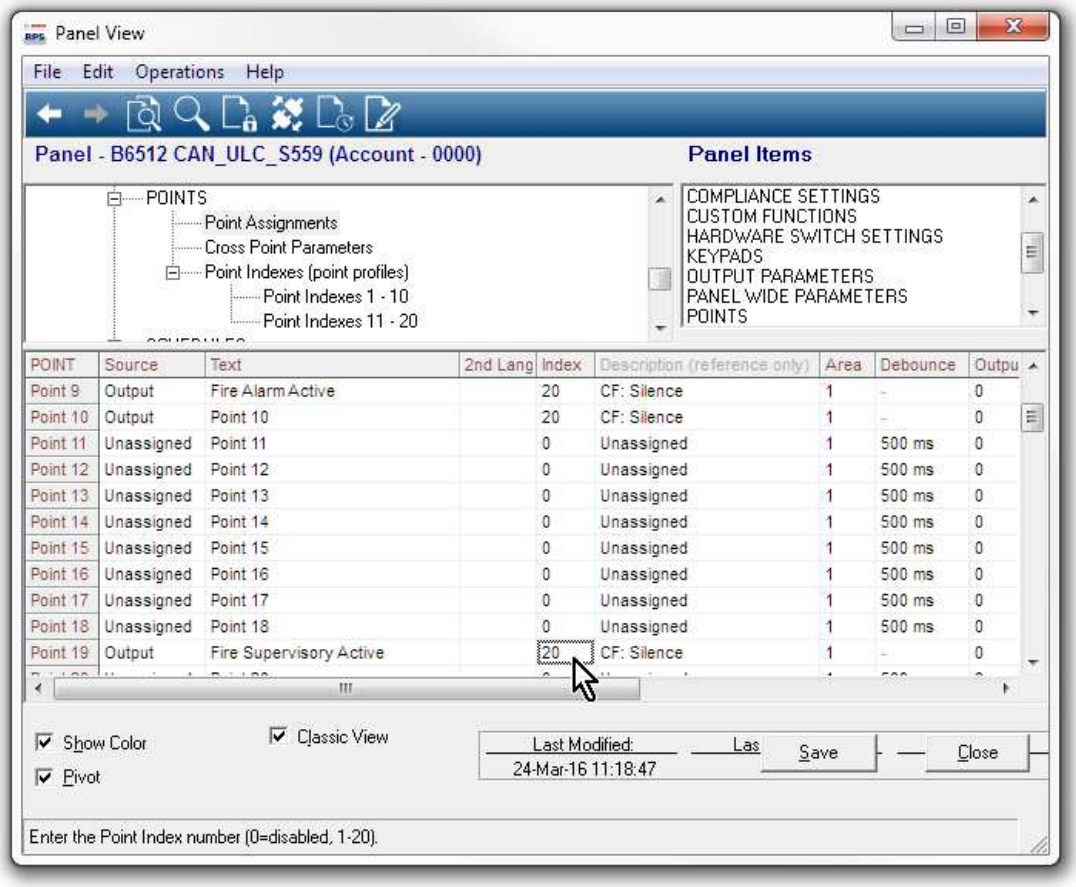


Figure 3.11: Affectations de point

3.3 Configuration de la supervision

Optimisation des données utilisées pour la supervision :

Type d'installation	Intrusion commercial (UL1610)	Intrusion commercial (ULC S304)	Supervision élevée	Toutes les heures	Sécurité moyenne ou Incendie de maison familiale	Supervision quotidienne
Intervalle de supervision requis	200 secondes	180 secondes	300 secondes	1 heure	4 heures	25 heures
Plan de service recommandé	Étendu	Étendu	Supervision élevée	Standard	Standard	Sauvegarde
Paramétrage de la centrale						
Temps de supervision du récepteur	200 secondes	Personnalisé	300 secondes	1 heure – NFPA	4 heures – Sécurité moyenne	25 heures

Type d'installation	Intrusion commercial (UL1610)	Intrusion commercial (ULC S304)	Supervision élevée	Toutes les heures	Sécurité moyenne ou Incendie de maison familiale	Supervision quotidienne
Cadence d'interrogation de centrale (s)	n/a	89 secondes	n/a	n/a	n/a	n/a
En attente d'accusé de réception centrale (s)	n/a	15	n/a	n/a	n/a	n/a
Compte nouvelles tentatives de centrale	n/a	5	n/a	n/a	n/a	n/a

3.4 Application européenne

Valeur par défaut : Non
Choix :
Oui - application destinée au marché européen. Le format de transmetteur SIA DC-09 sera disponible.
Non - non destiné au marché européen. Le format de transmetteur SIA DC-09 ne sera pas disponible.

Remarque!
UL n'ayant pas procédé à la vérification de conformité du transmetteur SIA DC-09, celui-ci ne sera pas disponible en dehors du marché européen. Ne sélectionnez pas le format de transmetteur SIA DC-09 pour les applications UL ou ULC.

Emplacement du menu RPS
Paramètres de conformité > Application européenne

4 Paramètres liés à la centrale

4.1 Téléphone et paramètres du téléphone

4.1.1 Destination téléphonique 1 (à 4)

Valeur par défaut : Vide

Choix :

- Vide : la centrale ne compose aucun numéro de téléphone.
- 0 à 9 : la centrale compose ces caractères.
- C : la centrale effectue une pause de 2 secondes lorsqu'elle détecte un C dans la séquence de numérotation.
- D : la centrale compose un numéro lorsqu'elle détecte une tonalité, ou lorsque le délai de détection de tonalité de 7 secondes initial arrive à expiration. Pour rallonger le délai de détection de tonalité, insérez D au début de la séquence de numérotation.
- #,* : la centrale compose ces caractères comme s'ils étaient entrés sur le clavier d'un téléphone.

Entrez la séquence de numérotation (numéro de téléphone) utilisée par la centrale pour envoyer des rapports au récepteur du centre de télésurveillance.

Si ce paramètre est laissé vide, cela ne désactive pas le champ Destination téléphonique. Pour éviter l'utilisation de la destination téléphonique, ne l'affectez pas à un dispositif de destination principal ou de sauvegarde. Pour plus d'informations, voir *Communicateur, vue d'ensemble, page 66*.

Configuration des destinations téléphoniques pour un appel en instance

La numérotation d'une séquence d'appel en instance sur une ligne ne gérant pas cette fonction ne permet pas à la centrale d'envoyer des rapports au récepteur du centre de télésurveillance. Si un client annule le service d'appel en instance sans en informer sa société de sécurité, la centrale ne peut pas envoyer des rapports à l'aide du dispositif de destination de sauvegarde.

Si vous configurez une destination téléphonique avec un numéro de téléphone qui comprend une séquence d'annulation d'appel en instance, choisissez cette destination téléphonique comme *Dispositif destinataire principal, page 68* d'un groupe destinataire. Configurez une autre destination téléphonique sans séquence d'annulation d'appel en instance et choisissez-la comme *Dispositifs de destination de sauvegarde, page 69* du groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Destination téléphonique 1 à 4

4.1.2 Format de destination téléphonique 1 (à 4)

Valeur par défaut : Modem4

Choix :

- Modem4 : la centrale envoie des rapports Modem4 étendus au récepteur du centre de télésurveillance. Les informations étendues incluent le texte du point, le texte de sortie et les noms d'utilisateur.
- Contact ID : la centrale envoie des rapports Contact ID. Utilisez ce format lorsque le récepteur du centre de télésurveillance ne prend pas en charge le format Modem4.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Format de destination téléphonique 1 (à 4)

4.1.3 Numérotation DTMF

Valeur par défaut : Oui

Choix :

– Oui : la centrale compose les numéros de téléphone à l'aide de DTMF.
– Non : la centrale compose les numéros de téléphone à l'aide de la numérotation à impulsions.

Avant de définir ce paramètre sur Non, assurez-vous que le réseau RTC (réseau téléphonique commuté public) auquel est connectée la centrale prend en charge la numérotation à impulsions.

Emplacement dans le menu RPS :

Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Numérotation DTMF

4.1.4 Durée de supervision téléphonique

Valeur par défaut : 0

Choix :

– 0 : désactivé, aucune supervision de la ligne téléphonique.
– 10 à 240 (secondes) : nombre de secondes (par incréments de 10 secondes) pendant lesquelles une ligne téléphonique doit être en défaut avant que la centrale crée un événement de défaillance de la ligne téléphonique.

La centrale vérifie la ligne téléphonique environ neuf fois par minute. Si elle détecte une défaillance de la ligne téléphonique qui dure le nombre de secondes défini au niveau de ce paramètre, elle crée un événement de défaillance de la ligne téléphonique.

Les claviers affichent une défaillance de ligne téléphonique et émettent une tonalité de défaut si les paramètres *Échec d'activation de la sonnerie, page 33* et *Tonalité de défaut, page 127* sont définis sur Oui. Si le paramètre *Échec d'activation de l'alarme, page 32* est défini sur Oui, les claviers affichent un événement d'alarme et émettent une tonalité d'alarme.

Lorsque la ligne téléphonique est normale (défaut effacé) pendant le nombre de secondes défini au niveau de ce paramètre, la centrale crée un événement de rétablissement de la ligne téléphonique.

La centrale envoie des rapports de défaillance de la ligne téléphonique et de rétablissement de la ligne téléphonique lorsque les événements se produisent. Ils sont également inclus dans les *Transmission rapport de test, page 33*.

Les événements de défaillance de la ligne téléphonique sont liés à la Partition 1 et ils utilisent la configuration de la Partition 1.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Durée de supervision téléphonique

4.1.5 Échec d'activation de l'alarme

Valeur par défaut : Non

Choix :

– Oui : réponse aux alarmes (sirène intrusion, tonalité d'alarme au clavier, rapport d'alarme) pour les événements de défaillance de la ligne téléphonique.
– Non : aucune réponse aux alarmes pour les événements de défaillance de la ligne téléphonique

Pour utiliser cette fonction Échec d'activation de l'alarme, activez la supervision de la ligne téléphonique au niveau du paramètre Durée de supervision téléphonique.

Voir *Durée de supervision téléphonique, page 32*.

La réponse aux alarmes pour les événements de défaillance de la ligne téléphonique comprend :

– l'activation de la sirène intrusion de la Partition 1,
– l'activation de la tonalité d'alarme au niveau des claviers,
– l'envoi de rapports d'alarme.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Échec d'activation de l'alarme

4.1.6 Échec d'activation de la sonnerie

Valeur par défaut : Non

Choix :

– Oui : tonalité de défaut de niveau centrale sur tous les claviers lorsqu'un événement de défaillance de la ligne téléphonique se produit.
– Non : aucune tonalité de défaut sur aucun clavier lorsqu'un événement de défaillance de la ligne téléphonique se produit.

Pour utiliser cette fonction Échec d'activation de la sonnerie, définissez la supervision de la ligne téléphonique au niveau du paramètre Durée de supervision téléphonique.

Voir *Durée de supervision téléphonique, page 32*.

Les tonalités de défaut de niveau centrale sont définies pour les claviers individuels au niveau du paramètre Tonalité de défaut (*Tonalité de défaut, page 127*). La valeur par défaut pour le paramètre Tonalité de défaut pour tous les claviers est Non (aucune tonalité de défaut pour les défauts de niveau centrale).

Emplacement dans le menu RPS

Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Échec d'activation de la sonnerie

4.1.7 Transmission rapport de test

Valeur par défaut : Non

Choix :

– Oui : transmettre les rapports de test utilisateurs et les rapports de test de planification (planifiés) afin d'inclure les informations sur l'état du système anormales.
– Non : ne pas transmettre les rapports de test.

Lorsque ce paramètre est défini sur Oui, le rapport de test (ou rapport de test anormal) est suivi d'un rapport de diagnostic pour chaque état anormal du système. Accédez à Paramètres liés à la centrale > Routage des rapports > *Rapports diagnostiques, page 61* pour obtenir une liste des rapports inclus.

Remarque!

Rapport de test étendu défini sur Oui

Lorsque le rapport de test étendu est défini sur **Oui**, vous devez définir le format de rapport sur **Modem4**.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Transmission rapport de test

4.1.8 Compatibilité RTC

Valeur par défaut : valeur appropriée pour la région

Choix :

Algérie	El Salvador	Liban	Réunion
Argentine	Équateur	Lesotho	Roumanie
Arménie	Estonie	Liechtenstein	Russie
Australie	Finlande	Lituanie	Arabie saoudite
Autriche	France	Luxembourg	Singapour
Bahamas	Géorgie	Macao	Slovaquie
Bahreïn	Allemagne	Malaisie	Slovénie
Biélorussie	Ghana	Malte	Afrique du Sud
Belgique	Grèce	Martinique	Espagne
Bermudes	Guadeloupe	Mexique	Sri Lanka
Brésil	Guam	Moldavie	Suède
Brunei	Hong Kong	Maroc	Suisse
Bulgarie	Hongrie	Pays-Bas	Taïwan
Canada	Islande	Nouvelle-Zélande	Thaïlande
Caraïbes	Inde	Nigeria	Tunisie
Chili	Indonésie	Norvège	Turquie
Chine	Irlande	Oman	ÉAU
Colombie	Israël	Pakistan	Ukraine
Costa Rica	Italie	Paraguay	Royaume-Uni
Croatie	Japon	Pérou	Uruguay
Chypre	Jordanie	Philippines	États-Unis
République tchèque	Kazakhstan	Pologne	Ouzbékistan
Danemark	Corée	Polynésie (française)	Venezuela
République dominicaine	Koweït	Portugal	Yémen
	Kirghizstan	Porto Rico	Zambie
Dubaï	Lettonie	Qatar	
Égypte			

Ce paramètre configure la centrale et le communicateur téléphonique enfichable B430 pour les réseaux téléphoniques commutés publics (RTC).

Remarque!
Exigences RTC pour l'Australie/la Nouvelle-Zélande, désactivation de la réponse RPS armé/désarmé
Si vous définissez ce paramètre Compatibilité RTC sur Australie ou Nouvelle-Zélande, vous devez définir Paramètres liés à la centrale > Paramètres RPS > Réponse armée et Réponse désarmée sur 0 (désactivé).

Emplacement dans le menu RPS
Paramètres liés à la centrale > Téléphone et paramètres du téléphone > Compatibilité RTC

4.2 Communicateur Ethernet (IP) embarqué

4.2.1 Mode IPv6

Valeur par défaut : Non
Choix :
– Oui : utiliser le mode IPv6 (Internet Protocol version 6) pour les communications IP
– Non : utiliser le mode IPv4 (Internet Protocol version 4) pour les communications IP
Lorsque IPv6 activé est défini sur Oui, définissez DHCP/IP automatique activé sur Oui.

Lorsque IPv6 activé est défini sur Non, les paramètres IPv6 sont en grisé (inaccessibles).
Lorsque IPv6 activé est défini sur Oui, les paramètres IPv4 sont en grisé (inaccessibles).

Emplacements dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Mode IPv6,

4.2.2 DHCP IPv6

Valeur par défaut : Activé (Oui)

Choix :

- Activé (Oui) : DHCP définit automatiquement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP. AutoIP permet l'affectation d'adresses IP dynamiques aux dispositifs au démarrage.
- Désactivé (Non) : définissez ce paramètre sur Désactivé s'il n'y a aucun service DHCP. Définissez manuellement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP.

DHCP nécessite un serveur DHCP.

Emplacements dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > DHCP IPv6

4.2.3 DHCP IPv4/IP automatique activé

Valeur par défaut : Activé (Oui)

Choix :

- Activé (Oui) : DHCP définit automatiquement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP. AutoIP permet l'affectation d'adresses IP dynamiques aux dispositifs au démarrage.
- Désactivé (Non) : définissez ce paramètre sur Désactivé s'il n'y a aucun service DHCP. Définissez manuellement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP.

DHCP nécessite un serveur DHCP.
Lorsque ce paramètre est défini sur Oui, l'adresse IPv4, le masque de sous-réseau IPv4 et la passerelle par défaut IPv4 sont grisés. Vous ne pouvez pas les modifier.
Lorsque le paramètre Mode IPv6 est défini sur Oui, ce paramètre est grisé (inaccessible).

Emplacements dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > DHCP IPv4/IP automatique activé

4.2.4 Adresse IPv4

Valeur par défaut : 0.0.0.0

Choix : 0.0.0.0 à 255.255.255.255

Si DHCP IPv4/IP automatique activé est défini sur Oui, ce paramètre est grisé (inaccessible).
Si DHCP IPv4/IP automatique activé est défini sur Non, entrez ici l'adresse IPv4.

Pour obtenir de plus amples informations

Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Adresse IPv4

4.2.5 Masque de sous-réseau IPv4

Valeur par défaut : 255.255.255.0

Choix : 0.0.0.0 à 255.255.255.255

Si DHCP IPv4/IP automatique activé est défini sur Oui, ce paramètre est grisé (inaccessible).

Si DHCP IPv4/IP automatique activé est défini sur Non, entrez ici le masque de sous-réseau IPv4.
La centrale utilise le masque de sous-réseau pour identifier de manière plus efficace le réseau et les éléments de nœud de l'adresse.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303
Emplacements dans le menu RPS
Paramètres liés à la centrale > Communicateur Ethernet embarqué > Masque de sous-réseau IPv4

4.2.6 Passerelle par défaut IPv4

Valeur par défaut : 0.0.0.0
Choix : 0.0.0.0 à 255.255.255.255
Si DHCP IPv4/IP automatique activé est défini sur Oui, ce paramètre est grisé (inaccessible).
Si DHCP IPv4/IP automatique activé est défini sur Non, entrez ici l'adresse de passerelle par défaut.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303
Emplacements dans le menu RPS
Paramètres liés à la centrale > Communicateur Ethernet embarqué > Passerelle par défaut IPv4

4.2.7 Adresse IP du serveur DNS IPv4

Valeur par défaut : 0.0.0.0
Choix : 0.0.0.0 à 255.255.255.255
Un serveur de noms de domaine (DNS pour Domain Name Server) utilise les noms de domaine interne ou noms d'hôte pour fournir les adresses IP correspondantes. En mode DHCP, le DNS par défaut du serveur est utilisé. Pour utiliser un serveur DNS personnalisé en mode DHCP, saisissez ici l'adresse IP du serveur DNS personnalisé.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303
Emplacements dans le menu RPS
Paramètres liés à la centrale > Communicateur Ethernet embarqué > Autre adresse IP du serveur DNS IPv4

4.2.8 Autre adresse IP du serveur DNS IPv6

Valeur par défaut :
Choix : 0000:0000:0000:0000:0000:0000:0000:0000 à
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Ce paramètre définit l'adresse de serveur DNS IPv6 pour le mode IP statique.
Lorsque cette adresse est définie par le service DHCP, ne la modifiez pas.
Un serveur de noms de domaine (DNS pour Domain Name Server) utilise les noms de domaine interne ou noms d'hôte pour fournir les adresses IP correspondantes. En mode DHCP, le DNS par défaut du serveur est utilisé. Pour utiliser un serveur DNS personnalisé en mode DHCP, modifiez le paramètre sur l'adresse IP du serveur DNS personnalisé.
Cette adresse de serveur DNS IPv6 est la seule adresse IPv6 saisie sous la forme de nombres.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303
Emplacements dans le menu RPS
Paramètres liés à la centrale > Communicateur Ethernet embarqué > Adresse IP du serveur DNS IPv6

4.2.9 UPnP (Universal Plug and Play) activé

Valeur par défaut : Oui
Choix :
Oui (Activé) : utiliser UPnP pour ouvrir un programme d'acheminement de port pour les connexions RPS et RSC (Contrôle de sécurité à distance) entrantes
Non (Désactivé) : ne pas utiliser UPnP
Le paramètre UPnP n'a aucun effet sur la génération de rapport d'événements IP pour un récepteur du centre de télésurveillance.
Lorsque ce paramètre est défini sur Oui, la centrale envoie une demande au routeur des locaux afin d'ouvrir un programme d'acheminement de port. L'acheminement de port autorise les connexions RPS et RSC (Contrôle de sécurité à distance) entrantes.

Remarque!
UPnP requiert une adresse IP/un nom d'hôte et un port de centrale
Sous l'onglet Données de centrale – Vue, Réseau, assurez-vous que les paramètres Adresse IP/Nom d'hôte et Port centrale sont renseignés.

Emplacements dans le menu RPS
Paramètres liés à la centrale > Communicateur Ethernet embarqué > UPnP (Universal Plug and Play) activé

4.2.10 Délai du cache ARP (secondes)

Valeur par défaut : 600
Choix : 1 à 600 (secondes)
Ce paramètre spécifie le délai des entrées du cache ARP.
Emplacements dans le menu RPS
Paramètres liés à la centrale > Communicateur Ethernet embarqué > Délai du cache ARP

4.2.11 Nom d'hôte du module

Valeur par défaut : Vide
Choix : 1-63 caractères, a-z, a-z, 0-9, tiret (-) au format 0000.0000.0000.0000. Notez que le nom d'hôte du module ne peut pas commencer ou finir par un tiret (-).
Le nom d'hôte identifie le communicateur IP (module intégré ou SDI2) sur le réseau. Laissez ce paramètre vide pour utiliser le nom d'hôte par défaut défini en usine.

Remarque!
Laissez ce paramètre vide si vous voulez utiliser le nom d'hôte par défaut défini en usine
Le nom d'hôte par défaut défini en usine commence par la lettre B, suivie des six derniers chiffres de l'adresse MAC des modules.
Utilisez les diagnostics RPS ou le programme d'installation (clavier) pour afficher le nom d'hôte.

Utilisez le nom d'hôte sur le réseau local en utilisant DHCP. Pour utiliser le nom d'hôte en externe, vous devez entrer le nom d'hôte dans le serveur DNS.

Vous pouvez utiliser le nom d'hôte pour vous connecter à la centrale avec RPS ou RSC (Contrôle de sécurité à distance), ou pour la configuration Web du module et les diagnostics.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Nom d'hôte du module

4.2.12 Numéro de port TCP/UDP

Valeur par défaut : 7700

Choix : 0 - 65535

Pour les communications dotées de RPS, de l'automatisation ou du Contrôle de sécurité à distance (RSC) dans les installations standard, conservez le port TCP/UDP par défaut

Remarque!

Limitation du trafic indésirable, sélection d'un numéro de port supérieur à 1023

Si vous choisissez de modifier le numéro de port par défaut, sélectionnez un numéro de port supérieur à 1023 afin de réduire le trafic réseau indésirable.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Numéro de port TCP/UDP

4.2.13 Durée de conservation TCP

Valeur par défaut : 4 minutes

Choix : Désactivé - 8 heures

La durée entre les messages d'activité TCP peut être définie en minutes ou en heures. Les messages d'activité permettent de s'assurer qu'une connexion demeure active.

Emplacements dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Durée de conservation TCP

4.2.14 Adresse de test IPv4

Valeur par défaut : 8.8.8.8

Choix : adresse IPv4 ou nom de domaine

La centrale effectue un ping de l'adresse de test IPv4 afin de vérifier que les paramètres de configuration réseau sont corrects et que le réseau est opérationnel.

L'adresse de test par défaut fonctionne pour la plupart des réseaux.

Pour obtenir de plus amples informations

Formats de l'adresse IP et du nom de domaine, page 303

Emplacements dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Adresse de test IPv4

4.2.15 Adresse de test IPv6

Valeur par défaut : 2001:4860:4860::8888

Choix : adresse IPv6 ou nom de domaine

La centrale effectue un ping de l'adresse de test IPv6 afin de vérifier que les paramètres de configuration réseau sont corrects et que le réseau est opérationnel.

L'adresse de test par défaut fonctionne pour la plupart des réseaux.

Pour obtenir de plus amples informations

Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Adresse de test IPv6.

4.2.16 Autre adresse IP du serveur DNS IPv4

Valeur par défaut : 0.0.0.0

Choix : 0.0.0.0 à 255.255.255.255

Si le transmetteur IP ne parvient pas à obtenir une adresse à partir du serveur principal, il essaie avec le serveur DNS secondaire. Saisissez l'adresse IP du serveur DNS IPv4 secondaire.

Pour obtenir de plus amples informations

Formats de l'adresse IP et du nom de domaine, page 303

Emplacements dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Autre adresse IP du serveur DNS IPv4

Adresse IP

4.2.17 Autre adresse IP du serveur DNS IPv6

Valeur par défaut :

Choix : 0000:0000:0000:0000:0000:0000:0000:0000 à FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Si le communicateur IP ne parvient pas à obtenir une adresse à partir du serveur principal, il essaie avec le serveur DNS secondaire. Saisissez l'adresse IP du serveur DNS IPv6 secondaire.

Pour obtenir de plus amples informations

Formats de l'adresse IP et du nom de domaine, page 303

Emplacements dans le menu RPS

Paramètres liés à la centrale > Communicateur Ethernet embarqué > Autre adresse IP du serveur DNS IPv6

4.3 Module enfichable cellulaire

4.3.1 SMS entrant

Valeur par défaut : Oui

Choix :

- Activé (Oui) - vous pouvez utiliser des messages de texte SMS entrants pour configurer le module.
- Désactivé (Non) - le module ne traite pas les messages de texte SMS entrants.

Remarque!

Informations de configuration importantes pour la communication cellulaire

Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Module enfichable cellulaire > Cellulaire SMSB450 entrant > SMS entrant

4.3.2 Durée de conservation de la session (minutes)

Valeur par défaut : 0

Choix : 0 (désactivé) à 1000 (minutes) (0 (disable) to 1000 (minutes))
Temps en minutes entre les messages d'activité. Les messages d'activité permettent de s'assurer qu'une connexion demeure active.
Modifiez uniquement la valeur par défaut pour les installations commerciales homologuées UL1610 haut niveau de sécurité.

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Module enfichable cellulaire > Durée de conservation de la session

4.3.3 Délai d'inactivité (minutes)

Valeur par défaut : 0
Choix : 0 (désactiver) à 1000 (minutes) (0 (disable) to 1000 (minutes))
– 0 (désactivé) (0 (disabled)) - la centrale ne surveille pas le trafic de données.
– 1 à 1 000 (1 to 1000) - délai sans trafic de données avant que la centrale ne mette fin à une session.

Modifiez uniquement la valeur par défaut pour les installations commerciales homologuées haute sécurité UL 1610 qui nécessitent une notification de signal faible.

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Module enfichable cellulaire > Délai d'inactivité

4.3.4 Délai de signalisation de signal de faible puissance (secondes)

Valeur par défaut : 0 (désactivé) (0 (disabled))
Choix : 0 (désactivé) (0 (disabled), 1 - 3600 (secondes) (1 - 3600 (seconds))
Durée de signal faible (LED rouge sur le transmetteur cellulaire) avant que la centrale ne déclenche un événement Signal faible cellulaire.
La centrale crée un événement Rétablissement de signal faible cellulaire lorsque l'intensité du signal est bonne (voyant LED vert sur le communicateur cellulaire) pour la durée que vous entrez au niveau de ce paramètre Délai de signalisation de signal de faible puissance (secondes).

Remarque!
Exigence UL
Pour répondre aux exigences de la norme UL, la valeur entrée pour ce paramètre ne doit pas dépasser 200 secondes.

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Module enfichable cellulaire > Délai de signalisation de signal de faible puissance

4.3.5 Délai de signalisation d'absence de tour (secondes)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : 0
Choix : 0 (désactivé) - 3600 (secondes) (0 (disabled) - 3600 (seconds))
Lorsque le module enfichable cellulaire ne détecte aucune tour pour les secondes définies par ce paramètre, la centrale enregistre un événement Absence de tour (No Towers) et un événement Pas d'adresse IP (No IP Address).
La centrale enregistre un événement Rétablissement cellulaire aucune tour disponible (Cellular No Tower Available Restoral) lorsque le module enfichable cellulaire détecte une ou plusieurs tours pendant les secondes définies par ce paramètre.
La centrale enregistre un événement Rétablissement Pas d'adresse IP (No IP Address restoral) lorsque le module cellulaire enfichable enregistre une ou plusieurs tours et reçoit une adresse IP dans les 60 secondes.

Remarque!
Lorsqu'une ou plusieurs tours sont disponibles, un délai de 60 secondes pour l'événement Pas d'adresse IP
Si le module enfichable cellulaire s'enregistre auprès d'une ou plusieurs tours, mais ne reçoit pas d'adresse IP dans les 60 secondes, la centrale crée un événement Pas d'adresse IP.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Module enfichable cellulaire > Délai de signalisation d'absence de tour

4.3.6 Longueur SMS sortant

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : 160
Choix : 0 (désactivé) à 3 600 (caractères)
Les fournisseurs cellulaires définissent la limite pour la longueur de message SMS à 160 caractères (par défaut). Les fournisseurs rejettent les messages SMS au-dessus de cette limite.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Module enfichable cellulaire > Longueur du SMS sortant

4.3.7 Adresse IP du serveur DNS IPv4

Valeur par défaut : 0.0.0.0

Choix : 0.0.0.0 à 255.255.255.255
Un serveur de noms de domaine (DNS pour Domain Name Server) utilise les noms de domaine interne ou noms d'hôte pour fournir les adresses IP correspondantes. En mode DHCP, le DNS par défaut du serveur est utilisé. Pour utiliser un serveur DNS personnalisé en mode DHCP, saisissez ici l'adresse IP du serveur DNS personnalisé.
Emplacement du menu RPS
Paramètres liés à la centrale (Panel Wide Parameters) > Modules enfichables cellulaires (Cellular Plug-In Modules) > Adresse IP du serveur DNS IPv4 (IPv4 DNS server IP address)

4.3.8 Autre adresse IP du serveur DNS IPv4

Valeur par défaut : 0.0.0.0
Choix : 0.0.0.0 à 255.255.255.255
Saisissez l'adresse IP du serveur DNS IPv4 secondaire.
Si le module enfichable cellulaire ne parvient pas à obtenir une adresse du serveur principal, l'autre serveur IPv4 spécifié dans ce paramètre est utilisé.
Emplacement du menu RPS
Paramètres liés à la centrale (Panel Wide Parameters) > Modules enfichables cellulaires (Cellular Plug-In Modules) > Adresse IP de l'autre serveur DNS IPv4 (Alternate IPv4 DNS server IP address)

4.3.9 Adresse de test IPv4

Valeur par défaut : 8.8.8.8
Choix : adresse IPv4 ou nom de domaine
La centrale effectue un ping de l'adresse de test IPv4 afin de vérifier que les paramètres de configuration réseau sont corrects et que le réseau est opérationnel.
L'adresse de test par défaut fonctionne pour la plupart des réseaux.
Emplacement du menu RPS
Paramètres liés à la centrale (Panel Wide Parameters) > Modules enfichables cellulaires (Cellular Plug-In Modules) > Adresse de test IPv4 (IPv4 Test Address)

4.3.10 Nom du point d'accès réseau (APN)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : eaaa.bssd.vzwentp
Choix : 0-9, A-Z, a-z, **-** , **:** , **.** (jusqu'à 60 caractères)
Pour modifier le nom du point d'accès (APN) défini sur la valeur par défaut, entrez jusqu'à 60 caractères. Le champ est sensible à la casse.

Firmware de centrale version 3.07 ou ultérieure
Avec le firmware de centrale version 3.07 ou ultérieure, lorsque le paramètre APN est vide, la centrale utilise une liste interne des valeurs de Network Access Point Name (APN). Lorsqu'un transmetteur cellulaire enfichable B442, B443 ou B444 est branché, la liste interne comprend :
– Iotst.aer.net
– gne
– wyless.apn (valide uniquement pour les versions antérieures à RPS 6.07)
– wyless.com.attz

– bosch.vzwentp

Lorsqu'un transmetteur cellulaire enfichable B444-V est branché, la liste interne comprend :

– bssd.vzwentp

Lorsqu'un transmetteur cellulaire enfichable B444-A est branché, la liste interne comprend :

– bssd.attentp

Emplacement dans le menu RPS

Paramètres liés à la centrale > Module enfichable cellulaire > Nom du point d'accès réseau

4.3.11 Nom d'utilisateur du point d'accès réseau

Valeur par défaut : Blanc

Choix : Caractères ASCII (jusqu'à 30)

Entrez jusqu'à 30 caractères ASCII pour le nom d'utilisateur du Point d'accès réseau.
Le nom d'utilisateur est sensible à la casse.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Module enfichable cellulaire > Nom d'utilisateur du point d'accès réseau

4.3.12 Mot de passe du point d'accès réseau

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : Blanc

Choix : Caractères ASCII (jusqu'à 30 caractères)

Entrez jusqu'à 30 caractères ASCII pour le mot de passe de Point d'accès réseau.
Le mot de passe est sensible à la casse.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Module enfichable cellulaire > Mot de passe du point d'accès réseau

4.3.13 PIN SIM

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : Vide

Choix : 0-9 (minimum 4 chiffres, minimum 8 chiffres)

Utilisez ce paramètre uniquement lorsqu'un code PIN est nécessaire pour les cartes ICCID.
Si aucun code PIN SIM n'est nécessaire, laissez ce champ à blanc.
Le code PIN SIM s'affiche sous forme d'astérisques (********) lors de la saisie. Si vous saisissez un code PIN SIM non valide, un événement est enregistré. Un rapport est envoyé uniquement si la fonction de rapport est définie.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Module enfichable cellulaire > PIN SIM

4.4 Cloud Remote Connect

4.4.1 Cloud Remote Connect (Ethernet)

Valeur par défaut : Activé
Choix : : Activé, Désactivé
Utilisez ce paramètre pour activer le Service Bosch basé sur le Cloud, Remote Connect, pour la communication via une connexion Ethernet.

Remarque!
Inscription aux services d'installation Bosch, Remote Connect, requise
Pour pouvoir utiliser Remote Connect pour les connexions RPS ou RSC, vous devez contacter votre support technique Bosch régional pour configurer ou obtenir les détails de votre compte.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Connexion à distance au Cloud > Cloud Remote Connect (Ethernet)

4.4.2 Cloud Remote Connect (Cellulaire)

Valeur par défaut : Désactivé
Choix : : Activé, Désactivé
Utilisez ce paramètre pour activer le Service Bosch basé sur le Cloud, Remote Connect, pour la communication via une connexion cellulaire.

Remarque!
Inscription aux services d'installation Bosch, Remote Connect, requise
Pour pouvoir utiliser Remote Connect pour les connexions RPS ou RSC, vous devez contacter votre support technique Bosch régional pour configurer ou obtenir les détails de votre compte.

Emplacement du menu RPS
Paramètres liés à la centrale > Connexion à distance au Cloud > Connexion à distance au Cloud via cellulaire

4.5 Caméras IP

Le B6512 prend en charge les caméras 1 à 6.
Les caméras IP Bosch sont intégrées aux centrales en configurant les détails de connexion IP en plus d'aligner les points de centrale et les sorties de centrale spécifiques avec chaque caméra IP.
Les opérateurs RPS ont la possibilité d'importer les détails de connexion IP à l'aide d'un fichier d'exportation créé à partir de l'application Bosch Configuration Manager.

4.5.1 Nom de la caméra (première langue)

Valeur par défaut : n° de la caméra
Choix : 0 à 32 caractères (jeu de caractères Latin-1 8 bits (ISO/IEC 8859-1))
Entrez un nom de caméra IP Bosch dans la première langue de la centrale.
Définissez les première et seconde langues dans la fenêtre Données de centrale - Vue. Voir Données de centrale - Vue > Onglet Informations sur la centrale > Informations supplémentaires.
Les langues possibles sont : Anglais, Espagnol, Français et Portugais.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Caméras IP > Nom de la caméra

4.5.2 Nom de la caméra (deuxième langue)

Valeur par défaut : Vide
Choix : 0 à 32 caractères (jeu de caractères Latin-1 8 bits (ISO/IEC 8859-1))
Entrez un nom de caméra IP Bosch dans la seconde langue de la centrale.
Définissez les première et seconde langues dans la fenêtre Données de centrale - Vue. Voir Données de centrale - Vue > Onglet Informations sur la centrale > Informations supplémentaires.
Les langues possibles sont : Anglais, Espagnol, Français et Portugais.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Caméras IP > Nom de la caméra (deuxième langue)

4.5.3 URL ou adresse IP

Valeur par défaut : Vide
Choix : 0 à 128 caractères ASCII
Ce paramètre définit l'URL ou l'adresse IP de la caméra IP Bosch.
La centrale ou l'application RSC utilisent l'URL ou l'adresse IP de la caméra pour communiquer avec la caméra sur un réseau.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Caméras IP > URL ou adresse IP

4.5.4 Entrées-sorties de caméra

Grâce à cette option, les opérateurs RPS peuvent interagir avec une vue consolidée des intégrations de caméras IP Bosch, y compris les affectations de point de centrale et les affectations de sortie de centrale. La fenêtre fournit une carte visuelle qui permet de faciliter la revue et l'affectation des points de centrale et des sorties de centrale disponibles pour chaque caméra IP individuelle.
Les centrales agissent sur la fonction Video Analytics de la caméra IP Bosch en enregistrant et en recevant les informations provenant des alarmes de tâches de caméra IP (1-8) et des entrées filaires (1, 2).
Les centrales permettent aux caméras IP Bosch de fonctionner à l'aide des alarmes de caméra IP (1-4).
Utilisez la fenêtre pour :

- afficher et attribuer les points disponibles pour la caméra IP. La source du point en cours indique la programmation actuelle pour chaque point disponible avec la caméra IP spécifique. L'affectation à la caméra IP affecte la source de point du ou des points de centrale correspondants. Il s'agit du même paramétrage défini à l'aide de Points > Affectation de point > Source de point > Caméra IP.
- afficher et affecter la source de sortie disponible pour la caméra IP. La source de sortie en cours indique la programmation actuelle pour chaque sortie disponible avec la caméra IP spécifique. L'affectation à la caméra IP affecte la source de sortie à la caméra IP pour la ou les sorties de centrale correspondantes. Il s'agit du même paramétrage défini à l'aide de Sorties>Affectations de sortie>Source de sortie>Caméra IP.

Par exemple, une caméra (Caméra 1) configurée sur les points physiques 10-19 peut utiliser la sortie 11-14. Une autre caméra (Caméra 32) configurée sur le point 320-329 peut utiliser la sortie 321-324.

– **Ouvrir l'URL de la caméra IP Bosch** -sélectionnez ce bouton pour que le logiciel RPS utilise les détails de connexion de la caméra IP et ouvre un navigateur sur la page Web individuelle de la caméra.
– **Ouvrir Bosch Configuration Manager** -sélectionnez ce bouton pour que RPS ouvre l'application Bosch Configuration Manager.

Pour affecter automatiquement des points et des sorties à une caméra IP :

1. Sélectionnez une caméra à configurer et sélectionnez le paramètre Entrée-Sorties de la caméra.
2. Double-cliquez sur **Tâches/Alarmes**.
3. Dans le tableau Communication caméra vers centrale, sélectionnez Affecter à la caméra IP pour affecter un point disponible à la caméra.
4. Dans le tableau Communication centrale vers caméra, sélectionnez une source de sortie disponible pour la caméra.
5. Cliquez sur **OK**.

Accédez aux affectations de point et aux affectations de sortie pour afficher les résultats de l'affectation.

Emplacement du menu RPS

Paramètres liés à la centrale > Caméras IP > Entrées-Sorties de la caméra

4.6 Caméras connectées de Bosch

Produits

– B6512 avec communicateur IP intégré
– Toutes les caméras IP Bosch

Implémentation

Après avoir établi que chaque caméra IP est disponible pour les opérations réseau, vous pouvez configurer les centrales pour intégrer les caméras IP Bosch en tant qu'entrées et/ou sorties de centrale.

Conditions ambiantes

Installez les centrales compatibles et les caméras IP Bosch sur le même réseau (LAN).

Configuration de la centrale

Configurez la centrale avec l'adresse IP de chaque caméra. Les paramètres Nº de port RCP+, Mot de passe du service et Durée de supervision permettent de configurer la communication et la supervision du réseau avec des caméras IP Bosch connectées.

Autre configuration de centrale pour l'intégration des caméras IP Bosch

Paramètre Source de point « Caméra IP » (*Source, page 200*)
Paramètre Source de sortie « Caméra IP » (*Source de sortie, page 155*)

4.6.1 Nº de port RCP+

Valeur par défaut : 1756
Choix : 0 à 65535

Ce paramètre définit le numéro de port surveillé par une caméra IP Bosch pour le protocole RCP+.

Ne modifiez la valeur par défaut, 1756, que si une caméra IP est configurée pour surveiller un autre port.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Caméras IP > Caméras connectées Bosch > Nº de port RCP+

4.6.2 Mot de passe du service

Valeur par défaut : Vide

Choix : vide (désactivé), 1 à 32 caractères

Saisissez le mot de passe nécessaire pour accéder aux données de la caméra IP Bosch. Le mot de passe est sensible à la casse.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Caméras IP > Caméras connectées Bosch > Mot de passe du service

4.6.3 Période de supervision

Valeur par défaut : 0 (désactivé)

Choix : 0 (désactivé), 1 - 10 (minutes)

Durée pendant laquelle une caméra IP Bosch doit être manquante avant que la centrale crée un événement de caméra manquante.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Caméras IP > Caméras connectées Bosch > Durée de supervision

4.7 Vidéo en temps réel

Produits

- B6512 avec communicateur IP intégré
- Toutes les caméras IP Bosch
- Application mobile RSC (Remote Security Control)
- Application mobile BSM (Bosch Security Manager)

Applications

La vidéo en temps réel permet aux utilisateurs de voir les vidéos des caméras IP associées lorsqu'elles sont connectées et autorisées au moyen d'applications mobiles Bosch.

Implémentation

La vidéo en temps réel peut être configurée pour Bosch ou d'autres caméras IP qui prennent en charge l'accès aux images vidéo en temps réel par le biais d'un accès authentifié HTTP ou HTTPs. Lors de la mise en réseau de chaque caméra IP, assurez-vous que les détails de paramètre réseau permettent une authentification de base lorsque l'utilisation de HTTP est activée.

Configuration de la centrale

Les applications mobiles RSC et Bosch utiliseront les paramètres N° de port, Protocole HTTPs ?, Nom d'utilisateur et Mot de passe pour accéder aux images vidéo des caméras IP.

Remarque!

Authentification de base et HTTP

L'utilisateur et le mot de passe de l'affichage en temps réel RPS peuvent ne pas fonctionner tant que la caméra n'est pas configurée (autrement que dans la configuration RPS) pour permettre une authentification de base pour les connexions HTTP. Une fois activée, l'utilisateur et le mot de passe de l'affichage en temps réel configurés pour RPS seront utilisés par les applications mobiles Bosch pour accéder à la vidéo de manière sécurisée.

Programmation RPS pour les caméras IP

La configuration recommandée permet aux utilisateurs de l'application Bosch Mobile d'utiliser l'affichage en temps réel de la caméra IP (vidéo) en toute sécurité :

- URL ou adresse IP : <correspondent aux paramètres réels de la caméra IP>
- Temps réel (vidéo) > n° port : <correspondent aux paramètres de la caméra IP>
- Chaque caméra IP avec un port unique (p. ex. caméra 2 ; port n° 10042, caméra 3 ; port n° 10043)
- Temps réel (vidéo) utilise le protocole HTTPs ? : Oui
- Nom d'utilisateur temps réel (vidéo) : <correspond aux paramètres de la caméra IP>
- Mot de passe temps réel (vidéo) : <correspond aux paramètres de la caméra IP>

4.7.1 Nº de port

Valeur par défaut : 80

Choix : 0 à 65535

Entrez le numéro de port utilisé par l'application RSC (Contrôle de sécurité à distance) pour les communications IP et la vidéo en temps réel avec la caméra.

Lorsque l'URL du visionneur en temps réel est liée à un routeur, configurez ce dernier avec le numéro de port que vous entrez ici.

Lorsque vous utilisez HTTPS, définissez ce numéro de port sur 443.

Le B6512 prend en charge les caméras 1 à 6.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Caméras IP >Vidéo en direct > Nº de port

4.7.2 Utiliser HTTPS ?

Valeur par défaut : Non

Choix :

Oui : activer HTTPS (chiffre les données pour sécuriser les communications entre la caméra IP Bosch et RSC).

Non : désactiver HTTPS

Définissez ce paramètre sur la valeur Oui si le visionneur requiert HTTPS.

Lorsque HTTPS est défini sur Oui, définissez Paramètres liés à la centrale > Caméras IP > Vidéo en direct > Nº de port sur 443

Le B6512 prend en charge les caméras 1 à 6.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Caméras IP > Vidéo en direct > Utiliser HTTPS ?

4.7.3 Nom d'utilisateur

Valeur par défaut : direct

Choix : A-Z, a-z, 0-9, jusqu'à 32 caractères.

Entrez le nom d'utilisateur tel qu'il est entré dans la caméra. L'application RSC utilise le nom d'utilisateur et le mot de passe pour afficher la vidéo depuis la caméra.

Le B6512 prend en charge les caméras 1 à 6.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Caméras IP > Vidéo en direct > Nom d'utilisateur

4.7.4 Mot de passe

Valeur par défaut : Vide

Choix : A-Z, a-z, 0-9, jusqu'à 32 caractères.

Saisissez le mot de passe tel qu'il est entré dans la caméra. L'application RSC utilise le nom d'utilisateur et le mot de passe pour afficher la vidéo depuis la caméra.

Le B6512 prend en charge les caméras 1 à 6.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Caméras IP > Vidéo en direct > Mot de passe

4.8 Vue d'ensemble de la génération de rapports

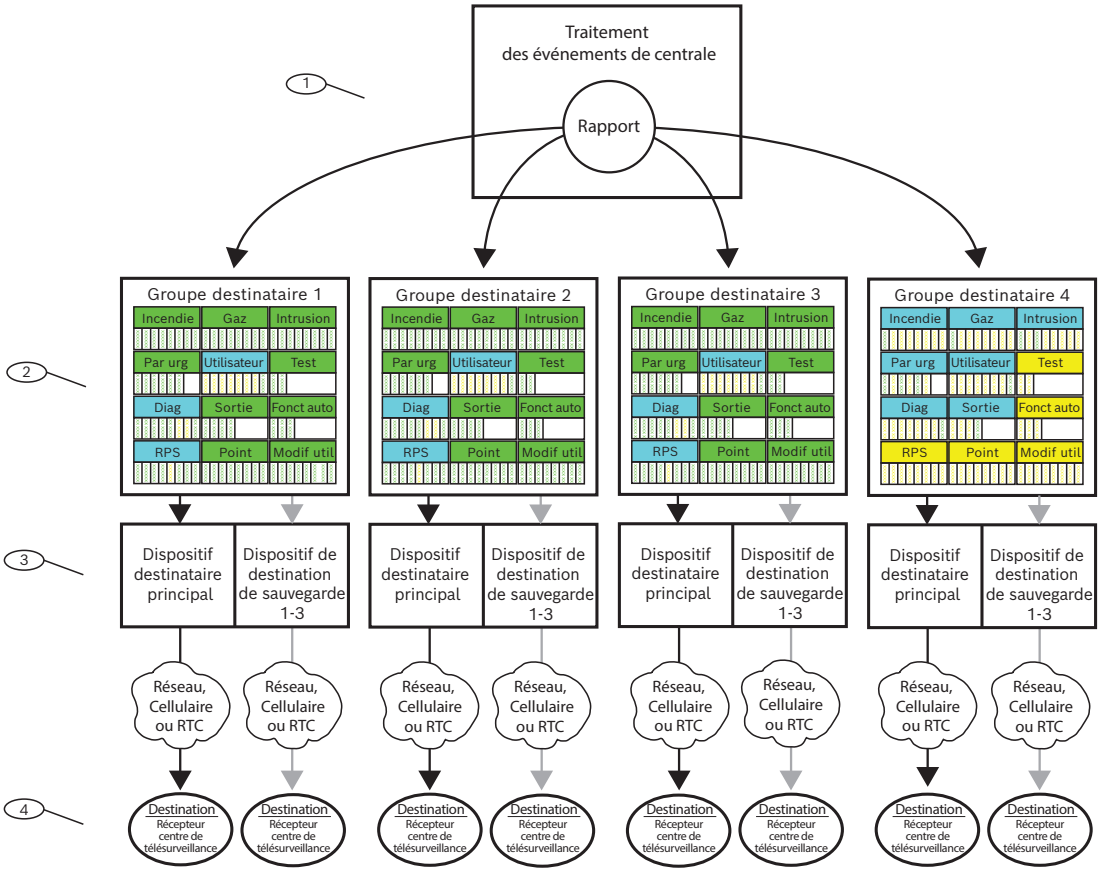


Figure 4.1:

1 - Les rapports commencent avec des événements

La centrale surveille ses points, ses modules, ses claviers et son alimentation (secteur et batterie) afin de détecter des conditions anormales. Lorsque la centrale détecte une condition anormale (ou un rétablissement à partir d'une condition anormale), elle génère un événement. La centrale ajoute des événements dans l'historique et peut envoyer des événements en tant que rapports au récepteur d'un centre de télésurveillance ou à des utilisateurs sous la forme de notifications personnelles.

Lorsque la centrale comporte des rapports à envoyer, elle les trie dans des groupes destinataires (1 à 4). Chaque groupe destinataire dispose de son propre communicateur, avec un dispositif de destination principal et jusqu'à 3 dispositifs de destination de sauvegarde, pour l'envoi des rapports du groupe destinataire au récepteur d'un centre de télésurveillance.

2 - Paramètres de routage des rapports

Utilisez le paramètre *Routage des rapports, page 52* pour configurer les quatre groupes destinataires (1 à 4). Les paramètres sous l'en-tête Routage des rapports permettent de lier des rapports aux groupes destinataires par catégorie (tous les Rapports d'incendie ou tous les Rapports d'intrusion, par exemple) ou de manière individuelle (Alarme incendie, par exemple).

Vous pouvez lier des rapports à un ou à plusieurs groupes destinataires.

3 - Paramètres du communicateur

Les paramètres au-dessous de l'en-tête *Communicateur, vue d'ensemble, page 66* permettent de lier un dispositif de destination principal et jusqu'à 3 dispositifs de destination de sauvegarde à chaque groupe destinataire. La centrale utilise en premier le dispositif de destination principal du groupe destinataire pour l'envoi de rapports. Si le dispositif de destination principal ne parvient pas à envoyer le rapport, la centrale crée un événement d'échec de communication et bascule sur le premier dispositif de destination de sauvegarde, et s'il est configuré, sur le deuxième dispositif de destination de sauvegarde, et enfin sur le troisième dispositif de destination de sauvegarde.

La centrale accepte jusqu'à dix tentatives de communication, avec basculement entre les dispositifs de destination principaux et de sauvegarde, pour envoyer des rapports à partir d'un Groupe de destinataires en fonction d'un ensemble de combinaisons de tentatives affichées dans le tableau de la rubrique d'aide *Communicateur, vue d'ensemble, page 66*. En cas d'échec au bout de 10 tentatives, un événement Échec de comm. est créé.

4 - Destinations

La centrale envoie des rapports depuis chaque groupe destinataire à l'aide de leurs dispositifs de destination principaux et de sauvegarde configurés pour le dispositif.

Pour configurer les destinations IP intégrées, voir *Communicateur Ethernet (IP) embarqué, page 34* et *Communication améliorée, page 71*.

Pour configurer les destinations IP cellulaires enfichables, voir *Module enfichable cellulaire, page 39* et *Communication améliorée, page 71*. Voir *Configuration du service Cellulaire, page 300* pour plus d'informations.

Pour configurer les destinations Téléphone enfichable, voir *Téléphone et paramètres du téléphone, page 31*.

Pour configurer les destinations Adresse SDI2, voir *Transmetteur IP (B42x), page 282* ou *B450 Cellulaire, page 288*, et *Communication améliorée, page 71*.

Priorité de groupe destinataire

Le groupe destinataire 1 a la priorité la plus élevée. Le groupe destinataire 4 a la priorité la plus faible. Lorsqu'il y a des rapports dans plusieurs groupes destinataires pour un envoi simultané, la centrale envoie d'abord le rapport du groupe avec la priorité la plus élevée. Par exemple, s'il y a des rapports dans les groupes destinataires 2 et 3, la centrale envoie d'abord le rapport du groupe destinataire 2.

Priorité au sein d'un groupe destinataire

Au sein d'un groupe destinataire, les rapports à envoyer doivent être hiérarchisés comme indiqué. La centrale envoie d'abord le rapport avec la priorité la plus élevée. 1 représente la priorité la plus élevée.

1. **Rapports diagnostiques** : Réinitialisation surveillance, Redémarrer.
   Rapports RPS : Réinitialisation à distance.
2. **Rapports d'incendie** : Alarme incendie.
3. **Rapports de gaz** : Alarme gaz.

4. **Rapports d'urgence personnelle** : Alarme médicale, Alarme silencieuse/effraction, Alarme de panique, Contrainte.
5. **Rapports d'intrusion** : Rapport d'alarme.
6. **Rapports d'incendie** : Annulation incendie.
   Rapports de gaz : Annulation Gaz.
   Rapports d'intrusion : Annulation d'alarme non incendie.
   Rapports diagnostiques : Échec dispositif SDI2, Défaut paramètre checksum, Échec de la ligne téléphonique, Défaut secteur, Batterie manquante, Batterie faible, Rétablissement batterie, Échec de comm. destinataire, Rétablissement de comm. destinataire.
7. **Rapports d'incendie** : Rétablissement incendie (après Alarme), Incendie manquant, Défaut incendie, Supervision incendie, Rétablissement incendie (après Défaut), Supervision incendie manquante, Rétablissement supervision incendie.
   Rapports de gaz : Rétablissement gaz après alarme, Gaz manquant, Défaut gaz, Supervision gaz, Rétablissement gaz après défaut, Supervision gaz manquante, Supervision gaz.
   Rapports d'intrusion : Supervision non incendie.
   Rapports d'urgence personnelle : Rétablissement d'alarme médicale, Rétablissement Alarme silencieuse/intrusion, Rétablissement d'alarme panique.
8. **Rapports d'intrusion** : Rétablissement intrusion (après défaut), Alarme manquante, Rapport de défaut, Défaut manquant, Défaut de point bus, Rétablissement de point bus, Rétablissement d'alarme, Supervision manquante, Événement non vérifié.
9. **Rapports d'utilisateur** : Point forcé, Armement forcé, Fermeture forcée, Fermeture instantanée forcée, Fermeture forcée avant fin de temporisation.
   Rapports diagnostiques : Service - Détecteur de fumée, Service - Rétablissement détecteur de fumée.
   Rapports de sortie : Réinitialisation des détecteurs, Définition sortie, Réinitialisation sortie.
   Rapports de fonction auto : RV exécuté, RV modifié, Échec d'exécution (RV).
   Rapports de point : Inhibition, Rétablissement inhibition.
   Rapports modification utilisateur : Niveau de modification.
10. **Rapports d'intrusion** : Auto-surveillance code utilisateur.
    Rapports d'utilisateur : Échec d'ouverture, Échec de fermeture, Étendre l'heure de fermeture, Rapport d'ouverture, Rapport de fermeture, Ouverture du point, Fermeture du point, Partielle Instantané, Partielle Temporisée.
    Rapports de test : Rapport de statut, Rapport de test.
    Rapports diagnostiques : Rétablissement dispositif SDI2, Rétablissement de la ligne téléphonique, Rétablissement secteur, Défaut checksum, Échec de réseau (et Rétablissement), Condition réseau, Interférence radio (et Rétablissement), Défaut d'équipement (et Rétablissement), Notification personnelle, défaut de communication (et Rétablissement).
    Rapports RPS : Capacité du journal d'événements, Saturation du journal d'événements, Paramètres modifiés, Accès RPS OK, Erreur d'accès RPS, Réinitialisation à distance, Accès programme OK, Erreur d'accès programme.
    Rapports de point : Début service, Fin service, Début détection incendie, Fin détection incendie, Début test de détection, Fin test de détection, Point supplémentaire, Batterie faible radio, Rétablissement batterie radio.
    Rapports de modification utilisateur : Date modifiée, Heure modifiée, Supprimer l'utilisateur, Modification du code utilisateur, Surveillance de partition, Télécommande

liée, Télécommande retirée, Niveau de modification.
Rapports d'accès : Accès octroyé, Accès refusé, Porte laissée ouverte, Cycle de porte, Porte déverrouillée, Porte sécurisée, Demande d'accès aux portes, Porte verrouillée.

4.9 Routage des rapports

Valeur par défaut :

Catégorie de rapport	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Rapports d'incendie, page 53	Oui	Oui	Oui	Personnalisé
Rapports de gaz, page 53	Oui	Oui	Oui	Personnalisé
Rapports d'intrusion, page 53	Oui	Oui	Oui	Personnalisé
Rapports d'urgence personnelle, page 54	Oui	Oui	Oui	Personnalisé
Rapports d'utilisateur, page 54	Personnalisé	Personnalisé	Personnalisé	Personnalisé
Rapports de test, page 54	Oui	Oui	Oui	Non
Rapports diagnostiques, page 54	Personnalisé	Personnalisé	Personnalisé	Personnalisé
Rapports de sortie, page 55	Oui	Oui	Oui	Personnalisé
Rapports de fonction auto, page 55	Oui	Oui	Oui	Non
Rapports RPS, page 55	Personnalisé	Personnalisé	Personnalisé	Non
Rapports de point, page 56	Oui	Oui	Oui	Non
Rapports de modification utilisateur, page 56	Oui	Oui	Oui	Non
Rapports d'accès, page 56	Oui	Oui	Oui	Oui
Rapports environnementaux, page 65	Oui	Oui	Oui	Personnalisé

Choix :

– Oui : attribuer tous les rapports de cette catégorie au groupe destinataire.
– Non : ne lier aucun rapport de cette catégorie au groupe destinataire.

Personnalisé : vous ne pouvez pas sélectionner Personnalisé. Personnalisé affiche une catégorie lorsque au moins l'un des rapports de la catégorie est configuré de manière individuelle.

Remarque!

Configuration des rapports individuels perdue lors du passage de Personnalisé à Oui ou Non

Lorsque Personnalisé s'affiche pour une catégorie de rapports, cela indique que tous les rapports ne sont pas définis de la même manière (sur Oui ou Non). Les rapports ont été définis individuellement.

Si vous définissez les rapports d'une catégorie Personnalisé sur Oui ou Non, la configuration des rapports individuels de la catégorie est perdue. Pour rélier individuellement des rapports d'une catégorie de rapport à un groupe destinataire, vous devez cliquer sur la catégorie de rapport dans l'arborescence de menu, *Rapports d'incendie, page 57*, par exemple.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports

Rapports d'incendie

Rapports de la catégorie Incendie :

- Alarme incendie
- Rétablissement incendie (après alarme)
- Incendie manquant
- Défaut incendie
- Supervision incendie
- Rétablissement incendie (après défaut)
- Annulation incendie
- Supervision incendie manquante
- Rétablissement supervision incendie

Pour lier individuellement des rapports de la catégorie Incendie à un groupe destinataire, cliquez sur *Rapports d'incendie, page 57* dans l'arborescence de menu.

Rapports de gaz

Rapports de la catégorie Gaz :

- Alarme gaz
- Rétablissement gaz après alarme
- Gaz manquant.
- Défaut gaz
- Supervision gaz
- Rétablissement gaz après défaut
- Annulation gaz
- Supervision gaz manquante
- Rétablissement supervision gaz

Pour lier individuellement des rapports de la catégorie Gaz à un groupe destinataire, cliquez sur *Rapports de gaz, page 58* dans l'arborescence de menu.

Rapports d'intrusion

Rapports de la catégorie Intrusion :

- Rapport d'alarme
- Rétablissement intrusion (après défaut)
- Contrainte
- Alarme manquante
- Auto-surveillance code utilisateur
- Rapport de défaut
- Défaut manquant

– Supervision non incendie
– Défaut de point bus
– Rétablissement de point bus
– Annulation non incendie
– Rétablissement d'alarme
– Supervision manquante
– Événement non vérifié

Pour lier individuellement des rapports de la catégorie Intrusion à un groupe destinataire, cliquez sur *Rapports d'intrusion, page 58* dans l'arborescence de menu.

Rapports d'urgence personnelle

Rapports de la catégorie Urgence personnelle :

– Alarme médicale
– Rétablissement d'alarme médicale (réservé pour un usage ultérieur)
– Alarme silencieuse/intrusion
– Rétablissement Alarme silencieuse/intrusion
– Alarme panique
– Rétablissement d'alarme panique (réservé pour un usage ultérieur)

Pour lier individuellement des rapports de la catégorie Urgence personnelle à un groupe destinataire, cliquez sur *Rapports d'urgence personnelle, page 59* dans l'arborescence de menu.

Rapports d'utilisateur

Rapports de la catégorie Utilisateur :

– Point forcé : signale un événement de point forcé.
– Ouverture du point : signale un événement de d'ouverture de point.
– Fermeture du point : signale un événement de fermeture de point.
– Armement forcé : signale que l'armement d'un point a été forcé.
– Échec d'ouverture : signale un événement d'échec d'ouverture.
– Échec de fermeture : signale un événement d'échec de fermeture.
– Étendre l'heure de fermeture : signale un événement d'extension de fermeture.
– Rapport d'ouverture : signale des événements d'ouverture.
– Fermeture forcée
– Rapport de fermeture
– Fermeture instantanée forcée
– Fermeture forcée avant fin de temporisation
– Partielle Instantané
– Partielle Temporisée

Pour lier individuellement des rapports de la catégorie Utilisateur à un groupe destinataire, cliquez sur *Rapports d'utilisateur, page 60* dans l'arborescence de menu.

Rapports de test

Rapports de la catégorie Test :

– Rapport de statut
– Rapport de test

Pour lier individuellement des rapports de la catégorie Test à un groupe destinataire, cliquez sur *Rapports de test, page 60* dans l'arborescence de menu.

Rapports diagnostiques

Rapports de la catégorie Diagnostic :

– Défaillance de dispositif SDI2
– Rétablissement dispositif SDI2

- Réinitialisation surveillance
- Défaut paramètre checksum
- Redémarrage
- Échec de la ligne téléphonique
- Rétablissement ligne téléphonique
- Défaut secteur
- Rétablissement secteur
- Batterie manquante
- Batterie faible
- Rétablissement de la batterie
- Échec de comm. destinataire
- Rétablissement de comm. destinataire
- Défaut checksum
- Échec de réseau
- Rétablissement de réseau
- Condition réseau
- Interférence radio
- Rétablissement d'interférence radio
- Défaut d'équipement
- Rétablissement de défaut d'équipement
- Service - Détecteur de fumée
- Service - Rétablissement détecteur de fumée
- Notification personnelle, défaut de communication
- Notification personnelle, rétablissement du défaut de communication

Pour lier individuellement des rapports de la catégorie Diagnostic à un groupe destinataire, cliquez sur *Rapports diagnostiques, page 61* dans l'arborescence de menu.

Rapports de sortie

Rapports de la catégorie Sortie :

- Réinitialisation capteur
- Définition de sortie
- Réinitialisation de sortie

Pour lier individuellement des rapports de la catégorie Sortie à un groupe destinataire, cliquez sur *Rapports de sortie, page 62* dans l'arborescence de menu.

Rapports de fonction auto

Rapports de la catégorie Fonction auto :

- RV exécuté
- RV modifié
- Échec d'exécution

Pour lier individuellement des rapport de la catégorie Fonction Auto à un groupe destinataire, cliquez sur *Rapports de fonction auto, page 62* dans l'arborescence de menu.

Rapports RPS

Rapports de la catégorie RPS :

- Capacité du journal d'événements
- Saturation du journal d'événements
- Paramètres modifiés
- Accès RPS OK
- Échec d'accès RPS
- Réinitialisation à distance
- Accès programme OK

– Échec d'accès programme

Pour lier individuellement des rapports de la catégorie RPS à un groupe destinataire, cliquez sur *Rapports RPS, page 63* dans l'arborescence de menu.

Rapports de point

Rapports de la catégorie Point :

– Début service
– Fin service
– Début détection incendie
– Fin détection incendie
– Début test de détection
– Fin test de détection
– Point supplémentaire
– Attribution d'un nom au point
– Batterie faible radio
– Rétablissement batterie faible radio
– Inhibition
– Rétablissement inhibition

Pour lier individuellement des rapports de la catégorie Point à un groupe destinataire, cliquez sur *Rapports de point, page 63* dans l'arborescence de menu.

Rapports de modification utilisateur

Rapports de la catégorie Modification utilisateur :

– Date modifiée
– Heure modifiée
– Supprimer l'utilisateur
– Modification de code utilisateur
– Surveillance de partition
– Carte/Télécommande liée
– Télécommande retirée
– Niveau de modification

Pour lier individuellement des rapports de la catégorie Modification utilisateur à un groupe destinataire, cliquez sur *Rapports de modification utilisateur, page 64* dans l'arborescence de menu.

Rapports d'accès

Rapports de la catégorie Accès :

– Accès octroyé
– Accès refusé
– Porte laissée ouverte
– Cycle de porte
– Porte déverrouillée
– Porte sécurisée
– Demande d'accès aux portes
– Porte verrouillée

Pour lier individuellement des rapports de la catégorie Accès à un groupe destinataire, cliquez sur *Rapports d'accès, page 65* dans l'arborescence de menu.

Remarque!

Exigence de la norme UL 985 relative aux unités d'alarme incendie de maison familiale
Lors de la configuration des paramètres de transmission par défaut, assurez-vous que les tests de la transmission sont réalisés tous les mois ou plus rapidement, et que l'échec de la communication (délai total créé par les paramètres de fréquence et le nombre de tentatives) est annoncé dans les 7 jours.

Rapports environnementaux
Rapports de la catégorie Caractéristiques environnementales :
- Alarme eau
- Rétablissement eau
- Alarme Temp élevée
- Rétablissement Temp élevée
- Alarme Temp faible
- Rétablissement Temp faible

Pour lier individuellement des rapports de la catégorie Caractéristiques environnementales à un groupe destinataire, cliquez sur *Rapports environnementaux, page 65* dans l'arborescence de menu.

4.9.1 Rapports d'incendie

Valeur par défaut :

Rapports d'incendie	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Alarme incendie	Oui	Oui	Oui	Oui
Rétablissement incendie (après alarme)	Oui	Oui	Oui	Non
Incendie manquant	Oui	Oui	Oui	Non
Défaut incendie	Oui	Oui	Oui	Non
Supervision incendie	Oui	Oui	Oui	Non
Rétablissement incendie (après défaut)	Oui	Oui	Oui	Non
Annulation incendie	Oui	Oui	Oui	Non
Supervision incendie manquante	Oui	Oui	Oui	Non
Rétablissement supervision incendie	Oui	Oui	Oui	Non

Choix :
- Oui : attribuer ce rapport au groupe destinataire.
- Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Routage des rapports > Rapports d'incendie.

4.9.2 Rapports de gaz

Valeur par défaut :

Rapports de gaz	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Alarme gaz	Oui	Oui	Oui	Oui
Rétablissement gaz (après alarme)	Oui	Oui	Oui	Non
Gaz manquant	Oui	Oui	Oui	Non
Défaut gaz	Oui	Oui	Oui	Non
Supervision gaz	Oui	Oui	Oui	Non
Rétablissement gaz après défaut	Oui	Oui	Oui	Non
Annulation gaz	Oui	Oui	Oui	Non
Supervision gaz manquante	Oui	Oui	Oui	Non
Rétablissement supervision gaz	Oui	Oui	Oui	Non

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports de gaz

4.9.3 Rapports d'intrusion

Valeur par défaut :

Rapports d'intrusion	Groupe de routage 1	Groupe de routage 2	Groupe de routage 3	Groupe destinataire 4
Rapport d'alarme	Oui	Oui	Oui	Oui
Rétablissement intrusion (après alarme)	Oui	Oui	Oui	Non
Sous contrainte	Oui	Oui	Oui	Oui
Alarme manquante	Oui	Oui	Oui	Non
Auto-surveillance code utilisateur *	Oui	Oui	Oui	Non
Rapport de défaut	Oui	Oui	Oui	Non
Défaut manquant	Oui	Oui	Oui	Non
Supervision non incendie	Oui	Oui	Oui	Non
Défaut de point bus	Oui	Oui	Oui	Non

Rapports d'intrusion	Groupe de routage 1	Groupe de routage 2	Groupe de routage 3	Groupe destinataire 4
Rétablissement de point bus	Oui	Oui	Oui	Non
Annulation non incendie	Oui	Oui	Oui	Non
Rétablissement d'alarme	Oui	Oui	Oui	Non
Supervision manquante	Oui	Oui	Oui	Non
Événement non vérifié	Oui	Oui	Oui	Non

Choix :
– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

***** Une centrale envoie un événement d'auto-surveillance de code utilisateur lorsqu'un utilisateur saisit de manière consécutive un code non valide 7 fois sur le clavier.
Pour les types de connexion Mode 2, tels que les RSC ou l'automatisation, une centrale envoie un événement d'auto-surveillance de code utilisateur lorsque l'utilisateur entre de manière consécutive 15 codes non valides.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Routage des rapports > Rapports d'intrusion.

4.9.4 Rapports d'urgence personnelle

Valeur par défaut :

Rapports d'urgence personnelle	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Alarme médicale	Oui	Oui	Oui	Oui
Rétablissement d'alarme médicale	Oui	Oui	Oui	Non
Alarme silencieuse/intrusion	Oui	Oui	Oui	Oui
Rétablissement Alarme silencieuse/intrusion	Oui	Oui	Oui	Non
Alarme panique	Oui	Oui	Oui	Oui
Rétablissement d'alarme panique	Oui	Oui	Oui	Non

Choix :
– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Routage des rapports > Rapports d'urgence personnelle.

4.9.5 Rapports d'utilisateur

Valeur par défaut :

Rapports d'utilisateur	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Point forcé	Oui	Oui	Oui	Non
Ouverture du point	Oui	Oui	Oui	Non
Fermeture du point	Oui	Oui	Oui	Non
Armement forcé	Oui	Oui	Oui	Non
Échec d'ouverture	Oui	Oui	Oui	Non
Échec de fermeture	Oui	Oui	Oui	Non
Étendre l'heure de fermeture	Oui	Oui	Oui	Non
Rapport d'ouverture	Non	Non	Non	Non
Fermeture forcée	Non	Non	Non	Non
Rapport de fermeture	Non	Non	Non	Non
Fermeture instantanée forcée	Non	Non	Non	Non
Fermeture forcée avant fin de temporisation	Non	Non	Non	Non
Partielle Instantané	Non	Non	Non	Non
Partielle Temporisée	Non	Non	Non	Non
Envoyer texte utilisateur	Oui	Oui	Oui	Oui

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports d'utilisateur.

4.9.6 Rapports de test

Valeur par défaut :

Rapports de test	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Rapport de statut	Oui	Oui	Oui	Non
Rapport de test	Oui	Oui	Oui	Non

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Routage des rapports > Rapports de test.

4.9.7 Rapports diagnostiques

Valeur par défaut :

Rapports diagnostiques	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Défaillance de dispositif SDI2	Oui	Oui	Oui	Non
Rétablissement dispositif SDI2	Oui	Oui	Oui	Non
Réinitialisation surveillance	Oui	Oui	Oui	Non
Défaut paramètre checksum	Oui	Oui	Oui	Non
Redémarrage	Oui	Oui	Oui	Non
Échec de la ligne téléphonique	Oui	Oui	Oui	Non
Rétablissement de la ligne téléphonique	Oui	Oui	Oui	Non
Défaut secteur	Oui	Oui	Oui	Non
Rétablissement secteur	Oui	Oui	Oui	Non
Batterie manquante	Oui	Oui	Oui	Non
Batterie faible	Oui	Oui	Oui	Non
Rétablissement de la batterie	Oui	Oui	Oui	Non
Échec de comm. destinataire	Oui	Oui	Oui	Non
Rétablissement de comm. destinataire	Oui	Oui	Oui	Non
Défaut checksum	Oui	Oui	Oui	Non
Échec de réseau	Non	Non	Non	Non
Rétablissement de réseau	Non	Non	Non	Non
Condition réseau	Non	Non	Non	Non
Interférence radio	Oui	Oui	Oui	Non
Rétablissement d'interférence radio	Oui	Oui	Oui	Non
Défaut d'équipement	Oui	Oui	Oui	Non
Rétablissement de défaut d'équipement	Oui	Oui	Oui	Non

Rapports diagnostiques	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Service - Détecteur de fumée	Oui	Oui	Oui	Non
Service - Rétablissement détecteur de fumée	Oui	Oui	Oui	Non
Notification personnelle, défaut de communication	Non	Non	Non	Non
Notification personnelle, rétablissement du défaut de communication	Non	Non	Non	Non
Envoyer la version du texte	Oui	Oui	Oui	Oui

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Activez les rapports Échec de comm. destinataire et Rétablissement de comm. destinataire dans un seul groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports diagnostiques.

4.9.8 Rapports de sortie

Valeur par défaut :

Rapports de sortie	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Réinitialisation capteur	Oui	Oui	Oui	Non
Définition de sortie	Oui	Oui	Oui	Non
Réinitialisation de sortie	Oui	Oui	Oui	Non
Envoyer le texte du nom de sortie	Oui	Oui	Oui	Oui

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports de sortie

4.9.9 Rapports de fonction auto

Valeur par défaut :

Rapports de fonction auto	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
RV exécuté	Oui	Oui	Oui	Non

Rapports de fonction auto	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
RV modifié	Oui	Oui	Oui	Non
Échec d'exécution	Oui	Oui	Oui	Non

Choix :
- Oui : attribuer ce rapport au groupe destinataire.
- Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Routage des rapports > Rapports de fonction auto.

4.9.10 Rapports RPS

Valeur par défaut :

Rapports RPS	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Capacité du journal d'événements	Oui	Oui	Oui	Non
Saturation du journal d'événements	Oui	Oui	Oui	Non
Paramètres modifiés	Oui	Oui	Oui	Non
Accès RPS OK	Oui	Oui	Oui	Non
Échec d'accès RPS	Non	Non	Non	Non
Réinitialisation à distance	Oui	Oui	Oui	Non
Accès programme OK	Oui	Oui	Oui	Non
Échec d'accès programme	Oui	Oui	Oui	Non

Choix :
- Oui : attribuer ce rapport au groupe destinataire.
- Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Routage des rapports > Rapports RPS.

4.9.11 Rapports de point

Valeur par défaut :

Rapports de point	Groupe de routage 1	Groupe de routage 2	Groupe de routage 3	Groupe destinataire 4
Début service	Oui	Oui	Oui	Non
Fin service	Oui	Oui	Oui	Non
Début détection incendie	Oui	Oui	Oui	Non
Fin détection incendie	Oui	Oui	Oui	Non

Rapports de point	Groupe de routage 1	Groupe de routage 2	Groupe de routage 3	Groupe destinataire 4
Début test de détection	Oui	Oui	Oui	Non
Fin test de détection	Oui	Oui	Oui	Non
Point supplémentaire	Oui	Oui	Oui	Non
Attribution d'un nom au point	Oui	Oui	Oui	Non
Batterie faible radio	Oui	Oui	Oui	Non
Rétablissement batterie faible radio	Oui	Oui	Oui	Non
Inhibition	Oui	Oui	Oui	Non
Rétablissement inhibition	Oui	Oui	Oui	Non
Alarme d'auto-surveillance point	Oui	Oui	Oui	Oui
Rétablissement alarme auto-surveillance point	Oui	Oui	Oui	Oui

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports de point

4.9.12 Rapports de modification utilisateur

Valeur par défaut :

Rapports de modification utilisateur	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Date modifiée	Oui	Oui	Oui	Oui
Heure modifiée	Oui	Oui	Oui	Non
Supprimer l'utilisateur	Oui	Oui	Oui	Non
Modification de code utilisateur	Oui	Oui	Oui	Non
Surveillance de partition	Oui	Oui	Oui	Non
Carte/Télécommande liée	Oui	Oui	Oui	Non
Télécommande retirée	Oui	Oui	Oui	Non
Niveau de modification	Oui	Oui	Oui	Oui

Choix :

– Oui : attribuer ce rapport au groupe destinataire.

– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports de modification utilisateur.

4.9.13 Rapports d'accès

Valeur par défaut :

Rapports d'accès	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Accès octroyé	Oui	Oui	Oui	Oui
Accès refusé	Oui	Oui	Oui	Oui
Porte laissée ouverte	Oui	Oui	Oui	Oui
Cycle de porte	Oui	Oui	Oui	Oui
Porte déverrouillée	Oui	Oui	Oui	Oui
Porte sécurisée	Oui	Oui	Oui	Oui
Demande d'accès aux portes	Oui	Oui	Oui	Oui
Porte verrouillée	Oui	Oui	Oui	Oui

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports d'accès.

4.9.14 Rapports environnementaux

Valeur par défaut :

Rapports environnementaux	Groupe destinataire 1	Groupe destinataire 2	Groupe destinataire 3	Groupe destinataire 4
Alarme eau	Oui	Oui	Oui	Oui
Rétablissement eau	Oui	Oui	Oui	Non
Alarme Temp élevée	Oui	Oui	Oui	Oui
Rétablissement Temp élevée	Oui	Oui	Oui	Non
Alarme Temp faible	Oui	Oui	Oui	Oui
Rétablissement Temp faible	Oui	Oui	Oui	Non

Choix :

– Oui : attribuer ce rapport au groupe destinataire.
– Non : ne pas attribuer ce rapport au groupe destinataire.

Emplacement du menu RPS

Paramètres liés à la centrale > Routage des rapports > Rapports environnementaux

4.10 Communicateur, vue d'ensemble

Il existe quatre groupes destinataires. Les rapports sont liés à des groupes destinataires par catégorie (Rapports d'incendie ou Rapports d'intrusion) ou de manière individuelle (Alarme incendie). Voir *Vue d'ensemble de la génération de rapports, page 49* pour plus d'informations sur l'affectation de rapports à des groupes destinataires.
Utilisez les paramètres pour lier un dispositif de destination principal et jusqu'à 3 dispositifs de destination de sauvegarde à chaque groupe destinataire.
Si le dispositif de destination principal ne parvient pas à envoyer le rapport, la centrale bascule sur le premier dispositif de destination de sauvegarde et poursuit avec chacun des dispositifs de destination de sauvegarde configurés (premier, deuxième et troisième) jusqu'à ce que le rapport soit envoyé.

Remarque!
Les centrales B5512, B4512 et B3512 V2 ne sont pas dotées d'un deuxième ou d'un troisième dispositif de destination de sauvegarde.

La centrale effectue jusqu'à dix tentatives d'envoi des rapports d'un groupe destinataire en utilisant les dispositifs de destination principaux et de sauvegarde. La centrale bascule entre les dispositifs de destination principaux et de sauvegarde comme illustré dans le tableau. Au bout de 10 tentatives infructueuses, la centrale émet un événement Défaillance comm.
Si aucun dispositif de destination de sauvegarde n'est configuré, la centrale utilise le dispositif de destination principal pour l'ensemble des dix tentatives.

Destinations configurées	**Dispositif de destination principal et premier dispositif de destination de sauvegarde**	**Dispositif de destination principal, premier et deuxième dispositifs de destination de sauvegarde**	**Dispositif de destination principal et premier, deuxième et troisième dispositifs de destination de sauvegarde**
Tentative d'envoi :			
1	Dispositif de destination principal	Dispositif de destination principal	Dispositif de destination principal
2	Dispositif de destination principal	Dispositif de destination principal	Dispositif de destination principal

3	Premier dispositif de destination de sauvegarde	Premier dispositif de destination de sauvegarde	Premier dispositif de destination de sauvegarde
4	Premier dispositif de destination de sauvegarde	Premier dispositif de destination de sauvegarde	Premier dispositif de destination de sauvegarde
5	Dispositif de destination principal	Deuxième dispositif de destination de sauvegarde	Deuxième dispositif de destination de sauvegarde
6	Premier dispositif de destination de sauvegarde	Deuxième dispositif de destination de sauvegarde	Deuxième dispositif de destination de sauvegarde
7	Dispositif de destination principal	Dispositif de destination principal	Troisième dispositif de destination de sauvegarde
8	Premier dispositif de destination de sauvegarde	Premier dispositif de destination de sauvegarde	Troisième dispositif de destination de sauvegarde
9	Dispositif de destination principal	Deuxième dispositif de destination de sauvegarde	Dispositif de destination principal
10	Premier dispositif de destination de sauvegarde	Dispositif de destination principal	Premier dispositif de destination de sauvegarde

Événements DÉFAUT COMM, DÉFAILLANCE COMM

Lorsque le dispositif de destination principal ne parvient pas à se connecter au récepteur du centre de télésurveillance au bout de deux tentatives, la centrale bascule vers le dispositif de destination de sauvegarde. La centrale envoie le rapport d'origine ainsi qu'un rapport DÉFAUT COMM. Si aucun dispositif de destination de sauvegarde n'est configuré, un rapport DÉFAUT COMM est envoyé.

La centrale envoie un événement RÉTABLISSEMENT COMM si elle parvient à envoyer un rapport à l'aide du dispositif de destination principal.

Si le dispositif de destination principal est une destination IP (IP intégrée, IP cellulaire enfichable, adresse SDI2 1 ou adresse SDI2 2), la centrale envoie l'événement d'origine ainsi qu'un rapport DÉFAUT COMM incluant un modificateur de nombre SDI2 (SDI2 ##). Le modificateur SDI2 identifie le type de dispositif de destination IP comme illustré dans les tableaux :

Type de destination IP	Modificateur de nombre SDI2 pour la destination IP 1	Modificateur de nombre SDI2 pour la destination IP 2	Modificateur de nombre SDI2 pour la destination IP 3	Modificateur de nombre SDI2 pour la destination IP 4
Ethernet intégré	10	20	30	40

Type de destination IP	Modificateur de nombre SDI2 pour la destination IP 1	Modificateur de nombre SDI2 pour la destination IP 2	Modificateur de nombre SDI2 pour la destination IP 3	Modificateur de nombre SDI2 pour la destination IP 4
Cellulaire enfichable	18	28*	38	48
Adresse SDI2 1	11	21	31	41

*Par exemple, un rapport DÉFAUT COMM pour le groupe destinataire 1 avec le dispositif de destination principal lié à Cellulaire enfichable ou Cellulaire intégré, Destination 2 serait nommé : DÉFAUT COMM RG1 SDI228.
La centrale crée des événements DÉFAUT COMM lorsqu'aucun accusé de réception positif des interrogations du récepteur du centre de télésurveillance n'est reçu après le nombre de tentatives configuré.
En cas d'échec de toutes les tentatives pour le dispositif de destination principal et le dispositif de destination de sauvegarde, la centrale crée un événement DÉFAILLANCE COMM RG#. La centrale ne crée pas d'événement RÉTABLISSEMENT COMM pour les événements DÉFAILLANCE COMM.

Remarque!
Exigence CAN/ULC S304, ne pas effacer les rapports en attente
Lorsque CAN/ULC S304 est défini sur OUI, la centrale n'efface pas les rapports en attente avant de créer un événement DÉFAILLANCE COMM. Elle continue de mettre les rapports en file d'attente pour le destinataire en échec jusqu'à ce que l'un de ces destinataires dans le groupe destinataire soit restauré. Si la file d'attente atteint la capacité du journal des événements de la centrale, les rapports les plus anciens sont effacés (remplacés).

Remarque!
Exigence de la norme UL 985 relative aux unités d'alarme incendie de maison familiale
Lors de la configuration des paramètres de transmission par défaut, assurez-vous que les tests de la transmission sont réalisés tous les mois ou plus rapidement, et que l'échec de la communication (délai total créé par les paramètres de fréquence et le nombre de tentatives) est annoncé dans les 7 jours.

4.10.1 Dispositif destinataire principal

Valeur par défaut : Aucun dispositif

Choix :
- Aucun dispositif
- Destination IP intégrée 1
- Destination IP intégrée 2
- Destination IP intégrée 3
- Destination IP intégrée 4
- Cellulaire (enfichable) Destination 1
- Cellulaire (enfichable) Destination 2
- Cellulaire (enfichable) Destination 3
- Cellulaire (enfichable) Destination 4
- Téléphone (enfichable) Destination 1
- Téléphone (enfichable) Destination 2

- Téléphone (enfichable) Destination 3
- Téléphone (enfichable) Destination 4
- Adresse SDI2 1 Destination 1
- Adresse SDI2 1 Destination 2
- Adresse SDI2 1 Destination 3
- Adresse SDI2 1 Destination 4

Sélectionnez le dispositif de destination principal pour les groupes destinataires. La centrale utilise ce dispositif pour l'envoi de rapports au récepteur du centre de télésurveillance.
Le dispositif de destination principal sélectionné affecte un communicateur (communicateur IP intégré, communicateur cellulaire enfichable, communicateur téléphonique enfichable ou module SDI2) à une destination (*Adresse réseau, page 72* ou *Téléphone et paramètres du téléphone, page 31*)

Pour obtenir de plus amples informations
Pour plus d'informations sur l'envoi de rapports par la centrale, voir *Vue d'ensemble de la génération de rapports, page 49* et *Communicateur, vue d'ensemble, page 66*.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Communicateur > Dispositif de destination principal

4.10.2 Dispositifs de destination de sauvegarde

Valeur par défaut : aucun dispositif
Choix :

- Aucun dispositif
- Destination IP intégrée 1
- Destination IP intégrée 2
- Destination IP intégrée 3
- Destination IP intégrée 4
- Cellulaire (enfichable) Destination 1
- Cellulaire (enfichable) Destination 2
- Cellulaire (enfichable) Destination 3
- Cellulaire (enfichable) Destination 4
- Téléphone (enfichable) Destination 1
- Téléphone (enfichable) Destination 2
- Téléphone (enfichable) Destination 3
- Téléphone (enfichable) Destination 4
- Adresse SDI2 1 Destination 1
- Adresse SDI2 1 Destination 2
- Adresse SDI2 1 Destination 3
- Adresse SDI2 1 Destination 4

Sélectionnez jusqu'à 3 dispositifs de destination de sauvegarde (premier, deuxième, troisième) pour un groupe destinataire. La centrale utilise le dispositif de sauvegarde pour l'envoi de rapports au récepteur du centre de télésurveillance lorsque le dispositif principal est défaillant.
Le dispositif de destination de sauvegarde sélectionné affecte un communicateur (communicateur IP intégré, communicateur enfichable, communicateur téléphonique enfichable ou module SDI2) à une destination (*Adresse réseau, page 72* ou *Téléphone et paramètres du téléphone, page 31*).
Ne sélectionnez pas le même dispositif de destination comme dispositif de destination principal et dispositif de destination de sauvegarde pour un groupe destinataire.

Pour obtenir de plus amples informations

Pour plus d'informations sur l'envoi de rapports par la centrale, voir *Vue d'ensemble de la génération de rapports, page 49* et *Communicateur, vue d'ensemble, page 66*.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Communicateur > Dispositif de destination de sauvegarde

4.10.3 Récepteur réseau identique RG

Valeur par défaut : Oui

Choix :

- Oui : la centrale utilise la même clé d'authentification pour les destinations principale et de sauvegarde.
- Non : la centrale utilise des clés d'authentification distincts pour les destinations principale et de sauvegarde.

Définissez ce paramètre sur Oui dans les cas suivants :

- Le dispositif de destination principal et le dispositifs de destination de sauvegarde sont définis sur des dispositifs IP (intégré, cellulaire ou SDI2) et des destinations configurées dans les paramètres de communication avancée.
- Les destinations sont configurées pour le même récepteur du centre de télésurveillance, mais avec des adresses IP différentes qui sont accessibles depuis des réseaux différents (LAN/WAN et Internet, par exemple).

Lorsque ce paramètre est défini sur Oui, que la destination principale et la destination de sauvegarde utilisent des cadences d'interrogation différentes et que la centrale détecte une défaillance de communication sur le dispositif de destination principal ou de sauvegarde, le dispositif de destination opérationnel passe immédiatement à la cadence d'interrogation la plus rapide.

Lorsque ce paramètre est défini sur Non et que la centrale détecte une défaillance de communication sur le dispositif de destination principal ou de sauvegarde, le dispositif de destination opérationnel continue d'utiliser la cadence d'interrogation configurée.

Ce paramètre est généralement défini sur Non lorsque l'un des dispositifs de destination est défini sur un dispositif IP intégré ou SDI2 et que l'autre dispositif est défini sur un dispositif IP cellulaire enfichable. La cadence d'interrogation des destinations cellulaires est habituellement définie sur un taux plus lent (4 heures).

Les cadences d'interrogation définies sur 5 minutes ou sur une cadence supérieure peuvent dépasser votre plan de données cellulaire. Participez à des événements de défaillance de communication dès que possible.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Communicateur > Récepteur réseau identique RG

4.10.4 Synchronisation horaire

Valeur par défaut :

Groupe destinataire 1 : Oui

Groupes destinataires 2-4 : Non

Choix :

- Oui : synchroniser la date et l'heure de la centrale avec le récepteur du centre de télésurveillance.
- Non : ne pas synchroniser la date et l'heure de la centrale avec le récepteur du centre de télésurveillance.

Remarque!
Synchronisation horaire définie sur Oui
Lorsque la synchronisation horaire est définie sur **Oui**, vous devez définir le dispositif de destination principal ou les dispositifs de destination de sauvegarde sur **IP intégré**, **IP cellulaire enfichable** ou **SDI2** et également définir le format de rapport pour la destination sur **Modem4**.

Le paramètre Synchronisation horaire est disponible pour tous les groupes destinataires, mais il peut uniquement être défini sur Oui pour un groupe destinataire à la fois.

Décalage de la centrale de 30 minutes ou moins
Lorsque l'heure de la centrale est décalée de 30 minutes ou moins et qu'elle est antérieure à l'heure correcte, la centrale décompte les secondes à une vitesse supérieure à une par seconde. Si l'heure de la centrale est postérieure à l'heure correcte, la centrale décompte les secondes à une vitesse inférieure à une par seconde.
La centrale décompte le secondes dans ce mode jusqu'à ce que son heure soit synchronisée avec le récepteur du centre de télésurveillance. Chaque seconde s'écoule et aucune seconde n'est répétée. Par conséquent, aucun horaire, événement planifié ni aucun démarrage et arrêt de fenêtre n'est omis ou répété.

Décalage de la centrale de plus de 30 minutes
Lorsque l'heure de la centrale est décalé de plus de 30 minutes, la centrale définit ses date et heure sur les date et heure du récepteur de centre de télésurveillance.
Si ce changement avance l'heure de la centrale, des horaires, événements planifiés, ou démarrages et arrêts de fenêtre peuvent être omis. Si ce changement recule l'heure de la centrale, des horaires, événements planifiés, ou démarrages et arrêts de fenêtre peuvent être répétés.

Emplacement dans le menu RPS :
Paramètres liés à la centrale > Communicateur > Synchronisation horaire

4.11 Communication améliorée

4.11.1 Format de rapport

Valeur par défaut : Conettix : Modem4
Choix :

- Conettix : Modem4 - la centrale envoie des rapports au format de communication Modem4 étendu au récepteur du centre de télésurveillance.
- Conettix :Contact ID - utilisez ce format lorsque le récepteur du centre de télésurveillance ne prend pas en charge le format Modem4.
- DC-09 : Contact ID, TCP - la centrale envoie le contact ID via le protocole de transmission d'alarme TCP SIA DC-09 aux récepteurs et aux applications.
- DC-09 : Contact ID, UDP - la centrale envoie le contact ID via le protocole de transmission d'alarme UDP SIA DC-09 aux récepteurs et aux applications.
- DC-09 : SIA, TCP - la centrale envoie des rapports au format de communication SIA via le protocole de transmission d’alarme TCP SIA DC-09 aux récepteurs et aux applications.
- DC-09 : SIA, UDP - la centrale envoie des rapports au format de communication SIA via le protocole de transmission d’alarme UDP SIA DC-09 aux récepteurs et aux applications.

Sélectionnez le format de rapport utilisé par la centrale pour l'envoi de rapports au récepteur du centre de télésurveillance.

Remarque!
Les choix de format de rapport DC-09 ne sont pas disponibles lorsque Application européenne n'est pas activée (définie sur Non) dans Paramètres de conformité.

Remarque!
Contact ID ne prend pas en charge la synchronisation horaire
Si vous sélectionnez Contact ID, vous devez définir le paramètre *Synchronisation horaire, page 70* sur Non.

Remarque!
La valeur recommandée pour Durée de supervision du récepteur est de 300 secondes ou plus lors de l'utilisation du DC09 : SIA, protocole de transmission d'alarme TCP pour le format des rapports.

Emplacement dans le menu RPS :
Paramètres liés à la centrale > Communications améliorées > Format de rapport

4.11.2 Récepteur

Valeur par défaut : N/A
Configurez les destinations de rapports pour pouvoir utiliser jusqu'à 4 récepteurs différents (A-D).
Choix :
– A
– B
– C
– D
Pour identifier les destinations à l'aide d'un seul récepteur, liez une étiquette A, B, C ou D. Pour identifier les récepteurs qui sont différents, liez une étiquette A, B, C, D unique.

Emplacement dans le menu RPS :
Paramètres liés à la centrale > Communications améliorées > Récepteur

4.11.3 Adresse réseau

Valeur par défaut : Vide
Choix : adresse IPv4 (0.0.0.0 à 255.255.255.255) ou nom d'hôte (jusqu'à 255 caractères)
Pour acheminer des événements vers une adresse IP (dans une application privée locale ou une application de réseau étendu), sélectionnez une destination (Destination 1 – Destination 4) et entrez l'adresse IP de cette destination ici.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Communications améliorées > Adresse réseau (Destinations 1 à 4)

4.11.4 Numéro de port

Valeur par défaut : 7700
Choix : 1 à 65 535
Pour les communications IP avec un récepteur de centre de télésurveillance dans les installations classiques, conservez la valeur par défaut pour le port.

Remarque!
Limitation du trafic indésirable, sélection d'un numéro de port supérieur à 1023
Si vous choisissez de modifier le numéro de port par défaut, sélectionnez un numéro de port supérieur à 1023 afin de réduire le trafic réseau indésirable.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Communications améliorées > Numéro de port (Destination 1 à 4)

4.11.5 Temps de supervision du récepteur

Valeur par défaut : 4 heures - Sécurité moyenne
Choix :
- 200 secondes - UL1610
- 300 secondes - NFPA 72 2010
- 1 heure - NFPA 72 2013
- 4 heures - Sécurité moyenne
- 24 heures - Quotidien
- 25 - Heures
- 90 secondes - Sécurité élevée-UL 2050
- Aucune interrogation
- 95-195, 205-295, 305-1275 secondes - choix possibles par intervalles de 5 secondes
- 2, 3, 5-23, 26-255 heures
- Personnalisé

À l'exception du choix Personnalisé, le choix Temps de supervision du récepteur permet de définir automatiquement les paramètres Cadence d'interrogation, En attente d'accusé de réception et Compte de retentative.
Les paramètres Cadence d'interrogation, En attente d'accusé de réception et Compte de retentative associés permettent de configurer la supervision des connexions réseau au récepteur du centre de télésurveillance pour les destinations 1 à 4.

Remarque!
La valeur recommandée pour Durée de supervision du récepteur est de 300 secondes ou plus lors de l'utilisation du DC09 : SIA, protocole de transmission d'alarme TCP pour le format des rapports.

Le paramètre Cadence d'interrogation définit le délai entre les fréquences de polling envoyées par la centrale au récepteur du centre de télésurveillance.
Le paramètre En attente d'accusé de réception définit la délai d'attente observé par la centrale le temps que le récepteur du centre de télésurveillance envoie l'accusé de réception (ACK) d'une fréquence de polling.
Si l'accusé de réception n'est pas reçu, la centrale renvoie la fréquence de polling le nombre de fois entré au paramètre Compte de retentative. Lorsque le nombre de renvois est atteint, la centrale crée un événement Défaillance comm ##. (Consultez le tableau ci-dessous pour connaître la valeur ## correcte.)

Dispositif	Destination 1	Destination 2	Destination 3	Destination 4
SDI2-1	11	21	31	41
Ethernet Intégré	10	20	30	40

Dispositif	Destination 1	Destination 2	Destination 3	Destination 4
Cellulaire intégré	18	28	38	48

Même après un événement Défaillance comm ##, la centrale continue de renvoyer la fréquence de polling toutes les 10 secondes jusqu'à ce qu'elle reçoive un accusé de réception.
Lorsque la centrale reçoit un accusé de réception du centre de télésurveillance, la centrale revient au taux d'envoi normal.

Plusieurs destinations réseau
Lorsque plusieurs destinations réseau sont configurées, la centrale les utilise successivement. Par exemple, si aucun accusé de réception n'est reçu de la Destination 1 dans les 10 secondes, la centrale passe à la Destination 2 pour l'envoi de la fréquence de polling, puis elle attend l'accusé de réception avant de revenir la Destination 1 SDI pour renvoyer la fréquence de polling.
Si les fréquences de polling envoyées par une Destination SDI, et si l'attente d'accusé de réception (Destinations 1 à 4) est dépassé, un événement DÉFAILLANCE COMM ## se produit. Lorsque cet événement se produit, tous les événements routés vers cette destination se dirigent immédiatement vers la destination de sauvegarde.

Remarque!
Lors de l'envoi des rapports à un récepteur du centre de télésurveillance via une destination réseau, définissez ce paramètre sur une valeur différente de zéro. Si aucune valeur n'est paramétrée dans ce paramètre, cela peut empêcher le rétablissement normal d'une destination de communication réseau défaillante.

Si la centrale est paramétrée pour l'envoi d'une fréquence de polling au centre de télésurveillance, une cadence de 75 secondes permet de maintenir la liaison virtuelle dans la plupart des configurations réseau. Si la valeur de ce paramètre est diminuée, le nombre de communications inactives entre le dispositif SDI2 et le récepteur du centre de télésurveillance est accru. Un nombre accru de communications inactives entre la centrale et le récepteur réduit l'efficacité de la génération de rapports d'événement de la centrale.
La centrale réajuste la fréquence de polling temporairement de moins de 300 secondes à 300 secondes lorsqu'elle est en ligne avec le logiciel RPS. La cadence d'interrogation revient à la valeur programmée après la fin de la session RPS.
La première fois que vous sélectionnez Personnalisé, la valeur par défaut pour les paramètres *Cadence d'interrogation (secondes), page 75*, *En attente d'accusé de réception (secondes), page 75* et *Compte de retentative, page 76* est zéro. Dès que vous modifiez la valeur par défaut de ces paramètres, RPS conserve les valeurs même si vous modifiez la valeur Personnalisé du paramètre Temps de supervision du récepteur. Si Personnalisé est de nouveau sélectionné, les paramètres Cadence d'interrogation, En attente d'accusé de réception et Compte de retentative reprennent les valeurs enregistrées.

Remarque!
Le paramètre Temps de supervision du récepteur est essentiel pour le service cellulaire optimisé
Afin d'éviter des surcharges mensuelles et garantir que ce paramètre est correctement défini, consultez *Configuration du service Cellulaire, page 300*.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Communication améliorée > Temps de supervision du récepteur

4.11.6 Cadence d'interrogation (secondes)

Valeur par défaut : 12600 (lorsque le paramètre Temps de supervision du récepteur est défini sur la valeur par défaut de 4 heures, 0 lorsque le paramètre Temps de supervision du récepteur est d'abord défini sur Personnalisé)
Choix : (secondes)
- 0 - la fréquence de polling est désactivée.
- 5 à 65534 : active la cadence d'interrogation pendant la durée programmée ici (en secondes).
- 65535 : la fréquence de polling ne se produit qu'une fois par jour.

Le paramètre Temps de supervision du récepteur doit être défini sur Personnalisé afin de pouvoir modifier ce paramètre Cadence d'interrogation. Entrez l'intervalle (en secondes) observé par la centrale pour l'envoi d'une fréquence de polling au récepteur du centre de télésurveillance.
- 5 minutes = 300 secondes
- 1 heure = 3 600 secondes
- 12 heures = 43 200 secondes
- 18 heures = 64 800 secondes

Remarque!
Pour modifier les paramètres *Cadence d'interrogation (secondes), page 75*, *En attente d'accusé de réception (secondes), page 75* et *Compte de retentative, page 76*, définissez le paramètre *Temps de supervision du récepteur, page 73* sur Personnalisé.
La première fois que vous sélectionnez Personnalisé, la valeur par défaut pour les paramètres *Cadence d'interrogation (secondes), page 75*, *En attente d'accusé de réception (secondes), page 75* et *Compte de retentative, page 76* est zéro. Dès que vous modifiez la valeur par défaut de ces paramètres, RPS conserve les valeurs même si vous modifiez la valeur Personnalisé du paramètre Temps de supervision du récepteur. Si Personnalisé est de nouveau sélectionné, les paramètres Cadence d'interrogation, En attente d'accusé de réception et Compte de retentative reprennent les valeurs enregistrées.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Communications améliorées > Cadence d'interrogation

4.11.7 En attente d'accusé de réception (secondes)

Valeur par défaut : 300 (lorsque le paramètre Temps de supervision du récepteur est défini sur la valeur par défaut de 4 heures, 0 lorsque le paramètre Temps de supervision du récepteur est d'abord défini sur Personnalisé)
Choix : 5 à 65 535 (secondes)
Le paramètre Temps de supervision du récepteur doit être défini sur Personnalisé afin de pouvoir modifier ce paramètre En attente d'accusé de réception. Entrez la durée pendant laquelle la centrale attend un accusé de réception du récepteur du centre de télésurveillance pour les fréquences de polling ou les rapports (événements). Pour les rapports, la centrale attend un maximum de 15 secondes avant d'effectuer une nouvelle tentative.

Remarque!
Pour modifier les paramètres *Cadence d'interrogation (secondes), page 75*, *En attente d'accusé de réception (secondes), page 75* et *Compte de retentative, page 76*, définissez le paramètre *Temps de supervision du récepteur, page 73* sur Personnalisé.
La première fois que vous sélectionnez Personnalisé, la valeur par défaut pour les paramètres *Cadence d'interrogation (secondes), page 75*, *En attente d'accusé de réception (secondes), page 75* et *Compte de retentative, page 76* est zéro. Dès que vous modifiez la valeur par défaut de ces paramètres, RPS conserve les valeurs même si vous modifiez la valeur Personnalisé du paramètre Temps de supervision du récepteur. Si Personnalisé est de nouveau sélectionné, les paramètres Cadence d'interrogation, En attente d'accusé de réception et Compte de retentative reprennent les valeurs enregistrées.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Communications améliorées > En attente d'accusé de réception

4.11.8 Compte de retentative

Valeur par défaut : 5 (lorsque le paramètre Temps de supervision du récepteur est défini sur la valeur par défaut de 4 heures, 0 lorsque le paramètre Temps de supervision du récepteur est d'abord défini sur Personnalisé)
Choix :
0 - nouvelles tentatives en continu. Aucun événement d'échec de comm. pour la fréquence de polling.
1 à 255 : nombre de fois où la centrale renvoie la fréquence de polling.
Entrez le nombre de fois que la centrale renvoie la fréquence de polling avant d'effectuer un événement Échec de comm. SDI2 ##. (Consultez le tableau ci-dessous pour connaître la valeur ## correcte.)

Dispositif	Destination 1	Destination 2	Destination 3	Destination 4
SDI2-1	11	21	31	41
Ethernet Intégré	10	20	30	40
Cellulaire intégré	18	28	38	48

Remarque!
Pour modifier les paramètres *Cadence d'interrogation (secondes), page 75*, *En attente d'accusé de réception (secondes), page 75* et *Compte de retentative, page 76*, définissez le paramètre *Temps de supervision du récepteur, page 73* sur Personnalisé.
La première fois que vous sélectionnez Personnalisé, la valeur par défaut pour les paramètres *Cadence d'interrogation (secondes), page 75*, *En attente d'accusé de réception (secondes), page 75* et *Compte de retentative, page 76* est zéro. Dès que vous modifiez la valeur par défaut de ces paramètres, RPS conserve les valeurs même si vous modifiez la valeur Personnalisé du paramètre Temps de supervision du récepteur. Si Personnalisé est de nouveau sélectionné, les paramètres Cadence d'interrogation, En attente d'accusé de réception et Compte de retentative reprennent les valeurs enregistrées.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Communications améliorées > Compte de retentative

4.11.9 Taille de la clé AES

Valeur par défaut : Pas de chiffrement

Choix :

– Pas de chiffrement
– 128 bits - 16 bits
– 192 bits - 24 bits
– 256 bits - 32 bits

Sélectionnez la taille de clé AES.

Emplacement dans le menu RPS :

Paramètres liés à la centrale > Communications améliorées > Taille de la clé AES

4.11.10 Clé de chiffrement AES

Valeur par défaut : <Default>(Représente l'ID de clé 1 répertorié dans Configuration RPS > Système > Applicable à tous les comptes > Clé de chiffrement)

Choix : Trente-deux caractères hexadécimaux représentés par un ID (01 à 100).

Utilisez ce paramètre pour configurer chaque destination de récepteur avec une clé de chiffrement AES unique.

La clé de chiffrement AES repose sur la *Taille de la clé AES, page 77*. Pour la configuration de la clé de chiffrement, seuls l'ID de clé et le nom sont affichés.

Si au moins deux destinations réseau ont la même adresse réseau, RPS demande à l'opérateur d'utiliser la même clé de chiffrement pour ces destinations réseau.

Les chaînes de clé AES sont configurées dans Config > Système (System) > Applicable à tous les comptes (Global to all Accounts) > Clé de chiffrement (Encryption Key)

Emplacement dans le menu RPS

Paramètres liés à la centrale > Communications améliorées > Clé de chiffrement AES

4.12 SDI2 RPS / Comm. améliorée

4.12.1 Activer les communications améliorées ?

Valeur par défaut : Oui

Choix :

– Oui : permet la génération de rapports à l'aide d'un communicateur IP (intégré, cellulaire enfichable ou SDI2).
– Non : désactive la création de rapports à l'aide d'un communicateur IP.

Pour activer la génération de rapports à l'aide d'un communicateur IP (intégré, cellulaire enfichable ou SDI2), définissez ce paramètre sur Oui.

Définissez le *Dispositif destinataire principal, page 68* ou le *Dispositifs de destination de sauvegarde, page 69* pour au moins un groupe destinataire sur un dispositif IP intégré, Cellulaire enfichable ou SDI2.

4.12.2 RPS de réponse sur réseau activé ?

Valeur par défaut : Oui

Choix :

– Oui : activer les connexions automatiques initiées par RPS via le communicateur Ethernet embarqué ou un module d'interface réseau sur le bus SDI2.
– Non : empêche les connexions automatiques initiées par RPS sur le réseau.

Si ce paramètre est défini sur Non, les connexions initiées par RPS peuvent être acceptées au niveau du clavier en sélectionnant Réponse dans le menu RPS (Actions > RPS > Réponse).

Remarque!
Le mode Service autorise les connexions RPS sur le réseau
Lorsque la centrale est en mode service, elle accepte automatiquement les connexions initiées par RPS sur le réseau, même si ce paramètre est défini sur Non.
Pour placer la centrale en mode installateur, maintenez enfoncé le bouton de réinitialisation de la centrale jusqu'à ce que le voyant LED de polling clignote rapidement. Le clavier affiche MODE SERVICE et vous invite à entrer le code installateur. Saisissez le code installateur et appuyez sur [ENTRÉE].

Emplacement dans le menu RPS
Paramètres liés à la centrale > SDI RPS/Comm. améliorée > RPS de réponse sur réseau activé

4.12.3 Vérification de l'adresse RPS

Valeur par défaut : Non
Choix :
– Oui : la centrale vérifie que l'adresse IP à partir de laquelle RPS essaie de se connecter correspond à l'adresse réseau de RPS.
– Non : permet à RPS de se connecter à la centrale à partir de n'importe quelle adresse IP.

Pour obtenir de plus amples informations
Adresse réseau RPS, page 78

Emplacement dans le menu RPS
Paramètres liés à la centrale > SDI RPS/Comm. améliorée > Vérification de l'adresse RPS

4.12.4 Adresse réseau RPS

Valeur par défaut : Vide
Choix : adresse IPv4 ou nom d'hôte
Entrez l'adresse IP ou le nom d'hôte pour RPS.
Contactez votre administrateur réseau pour déterminer l'adresse IP ou le nom d'hôte auquel votre ordinateur RPS est connecté.

Emplacement dans le menu RPS
Paramètres liés à la centrale > SDI RPS/Comm. améliorée > Adresse réseau RPS

4.12.5 Numéro de port RPS

Valeur par défaut : 7 750
Choix : 1 - 65535
Entrez le port UDP de destination pour les sessions de réseau RPS initiées par la centrale.

Emplacement dans le menu RPS
Paramètres liés à la centrale > SDI RPS/Comm. améliorée > Numéro de port RPS

4.13 Supervision de la puissance

4.13.1 Temps de défaut secteur

Valeur par défaut : 01:00
Choix : 00:01 à 90:00 (Minutes:Secondes)
Entrez la durée pendant laquelle l'alimentation secteur (CA) est désactivée avant que la centrale envoie un rapport Défaut secteur.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Supervision de la puissance > Temps de défaut secteur

4.13.2 Renvoyer défaut secteur

Valeur par défaut : Aucun rapport
Choix :
– Aucun rapport : ne pas renvoyer de rapport Défaut secteur.
– Après 6 heures : renvoyer un rapport Défaut secteur au centre de télésurveillance au bout de 6 heures.
– Après 12 heures : renvoyer un rapport Défaut secteur au centre de télésurveillance au bout de 12 heures.

Temps d'attente observé par la centrale sans rétablissement de l'alimentation secteur avant le renvoi d'un rapport Défaut secteur.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Supervision de la puissance > Renvoyer défaut secteur

4.13.3 Affichage de défaut secteur

Valeur par défaut : 60
Choix : 10 à 300 (secondes) (par incréments de 5)
Délai d'attente observé par la centrale avant l'affichage du défaut secteur.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Supervision de la puissance > Affichage de défaut secteur

4.13.4 Rapport défaut secteur/rétablissement secteur

Valeur par défaut : Non
Choix :
– Oui : envoyer des rapports Défaut secteur et Rétablissement secteur.
– Non : ne pas envoyer des rapports Défaut secteur et Rétablissement secteur.

La centrale observe le délai d'attente défini dans le paramètre Temps de défaut secteur avant d'envoyer des rapports Défaut secteur.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Supervision de la puissance > Rapport Défaut secteur/ Rétablissement secteur

4.13.5 Accompagnement secteur

Valeur par défaut : Oui
Choix :
– Oui : envoyer uniquement si un autre événement se produit alors que l'alimentation secteur est anormale.
– Non : ne pas envoyer des rapports Défaut secteur en tant que rapports Accompagnement secteur.

Les centrales envoient des rapports de panne Accompagnement secteur uniquement si un autre événement se produit lorsque l'alimentation secteur est anormale.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Supervision de la puissance > Accompagnement secteur.

4.13.6 Sonnerie secteur/batterie

Valeur par défaut : Non

Choix :
- Oui : émettre une tonalité de défaillance de niveau centrale sur tous les claviers en cas de défaut secteur, batterie faible et batterie manquante.
- Non : ne pas émettre une tonalité de défaillance de niveau centrale sur tous les claviers en cas de défaut secteur, batterie faible et batterie manquante.

Ce paramètre n'empêche pas l'affichage d'un défaut secteur ou d'une batterie faible au niveau du clavier.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Supervision de la puissance > Sonnerie secteur/batterie

4.13.7 Rapport d'échec/de rétablissement de batterie

Valeur par défaut : Oui
Choix :
- Oui : les centrales envoient des rapports d'échec de batterie et des rapports de rétablissement au récepteur du centre de télésurveillance.
- Non : les rapports d'échec de batterie et rapports de rétablissement ne sont PAS envoyés au récepteur du centre de télésurveillance. Ce paramètre détermine si un rapport est envoyé lorsque la batterie est faible ou manquante.

Les rapports d'échec de batterie et les rapports de rétablissement sont routés vers les dispositifs de destination liés aux groupes destinataires configurés pour les rapports diagnostiques.
La batterie doit être déchargée au-dessous de 12,1 Vcc pendant 16 secondes avant que la centrale réponde à un événement de batterie faible. Entre 10 et 60 secondes sont nécessaires pour qu'une batterie manquante soit détectée.
Rapports de modem : manquante ou court-circuitée, BATTERIE MANQUANTE ; déchargée au-dessous de 12,1 Vcc, BATTERIE FAIBLE
Rapports Contact ID : manquante ou court-circuitée, BATTERIE MANQUANTE/ DÉFECTUEUSE ; déchargée au-dessous de 12,1 Vcc, BATTERIE SYSTÈME FAIBLE

Emplacement dans le menu RPS
Paramètres liés à la centrale > Supervision de la puissance > Rapport d'échec/de rétablissement de batterie.

4.14 Paramètres RPS

4.14.1 Code RPS

Valeur par défaut : 999999
Choix : 6 à 24 caractères alphanumériques (n’utilisez pas d’espaces dans le code. Le code est sensible à la casse.)
Il s’agit du code que RPS enregistre et utilise pour établir une connexion à la centrale.

Remarque!
Exigence UL 2610
Pour être conforme à la norme UL 2610, la longueur du mot de passe doit être d’au moins 6 caractères et contenir une combinaison de chiffres, de lettres et de symboles.

Remarque!
IMPORTANT ! Toutes les centrales sont conçues avec un code d'usine par défaut. Définissez et synchronisez un nouveau code RPS non défini par défaut dans la configuration de votre compte de centrale pour sécuriser l'accès et contrôler les connexions à votre centrale.

Pour la connexion de centrale initiale, le code d'usine par défaut doit être utilisé comme code RPS dans la fenêtre de connexion. Une fois connecté, les utilisateurs peuvent modifier le code RPS via la configuration ou la synchronisation.

- Pour les nouvelles centrales avec le firmware v 3.09+ et les modules B465 avec le firmware v 2.09+, utilisez le code d'ID du cloud par défaut défini en usine. Recherchez ce code unique de centrale sur l'étiquette imprimée de chaque centrale physique.
- Pour les centrales existantes avec un firmware antérieur a v 3.09 et les modules B465 avec un firmware antérieur à v 2.09, utilisez le code d'usine par défaut 999999.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Code RPS

4.14.2 Journal % complet

Valeur par défaut : 0
Choix: 0 (désactivé), 1 à 99 (%)
Lorsque le journal de la centrale est complet au taux indiqué, la centrale ajoute un événement Capacité du journal au journal et envoie un rapport au récepteur du centre de télésurveillance.
Entrez 0 pour désactiver les événements Capacité du journal et Saturation du journal (aucun événement ajouté au journal ou aux rapports envoyés).
Le rapport Capacité du journal alerte le centre de télésurveillance pour la connexion à la centrale et copie le journal de la centrale avant que des événements soient remplacés.
La centrale continue d'enregistrer des événements après l'envoi du rapport Capacité du journal. Lorsqu'elle atteint une capacité de 100 % (le journal est saturé et des événements stockés sont remplacés), la centrale crée un événement SATURATION DU JOURNAL local.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Journal % complet.

4.14.3 Contacter RPS si journal % plein

Valeur par défaut : Non
Choix :

- Oui : la centrale contacte automatiquement RPS lorsque le seuil de « Journal % complet » est atteint.
- Non : la centrale ne contacte pas automatiquement RPS lorsque le seuil de « Journal % complet » est atteint.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Contacter RPS si journal % plein.

4.14.4 Rappel RPS

Valeur par défaut : Non
Choix :

- Oui : dès que la centrale reçoit le code RPS de RPS, elle se déconnecte, puis compose le numéro de téléphone RPS afin d'établir une connexion avec RPS.
- Non : la centrale se connecte à RPS après vérification du code RPS.

Lorsque vous utilisez la fonction Rappel RPS avec le mode de composition de type DTMF, entrez un « C » comme dernier chiffre dans le numéro de téléphone RPS.

Pour obtenir de plus amples informations
Numéro de téléphone RPS, page 83

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Rappel RPS

4.14.5 Surveillance de ligne RPS

Valeur par défaut : Oui
Choix :
- Oui : si la centrale entend la tonalité Surveillance de ligne RPS après qu'un répondeur, un autre dispositif ou une personne répond à un appel entrant, elle saisit la ligne téléphonique.
- Non : la centrale ne saisit pas la ligne téléphonique pour se connecter avec RPS lorsqu'elle entend la tonalité Surveillance de ligne RPS.

Vous devez définir *Réponse armée, page 82* et/ou *Réponse désarmée, page 83*, et la centrale doit être dans l'état armé associé (armé ou désarmé).
Si vous définissez ce paramètre Surveillance de ligne RPS sur Oui, configurez les répondeurs qui partagent la ligne téléphonique avec la centrale afin qu'ils répondent au bout d'au moins deux sonneries.
Si *Rappel RPS, page 81* est défini sur Oui, la centrale raccroche le téléphone après avoir reçu le code RPS, puis elle appelle le numéro de téléphone RPS.

Remarque!
Définissez Surveillance de ligne RPS sur Non si la centrale effectue une fausse prise de ligne téléphonique
Une fausse prise de la ligne téléphonique indique qu'un dispositif partageant la ligne téléphonique utilise une tonalité avec la même fréquence que la tonalité Surveillance de ligne RPS.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Surveillance de ligne RPS

4.14.6 Réponse armée

Valeur par défaut : 7
Choix : 0 à 15 (sonneries)
- 1 à 15 : la centrale attend ce nombre de sonneries avant de répondre (prise de la ligne téléphonique) lorsque toutes les partitions sont armées Tout actif. Si la centrale partage la ligne téléphonique avec un répondeur, entrez un nombre supérieur de 2 sonneries au nombre de sonneries du répondeur.
- 0 (désactivé) : la centrale ne répond pas (prise de la ligne téléphonique) lorsque toutes les partitions sont armées Tout actif.

Remarque!
Pour RPS, Partielle est un état désarmé.

Si une partition est en Partielle ou désarmée (désactivée), la centrale utilise le compteur de sonneries *Réponse désarmée, page 83*.

Remarque!
Exigences RTC pour l'Australie/la Nouvelle-Zélande, désactivation de la réponse RPS armé/désarmé
Si vous définissez le paramètre Paramètres liés à la centrale > Paramètres du téléphone > Compatibilité RTC sur Australie ou Nouvelle-Zélande, vous devez définir les paramètres Réponse armée et Réponse désarmée sur 0 (désactivé).

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Réponse armée

4.14.7 Réponse désarmée

Valeur par défaut : 7
Choix : 0 à 15 (sonneries)
- 1 à 15 : la centrale attend ce nombre de sonneries avant de répondre (prise de la ligne téléphonique) lorsqu'au moins une partition est désarmée (désactivée) ou armée Partielle. Si la centrale partage la ligne téléphonique avec un répondeur, entrez un nombre supérieur de 2 sonneries au nombre de sonneries du répondeur.
- 0 (désactivé) : la centrale ne répond pas (prise de la ligne téléphonique) lorsqu'au moins une partition est désarmée (désactivée) ou armée Partielle.

Remarque!
Pour RPS, Partielle est un état désarmé.

Remarque!
Exigences RTC pour l'Australie/la Nouvelle-Zélande, désactivation de la réponse RPS armé/désarmé
Si vous définissez le paramètre Paramètres liés à la centrale > Paramètres du téléphone > Compatibilité RTC sur Australie ou Nouvelle-Zélande, vous devez définir les paramètres Réponse armée et Réponse désarmée sur 0 (désactivé).

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Réponse désarmée.

4.14.8 Numéro de téléphone RPS

Valeur par défaut : Vide
Choix : jusqu'à 24 caractères
Entrez le numéro de téléphone que la centrale compose pour se connecter à RPS.
La centrale appelle RPS pour les événements suivants :
- Le seuil *Journal % complet, page 81* est atteint (si activé).
- RPS appelle la centrale et le paramètre *Rappel RPS, page 81* est défini sur Oui.
- Au niveau du clavier, un utilisateur sélectionne MENU > Actions > RPS > Appeler via téléphone (une seule tentative est effectuée).

Si ce paramètre est vide, la centrale ne compose pas un numéro de téléphone pour RPS.
Pour plus d'informations sur les caractères que peut composer la centrale, consultez *Destination téléphonique 1 (à 4), page 31*.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Paramètres RPS > Téléphone RPS

4.14.9 Vitesse du modem RPS

Valeur par défaut : 1200

Choix :

– 300
– 1200
– 2400

Définissez le débit en bauds pour la communication RPS-centrale lors de l'utilisation d'une connexion RTC.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Paramètres RPS > Vitesse du modem RPS.

4.15 Divers

4.15.1 Type de contrainte

Valeur par défaut : 0

Choix :

– 0 : désactivé, aucun rapport d'alarme sous contrainte.
– 1 : +1, les utilisateurs ajoutent 1 au dernier chiffre de leur code pour envoyer un rapport d'alarme sous contrainte lorsqu'ils entrent le code au niveau d'un clavier.
– 2 : +2, les utilisateurs ajoutent 2 au dernier chiffre de leur code pour envoyer un rapport d'alarme sous contrainte lorsqu'ils entrent le code au niveau d'un clavier.
– 3 : la centrale envoie un rapport d'alarme sous contrainte chaque fois qu'un utilisateur lié à un niveau d'autorisation avec le paramètre Envoyer la contrainte défini sur Oui entre son code au niveau d'un clavier.

Par exemple, lorsque Type de contrainte est défini sur 1 (+ 1) :

– Si le code est 6123, 6124 active une alarme sous contrainte.
– Si le dernier chiffre du code est 0, une alarme sous contrainte se produit lorsque l'utilisateur entre 1 comme dernier chiffre du code.
– Si le dernier chiffre du code est 9, une alarme sous contrainte se produit lorsque l'utilisateur entre 0 comme dernier chiffre du code.

Par exemple, lorsque Type de contrainte est défini sur 2 (+ 2) :

– Si le dernier chiffre du code est 8, une alarme sous contrainte se produit lorsque l'utilisateur entre 0 comme dernier chiffre du code.
– Si le dernier chiffre du code est 9, une alarme sous contrainte se produit lorsque l'utilisateur entre 1 comme dernier chiffre du code.

Lorsque Type de contrainte est défini sur 3, et que des utilisateurs liés à un niveau d'autorisation avec le paramètre *Envoyer la contrainte, page 194* défini sur Oui entrent son code au niveau d'un clavier, la centrale envoie une alarme sous contrainte.

La génération de rapports d'alarme sous contrainte est activée ou désactivée par partition dans Paramètres de partition, *Contrainte activée, page 106*.

Remarque!

SIA CP-01 Exigence de réduction des fausses alarmes

Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur 3. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Divers > Type de contrainte.

4.15.2 Rapports d'annulation

Valeur par défaut : Oui

Choix :

- Oui : envoyer des rapports d'annulation, d'annulation incendie et d'annulation gaz.
- Non : ne pas envoyer des rapports d'annulation, d'annulation incendie et d'annulation gaz.

Un rapport d'annulation, d'annulation incendie et d'annulation gaz est créé lorsqu'un code est entré pour rendre silencieuse une sirène d'alarme, une sirène de gaz ou une sirène incendie avant expiration de la durée de sirène.

Remarque!

SIA CP-01 Exigence de réduction des fausses alarmes

Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Oui. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Divers > Rapports d'annulation

4.15.3 Texte Appeler votre installateur (première langue)

Valeur par défaut : contacter votre revendeur

Choix : entrez jusqu'à 32 caractères de texte, nombres, symboles ou espaces.

Le Texte Appeler votre installateur indique au niveau des claviers les événements de défaut système.

Les espaces avant, après et au sein d'une chaîne de texte sont inclus dans les 32 caractères. Les claviers affichent les 20 premiers caractères, puis ils font défiler les autres caractères sur l'écran une seule fois. Pour faire défiler à nouveau, appuyez sur la touche [ÉCHAP].

Une première et une seconde langues sont paramétrées lors de la configuration du compte de la centrale dans la fenêtre Données de la centrale. Les langues prises en charge incluent l'anglais, l'espagnol, le français et le portugais. Pour afficher les langues sélectionnées lors de la configuration du compte, consultez Paramètres liés à la centrale > Notification personnelle > Langue utilisateur.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Divers > Texte Appeler votre installateur - Anglais

4.15.4 Texte Appeler votre installateur (deuxième langue)

Valeur par défaut : Vide

Valeur par défaut : contacter votre revendeur

Choix : entrez jusqu'à 32 caractères de texte, nombres, symboles ou espaces.

Le Texte Appeler votre installateur indique au niveau des claviers les événements de défaut système.

Les espaces avant, après et au sein d'une chaîne de texte sont inclus dans les 32 caractères. Les claviers affichent les 20 premiers caractères, puis ils font défiler les autres caractères sur l'écran une seule fois. Pour faire défiler à nouveau, appuyez sur la touche [ÉCHAP].

Une première et une seconde langues sont paramétrées lors de la configuration du compte de la centrale dans la fenêtre Données de la centrale. Les langues prises en charge incluent l'anglais, l'espagnol, le français et le portugais. Pour afficher les langues sélectionnées lors de la configuration du compte, consultez Paramètres liés à la centrale > Notification personnelle > Langue utilisateur.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Divers > Texte Appeler votre installateur (deuxième langue)

4.15.5 Autorisation sur site pour mise à jour du firmware

Valeur par défaut : Non

Choix :

– Oui : exiger une autorisation sur site pour la mise à jour du firmware.
– Non : aucune autorisation sur site n'est requise.

Ce paramètre exige que le personnel sur site autorisé entre le code d'autorisation sur l'un des claviers à l'heure indiquée pendant le processus de mise à jour du firmware à distance.

Remarque!
Les mises à jour du firmware à distance doivent être autorisées sur site pour les systèmes homologués UL
Définissez ce paramètre sur « Oui » pour les systèmes homologués UL.

Effectuez un test du système complet à chaque mise à jour du firmware en local ou à distance.

Pour obtenir de plus amples informations
Mise à jour du firmware, page 198

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Autorisation sur site pour mise à jour du firmware.

4.15.6 Réponse de l'auto-surveillance du système

Valeur par défaut : Défaut

Choix :

– Défaut - les auto-surveillances de système sont des événements de défaut.
– Alarme permanente - les auto-surveillances de système sont des événements d'alarme sonore et visible.
– Alarme quand désarmé - lorsqu'au moins une zone est armée, les auto-surveillances du système sont des événements d'alarme silencieuse et invisible. Lorsque toutes les zones sont désarmées, les auto-surveillances de système sont des événements d'alarme sonore et visible.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Réponse de l'auto-surveillance du système

4.15.7 Auto-surveillance du coffret activée

Valeur par défaut : Non

Choix :

– Oui : activer l'entrée d'auto-surveillance de la centrale.
– Non : désactiver l'entrée d'auto-surveillance de la centrale.

Lorsque l'entrée d'auto-surveillance du coffret est activée, la centrale crée un événement d'auto-protection du coffret lorsque le coffret de la centrale est ouvert.
Les événements d'auto-surveillance n'affectent pas le processus d'armement ou de désarmement.
Lorsque vous passez le paramètre de la valeur Non à la valeur Oui, la centrale ne crée pas d'événements d'auto-surveillance tant qu'elle voit l'entrée d'auto-protection dans un état normal (la porte du coffret est fermée).
Si vous faites passer ce paramètre de la valeur Oui à la valeur Non et qu'il existe une événement d'auto-surveillance du coffret, l'événement, est effacé. Aucun événement de rétablissement n'est enregistré ou signalé.

Lorsque la centrale est mise sous tension, ou lorsqu'elle redémarre pour quelque raison que ce soit, l'entrée d'auto-surveillance est ignorée jusqu'à ce que la centrale voit l'entrée d'auto-protection dans un état normal.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Auto-surveillance du coffret activée

4.15.8 Résumé incendie et gaz

Valeur par défaut : Oui
Choix :
- Oui : les sorties Résumé incendie et Résumé sortie de gaz demeurent actives après la commande Rendre l'alarme silencieuse.
- Non : Résumé sorties incendie et Résumé sortie de gaz sont actives jusqu'à ce que tous les points incendie et gaz rendus silencieux sur le système fonctionnent normalement.

Définissez ce paramètre sur Oui pour conserver les flash incendie ou gaz actifs une fois les sirènes incendie ou gaz rendues silencieuses.

Emplacement du menu RPS
Paramètres de la centrale > Divers > Résumé incendie et gaz

4.15.9 Type d'événement de supervision d'incendie

Valeur par défaut : Rétablissement supervision incendie
Choix :
- Rétablissement défaut incendie : la centrale envoie un rapport RÉTABLISSEMENT DÉFAUT INCENDIE lorsqu'un point de supervision incendie est restauré à un état normal.
- Rétablissement alarme incendie : la centrale envoie un rapport RÉTABLISSEMENT ALARME INCENDIE lorsqu'un point de supervision incendie est restauré à un état normal.
- Rétablissement supervision incendie : la centrale envoie un rapport RÉTABLISSEMENT SUPERVISION INCENDIE lorsqu'un point de supervision incendie est restauré à un état normal.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Type d'événement de supervision d'incendie

4.15.10 Avertissement Incendie et Gaz

Valeur par défaut : Aucun
Choix :
- Aucun - les claviers ne font pas retentir la tonalité de défaut.
- Midi - les claviers font retentir la tonalité de défaut à midi. (Le midi) si un point incendie ou gaz se trouvant dans la portée d'un clavier est dans un état anormal.
- Minuit - les claviers font retentir la tonalité de défaut à minuit. (A minuit) si un point incendie ou gaz se trouvant dans la portée d'un clavier est dans un état anormal.

Lorsque l'avertissement sonore est activé, les événements de défaut incendie ou gaz précédemment confirmés et rendus silencieux déclenchent automatiquement un avertissement sonore sous forme de tonalité de défaut.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Avertissement Incendie et Gaz

4.15.11 Délai pour contrainte en avance

Valeur par défaut : 10

Choix : 5 à 30 (par incréments de 1 minute)

Entrez le délai dont dispose un utilisateur pour la saisie d'un deuxième code au clavier lors du désarmement (désactivation). Si aucun deuxième code n'est saisi avant la fin du délai défini au paramètre Délai pour Contrainte en avance, la centrale crée un événement Contrainte.

Pour plus de détails sur l'activation de la fonction Contrainte en avance, consultez le paramètre de partition, *Contrainte en avance ?, page 109*.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Divers > Délai pour Contrainte en avance

4.15.12 Deuxième code Contrainte

Valeur par défaut : Unique

Choix :

- Unique : le deuxième code saisi pour le processus Contrainte en avance doit être différent du premier code saisi pour désarmer la partition.
- N'importe lequel : le second code saisi pour le processus Contrainte en avance peut être différent du premier code saisi pour désarmer la partition, ou il peut s'agir du même code.

Consultez le paramètre Partition, processus *Contrainte en avance ?, page 109*.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Divers > Deuxième code Contrainte

4.15.13 Période d'interruption

Valeur par défaut : 30 secondes

Choix : 15 à 45 (secondes) (par incréments de 1 seconde)

Entrez le délai d'attente (en secondes) que doit observer la centrale avant d'envoyer un rapport d'alarme pour un point lié à un profil de point avec la fonction Annulation d'alarme est activée.

Pour une description de la fonction d'annulation d'alarme, consultez *Annulation d'alarme, page 237*.

Remarque!
Exigence UL
Pour répondre aux exigences de la norme UL, le temps total des valeurs *Temporisation d'entrée, page 227* et Période d'interruption ne doit pas dépasser 60 secondes.

Remarque!
Exigence SIA CP-01
Pour la conformité SIA CP-01, le paramètre Période d'interruption est obligatoire.

Si un utilisateur rend silencieuse l'alarme avant la fin de la période d'interruption, le rapport d'alarme est abandonné (il n'est pas envoyé) et le clavier affiche un message facultatif (voir *Affichage d'interruption, page 129*).

Cette fonctionnalité ne concerne pas les alarmes incendie ou les alarmes de point invisible.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Divers > Période d'interruption

4.15.14 Longueur du code

Valeur par défaut : Désactivé

Choix :

– Désactivé
– 3, 4, 5 ou 6 chiffres

Lorsque ce paramètre est défini sur 3, 4, 5 ou 6 chiffres, la longueur de code est fixe pour tous les codes. Les utilisateurs n'ont pas besoin d'appuyer sur la touche ENTRÉE après la saisie du code.

Lorsque le paramètre est défini sur Désactivé, la longueur de code n'est pas fixe. Les codes individuels peuvent avoir une longueur de 3 à 6 chiffres. Les utilisateurs doivent appuyer sur la touche ENTRÉE après la saisie du code.

Remarque!

Exigence SIA CP-01

Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur 3 à 6 chiffres. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Si la longueur de code est modifiée, cela crée des codes en double ou inutilisables ; dans ce cas une fenêtre AVERTISSEMENT Présence de codes en double/inutilisables s'affiche.

Les codes en double sont affichés en gras et en rouge.

Les codes inutilisables (dont la longueur est inférieure ou supérieure à la longueur saisie dans ce paramètre) s'affichent en gras et en bleu.

Pour corriger les codes en double ou inutilisables :

1. Sélectionnez le code (cliquez sur la cellule dans la colonne Code utilisateur).
2. Appuyez sur la touche [Retour arrière] du clavier pour effacer le contenu de la cellule.
3. Entrez le nouveau code.
4. Cliquez sur Enregistrer les codes corrigés pour enregistrer vos modifications. Tous les codes marqués en double ou inutilisables doivent être corrigés avant que vous cliquiez sur OK.

   - ou -

   Cliquez sur Désactiver la longueur de code et enregistrer les données dans ce compte. Cette option définit le paramètre Longueur de code sur Désactivé et vous permet d'enregistrer des codes de différentes longueurs dans le compte RPS.

Remarque!

Modification du paramètre Longueur du code

RPS affiche la boîte de dialogue de message suivante : « Cette opération va entraîner la désactivation du paramètre Longueur du code, SIA CP-01. Le paramètre Vérification sera défini sur Non et les données de code RPS préalablement existantes seront enregistrées. Souhaitez-vous vraiment continuer ? »

Codes similaires et en double

– Codes similaires : si le code que vous entrez est semblable à un autre code existant, ce dernier s'affiche dans le champ Codes similaires existants.
– Codes en double : si vous entrez un code qui correspond à un code existant, les codes existants s'affichent dans le champ Codes en double/sous contrainte. Les correspondances de code sont basées sur les entrées en double dont la longueur est définie sur la valeur la plus faible conforme à la norme SIA CP-01 (3).

Par exemple, si vous entrez « 478123 » comme code pour l'utilisateur 2 et « 478321 » comme code pour l'utilisateur 3, et que vous définissez la longueur du code sur trois chiffres, les codes des utilisateurs 2 et 3 apparaissent dans le champ Codes en double/sous contrainte, car ils partagent tous les deux les trois premiers chiffres « 478 ». Si la longueur du code est passée de quatre à trois chiffres, tous ces codes deviennent des codes en double de « 478 ».

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Longueur du code

4.15.15 Nombre de points inhibables

Valeur par défaut : 2
Choix : 1 à 4
Ce paramètre définit le nombre maximal de défauts autorisés sur un point contrôlé au sein d'un cycle d'armement avant que le point soit inhibé.

Remarque!
Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur 1 ou 2. Pour plus d'informations, consultez SIA CP-01 Vérification.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Nombre de points inhibables

4.15.16 Avertissement à distance

Valeur par défaut : Non
Choix :
- Oui : lorsque la partition est armée à distance, la centrale déclenche une fois la sirène d'alarme. Lorsque la partition est désarmée à distance, elle déclenche la sirène d'alarme deux fois.
- Non : aucun avertissement à distance pour l'armement à distance.

Les utilisateurs peuvent effectuer l'armement ou le désarmement à distance à l'aide d'une télécommande RADION, d'un médaillon Inovonics, d'un interrupteur à clé ou d'un logiciel distant.

Remarque!
Vérification SIA CP-01
Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Oui. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Pour obtenir de plus amples informations
Sirène d'alarme, page 146

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Avertissement à distance

4.15.17 Ajustement de l'heure

Valeur par défaut : Non
Choix :
- Oui : la centrale utilise la fréquence intégrée pour régler l'heure de son horloge.
- Non : la centrale utilise la fréquence secteur (de la source d'alimentation principale) pour régler l'heure de son horloge.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Ajustement de l'heure

4.15.18 Sortie de Partielle

Valeur par défaut : Non
Choix :
- Oui : la fonction de sortie Échec de fermeture devient la fonction Sortie de Partielle. Les sorties de Partielles s'activent lorsque toutes les partitions liées à la même sortie sont armées avec Partielle Instantané ou Partielle Temporisée.
- Non : les sorties Échec de fermeture sont opérationnelles lorsque la fenêtre de fermeture expire pour la partition spécifiée.

Lorsque ce paramètre Partielle est défini sur Oui, utilisez le paramètre *Armement anticipé de la partition, page 91* pour sélectionner si la sortie Partielle s'active au début de la temporisation de sortie, ou à la fin de la temporisation de sortie. Par défaut, la sortie s'active à la fin de la temporisation de sortie.

Pour obtenir de plus amples informations
Échec de fermeture/Partielle armée, page 147

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Sortie de Partielle

4.15.19 Armement anticipé de la partition

Valeur par défaut : Non
Choix :
- Oui : active la sortie Partition armée ou la sortie Partielle au début de la temporisation de sortie.
- Non : active la sortie Partition armée ou la sortie Partielle à la fin de la temporisation de sortie.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Armement anticipé de la partition

4.15.20 Heure d'été

Valeur par défaut : Heure d'été - États-Unis
Choix :
- Pas d'heure d'été - La centrale ne règle pas son horloge sur l'heure d'été.
- Heure d'été - États-Unis
- Heure d'été - Brésil
- Heure d'été - Mexique
- Heure d'été - Paraguay
- Heure d'été - Australie
- Heure d'été - Nouvelle-Zélande
- Heure d'été - Europe

L'horloge de la centrale applique les règles d'heure d'été des pays affichés.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Heure d'été

4.15.21 Format de la date

Valeur par défaut : mm jj aa
Choix :

– mm jj aa
– jj mm aa
– aa mm jj

Choisissez comment le mois, le jour et l'année sont délimités (séparés) dans le paramètre Délimiteur de date.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Format de la date

4.15.22 Délimiteur de date

Valeur par défaut : / (barre oblique)
Choix :
– / (barre oblique)
– . (point)
– - (tiret)

Sélectionnez comment le mois (mm), le jour (jj) et l'année (aa) sont délimités (séparés). Choisissez comment le mois, le jour et l'année sont affichés dans le paramètre Format de la date.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Délimiteur de date

4.15.23 Format de l'heure

Valeur par défaut : 12 heures (avec AM/PM)
Choix :
– 12 heures (avec AM/PM)
– 24 heures

Choisissez le format 12 heures, hh:mm AM (ou PM), ou 24 heures, hh:mm (00:00 à 23:59).

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Format de l'heure

4.15.24 Fuseau horaire

Valeur par défaut : UTC-05:00 (Heure de l'est, États-Unis & Canada)
Choix : Fuseaux horaires et UTC
Ce paramètre permet d'identifier le fuseau horaire dans lequel la centrale est installée.
(UTC-12:00) Ouest de la Ligne internationale de changement de date
(UTC-11:00) Îles Midway, Samoa
(UTC-10:00) Hawaï
(UTC-09:00) Alaska
(UTC-08:00) Heure du Pacifique (États-Unis & Canada)
(UTC-08:00) Tijuana, Basse Californie
(UTC-07:00) Arizona
(UTC-07:00) Chihuahua, La Paz, Mazatlán
(UTC-07:00) Heures des Rocheuses (États-Unis & Canada)
(UTC-06:00) Amérique centrale
(UTC-06:00) Heure du Centre (États-Unis & Canada)
(UTC-06:00) Guadalajara, Mexico, Monterrey
(UTC-06:00) Saskatchewan
(UTC-05:00) Bogota, Lima, Quito
(UTC-05:00) Heure de l'Est (États-Unis & Canada)
(UTC-05:00) Indiana (Est)

(UTC-04:30) Caracas
(UTC-04:00) Asunción
(UTC-04:00) Heure de l'Atlantique (Canada)
(UTC-04:00) Georgetown, La Paz, San Juan
(UTC-04:00) Manaus
(UTC-04:00) Santiago
(UTC-03:30) Terre-Neuve
(UTC-03:00) Brasilia
(UTC-03:00) Buenos Aires
(UTC-03:00) Cayenne
(UTC-03:00) Groenland
(UTC-03:00) Montevideo
(UTC-02:00) Centre-Atlantique
(UTC-01:00) Açores
(UTC-01:00) Îles du Cap-Vert
(UTC) Casablanca
(UTC) Temps universel coordonné
(UTC) Dublin, Édimbourg, Lisbonne, Londres
(UTC) Monrovia, Reykjavik
(UTC+01:00) Amsterdam, Berlin, Berne, Rome, Stockholm, Vienne
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(UTC+01:00) Bruxelles, Copenhague, Madrid, Paris
(UTC+01:00) Sarajevo, Skopje, Varsovie, Zagreb
(UTC+01:00) Ouest de l'Afrique centrale
(UTC+02:00) Amman
(UTC+02:00) Athènes, Bucarest, Istanbul
(UTC+02:00) Beyrouth
(UTC+02:00) Le Caire
(UTC+02:00) Harare, Pretoria
(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(UTC+02:00) Jérusalem
(UTC+02:00) Minsk
(UTC+02:00) Windhoek
(UTC+03:00) Bagdad
(UTC+03:00) Koweït, Riyadh
(UTC+03:00) Moscou, St Pétersbourg, Volgograd
(UTC+03:00) Nairobi
(UTC+03:00) Tbilissi
(UTC+03:30) Téhéran
(UTC+04:00) Abu Dhabi, Muscat
(UTC+04:00) Bakou
(UTC+04:00) Port Louis
(UTC+04:00) Erevan
(UTC+04:30) Kaboul
(UTC+05:00) Ekaterinbourg
(UTC+05:00) Islamabad, Karachi
(UTC+05:00) Tachkent
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
(UTC+05:30) Sri Jayawardenepura

(UTC+05:45) Katmandou
(UTC+06:00) Almaty, Novosibirsk
(UTC+06:00) Astana, Dhaka
(UTC+06:30) Yangon (Rangoon)
(UTC+07:00) Bangkok, Hanoï, Jakarta
(UTC+07:00) Krasnoyarsk
(UTC+08:00) Pékin, Chongqing, Hong Kong, Urumqi
(UTC+08:00) Irkoutsk, Oulan Bator
(UTC+08:00) Kuala Lumpur, Singapour
(UTC+08:00) Perth
(UTC+08:00) Taipei
(UTC+09:00) Osaka, Sapporo, Tokyo
(UTC+09:00) Séoul
(UTC+09:00) Iakoutsk
(UTC+09:30) Adélaïde
(UTC+09:30) Darwin
(UTC+10:00) Brisbane
(UTC+10:00) Canberra, Melbourne, Sydney
(UTC+10:00) Guam, Port Moresby
(UTC+10:00) Hobart
(UTC+10:00) Vladivostok
(UTC+11:00) Magadan, Îles Salomon, Nouvelle-Calédonie
(UTC+12:00) Auckland, Wellington
(UTC+12:00) Fidji, Îles Marshall
(UTC+12:00) Petropavlovsk-Kamchatsky
(UTC+13:00) Nuku'alofa

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Fuseau horaire

4.15.25 Format de texte personnalisé

Remarque!
Paramètre en lecture seule
Vous ne pouvez pas modifier ce paramètre.
RPS le définit automatiquement le Format de texte personnalisé lorsque vous configurez les paramètres Données de centrale - Vue > Informations sur la centrale > Première langue et Deuxième langue.

Choix (en lecture seule) :
- Standard - RPS permet de définir ce paramètre Format de texte personnalisé sur Standard (Jeu de caractères Latin-1) lorsque les deux paramètres Données de centrale - Vue > Informations sur la centrale > Première langue et Deuxième langue sont définis sur Anglais, Néerlandais, Français, Allemand, Hongrois, Italien, Portugais, Espagnol ou Suédois.
- Étendu - RPS définit le paramètre F texte personnalisé sur Étendu (jeu de caractères Unicode UTF-8) lorsque la langue de la centrale est réglée sur le chinois, le polonais ou le grec ou si un compte est connecté à une centrale dont la langue est déjà définie sur le chinois, le polonais ou le grec.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Divers > Format de texte personnalisé

4.15.26 Version TLS minimale

Valeur par défaut : disponibilité maximale

Choix :

- Disponibilité maximale
- TLS 1.0
- TLS 1.1
- TLS 1.2

Sélectionnez la version TLS (Transport Layer Security) minimale prise en charge à utiliser pour les connexions entre la centrale et le transmetteur. Ce paramètre permet de prendre en charge la version sélectionnée et les versions ultérieures. La valeur par défaut est la version TLS la plus élevée actuellement disponible.

Emplacement du menu RPS

Paramètres liés à la centrale > Divers > Version TLS minimale

4.16 Destinations de notification personnelle

4.16.1 Description

Valeur par défaut : vide (texte pour référence uniquement)

Choix : 0 à 32 caractères de long

Entrez le texte permettant d'identifier le dispositif de notification personnelle ou le destinataire de notification.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Destinations de notification personnelle > Description.

4.16.2 Nº de téléphone SMS / Adresse de messagerie

Valeur par défaut : Vide

Choix : jusqu'à 255 caractères alphanumériques

Saisissez un numéro de téléphone de destination pour recevoir des notifications de texte SMS ou une adresse e-mail pour recevoir des messages électroniques.

Numéro de téléphone SMS

La centrale envoie les notifications personnelles à un dispositif cellulaire lorsque la destination est un numéro de téléphone cellulaire contenant uniquement les chiffres 0 à 9. Les tirets ne sont pas autorisés.

Adresse de messagerie

La centrale envoie des notifications personnelles aux comptes de messagerie lorsque la destination est une adresse de messagerie.

Remarque!

Notification personnelle non envoyée pour les entrées incorrectes

Si votre entrée n'est ni un numéro de téléphone correct ni une adresse de messagerie correcte, la centrale n'envoie pas de message de notification personnelle. La centrale consigne une erreur d'envoi SMS.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Destinations de notification personnelle > Nº de téléphone SMS / Adresse de messagerie

4.16.3 Langue utilisateur

Valeur par défaut : 1 : [langue définie comme première langue dans Données de centrale - Vue]

Choix :

– 1 : [langue définie comme première langue dans Données de centrale - Vue]
– 2 : [langue définie comme seconde langue dans Données de centrale - Vue]

Sélectionnez la langue dans laquelle sont envoyés les messages de notification personnelle. Une première et une seconde langues sont paramétrées lors de la configuration du compte de la centrale dans Données de centrale - Vue.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Destinations de notification personnelle > Langue utilisateur

4.16.4 Méthode

Valeur par défaut : Module SMS cellulaire enfichable

Choix :

– Aucun
– SMS cellulaire enfichable : peut être sélectionné si vous disposez d'un module cellulaire enfichable B44x.
– E-mail cellulaire enfichable : peut être sélectionné si vous disposez d'un module cellulaire enfichable B44x.
– Élément de bus, SMS cellulaire : peut être sélectionné si vous disposez d'un module B450 v2.
– Élément de bus, E-mail : peut être sélectionné si vous disposez d'un module B450 v2 ou d'un module B426 v3.
– E-mail Ethernet intégré : peut être sélectionné si votre connexion est IP intégré.

Sélectionnez la destination de notification personnelle et le dispositif de destination utilisés pour l'envoi de la notification.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Destinations de notification personnelle > Méthode

4.17 Rapports de notification personnelle

INFORMATIONS IMPORTANTES CONCERNANT LE SERVICE CELLULAIRE

Pour des informations importantes concernant la configuration de votre centrale pour permettre une communication cellulaire correcte avec le récepteur du centre de télésurveillance, consultez *Configuration du service Cellulaire, page 300*.

Utilisez ce paramètre pour lier des notifications personnelles aux destinations et groupes destinataires.

La centrale envoie des notifications personnelles à un dispositif cellulaire lorsque la destination est un numéro de téléphone cellulaire.

La centrale envoie des notifications personnelles aux comptes de messagerie lorsque la destination est une adresse de messagerie.

Remarque!
Notification personnelle non envoyée pour une destination incorrecte
Si la destination n'est pas définie sur un numéro de téléphone ou une adresse de messagerie correcte, la centrale n'envoie pas le message de notification personnelle. La centrale consigne une erreur d'envoi SMS.

Remarque!
IP cellulaire pour dispositif de destination principal ou dispositif de destination de sauvegarde non requis
Vous n'êtes pas tenu du définir les paramètres Dispositif de destination principal ou Dispositif de destination de sauvegarde sur IP cellulaire pour que la notification personnelle par SMS fonctionne.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Notification personnelle > Rapports de notification personnelle > Notification personnelle 1 à 4

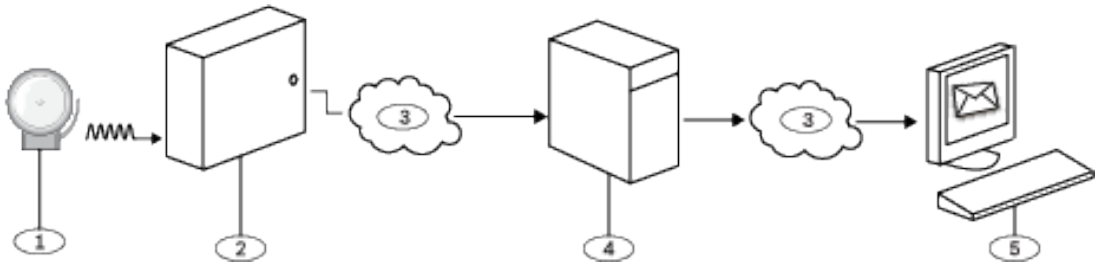
4.18 Tentatives de routage de notification personnelle

Valeur par défaut : 3
Choix : 1-6
Définissez le nombre de tentatives effectuées par la centrale pour l'envoi d'une notification personnelle.

Emplacement dans le menu RPS
Paramètres liés à la centrale > Notification personnelle > Tentatives de routage de notification personnelle

4.19 Configuration du serveur de messagerie

Vous pouvez configurer la centrale pour l'envoi des notifications personnelles à jusqu'à 16 adresses de messagerie.
Lorsqu'un événement se produit, la centrale transmet un rapport via un réseau IP à un serveur de messagerie. Le serveur de messagerie SMTP (Simple Mail Transfer Protocol) convertit les données entrantes en texte, puis les intègre aux destinations que vous avez configurées. Il s'agit d'une communication unidirectionnelle entre la centrale et l'utilisateur.



Légende - Description
1 - Événement d'alarme
2 - Centrale Bosch compatible
3 - Internet
4 - Serveur de messagerie SMTP

Légende - Description
5 - Ordinateur ou autre dispositif utilisé pour recevoir les e-mails

Configuration d'un compte de messagerie

Pour configurer un compte de messagerie qui envoie des e-mails aux destinations de notification personnelle :

1. Inscrivez-vous pour un compte de messagerie à partir d'un fournisseur de messagerie (par exemple : Google, Yahoo, AOL, Microsoft).
2. Choisissez un nom d'utilisateur afin qu'il soit plus simple pour les personnes qui reçoivent les notifications d'identifier les e-mails en provenance de la centrale (par exemple : panelacctstore52).
3. Entrez l'adresse associée au serveur de messagerie SMTP choisi dans le paramètre Nom/adresse du serveur de messagerie.
4. Entrez le nom d'utilisateur spécifié lors de l'enregistrement de ce compte dans le paramètre Nom de l'utilisateur d'authentification.
5. Saisissez le mot de passe spécifié lors de l'enregistrement de ce compte dans le paramètre Mot de passe d'authentification.

4.19.1 Nom/adresse du serveur de messagerie

Valeur par défaut : Vide

Choix : nom de domaine ou adresse IP

Entrez le nom de domaine ou l'adresse du serveur de messagerie SMTP (Simple Mail Transfer Protocol) de votre fournisseur.

La centrale utilise le nom de domaine (ou l'adresse) du serveur pour l'envoi de messages de notification personnelle depuis la centrale aux destinataires d'e-mail de notification personnelle.

Serveurs de messagerie SMTP

Le tableau ci-dessous comporte quelques fournisseurs de messagerie courants et le nom de domaine de leur serveur. Si votre fournisseur ne figure pas dans ce tableau, contactez-le pour connaître son nom de domaine (ou son adresse IP).

Fournisseur de messagerie	Nom de domaine
1&1	smtp.1and1.com
Airmail	mail.airmail.net
AOL	smtp.aol.com
AT&T	outbound.att.net
Bluewin	smtpauths.bluewin.ch
BT Connect	mail.btconnect.tom
Comcast	smtp.comcast.net
EarthLink	smtpauth.earthlink.net
Gmail	smtp.gmail.com
Gmx	mail.gmx.net
HotPop	mail.hotpop.com

Fournisseur de messagerie	Nom de domaine
Libero	mail.libero.it
Lycos	smtp.lycos.com
O2	smtp.o2.com
Orange	smtp.orange.net
Outlook.com (ancien Hotmail)	smtp.live.com
Tin	mail.tin.i
Tiscali	smtp.tiscali.co.uk
Verizon	outgoing.verizon.net
Virgin	smtp.virgin.net
Wanadoo	smtp.wanadoo.fr
Yahoo	smtp.mail.yahoo.com

Pour obtenir de plus amples informations

Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Configuration du serveur de messagerie > Nom/adresse du serveur de messagerie

4.19.2 Numéro de port du serveur de messagerie

Valeur par défaut : 25

Choix : 1-65535

Le port 25 est le port SMTP par défaut pour la plupart des serveurs sortants. Si l'adresse IP refuse le numéro de port par défaut (généralement en raison du trafic de courrier indésirable et de logiciels malveillantes), essayez un autre port couramment utilisé, comme le port 587 ou 465, afin d'éviter le blocage.

Exemples de fournisseurs, serveurs de messagerie, ports et sécurité :

Fournisseur	URL serveur SMTP	Port	Authentification / Chiffrement
Gmail	smtp.gmail.com	465	Chiffré
Yahoo (non chiffré)	smtp.mail.yahoo.com	25	Authentifier
Yahoo (chiffré)	smtp.mail.yahoo.com	465	Chiffré
Verizon	smtp.verizon.net	465	Chiffré
AT&T	AT&T outbound.att.net	465	Chiffré
Comcast	smtp.comcast.net	465	Chiffré
Time Warner	smtp-server.<region>.rr.com	25	Authentifier

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Configuration du serveur de messagerie > E-mail

Numéro de port du serveur

4.19.3 Authentification/Chiffrement du serveur de messagerie

Valeur par défaut : Authentification (Authenticate)

Choix :

De base (Basic) - aucune authentification, aucun chiffrement

Authentification (Authenticate) - authentification requise, pas de chiffrement

Chiffrement (Encrypted) - authentification requise, chiffrement requis

Sélectionnez le paramètre de sécurité requis par le serveur de messagerie pour la réception des messages de la centrale.

Authentification signifie que le serveur de messagerie requiert un nom d'utilisateur d'authentification et un mot de passe d'authentification. On appelle parfois cela SMTP-AUTH.

Le chiffrement utilisé est Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Configuration du serveur de messagerie > Authentification/Chiffrement du serveur de messagerie

4.19.4 Nom de l'utilisateur d'authentification

Valeur par défaut : Blanc

Choix : Blanc, 1 à 255 caractères

Entrez le nom d'utilisateur du compte de messagerie qui reçoit l'e-mail de notification personnel envoyé par la centrale.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Configuration du serveur de messagerie> Nom de l'utilisateur d'authentification

4.19.5 Mot de passe d'authentification

Valeur par défaut : Blanc

Choix : Blanc, 1 à 49 caractères

Entrez le mot de passe que le serveur SMTP utilise pour envoyer des e-mails aux destinations de notification personnelle.

Emplacement dans le menu RPS

Paramètres liés à la centrale > Notification personnelle > Configuration du serveur de messagerie> Mot de passe d'authentification

5 Paramètres liés à la partition

5.1 Paramètres de partition/sirène, Options d'ouverture/de fermeture

Une partition est définie comme un ensemble de points regroupés géographiquement.

Configurations

La programmation par partitions offre un grand choix de configurations du système. La centrale attribue un numéro de compte à chaque partition afin de définir les fonctions d'annonce, de contrôle et de création de rapports. Vous pouvez, si vous le souhaitez, faire en sorte que l'armement de partition soit conditionné à l'état d'autres partitions (maître ou associé). Vous pouvez configurer n'importe quelle zone pour l'armement périmétrique et intérieur, sans avoir besoin d'une zone distincte pour cette fonction. Reliez plusieurs partitions entre elles au sein d'une partition partagée soumise à un contrôle automatique (entrée ou hall).

Pour les systèmes comportant plusieurs partitions, toutes les partitions doivent être sous la responsabilité d'un propriétaire et d'une direction. Il peut s'agir d'un groupe de bâtiments liés ou non, qui peuvent même avoir différentes adresses, mais qui sont sous la responsabilité d'une personne ayant un intérêt mutuel (en plus de l'entreprise qui installe l'alarme). Cela ne s'applique pas aux applications de rue commerçante dans lesquelles chaque entreprise indépendante doit avoir son propre système d'alarme séparé.

Comme exemple de système commercial, on pourrait avoir une entreprise qui a une zone BUREAU et une zone ENTREPÔT dans un bâtiment où chaque zone peut être armée ou désarmée indépendamment.

Un exemple résidentiel serait un système configuré avec le garage et la maison comme des partitions séparées.

Dans chacun des exemples ci-dessus, toutes les partitions sont sous la seule responsabilité du propriétaire unique.

Dans des systèmes à plusieurs partitions, la sirène et la centrale doivent se trouver dans l'une des partitions protégées.

La sirène doit se trouver à un emplacement où elle peut être entendue par les utilisateurs qui activent et désactivent (arment et désarment) les partitions.

Le B6512 prend en charge jusqu'à 6 partitions.

5.1.1 Texte du nom de partition (première langue)

Valeur par défaut : n° de partition

Choix : jusqu'à 32 caractères de texte, nombres, espaces et symboles

Entrez un nom de partition pour l'affichage au niveau des claviers.

Emplacement dans le menu RPS

Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Texte du nom de partition

5.1.2 Texte du nom de partition (deuxième langue)

Valeur par défaut : Vide

Choix : jusqu'à 32 caractères de texte, nombres, espaces et symboles

Entrez un nom de partition pour l'affichage au niveau des claviers.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Texte du nom de partition
(Deuxième langue)

5.1.3 Partition activée

Valeur par défaut :
- B6512 :
  - Partition 1 : Oui
  - Partitions 2 à 6 : Non

Choix :
Oui : la partition est activée.
Non : la partition est désactivée.

Remarque!
Exigence UL 864
Pour vous conformer aux exigences de la norme UL 864 relative aux systèmes d'applications d'alarme incendie commerciales, définissez ce paramètre sur Oui.

Lorsqu'une partition est définie sur Non :
- Les points liés à cette partition ne génèrent pas d'événements.
- Lors de l'armement et du désarmement, ce numéro de partition n'est pas affiché au niveau des claviers avec la portée d'affichage de cette partition.
- L'état de cette partition n'est pas signalé dans les rapports d'état.
- Tous les niveaux d'autorité de l'utilisateur dans cette partition sont désactivés lorsque cette partition est désactivée.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Partition activée

5.1.4 Numéro de compte

Valeur par défaut : 0000
Choix : 4 ou 10 chiffres, 0 à 9, B à F
Ce paramètre détermine le numéro de compte signalé pour cette partition. Un numéro de compte doit être lié à chaque partition active.
Si au moins 5 chiffres sont utilisés dans le numéro de compte, RPS remplit automatiquement le nombre par des zéros de début pour pouvoir en faire un numéro à dix chiffres.

Remarque!
Assurez-vous que l'automatisation du centre de télésurveillance est compatible avec les numéros de compte à 10 chiffres avant de programmer un numéro de compte à 10 chiffres sur la centrale.

Remarque!
Les numéros de compte ne doivent pas inclure de « A » à la place d'un chiffre.

Les numéros de compte sont utilisés pour regrouper les partitions. Chaque partition peut avoir un numéro de compte différent, ou plusieurs partitions peuvent partager le même numéro de compte. La centrale utilise le numéro de compte comme référence pour l'armement et les affichages de texte de clavier.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Numéro de compte.

5.1.5 Forcer armement/inhibition max

Valeur par défaut : 2
Choix :
B6512 : 0 à 30
Entrez le nombre de points contrôlés qui peuvent être en défaut ou à un état inhibé lors de l'armement de la partition.
Consultez *Forcer armement retournable, page 232* et *Inhibition retournable, page 232* dans le profil de point pour retourner un point au système lorsque le point retourne à l'état normal ou lorsque la partition est désarmée.

Remarque!
Le paramètre *Inhibable, page 233* doit être défini sur Oui pour que les points soient inhibés ou armés de force. L'armement forcé n'inhibe pas les points 24 heures.

Remarque!
Pour être en conformité avec la norme UL1610, définissez ce paramètre sur 0 pour les télécommandes radio.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Forcer armement/inhibition max

5.1.6 Rétablissements de temporisation

Valeur par défaut : Aucune temporisation
Choix :
Aucune temporisation : les événements de rétablissement de point sont consignés et signalés lors de la restauration physique du point.
Temporisation jusqu'à ce que la sirène soit rendue silencieuse : les événements de rétablissement de point ne sont pas consignés ou signalés tant que le point n'est pas restauré physiquement et que la sirène est rendue silencieuse (ou que le délai de la sirène expire).
Pour les points alarme/supervision incendie/gaz, les événements de rétablissement ne sont pas consignés ou signalés tant que le point n'est pas restauré physiquement, la sirène rendue silencieuse et l'événement effacé des claviers.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Rétablissements de temporisation

5.1.7 Tonalité de sortie

Valeur par défaut : Oui

Choix :
Oui : déclencher une tonalité de sortie au niveau de tous les claviers pendant la temporisation de sortie.
Non : activer/désactiver les tonalités de sortie pour les claviers individuellement (dans la configuration du clavier).

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Tonalité de sortie

5.1.8 Durée de la temporisation de sortie

Valeur par défaut : 60
Choix : 0 à 600 (secondes, par incréments de 5)
Définissez la durée pendant laquelle les utilisateurs doivent quitter les locaux sans déclencher un événement d'alarme après l'armement de leur système Tout activé - Temporisation ou Partielle - Temporisation.
Ils doivent sortir par un point lié à un profil de point qui est configuré pour un type de point contrôlé par une réponse d'alarme différée (voir *Réponse du point, page 213*)
Les points programmés pour une réponse d'alarme instantanée génèrent des alarmes immédiatement, même pendant la temporisation de sortie.

Remarque!
Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur 45 à 255 secondes. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Durée de la temporisation de sortie

5.1.9 Détection automatique

Valeur par défaut : manuel

Choix :
- Manuel : les utilisateurs activent et désactivent le mode de détection manuellement à partir d'un clavier.
- Prêt à être désarmé : la centrale active automatiquement le mode de détection lorsque la partition est désarmée (désactivée).

Si une partition est désarmée et que le mode de détection est activé, la tonalité de détection se déclenche au niveau des claviers lorsque des points configurés en tant que points de détection sont en défaut.
Consultez *Point de détection, page 230* pour savoir comment configurer les points de la fonction de détection.
Lorsque la partition est armée Partielle, seuls les points intérieurs configurés en tant que points de détection déclenchent la tonalité de détection lorsqu'ils sont en défaut. Les points de périmètre signalent les défauts en tant qu'alarmes ou problèmes.
Si ce paramètre Détection automatique est défini sur Manuel et si le mode de détection est activé alors que la partition est armée (Tout activé ou Partielle), le mode de détection est activé lorsque la partition est désarmée (désactivée).

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Détection automatique

5.1.10 Durée de redémarrage

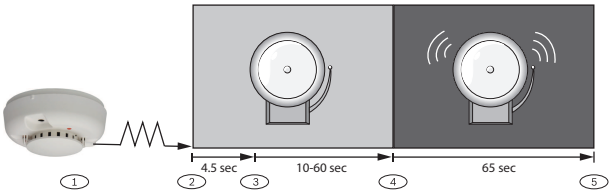
Valeur par défaut : 5
Choix : 5 à 55 (secondes), (par incréments de 1 seconde)
Définissez la durée du délai de stabilisation des détecteurs après qu'un point de vérification d'alarme soit en défaut et que la réinitialisation du détecteur ait réappliqué de la puissance aux détecteurs.
La vérification d'alarme est une fonction des systèmes de détection et d'alarme incendie qui permettent de réduire les fausses alarmes lorsque des détecteurs signalent des conditions d'alarme pendant une période minimum, ou qui permettent de confirmer des conditions d'alarme au cours d'une période donnée après réinitialisation, afin d'être acceptée en tant que signal d'initiation d'alarme valide. La vérification d'alarme s'applique également aux points gaz.

Remarque!
N'activez pas la fonction de point de croisement dans les profils de point qui sont désignés pour les points incendie et gaz.

Remarque!
Consultez la durée de stabilisation dans la fiche technique du détecteur et entrez une valeur d'au moins 5 secondes supérieure à la durée la plus longue spécifiée par un détecteur de la boucle.

Remarque!
Vérifiez les réglementations locales en vigueur afin de déterminer la durée de vérification maximum autorisée.

Les points de vérification d'alarme sont programmés individuellement pour activer la fonction de vérification. Consultez *Profils de point, page 206*. Tout point incendie ou gaz réinitialisable peut activer la vérification d'alarme pour la partition à laquelle il est lié. Bosch recommande d'utiliser des sorties de vérification d'alarme de partition séparées.
Pour activer la vérification d'alarme sur un point, définissez Type de Point sur Incendie ou Gaz, et Vérification d'alarme et Réinitialisable sur Oui.
Lorsqu'un point de vérification d'alarme est en défaut, la centrale retire automatiquement l'alimentation sur tous les points réinitialisables connectés à la sortie Réinitialiser les détecteurs des partitions. L'alimentation est retirée pendant 4,5 secondes. Lorsque l'alimentation est de nouveau appliquée, la centrale ignore les alarmes des points réinitialisables pendant la durée programmée dans Durée de redémarrage. Après expiration de la durée de redémarrage, une période de confirmation de 65 secondes commence. Si le point de vérification d'alarme est toujours en alarme, ou est de nouveau en défaut pendant la période de confirmation, ou si un autre point de vérification d'alarme dans la partition est en défaut, une alarme est générée.



Légende - Description
1 : le détecteur détecte un événement possible.
2 : alimentation retirée des points réinitialisables.
3 : alimentation appliquée de nouveau aux points réinitialisables. La durée de redémarrage commence.
4 : la période de confirmation commence. Toute alarme pendant cette période est indiquée.
5 : la période de confirmation se termine. La séquence est réinitiée la prochaine fois qu'un point de vérification d'alarme est en défaut.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Durée du redémarrage

5.1.11 Contrainte activée

Valeur par défaut : Non
Choix :
- Oui : activer l'alarme sous contrainte pour cette partition.
- Non : désactiver l'alarme sous contrainte pour cette partition.

Remarque!
Exigence SIA CP-01
Pour être en conformité avec la norme SIA CP-01, définissez ce paramètre sur Oui.

Si un utilisateur utilise la commande Déplacer pour déplacer le clavier vers une partition où ce paramètre est défini sur Non, un code de désarmement sous contrainte valide n'envoie pas de rapport sous contrainte. Si vous définissez le paramètre sur Non dans une partition spécifique, le code que vous entrez normalement pour la contrainte n'est plus valide dans cette partition. Si ce paramètre est défini sur Non, et si un code avec l'autorité de désarmement appropriée est utilisé pour désarmer sous contrainte la partition, AUCUNE AUTORITÉ s'affiche sur l'écran du clavier.

Pour obtenir de plus amples informations
Pour une description de la contrainte, consultez *Type de contrainte, page 84*

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Contrainte activée

5.1.12 Type de partition

Valeur par défaut : Régulier
Choix :

Régulier : armé et désarmé indépendamment des autres partitions.
Principal : avant d'armer une partition principale, les partitions associées avec le même numéro de compte que la partition principale doivent présenter la même temporisation de sortie, ou être armées Tout activée Temporisée. Plusieurs partitions principales peuvent partager un numéro de compte.
Associer : un numéro de compte partagé lie les partitions associées aux partitions principales. Les partitions associées peuvent être armées et désarmées indépendamment des autres partitions associées avec le même numéro de compte et la partition principale.
Partagé : les partitions partagées ne sont pas liées aux autres partitions par numéro de compte. Elles s'arment lorsque toutes les partitions associées dans la centrale sont armées Tout activée Temporisée. Les partitions partagées se désarment lorsqu'au moins une partition associée dans la centrale n'est pas armée Tout activée Temporisée (armée Partielle ou désarmée).

Armement des partitions principales et associées
Lors de l'armement d'une partition principale lorsque les partitions associées ne sont pas armées, un message de vérification de partition s'affiche.
Une partition principale peut être désarmée quel que soit l'état armé des autres partitions du compte.

Remarque!
La portée du clavier affecte l'armement principal.
L'armement d'une partition principale depuis un clavier avec le paramètre Portée du clavier défini sur Lié à la centrale ou Lié au compte, démarre la temporisation de sortie de toutes les partitions associées (avec le même numéro de compte).

Remarque!
Pour utiliser une planification pour l'armement d'une partition principale, utilisez d'abord des planifications pour armer des partitions associées
Le recours à la planification d'armement exige que vous utilisiez d'abord un horaire d'armement pour armer les partitions associées avant d'utiliser une planification d'armement pour armer la partition principale.

Remarque!
RPS, un interrupteur à clé ou la fonction Fermeture automatique arment les partitions principales sans associer des partitions en cours d'armement
L'armement de partitions principales à l'aide de RPS, d'interrupteurs à clé ou de la fonction Fermeture automatique n'exige pas que toutes les partitions associées soient armées.

Armement de partitions partagées et associées
L'armement de toutes les partitions associées arme les partitions partagées. Dès que la dernière partition associée est armée, la partition partagée commence à s'armer automatiquement en utilisant la temporisation de sortie de la partition à laquelle le clavier est lié.
Les partitions partagées ne peuvent pas être armées à l'aide d'un code, d'une carte, d'un interrupteur à clé, d'une planification ou de RPS.
Les partitions partagées se désarment automatiquement lorsqu'une partition associée sur la centrale est désarmée. Les partitions partagées ne peuvent pas être désarmées par code, carte, interrupteur à clé ou RPS.

Remarque!
Les commandes d'armement nécessitent une portée de niveau centrale
Les commandes d'armement destinées à une partition partagée doivent être exécutées sur un clavier avec une portée de niveau centrale par un utilisateur disposant d'une autorité sur toutes les partitions associées.

Lorsqu'une partition partagée n'est pas prête pour l'armement
Si un point est en défaut dans la partition partagée, [VÉRIFIER PARTITION] s'affiche sur le clavier pour la dernière partition associée à armer.

Remarque!
La portée de clavier de la partition associée doit inclure des partitions partagées
Pour afficher les points en défaut d'une partition partagée au niveau des claviers d'une partition associée, les partitions partagées et associées doivent partager le même numéro de compte. La portée des claviers liés aux partitions associées doit inclure les partitions partagées.

Armement forcé d'une partition partagée
Lorsque le clavier affiche [VÉRIFIER PARTITION], appuyez sur la touche SUIVANT jusqu'à ce que l'invite Forcer l'armement ? s'affiche. Une pression sur la touche ENTRÉE arme la partition partagée si l'utilisateur a le droit d'inhiber des points, si le point est inhibable, et si le nombre de points en défaut ne dépasse pas la valeur de Forcer armement max pour la partition partagée.

Affichage de l'état armé d'une partition partagée
Pour afficher l'état armé d'une partition partagée, utilisez la commande [AFFICHER LE STATUT DE LA PARTITION]. Les utilisateurs doivent disposer d'un niveau d'autorité lié à la partition partagée.

Rendre silencieux les alarmes et les défauts dans les partitions partagées
Les utilisateurs peuvent rendre les alarmes et les défauts silencieux dans les partitions partagées depuis n'importe quel clavier. Les utilisateurs doivent disposer d'un niveau d'autorité lié à la partition partagée.

Lecteurs de contrôle d'accès liés aux partitions partagées
Si la partition d'entrée est armée et est une partition partagée, la temporisation de sortie redémarre et permet à un utilisateur d'accéder à une partition associée et de désarmer. Si le lecteur de carte lié à la partition partagée comprend des partitions associées dans la portée D## KP# (dans la section CONTRÔLE DES ACCÈS), la partition associée et la partition partagée se désarment lors de la présentation de la carte.

Rapports de fermeture pour les partitions partagées
Pour les rapports de fermeture des partitions partagées, les utilisateurs doivent disposer d'un niveau d'autorité valide attribué à la partition partagée.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Type de partition

5.1.13 Règle de présence de deux personnes ?

Valeur par défaut : Non
Choix :
Oui : pour désarmer la partition, deux codes différents doivent être saisis sur le même clavier.

Non : la saisie d'un code désarme la partition.

Remarque!
Exigence SIA CP-01
Pour être en conformité avec la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Non pour toutes les partitions activées. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Utilisez ce paramètre dans une partition désarmée depuis Tout activé à l'aide de claviers avec une *Portée, page 123*. Un événement d'alarme se déclenche si la temporisation d'entrée se termine avant que l'utilisateur entre le second code.
Si la sirène d'alarme de partition se déclenche, la saisie du premier code rend l'alarme silencieuse. La saisie du second code désarme la partition.
Si le second code est saisi sur un clavier différent de celui utilisé pour le premier code, le second clavier informe l'utilisateur que la règle de présence de deux personnes est active, et que les deux codes doivent être saisis sur le même clavier.
Vous pouvez créer une fonction personnalisée qui désarme la partition à l'aide d'un désarmement par code.
Définissez ce paramètre sur Oui sur les sites qui nécessitent un niveau de sécurité plus élevé pour accéder à la partition sécurisée. Par exemple, une banque peut activer ce paramètre pour l'accès à la chambre forte.
Si ce paramètre est activé, définissez le paramètre *Portée, page 123* pour les claviers des partitions liées sur « Lié à la partition ».
Ne définissez pas le paramètre Règle de présence de deux personnes sur Oui dans une partition pour laquelle le paramètre *Contrainte en avance ?, page 109* est défini sur Oui.
Cette fonction n'est opérationnelle que lorsque vous utilisez le désarmement par code.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Règle de présence de deux personnes

5.1.14 Contrainte en avance ?

Valeur par défaut : Non
Choix :
Oui - après désarmement de la partition, un relais sous contrainte active et envoie un rapport sous contrainte si un deuxième code valide n'est pas entré au cours de la période Arrêt avec 2 codes.
Non - une saisie unique du code avec un niveau d’autorité valide peut désarmer la partition.

Remarque!
Exigence SIA CP-01
Pour être en conformité avec la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Non pour toutes les partitions activées. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Ce paramètre contrôle le désarmement d’une partition sans contrainte. Un rapport sous contrainte est automatiquement envoyé si un deuxième code de désarmement valide n’est pas entré au cours de la période définie dans *Délai pour contrainte en avance, page 88*.
Le premier code entré désarme la partition ; le deuxième code entré valide le désarmement.
Les codes peuvent être identiques et peuvent être saisis à partir de 2 claviers de la partition.

Vous pouvez configurer un deuxième code contrainte à l'aide du paramètre *Deuxième code Contrainte , page 88*. Cette fonction n'est opérationnelle que lorsque vous utilisez le désarmement par code.

Remarque!
Règle de présence de deux personnes
Ne définissez pas le paramètre Contrainte en avance sur Oui dans une partition pour laquelle le paramètre *Règle de présence de deux personnes ?, page 108* est défini sur Oui.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Contrainte en avance

5.1.15 Durée Incendie et Gaz

Valeur par défaut : 6
Choix : 0 à 90 (minutes)
Entrez la durée en minutes pendant laquelle la sirène incendie s'active pour les points d'alarme incendie et gaz. La valeur de 0 minute demeure en sortie jusqu'au rétablissement.

Remarque!
Vérifier les réglementations locales en vigueur
Vérifiez les réglementations locales en vigueur pour confirmer la durée de sirène appropriée pour l'installation.

La sortie activée pour cette durée est programmée dans la sirène incendie A#. La sirène gaz A## est complètement indépendante de la sirène incendie A##, mais elle suit également le délai programmé à cette invite. La sortie de sirène démarre dès que l'alarme incendie se déclenche. Elle éteint la sirène lorsque le nombre programmé de minutes est écoulé. Définissez ce paramètre sur au moins deux minutes.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Durée incendie et gaz

5.1.16 Modèle incendie

Valeur par défaut : Impulsion
Choix :
- Continu : sortie stable.
- Impulsion : durée de l'impulsion. 60 battements par minute à un rythme régulier (0,5 seconde activé et 0,5 seconde désactivé).
- Norme californienne : audible 10 secondes + silence de 5 secondes + audible 10 secondes + silence de 5 secondes.
- Code temporel 3 : actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 1,5 secondes.

Sélectionnez le modèle utilisé par cette partition pour les alarmes sur un point incendie. Les modèles se répètent jusqu'à expiration de la durée d'incendie.
Les modèles se répètent pendant un minimum de 3 minutes avec une tolérance de temps de ± 10 %.
(Les normes 1999 NFPA autorisent le mode silencieux automatique tel que permis par les réglementations locales en vigueur et indiquent une durée minimum de sonnerie de 5 minutes.)

Remarque!
Deux points qui partagent une sortie dans une alarme
Lorsque deux points incendie partageant la même sortie passent en mode alarme, le modèle de sirène de l'événement incendie le plus récent est prioritaire.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Modèle incendie

5.1.17 Durée intrusion

Valeur par défaut : 6
Choix : 0 à 90 (minutes)
Entrez la durée en minutes pendant laquelle la sirène d'alarme s'active pour les points d'alarme intrusion. La valeur de 0 minutes demeure en sortie jusqu'au rétablissement.

Remarque!
Contacter l'autorité locale
Contactez l'autorité locale compétente pour connaître la temporisation de sirène appropriée pour l'installation.

Remarque!
SIA CP-01
Pour être en conformité avec la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur 6 minutes ou plus dans toutes les partitions activées. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

La sortie *Sirène d'alarme, page 146* A# s'active lorsque l'alarme intrusion se déclenche. Elle s'arrête à l'expiration de l'alarme intrusion.
Définissez ce paramètre sur un minimum de deux minutes.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Durée intrusion

5.1.18 Modèle intrusion

Valeur par défaut : Continu
Choix :
- Continu : sortie stable.
- Impulsion : durée de l'impulsion. 60 battements par minute à un rythme régulier (0,5 seconde activé et 0,5 seconde désactivé).
- Norme californienne : audible 10 secondes + silence de 5 secondes + audible 10 secondes + silence de 5 secondes. Se répète jusqu'à expiration de la durée de la sirène incendie.
- Code temporel 3 : actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 1,5 secondes. Se répète jusqu'à expiration de la durée de la sirène.

Sélectionnez le modèle de sirène utilisé par cette partition pour les alarmes sur les points non incendie. Les modèles se répètent jusqu'à expiration de la durée d'intrusion.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Modèle intrusion

5.1.19 Modèle gaz

Valeur par défaut : Code temporel 4
Choix :

- Continu : sortie stable
- Impulsion : durée de l'impulsion. 60 battements par minute à un rythme régulier (0,5 seconde activé et 0,5 seconde désactivé).
- Norme californienne : audible 10 secondes + silence de 5 secondes + audible 10 secondes + silence de 5 secondes.
- Code temporel 3 : actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 1,5 secondes.
- Code temporel 4 :0,1 seconde actif, 0,1 seconde inactif, 0,1 seconde actif, 0,1 seconde inactif, 0,1 seconde actif, 0,1 seconde inactif, 0,1 seconde actif, 5 secondes inactif.

Sélectionnez le modèle de sirène utilisé par cette partition pour les alarmes sur un point gaz. Les modèles se répètent jusqu'à expiration de la durée d'incendie.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Modèle gaz

5.1.20 Une seule sonnerie

Valeur par défaut : Non
Choix :

- Oui : après un événement d'alarme, les événements d'alarme suivants sur les points non incendie dans la même partition pendant la même période armée, n'activent pas la sortie de sirène.
- Non : la sortie de sirène s'active pour chaque événement d'alarme.

Une seule sonnerie n'a aucune incidence sur la tonalité d'alarme du clavier et elle n'empêche aucun rapport.
Les points incendie ne sont pas liés et l'heure de la sirène redémarre à chaque nouvelle alarme.
Le fait de rendre la sirène silencieuse réinitialise le paramètre Une seule sonnerie.

Remarque!
L'interrupteur à clé n'efface pas le paramètre Une seule sonnerie
Si une alarme se déclenche sur un point 24 heures, alors que la partition est désarmée, l'armement de cette partition avec un interrupteur à clé ne réinitialise par le paramètre Une seule sonnerie.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Une seule sonnerie

5.1.21 Test de sirène

Valeur par défaut : non
Choix :

– Oui : dans le cadre d'un test de sirène, activer la sortie de sirène d'alarme pendant deux secondes après la réception de l'accusé de réception du récepteur du centre de télésurveillance pour le rapport de fermeture (ou à la fin de la temporisation de sortie pour les centrales qui n'envoient pas de rapports de fermeture).
– Non : le test sirène est désactivé.

Remarque!
Test sirène pour tous les armements Activation totale uniquement
La fonction Test sirène ne fonctionne que lorsque la partition est armée sur Tous activés.
La fonction Test sirène ne fonctionne pas lorsque la zone est armée Partielle.

Test sirène après le rapport de fermeture
Pour les partitions configurées pour l'envoi de rapports d'ouverture et de fermeture, la sortie de la sirène d'alarme s'active pendant deux secondes lorsque la centrale reçoit l'accusé de réception d'un rapport de fermeture depuis le récepteur du centre de télésurveillance.
Lorsque ce paramètre Test sirène est défini sur Oui, ne configurez pas la partition pour les ouvertures et les fermetures restreintes, ou les périodes d'ouverture et de fermeture.

Test sirène après temporisation de sortie
Lorsque ce paramètre Test sirène est défini sur Oui et que la partition n'est pas configurée pour l'envoi de rapports d'ouverture et de fermeture, la sortie de la sirène d'alarme s'active pendant deux secondes lorsque le temps de sortie est écoulé.

Armement de plusieurs partitions en même temps
Lors de l'armement de plusieurs partitions en même temps (à l'aide de la fonction ARMER TOUTES LES PARTITIONS ?, par exemple), la centrale envoie simultanément des rapports de fermeture pour chaque partition au récepteur du centre de télésurveillance. Le test de sirène se produit lorsque la centrale reçoit l'accusé de réception pour chaque rapport.
Si les rapports de fermeture ne sont pas envoyés, et si toutes les partitions ont la même la temporisation de sortie, la sortie de sirène d'alarme s'active pendant deux secondes pour chaque partition, avec une pause de deux secondes entre chacune d'elles.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Test de sirène

5.1.22 O/F de compte

Valeur par défaut : Non
Choix :
– Oui : envoyer des rapports d'ouverture et de fermeture par compte pour cette partition.
– Non : ne pas envoyer des rapports d'ouverture et de fermeture par compte.

La centrale envoie un rapport de fermeture de compte lorsque la dernière partition du compte est fermée (armée).
La centrale envoie un rapport d'ouverture de compte lorsque la première partition d'un compte est ouverte (désarmée).
Une fois le rapport d'ouverture de compte envoyé, le désarmement des autres partitions du compte ne génère pas un autre rapport d'ouverture de compte. Les rapports d'ouverture et de fermeture de compte ne contiennent pas d'informations de partition.
Définissez ce paramètre de la même manière pour toutes les partitions du compte.
Confirmez que le numéro de compte est le même pour toutes les partitions du compte.

Si une ouverture ou fermeture de compte est générée alors qu'une période d'ouverture ou de fermeture de compte est en vigueur pour cette partition, et si le paramètre *Désactiver O/F dans la période, page 114* est défini sur Oui, le rapport n'est pas envoyé. Bosch recommande que toutes les partitions partageant le même numéro de compte utilisent les mêmes périodes d'ouverture et de fermeture.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > O/F de compte.

5.1.23 O/F de partition

Valeur par défaut : Oui
Choix :

- Oui : inclure les informations de partition dans les rapports d'ouverture et de fermeture pour cette partition. Envoyez les rapports pour les partitions individuellement.
- Non : aucun rapport d'ouverture et de fermeture de partition pour cette partition.

Lorsque ce paramètre est défini sur Oui et que le paramètre *O/F de compte, page 113* est défini sur Non, les rapports d'ouverture et de fermeture incluent des informations de partition. La centrale envoie des rapports pour les partitions individuelles.
Si le paramètre O/F de compte est défini sur Oui, la centrale envoie un rapport de fermeture de compte (aucune information de partition) lorsque la dernière partition avec le même numéro de compte est armée. La centrale envoie un rapport d'ouverture de compte (aucune information de partition) lorsque la première partition avec le même numéro de compte est désarmée.
Ne définissez pas ce paramètre sur Oui si la centrale envoie les rapports à un système d'automatisation qui ne peut pas interpréter plusieurs rapports d'ouverture/de fermeture de partition.
Les rapports d'ouverture/de fermeture sont uniquement envoyés avec des *Niveaux d'autorité, page 179* attribués comme
suit :

- Prêt pour armement : ouverture/fermeture de partition = E
- Non prêt pour armement (Forcer armement/inhibition max) : ouverture/fermeture restreinte = E
- Partielle armée : ouverture/fermeture Partielle = E

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > O/F de partition

5.1.24 Désactiver O/F dans la période

Valeur par défaut : Oui
Choix :

- Oui : ne pas envoyer de rapports d'ouverture et de fermeture au centre de télésurveillance si l'événement d'ouverture ou de fermeture se produit à l'intérieur d'une période active.
- Non : envoyer des rapports d'ouverture et de fermeture au centre de télésurveillance même lorsqu'un événement d'ouverture ou de fermeture se produit à l'intérieur d'une période programmée.

Si ce paramètre est défini sur Oui et qu'un événement d'ouverture ou de fermeture se produit en dehors d'une période, la centrale envoie le rapport d'ouverture ou de fermeture avec un modificateur précoce ou tardif. Se reporter aux périodes O/F

Si ce paramètre est défini sur Non et qu'un événement d'ouverture ou de fermeture se produit en dehors de la période appropriée, la centrale n'inclut pas des modificateurs précoces ou tardifs avec les rapports d'ouverture ou de fermeture.
Les événements d'ouverture et de fermeture sont toujours consignés.
Si vous voulez surveiller toutes les activités d'ouverture et de fermeture, mais que vous souhaitez utiliser les fonctions fournies par les périodes d'ouverture et de fermeture, définissez ce paramètre sur Non et programmez des périodes O/F.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Désactiver O/F dans la période

5.1.25 Fermeture automatique

Valeur par défaut : Non
Choix :
- Oui : la partition s'arme automatiquement Tout activée Temporisée en fin de période de fermeture. Lorsque la partition s'arme automatiquement, la centrale envoie un rapport de fermeture si les rapports de partition et/ou de compte sont programmés pour cela.
- Non : ne pas armer automatiquement la partition en fin de période de fermeture.

Quelle que soit la valeur des paramètres *Forcer armement/inhibition max, page 103* ou *Inhibable, page 233*, un armement forcé inconditionnel a lieu avec comme conséquence des points en défaut laissés hors du système. Pour plus de détails sur le retour de ces points au service, consultez *Forcer armement retournable, page 232* ou *Inhibition retournable, page 232*.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Fermeture automatique

5.1.26 Échec d'ouverture

Valeur par défaut : Non
Choix :
- Oui : la centrale alarme envoie un rapport Échec d'ouverture si la partition n'est pas désarmée à l'heure de Fin de période d'ouverture.
- Non : des rapports Échec d'ouverture ne sont pas envoyés pour cette partition.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Échec d'ouverture

5.1.27 Échec de fermeture

Valeur par défaut : Non
Choix :
- Oui : la centrale envoie un rapport Échec de fermeture si la partition n'est pas armée à l'heure de Fin de la période de fermeture.
- Non : des rapports Échec de fermeture ne sont pas envoyés pour cette partition.

Il n'est pas nécessaire de programmer des rapports d'ouverture et de fermeture pour l'envoi de rapports Échec de fermeture.
Une durée de temporisation de sortie doit être programmée dans *Durée de la temporisation de sortie, page 104*.
Si le paramètre *Fermeture automatique, page 115* est défini sur Oui, un rapport est envoyé à l'heure d'arrêt de la période de fermeture.

Si le paramètre *Désactiver O/F dans la période, page 114* est défini sur Oui, le rapport Échec de fermeture est suivi d'un rapport Fermeture tardive ou Fermeture tardive forcée.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Échec de fermeture

5.1.28 Heure de fermeture la plus tardive

Par défaut : Désactivé
Choix :
– Désactivé - la fonctionnalité est désactivée pour cette zone.
Utilisez Heure de fermeture la plus tardive avec la fonctionnalité *Étendre la fermeture, page 260* pour limiter l'extension de l'heure de fermeture d'une zone. Par exemple, si l'heure de fermeture la plus tardive est définie sur 19:30, vous ne pouvez prolonger l'heure de fermeture attendue que jusqu'à 19:29.
Si le paramètre Heure de fermeture la plus tardive est défini sur une valeur différente de zéro, l'heure du jour spécifiée dans le paramètre *Début de la période de fermeture, page 251* ne peut pas être postérieure ou égale à celle du paramètre Heure de fermeture la plus tardive. Par exemple, si le paramètre Heure de fermeture la plus tardive est défini sur 17:30, le paramètre Début de la période de fermeture ne peut pas être défini sur 17:30 ou une heure postérieure.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Heure de fermeture la plus tardive

5.1.29 O/F restreinte

Valeur par défaut : Non
Choix :
– Oui : restreindre les rapports d'ouverture et de fermeture pour cette partition
– Non : ne pas restreindre les rapports d'ouverture et de fermeture pour cette partition.
Lorsque ce paramètre est défini sur Oui, les rapports d'ouverture sont envoyés uniquement lorsque la partition est désarmée après une alarme incendie/gaz. Les rapports de fermeture sont envoyés uniquement lorsque la partition est armée Tout activé avec des points en défaut.
Séquence de rapports générée par une fermeture restreinte : Armement forcé, Point forcé, Fermeture forcée, Rapport de fermeture.
Si aucun code n'est nécessaire pour l'activation du système, les rapports de fermeture sont toujours restreints lorsque le paramètre O/F restreinte est défini sur Oui. Si un code est nécessaire pour l'activation du système, l'utilisateur doit également disposer d'un *Niveaux d'autorité, page 179* avec ouverture/fermeture restreinte = E (activé) afin que les rapports d'ouverture/de fermeture puissent être restreints.
Le paramètre *O/F de partition, page 114* doit être défini sur Oui pour générer des rapports d'ouverture et de fermeture restreints.
Les périodes d'ouverture/de fermeture actives n'empêchent pas les rapports d'ouverture et de fermeture restreints. Les désignations Précoce ou Tardif ne sont pas ajoutées aux rapports d'ouverture/de fermeture lorsque ceux-ci sont envoyés en fonction de règles pour les rapports d'ouverture/de fermeture restreints.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > O/F restreinte

5.1.30 O/F de Partielle

Valeur par défaut : Non

Choix :

– Oui : envoyer des rapports d'ouverture et de fermeture pour Partielle Instantané et Partielle Temporisée.
– Non : ne pas envoyer de rapports d'ouverture et de fermeture pour Partielle Instantané et Partielle Temporisée.

Les rapports d'ouverture et de fermeture Partielle ne sont pas supprimés par Périodes d'ouverture/de fermeture.

Emplacement dans le menu RPS

Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > O/F de Partielle

5.1.31 Redémarrage de la temporisation de sortie

Valeur par défaut : Oui

Choix :

Oui : activer le redémarrage de la temporisation de sortie

Non : désactiver le redémarrage de la temporisation de sortie.

La fonction de redémarrage de la temporisation de sortie redémarre la temporisation de sortie lorsqu'un utilisateur entre de nouveau dans les locaux avant expiration de la temporisation de sortie.

Par exemple, un propriétaire active (arme) son système, part et ferme la porte, puis réalise qu'il a oublié de prendre les clés de voiture. Lorsqu'il ouvre la porte pour récupérer ses clés, la centrale redémarre la temporisation de sortie, en donnant suffisamment de temps au système pour qu'il se désactive.

Si ce paramètre est défini sur Oui, la procédure suivante permet de redémarrer la temporisation de sortie (*Durée de la temporisation de sortie, page 104*) :

1. Activez le système sur Tout activé ou Partielle.
2. Neutralisez et restaurez un point (ouvrir et fermer une porte) lié à un profil de point configuré pour le type de point, Partielle, et une réponse du point d'alarme différée (4, 5, 6, 7 ou 8). (*Profils de point, page 206*, *Type de point, page 207*, *Réponse du point, page 213*)
3. Avec une temporisation de sortie toujours en cours, mettez en défaut un point (ouvrir une porte) lié à un profil de point configuré pour le type de point, Partielle, et une réponse du point d'alarme différée (4, 5, 6, 7 ou 8). La temporisation de sortie redémarre.

Remarque!

La temporisation de sortie redémarre une seule fois

La temporisation de sortie peut uniquement être redémarrée une fois. Si le même point est de nouveau en défaut, ou si un point différent est mis en défaut dans la temporisation de sortie redémarrée, la temporisation ne redémarre pas une seconde fois.

Emplacement dans le menu RPS

Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Redémarrage de la temporisation de sortie

5.1.32 Tous activés - Aucune sortie

Valeur par défaut : Oui

Choix :

Oui : la centrale commute l'armement de Tout activée Temporisée sur Partielle Temporisée si aucun point Partielle Temporisée n'est mis en défaut et restauré pendant la durée de la temporisation de sortie.
Non : la centrale ne commute pas l'armement.
L'état armé final est signalé et affiché sur les claviers.
Lors de l'armement depuis une télécommande ou une PLANIFICATION, la centrale ignore cette option.

Remarque!
Utilisation du réarmement automatique de la partition (temporisation d'activation)
Définissez le paramètre Activation totale - Aucune sortie sur Non pour une partition lors de l'utilisation du réarmement automatique.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Tous activés - Aucune sortie

5.1.33 Avertissement de temporisation de sortie

Valeur par défaut : Non
Choix :
- Oui : activer et désactiver l'impulsion de sortie d'alarme toutes les deux secondes pendant les 10 dernières secondes de la temporisation de sortie.
- Non : ne pas activer l'impulsion de sortie d'alarme pendant la temporisation de sortie

Remarque!
Exigence SIA CP-01
Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Oui. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Avertissement de temporisation de sortie

5.1.34 Avertissement de temporisation d'entrée

Valeur par défaut : Non
Choix :
- Oui : activer et désactiver l'impulsion de sortie d'alarme toutes les deux secondes pendant les 10 dernières secondes de la temporisation d'entrée.
- Non : ne pas activer l'impulsion de sortie d'alarme pendant la temporisation d'entrée.

Remarque!
Exigence SIA CP-01
Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Oui. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Avertissement de temporisation d'entrée

5.1.35 Durée de réarmement de partition

Valeur par défaut : 00:00

Choix : 00:00 (désactivé) à 23:59
Ce paramètre définit la durée (hh : mm) pendant laquelle une partition désarmée temporise jusqu'à ce qu'elle se réarme sur Tout activée Temporisée.
Par exemple, si le paramètre Durée de réarmement de partition est défini sur quatre heures (04:00) et que la partition est désarmée (désactivée) à 13:30, elle se réarme sur Tout activée Temporisée à 17:30. Tous les points non prêts pour armement (en défaut) sont armés de force.

Remarque!
Le paramètre Forcer armement / inhibition max est ignoré lors du réarmement
Tous les points non prêts pour armement (en défaut) sont armés de force lorsque la partition se réarme en fin de Durée de réarmement de partition.

La partition se réarme automatiquement à 23:59 quelle que soit l'heure à laquelle le temporisateur de réarmement de partition a démarré.
Par exemple, si le temporisateur de réarmement de partition est défini sur 4 heures (04:00) et que la partition est désarmée (désactivée) à 22:30, la partition se réarme sur Tout activée Temporisée à 23:59 (1 heure et 29 minutes après le désarmement).
Les utilisateurs peuvent utiliser Étendre l'heure de fermeture depuis un clavier système pour étendre une temporisation de réarmement de partition active
(Menu Actif/Inactif > Étendre l'heure de fermeture).

Remarque!
La configuration d'une période de fermeture et d'une durée de réarmement de partition peut entraîner un comportement de partition inattendu.
Lorsqu'une période de fermeture et d'une durée de réarmement de partition sont configurées pour la même partition,
la période de fermeture s'exécute simultanément avec le temporisateur de réarmement de partition,
et un utilisateur utilise Étendre l'heure de fermeture depuis un clavier système,
la centrale étend uniquement la période de fermeture, et non la durée de réarmement de partition.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Durée de réarmement de partition

5.1.36 Durée environnementale

Valeur par défaut : 6
Choix : 0 à 90 (minutes)
Entrez la durée en minutes pendant laquelle la sirène d'alarme s'active pour les points d'alarme environnementaux. La valeur de 0 minutes demeure en sortie jusqu'au rétablissement.

Emplacement du menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Durée environnementale

5.1.37 Schéma environnemental

Valeur par défaut : Continu
Choix :
– Continu : sortie stable

- Impulsion : durée de l'impulsion. 60 battements par minute à un rythme régulier (0,5 seconde activé et 0,5 seconde désactivé).
- Norme californienne : audible 10 secondes + silence de 5 secondes + audible 10 secondes + silence de 5 secondes.
- Code temporel 3 : actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 1,5 secondes.
- Code temporel 4 :0,1 seconde actif, 0,1 seconde inactif, 0,1 seconde actif, 0,1 seconde inactif, 0,1 seconde actif, 0,1 seconde inactif, 0,1 seconde actif, 5 secondes inactif.

Sélectionnez le modèle de sirène utilisé par cette partition pour les alarmes sur un type de point Environnemental. Les modèles se répètent jusqu'à expiration de la durée environnementale.

Emplacement du menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Modèle environnemental

5.2 Texte de l'armement de partition

Le B6512 prend en charge jusqu'à 6 partitions.

5.2.1 Texte du nom de partition

Valeur par défaut : n° de partition
Choix : jusqu'à 32 caractères de texte, nombres, espaces et symboles
Entrez un nom de partition pour l'affichage au niveau des claviers.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Texte de l'armement de partition > Texte du nom de partition

5.2.2 Texte Le compte est actif

Valeur par défaut : Vide
Choix : jusqu'à 32 caractères.
Entrez le texte à afficher sur le clavier pour chaque partition si nécessaire.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Texte de l'armement de partition > Texte Le compte est actif

5.2.3 Texte La partition n° est active

Valeur par défaut : Vide
Choix : jusqu'à 32 caractères.
Entrez le texte à afficher sur le clavier pour chaque partition si nécessaire.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Texte de l'armement de partition > Texte La partition n° est active

5.2.4 Texte La partition n° n'est pas encore prête

Valeur par défaut : Vide
Choix : jusqu'à 32 caractères.
Entrez le texte à afficher sur le clavier lorsque la partition n'est pas prête pour l'armement.

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Texte de l'armement de partition > Texte La partition n° n'est pas encore prête

5.2.5 Texte La partition n° est désactivée

Valeur par défaut : Vide
Choix : jusqu'à 32 caractères.
Entrez le texte à afficher sur le clavier lorsque la partition est désactivée (désarmée).

Emplacement dans le menu RPS
Paramètres liés à la partition > Paramètres de partition/sirène, Options d'ouverture/de fermeture > Texte de l'armement de partition > Texte La partition n° est désactivée

6 Claviers

6.1 Affectations de clavier

La centrale B6512 prend en charge les claviers SDI2 1 à 12.
Le clavier B940W est une partie du clavier B942. En raison des différences matérielles du clavier, certaines fonctionnalités de programmation RPS ne s'appliquent pas au clavier B940W :

Fonction de programmation	B940W	B942
Lecteur de proximité	Non disponible	Disponible
Entrées et sorties intégrées	Non disponible	Disponible
Détecteur de présence	Non disponible	Disponible
Alimentation requise	Veille : 250 mA Alarme : 365 mA	Lecteur de proximité désactivé : – Veille : 200 mA ; alarme : 300 mA Lecteur de proximité activé : – Veille : 300 mA ; alarme : 400 mA

6.1.1 Nom du clavier (première langue)

Valeur par défaut : n° de clavier
Choix : jusqu'à 32 caractères
Entrez jusqu'à 32 caractères de texte, nombres et symboles pour décrire le clavier.
Les claviers affichent les 20 premiers caractères. Lorsque plus de 20 caractères sont utilisés, le clavier fait défiler l'intégralité du texte sur l'écran une fois. Pour faire défiler le texte de nouveau, appuyez sur la touche [ÉCHAP].
Les espaces comptent comme du texte et ils sont inclus dans la limite de 32 caractères.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Nom du clavier

6.1.2 Nom du clavier (deuxième langue)

Valeur par défaut : vide
Choix : jusqu'à 32 caractères
Entrez jusqu'à 32 caractères de texte, nombres et symboles pour décrire le clavier.
Les claviers affichent les 20 premiers caractères. Lorsque plus de 20 caractères sont utilisés, le clavier fait défiler l'intégralité du texte sur l'écran une fois. Pour faire défiler le texte de nouveau, appuyez sur la touche [ÉCHAP].
Les espaces comptent comme du texte et ils sont inclus dans la limite de 32 caractères.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Nom du clavier (deuxième langue)

6.1.3 Type de clavier

Valeur par défaut :
– Adresse 1 = Clavier B92x deux lignes
– Toutes les autres adresses = Aucun clavier installé
Choix :

- Aucun clavier installé
- Clavier de base B91x
- Clavier à deux lignes B92x
- Clavier de type Distributeur de billets B93x
- Clavier écran tactile B94x

Sélectionnez le type du clavier connecté à la centrale à cette adresse. Le paramètre Type de Clavier est configuré automatiquement lors de l'installation initiale du clavier.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Type de Clavier

6.1.4 Affectation de partition

Valeur par défaut : 1 (partition 1) (pour toutes les adresses KP)
Choix :
- B6512 : 1 à 6

Sélectionnez une partition à lier au clavier.
Si vous avez créé des noms spécifiques pour le paramètre, ce nom s'affiche comme <*Numéro index*> : <*nom descriptif*> dans la sélection de paramètre.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Affectation de partition

6.1.5 Langue du clavier

Valeur par défaut : Première langue, suivre Langue utilisateur
Choix :
- Première langue, suivre Langue utilisateur
- Première langue, ignorer Langue utilisateur
- Seconde langue, suivre Langue utilisateur
- Seconde langue, ignorer Langue utilisateur

Sélectionnez une langue pour le clavier.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Langue du clavier

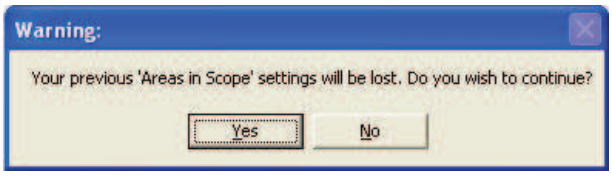
6.1.6 Portée

Valeur par défaut :
- Adresse 1 : Lié à la centrale
- Toutes les autres adresses : Lié à la partition

Choix :
- Lié à la partition : le clavier affiche uniquement des informations et des fonctions d'armement/désarmement pour la partition à laquelle il est lié.
- Lié au compte : le clavier permet d'afficher des informations et des fonctions d'armement/de désarmement pour les partitions qui partagent le même numéro de compte. Généralement utilisé pour le type de partition associée.
- Lié à la centrale : un clavier de centrale permet d'afficher des informations et d'exécuter les fonctions d'armement/de désarmement pour toutes les partitions couvertes par la centrale. Généralement utilisé avec une partition principale.
- Personnalisé : pour une portée personnalisée, vous sélectionnez les partitions dans la portée.

La portée détermine les partitions qui peuvent être affichées depuis le clavier, qui sont incluses lors de l'armement depuis le clavier, et le clavier vers lequel elles peuvent être déplacées.

Chaque fois que Personnalisé est sélectionné, RPS affiche la fenêtre d'avertissement suivante :



Si vous sélectionnez Oui, les partitions dans la portée sont réinitialisées à leur valeur par défaut.
Si vous cliquez sur Non, aucune modification n'est effectuée.

Pour obtenir de plus amples informations
Numéro de compte, page 102
Type de partition, page 106
Partitions dans la portée, page 124

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Portée

6.1.7 Partitions dans la portée

Valeur par défaut :
- Adresse 1 : Tous
- Toutes les autres adresses : Partition1

Choix :
- Cliquez sur un n° de partition pour sélectionner ou désélectionner une partition
- Cliquez sur Tous pour sélectionner toutes les partitions.
- Cliquez sur Désélectionner tout pour désélectionner toutes les partitions (aucune sélection).

Double-cliquez pour afficher et sélectionner des partitions.
Cliquez sur les partitions à inclure dans la portée Personnalisée pour ce clavier.

Pour obtenir de plus amples informations
Portée, page 123

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Partitions dans la portée

6.1.8 Le code suit la portée ?

Valeur par défaut : Oui
Choix :
- Oui : lorsque la partition à laquelle le clavier est lié est armée, la saisie d'un code désarme la partition et toutes les autres partitions incluses dans la portée du clavier. Lorsque la partition est désarmée, celle-ci ainsi que les autres partitions incluses dans la portée du clavier sont armées.
- Non : la saisie d'un code arme ou désarme uniquement la partition à laquelle est lié le clavier.

Le paramètre Le code suit la portée s'applique à l'armement par code uniquement. Il s'applique aux fonctions d'armement de la liste de fonctions.
Les utilisateurs doivent être liés à un niveau d'autorité avec les paramètres Armement par code et Désarmement par code activés.

Pour obtenir de plus amples informations
Portée, page 123

Partition, page 202
Armement par code, page 194
Désarmement par code, page 195

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Le code suit la portée

6.1.9 Entrer clé de sortie

Valeur par défaut : 0 (Non affecté)
Choix :
- 1 à 3, 9 à 96 : affecte une sortie pour les paramètres Fonction de saisie du code, Cycle de sortie.
- 0 : aucune sortie liée aux paramètres Fonction de saisie du code, Cycle de sortie.

Lorsque le paramètre *Fonction de saisie de code, page 125* est défini sur Cycle de sortie, et qu'un utilisateur entre son code et appuie sur [Entrée], Entrer clé de sortie s'active pendant 10 secondes. Deux événement sont ajoutés au journal de la centrale : Sortie ### définie avec ID utilisateur et Sortie ### réinitialisée sans ID utilisateur.

Remarque!
Ne partagez pas Entrer clé de sortie avec d'autres fonctions de sortie
La sortie que vous attribuez dans ce paramètre Entrer clé de sortie ne doit être liée à aucune autre fonction de sortie. Il peut en résulter un fonctionnement de sortie erroné.

Vous pouvez utiliser les paramètres Fonction de saisie du code, Cycle de porte et Entrer clé de sortie pour une gâche de contrôle d'accès de bas niveau sur une porte. Il n'y a pas de shuntage de point.

Pour obtenir de plus amples informations
Fonction de saisie de code, page 125
Si vous avez créé des noms spécifiques pour le paramètre, ce nom s'affiche comme <*Numéro index*> : <*nom descriptif*> dans la sélection de paramètre.

Emplacement dans le menu RPS
Claviers > Affectations de clavier >Entrer clé de sortie

6.1.10 Fonction de saisie de code

Valeur par défaut : Armer/Désarmer
Choix :
- Armer/Désarmer : lorsque la partition en cours est désarmée, la saisie de code + [ENTRÉE] démarre l'armement Tout activée Temporisée pour toutes les partitions dans la portée des utilisateurs. Si la partition en cours est armée, toutes les partitions dans la portée des utilisateurs sont désarmées.
- Cycle de porte : la saisie d'un code + [ENTRÉE] effectue un cycle de contrôleur de cycle programmé dans lier une porte # pendant la durée de la gâche, puis exécute les fonctions d'armement (désarmement, par exemple) et des fonctions personnalisées en fonction du niveau d'autorité de l'utilisateur.
- Cycle de sortie : la saisie d'un code + [ENTRÉE] active le paramètre Entrer clé de sortie pendant 10 secondes.
- Réarmer automatiquement : si la partition liée au clavier est armée Tout activée Temporisée, la saisie d'un code + [ENTRÉE] redémarre la temporisation de sortie. Lorsque la partition est désarmée, la saisie d'un code + [ENTRÉE] n'arme pas.

– Connexion uniquement : la saisie d'un code + [ENTRÉE] connecte l'utilisateur. La double authentification ne s'applique pas.
– Connexion/Désarmement : la saisie d'un code + [ENTRÉE] connecte l'utilisateur et désarme toutes les partitions dans la portée des utilisateurs. La double authentification ne s'applique pas.

La saisie d'un code avec autorité dans la partition en cours rend toujours les alarmes et les défauts silencieux.

Remarque!
Utilisation du réarmement automatique de la partition (temporisation d'activation)
Définissez le paramètre Activation totale - Aucune sortie sur Non pour une partition lors de l'utilisation du réarmement automatique.

Lorsque la Fonction de saisie du code ne peut pas être exécutée en raison de conflits de configuration, la centrale exécute la fonction Armement/Désarmement quel que soit le paramètre.
Le code de service (ID utilisateur 0) ne peut pas être utilisé pour les Fonctions de saisie du code.
Les sorties utilisées pour la fonction de sortie Cycle ne doivent être partagées avec aucune autre fonction de point, de réinitialisation de capteur, de centrale ou de sirène. Le partage peut provoquer des erreurs de fonctionnement de sortie.

Remarque!
Double authentification non compatible avec le réarmement automatique
Si le paramètre Double authentification est défini sur Oui, ne définissez pas ce paramètre Fonction de saisie du code sur Réarmer automatiquement.

Remarque!
Exigence SIA CP-01
Pour être en conformité avec la norme SIA CP-01 Réduction des fausses alarmes, conservez la valeur par défaut de ce paramètre.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Fonction de saisie du code

6.1.11 Double authentification

Valeur par défaut : Non
Choix :

– Oui : les utilisateurs doivent entrer un code **et** présenter un badge (carte ou clé) devant un lecteur de carte ou un clavier à écran tactile B94X pour l'armement, le désarmement et les fonctions utilisateur protégées par mot de passe.
– Non : les utilisateurs entrent un code **ou** présentent un badge (carte ou clé) devant un clavier à écran tactile B94X.

Remarque!
Double authentification non compatible avec le réarmement automatique
Si ce paramètre Double authentification est défini sur Oui, ne définissez pas le paramètre Fonction de saisie du code sur Réarmer automatiquement.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Double authentification

6.1.12 Durée de la double authentification

Valeur par défaut : 20 secondes

Choix : 10, 15, 20, 25, 30, 35, 40, 45 secondes

Lorsque le paramètre Double authentification est activé, les utilisateurs doivent entrer un code **et** présenter un badge (carte ou clé) pendant ce laps de temps.

Emplacement dans le menu RPS

Claviers > Affectations de clavier > Durée de la double authentification

6.1.13 Lier une porte

Valeur par défaut : 0 (Aucune porte)

Choix :

- Aucune porte : aucun contrôleur de porte n'est lié au clavier.
- Porte 1 à Porte 4 : lier un contrôleur de porte au clavier en sélectionnant son numéro.

Sélectionnez le contrôleur de porte (Porte ##) utilisé par le clavier pour l'ajout de cartes/clés et l'affichage Fermer la porte.

Lorsque ce paramètre lier une porte est défini sur Aucune porte, NON PRÊT s'affiche sur le clavier lorsque les utilisateurs essaient d'ajouter un utilisateur. Jusqu'à ce qu'un contrôleur de porte soit lié, les utilisateurs ne peuvent pas utiliser le clavier pour lier des cartes/clés à l'aide de la commande Ajouter/Modifier un utilisateur.

Lorsqu'aucun contrôleur de porte n'est lié au clavier, les utilisateurs peuvent contrôler les portes à l'aide des fonctions CONTRÔLE DE LA PORTE.

La définition du paramètre lier une porte sur Non désactive :

- l'option Cycle de porte de la Fonction de saisie du code
- l'option Ajouter une carte de la commande Ajouter/Modifier un utilisateur
- la double authentification

Si vous avez créé des noms spécifiques pour le paramètre, ce nom s'affiche comme <*Numéro index*> : <*nom descriptif*> dans la sélection de paramètre.

Emplacement dans le menu RPS

Claviers > Affectations de clavier > lier une porte

6.1.14 Tonalité de défaut

Valeur par défaut :

- Oui : centrales B9512G/B8512G

Choix :

- Oui : les tonalités de défaut liées à la centrale sont émises et des affichages visuels s'affichent sur ce clavier.
- Non : aucune tonalité n'est émise pour les défauts liés à la centrale, mais des affichages visuels s'affichent encore sur ce clavier.

Les tonalités de défaut liées à la centrale concernent l'alimentation, le téléphone, le bus SDI et le bus SDI2. Elles n'incluent pas les défauts de point ou les sonneries de panne.

Emplacement dans le menu RPS

Claviers > Affectations de clavier > Tonalité de défaut

6.1.15 Tonalité d'entrée

Valeur par défaut : Oui

Choix :

- Oui : ce clavier émet une tonalité d'entrée pendant la temporisation d'entrée.
- Non : ce clavier n'émet de pas de son pour la tonalité d'entrée.

La mise en défaut d'un point de temporisation dans la portée de partition du clavier démarre la temporisation d'entrée.
Pour supprimer la tonalité d'entrée par point, définissez Points > Profil de point > *Tonalité d'entrée désactivée, page 227* sur Oui.
Définissez ce paramètre sur Oui pour les installations UL.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Tonalité d'entrée

6.1.16 Tonalité de sortie

Valeur par défaut : Oui
Choix :
- Oui : ce clavier émet un son pour la tonalité de sortie pendant la temporisation de sortie.
- Non : ce clavier n'émet pas de son pour la tonalité de sortie.

L'armement à partir d'un clavier qui a une portée d'armement de la partition démarre la temporisation de sortie.
Pour supprimer la tonalité de sortie par partition, définissez le paramètre Lié à la partition > Tonalité de sortie sur Non.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Tonalité de sortie

6.1.17 Tonalité d'avertissement d'armement de la partition

Valeur par défaut : Oui
Choix :
- Oui : au début de la période de fermeture, le clavier émet une tonalité et affiche un avertissement.
- Non : ce clavier n'émet pas de tonalité et n'affiche pas d'avertissement.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Tonalité d'avertissement d'armement de la partition

6.1.18 Tonalité d'avertissement de fermeture de porte

Valeur par défaut : Oui
Choix :
- Oui : lorsqu'une porte est maintenue ouverte au-delà de la durée de shuntage, le clavier émet une tonalité d'avertissement et affiche Fermer la porte.
- Non : ce clavier n'active pas une tonalité d'avertissement et n'affiche pas Fermer la porte.

Le paramètre Accès/Porte/*Durée d'extension, page 272* défini pour la porte liée au clavier dans le paramètre *Lier une porte, page 127* doit être défini sur une valeur supérieure à zéro.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Tonalité d'avertissement de fermeture de porte

6.1.19 Arrêt de défilement inactif

Valeur par défaut : Non
Choix :
- Oui : lorsque le clavier est inactif, il ne fait pas défiler automatiquement le texte des événements d'alarme ou de défaut rendus silencieux.
- Non : autoriser le défilement automatique du texte.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Arrêt de défilement inactif

6.1.20 Verrouillage de fonction

Valeur par défaut : Non
Choix :
– Oui : après avoir appuyé sur la touche Inhibition, Menu ou Raccourcis, les utilisateurs doivent entrer un code pour continuer.
– Non : aucun code n'est nécessaire pour continuer.

Lorsque ce paramètre est défini sur Oui, les utilisateurs sont invités à entrer un code après avoir appuyé sur la touche Inhibition, Menu ou Raccourcis. Les éléments programmés dans la liste de fonctions pour ce clavier sont filtrés en fonction du niveau d'autorité de l'utilisateur. Seuls les éléments de la liste de fonctions pour lesquels l'utilisateur dispose d'une autorité sont affichés.
Si ce paramètre est défini sur Non, lorsque l'utilisateur appuie sur la touche Inhibition, Menu ou Raccourcis, tous les éléments qui sont programmés dans la liste de menus pour l'adresse de clavier s'affichent, quel que soit le niveau d'autorité de l'utilisateur.

Remarque!
Claviers incendie D1256 et modules de signalisation incendie D1257
Si vous utilisez un clavier incendie D1256 et un module de signalisation incendie D1257, Bosch vous recommande de ne pas définir le paramètre Verrouillage de fonction sur Oui. Le paramètre Oui invite l'opérateur à saisir un code. Le clavier incendie D1256 ne dispose d'aucune touche pour saisir ce code.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Verrouillage de fonction

6.1.21 Affichage d'interruption

Valeur par défaut : Oui
Choix :
– Oui : ce clavier affiche ALARME NON ENVOYÉE si une alarme intrusion est interrompue avant l'envoi d'un rapport d'alarme.
– Non : ce clavier n'affiche pas ALARME NON ENVOYÉE.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Affichage d'interruption

6.1.22 Affichage d'annulation

Valeur par défaut : Oui
Choix :
– Oui : ce clavier affiche ALARME ANNULÉE lorsqu'une alarme intrusion est annulée.
– Non : ce clavier n'affiche pas ALARME ANNULÉE.

Si ce paramètre est défini sur Oui, le paramètre Lié à la centrale/Divers/*Rapports d'annulation, page 85* doit être défini sur Oui.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Affichage d'annulation.

6.1.23 Activation de l'éclairage nocturne

Valeur par défaut : Non
Choix :

– Oui : le rétroéclairage de l'écran et du clavier sont définis au niveau minimum lorsque le clavier est inactif.
– Non : le rétroéclairage de l'écran et du clavier sont désactivés lorsque le clavier est inactif.

Lorsque ce paramètre est défini sur Oui, les utilisateurs peuvent activer ou désactiver la fonction d'éclairage nocturne au niveau du clavier.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Activation de l'éclairage nocturne

6.1.24 Luminosité de l'éclairage nocturne

Valeur par défaut : 2
Choix :
– 0 : éclairage nocturne désactivé
– 1 à 6 : plus le nombre est élevé, plus l'éclairage nocturne est lumineux.

Ce paramètre définit le niveau de luminosité de la fonction Éclairage nocturne.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Luminosité de l'éclairage nocturne

6.1.25 Rendre silencieuse la tonalité de pression de touche

Valeur par défaut : Non
Choix :
– Oui : le clavier passe en mode silencieux lorsque les touches sont utilisées.
– Non : le clavier émet une tonalité de pression des touches lorsque l'utilisateur appuie sur une touche.

Lorsque ce paramètre est défini sur Non, les utilisateurs ne peuvent pas désactiver la tonalité des touches.
Lorsque ce paramètre est défini sur Oui, les utilisateurs ne peuvent pas activer la tonalité des touches.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Rendre silencieuse la tonalité de pression de touche

6.1.26 Afficher la date et l'heure

Valeur par défaut : Non
Choix :
– Oui : le clavier affiche la date et l'heure.
– Non : le clavier n'affiche pas la date et l'heure.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Afficher la date et l'heure

6.1.27 Volume du clavier

Valeur par défaut : 7
Choix : 0 à 7
0 est le volume le plus faible.
7 est le volume le plus élevé.
Les tonalités à priorité élevée, comme la tonalité d'alarme, émettent toujours un son au volume maximal.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Claviers > Volume du clavier

6.1.28 Luminosité du clavier

Valeur par défaut : 6

Choix : 0 à 6

0 : l'écran du clavier est plus sombre.

6 : l'écran du clavier est plus lumineux.

Les utilisateurs peuvent définir la luminosité du clavier sur le clavier.

Emplacement dans le menu RPS

Claviers > Affectations de clavier > Luminosité du clavier

6.1.29 Désactiver le détecteur de présence

Valeur par défaut : Non

Choix :

- Oui : désactiver le détecteur de présence.
- Non : lorsque le détecteur de présence détecte un mouvement à proximité du clavier, ce dernier éclaire l'écran sombre.

Seuls les claviers à écran tactile B94x disposent de la fonction de détecteur de présence.

Emplacement dans le menu RPS

Claviers > Affectations de clavier > Désactiver le détecteur de présence

6.1.30 Désactiver le lecteur de clé

Valeur par défaut : Oui

Choix :

- Oui : désactiver le lecteur de clé.
- Non : activer le lecteur de clé.

Seuls les claviers à écran tactile B94x disposent de la fonction Lecteur de clé.

La désactivation du lecteur de clé permet de réduire la consommation électrique.

Emplacement dans le menu RPS

Claviers > Affectations de clavier > Désactiver le lecteur de clé

6.1.31 Activer le contact d'auto-surveillance

Valeur par défaut : Non

Choix :

- Oui : activer le contact d'auto-surveillance.
- Non : désactiver le contact d'auto-surveillance.

Ce paramètre s'applique uniquement aux claviers SDI au clavier B915.

Emplacement dans le menu RPS

Claviers > Affectations de clavier > Activer le contact d'auto-surveillance

6.1.32 Option du bouton de fonction

Valeur par défaut : sélection de la langue

Choix :

- Sélection de la langue : les utilisateurs appuient sur le bouton pour basculer entre la première et la seconde langues de la centrale.
- Mémoire d'événement : les utilisateurs appuient sur le bouton pour accéder rapidement à la mémoire d'événement et la consulter.

Ce paramètre permet de configure le bouton de fonction dans l'angle supérieur gauche du clavier à écran tactile B94x.

Emplacement dans le menu RPS
Claviers > Affectations de clavier SDI2 > Option du bouton de fonction

6.1.33 Supervision

Valeur par défaut : Oui
Choix :
- Oui : cette adresse de clavier est supervisée. Ne connectez qu'un seul clavier SDI défini à cette adresse.
- Non : cette adresse de clavier n'est pas supervisée. Vous pouvez connecter plusieurs claviers SDI définis à cette adresse.

Ce paramètre s'applique uniquement aux claviers SDI. Les claviers SDI2 sont toujours supervisés.
Le paramètre *Type de clavier, page 122* doit être défini sur un clavier SDI.
Lorsque ce paramètre est défini sur Oui et qu'un problème se produit au niveau du clavier ou du bus SDI, la centrale crée un événement DÉFAUT SDI ##.
Les claviers incendie SDI D125xRB sont supervisés, même lorsque ce paramètre est défini sur Non.
Les claviers SDI partageant le même paramètre d'adresse affichent le même texte et émettent les mêmes tonalités lorsque des touches sont utilisées sur un d'eux.
Les événements Défaut SDI sont toujours pour la Partition 1, Compte 1 quelle que soit la partition à laquelle le dispositif SDI est lié.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Supervision

6.1.34 Options [Échap] du code

Valeur par défaut :
- Non pour le clavier 1 (clavier SDI2) et Oui pour tous les autres.

Choix :
- Oui - la saisie d'un code suivi de la touche [Échap] rend les alarmes actives silencieuses. Si les alarmes reconnues s'affichent, la saisie du code plus [Échap] efface les alarmes à l'écran.
- Non - la saisie d'un code et la pression de la touche [Échap] efface le dernier chiffre du code. En continuant d'appuyer sur [Échap], les chiffres sont effacés un à la fois. Lorsqu'il ne reste aucun chiffre, la pression de la touche [Échap] permet de quitter la tâche.

Remarque!
PARAMÈTRES LIÉS À LA CENTRALE > Divers > Longueur du code doit être défini sur Désactivé
Lorsque PARAMÈTRES LIÉS À LA CENTRALE > Divers > Longueur du code est défini sur 3 chiffres, 4 chiffres, 5 chiffres ou 6 chiffres, le paramètre Options [Échap] du code est désactivé, même lorsqu'il défini sur Oui.
Lorsque Options [Échap] du code est défini sur Oui, vous devez définir PARAMÈTRES LIÉS À LA CENTRALE > Divers > Longueur du code sur Désactivé.

Remarque!
Exigences de la norme UL 985 relative aux unités d'alarme incendie de maison familiale
Configurez ce paramètre sur Yes (nécessite un code) pour répondre aux exigences UL 985.

Emplacement dans le menu RPS
Claviers > Affectations de clavier > Options [Échap] du code

6.2 Paramètres globaux de clavier

6.2.1 Réponse de la touche A

Valeur par défaut : Aucune réponse
Choix :
- Aucune réponse : tonalité de touche non valide.
- Alarme incendie manuelle : crée un événement d'alarme incendie lorsque des utilisateurs maintiennent enfoncées les touches A et 1 en même temps pendant 2 secondes, ou lorsque des utilisateurs appuient sur CMD, puis sur 7 (Commande 7).
- Fonction personnalisée : exécute la fonction personnalisée sélectionnée lorsque des utilisateurs maintiennent la touche A enfoncée pendant 2 secondes. Utilisez le paramètre Fonction personnalisée de la touche A pour sélectionner la fonction personnalisée.
  La sélection d'une fonction personnalisée ne concerne pas les claviers à écran tactile B942.

Lorsque ce paramètre est défini sur Alarme incendie manuelle, un événement d'alarme se produit chaque fois que l'utilisateur appuie sur les touches appropriées, que les alarmes précédentes aient ou non été effacées de l'écran.

Remarque!
Alarme incendie manuelle inclut CMD-7, définissez le paramètre Niveau d'autorité/ Commande utilisateur 7 sur « E »
Si le paramètre Réponse de la touche A est défini sur Alarme incendie manuelle, CMD-7 (Commande 7) est également configuré pour l'alarme incendie manuelle lorsque des utilisateurs appuient sur CMD + 7.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Réponse de la touche A.

Se reporter à
- *Emplacement dans le menu RPS, page 227*

6.2.2 Fonction personnalisée de la touche A

Valeur par défaut : Désactivé
Choix :
- B6512G : Désactivé, Fonction 128 à Fonction 133

Sélectionnez la fonction personnalisée qui s'exécute lorsque les utilisateurs maintiennent la touche A enfoncée pendant 2 secondes.
Le paramètre Réponse de la touche A doit être défini sur Fonction personnalisée.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Fonction personnalisée de la touche A

6.2.3 Réponse de la touche B

Valeur par défaut : Aucune réponse
Choix :
- Aucune réponse : tonalité de touche non valide.

- Alarme médicale manuelle, aucune sortie d'alarme : crée un événement d'alarme médicale lorsque des utilisateurs maintiennent les touches B et 4 enfoncées en même temps pendant 2 secondes. La sortie d'alarme n'est **pas** activée pour l'événement d'alarme médicale.
- Alarme médicale manuelle, avec sortie d'alarme : crée un événement d'alarme médicale lorsque des utilisateurs maintiennent les touches B et 4 enfoncées en même temps pendant 2 secondes. La sortie d'alarme est activée pour l'événement d'alarme médicale.
- Fonction personnalisée : exécute la fonction personnalisée sélectionnée lorsque des utilisateurs maintiennent la touche B enfoncée pendant 2 secondes. Utilisez le paramètre Fonction personnalisée de la touche B pour sélectionner la fonction personnalisée.
  La sélection d'une fonction personnalisée ne concerne pas les claviers à écran tactile B942.

Lorsque ce paramètre est défini sur Alarme médicale manuelle, aucune sortie d'alarme ou Alarme médicale manuelle, avec sortie d'alarme, un événement d'alarme se produit chaque fois que l'utilisateur appuie sur les touches appropriées, que les alarmes précédentes aient ou non été effacées de l'écran.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Réponse de la touche B.

6.2.4 Fonction personnalisée de la touche B

Valeur par défaut : Désactivé
Choix :

- B6512G : Désactivé, Fonction 128 à Fonction 133

Sélectionnez la fonction personnalisée qui s'exécute lorsque les utilisateurs maintiennent la touche B enfoncée pendant 2 secondes.
Le paramètre Réponse de la touche B doit être défini sur Fonction personnalisée.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Fonction personnalisée de la touche B

6.2.5 Réponse de la touche C

Valeur par défaut : Aucune réponse
Choix :

- Aucune réponse : tonalité de touche non valide.
- Alarme de panique manuelle, sortie d'alarme silencieuse et invisible : crée un événement d'alarme panique lorsque des utilisateurs maintiennent les touches C et 7 enfoncées en même temps pendant 2 secondes, ou lorsque des utilisateurs appuient sur CMD, puis sur 9 (Commande 9).
  L'événement ne s'affiche **pas** sur l'écran du clavier. La sortie d'alarme **silencieuse** s'active.
- Alarme de panique manuelle, visible avec sortie d'alarme : crée un événement d'alarme panique lorsque des utilisateurs maintiennent les touches C et 7 enfoncées en même temps pendant 2 secondes, ou lorsque des utilisateurs appuient sur CMD, puis sur 9 (Commande 9).
  L'événement s'affiche sur l'écran du clavier. La sortie d'alarme s'active.
- Fonction personnalisée : exécute la fonction personnalisée sélectionnée lorsque des utilisateurs maintiennent la touche C enfoncée pendant 2 secondes. Utilisez le paramètre Fonction personnalisée de la touche C pour sélectionner la fonction

personnalisée.
La sélection d'une fonction personnalisée ne concerne pas les claviers à écran tactile B942.

Lorsque ce paramètre est défini sur Alarme de panique manuelle, sortie d'alarme silencieuse et invisible, ou sur Alarme de panique manuelle, visible avec sortie d'alarme, un événement d'alarme se produit chaque fois que l'utilisateur appuie sur les touches appropriées, que les alarmes précédentes aient ou non été effacées de l'écran.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Réponse de la touche C.

6.2.6 Fonction personnalisée de la touche C

Valeur par défaut : Désactivé
Choix :
– B6512G : Désactivé, Fonction 128 à Fonction 133

Sélectionnez la fonction personnalisée qui s'exécute lorsque les utilisateurs maintiennent la touche C enfoncée pendant 2 secondes.
Le paramètre Réponse de la touche C doit être défini sur Fonction personnalisée.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Fonction personnalisée de la touche C

6.2.7 Alarme silencieuse manuelle, Audible sur défaut de comm.

Valeur par défaut : Non
Choix :
– Oui : la sirène d'alarme s'active lorsqu'un rapport d'alarme silencieuse ne parvient pas à atteindre le centre de télésurveillance au bout de deux tentatives.
– Non : la sirène d'alarme ne s'active **pas** lorsqu'un rapport d'alarme silencieuse ne parvient pas à atteindre un centre de télésurveillance.

Ce paramètre s'applique lorsque la touche C d'un clavier, ou une panique de télécommande RADION, crée des événements d'alarme silencieuse.
Lorsque ce paramètre est défini sur Oui, la sortie Sirène d'alarme s'active pendant la durée de la sirène intrusion moins la durée des deux tentatives d'envoi du rapport d'alarme silencieuse. Le minuteur de sirène intrusion se déclenche lors de la création de l'événement d'alarme silencieuse.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Alarme silencieuse manuelle, Audible sur défaut de comm.

6.2.8 Type de carte

Valeur par défaut : 26 bits
Choix :
26 bits
Corporate 1000 35 bits (B9612G, B8612G, B6612 uniquement)
37 bits

***Code du site, page 165* par défaut pour les types de carte**
26 bits : le code de site par défaut est 255
Corporate 1000 35 bits : le code de site par défaut est 4095 (B9612G, B8612G, B6612 uniquement)

37 bits aucun code de site : le code de site est vide. Le code de site n'est pas configurable (Le paramètre Code de site est grisé).
37 bits avec code de site : le code de site par défaut est 65535 (B9612G, B8612G, B6612 uniquement).

Emplacement dans le menu RPS
Claviers > Paramètres globaux de clavier > Type de carte

6.2.9 Options de défaut de comm.

Valeur par défaut : Les défaut de comm. sont audibles et visibles.
Choix :

- Les défauts de comm. sont silencieux et invisibles : les événements de défaut de communication ne s'affichent pas au niveau des claviers et n'émettent aucune tonalité de défaut.
- Les défauts de comm. sont audibles et visibles : les événements de défaut de communication s'affichent au niveau des claviers et émettent la tonalité de défaut.

Remarque!
Activer une tonalité de défaut pour chaque clavier
Utilisez le paramètre *Tonalité de défaut, page 127* dans les affectations de clavier pour activer les tonalités de défaut liés à la centrale (y compris le défaut de comm.) pour les claviers individuels.

Emplacement dans le menu RPS
Clavier > Paramètres globaux de clavier > Options de son de défaut de comm.

6.3 Paramètres globaux Télécommande radio

6.3.1 Télécommande Fonction personnalisée A

Valeur par défaut : Désactivé
Choix :

- B6512G : Désactivé, Fonction 128 à Fonction 133

Sélectionnez la fonction personnalisée qui s'exécute lorsque des utilisateurs appuient sur le bouton A de fonction sur les télécommandes RADION.

Emplacement dans le menu RPS
Claviers > Paramètres globaux Télécommande radio > Télécommande Fonction personnalisée A

6.3.2 Télécommande Fonction personnalisée B

Valeur par défaut : Désactivé
Choix :

- B6512G : Désactivé, Fonction 128 à Fonction 133

Sélectionnez la fonction personnalisée qui s'exécute lorsque des utilisateurs appuient sur le bouton B de fonction sur les télécommandes RADION.

Emplacement dans le menu RPS
Claviers > Paramètres globaux Télécommande radio > Télécommande Fonction personnalisée B

6.3.3 Options Télécommande Panique

Valeur par défaut : Réponse Panique désactivée

Choix :

- Réponse Panique désactivée : la centrale ignore les pressions sur le bouton panique depuis toutes les télécommandes.
- Réponse de panique audible activée : lorsqu'un utilisateur appuie sur un bouton panique d'un clavier, la centrale crée un événement d'alarme panique, affiche l'alarme et émet la tonalité d'alarme au niveau des claviers, puis active la sortie de sirène d'alarme.
- Réponse de panique silencieuse activée : lorsque des utilisateurs appuient sur un bouton panique d'un clavier, la centrale crée un événement d'alarme silencieuse et active la sortie d'alarme silencieuse. Les claviers restent silencieux et n'affichent pas l'alarme.

Lorsque la sortie de sirène d'alarme est active, le fait de rendre l'alarme silencieuse crée un événement d'annulation.

Lorsque la réponse de panique silencieuse est active, un accusé de réception de l'alarme crée un événement d'annulation.

La fonction Annulation d'alarme ne s'applique pas aux événements d'alarme panique ou d'alarme silencieuse

La centrale ne crée pas d'événements de rétablissement pour les événements d'alarme panique ou d'alarme silencieuse

Emplacement dans le menu RPS

Claviers > Télécommande radio > Options Télécommande Panique

7 Fonctions personnalisées

Utilisez les paramètres de cette section pour configurer les fonctions personnalisées.
La centrale B6512 prend en charge 6 fonctions personnalisées.

7.1 Texte de fonction personnalisée (première langue)

Valeur par défaut : fonction ###
Choix : jusqu'à 18 caractères de texte, nombres, espaces et symboles.
Entrez du texte pour identifier la fonction personnalisée au niveau des claviers.

Emplacement dans le menu RPS
Fonction personnalisée > Texte de fonction personnalisée

7.2 Texte de fonction personnalisée (seconde langue)

Valeur par défaut : (vide)
Choix : jusqu'à 18 caractères de texte, nombres, espaces et symboles.
Entrez du texte pour identifier la fonction personnalisée au niveau des claviers.

Emplacement dans le menu RPS
Fonction personnalisée > Texte de fonction personnalisée (seconde langue)

7.3 Fonctions

Valeur par défaut : Non utilisé

Choix : consultez la liste ci-dessous.
Utilisez ces paramètres Fonction (Fonction 1 à Fonction 6) pour lier jusqu'à six fonctions à une fonction personnalisée.
Double-cliquez sur le champ Fonction 1 (à Fonction 6) pour afficher la boîte de dialogue de sélection de fonction. Certaines fonctions requièrent la configuration de un ou deux paramètres. Par exemple, si vous sélectionnez la fonction Désarmer, vous sélectionnez les partitions à désarmer dans le Paramètre 1.

Remarque!
Lorsqu'une fonction personnalisée démarre, les fonctions liées s'exécutent dans l'ordre, de 1 à 6
La centrale exécute les fonctions liées à une fonction personnalisée de manière consécutive. La centrale démarre les fonctions immédiatement après le démarrage de la fonction précédente. Elle n'attend pas que la fonction précédente se termine.
Utilisez la fonction de temporisation pour créer une temporisation entre le début de deux fonctions. Le paramètre 1 configure la longueur de la temporisation (1 à 90 secondes).
Par exemple, pour activer/désactiver une sortie à la fin d'une temporisation Partielle avec une temporisation de sortie de 30 secondes, définissez la fonction 1 sur « Partielle Temporisée », définissez la fonction 2 sur « Temporisation » avec le paramètre 1 défini sur une valeur supérieure à 30 secondes, et définissez la fonction 3 sur « Activer/Désactiver la sortie ».

Remarque!

Règles Forcer armement / inhibition max spéciales pour l'armement avec des fonctions personnalisées

Lorsqu'une fonction personnalisée comprend une fonction d'armement (Tout activée Temporisée, Tout activé Instantané, Partielle Instantané, Partielle Temporisée), des règles spéciales pour la limite *Forcer armement/inhibition max, page 103* s'appliquent pour les points en défaut.

Si un utilisateur active le paramètre Fonction personnalisée depuis un clavier en utilisant un raccourci ou une touche de fonction, depuis une télécommande radio, ou en présentant son badge (carte ou clé) devant un lecteur ou un clavier,
et si la fonction personnalisée exige un code (*Fonction personnalisée, page 179* = P),
la centrale applique la limite Forcer armement / inhibition max pour les points en défaut. Si le nombre de points en défaut est supérieur à la limite Forcer armement / inhibition max, la fonction échoue et la centrale n'arme pas la partition. Il n'y a aucune indication au niveau des claviers concernant la fonction qui a échoué. La centrale inclut le numéro d'utilisateur dans l'événement d'armement (historique et rapport).

Si un utilisateur active un paramètre Fonction personnalisée depuis un clavier en utilisant un raccourci ou une touche de fonction, depuis une télécommande radio, ou en présentant son badge (carte ou clé) devant un lecteur ou un clavier,
et si la fonction personnalisée n'exige pas un code (*Fonction personnalisée, page 179* = E),
la centrale applique la limite Forcer armement / inhibition max pour les points en défaut. Si le nombre de points en défaut est supérieur à la limite Forcer armement / inhibition max, la fonction échoue et la centrale n'arme pas la partition. Il n'y a aucune indication au niveau des claviers concernant la fonction qui a échoué. La centrale n'inclut pas le numéro d'utilisateur dans l'événement d'armement (historique et rapport).

Si une fonction personnalisée est activée par un horaire, un point ou une automatisation, la centrale n'applique *pas* la limite Forcer armement / inhibition max pour les points en défaut. La centrale arme tous les points en défaut, même si la limite Forcer armement / inhibition max est dépassée.

FONCTION :

Non utilisé : cette fonction est désactivée et aucune fonction après celle-ci ne sera exécutée.

Tout activée Temporisée, page 260
Tout activé Instantané, page 260
Partielle Temporisée, page 260
Partielle Instantané, page 260
Désarmer, page 260
Étendre la fermeture, page 260
Inhiber un point, page 261
Rétablir un point, page 261
Rétablir tous les points, page 261
Réinitialiser les détecteurs, page 140
Activer la sortie, page 261
Désactiver la sortie, page 261
Activer/désactiver la sortie, page 261
Commande instantanée, page 140
Réinitialiser toutes les sorties, page 261
Temporisation, page 140
Cycle de porte, page 140

Déverrouiller la porte, page 261
Verrouiller la porte, page 262
Porte sécurisée, page 262
Niveau de contrôle d'accès, page 262
Événements avec accès octroyé, page 262
Événements avec accès refusé, page 262
RPS de réponse, page 141
Connecter vous à RPS, page 262
Port utilisateur du contact RPS, page 263
Envoyer le rapport de statut, page 263
Envoyer le rapport de test, page 263
Envoyer test même si état anormal, page 265
Accéder à la partition, page 141
Détection activée, page 265
Détection désactivée, page 265
Afficher la date et l'heure, page 265
Émettre tonalité de détection, page 266
Définir le volume du clavier, page 266
Définir la luminosité du clavier, page 266
Rendre le défaut silencieux, page 141
Rendre l'alarme silencieuse, page 141

Emplacement dans le menu RPS
Fonction personnalisée > Fonction 1-6

7.4 Descriptions des fonctions personnalisées

Les fonctions de cette section ne sont pas activées par un horaire et ne sont pas disponibles en tant que *Fonction, page 257* horaire.

7.4.1 Réinitialiser les détecteurs

Cette fonction émule le raccourci clavier Réinitialiser les détecteurs. Lorsqu'elle est activée, cette fonction active la sortie de niveau partition Réinitialiser les détecteurs pendant 5 secondes. Cette fonction désactive la sortie d'alarme pour les partitions sélectionnées dans le paramètre 1 pendant 5 secondes.

7.4.2 Commande instantanée

Cette fonction n'est pas disponible en tant que fonction de raccourci clavier et elle est uniquement disponible en tant que fonction personnalisée. La fonction active la sortie sélectionnée au Paramètre 1 pour le nombre de secondes sélectionné au Paramètre 2.

7.4.3 Temporisation

Utilisez cette fonction pour créer une temporisation configurable (0 à 90 secondes) entre ou avant les fonctions. Le Paramètre 1 configure la temporisation.

7.4.4 Cycle de porte

Cette fonction émule la fonction de raccourci clavier Cycle de porte et est uniquement disponible dans une fonction personnalisée. Cette fonction déverrouille momentanément la ou les portes programmées dans le Paramètre 1 : Porte n°.

7.4.5 RPS de réponse

Cette fonction émule le raccourci clavier RPS de réponse qui demande à la centrale de répondre à la demande suivante de RPS afin d'établir une session via un téléphone ou un réseau. Cette fonction est uniquement disponible dans une fonction personnalisée. Cette période de réponse automatique dure au moins 2 minutes et se substitue aux paramètres d'invite RPS de réponse sur réseau ? et Vérification d'adresse RPS.

7.4.6 Accéder à la partition

Cette fonction émule le raccourci clavier Accéder à la partition et elle est uniquement disponible pour les fonctions personnalisées activées via un clavier. Lorsqu'elle est activée, cette fonction peut remplacer la partition active des claviers par celle programmée au Paramètre 1 : partition n°.

7.4.7 Rendre le défaut silencieux

Cette fonction n'est pas disponible en tant que raccourci clavier, mais elle peut être exécutée depuis n'importe quel clavier ou par d'autres moyens. Lorsqu'elle est activée, cette fonction rend silencieuses toutes les tonalités de défaut et les sonneries système dans les partitions programmées au Paramètre 1 : partition n°.

7.4.8 Rendre l'alarme silencieuse

Cette fonction n'est pas disponible en tant que raccourci clavier, mais elle peut être exécutée depuis n'importe quel clavier ou par d'autres moyens. Lorsqu'elle est activée, cette fonction rend silencieuses toutes les alarmes dans les partitions programmées au Paramètre 1 : partition n°.

8 Menu de raccourcis

8.1 Fonction

Valeur par défaut :

- Élément 1 du menu de raccourcis : Activer toute la partition sélectionnée
- Élément 2 du menu de raccourcis : Désactiver la partition sélectionnée
- Élément 3 du menu de raccourcis : Afficher l'état de point
- Élément 4 du menu de raccourcis : Réinitialiser les détecteurs
- Élément 5 du menu de raccourcis : Modifier le mode de détection
- Élément 6 du menu de raccourcis : Luminosité (SDI2) / Lumineux (SDI)
- Élément 7 du menu de raccourcis : Volume (SDI2) / Atténué (SDI)
- Élément 8 du menu de raccourcis : Afficher le journal
- Éléments 9 à 32 du menu de raccourcis : Éléments désactivés

Choix :

Utilisez ce paramètre pour lier des fonctions aux éléments de menu.

Sélectionnez la fonction dans la liste déroulante de la boîte de dialogue qui s'affiche lorsque vous double-cliquez sur une cellule de la colonne Fonction et en regard de la section Configuration utilisateur.

Toutes les fonctions personnalisées prises en charge sont répertoriées en fonction de leur *Texte de fonction personnalisée (première langue), page 138*.

Il n'existe aucune restriction concernant la fréquence à laquelle vous pouvez lier une fonction spécifique au menu. Ainsi, vous pouvez lier la même fonction sur des claviers différents afin qu'ils apparaissent sur certaines partitions dans un ordre différent de celui où ils apparaissent sur d'autres.

Fonction	Fonction	Fonction
Élément désactivé	Test de détection invisible	Définir l'heure de la centrale
Tout activée Temporisée	Envoyer le rapport de test	Afficher la date et l'heure
Tout activé Instantané	Montrer les révisions	Modifier les planifications
Tout activé Partition sélectionnée	Réponse RPS	Luminosité (SDI2)
Partielle Temporisée	RPS via Réseau	Volume (SDI2)
Partielle Instantané	RPS via le port de changement de réseau	Éclairage nocturne du clavier
Partielle Partition sélectionnée	RPS via le téléphone	Tonalité des touches clavier mode silence
Désactivé	Accéder à la partition	Afficher la mémoire des événements
Désactiver la partition sélectionnée	Mettre à jour le firmware	Effacer la mémoire d'événements
Étendre la fermeture	Afficher la fonction d'inhibition	Afficher le journal
Inhiber un point	Cycle de porte	Alarme à incendie touche A
Rétablir un point	Déverrouiller la porte	Alarme médicale touche B
Afficher le statut de la partition	Verrouiller la porte	Alarme panique silencieuse touche C
Afficher le statut du point	Porte sécurisée	Fonction ### (128 à 133)
Envoyer le rapport de statut	Changer le code	
Réinitialiser les détecteurs	Ajouter un utilisateur	
Modification de l'état de sortie	Modifier un utilisateur	
Test de détection incendie	Supprimer l'utilisateur	
	Changer le mode de détection	
	Définir la date de la centrale	

Fonction	Fonction	Fonction
Test de détection intrusion Test de détection de service		

Emplacement dans le menu RPS
Menu de raccourcis > Fonction
Non utilisé : cette fonction est désactivée et aucune fonction après celle-ci ne sera exécutée.
Tout activée Temporisée, page 260
Tout activé Instantané, page 260
Partielle Temporisée, page 260
Partielle Instantané, page 260
Désarmer, page 260
Étendre la fermeture, page 260
Inhiber un point, page 261
Rétablir un point, page 261
Rétablir tous les points, page 261
Activer la sortie, page 261
Désactiver la sortie, page 261
Activer/désactiver la sortie, page 261
Réinitialiser toutes les sorties, page 261
Déverrouiller la porte, page 261
Verrouiller la porte, page 262
Porte sécurisée, page 262
Niveau de contrôle d'accès, page 262
Événements avec accès octroyé, page 262
Événements avec accès refusé, page 262
Connecter vous à RPS, page 262
Port utilisateur du contact RPS, page 263
Envoyer le rapport de statut, page 263
Envoyer le rapport de test, page 263
Envoyer test même si état anormal, page 265
Détection activée, page 265
Détection désactivée, page 265
Afficher la date et l'heure, page 265
Émettre tonalité de détection, page 266
Définir le volume du clavier, page 266
Définir la luminosité du clavier, page 266
Exécuter la fonction personnalisée, page 266

8.2 Définir/Effacer tout

Valeur par défaut : Définir/Effacer tout
Choix : Adresse 1 à 12
Utilisez ce paramètre pour activer ou désactiver les fonctions à toutes les adresses.

Emplacement dans le menu RPS
Menu de raccourcis > Définir/Effacer tout

8.3 Adresse n°

Valeur par défaut : Oui (Menu de raccourcis 1 à 8)

Choix :

– Oui : inclure dans le menu pour les claviers définis à cette adresse.

– Non : ne pas inclure dans le menu.

Emplacement du menu RPS

Menu raccourci > N° adresse (1 à 32)

9 Sorties

Les sorties de la centrale sont programmées pour fonctionner en fonction d'une série de déclencheurs disponibles pour une partition spécifique ou l'ensemble du système (Niveau centrale). Les sorties fournissent des sorties de contact sec (normalement ouvert/fermé) pour les annonces par voyants et autres applications, ainsi que des sorties à tension (12 Vcc activée/désactivée) de contact sec pour des fonctions de système d'alarme de base (comme la sortie Sirène, Réinitialiser les détecteurs, etc.). Dans certains cas, les sources fonctionnelles pour les sorties peuvent inclure le paramètre Non attribué, également appelé sortie virtuelle, ou une caméra IP.

Type de sortie

- Les sorties liées à la centrale fournissent une sortie relative à une indication « Niveau centrale ». Pour les annonces, ces sorties peuvent être utilisées pour indiquer les défauts de « niveau système » liées à l'alimentation, au téléphone et une synthèse de centrale globale des événements d'alarme, de défaut et de supervision.
- Les sorties de partition sont utilisées pour fournir une sortie « en fonction de la partition » à laquelle est liée la sortie. Une partition peut avoir ses propres indications de sirène et de réinitialisation des détecteurs. Les sorties peuvent aussi être utilisées pour indiquer l'état armé de partition et si un événement anormal, tel qu'un armement forcé, s'est produit.
- Sorties intégrées : sorties d'une tension 12 Vcc intégrées fournissent une alimentation lorsqu'elles sont activées sur la centrale. Ces sorties sont programmées par défaut en usine comme les sorties A(1), B(2) et C(3). En général, la sortie A(1) est utilisée pour la sirène, la sortie B(2) pour une sortie d'alarme secondaire (une autre sirène, par exemple) et la sortie C(3) pour la réinitialisation de détecteurs.
- Les sorties non intégrées liées à la centrale B6512 peuvent contrôler jusqu'à 64 sorties de relais de contact sec de forme « C » lorsque 8 modules huit sorties en option B308 sont installés. Ces sorties sont utilisées pour la sortie de partition, la sortie de niveau centrale et les sorties de défaillance de point individuelles.

Profils de sortie

Les profils de sortie permettent une programmation et des opérations de sortie avancées en permettant à une sortie de fonctionner selon plusieurs types de sorties, y compris Niveau centrale, des déclencheurs de la partition, des états de points, etc. Une fois qu'un profil de sortie est programmé et enregistré, il peut être réutilisé et affecté à plusieurs sorties, ce qui permet une programmation rapide des sorties.

Vous pouvez créer des profils de sortie pour définir le mode de fonctionnement d'une sortie lorsque des événements spécifiques se produisent. Les profils de sortie offrent un moyen d'attribuer et d'utiliser des effets de sortie homogènes sur une centrale, une partition ou un point.

Les profils de sortie contiennent 1 ou 2 déclencheurs qui peuvent inclure des paramètres de portée, de filtre de portée, de modèle, de temporisation et de durée pour produire un effet de sortie spécifique.

Remarque!

Exigences de firmware

Les profils de sortie requièrent un firmware de centrale 3.10 ou plus récent pour fonctionner. Toute autre programmation utilisant la même sortie est ignorée.

Rapports de sortie
Les rapports de sortie sont stockés dans le journal mémoire de la centrale.

Contrôle des sorties
Les sorties peuvent être activées en fonction d'événements qui existent au niveau de la centrale. En outre, les sorties peuvent être contrôlées par l'utilisateur à l'aide de la fonction [MODIFIER SORTIE ?], Planifications Sortie activée/Sortie désactivée et de RPS.
La sortie C est toujours SOUS TENSION. L'affectation d'une autre sortie désactive la sortie C de sorte que cette sortie peut être utilisée pour d'autres fonctions. Lorsque la sortie C est programmée sur Réinitialiser les détecteurs, l'alimentation est toujours fournie par la borne AUX de la centrale et la sortie C offre un chemin à la borne commune. La sortie C désactive la connexion commune lors de la réinitialisation des détecteurs.
Vérifiez l'état de sortie après la reprogrammation ou la réinitialisation de la centrale. Toutes les sorties sont désactivées après la réinitialisation de la centrale. Certaines fonctions de sortie sont vérifiées toutes les minutes par la centrale et elle retournent à un état correct après la réinitialisation. Les autres sorties doivent être définies manuellement à l'état correct à l'aide de la fonction de sortie Changer (MENU 32).
Ces fonctions de sortie retournent à l'état approprié dans un délai d'une minute :

Sirène incendie	Défaut de partition	Défaut de la Partielle
Résumé incendie	Résumé alarme	Défaut secteur
Résumé de défaut	Défaillance du téléphone	Échec de communication
Alarme silencieuse	Mode de détection	Réinitialiser les détecteurs
Résumé de supervision d'incendie	Sirène d'alarme	Défaut de batterie
Résumé défaut d'incendie	Partition armée	Liste des surveillance de point d'intrusion

Ces fonctions de sortie doivent être réinitialisées manuellement à l'aide de la fonction Changer la sortie :

Échec fermeture	Armement forcé
Sous contrainte	Journal % complet

9.1 Sorties liées à la partition

9.1.1 Sirène d'alarme

Valeur par défaut : 1
Choix :
– 0 (désactivé), 1 à 96
Cette sortie s'active lorsqu'un point d'intrusion lié à la partition déclenche une alarme. Il s'active également pour les alarmes de clavier (non incendie) et les alarmes Télécommande qui sont configurées pour la sirène d'alarme.
La sortie s'active pendant la durée entrée au paramètre *Durée intrusion, page 111*. La sortie suit la cadence définie dans le paramètre *Modèle intrusion, page 111*. Le paramètre *Alarme silencieuse, page 150* doit être défini sur Non pour que la sirène se déclenche en cas d'alarme.

Remarque!
Exigence SIA CP-01
Pour vous conformer à la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur une valeur autre que 0 pour chaque partition activée. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Sirène d'alarme

9.1.2 Sirène incendie

Valeur par défaut : 1
Choix :
– 0 (désactivé), 1 à 96

Cette sortie Sirène incendie s'active lorsqu'un point incendie lié à la partition déclenche une alarme. Il s'active également pour les alarmes incendie de clavier et les exercices d'incendie. La sortie s'active pendant la durée entrée au paramètre *Durée Incendie et Gaz, page 110*. La sortie suit la cadence définie au paramètre Modèle incendie.

Remarque!
Exigence UL 864
Pour être en conformité avec la norme UL 864 relative aux systèmes d'applications d'alarme incendie commerciales, programmez ce paramètre avec un relais.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Sirène incendie

9.1.3 Réinitialiser les détecteurs

Valeur par défaut : 3 (SORTIE C)
Choix :
– 0 (désactivé), 1 à 96

La sortie que vous entrez ici s'active pendant 5 secondes lorsque des utilisateurs démarrent la fonction utilisateur Réinitialiser les détecteurs ou pendant un test de détection incendie. Lors de l'affectation d'une sortie Réinitialiser les détecteurs pour au moins deux partitions, vous devez définir les paramètres ci-dessous. À défaut, un événement de défaut peut se produire pour les points *Réinitialisable, page 236*.
– La *Portée, page 123* du clavier doit inclure toutes les partitions qui partagent la sortie.
– Les utilisateurs doivent disposer d'une autorisation pour *Réinitialiser le ou les détecteurs, page 190* dans toutes les partitions qui partagent la sortie.
– Le paramètre *Durée de redémarrage, page 105* doit être défini sur le même nombre de secondes pour toutes les partitions qui partagent la sortie.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Réinitialiser les détecteurs

9.1.4 Échec de fermeture/Partielle armée

Valeur par défaut : 0 (désactivé).
Choix :
– 0 (désactivé), 1 à 96

Lorsque le paramètre Sortie de partition activée est défini sur Non, cette sortie Échec de fermeture/Partielle armée s'active lorsque la période de fermeture de la partition expire. Elle reste activée jusqu'à minuit, jusqu'à ce qu'une autre période de fermeture démarre, ou que la centrale soit réinitialisée.
Lorsque le paramètre Sortie de partition activée est défini sur Oui, cette sortie Échec de fermeture/Partielle armée s'active lorsque toutes les partitions liées à la même sortie sont armées avec Partielle Instantané ou Partielle Temporisée.
Consultez *Sortie de Partielle, page 91*.
Utilisez le paramètre *Armement anticipé de la partition, page 91* pour indiquer si une sortie Partielle Temporisée s'active en début de temporisation de sortie ou en fin de temporisation de sortie. Par défaut, la sortie s'active à la fin de la temporisation de sortie.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Échec de fermeture/Partielle

9.1.5 Armement forcé

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

Cette sortie est s'active lorsque l'armement de cette partition est forcé. Elle reste active jusqu'à ce que la partition soit désarmée ou que la centrale soit réinitialisée. Cette sortie ne s'active pas en cas d'armement forcé Partielle.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Armement forcé

9.1.6 Mode de détection

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

Cette sortie s'active lorsqu'un Point de surveillance est en défaut alors que le Mode de détection est activé et que la partition est désarmée
Les points de détection sont actifs lorsque la réponse du point est vide (aucune réponse). Le type de point doit être 24 heures, Part active ou Intérieur.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Mode de détection

9.1.7 Partition armée

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsque la partition est Tout activé (armée).
Si plusieurs partitions utilisent la même sortie, la sortie s'active lorsque toutes les partitions sont armées. Elle se désactive lorsque la première partition se désarme.
La sortie reste activée jusqu'à ce que la partition soit désactivée (désarmée). La partition ne se désactive pas pendant la temporisation d'entrée.

Utilisez le paramètre *Armement anticipé de la partition, page 91* pour indiquer si la sortie Partition armée s'active en début de temporisation de sortie ou en fin de temporisation de sortie Par défaut, la sortie s'active à la fin de la temporisation de sortie.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Partition armée

9.1.8 Partition désactivée

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie saisie ici s'active lorsque la partition passe de Tout activé (Temporisation ou Instantané) à Partielle ou Désactivée (désarmée).
Si la partition passe de Partielle ou Désactivée à Tout activé, la sortie se désactive.
Si la même sortie est utilisée pour plusieurs partitions, lorsque toutes les partitions sont Tout activé, la sortie est désactivée. Lorsque la première partition passe à Désactivée (désarmée) ou Partielle, la sortie se désactive.
Lorsque le paramètre *Armement anticipé de la partition, page 91* est défini sur Non, cette sortie Partition désactivée ne s'active pas jusqu'à la fin de la temporisation de sortie.
Lorsque le paramètre Armement anticipé de la partition est défini sur Oui, la sortie Partition désactivée se désactive dès le début de la temporisation de sortie et dès que la partition est armée Tout activé.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Partition désactivée

9.1.9 Défaut de partition

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active chaque fois qu'un point Partielle, Intérieur ou Suiveur intérieur est en défaut. La sortie reste active jusqu'à ce que tous les points périmètre et intérieur de la partition ne soient plus en défaut.
Vous pouvez utiliser la sortie Défaut de partition pour indiquer que la partition n'est pas prête pour l'armement.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Défaut de partition

9.1.10 Sortie contrainte

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un utilisateur crée un événement de contrainte au niveau d'un clavier qui est lié à la partition.
La sortie s'active de manière constante pendant la durée entrée au paramètre *Durée intrusion, page 111*. Le paramètre *Modèle intrusion, page 111* n'a aucun effet sur cette sortie.
Le paramètre *Contrainte activée, page 106* doit être défini sur Oui.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Sortie contrainte

9.1.11 Défaut de la Partielle

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point Partielle lié à la partition est en défaut. La sortie s'active quel que soit l'état armé des partitions (Tout activé, Part activée ou Désactivé).
Cette sortie fournit une sortie constante jusqu'à ce que tous les points Partielle de la partition ne soient plus en défaut.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Défaut activation partielle

9.1.12 Alarme silencieuse

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point lié à un profil de point avec le paramètre Sirène silencieuse défini sur Oui déclenche une alarme.
Utilisez cette sortie pour les applications panique/intrusion.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Alarme silencieuse

9.1.13 Sirène gaz

Valeur par défaut : 1
Choix :
– 0 (désactivé), 1 à 96

Cette sortie Sirène gaz s'active lorsqu'un point gaz lié à la partition déclenche une alarme. La sortie s'active pendant la durée entrée au paramètre *Durée Incendie et Gaz, page 110*. La sortie suit la cadence définie au paramètre *Modèle gaz, page 112*.

Emplacement du menu RPS
Sorties > Sorties de niveau partition > Sirène gaz

9.1.14 Sirène environnementale

Valeur par défaut : 0
Choix :
– 0 (désactivé), 1 à 3, 9 à 96
La sortie s'active pendant la durée entrée au paramètre *Durée environnementale, page 119*.
La sortie suit la cadence définie au paramètre *Schéma environnemental, page 119*.

Emplacement du menu RPS
Sorties > Sorties liées à la partition > Sirène environnementale

9.2 Sorties liées de la centrale

9.2.1 Défaut secteur

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsque la centrale crée un événement Défaut secteur. La sortie se désactive lorsque la centrale crée un événement Rétablissement secteur.
La centrale observe le délai d'attente indiqué dans le paramètre *Temps de défaut secteur, page 78* pour les événements Défaut secteur et Rétablissement secteur.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Défaut secteur

9.2.2 Défaut de batterie

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96
La sortie s'active lorsque la tension de batterie est inférieure à 12,1 Vcc, ou lorsque la batterie est manquante. La sortie se réinitialise lorsque l'alimentation de la batterie est restaurée.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Défaut de batterie

9.2.3 Défaillance du téléphone

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsque la centrale crée un événement de défaillance de la ligne téléphonique. La sortie se réinitialise automatiquement lorsque la ligne téléphonique est restaurée.
La centrale observe le délai d'attente indiqué dans le paramètre *Durée de supervision téléphonique, page 32* avant de créer des événements de défaillance de ligne téléphonique et des événements de rétablissement de ligne téléphonique.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Défaillance téléphone

9.2.4 Défaillance comm

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

Lorsqu'il existe un événement Défaillance comm pour un groupe destinataire, la sortie s'active. La sortie se réinitialise lorsqu'un rapport depuis le groupe destinataire est envoyé au récepteur du centre de télésurveillance.
Pour en savoir plus sur les événements Défaillance comm, consultez *Communicateur, vue d'ensemble, page 66*.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Échec de comm.

9.2.5 Journal % complet

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsque le journal atteint le pourcentage de sa capacité défini dans le paramètre Journal % complet. La sortie se désactive lorsque RPS réinitialise le pointeur de journal.
Consultez *Journal % complet, page 81*.

Pour obtenir de plus amples informations
Consultez Obtenir l'historique pour plus d'informations.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Journal % complet (Sorties)

9.2.6 Résumé incendie

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point incendie du système déclenche une alarme. La sortie se désactive lorsque tous les points incendie du système reviennent à la normale et que tous les événements d'alarme incendie sont effacés des écrans de clavier.

Remarque!
Cette sortie Résumé incendie fonctionne uniquement comme décrit lorsque le paramètre *Résumé incendie et gaz, page 87* est défini sur Non.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction Résumé incendie.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé incendie

9.2.7 Résumé alarme

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point non incendie ou non gaz déclenche une alarme. La sortie se désactive lorsque tous les points non incendie et non gaz reviennent à la normale, lorsque toutes les alarmes non incendie et non gaz sont rendues silencieuses et que les événements d'alarme sont effacés des écrans de clavier.

Cette sortie ne s'active pas pour les points invisibles.

Remarque!
N'affectez pas plusieurs fonctions à la sortie associée à cette fonction Résumé alarme.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé alarme

9.2.8 Résumé défaut incendie

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point incendie du système déclenche un défaut. La sortie se désactive lorsque tous les points incendie du système reviennent à la normale et que tous les événements de défaut incendie sont effacés des écrans de clavier.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction de résumé.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé défaut incendie

9.2.9 Résumé de supervision d'incendie

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point de supervision incendie du système déclenche une alarme. La sortie se désactive lorsque tous les points de supervision incendie du système reviennent à la normale et que tous les événements d'alarme de supervision incendie sont effacés des écrans de clavier.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction de résumé.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé de supervision d'incendie

9.2.10 Résumé de défaut

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point non incendie ou non gaz déclenche une condition de défaut. La sortie se désactive lorsque tous les points non incendie et non gaz du système reviennent à la normale et que tous les événements de défaut non incendie et non gaz sont effacés des écrans de clavier.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction de résumé.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé de défaut

9.2.11 Liste des surveillance de point d'intrusion

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point de supervision non incendie/non gaz du système déclenche une alarme. La sortie se désactive lorsque tous les points de supervision non incendie/non gaz du système reviennent à la normale et que tous les événements d'alarme de supervision non incendie/non gaz sont effacés des écrans de clavier.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction de résumé.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé de supervision d'intrusion

9.2.12 Résumé sortie de gaz

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point gaz du système déclenche une alarme. La sortie se désactive lorsque tous les points gaz du système reviennent à la normale et que tous les événements d'alarme gaz sont effacés des écrans de clavier.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction de résumé.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé sortie de gaz

9.2.13 Résumé sortie de supervision de gaz

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96

La sortie s'active lorsqu'un point de supervision gaz du système déclenche une alarme. La sortie se désactive lorsque tous les points de supervision gaz du système reviennent à la normale et que tous les événements d'alarme de supervision gaz sont effacés des écrans de clavier.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction de résumé.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé sortie de supervision de gaz

9.2.14 Résumé de sortie de défaut de gaz

Valeur par défaut : 0 (désactivé)
Choix :
– 0 (désactivé), 1 à 96
La sortie s'active lorsqu'un point gaz du système déclenche un défaut. La sortie se désactive lorsque tous les points gaz du système reviennent à la normale et que tous les événements de défaut gaz sont effacés des écrans de clavier.

Remarque!
N'affectez pas plusieurs fonctions à la sortie liée à cette fonction de résumé.

Emplacement du menu RPS
Sorties > Sorties liées à la centrale > Résumé de sortie de défaut de gaz

9.3 Affectations de sortie

9.3.1 Source de sortie

Valeur par défaut :
– Sortie A(1) : Intégré A
– Sortie B(2) : Intégré B
– Sortie C(3) : Intégré C
– Toutes les autres sorties : Non lié
Choix :
– Intégrée
– Non affecté
– Huit sorties
– Clavier
– Caméra IP
– Alimentation auxiliaire
Utilisez ce paramètre pour lier des numéros de sortie à des sources de sortie (dispositifs physiques). Les choix en grisé ne sont pas disponibles.
Les modules huit sorties B308 comportent des limites de numéro de sortie qui commencent à la Sortie 11.
Pour les caméras IP, utilisez *Entrées-sorties de caméra, page 45* pour vous aider à affecter des points de centrale et des sorties de centrale.

L'utilisation d'une caméra IP comme source de sortie est limitée
Les centrales d'alarme peuvent être configurées pour démarrer les communications avec les caméras IP utilisant jusqu'à 4 affectations de sortie centrale par caméra IP. Les sorties de centrale disponibles sont spécifiques à chaque caméra IP.
Par exemple, pour « Caméra 1 », vous pouvez affecter les sorties de centrale 11-18. Pour « Caméra 2 », vous pouvez attribuer les sorties 21-28, pour « Caméra 4 », vous pouvez affecter les sorties 41-48, et ainsi de suite.
La caméra IP en tant que source de sortie n'est pas disponible pour les sorties 19 à 20, 29 à 30, 39 à 40, 49 à 50, 69 à 96.

Prise en charge de la source de sortie de l'alimentation auxiliaire
L'alimentation auxiliaire est prise en charge sur les sorties de centrale suivantes :
– B6512 : sorties 17 à 18, 27 à 28, 37 à 38, 47 à 48

Emplacement du menu RPS
Sorties > Affectations de sortie > Source de sortie

Se reporter à
– *Entrées-sorties de caméra, page 45*
– *Réglages de commutateur du module huit sorties B308, page 297*

9.3.2 Texte de sortie (première langue)

Valeur par défaut : n° de sortie
Choix : jusqu'à 32 caractères alphanumériques
Entrez une description de la sortie dans la première langue. Les installateurs, le personnel de service et les utilisateurs voient cette description.

Emplacement du menu RPS
Sorties > Affectations de sortie > Texte de la sortie

9.3.3 Texte de sortie (deuxième langue)

Valeur par défaut : Vide
Choix : jusqu'à 32 caractères alphanumériques
Entrez une description de la sortie dans la deuxième langue. Les installateurs, le personnel de service et les utilisateurs voient cette description.

Emplacement du menu RPS
Sorties > Affectations de sortie > Texte de sortie (deuxième langue)

9.3.4 Profil de sortie

Valeur par défaut : Non attribué
Choix :
– Jusqu'à 20 profils
Sélectionnez le profil de sortie à attribuer à une sortie. La sortie fonctionne exclusivement selon la programmation du profil de sortie. Lorsqu'un profil de sortie est affecté à une sortie, les paramètres de déclenchement et de comportement du profil de sortie annulent tout autre paramètre de sortie.
– Utilisez un profil de sortie pour attribuer un comportement de sortie avancé à 1 ou plusieurs sorties.

Contrôle manuel (activé/désactivé) des sorties
Les sorties basées sur des profils de sortie peuvent être activées manuellement (par le biais du clavier ou à distance) et resteront activées.
Désactivez manuellement les sorties pour revenir au fonctionnement automatique.

Pour de plus amples informations
Sorties liées de la centrale, page 151
Sorties liées à la partition, page 146
Points, page 200
Profils de point, page 206

Emplacement du menu RPS
Sorties > Affectations de sortie > Profil de sortie

9.3.5 Masquer pour l'utilisateur

Valeur par défaut : Non
Choix :
– Oui : les claviers, l'application mobile RSC, les interfaces d'automatisation du SDK (telles que Mode 1, Mode 2, SDK, VMS) et l'application mobile BSM ne peuvent pas afficher ou contrôler la sortie.
– No : les claviers, l'application mobile RSC, les interfaces d'automatisation du SDK (telles que Mode 1, Mode 2, SDK, VMS) et l'application mobile BSM peuvent afficher ou contrôler la sortie.

Utilisez ce paramètre pour désactiver l'affichage ou le contrôle des sorties depuis les claviers, RSC, les interfaces d'intégration SDK et l'application mobile BSM.

Emplacement du menu RPS
Sorties > Affectations de sortie > Masquer pour l'utilisateur

9.4 Profils de sortie

9.4.1 Nom de profil

Valeur par défaut : les profils de sortie 1-13 possèdent différentes valeurs par défaut prédéfinies, qui s'affichent dans le tableau. Les profils de sortie 14 et supérieurs sont désactivés sans les paramètres par défaut prédéfinis.
Choix : jusqu'à 32 caractères alphanumériques
Utilisez ce paramètre pour nommer le profil de sortie.
Les profils de sortie contiennent 1 ou 2 déclencheurs qui peuvent inclure des paramètres de portée, de filtre de portée, de modèle, de temporisation et de durée pour produire un effet de sortie spécifique.

Valeurs par défait de profil de sortie pour les profils 1-13

Profil de sortie	Nom de profil	Déclenchement 1	Portée 1	Filtre de portée 1	Schéma	Durée
1	Alarme intrusion, incendie, gaz	Sortie active	Sortie	1 - Sortie A (1)	Allumé en permanence	Suit le déclencheur

Profil de sortie	Nom de profil	Déclenchement 1	Portée 1	Filtre de portée 1	Schéma	Durée
2	Réinitialiser les détecteurs	Sortie active	Sortie	3 - Sortie C (3)	Allumé en permanence	Suit le déclencheur
3	Alarme intrusion	Alarme intrusion	Lié à la centrale	0	Allumé en permanence	Jusqu'à désactivation
4	Alarme Incendie	Alarme Incendie	Lié à la centrale	0	Impulsions demi-seconde	Jusqu'à désactivation
5	Échec fermeture	Échec fermeture	Lié à la centrale	0	Allumé en permanence	Suit le déclencheur
6	Partielle armée	Partielle armée	Lié à la centrale	0	Allumé en permanence	Suit le déclencheur
7	Surveill. active	Surveill. active	Lié à la centrale	0	Allumé en permanence	Suit le déclencheur
8	Tout act. (armé)	Tout act. (armé)	Lié à la centrale	0	Allumé en permanence	Suit le déclencheur
9	Partition désarmée	Partition désarmée	Lié à la centrale	0	Allumé en permanence	Suit le déclencheur
10	Défaut de partition	Défaut de partition	Lié à la centrale	0	Allumé en permanence	Suit le déclencheur
11	Alarme gaz	Alarme gaz	Lié à la centrale	0	Code temporel 4	Jusqu'à désactivation
12	Supervision intrusion (Temps de surveillance)	Supervision intrusion	Lié à la centrale	0	Allumé en permanence	Jusqu'à désactivation
13	Temporisation d'entrée/ de sortie	Temporisation d'entrée/ de sortie	Lié à la centrale	0	Impulsions demi-seconde	Suit le déclencheur

Remarque!
Exigences de firmware
Les profils de sortie requièrent un firmware de centrale 3.10 ou plus récent pour fonctionner. Toute autre programmation utilisant la même sortie est ignorée.

Emplacement du menu RPS
Sorties > Profils de sortie > Nom de profil

9.4.2 Comportement de sortie

Nom du comportement :
– Comportement de sortie [A]
Vous pouvez programmer un profil de sortie avec un comportement de sortie différent. Un comportement de sortie permet de combiner jusqu'à 2 déclencheurs (un type de sortie identique ou différent) afin de générer des effets de sortie spécifiques. Un effet de comportement de sortie correspond à une temporisation, une durée et un diagramme. Chaque déclencheur sélectionné doit être exécuté pour répondre aux conditions de profil de sortie. Une fois satisfaite, toute sortie affectée à ce profil est activée et fonctionne selon le modèle de profil, la temporisation et la durée.

Emplacement du menu RPS
Sorties > Profils de sortie > Comportement de sortie

9.4.3 Déclenchement

Par défaut : Désactivé
Sélections : événements, états ou autres paramètres qui génèrent un effet de sortie. Par exemple, une alarme incendie, une alarme cambriolage ou un point.
Utilisez ce paramètre pour sélectionner le type d'événement qui doit se produire pour provoquer un effet de sortie. Vous pouvez définir jusqu'à 2 déclencheurs pour le comportement de sortie. Le déclencheur sélectionné contrôle les sélections de portée et de filtre de portée disponibles.

Remarque!
Activation de sortie par des déclencheurs configurés
Chaque déclencheur programmé est nécessaire pour répondre aux conditions de profil de sortie et pour activer une sortie.

Emplacement du menu RPS
Sorties > Profils de sortie > Déclencheur

Pour de plus amples informations
Les événements, états et paramètres suivants peuvent être utilisés individuellement ou ensemble pour configurer des déclencheurs :
Alarme incendie *Sirène incendie, page 147*
Alarme gaz *Sirène gaz, page 150*
Alarme cambriolage *Sirène d'alarme, page 146*
Supervision cambriolage *Liste des surveillance de point d'intrusion, page 154*
Temporisation Entrée/Sortie *Temporisation d'entrée, page 227* / *Durée de la temporisation de sortie, page 104*

Défaut de partition *Défaut de partition, page 149*
Tout act. (armé) : s'active lorsqu'une partition est armée à l'état Tout actif.
Partielle armée : s'active à la fin de la fenêtre de fermeture lorsqu'une sortie est définie pour *Échec d'ouverture, page 115* et que la partition n'est pas armée.
Partition désarmée *Partition désactivée, page 149*
Échec fermeture *Échec de fermeture, page 115*
Surveill. active *Mode de détection, page 148*
Point actif : s'active (la sortie assignée s'active) lorsque le point configuré est défaillant, ouvert ou court-circuité. Vous pouvez attribuer n'importe quel numéro de point valide. *Source, page 200*
Sortie active *Sortie, page 203*
Fonction activée par SKED : s'active lorsque le SKED configuré s'exécute aux date et heure planifiées. *Fonction, page 257*
Fonction personnalisée activée : s'active (la sortie affectée est activée) lorsqu'une fonction personnalisée configurée dans le *Filtre de portée, page 161* pour le déclencheur s'exécute sur la centrale. *Fonctions, page 138*
Défaut ligne Ethernet : s'active (la sortie affectée s'active) lorsque la centrale présente un problème d'affichage pour la connexion Ethernet intégrée. *Communicateur Ethernet (IP) embarqué, page 34*
Défaut secteur *Défaut secteur, page 151*
Défaut batterie *Défaut de batterie, page 151*
Échec de communication *Défaillance comm, page 151*
Défaut système : s'active lorsque la centrale présente une défaillance générale du système, telle qu'un périphérique absent, un clavier absent ou une défaillance de bus SDI.
Partition prête - s'active lorsque tous les points Part active, Intérieur ou Suiveur intérieur qui sont affectés à une partition sont normaux. La sortie se désactive si l'un des points Part active, Intérieur ou Suiveur intérieur qui sont affectés à une partition est défaillant.

9.4.4 Portée

Par défaut : Niveau centrale

Choix :

- Niveau centrale - effet système ou centrale
- Niveau partition - effet partition
- Point - effet point ou partition
- Sortie - effet sortie
- Sked - effet Sked
- Fonction personnalisée - effet fonction personnalisée

Utilisez ce paramètre pour mettre l'accent sur le déclencheur. La portée sélectionnée détermine les options de filtre de portée disponibles pour la sélection.

Pour obtenir de plus amples informations

Les paramètres suivants sont disponibles lors de la configuration de la portée et du filtre de portée :
Paramètres liés à la centrale, page 31
Paramètres de partition/sirène, Options d'ouverture/de fermeture, page 101
Points, page 200
Sorties liées de la centrale, page 151
Sorties liées à la partition, page 146
Fonctions, page 138
Descriptions des fonctions de planification, page 260

Emplacement du menu RPS
Sorties > Profils de sortie > Portée

9.4.5 Filtre de portée

Valeur par défaut : 0
Les sélections sont automatiquement filtrées par la sélection du paramètre de portée (Niveau centrale, Niveau partition, Point, Sortie, Sked, Fonction personnalisée). Les chaînes de sélection réelles sont dynamiques en fonction de la programmation de la centrale :
- Partition et nom de la centrale
- Point et nom de la centrale
- Sortie et nom
- Sked et nom
- Nom et fonction personnalisée

Utilisez ce paramètre pour diriger le déclencheur sur une partie de la portée. Par exemple, partition 1 ou fonction personnalisée 2.

Emplacement du menu RPS
Sorties > Profils de sortie > Filtre de portée

Pour obtenir de plus amples informations
Les paramètres suivants sont disponibles lors de la configuration de la portée et du filtre de portée :
Paramètres liés à la centrale, page 31
Paramètres de partition/sirène, Options d'ouverture/de fermeture, page 101
Points, page 200
Sorties liées de la centrale, page 151
Sorties liées à la partition, page 146
Fonctions, page 138
Descriptions des fonctions de planification, page 260

9.4.6 Schéma

Valeur par défaut : désactivé
Choix :
- Éteint - aucun.
- Continu - sortie stable.
- Impulsion demi-seconde - durée de l'impulsion. 60 battements par minute à un rythme régulier (actif 0,5 seconde et inactif 0,5 seconde).
- Impulsion 1 seconde - durée de l'impulsion. 30 battements par minute à un rythme régulier (actif 1 seconde et inactif 1 seconde).
- Impulsion 2 secondes - durée de l'impulsion. 15 battements par minute à un rythme régulier (actif 2 secondes et inactif 2 secondes).
- Code temporel 3 : séquence de répétition (actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 1,5 seconde).
- Code temporel 4 - séquence de répétition (actif 100 ms, inactif 100 ms, actif 100 ms, inactif 100 ms, actif 100 ms, inactif 100 ms, actif 100 ms, inactif 5 secondes). Sorties Zonex (actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 0,5 seconde, actif 0,5 seconde, inactif 5 seconde).
- Marche de Californie - séquence de répétition (actif 10 secondes, inactif 5 secondes).

Utilisez ce paramètre pour sélectionner le modèle d'effet de sortie.

Emplacement du menu RPS
Sorties > Profils de sortie > Modèle

9.4.7 Temporisation

Valeur par défaut : 00:00:00
Choix (00:00:00, 00:00:05 - 02:00:00):
– hh - heures
– mm - minutes
– ss - secondes

Utilisez ce paramètre pour spécifier le temps d'attente (de 5 secondes à 2 heures) après un déclenchement et avant l'activation de la sortie.
Si le déclencheur 1 ou 2 d'un profil de sortie est défini sur Surveillance active, le paramètre de temporisation ne peut pas être modifié. La temporisation par défaut est indiquée en grisé (aucune modification acceptée).

Emplacement du menu RPS
Sorties > Profils de sortie > Temporisation

9.4.8 Durée

Valeur par défaut : jusqu'à désactivation
Choix :
– Jusqu'à désactivation - persiste jusqu'au déclenchement de la fonction silence.
– Temporisé - persiste de 5 secondes à 2 heures.
– Jusqu'à effacement - persiste jusqu'à l'effacement de l'alarme et de la défaillance. Cette sélection ne peut pas être silencieuse.
– Suivi du déclencheur - persiste jusqu'à l'effacement du déclencheur. Cette sélection ne peut pas être silencieuse.

Utilisez ce paramètre pour sélectionner la manière dont la sortie attribuée persiste après l'activation.

Emplacement du menu RPS
Sorties > Profils de sortie > Durée

10 Configuration utilisateur

10.1 Affectations utilisateur (codes)

10.1.1 Nom d'utilisateur

Valeur par défaut :

- Utilisateur 0 : = installateur
- Tous les autres : UTILISATEUR [numéro d'utilisateur]

Choix : jusqu'à 32 caractères (texte, nombres, espaces et symboles). Les espaces avant, après et dans le nom, sont traités en tant que texte et sont inclus dans la limite de 32 caractères.

Entrez le nom d'utilisateur à afficher au niveau des claviers. Le nom d'utilisateur est inclus dans les rapports transmis au récepteur du centre de télésurveillance dans le format de rapport Modem4.

Si le nom d'utilisateur est supérieur à 20 caractères, les claviers font défiler le nom complet une fois, puis affichent les vingt premiers caractères. Pour faire défiler le nom de nouveau, appuyez sur la touche [ÉCHAP].

Emplacement dans le menu RPS

Configuration utilisateur > Affectations utilisateur > Nom d'utilisateur

10.1.2 Code

Valeur par défaut :

- Utilisateur 0 : 123
- Utilisateur 1 : 123456
- Tous les autres : vide

Choix : 0 à 9

Saisissez un code de 3 à 6 chiffres.

Le paramètre *Longueur du code, page 89* définit la longueur du code. Lorsqu'il est défini sur 3, 4, 5 ou 6 chiffres, la longueur de code est fixe pour tous les codes. Les utilisateurs n'ont pas besoin d'appuyer sur la touche ENTRÉE après la saisie du code.

Lorsque le paramètre Longueur du code est défini sur Désactivé, la longueur de code n'est pas fixe pour tous les codes. Les codes individuels peuvent avoir une longueur de 3 à 6 chiffres. Les utilisateurs doivent appuyer sur la touche ENTRÉE après la saisie du code. RPS ne vous permettra pas d'entrer un code qui pourrait être en conflit avec un code de contrainte. Vous ne pouvez pas saisir un code dans une plage de 2 codes existants. Par exemple, si 654327 est un code existant, vous ne pouvez pas entrer 654325, 654326, 654328 ou 654329. RPS applique cette règle même si la contrainte est désactivée.

Code installateur

L'utilisateur 0 (Installateur) ne peut pas être ajouté ou modifié au niveau d'un clavier. Lorsqu'un utilisateur autre que l'utilisateur 0 essaie de supprimer le code de l'utilisateur 0, le clavier affiche NON UTILISÉ.

Emplacement dans le menu RPS

Configuration utilisateur > Affectations utilisateur (codes) > Code

10.1.3 Accès mobile

Valeur par défaut : Non

Choix :

- Oui (autoriser l'accès au système de cet utilisateur avec l'application mobile)
- Non (interdire l'accès au système de cet utilisateur avec l'application mobile)

Lorsque ce paramètre est défini sur Oui, cet utilisateur peut contrôler son système de sécurité avec un dispositif mobile à l'aide des applications mobiles RSC (contrôle de sécurité à distance) et BSM (Bosch Security Manager).

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur > Accès à distance

10.1.4 Groupe d'utilisateurs

Valeur par défaut : 0 (Non affecté)
Cette sélection signifie qu'aucun groupe n'est affecté à l'enregistrement utilisateur et les Périodes de groupe d'utilisateurs ou les Autorités de partition de niveau groupe ne sont pas appliquées.
Choix :
Groupes B6512 :
– 0 : non affecté, Groupe d'utilisateurs 1- Groupe d'utilisateurs 6
Utilisez ce paramètre pour créer un groupe d'utilisateurs dont le badge (code, carte d'accès ou clé et télécommande radio) est activé et désactivé par une Période de groupes d'utilisateurs. Affectez un Groupe d'utilisateurs pour restreindre l'autorité de code et appliquer de nouveau les autorités de partition de groupe. Vous pouvez lier un groupe d'utilisateurs à plusieurs périodes de groupes d'utilisateurs.
La valeur 0 (non affecté) signifie qu'un groupe d'utilisateurs n'est limité à aucun SKED et n'est accordé à aucun niveau d'autorité de groupe.
– Vous pouvez remplacer n'importe quelle autorité appliquée au niveau groupe sur une partition en modifiant l'affectation de partition spécifique à un utilisateur.
– Les modifications apportées aux autorités de partition à l'aide de Affectations utilisateur > Groupe d'utilisateurs ne mettent pas automatiquement à jour les affectations utilisateur existantes Vous pouvez appliquer de nouveau les autorités de partition définies au niveau du groupe en affectant de nouveau le groupe d'utilisateurs à un utilisateur.

Entrez le numéro du groupe d'utilisateurs dans le paramètre Planifications > Périodes de groupes d'utilisateurs >*Groupe d'utilisateurs, page 254* pour une période activée.
Par exemple, si le groupe d'utilisateurs 1 est lié à une période qui s'exécute entre 8:00 (heure de début) à 16:00 (heure de fin), les utilisateurs du groupe peuvent utiliser leur badge uniquement entre 8:00 et 16:00.

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur (codes) > Groupe d'utilisateurs

10.1.5 Autorités de partition

Valeur par défaut :
– Utilisateur 0 : Niveau d'autorité de tous les n° de partition (A1-An) = 15
– Utilisateur 1 :
  – Niveau d'autorité de la partition 1 (A1) = 1
  – Niveau d'autorité de tous les autres n° de partition = 0
– Toutes les autres utilisateurs :
  – Toutes les partitions (A1-An) : niveau d'autorité = 0

Partitions B6512 (A1-A6) :
– 0 : aucune autorité, niveau d'autorité 1 - Niveau d'autorité 14

Remarque!
Réservé à l'utilisateur installateur 0 (Niveau d'autorité 15)
Le niveau d’autorité 15 ne peut pas être défini pour l’autorité de partition de groupe d’utilisateurs.

Lorsque vous configurez un nouvel utilisateur, veillez à attribuer un niveau d'autorité pour au moins une partition à l'utilisateur. Le paramètre Autorités de partition est défini par défaut sur 0 (zéro) pour les nouveaux utilisateurs, ce qui signifie que l’utilisateur ne dispose d’aucune autorité dans la partition indiquée. Le niveau d'autorité 15 est réservé à l'utilisateur 0, Installateur.
Utilisez les colonnes Partition (A1-An) pour définir le niveau d’autorité des utilisateurs pour chaque partition. Vous pouvez également appliquer des autorités de partition de niveau groupe au sein de plusieurs partitions à l’aide de groupes d’utilisateurs.
Lors de l’utilisation des autorités de partition définies pour l’application d'autorités utilisateur dans plusieurs partitions (A1-An) :
– Vous pouvez remplacer n’importe quelle autorité appliquée au niveau groupe sur une partition en modifiant l’affectation de partition spécifique à un utilisateur.
– Les modifications apportées aux autorités de partition à l’aide de Affectations utilisateur > Groupe d’utilisateurs ne mettent pas automatiquement à jour les affectations utilisateur existantes Les autorités de partition définies au niveau du groupe s’appliquent uniquement aux enregistrements utilisateur en réaffectant le groupe d’utilisateurs à un utilisateur.

Reportez-vous à Configuration utilisateur > *Niveaux d'autorité, page 179* et Configuration utilisateur > Groupes d’utilisateurs > *Autorités de partition, page 168* dans RPS pour afficher les paramètres de chaque niveau d’autorité.

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur > Autorités de partition

10.1.6 Code du site

Valeur par défaut (par type de carte) **:**
– Type de carte 26 bits : 255
– Type de carte MIFARE Classic 32 bits : vierge (lecture seule)
– Type de carte Corporate 1000 35 bits : 4095
– Type de carte 37 bits sans code de site : blanc
– Type de carte 37 bits avec code de site : 65535

Choix (par type de carte) **:**
– Type de carte 26 bits : 0 à 254, 255 = désactivé
– Type de carte MIFARE Classic 32 bits : vierge
– Type de carte Corporate 1000 35 bits : 0 à 4094, 4095 = désactivé
– Type de carte 37 bits sans code de site : blanc
– Type de carte 37 bits avec code de site : 0 à 65534, 65535 = désactivé

Pour le type de carte 37 bits sans code de site, le paramètre Code du site est grisé.
Pour le type de carte 26 bits et 37 bits avec code de site, entrez le code de site (code d'installation) comme indiqué sur l'emballage de la carte ou du clé.
Pour le type de carte 35 bits, entrez le code du site au clavier (menu Utilisateur) ou passez la carte devant le lecteur/pavé numérique. Une fois la carte passée, le code de site est associé à l’utilisateur et il est disponible dans les paramètres Configuration utilisateur (User Configuration) > Affectations utilisateurs paramètres (codes) (User Assignment (passcodes).

Pour obtenir le code de site à l'aide de RPS, ajoutez la carte ou le clé dans le système au niveau des locaux à l'aide d'un lecteur et d'un clavier (MENU 42). Connectez-vous ensuite à la centrale à l'aide de RPS et recevez le compte de centrale.
Lorsque vous supprimez une carte (ou supprimez les données de la carte), RPS définit automatiquement le code de site sur la valeur par défaut (255 pour le type de carte 26 bits, 4095 pour le type de carte 35 bits, 65535 pour le type de carte 37 bits).

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur > Code du site

10.1.7 Données de carte

Valeur par défaut : vide
Choix :
- Type de carte 26 bits : 0 à 65534, vide
- Type de carte MIFARE Classic 32 bits : 0 à 4294967294, vide
- Type de carte Corporate 1000 35 bits : 0 à 1048574, blanc
- Type de carte 37 bits sans code de site : 0 à 34359738366, vide
- Type de carte 37 bits avec code de site : 0 à 524286, vide

Saisissez les données de carte imprimées sur la carte ou le clé.

Pour les types de carte **26 bits, 35 bits** et **37 bits avec le code de site** *Type de carte, page 276*, saisissez le *Code du site, page 165* avant de saisir les données de carte. Les valeurs maximales sont réservées et rétablissent les valeurs par défaut du code de site et des paramètres de données de carte si une valeur plus élevée est saisie. Par exemple, si vous saisissez 65535 pour le type de carte 26 bits, cela rétablit le code du site et permet de rétablir les valeurs par défaut pour la sélection des données de la carte.

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur > Données de carte

10.1.8 Télécommande Inovonics RFID (B820)

Valeur par défaut : N/A
Choix : 0 - 99999999
Pour lier une télécommande Inovonics à cet utilisateur, entrez le numéro RFID. Ce numéro est imprimé sur la télécommande.
Les télécommandes Inovonics ne sont pas supervisés lorsqu'ils sont liés à un utilisateur.
Vous pouvez également auto-apprendre le RFID en local à l'aide du récepteur radio de bus SDI2 et d'un clavier système.
Si le paramètre RFID est défini sur 0, la télécommande de l'utilisateur est désactivé.

Remarque!
Les mises à jour RFID sont transmises au récepteur radio du bus SDI2 après déconnexion de RPS
Lors de l'envoi de mises à jour RFID depuis RPS vers la centrale, celle-ci ne télécharge pas les RFID vers le récepteur radio de bus SDI2 jusqu'à ce que vous vous déconnectiez de RPS.

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur > Récepteur RFID (B820 Inovonics radio)

10.1.9 RADION Récepteur (B810)

Valeur par défaut : 0

Choix : 0, 11 - 167772156
Pour lier un récepteur RADION à cet utilisateur, entrez le numéro RFID. Ce numéro est imprimé sur la télécommande.
Vous pouvez également auto-apprendre le RFID en local à l'aide du récepteur radio de bus SDI2 et d'un clavier système.
Si le paramètre RFID est défini sur 0, la télécommande de l'utilisateur est désactivé.

Remarque!
Les mises à jour RFID sont transmises au récepteur radio du bus SDI2 après déconnexion de RPS
Lors de l'envoi de mises à jour RFID depuis RPS vers la centrale, celle-ci ne télécharge pas les RFID vers le récepteur radio de bus SDI2 jusqu'à ce que vous vous déconnectiez de RPS.

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur > Récepteur RFID (radio RADION B810)

10.1.10 Supervisé

Valeur par défaut : Non
Choix :
– Oui : la télécommande RADION liée à cet utilisateur est supervisée.
– Non : la télécommande RADION liée à cet utilisateur n'est pas supervisée.

Lorsque ce paramètre est défini sur Oui, la centrale crée un événement manquant lorsque la télécommande est hors de portée du récepteur RADION pendant 4 heures.
Les télécommandes Inovonics ne sont pas supervisées.

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur > Supervisé

10.1.11 Langue utilisateur

Valeur par défaut : 1 : [première langue]
Choix :
– 1 : [première langue]
– 2 : [deuxième langue]

Sélectionnez la langue que l'utilisateur voit au niveau des claviers configurés pour l'affichage de la langue utilisateur.
La première et la deuxième langues sont définies lors de l'installation du compte de centrale dans la Vue Données de centrale.

Emplacement dans le menu RPS
Configuration utilisateur > Affectations utilisateur (codes) > Langue utilisateur

10.2 Groupes d'utilisateurs

10.2.1 Nom du groupe d'utilisateurs

Valeur par défaut : Vide
Choix : jusqu'à 32 caractères (texte, nombres, espaces et symboles). Les espaces avant, après et dans le nom, sont traités en tant que texte et sont inclus dans la limite de 32 caractères.
Utilisez ce paramètre pour entrer un nom pour le groupe d'utilisateurs.

Emplacement dans le menu RPS
Configuration utilisateur > Groupes d'utilisateur > Nom du groupe d'utilisateurs

10.2.2 Autorités de partition

Valeur par défaut :
– Pas de remplacement
Partitions B6512 (A1-A6) :
– Pas de remplacement, 0 : aucune autorité, Niveau d’autorité 1- Niveau d'autorité 14

Remarque!
Réservé à l'utilisateur installateur 0 (Niveau d'autorité 15)
Le niveau d’autorité 15 ne peut pas être défini pour l’autorité de partition de groupe d’utilisateurs.

Utilisez les colonnes de partition (A1-An) pour définir une ou plusieurs autorités de partition que vous souhaitez appliquer à un enregistrement utilisateur. Les autorités de partition de groupe sont appliquées à un enregistrement utilisateur chaque fois que le groupe est affecté à un enregistrement utilisateur dans les affectations utilisateur.
– Vous pouvez remplacer n’importe quelle autorité appliquée au niveau groupe sur une partition en modifiant l’affectation de partition spécifique à un utilisateur.
– Les modifications apportées aux autorités de partition à l’aide de Affectations utilisateur > Groupe d’utilisateurs ne mettent pas automatiquement à jour les affectations utilisateur existantes Vous pouvez appliquer de nouveau les autorités de partition définies au niveau du groupe en affectant de nouveau le groupe d’utilisateurs à un utilisateur.

Emplacement du menu RPS
Configuration utilisateur > Groupes d'utilisateurs

Se reporter à
– *Groupe d'utilisateurs, page 164*

10.3 Fonctions (clavier) utilisateur

10.3.1 Tout activée Temporisée

Valeur par défaut : P
Choix :
– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.
Cette fonction utilisateur arme les partitions Tout activé avec une temporisation d'entrée et une temporisation de sortie. Tous les points contrôlés dans la partition sont inclus.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Tout activée Temporisée

10.3.2 Tout activé Instantané

Valeur par défaut : P
Choix :
– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.

– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur arme les partitions Tout activé sans temporisation d'entrée ni temporisation de sortie. Tous les points contrôlés dans la partition sont inclus.

Remarque!
Pour être en conformité avec la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Désactivé (-). Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Tout activé Instantané

10.3.3 Partielle Instantané

Valeur par défaut : P
Choix :
– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur arme les partitions Partielle sans temporisation d'entrée ni temporisation de sortie. Seuls les points Partielle de la partition sont inclus. Les points intérieurs ne sont pas inclus.

Remarque!
Pour être en conformité avec la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur Désactivé (-). Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement du menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Partielle Instantané

10.3.4 Partielle Temporisée

Valeur par défaut : P
Choix :
– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur arme les partitions Partielle avec une temporisation d'entrée et une temporisation de sortie. Seuls les points Partielle de la partition sont inclus. Les points intérieurs ne sont pas inclus.

Emplacement du menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Partielle Temporisée

10.3.5 Mode de détection

Valeur par défaut : E
Choix :
– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.

– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur permet d'activer ou de désactiver le mode de surveillance. Lorsque le mode de surveillance est activé et qu'un point de surveillance est en défaut, les claviers affichent le texte du point et émettent une tonalité de surveillance.

Emplacement dans le menu RPS

Configuration utilisateur > Fonctions (clavier) utilisateur > Mode de surveillance

10.3.6 Afficher le statut de la partition

Valeur par défaut : P

Choix :

– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur permet à l'utilisateur d'afficher l'état armé de toutes les partitions dans la portée du clavier.

Les états armés incluent :

– Désarmé
– Tout activée Temporisée armé
– Tout activé Instantané armé
– Partielle Instantané armé
– Partielle Temporisée armé

Tous les types de partition (Principale, Associée, Standard et Partagée) peuvent être affichées à l'aide de cette fonction.

Emplacement dans le menu RPS

Configuration utilisateur > Fonctions (clavier) utilisateur > Afficher le statut de la partition

10.3.7 Afficher/Effacer la mémoire des événements

Valeur par défaut : E

Choix :

– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur permet d'afficher la mémoire des événements. La mémoire des événements est supprimée (effacée) lorsque la partition est armée.

Emplacement dans le menu RPS

Configuration utilisateur > Fonctions (clavier) utilisateur > Afficher/Effacer la mémoire des événements

10.3.8 Afficher le statut du point

Valeur par défaut : E

Choix :

– Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
– Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
– Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur permet d'afficher le texte du point et l'état électrique (normal, ouvert, court-circuit ou manquant) de chaque point lié à la partition.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Afficher le statut du point

10.3.9 Test de détection (Tous les points intrusion non incendie)

Valeur par défaut : E

Choix :

- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

La fonction utilisateur Test de détection permet aux utilisateurs de tester les points contrôlés sans l'envoi de rapports d'alarme au récepteur du centre de télésurveillance.
Au début du test de détection, la sortie de sirène d'alarme s'active pendant 2 secondes. Si l'utilisateur met en défaut chaque point contrôlé, les claviers émettent un bip sonore.
Les points incendie, gaz et les points 24 heures ne peuvent pas être testés à l'aide de cette fonction utilisateur Test de détection.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Test de détection (Tous les points intrusion non incendie)

10.3.10 Test de détection de tous les points incendie

Valeur par défaut : P

Choix :

- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Ce paramètre désactive, active sans code requis ou active avec le code requis, la fonction utilisateur Test de la détection incendie.

Remarque!
Le test de détection incendie comprend des points gaz et environnementaux
Lorsque vous effectuez un test de détection incendie, le système de sécurité teste les points 24 h / 24 qui ne sont pas invisibles. Le test de détection incendie comprend les points gaz, environnementaux (eau, température élevée, température faible) et tous les points visibles non contrôlés.

Lorsqu'un Test de détection incendie démarre

- Les centrales envoient un rapport DÉBUT DÉTECTION INCENDIE au récepteur du centre de télésurveillance.
- Il y a une annonce d'alarme locale uniquement, aucun rapport d'alarme n'est envoyé au récepteur du centre de télésurveillance.
- La centrale est alimentée par batterie uniquement.
- La sortie *Sirène incendie, page 147* s'active pendant 2 secondes pour chaque point incendie ou point gaz qui est testé.
- Tous les points incendie et les points gaz avec le paramètre *Réinitialisable, page 236* défini sur OUI se réinitialisent automatiquement lorsqu'ils sont testés. [RÉINITIALISATION DES DÉTECTEURS] s'affiche sur les claviers.

- Le clavier affiche le texte du point pour chaque point dès qu'il est testé, ainsi qu'un nombre de « points testés » mis à jour.
- Le test se termine une fois tous les points testés ou au bout de 20 minutes sans activité. La centrale envoie un rapport FIN DÉTECTION INCENDIE au récepteur du centre de télésurveillance.

Si les points incendie ou les points gaz sont en défaut lorsque le Test de détection incendie se termine, les points sont inhibés et la tonalité de défaut est émise. Les claviers affichent les points inhibés et la condition de défaut.

Lorsqu'un exercice incendie démarre

- La centrale envoie un rapport DÉBUT EXERCICE INCENDIE au récepteur du centre de télésurveillance.
- La sortie *Sirène incendie, page 147* s'active jusqu'à ce qu'un utilisateur termine l'exercice en rendant silencieuse la sirène incendie.
- Les points incendie et les points gaz sont actifs. Une alarme sur un point incendie ou un point gaz met fin à l'exercice. La centrale envoie des rapports d'alarme incendie.

Lorsque l'exercice incendie se termine, la centrale envoie un rapport FIN EXERCICE INCENDIE.

Emplacement dans le menu RPS

Configuration utilisateur > Fonctions (clavier) utilisateur > Test de détection de tous les points incendie

10.3.11 Envoyer le rapport (Test/Statut)

Valeur par défaut : E

Choix :

- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur envoie le même rapport de test que la fonction de planification. Si un point dans n'importe quelle partition est anormal (défaut non effacé de l'écran du clavier), la centrale envoie un rapport de test anormal au lieu du rapport de test.
Si le paramètre Paramètres liés à la centrale > Routage des rapports > *Transmission rapport de test, page 33* est défini sur Oui, le rapport de test (ou le rapport de test anormal) est suivi d'un rapport de diagnostic pour chaque état anormal du système. Accédez à Paramètres liés à la centrale > Routage des rapports > *Rapports diagnostiques, page 61* pour obtenir une liste des rapports inclus.

Emplacement dans le menu RPS

Configuration utilisateur > Fonctions (clavier) utilisateur > Envoyer le rapport (Test/Statut)

10.3.12 Contrôle de la porte

Valeur par défaut : P

Choix :

- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Les fonctions utilisateur activées par ce paramètre sont : Cycle de porte, Déverrouiller la porte et Porte sécurisée.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Contrôle de la porte

10.3.13 Définir la luminosité/le volume/la pression des touches du clavier

Valeur par défaut : E
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet aux utilisateurs de régler le volume et la luminosité du clavier et d'activer ou de désactiver la tonalité de pression des touches.
Pour les claviers B942, les utilisateurs peuvent définir les fonctions de présence et de luminosité de nuit.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Définir la luminosité/le volume/la pression des touches du clavier

10.3.14 Définir/Afficher la date et l'heure

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur permet à l'utilisateur de définir la date et l'heure sur la centrale.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Définir/Afficher la date et l'heure

10.3.15 Changer le code

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur permet à un utilisateur de modifier son code.
Pour autoriser un utilisateur à modifier le code d'autres utilisateurs, consultez *Ajouter/ Modifier un utilisateur, page 173*.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Changer le code

10.3.16 Ajouter/Modifier un utilisateur

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet à un utilisateur disposant de l'autorité nécessaire d'ajouter ou de modifier des codes, et d'ajouter ou de modifier les niveaux d'autorité de la centrale pour d'autres utilisateurs par partition.

Remarque!
La commande Ajouter un utilisateur permet d'arrêter la réponse aux demandes de contrôle de porte et RTE/REX
Lorsque la commande AJOUTER UN UTILISATEUR est en cours d'exécution, les badges (cartes ou clés) ne sont pas traités. Il n'y a pas de réponse aux fonctions de contrôle de porte aux demandes RTE/REX. En cas d'activité élevée d'une porte, définissez la porte sur l'état Déverrouillé avant d'ajouter des utilisateurs.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Ajouter/Modifier un utilisateur

10.3.17 Supprimer l'utilisateur

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet à un utilisateur disposant de l'autorité nécessaire de supprimer les codes d'autres utilisateurs. Elle ne permet pas de supprimer des noms d'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Supprimer l'utilisateur

10.3.18 Étendre la fermeture

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet aux utilisateurs d'étendre la période de fermeture lorsque la durée définie au paramètre Début de fermeture anticipée est écoulée et que la période de fermeture est active.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Étendre la fermeture

10.3.19 Afficher le journal d'événements

Valeur par défaut : E
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet à l'utilisateur d'afficher le journal des événements.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Afficher le journal d'événements

10.3.20 Commande utilisateur 7

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

En appuyant sur [CMD], puis sur [7] provoque une réponse d'alarme incendie manuelle.
Avec les claviers B92x, maintenir les touches [A] et [1] ensemble entraîne également une réponse d'alarme incendie manuelle.
Pour activer Commande utilisateur 7, vous devez définir Claviers > Paramètres globaux de clavier > Réponse de la touche A sur Alarme incendie manuelle.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Commande utilisateur 7

10.3.21 Commande utilisateur 9

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

En appuyant sur [CMD], puis sur [9] provoque une réponse d'alarme panique manuelle.
Avec les claviers B92x, maintenir les touches [C] et [7] ensemble entraîne également une réponse d'alarme panique manuelle.
Pour activer Commande utilisateur 9, vous devez définir Claviers > Paramètres globaux de clavier > Réponse de la touche C sur Alarme panique manuelle, la sortie d'alarme invisible et silencieuse ou Alarme panique manuelle, visible avec sortie d'alarme.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Commande utilisateur 9

10.3.22 Inhiber un point

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction inhibe les points individuels dans les partitions au sein de la portée du clavier.
Les points inhibés ne créent pas d'événements d'alarme ou de défaut.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Inhiber un point

10.3.23 Rétablir un point

Valeur par défaut : P

Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction rétablit des points individuels qui sont programmés P## FA Retournable ou P## Inhibition retournable. Les points dans la portée du clavier où la fonction est saisie sont rétablis.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Rétablir un point

10.3.24 Réinitialiser le ou les détecteurs

Valeur par défaut : E
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction réinitialise les détecteurs dans les partitions de la portée du clavier.

Emplacement du menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Réinitialiser le ou les détecteurs

10.3.25 Modifier les sorties

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet à l'utilisateur de définir et réinitialiser manuellement les sorties.

Contrôle manuel (activé/désactivé) des sorties
Les sorties basées sur des profils de sortie peuvent être activées manuellement (par le biais du clavier ou à distance) et resteront activées.
Désactivez manuellement les sorties pour revenir au fonctionnement automatique.

Emplacement du menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Modifier la ou les sorties

10.3.26 Programme à distance

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur démarre des sessions de programmation à distance. Si l'utilisateur démarre cette fonction alors que la ligne téléphonique partagée avec la centrale est en train de sonner, la centrale saisit la ligne téléphonique.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Programme à distance

10.3.27 Accéder à la partition

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction affecte temporairement le clavier à une partition différente.
Les utilisateurs sont limités aux fonctions activées par leur niveau d'autorité pour la partition à laquelle le clavier est temporairement lié.
Au bout de 15 secondes sans activité de l'utilisateur sur le clavier, ce dernier revient à la partition qui lui est liée.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Accéder à la partition

10.3.28 Afficher le type de centrale et les révisions

Valeur par défaut : E
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction utilisateur affiche la révision du type de centrale et du firmware.
Lorsque le paramètre Nom de zone est modifié et n'est plus défini sur la valeur par défaut, cette fonction affiche le texte du nom de zone par défaut.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions clavier utilisateur > Afficher la révision et le type de centrale

10.3.29 Détection de service, Tous les points

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

La fonction utilisateur Test de détection de service permet aux utilisateurs de tester tous les points qui sont liés à une source (le paramètre Source n'est pas défini sur Non lié).
Si l'utilisateur met en défaut chaque point, les claviers émettent un bip sonore.
Les points incendie, les points gaz ou les points 24 heures laissés en défaut lors de la sortie du Test de la détection de service sont inhibés. La tonalité de défaut est émise au niveau des claviers.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Détection de service, Tous les points

10.3.30 Modifier les planifications

Valeur par défaut : P

Choix :

- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet à l'utilisateur de modifier l'heure à laquelle une planification s'exécute, et si cette planification s'exécute pendant les congés. Les utilisateurs peuvent exécuter cette fonction depuis n'importe quel clavier lié à une partition sur lequel l'utilisateur dispose d'une autorité.

Emplacement dans le menu RPS

Configuration utilisateur > Fonctions (clavier) utilisateur > Modifier les planifications

10.3.31 Test de détection de tous les points intrusion invisibles

Valeur par défaut : P

Choix :

- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

La fonction utilisateur Test de la détection invisible permet aux utilisateurs de tester des points invisibles (le paramètre Point invisible défini sur Oui) sans envoyer de rapports d'alarme au récepteur du centre de télésurveillance.

Les points 24 heures laissés en défaut lors de la sortie du Test de la détection invisible sont inhibés. La tonalité de défaut est émise au niveau des claviers.

Les points incendie et les points gaz ne peuvent pas être testés à l'aide de cette fonction utilisateur invisible Test de la détection.

Emplacement dans le menu RPS

Configuration utilisateur > Fonctions (clavier) utilisateur > Test de détection de tous les points intrusion invisibles

10.3.32 Rendre les fonctions silencieuses

Valeur par défaut : E

Choix :

- Activé (E) - active la fonction silencieuse au niveau de la centrale sans que l'utilisateur ait à saisir un code pour rendre les claviers silencieux.
- Code (P) - active la fonction silencieuse an niveau de la centrale et demande à l'utilisateur d'entrer un code pour rendre silencieux les claviers après avoir appuyé sur la touche Silence ou Entrée.

Si vous appuyez sur la touche Silence ou Entrée d'un clavier, le clavier cesse de déclencher la tonalité de défaillance. Configurez ce paramètre sur P pour activer la saisie d'un code sur le clavier après avoir appuyé sur la touche Silence ou Entrée.

Remarque!

Exigences de la norme UL 985 relative aux unités d'alarme incendie de maison familiale
Pour vous conformer aux exigences de la norme UL 985 relative aux unités d'alarme incendie de maison familiale, configurez l'option Rendre l'alarme incendie silencieuse pour l'exigence d'un code.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Fonction Rendre silencieux

10.3.33 Fonction personnalisée

Valeur par défaut : Code (P)
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Cette fonction permet à l'utilisateur d'exécuter des fonctions personnalisées depuis le menu de raccourcis, la touche A, la touche B ou la touche C.
Pour que l'utilisateur exécute des fonctions personnalisées à l'aide d'un télécommande, le niveau d'autorisation associé à l'utilisateur doit être réglé sur E.
La centrale B6512 prend en charge la fonction personnalisée 128 à 133.
La centrale B5512 prend en charge la fonction personnalisée 128 à 131.
La centrale B4512 prend en charge la fonction personnalisée 128 à 129.
La centrale B3512 prend en charge la fonction personnalisée 128.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Fonction personnalisée

10.3.34 Programmation du clavier

Valeur par défaut : P
Choix :
- Désactiver (-) : désactiver cette fonction au niveau de la centrale, quel que soit le niveau d'autorité de l'utilisateur.
- Activer (E) : activer le fonction au niveau de la centrale sans qu'un code soit nécessaire.
- Code (P) : exiger un code pour activer cette fonction au niveau de la centrale.

Notez que l'option Activer (E) n'est pas disponible en tant que sélection pour le paramètre Programmation du clavier.
Cette fonction permet aux la programmation depuis les claviers pour une liste de paramètres.
Seul le code installateur dispose de l'autorité nécessaire pour la programmation du clavier.
Si une partition est armée ou si la centrale est connectée à RPS, vous ne pouvez pas accéder à la programmation du clavier.

Emplacement dans le menu RPS
Configuration utilisateur > Fonctions (clavier) utilisateur > Programmation du clavier

Pour de plus amples informations
Consultez la documentation de la centrale pour plus d'informations sur la programmation du clavier.

10.4 Niveaux d'autorité

Les niveaux d'autorité déterminent les fonctions et fonctionnalités auxquelles les utilisateurs ont accès. Les paramètres de cette section sont utilisés pour configurer les niveaux d'autorité 1-14. Le niveau d'autorité 15 est réservé au code installateur (utilisateur 0) et il ne peut pas être modifié.

Utilisez le paramètre Configuration utilisateur > Affectations utilisateur (codes) > *Autorités de partition, page 164* pour affecter les utilisateurs à un niveau d'autorité pour chaque partition.

10.4.1 Nom du niveau d'autorité (première langue)

Valeur par défaut : Niveau aut. 1 (à 15)
Choix : jusqu'à 32 caractères.
Entrez jusqu'à 32 caractères pour décrire la partition.
La première langue et la deuxième langue sont programmées lors de l'installation du compte de centrale. Langues prises en charge : anglais, espagnol, français, portugais brésilien, chinois, polonais, italien, grec, hongrois, allemand, néerlandais et suédois.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Nom du niveau d'autorité

10.4.2 Nom du niveau d'autorité (deuxième langue)

Valeur par défaut : Niveau aut. 1 (à 15)
Choix : jusqu'à 32 caractères.
Entrez jusqu'à 32 caractères pour décrire la partition.
La première langue et la deuxième langue sont programmées lors de l'installation du compte de centrale. Langues prises en charge : anglais, espagnol, français, portugais brésilien, chinois, polonais, italien, grec, hongrois, allemand, néerlandais et suédois.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Nom du niveau d'autorité (deuxième langue)

10.4.3 Désarmement unique

Valeur par défaut : -
Choix :
– Désactivé (E)
– Désactivé (-)

Définissez ce paramètre pour désigner un accès temporaire pour un utilisateur sur toutes les partitions affectées à ce niveau d'autorité. Le niveau d'autorité temporaire n'expire à aucune date ou période.
Les utilisateurs disposant d'un niveau d'autorité avec désarmement unique activé, ne peuvent utiliser leur code qu'une seule fois dans chaque partition affectée. Lorsque la même partition est réarmée, la désarmement unique expire et le niveau d'autorité utilisateur pour la partition est défini sur 0 (non affecté).
Les autorisations utilisateur individuelles continuent à utiliser l'ensemble d'autorisations du niveau d'autorité.

Emplacement du menu RPS
Configuration utilisateur > Niveaux d'autorité > Désarmement unique

10.4.4 Désarmer la sélection

Valeur par défaut :
– Activé (E) : Niveaux d'autorité 1-5, 14
– Vide (-) - Niveaux d'autorité 6-13, 15

Choix :
– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ces fonctions de désarmement sont disponibles pour l'utilisateur avec cette autorité :

– Désarmer tout : désarme toutes les partitions dans la portée du clavier et incluses dans l'autorité de l'utilisateur.
– Désarmer la partition n° : désarme uniquement la partition sélectionnée.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Désarmer la sélection

10.4.5 Tout activée Temporisée

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-5
– Vide (-) : Niveaux d'autorité 6-15

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'armer les partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur Tout activée Temporisée (armement des points Partielle et des points intérieurs avec temporisation de sortie et temporisation d'entrée).

Si un utilisateur utilise la commande 1 pour armer Tout activée Temporisée, seule la partition à laquelle le clavier est lié est armée.

Si un utilisateur arme Tout activée Temporisée à l'aide de l'application RSC (Contrôle de sécurité à distance), toutes les partitions du niveau d'autorité de l'utilisateur sont armées.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Tout activée Temporisée

10.4.6 Tout activé Instantané

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1 & 2
– Vide (-) : Niveaux d'autorité 3-15

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'armer les partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur Tout activé Instantané (armement des points Partielle et des points intérieurs sans temporisation de sortie ni temporisation d'entrée).

Si un utilisateur utilise la commande 1 pour armer Tout activé Instantané, seule la partition à laquelle le clavier est lié est armée.

Si un utilisateur arme Tout activé Instantané à l'aide de l'application RSC (Contrôle de sécurité à distance), toutes les partitions du niveau d'autorité de l'utilisateur sont armées.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Tout activé Instantané

10.4.7 Partielle Instantané

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-4
– Vide (-) : Niveaux d'autorité 5-15

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'armer les partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur Partielle Instantané (armement des points Partielle sans temporisation de sortie ni temporisation d'entrée).
Si un utilisateur utilise la commande 2 pour armer Partielle Instantané, seule la partition à laquelle le clavier est lié est armée.
Si un utilisateur arme Partielle à l'aide de l'application RSC (Contrôle de sécurité à distance), toutes les partitions du niveau d'autorité de l'utilisateur sont armées.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Partielle Instantané

10.4.8 Partielle Temporisée

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-4
– Vide (-) : Niveaux d'autorité 5-15

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'armer les partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur Partielle Temporisée (armement des points Partielle avec temporisation de sortie et temporisation d'entrée).
Si un utilisateur utilise la commande 3 pour armer Partielle Temporisée, seule la partition à laquelle le clavier est lié est armée.
Si un utilisateur arme Partielle Temporisée à l'aide de l'application RSC (Contrôle de sécurité à distance), toutes les partitions du niveau d'autorité de l'utilisateur sont armées.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Partielle Temporisée

10.4.9 Mode de détection

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-3, 15
– Vide (-) : Niveaux d'autorité 4-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'activer ou de désactiver le mode de détection dans les partitions dans la portée du clavier et inclus dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Mode de détection

10.4.10 Afficher le statut de la partition

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 2, 15
- Vide (-) : Niveaux d'autorité 3-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs avec l'autorité d'armement/de désarmement d'afficher l'état d'armement/désarmement et prêt pour l'armement pour les partitions au sein de la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Afficher le statut de la partition

10.4.11 Afficher la mémoire des événements

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1-3, 15
- Vide (-) : Niveaux d'autorité 4-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'afficher la mémoire des événements pour les partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.
La centrale efface la mémoire des événements lorsque les partitions sont armées.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Afficher la mémoire des événements

10.4.12 Afficher le statut du point

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1-3, 15
- Vide (-) : Niveaux d'autorité 4-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'afficher l'état du point (normal, ouvert, court-circuit) pour les partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Afficher le statut du point

10.4.13 Test de détection (Tous les points intrusion non incendie)

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 2, 15
- Vide (-) : Niveaux d'autorité 3-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'effectuer un test de détection des points contrôlés (test sans l'envoi de rapports d'alarme au récepteur du centre de télésurveillance).
Au début du test de détection, la sortie de sirène d'alarme s'active pendant 2 secondes. Si l'utilisateur met en défaut chaque point contrôlé, les claviers émettent un bip sonore.
Les points incendie, gaz et les points 24 heures ne peuvent pas être testés à l'aide de cette fonction utilisateur Test de détection.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Test de détection (points intrusion non incendie)

10.4.14 Test de détection de tous les points incendie

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 2, 15
- Vide (-) : Niveaux d'autorité 3-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de lancer un test de la détection incendie pour les points d'incendie et les points de gaz.

Remarque!
Le test de détection incendie comprend des points gaz et environnementaux
Lorsque vous effectuez un test de détection incendie, le système de sécurité teste les points 24 h / 24 qui ne sont pas invisibles. Le test de détection incendie comprend les points gaz, environnementaux (eau, température élevée, température faible) et tous les points visibles non contrôlés.

Lorsqu'un Test de détection incendie démarre
- Les centrales envoient un rapport DÉBUT DÉTECTION INCENDIE au récepteur du centre de télésurveillance.
- Il y a une annonce d'alarme locale uniquement, aucun rapport d'alarme n'est envoyé au récepteur du centre de télésurveillance.
- La centrale est alimentée par batterie uniquement.
- La sortie *Sirène incendie, page 147* s'active pendant 2 secondes pour chaque point incendie ou point gaz qui est testé.

- Tous les points incendie et les points gaz avec le paramètre *Réinitialisable, page 236* défini sur OUI se réinitialisent automatiquement lorsqu'ils sont testés. [RÉINITIALISATION DES DÉTECTEURS] s'affiche sur les claviers.
- Le clavier affiche le texte du point pour chaque point dès qu'il est testé, ainsi qu'un nombre de « points testés » mis à jour.
- Le test se termine une fois tous les points testés ou au bout de 20 minutes sans activité. La centrale envoie un rapport FIN DÉTECTION INCENDIE au récepteur du centre de télésurveillance.

Si les points incendie ou les points gaz sont en défaut lorsque le Test de détection incendie se termine, les points sont inhibés et la tonalité de défaut est émise. Les claviers affichent les points inhibés et la condition de défaut.

Lorsqu'un exercice incendie démarre

- La centrale envoie un rapport DÉBUT EXERCICE INCENDIE au récepteur du centre de télésurveillance.
- La sortie *Sirène incendie, page 147* s'active jusqu'à ce qu'un utilisateur termine l'exercice en rendant silencieuse la sirène incendie.
- Les points incendie et les points gaz sont actifs. Une alarme sur un point incendie ou un point gaz met fin à l'exercice. La centrale envoie des rapports d'alarme incendie.

Lorsque l'exercice incendie se termine, la centrale envoie un rapport FIN EXERCICE INCENDIE.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Test de détection de tous les points incendie

10.4.15 Test de détection de tous les points intrusion invisibles

Valeur par défaut :

- Activé (E) : Niveaux d'autorité 1, 15
- Vide (-) : Niveaux d'autorité 2-14

Choix :

- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de tester des points invisibles (paramètre Point invisible défini sur Oui) sans l'envoi de rapports d'alarme au récepteur du centre de télésurveillance.

Les points 24 heures laissés en défaut lors de la sortie du Test de la détection invisible sont inhibés. La tonalité de défaut est émise au niveau des claviers.

Les points incendie et les points gaz ne peuvent pas être testés à l'aide de cette fonction utilisateur invisible Test de la détection.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Test de détection de tous les points intrusion invisibles

10.4.16 Détection de service, Tous les points

Valeur par défaut :

- Activé (E) : Niveaux d'autorité 1, 15
- Vide (-) : Niveaux d'autorité 2-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'utiliser le test de détection de service. Le test de détection de service inclut tous les points qui sont liés à une source (paramètre Source non défini sur Non lié).
Si l'utilisateur met en défaut chaque point, les claviers émettent un bip sonore.
Les points incendie, les points gaz ou les points 24 heures laissés en défaut lors de la sortie du Test de la détection de service sont inhibés. La tonalité de défaut est émise au niveau des claviers.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Détection de service, Tous les points

10.4.17 Envoyer le rapport (Test/Statut)

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 15
- Vide (-) : Niveaux d'autorité 2-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'envoyer un rapport de test à partir des claviers liés à une partition incluse dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Envoyer le rapport (Test/Statut)

10.4.18 Cycle de porte

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 2, 15
- Vide (-) : Niveaux d'autorité 3-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'effectuer un cycle de porte dans les partitions au sein de la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Cycle de porte

10.4.19 (Dé)verrouiller la porte

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 2, 15
- Vide (-) : Niveaux d'autorité 3-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'utiliser les fonctions de verrouillage et de déverrouillage de porte pour les portes dans les partitions au sein de la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > (Dé)verrouiller la porte

10.4.20 Porte sécurisée

Valeur par défaut :
– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :
– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'utiliser la fonction de sécurisation de porte pour les portes dans les partitions au sein de la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Porte sécurisée

10.4.21 Modifier l'affichage du clavier

Valeur par défaut :
– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :
– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de modifier les écrans du clavier (affichage clair, affichage atténué) pour les claviers dans les partitions incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Modifier l'affichage du clavier

10.4.22 Modifier la date et l'heure

Valeur par défaut :
– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :
– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de modifier la date et l'heure de la centrale.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Modifier la date et l'heure

10.4.23 Changer le code

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de modifier leur propre code.

Pour permettre aux utilisateurs de modifier les codes d'autres utilisateurs, consultez *Ajouter code/carte/niveau d'utilisateur, page 188*.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Changer le code

10.4.24 Ajouter code/carte/niveau d'utilisateur

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'ajouter et de changer (modifier) d'autres utilisateurs. Ils peuvent modifier le code, le nom, le niveau d'autorité, le clavier, la carte d'accès (ou le clé), la langue et l'accès à une application mobile Bosch d'un utilisateur.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Ajouter code/carte/niveau d'utilisateur

10.4.25 Supprimer code/carte/niveau d'utilisateur

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de supprimer d'autres utilisateurs.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Supprimer code/carte/niveau d'utilisateur

10.4.26 Étendre la fermeture

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de modifier l'heure de fermeture dans les partitions au sein de la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Étendre la fermeture

10.4.27 Afficher le journal d'événements

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1, 15
– Vide (-) : Niveaux d'autorité 2-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'afficher tous les événements dans le journal des événements de la centrale.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Afficher le journal d'événements

10.4.28 Commande utilisateur 7

Valeur par défaut :

– Activé (E) : Niveau d'autorité 1
– Vide (-) : Niveau d'autorité Tous les autres

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre active la commande utilisateur 7 pour les utilisateurs.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Commande utilisateur 7

10.4.29 Commande utilisateur 9

Valeur par défaut :

– Activé (E) : Niveau d'autorité 1
– Vide (-) : Niveau d'autorité Tous les autres

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre active la commande utilisateur 9 pour les utilisateurs.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Commande utilisateur 9

10.4.30 Inhiber un point

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-4, 15
– Vide (-) : Niveaux d'autorité 5-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'inhiber les points dans les partitions au sein de la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Inhiber un point

10.4.31 Rétablir un point

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-4, 15
– Vide (-) : Niveaux d'autorité 5-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de rétablir des points dans les partitions au sein de la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Rétablir un point

10.4.32 Réinitialiser le ou les détecteurs

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-4, 15
– Vide (-) : Niveaux d'autorité 5-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de réinitialiser les détecteurs.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Réinitialiser les détecteurs

10.4.33 Modifier les sorties

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1, 2, 15
– Vide (-) : Niveaux d'autorité 3-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de définir et de réinitialiser des sorties manuellement. N'utilisez pas la fonction MODIFIER LES SORTIES pour activer ou désactiver les sorties réservées à des fonctions spéciales. Les sorties de fonctions spéciales sont des fonctions de sortie liées à la partition et à la centrale ainsi que des sorties liées dans Entrer clé de sortie.

Contrôle manuel (activé/désactivé) des sorties

Les sorties basées sur des profils de sortie peuvent être activées manuellement (par le biais du clavier ou à distance) et resteront activées.
Désactivez manuellement les sorties pour revenir au fonctionnement automatique.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Modifier les sorties

10.4.34 Programme à distance

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-4, 15
– Vide (-) : Niveaux d'autorité 5-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de démarrer des sessions de programmation à distance. Si l'utilisateur démarre cette fonction alors que la ligne téléphonique partagée avec la centrale est en train de sonner, la centrale saisit la ligne téléphonique.

Emplacement dans le menu RPS

Configuration utilisateur > Niveaux d'autorité > Programmation à distance

10.4.35 Accéder à la partition

Valeur par défaut :

Activé (E) : Niveaux d'autorité 1, 2, 15
Vide (-) : Niveaux d'autorité 3-14

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Cette fonction affecte temporairement les claviers à une partition différente.
Les utilisateurs sont limités aux fonctions activées par leur niveau d'autorité pour la partition à laquelle le clavier est temporairement lié.

Au bout de 15 secondes sans activité de l'utilisateur sur le clavier, ce dernier revient à la partition qui lui est liée.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Accéder à la partition

10.4.36 Afficher le type de centrale et les révisions

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 15
- Vide (-) : Niveaux d'autorité 2-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'afficher la révision du firmware de la centrale. Les claviers affichent la version de firmware dans ce format : ##.##.###.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Afficher le type de centrale et les révisions

10.4.37 Modifier les planifications

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1, 15
- Vide (-) : Niveaux d'autorité 2-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de modifier (éditer) les planifications.
La modification des planifications peut être restreinte en définissant le paramètre Planifications > Planifications > *Modification de l'heure, page 256* sur Non.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Modifier les planifications

10.4.38 Fonction personnalisée

Valeur par défaut :
- Activé (E) : Niveau d'autorité 1
- Vide (-) : Niveaux d'autorité 2-15

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'utiliser des fonctions personnalisées.

Remarque!
Le niveau d'autorité de l'utilisateur pour les fonctions personnalisées se substitue au niveau d'autorité au sein des fonctions utilisateur
Lorsqu'un utilisateur ne dispose pas d'un niveau d'autorité pour une fonction via le menu du clavier, il n'empêche pas l'exécution de la fonction au sein d'une fonction personnalisée.

Emplacement du menu RPS
Configuration utilisateur > Niveaux d'autorité > Fonction personnalisée 128 à n°

10.4.39 Forcer l'armement

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1-6
- Vide (-) : Niveaux d'autorité 7-15

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de forcer l'armement de la centrale.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Forcer l'armement

10.4.40 Envoyer ouvertures/fermetures de partition

Valeur par défaut :
- Activé (E) : Niveau d'autorité 1-14
- Vide (-) : Niveau d'autorité 15

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet l'ouverture et la fermeture des rapports pour les utilisateurs dans les partitions incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Envoyer les ouvertures/fermetures de partition

10.4.41 Ouverture/Fermeture restreinte

Valeur par défaut : vide (-) pour tous les niveaux d'autorité

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre restreint l'ouverture et la fermeture des rapports pour les utilisateurs dans les partitions incluses dans le niveau d'autorité de l'utilisateur. La centrale envoie les rapports d'ouverture uniquement lorsque la sirène d'alarme est active et que l'utilisateur désarme. La centrale envoie les rapports de fermeture uniquement lorsque l'utilisateur force ou inhibe les armements.

Les partitions auxquelles ce niveau d'autorité est lié doivent être programmées pour des ouvertures et des fermetures restreintes (voir Paramètres liés à la partition > *O/F restreinte, page 116*).

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Ouverture/Fermeture restreinte

10.4.42 Ouverture/Fermeture Partielle

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1 - 14
- Vide (-) : Niveau d'autorité 15

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre active des rapports d'ouverture et de fermeture lorsque les utilisateurs arment Partielle et désarment pour les utilisateurs dans les partitions incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Ouverture/Fermeture Partielle

10.4.43 Envoyer la contrainte

Valeur par défaut :
- Activé (E) : Niveau d'autorité 14
- Vide (-) - Niveaux d'autorité 1-13, 15

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet des rapports sous contrainte pour les utilisateurs lorsque le paramètre Paramètres de partition > Contrainte activée est défini sur Oui pour les partitions incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Envoyer la contrainte

10.4.44 Armement par code

Valeur par défaut :
Activé (E) : Niveaux d'autorité 1-6
Vide (-) : Niveaux d'autorité 7-15

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'entrer leur code pour armer des partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Armement par code

10.4.45 Désarmement par code

Valeur par défaut :
Activé (E) : Niveaux d'autorité 1-5, 14
Vide (-) - Niveaux d'autorité 6-13, 15
Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'entrer leur code pour désarmer des partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur.

Profil de désarmement sous contrainte
Le niveau d'autorité de l'utilisateur 14 est programmé par défaut en tant que profil de désarmement sous contrainte. Lorsque le paramètre Type de contrainte est défini sur 3, la fonction de code de contrainte conforme à la norme SIA CP-01 est activée. Les types de contrainte 1 et 2 ne sont pas autorisés dans les installations conformes à la norme SIA CP-01.
Avec le niveau d'autorité 14 lié à un code utilisateur dans une partition, un utilisateur a le niveau d'autorité pour désarmer et envoyer un événement Contrainte depuis cette partition. Tous les codes de contrainte doivent être uniques et ils ne peuvent pas être dérivés d'autres codes. Pour simplifier ce caractère unique, le niveau d'autorité de l'utilisateur 14 est pré-programmé en usine, comme exemple de niveau d'autorité de désarmement sous contrainte. Un niveau d'autorité de l'utilisateur Désarmement sous contrainte exige l'activation des fonctions suivantes :
- Configuration utilisateur > Niveaux d'autorité > Désarmer
- Configuration utilisateur > Niveaux d'autorité > Envoyer la contrainte
- Et ce paramètre Désarmement par code

Définissez le paramètre Paramètres liés à la partition > Contrainte activée sur Oui dans les partitions applicables, sinon le clavier répond Aucune autorité.

Pour obtenir de plus amples informations
- *Désarmer la sélection, page 180*
- *Envoyer la contrainte, page 194*

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Désarmement par code

10.4.46 Niveau de sécurité

Valeur par défaut :
- Tout activé (A) : Niveaux d'autorité 1, 2
- Partielle (P) : Niveaux d'autorité 3-5
- Désarmé (D) : Niveau d'autorité 6
- Aucun accès (-) : Niveaux d'autorité 7-15

Choix :
- Tout activé (A) : les utilisateurs sont autorisés à accéder à cette partition quel que soit son état d'armement.

– Partielle (P) : les utilisateurs sont autorisés à accéder à cette partition lorsqu'elle est désarmée ou partiellement armée, mais pas lorsqu'elle est entièrement armée.
– Désarmé (D) : les utilisateurs sont autorisés à accéder à cette partition uniquement lorsqu'elle est désarmée.
– Aucun accès : les utilisateurs ne sont pas autorisés à accéder à cette partition.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Niveau de sécurité

10.4.47 Niveau de désarmement

Valeur par défaut :
Désarmement (D) : Niveaux d'autorité 1-5
Aucun droit de désarmement (-) : Niveaux d'autorité 6-15
Choix :

– Tout activé ou Partielle à Partielle Instantané (I) : lorsque les utilisateurs présentent leur badge (carte ou clé) et que la partition est Tout activée Temporisée (ou Instantané) ou Partielle Temporisée, la partition devient Partielle Instantané. Le paramètre Niveau d'autorité > Niveau de sécurité doit être défini sur Tout activé (A) pour la partition.
– Désarmement (D) : - lorsque les utilisateurs présentent leur badge d'accès (carte, jeton ou code lorsque le paramètre Fonction de saisie du code est défini sur Cycle de sortie) et que la partition est Tout activée Temporisée (ou Instantané) ou Partielle Temporisée (ou Instantané), les partitions dans la portée du clavier et incluses dans le niveau d'autorité de l'utilisateur passent à l'état désarmé.
– Aucun désarmement (-) : les utilisateurs ne peuvent pas présenter leur badge d'accès (carte ou jeton) pour désarmer.

Pour plus d'informations sur la programmation de cette invite pour une partition partagée, consultez le paragraphe Lecteurs de contrôle d'accès liés aux partitions partagées pour l'invite *Type de partition, page 106* dans les Paramètres de partition.

Remarque!
Sirènes intrusion rendues silencieuses lorsqu'un utilisateur présente un jeton/une carte
Les sirènes intrusion sont rendues silencieuses lorsqu'un utilisateur présente un jeton, une carte ou code lorsque la configuration est définie sur Porte Cyclée.
Les sirènes intrusion sont rendues silencieuses dans la partition locale lorsqu'un utilisateur désarme avec un jeton, une carte ou un code lorsque la configuration est définie sur Porte Cyclée, ou lorsqu'il présente un jeton, une carte ou un code pendant une alarme la configuration est définie sur Porte Cyclée. L'utilisateur doit utiliser un code pour rendre silencieuse une sirène incendie. Des rapports d'annulation sont envoyés après qu'un code valide ou un jeton/une carte a rendu la sirène silencieuse.

Remarque!
Niveau d'autorité 15 réservé
Le niveau d'autorité 15 est réservé au code de service (utilisateur 0). Vous ne pouvez modifier aucun paramètre dans la colonne 15 Niveau d'autorité.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Niveau de désarmement

10.4.48 Niveau de fonction

Valeur par défaut :

– Désarmé (D) : Niveau d'autorité 1
– Aucun niveau de fonction (-) : Niveaux d'autorité 2-15

Choix :

– Tout activé (A) : activer la fonction personnalisée liée à la porte dans cette partition lorsque celle-ci est Tout activé ou Partielle.
– Désarmé (D) : activer la fonction personnalisée liée à la porte dans cette partition lorsque la partition est désarmée.
– Tout activé et désarmé (C) : activer la fonction personnalisée liée à la porte dans cette partition, quel que soit l'état d'armement de la partition.
– Aucun niveau de fonction (-) : les utilisateurs ne peuvent pas activer une fonction personnalisée dans cette partition.

Les utilisateurs doivent disposer d'un code pour démarrer une fonction personnalisée avec une carte d'accès ou un jeton.
Il n'est pas nécessaire que les utilisateurs disposent du niveau d'autorité Niveau de sécurité ou Niveau de désarmement pour démarrer une fonction personnalisée avec une carte d'accès ou un jeton.
Lorsque les utilisateurs disposant du niveau d'autorité Niveau de désarmement et Niveau de fonction présentent une carte ou un jeton, le niveau de désarmement est appliqué en premier, puis le niveau de fonction (la partition est désarmée, puis la fonction personnalisée démarre).

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Niveau de fonction

10.4.49 Armement de la télécommande

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-6
– Vide (-) : Niveaux d'autorité 7-15

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs d'armer les partitions incluses dans le niveau d'autorité de l'utilisateur à l'aide d'une télécommande radio RADION.
Le fonctionnement sous contrainte lors de l'armement n'est pas applicable lors de l'utilisation des télécommandes radio RADION.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Armement de la télécommande

10.4.50 Désarmement de la télécommande

Valeur par défaut :

– Activé (E) : Niveaux d'autorité 1-6
– Vide (-) : Niveaux d'autorité 7-15

Choix :

– Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
– Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet aux utilisateurs de désarmer les partitions incluses dans le niveau d'autorité de l'utilisateur à l'aide d'une télécommande radio RADION.
Le fonctionnement sous contrainte lors du désarmement n'est pas applicable lors de l'utilisation des télécommandes radio RADION.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Désarmement de la télécommande

10.4.51 Mise à jour du firmware

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1 - 6
- Vide (-) : Niveaux d'autorité 7 - 15

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Lorsqu'une autorisation locale est nécessaire, seul un utilisateur de sécurité avec le niveau d'autorité de mise à jour du firmware peut autoriser la mise à jour.

Emplacement dans le menu RPS
Configuration utilisateur > Niveaux d'autorité > Mise à jour du firmware

10.4.52 Rendre les fonctions silencieuses

Valeur par défaut :
- Activé (E) : Niveaux d'autorité 1 et 15
- Vide (-) : Niveaux d'autorité 2-14

Choix :
- Vide (-) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.
- Activé (E) - cette fonction n'est pas activée pour les utilisateurs auxquels est attribué ce niveau d'autorité.

Ce paramètre permet de rendre silencieuse l'annonce des tonalités de défaillance sur les claviers pour les partitions dans la portée du clavier et dans le niveau d'autorité de l'utilisateur.

10.5 Sécurité des codes

Options configurables qui sécurisent l’accès au système après l’échec des tentatives de code via l'automatisation ou des claviers.

10.5.1 Réseau

Activer

Valeur par défaut : Oui

Choix :
- Oui : verrouillage automatique code activé.
- Non : verrouillage automatique code désactivé.

Utilisez ce paramètre pour activer la sécurité des codes pour l’automatisation de centrale. Le verrouillage automatique par code réseau s’applique au rappel réseau, cellulaire, IP Direct, Webconnect_Cell, cloud et cellulaire.

Un message d'erreur s'affiche pour l'opérateur lorsque le nombre maximal de codes non valides est atteint. Le message s'affiche jusqu'à la fin de la durée de verrouillage. À l'issue de la durée de verrouillage, RPS peut se connecter à une centrale à l'aide d'informations d'identification valides.

Échec de tentative

Valeur par défaut : 15

Choix : 0-21

Utilisez ce paramètre pour définir le nombre d'échecs de tentatives de code qui peuvent se produire avant que les connexions d'automatisation ne soient verrouillées pendant une durée définie.

Le nombre d'échecs de tentatives est incrémenté à chaque saisie d'un code non valide qui est différente de la tentative précédente non valide.

Si l'option Échec de tentative est définie sur 0, le verrouillage automatique du code réseau est désactivé.

Durée du verrouillage

Valeur par défaut : 900 (secondes)

Choix : 0 à 65535 (secondes)

Utilisez ce paramètre pour définir la durée en secondes pendant laquelle le logiciel d'automatisation sera verrouillé lorsque le nombre d'échecs de tentatives de code est atteint.

Emplacement du menu RPS

Configuration utilisateur > Sécurité des codes > Réseau

10.5.2 Clavier

Activer

Valeur par défaut : Oui

Choix :

- Oui : verrouillage automatique code activé.
- Non : verrouillage automatique code désactivé.

Utilisez ce paramètre pour activer la sécurité des codes pour les opérations au clavier.

Échec de tentative

Valeur par défaut : 6

Choix : 0-21

Utilisez ce paramètre pour définir le nombre d'échecs de tentative de mot de passe qui peuvent se produire avant le verrouillage du clavier pendant une durée définie.

Le nombre d'échecs de tentatives s'incrémente à chaque saisie d'un code non valide qui est différente de la tentative précédente non valide.

Durée du verrouillage

Valeur par défaut : 0 (non verrouillé)

Choix : 0-65535

Utilisez ce paramètre pour définir la durée en secondes pendant laquelle un clavier est verrouillé lorsque le nombre d'échecs de tentatives de code est atteint.

Emplacement du menu RPS

Configuration utilisateur > Sécurité des codes > Clavier

11 Points

Pour les vidéos en ligne de Points, voir :

– Améliorations de la navigation

Ressources en ligne disponibles : vidéos de présentation et d'instructions

11.1 Affectations de point

11.1.1 Source

Valeur par défaut :

– Intégré : points 1-8
– Non lié : tous les autres points

Choix :

– Non lié : le point n'est pas utilisé.
– Huit entrées : un point est installé sur le module huit entrées B208.
– Radio : un point est installé sur un récepteur radio de bus SDI2.
– Intégré : un point est installé sur la centrale (points 1-8).
– Sortie : un point est connecté de manière logique à la sortie du même numéro. Aucun dispositif physique n'est associé à ce point.
– Clavier : un point est installé sur un clavier de bus SDI2.
– Caméra IP : le point représente une entrée provenant de la fonction Video Content Analytics d'une caméra IP. Les centrales permettent d'attribuer jusqu'à 10 points par caméra IP, y compris jusqu'à 2 entrées filaires et 8 alarmes de tâches virtuelles. Les points de centrale disponibles sont spécifiques à chaque caméra IP.
– Porte : un point est installé sur un module de contrôleur de porte.

Utilisez ce paramètre pour lier des points aux dispositifs physiques. Lorsqu'une sélection est grisée, vous ne pouvez pas lier le point à ce dispositif.

La source du point des points 1 à 8 est définie en tant que Intégrée et elle ne peut pas être modifiée.

Pour les caméras IP, utilisez *Entrées-sorties de caméra, page 45* pour vous aider à affecter des points de centrale et des sorties de centrale.

Emplacement dans le menu RPS

Points > Affectations de point > Source

11.1.2 Texte (première langue)

Valeur par défaut : n° de point

Choix :

– Jusqu'à 32 caractères : les espaces avant, après et au sein d'une chaîne de texte sont considérés comme du texte et sont inclus dans la limite de 32 caractères.

Entrez jusqu'à 32 caractères de texte, nombres et symboles pour décrire le point. Le texte du point s'affiche sur les claviers et est inclus dans les rapports de point envoyés au récepteur du centre de télésurveillance (format de rapport Modem4 uniquement).

Les claviers affichent les 20 premiers caractères. Si le texte comporte plus de 20 caractères, le texte complet défile sur l'écran une fois. Pour faire défiler le texte de nouveau, appuyez sur la touche [ÉCHAP].

L'inclusion du numéro du point peut être utile
L'inclusion du numéro de point dans le texte du point peut être utile aux utilisateurs lorsqu'ils consultent des événements, démarrent des fonctions et des commandes, et effectuent un dépannage.

Emplacement dans le menu RPS
Points > Affectations de point > Texte

11.1.3 Texte (deuxième langue)

Valeur par défaut : vide
Choix :
– Jusqu'à 32 caractères : les espaces avant, après et au sein d'une chaîne de texte sont considérés comme du texte et sont inclus dans la limite de 32 caractères.

Entrez jusqu'à 32 caractères de texte, nombres et symboles pour décrire le point. Le texte du point s'affiche sur les claviers et est inclus dans les rapports de point envoyés au récepteur du centre de télésurveillance (format de rapport Modem4 uniquement).
Les claviers affichent les 20 premiers caractères. Si le texte comporte plus de 20 caractères, le texte complet défile sur l'écran une fois. Pour faire défiler le texte de nouveau, appuyez sur la touche [ÉCHAP].

L'inclusion du numéro du point peut être utile
L'inclusion du numéro de point dans le texte du point peut être utile aux utilisateurs lorsqu'ils consultent des événements, démarrent des fonctions et des commandes, et effectuent un dépannage.

Emplacement dans le menu RPS
Points > Affectations de point > Texte (deuxième langue)

11.1.4 Profil (Index)

Valeur par défaut :
– Détecteur de fumée (4) : point 1
– Partielle : Temporisation (8) - point 2, point 3
– Intérieur : Suiveur (13) : point 4, point 5
– Partielle : Instantané (7) : point 6, point 7
– Instantané 24h sur Ouverture/Tri (1) : point 8
– Désactivé (0) : tous les autres points

Choix :
– 0-20

Utilisez ce paramètre pour sélectionner un profil de point pour chaque point. Le profil de point détermine la façon dont la centrale répond aux modifications d'état du point (en défaut, normal, défaut, manquant, armé, désarmé).
Lorsque le paramètre Source du point est défini sur désactivé et que le point est lié à un profil, la centrale crée un événement POINT MANQUANT.
Lorsque le paramètre Source du point n'est pas défini sur 0 et que le profil de point est défini sur désactivé, la centrale crée un événement POINT SUPPLÉMENTAIRE.
Si un profil de point est affecté à un dispositif dont l’adresse est incorrecte ou qui n’est pas connecté au bus SDI/SDI2 ou lorsqu’un dispositif radio échoue à la vérification, une réponse de POINT MANQUANT est émise.
Lorsqu’un point manque, la centrale génère les réponses suivantes en fonction du type de point :
– Les points incendie et gaz génèrent des réponses de défaut manquant.

- Les points 24 heures autres qu'incendie/gaz génèrent des réponses d'alarme manquante.
- Les points autres qu'incendie/gaz, autres que 24 heures, génèrent des réponses d'alarme manquante en cas d'armement, et des réponses de défaut manquant en cas de désarmement. Cette exception se produit lorsque les points autres qu'incendie/gaz, autres que 24 heures avec une réponse de point de 9 à D, génèrent une réponse d'alarme manquante en cas de désarmement.
- Les points de supervision génèrent des réponses de supervision manquante.

Si vous avez créé des noms spécifiques pour le paramètre, ce nom s'affiche comme <*Numéro index*> : <*nom descriptif*> dans la sélection de paramètre.

Emplacement dans le menu RPS
Points > Affectations de point > Index

11.1.5 Partition

Valeur par défaut : 1 (partition 1)
Choix :
- 1-6 : B6512

Pour lier un point à une partition, sélectionnez le numéro de partition.
Si vous avez créé des noms spécifiques pour le paramètre, ce nom s'affiche comme <*Numéro index*> : <*nom descriptif*> dans la sélection de paramètre.

Emplacement dans le menu RPS
Points > Affectations de point > Partition

11.1.6 Stabiliser

Valeur par défaut : 500 ms
Choix :
- 250 ms
- 500 ms
- 750 ms
- 1,00 s
- 1,25 s
- 1,50 s
- 1,75 s
- 2,00 s

... à ...
- 6,00 s

Le paramètre Stabiliser définit la durée pendant laquelle la centrale analyse un point avant de créer un défaut.
Pour B Series, Bosch recommande de saisir 500 ms ou une valeur supérieure. Pour les points Suiveur intérieur, définissez Stabiliser sur au moins 750 ms.
Lorsque le point *Source, page 200* est défini sur Radio, Caméra IP ou Sortie, le programmeur définit automatiquement le paramètre Stabiliser sur un tiret (-) pour indiquer que le paramètre n'est pas applicable.
Consultez les instructions du fabricant pour plus de détails sur le dispositif connecté au point si vous ne savez pas comment définir ce paramètre.

Emplacement dans le menu RPS
Points > Affectations de point > Stabiliser

11.1.7 Sortie

Valeur par défaut : 0 (non affecté)

Choix :

– 0 (désactivé), 1 à 96

Utilisez ce paramètre pour activer une sortie lorsque le point déclenche une alarme. La sortie ne s'active pas pour les événements Défaut ou Supervision.

La sortie est réinitialisée lorsque l'alarme associée à une sortie de point est effacée du clavier.

Si vous avez créé des noms spécifiques pour le paramètre, ce nom s'affiche comme <*Numéro index*> : <*nom descriptif*> dans la sélection de paramètre.

Remarque!

Relais BFSK existant ou fonctionnalité de relais

Les paramètres d'affectation de point pour de nombreuses centrales Bosch existantes incluent un relais BFSK ou un paramètre Relais pour chaque point.

Vous pouvez émuler la fonctionnalité de relais BFSK en définissant ce paramètre Sortie sur le même numéro de sortie pour plusieurs points.

Emplacement dans le menu RPS

Points > Affectations de point > Sortie

11.1.8 RFID RADION (B810)

Valeur par défaut : vide

Choix : 0, 11 - 167772156

Le numéro RFID est un numéro unique lié aux dispositifs radio en usine.

Lorsque le paramètre Source du point est défini sur Radio, le programmeur définit ce paramètre RFID sur 0. Le RFID peut être Appris automatiquement via un récepteur radio de bus SDI2, ou il peut être entré ici.

Le RFID peut être modifié pour le remplacement du point, ou il peut être défini sur 0 pour désactiver un point radio.

Le programmeur a appliqué des limites radio

La définition du paramètre *Type de module radio, page 293* sur Récepteur RADION B810 limite la centrale à 1512 dispositifs radio : 1000 télécommandes, 504 points (paramètre Source du point défini sur Radio) et 8 répéteurs.

Emplacement dans le menu RPS

Points > Affectations de point > RFID RADION (B810)

11.1.9 Type de dispositif RADION

Valeur par défaut : vide

Choix :

– Bris de vitres
– Fumée
– Inertie
– Contact de fenêtre ou de porte
– Contact de fenêtre ou de porte encastré
– Double technologie
– Détection de mouvement IRP
– Détecteur de plafond
– Universal TX
– Pince à billets

– Détection rideaux
– Détecteur CO
– Panique, 1 bouton
– Panique, deux boutons
– Panique, position fixe
– Chaleur

Chaque type de dispositif RADION inclut quatre fonctions d'entrée. Reportez-vous au tableau ci-après.

Type de dispositif	Fonction d'entrée 1	Fonction d'entrée 2	Fonction d'entrée 3	Fonction d'entrée 4
Bris de vitres	Alarme bris de vitres	Non utilisé	Non utilisé	Non utilisé
Fumée	Alarme fumée	Non utilisé	Non utilisé	Non utilisé
Inertie	Alarme Reed	Boucle d'entrée	Alarme vibration	Non utilisé
Contact de fenêtre ou de porte	Alarme Reed	Non utilisé	Non utilisé	Non utilisé
Contact de fenêtre ou de porte encastré	Alarme Reed	Non utilisé	Non utilisé	Non utilisé
Double technologie	Détection de mouvement	Non utilisé	Non utilisé	Non utilisé
Détection de mouvement IRP	Alarme IRP	Non utilisé	Non utilisé	Non utilisé
Détecteur de plafond	Détection de mouvement	Non utilisé	Non utilisé	Non utilisé
Universal TX	Alarme Reed	Boucle d'entrée	Non utilisé	Non utilisé
Pince à billets	Alarme pince à billets	Non utilisé	Non utilisé	Non utilisé
Détection rideaux	Alarme IRP	Non utilisé	Non utilisé	Non utilisé
Détecteur CO	Alarme CO	Non utilisé	Non utilisé	Non utilisé
Bouton panique 1 bouton	Non utilisé	Non utilisé	Non utilisé	Non utilisé
Bouton panique 2 boutons	Non utilisé	Non utilisé	Non utilisé	Non utilisé
Panique, position fixe	Non utilisé	Non utilisé	Non utilisé	Non utilisé
Chaleur	Alarme de chaleur	Non utilisé	Non utilisé	Non utilisé

Lorsque vous sélectionnez le type de dispositif, vous pouvez activer ou désactiver les fonctions d'entrée en cliquant sur la case correspondante dans la boîte de dialogue.
Le programmeur réinitialise les fonctions d'entrée à leur valeur par défaut lors de la modification du type de dispositif radio.

Emplacement dans le menu RPS
Points > Affectations de point > Type de dispositif RADION

11.1.10 RFID Inovonics (B820)

Valeur par défaut : N/A
Choix : 0 - 167772156
Le numéro RFID est un numéro unique lié aux dispositifs radio en usine.
Lorsque le paramètre Source du point est défini sur Radio, le programmeur définit ce paramètre RFID sur 0. Le RFID peut être Appris automatiquement via un récepteur radio de bus SDI2, ou il peut être entré ici.
Le RFID peut être modifié pour le remplacement du point, ou il peut être défini sur 0 pour désactiver un point radio.

Le programmeur a appliqué des limites radio
La définition du paramètre *Type de module radio, page 293* sur Radio Inovonics B820 limite la centrale à 350 dispositifs radio, en n'incluant pas les répéteurs. La somme des points numériques (paramètre Source du point défini sur Radio) et du nombre de télécommandes ne peut pas être supérieure à 350.

Emplacement dans le menu RPS
Points > Affectations de point > RFID (Radio Inovonics B820)

11.2 Paramètres des points de croisement

11.2.1 Minuterie de points de croisement

Valeur par défaut : 20
Choix : 5-255 (secondes)
Ce paramètre définit le délai d'attente observé par la centrale après un défaut sur un point de croisement pour un deuxième point du même groupe de points de croisement en défaut avant la création d'un événement Alarme de point de croisement. Si un deuxième point n'est pas en défaut pendant la durée du point de croisement, aucune alarme d'événement n'est générée.

Remarque!
Points autres qu'incendie uniquement
Utilisez uniquement la fonction Point de croisement sur des points non incendie.

Paramètres de type de point pris en charge
- 24 heures
- Intérieur
- Suiveur intérieur
- Part active
- Temp. élevée
- Temp. faible
- Eau

Emplacement dans le menu RPS
Points > Paramètres des points de croisement > Minuterie de points de croisement

11.3 Profils de point

Les profils de point (indices de points) déterminent la manière dont la centrale répond aux modifications sur les points. Pour générer des profils de point, utilisez les paramètres de cette section. Affectez des profils de point aux points dans les affectations de point.

Remarque!
Nouvelles configurations de point non prises en charge avec les anciennes versions du firmware de la centrale
L'envoi de configurations de point à des versions antérieures du firmware de la centrale qui ne prennent pas en charge ces configurations ne se passera pas comme prévu. La centrale mettra à jour les types de points non pris en charge vers le type de point par défaut et les conditions d'alarme déclencheront un événement de défaut de point.

11.3.1 Texte du profil de point (première langue)

Valeur par défaut :
- Profil de point 1 - Inst 24h ouvert/court-circuit (24 heures, instantané sur ouvert ou court-circuit)
- Point de profil 2 - Inv 24h/Sil sur Crt (24 heures, invisible et silencieux sur court-circuit)
- Profil de point 3 - Dispositif d'alarme
- Profil de point 4 - Détecteur de fumée
- Profil de point 5 - Fumée avec vérif (détecteur de fumée avec vérification)
- Profil de point 6 - Sup Cloche - D192G (supervision de cloche pour D192G)
- Profil de point 7 - Partielle : Instantané
- Profil de point 8 - Partielle : Temporisation
- Profil de point 9 - Prt:Inst,Désa loc,Buz (partielle, instantané, local quand désarmé, buzz)
- Profil de point 10 - Intérieur : Instantané
- Profil de point 11 - Intérieur : Temporisation
- Profil de point 12 - Int : Inst, Désa loc (intérieur, instantané, local quand désarmé)
- Profil de point 13 - Intérieur : Suiveur
- Profil de point 14 - Interrupteur à clé maintenu
- Profil de point 15 - Interrupteur à clé à impulsion
- Profil de point 16 - Ouverture/Fermeture de point en cas de défaut
- Profil de point 17 - Gaz
- Profil de point 18 - Supervision Gaz
- Profil de point 19 - Supervision secteur auxiliaire
- Profil de point 20 - Partielle : Détection désactivée

Choix : jusqu'à 24 caractères alphanumériques
Entrez jusqu'à 24 caractères de texte pour décrire le profil de point.

Emplacement dans le menu RPS
Points > Profils de point > Texte du profil de point

11.3.2 Texte du profil de point (deuxième langue)

Valeur par défaut : Vide
Choix : jusqu'à 24 caractères alphanumériques

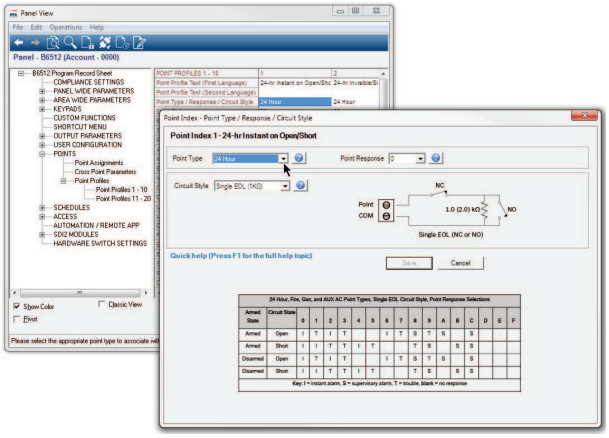
Entrez jusqu'à 24 caractères de texte pour décrire le profil de point (indice de point).

Emplacement dans le menu RPS

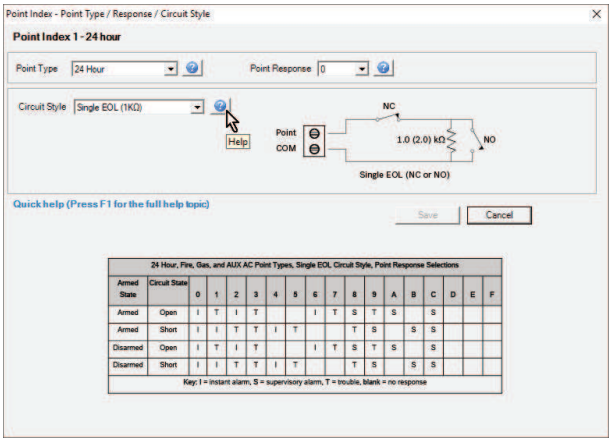
Points > Profils de point > Texte du profil de point (deuxième langue)

11.3.3 Type de point/Réponse/Type de surveillance de ligne

L'affichage des paramètres Type de point, Réponse du point et Type de surveillance de ligne dans une seule fenêtre vous permet de voir l'interaction entre les trois paramètres.



Les paramètres Réponse du point et Type de point déterminent tous les deux comment la centrale répond aux changements sur les boucles de détecteur de point (ouvert, court-circuit, normal) pour les points filaires, ou aux changements dans les états de point pour les dispositifs de point radio (défaillance, normal, défaut).
Pour obtenir de l'aide sur un paramètre individuel, appuyez sur les boutons individuels d'aide dans la fenêtre.



11.3.4 Type de point

Valeur par défaut :

- 24 heures : profils de point 1-2, 6
- Partielle : profils de point 7-9, 20
- Intérieur : profil de point 10-12
- Suiveur intérieur : profil de point 13
- Interrupteur à clé maintenu : profil de point 14
- Interrupteur à clé à impulsion : profil de point 15
- Point d'ouverture/de fermeture : profil de point 16

– Point incendie : profil de point 3-5
– Supervision secteur auxiliaire : profil de point 19
– Point gaz : profil de point 17, 18

Ces types de point peuvent également être utilisés, mais ils ne sont pas associés à des profils de points par défaut :

– Panique

Types de point environnementaux :

– Eau
– Temp. élevée
– Temp. faible

Le paramètre Type de point définit le type de point pour le profil de point.

Choix :

– **24 heures**

Les points 24 heures sont armés tout le temps. Ils peuvent être utilisés pour les alertes panique, médicale et de police.
Si vous créez un point 24 heures pouvant être inhibé (paramètre *Inhibable, page 233* défini sur Oui), définissez le paramètre *Sonnerie de panne, page 229* sur 1, 2 ou 3, et définissez le paramètre *Transmission rapport inhibition, page 234* sur Oui (si une partition n'est jamais armée, les rapports d'inhibition reportés ne sont jamais envoyés).

Remarque!
Exigence UL pour les dispositifs d'alarme effraction
Pour les dispositifs d'alarme effraction dans les installations UL, utilisez le type de point 24 heures. Le texte du point doit inclure « effraction ».

Remarque!
Porte incendie, trappe de toit et applications similaires
Pour les portes incendie, les trappes de toit et autres applications similaires qui nécessitent une surveillance 24 heures, pensez à utiliser le type de point Partielle. Les points 24 heures n'affichent pas un statut en défaut ou inhibé lors de l'armement d'une partition, alors que c'est le cas des points Partielle.
Définissez le paramètre *Réponse du point, page 213* sur 9, A, B, C, D ou E.
Pensez à activer le paramètre Sonnerie de défaut et les paramètres *Local quand désarmé, page 231*.

– **Part active**

Les points lors d'un armement Partiel sont généralement liés aux dispositifs dans le périmètre des locaux (portes et fenêtres).
Lorsqu'un utilisateur arme une partition Tout activé, les points Intérieur et les points Suiveur intérieur sont tous armés.
Lorsqu'un utilisateur arme une partition Partielle, seuls les points Partielle sont armés. Les points Intérieur et Suiveur intérieur ne sont pas armés. Dans un système standard, l'activation d'une partition Partielle arme uniquement la protection périmétrique, ce qui permet aux utilisateurs de rester dans les locaux sans déclencher d'événements d'alarme à partir de points intérieurs.
Le paramètre Points > Profil de point > Réponse du point détermine si les points lors d'un armement Partiel incluent une temporisation d'entrée, ou s'ils créent un événement d'alarme immédiatement en cas de défaut.

La temporisation d'entrée permet aux utilisateurs d'atteindre un clavier et de désarmer sans créer d'événement d'alarme. Par exemple, lorsqu'un utilisateur ouvre la porte d'entrée (mise en défaut d'un point Partielle), la temporisation d'entrée commence. L'utilisateur accède à un clavier et désarme (désactive la partition) avant l'expiration de la temporisation de sortie afin d'empêcher l'événement d'alarme.
Si la partition est en temporisation d'entrée et qu'un second point Partielle se déclenche, la centrale compare la temporisation d'entrée restante à la temporisation d'entrée programmée pour le second point Partielle. Si la temporisation d'entrée du second point est inférieure au temps restant, cela raccourcit la temporisation d'entrée.

Remarque!
Les points Partielle avec une réponse du point instantanée créent des événements d'alarme immédiats
Les points périmètre programmés pour une *Réponse du point, page 213* instantanée ne démarrent pas la temporisation d'entrée lorsqu'ils sont en défaut. Ils génèrent un événement d'alarme immédiatement, même pendant une temporisation d'entrée ou de sortie.

– **Intérieur**

Les points intérieurs sont généralement utilisés pour surveiller des dispositifs de détection intérieurs tels que les portes intérieures et les détecteurs de mouvement.
Les points intérieurs sont armés uniquement lorsque la partition est Tout activé. Ils ne sont pas armés lorsque la partition est Partielle.
Le paramètre Points > Profile de point > Réponse du point configure les points intérieurs pour une réponse d'alarme instantanée ou différée. Les points intérieurs sont généralement configurés pour une réponse d'alarme instantanée.

Remarque!
Les points intérieurs avec une réponse du point instantanée créent des événements d'alarme immédiats
Les points intérieurs programmés pour une *Réponse du point, page 213* instantanée sont en défaut, ils créent des événements d'alarme immédiatement, même pendant une temporisation d'entrée ou de sortie.

Lorsqu'un point intérieur configuré pour une réponse d'alarme différée est en défaut alors que la partition est Tout activé, il démarre la temporisation d'entrée. Il ne crée pas d'événement d'alarme à moins qu'une temporisation d'entrée ne se termine avant que la partition soit désarmée.
Si un point intérieur programmé pour une réponse du point différée est en défaut alors que la temporisation d'entrée est déjà démarrée, la centrale compare la temporisation d'entrée restante à la temporisation d'entrée programmée pour le point intérieur. Si la temporisation d'entrée du point intérieure est inférieure au temps restant, la centrale raccourcit la temporisation d'entrée.

Remarque!
Utilisez le type de point *Suiveur intérieur, page 242* pour une alarme instantanée si la partition n'est pas dans une temporisation d'entrée
Pour certaines installations, vous pouvez choisir un point intérieur qui suit, mais qui ne démarre pas une temporisation d'entrée.

– **Suiveur intérieur**

Les points suiveurs intérieurs sont généralement utilisés pour surveiller des dispositifs de détection intérieurs tels que les portes intérieures et les détecteurs de mouvement.
Les points suiveurs intérieurs sont armés uniquement lorsque la partition est Tout activé. Ils ne sont pas armés lorsque la partition est Partielle.
La neutralisation d'un point suiveur intérieur alors que la partition est Tout activé crée un événement d'alarme instantanée. Si la temporisation d'entrée est démarrée par un autre point avant que le point suiveur intérieur ne se déclenche, le point suiveur intérieur diffère l'événement d'alarme jusqu'à expiration de la temporisation de sortie. Si la partition est désarmée avant la fin de la temporisation d'entrée, il n'y a aucun événement d'alarme.
Pendant la temporisation de sortie, la neutralisation d'un point suiveur intérieur ne crée pas d'événement d'alarme.
Les points suiveurs intérieurs ne démarrent aucune temporisation d'entrée même s'ils sont configurés pour une réponse d'alarme différée (paramètre *Réponse du point, page 213* défini sur 4, 5, 6, 7 ou 8).

Remarque!
Utilisez le type de point Intérieur et la réponse d'alarme différée pour les points intérieurs qui démarrent une temporisation d'entrée
Pour certaines installations, vous pouvez choisir un point intérieur qui démarre un jour d'entrée. La neutralisation d'un point intérieur configuré pour la réponse d'alarme différée (voir *Réponse du point, page 213*) alors que la partition est Tout activé démarre la temporisation d'entrée. La réponse d'alarme est différée jusqu'à ce que la temporisation de sortie se termine. Si la partition est désarmée avant expiration de la temporisation d'entrée, il n'y a pas de réponse d'alarme.

– **Interrupteur à clé maintenu**

Les points Interrupteur à clé maintenu sont utilisés pour l'armement (Tout activé) et le désarmement des partitions.
Pour les points Interrupteur à clé maintenu, lorsque le paramètre Points >Profils de point > Réponse du point est défini sur 1 :

- Lorsque l'état du point est **normal**, la partition est désarmée (désactivée).
- Lorsque l'état du point passe de normal à **ouvert**, la partition est armée sur Tout activé.
- Lorsque l'état du point passe de ouvert à normal, la partition est désarmée (passe à DÉSACTIVÉ).
- Si l'état du point passe à **court-circuit** alors que la partition est armée (Tout activé ou Partielle), la centrale crée un événement d'alarme de point. Si l'état des points passe en court-circuit, alors que la partition est désarmée (désactivée), la centrale crée un événement de défaut de point. Lorsque l'état du point passe en court-circuit à normal ou ouvert, le défaut est rétabli.

Pour les points Interrupteur à clé maintenu, lorsque le paramètre Points >Profils de point > Réponse du point est défini sur 2 :

- Lorsque l'état du point est **ouvert**, la partition est désarmée (désactivée).
- Lorsque l'état du point passe de ouvert à **normal**, la partition est armée sur Tout activé.
- Lorsque l'état du point passe de normal à ouvert, la partition est désarmée (passe à DÉSACTIVÉ).
- Si l'état du point passe à **court-circuit** alors que la partition est armée (Tout activé ou Partielle), la centrale crée un événement d'alarme de point. Si l'état des points passe en court-circuit, alors que la partition est désarmée (désactivée), la centrale crée un événement de défaut de point. Lorsque l'état du point passe en court-circuit à normal ou ouvert, le défaut est rétabli.

Les rapports de défaut et de rétablissement ne sont pas envoyés si le paramètre *Local quand désarmé, page 231* est défini sur Oui.
Les rapports d'alarme et de rétablissement ne sont pas envoyés si le paramètre *Local quand armé, page 232* est défini sur Oui.

Remarque!
La réponse du point 2 est nécessaire pour les dispositifs Radio Inovonics FA113.

– **Interrupteur à clé à impulsion**

Les points interrupteur à clé à impulsion sont utilisés pour l'armement (Tout activé) et le désarmement des partitions.
Pour les points Interrupteur à clé à impulsion, définissez le paramètre Points > Profils de point > Réponse du point sur 1.
Lorsque l'état d'un point interrupteur à clé à impulsion passe de **normal** à **court-circuit** et à **normal**, l'état armé de la partition s'active et se désactive.
Si l'état du point passe à **ouvert** alors que la partition est armée (Tout activé ou Partielle), la centrale crée un événement d'alarme de point. Si l'état des points passé à **ouvert** alors que la partition est désarmée (désactivée), la centrale crée un événement de défaut de point.
Lorsque l'état du point passe de ouvert à normal, le défaut est rétabli.
Les rapports de défaut et de rétablissement ne sont pas envoyés si le paramètre *Local quand désarmé, page 231* est défini sur Oui.
Les rapports de défaut et de rétablissement ne sont pas envoyés si le paramètre *Local quand armé, page 232* est défini sur Oui.

– **Point d'ouverture/de fermeture**

Les points d'ouverture/de fermeture sont armés et désarmés indépendamment de partition à laquelle ils sont liés.
Pour les points d'ouverture/de fermeture, définissez le paramètre Points > Profils de point > Réponse du point sur 1.
Lorsque l'état du point passe en **court-circuit** à **normal**, le point est armé. Les centrales envoient un rapport FERMETURE DE POINT.
Lorsque l'état du point passe de **normal** à **court-circuit**, le point est désarmé. Les centrales envoient un rapport OUVERTURE DE POINT.
Lorsque l'état du point passe de **normal** à **ouvert**, la centrale crée un événement d'alarme de point.
Lorsque l'état du point passe de **court-circuit** à **ouvert**, la centrale crée un événement de défaut de point.

Les rapports FERMETURE DE POINT ne sont pas envoyés si le paramètre *Local quand armé, page 232* est défini sur Oui.
Les rapports ALARME et RÉTABLISSEMENT de point ne sont pas envoyés si le paramètre *Local quand désarmé, page 231* est défini sur Oui.
Les rapports OUVERTURE DE POINT ne sont pas envoyés si le paramètre *Local quand armé, page 232* est défini sur Oui.
Les sirènes locales sont rendues silencieuses à partir du clavier.

– **Point incendie**

Utilisez les points Incendie pour surveiller les dispositifs de détection incendie.
Les alarmes incendie sont les événements dont la priorité est la plus élevée sur la centrale.

– **Supervision CA aux**

Utilisez les points Supervision secteur auxiliaire pour surveiller la source d'alimentation secteur des modules d'alimentation auxiliaires.
Lorsque l'état du point est anormal, la centrale observe le temps d'attente programmé dans le paramètre Temps de défaut secteur avant de créer un événement de défaut de point.
Les points de supervision secteur auxiliaire n'utilisent pas le paramètre *Réponse du point, page 213*. Il n'y a pas d'événements d'alarme pour les points de supervision secteur auxiliaire.
Si des points de supervision secteur auxiliaire sont inhibés, POINT INHIBÉ 24 HEURES s'affiche sur les claviers.

– **Point gaz**

Utilisez les points gaz pour surveiller les dispositifs de détection gaz.

– **Fonction personnalisée**

Utilisez les points de fonction personnalisée pour activer les fonctions personnalisées.
Utilisez les paramètres de la section *Fonctions personnalisées, page 138* pour configurer des fonctions personnalisées.

– **Point Eau**

Utilisez le point Eau pour surveiller les dispositifs de détection d’eau.

– **Temp. élevée**

Utilisez le point Temp. élevée pour surveiller les dispositifs de détection de température élevée.

– **Temp. faible**

Utilisez le point Temp. faible pour surveiller les dispositifs de détection de température faible.

– **Panique**

Utilisez le point Panique pour surveiller les alarmes de panique. Un point Panique fonctionne de la même manière qu’un point 24 heures.

Emplacement dans le menu RPS

Points > Profils de point > Type de point/Réponse/Type de surveillance de ligne

11.3.5 Vue d'ensemble des réponses du point

Applications pour les réponses du point 9, D et E

Vous pouvez combiner les réponses du point 9, D et E avec les types de point périmètre pour créer une protection 24 heures plus flexible. Contrairement aux points 24 heures, un point périmètre en défaut avec une réponse du point D et E s'affiche sur le clavier lors de l'armement. Comme un point 24 heures, un point programmé de cette façon peut générer des alarmes si la partition est armée ou désarmée.
La combinaison de la réponse du point 9 avec la fonction Local quand désarmé permet une génération de rapports hors site lorsque la partition est armée, mais seulement une annonce d'alarme locale lorsque la partition est désarmée.
La combinaison de la réponse du point 9 avec la fonction Local quand armé permet une génération de rapports hors site lorsque la partition est désarmée, mais seulement une annonce d'alarme locale lorsque la partition est armée.
La réponse du point E utilise cela pour les détecteurs de mouvement Asic. Cela permet de signaler les défauts lorsque la centrale est Tout activé.
La réponse du point F n'émet pas de son sur les claviers locaux, mais elle active le Type de réponse de sortie et les défauts de clavier. Pour annoncer l'état anormal au niveau du clavier, définissez Affichage en tant que dispositif sur Oui et/ou Sonnerie de panne sur 1 ou 2. Cette réponse du point ne génère pas d'alarmes et n'active aucune sortie d'alarme.
Les réponses du point 8, 9, A, B et C fournissent des rapports de supervision (24 heures).

Caractéristiques du point incendie

1. Création de rapports : les rapports incendie sont les premiers événements envoyés par la centrale lorsqu'un groupe d'événements se produit.
2. Annonce visuelle : les défauts incendie continuent de défiler jusqu'à ce que le défaut soit effacé. Une fois reconnu, le défilement du DÉFAUT INCENDIE permet à l'utilisateur final de savoir si un point incendie, ou un groupe de points incendie, est toujours en défaut. Les sorties liées à la centrale, les résumés incendie et les défauts incendie s'activent si une sortie est liée lorsqu'un point incendie déclenche une alarme ou est en défaut.
3. Avertissement sonore : un point incendie active la sirène incendie. La durée et le modèle de l'activation de sortie sont programmés par partition dans le modèle Durée incendie et Incendie.
4. Supervision : un point incendie peut envoyer un rapport SUPERVISION INCENDIE et activer les sorties de niveau centrale Résumé de supervision d'incendie et Résumé défaut incendie avec une réponse du point 8, 9, A, B, C.
5. Vérification d'alarme : un point incendie peut temporiser une alarme par la durée programmée dans les paramètres Durée de redémarrage de la partition. Associé à Réinitialisable, un point incendie réinitialise également le circuit électrique pendant la Durée de redémarrage.
6. Réinitialiser les détecteurs : un dispositif incendie qui requiert une réinitialisation peut être manuellement réinitialisé à l'aide de la sortie de réinitialisation de détecteur pour la partition à laquelle il est lié.
7. Détection incendie : utilisez la fonction Détection incendie pour tester les points incendie sur le système.

Afin de fournir un signal sonore pour un point de supervision incendie qui est rétabli, utilisez le type de réponse de sortie et connectez-vous à un signalisateur graphique.
Vous devez dédier un dispositif d'annonce incendie à tous vos points incendie s'ils sont liés à une seule partition dans un système à plusieurs partitions.

11.3.6 Réponse du point

Valeur par défaut :

	Profil du point									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Valeur par défaut de la réponse du point	0	1	1	1	1	9	0	8	9	0

Tableau 11.1: B Series

	Profil du point									
	11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Valeur par défaut de la réponse du point	8	9	8	1	1	1	1	9	0	0

Choix : 0 - 9, A - F

L'affichage des paramètres Type de point, Réponse du point et Type de surveillance de ligne dans une seule fenêtre vous permet de voir l'interaction entre les trois paramètres.

Les paramètres Réponse du point et Type de point déterminent tous les deux comment la centrale répond aux changements sur les boucles de détecteur de point (ouvert, court-circuit, normal) pour les points filaires, ou aux changements dans les états de point pour les dispositifs de point radio (défaillance, normal, défaut).
Les tableaux ci-dessous affichent les sélections de réponse du point pour :

- 24 heures, Incendie, Gaz, Panique et Supervision secteur auxiliaire
- Types de point contrôlés : Partielle, Intérieur et Suiveur intérieur
- Interrupteur à clé maintenu
- Interrupteur à clé à impulsion
- Point d'ouverture/de fermeture
- Fonction personnalisée
- Eau, Temp. élevée et Temp. faible

Remarque!
La modification du type de point définit automatiquement le paramètre Réponse du point sur sa valeur par défaut
La sélection d'un type de point définit automatiquement le paramètre Réponse du point sur sa valeur par défaut pour ce type de point.

Types de point 24 heures, Incendie, Gaz, Panique et Secteur auxiliaire, Type de surveillance de ligne Résistance de fin de ligne unique, Sélections de réponse du point

Etat armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Ouvert	I	T	I	T			I	T	S	T	S		S			
Armé	Court-circuit	I	I	T	T	I	T			T	S		S	S			
Désarmé	Ouvert	I	T	I	T			I	T	S	T	S		S			
Désarmé	Court-circuit	I	I	T	T	I	T			T	S		S	S			

Touche : I = alarme instantanée, **S** = alarme de supervision, **T** = défaut, **vide** = aucune réponse

Exemple : Type de point = 24 heures et Réponse du point = 8, Point 24 heures avec réponse de supervision si ouvert et réponse de défaut si court-circuité.

Types de point 24 heures, Incendie, Panique et Gaz, Type de surveillance de ligne Résistance de fin de ligne double, Sélections de réponse du point

Etat armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Ouvert/ Court-circuit	T	I	T	I												
Armé	Défaut	I	I	S	S												
Désarmé	Ouvert/ Court-circuit	T	I	T	I												

Types de point 24 heures, Incendie, Panique et Gaz, Type de surveillance de ligne Résistance de fin de ligne double, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Désarmé	Défaut	I	I	S	S												
Touche : I = alarme instantanée, **S** = alarme de supervision, **T** = défaut, **vide** = aucune réponse																	

Exemple : Type de point = 24 heures et Réponse du point = 2, Point 24 heures avec réponse de supervision pour défaut et réponse de défaut pour ouvert ou court-circuité.

Types de point 24 heures, Incendie, Panique et Gaz, Résistance de fin de ligne unique avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert	TA	TA	TA	I	T			I	T							
Armé	Court-circuit	I	T	TA	TA	TA	I	T									
Désarmé	Ouvert	TA	TA	TA	I	T			I	T							
Désarmé	Court-circuit	I	T	TA	TA	TA	I	T									
Touche : I = alarme instantanée, **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																	

Exemple : Type de point = 24 heures et Réponse du point = 4, Point 24 heures avec réponse de défaut si ouvert et réponse d'alarme d'auto-surveillance si court-circuité.

Types de point 24 heures, Incendie, Panique et Gaz, Résistance de fin de ligne double avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert/ Court-circuit	TA	TA	TA	TA												
Armé	Défaut	I	T	TA													
Désarmé	Ouvert/ Court-circuit	TA	TA	TA	TA												
Désarmé	Défaut	I	T	TA													
Touche : I = alarme instantanée, **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																	

Exemple : Type de point = 24 heures et Réponse du point = 1. Point 24 heures avec réponse de défaut pour Défaut et réponse d'alarme d'auto-surveillance pour ouvert ou court-circuité.

Remarque!
Les exigences de firmware de la centrale pour une résistance de fin de ligne unique avec auto-surveillance et une résistance de fin de ligne double avec un type de surveillance de ligne d'auto-surveillance.
Pour utiliser une résistance de fin de ligne unique avec auto-surveillance ou une résistance de fin de ligne double avec un type de surveillance de ligne d'auto-surveillance, assurez-vous que le firmware de la centrale est v3.06 ou version ultérieure.

Remarque!
Pour les types de surveillance de ligne résistance de fin de ligne double, achetez une deuxième résistance de fin de ligne de 1 kΩ **séparément**
Commandez la référence ICP-1K22AWG-10, lot de 10 résistances.

Remarque!
Pour les types de surveillance de ligne de résistance de fin de ligne double, les états des circuits sont normal, défaillance, court-circuit, ouvert
Normal - le contact NF (normalement fermé) indiqué dans le schéma du circuit est fermé.
Défaillance - le contact NF indiqué dans le schéma du circuit est ouvert.
Court-circuit - la boucle de capteur est court-circuitée.
Ouvert - le circuit de boucle de capteur est ouvert.

Remarque!
Exigences de firmware pour la centrale et le module huit entrées B208 pour la double résistance
Pour utiliser le Type de surveillance de ligne Double résistance , assurez-vous que le firmware de la centrale est en version 3.01 ou supérieure.
Si vous utilisez un module huit entrées B208, assurez-vous que le firmware du module est version 2.1.1 ou supérieure.

Types de point 24 heures, Incendie, Panique et Gaz, Type de surveillance de ligne Aucune résistance de fin de ligne, Sélections de réponse du point

Etat armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Défaut	I	T	S													
Désarmé	Défaut	I	T	S													

Touche : I = alarme instantanée, **S** = alarme de supervision, **T** = défaut, **vide** = aucune réponse

Exemple : Type de point = 24 heures et Réponse du point = 2, Point 24 heures avec réponse de supervision pour défaut et réponse de défaut pour ouvert ou court-circuité.

Remarque!
Pour le Type de surveillance de ligne Aucune résistance de fin de ligne, les états des circuits sont normaux et défaillance,
dans la fenêtre Diagnostic de point, l'état du circuit est ouvert ou court-circuit
Dans les tableaux de réponse de point, les états des circuits sont normaux et défaillance pour Type de surveillance de ligne Aucune résistance de fin de ligne. Le paramètre *État normal, page 240* définit les états de circuit normal et défaillance.
Pour les points Type de surveillance de ligne Aucune résistance de fin de ligne, la fenêtre de diagnostics de point affiche ouvert ou court-circuit dans la colonne d'état du circuit.

Types de point contrôlés, Type de surveillance de ligne Résistance de fin de ligne unique, Sélections de réponse du point																
État armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvrir	I	I	I	I	D	D	I	I	D	I	I	I	I	I	T	
Armé	Court-circuit	I	I	I	I	I	I	D	D	D	I	I	I	I	I	I	
Désarmé	Ouvrir		T		T				T		I	I	T	I		T	
Désarmé	Court-circuit			T	T		T				I	T	I		I		
Touche : I = alarme instantanée, **D** = alarme différée, **T** = défaut, **vide** = aucune réponse																	

Exemple : Type de point = Partielle et Réponse du point = 8. Point périmètre avec réponse d'alarme différée si armé (ouvert ou court-circuité) et aucune réponse si désarmé.

Types de point contrôlés, Type de surveillance de ligne Résistance de fin de ligne double, Sélections de réponse du point																
État armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert/ Court-circuit	I	I	I	I	I	I	I	I								
Armé	Défaut	I	D	I	D	I	D	I	D								
Désarmé	Ouvert/ Court-circuit	T	T	I	I	T	T	I	I								
Désarmé	Défaut					T	T	T	T								
Touche : I = alarme instantanée, **D** = alarme différée, **T** = défaut, **vide** = aucune réponse																	

Exemple : Type de point = Partielle et Réponse du point = 1. Lorsque la partition est armée (Tout activé, Partielle), un défaut sur le circuit de point crée une réponse d'alarme différée. Une ouverture ou un court-circuit sur le circuit de point crée une alarme instantanée. Lorsque la partition est désarmée (désactivée), une ouverture ou un court-circuit sur le circuit de point crée un défaut de point. Il n'y a pas de réponse pour un défaut sur le circuit de point.

Types de point contrôlés, Résistance de fin de ligne unique avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert	TA	TA	TA	TA	TA	TA	I	D	T	T	I	D				
Armé	Court-circuit	I	D	T	T	I	D	TA	TA	TA	TA	TA	TA				
Désarmé	Ouvert	TA	TA	TA	TA	TA	TA				T	I	D				

Types de point contrôlés, Résistance de fin de ligne unique avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Désarmé	Court-circuit				T	I	D	TA	TA	TA	TA	TA	TA				
Touche : I = alarme instantanée, **D** = alarme différée, **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																	

Exemple : Type de point = Partie activée et Réponse de point = 3. Point périmètre avec réponse d'alarme d'auto-surveillance lorsqu'il est ouvert (armé ou désarmé). Réponse défaut lorsque court-circuit (armé ou désarmé)

Types de point contrôlés, Résistance de fin de ligne double avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert/ Court-circuit	TA	TA	TA	TA	TA	TA										
Armé	Panne	I	D	I	D	T	T										
Désarmé	Ouvert/ Court-circuit	TA	TA	TA	TA	TA	TA										
Désarmé	Panne			T	T		I										
Touche : I = alarme instantanée, **D** = alarme différée, **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																	

Exemple : Type de point = Partie activée et Réponse de point = 1. Point périmètre avec réponse d'alarme d'auto-surveillance lorsqu'il est court-circuité ou ouvert (armé ou désarmé). Retard de réponse de l'alarme pour défaut (armée ou désarmée).

Remarque!
Les exigences de firmware de la centrale pour une résistance de fin de ligne unique avec auto-surveillance et une résistance de fin de ligne double avec un type de surveillance de ligne d'auto-surveillance.
Pour utiliser une résistance de fin de ligne unique avec auto-surveillance ou une résistance de fin de ligne double avec un type de surveillance de ligne d'auto-surveillance, assurez-vous que le firmware de la centrale est v3.06 ou version ultérieure.

Remarque!
Pour le Type de surveillance de ligne double Résistance EOL, mettre des résistances 1 kΩ **séparément**
Commandez la référence ICP-1K22AWG-10, lot de 10 résistances.

Remarque!
Pour les types de surveillance de ligne de résistance de fin de ligne double, les états des circuits sont normal, défaillance, court-circuit, ouvert
Normal - le contact NF (normalement fermé) indiqué dans le schéma du circuit est fermé.
Défaillance - le contact NF indiqué dans le schéma du circuit est ouvert.
Court-circuit - la boucle de capteur est court-circuitée.
Ouvert - le circuit de boucle de capteur est ouvert.

Remarque!
Exigences de firmware pour la centrale et le module huit entrées B208 pour la double résistance
Pour utiliser le Type de surveillance de ligne avec une double résistance OEL, vérifiez que le firmware de la centrale est en version 3.01 ou supérieure.
Si vous utilisez un module huit entrées B208, vérifiez que le firmware du module est version 2.1.1 ou supérieure.

Types de point contrôlés, Type de surveillance de ligne Aucune résistance de fin de ligne, Sélections de réponse du point

État armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Défaut	I	I	D	D	T											
Désarmé	Défaut		T		T	T											
Touche : I = alarme instantanée, **D** = alarme différée, **T** = défaut, **vide** = aucune réponse																	

Exemple : Type de point = Partielle et Réponse du point = 2. Lorsque la partition est armée (Tout activé, Partielle), un défaut sur le circuit de point crée une réponse d'alarme différée. Lorsque la partition est désarmée (désactivée), il n'y a pas de réponse pour un défaut sur le circuit de point.

Remarque!
Pour le Type de surveillance de ligne Aucune résistance de fin de ligne, les états des circuits sont normaux et défaillance,
dans la fenêtre Diagnostic de point, l'état du circuit est ouvert ou court-circuit
Dans les tableaux de réponse de point, les états des circuits sont normaux et défaillance pour Type de surveillance de ligne Aucune résistance de fin de ligne. Le paramètre *État normal, page 240* définit les états de circuit normal et défaillance.
Pour les points Type de surveillance de ligne Aucune résistance de fin de ligne, la fenêtre de diagnostics de point affiche ouvert ou court-circuit dans la colonne d'état du circuit.

Type de point Interrupteur à clé maintenu, Sélections de réponse du point

État armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Ouvrir			D													
Armé	Court-circuit		I	I													
Désarmé	Ouvrir		A														

Type de point Interrupteur à clé maintenu, Sélections de réponse du point																	
État armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Désarmé	Court-circuit		T	T													
Touche : A = la transition de normal à ouvert change l'état d'armement à armé, **D** = la transition de normal à ouvert change l'état d'armement à désarmé, **I** = alarme instantanée, **T** = défaut, **vide** = aucune réponse																	

Lorsque la réponse du point est définie sur 1 et que le circuit de point est normal, la partition est désarmée (désactivée). Lorsque le circuit de point passe de l'état normal à ouvert, la partition est armée (Tout activé). Lorsque le circuit de point passe de l'état ouvert à normal, la partition est désarmée (désactivée).
Lorsque la réponse du point est définie sur 2 et que le circuit de point est normal, la partition armée (Tout activé). Lorsque le circuit de point passe de l'état normal à ouvert, la partition est désarmée (désactivée). Lorsque le circuit de point passe de l'état ouvert à normal, la partition est armée (Tout activé).
Un court-circuit sur le circuit de point crée un défaut de point alors que la partition est désarmée (désactivée). Un court-circuit sur le circuit de point alors que la partition est armée crée une alarme instantanée. Lorsque le circuit de point revient à l'état normal ou ouvert, le défaut est rétabli.

Type de point Interrupteur à clé à impulsion, Sélections de réponse du point																	
État armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvrir		I														
Armé	Court-circuit		D														
Désarmé	Ouvrir		T														
Désarmé	Court-circuit		A														
Touche : A = la transition de normal à court-circuit et normal change l'état d'armement à armé, **D** = la transition de normal à ouvert change l'état d'armement à désarmé, **I** = alarme instantanée, **T** = défaut, **vide** = aucune réponse																	

La réponse du point est fixée à 1 pour le type de point Interrupteur à clé à impulsion. Si le circuit de point passe de l'état normal en court-circuit et normal, l'état armé de la partition est activé/désactivé. Si la partition est armée (Tout activé, Partielle), elle est désarmée (désactivée). Si la partition est désarmée, elle est armée (Tout activé).
Une ouverture sur le circuit de point crée un défaut de point alors que la partition est désarmée (désactivée). Une ouverture sur le circuit de point alors que la partition est armée (Tout activé, Partielle) crée une alarme instantanée. Lorsque le circuit de point passe de l'état ouvert à normal, le défaut est rétabli.

Type de Point d'ouverture/de fermeture, Sélections de réponse du point																	
État armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvrir		I														

Type de Point d'ouverture/de fermeture, Sélections de réponse du point																	
État armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Court-circuit		D														
Désarmé	Ouvrir		T														
Désarmé	Court-circuit		D														
Touche : D = la transition de normal à court-circuit fait passer l'état d'armement du point à désarmé (l'étant d'armement du point est armé lorsque l'état du circuit de point est normal), **I** = alarme instantanée, **T** = défaut, **vide** = aucune réponse																	

La réponse du point est fixée à 1 pour le type de point d'ouverture/de fermeture.
Si le circuit du point passe à l'état normal, le point est armé. La centrale envoie un rapport de fermeture de point. Si le circuit passe de l'état normal à ouvert, une alarme de point instantanée est créée.
Si le circuit passe à l'état court-circuit, le point est désarmé. La centrale envoie un rapport de fermeture de point. Si le circuit passe de l'état court-circuit à ouvert, un défaut de point est créé.

Type de point Fonction personnalisée, Type de surveillance de ligne Résistance de fin de ligne unique, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert							CF	CF	T	CF		CF	CF	T	CF	
Armé	Court-circuit						CF		CF	CF	T	CF		CF	CF	T	
Désarmé	Ouvert		CF	CF	T	CF		CF	CF	T	CF						
Désarmé	Court-circuit	CF		CF	CF	T	CF		CF	CF	T						
Touche : CF = la centrale exécute une fonction personnalisée lors de la transition vers l'état du circuit. **T** = défaut, **vide** = aucune réponse																	

Lorsque l'état du circuit de point change, la centrale répond en commençant une fonction personnalisée.

Type de point Fonction personnalisée, Type de surveillance de ligne double Résistance , Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert/ Court-circuit						T	T	T	T	T	T	T	T	T	T	
Armé	Panne		T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	CF	T	

Type de point Fonction personnalisée, Type de surveillance de ligne double Résistance , Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Désarmé	Ouvert/ Court-circuit						T	T	T	T	T	T	T	T	T	T	
Désarmé	Panne		CF	T	CF		CF	CF	CF	T	CF	CF	CF	CF	CF	T	
Touche : CF = la centrale exécute une fonction personnalisée lors de la transition vers l'état du circuit. **T** = défaut, **vide** = aucune réponse																	

Lorsque l'état du circuit de point change, la centrale répond en commençant une fonction personnalisée.

Type de point Fonction personnalisée, Résistance de fin de ligne unique avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert	TA	TA	TA	TA	TA	CF	T	CF	CF							
Armé	Court-circuit	CF	T	CF	CF		TA	TA	TA	TA	TA						
Désarmé	Ouvert	TA	TA	TA	TA	TA	CF	CF	T		CF						
Désarmé	Court-circuit	CF	CF	T		CF	TA	TA	TA	TA	TA						
Touche : CF = la centrale exécute une fonction personnalisée lors de la transition vers l'état du circuit. **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																	

Lorsque l'état du circuit de point change, la centrale répond en commençant une fonction personnalisée.

Type de point Fonction personnalisée, Résistance de fin de ligne double avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																	
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert/ Court-circuit	TA	TA	TA	TA	TA											
Armé	Panne	CF		CF	T	CF											
Désarmé	Ouvert/ Court-circuit	TA	TA	TA	TA	TA											
Désarmé	Panne		CF	CF	CF	T											
Touche : CF = la centrale exécute une fonction personnalisée lors de la transition vers l'état du circuit. **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																	

Lorsque l'état du circuit de point change, la centrale répond en commençant une fonction personnalisée.

Remarque!
Les exigences de firmware de la centrale pour une résistance de fin de ligne unique avec auto-surveillance et une résistance de fin de ligne double avec un type de surveillance de ligne d'auto-surveillance.
Pour utiliser une résistance de fin de ligne unique avec auto-surveillance ou une résistance de fin de ligne double avec un type de surveillance de ligne d'auto-surveillance, assurez-vous que le firmware de la centrale est v3.06 ou version ultérieure.

Remarque!
Pour le Type de surveillance de ligne double Résistance EOL, mettre des résistances 1 kΩ **séparément**
Commandez la référence ICP-1K22AWG-10, lot de 10 résistances.

Remarque!
Pour les types de surveillance de ligne de résistance de fin de ligne double, les états des circuits sont normal, défaillance, court-circuit, ouvert
Normal - le contact NF (normalement fermé) indiqué dans le schéma du circuit est fermé.
Défaillance - le contact NF indiqué dans le schéma du circuit est ouvert.
Court-circuit - la boucle de capteur est court-circuitée.
Ouvert - le circuit de boucle de capteur est ouvert.

Remarque!
Exigences de firmware pour la centrale et le module huit entrées B208 pour la double résistance
Pour utiliser le Type de surveillance de ligne avec une double résistance OEL, vérifiez que le firmware de la centrale est en version 3.01 ou supérieure.
Si vous utilisez un module huit entrées B208, vérifiez que le firmware du module est version 2.1.1 ou supérieure.

Type de point Fonction personnalisée, Type de surveillance de ligne Aucune résistance de fin de ligne, Sélections de réponse du point

Etat armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Panne		T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	CF	T	
Désarmé	Panne		CF	T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	T	

Touche : CF = la centrale exécute une fonction personnalisée lors de la transition vers l'état du circuit. **T** = défaut, **vide** = aucune réponse

Lorsque l'état du circuit de point change, la centrale répond en activant une fonction personnalisée.

Remarque!
Pour le Type de surveillance de ligne Aucune résistance de fin de ligne, les états des circuits sont normaux et défaillance,
dans la fenêtre Diagnostic de point, l'état du circuit est ouvert ou court-circuit
Dans les tableaux de réponse de point, les états des circuits sont normaux et défaillance pour Type de surveillance de ligne Aucune résistance de fin de ligne. Le paramètre *État normal, page 240* définit les états de circuit normal et défaillance.
Pour les points Type de surveillance de ligne Aucune résistance de fin de ligne, la fenêtre de diagnostics de point affiche ouvert ou court-circuit dans la colonne d'état du circuit.

Types de point : Eau, Temp. élevée, Temp. faible, Type de surveillance de ligne Aucune résistance de fin de ligne, Sélections de réponse du point

Etat armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Défaut	I	T														
Désarmé	Défaut	I	T														

Touche : I = alarme instantanée, **S** = alarme de supervision, **T** = défaut, **vide** = aucune réponse

Types de point : Eau, Temp. élevée, Temp. faible, Type de surveillance de ligne Résistance de fin de ligne unique, Sélections de réponse du point

Etat armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Ouvert	I	T	I	T			I	T								
Armé	Court-circuit	I	I	T	T	I	T										
Désarmé	Ouvert	I	T	I	T			I	T								
Désarmé	Court-circuit	I	I	T	T	I	T										

Touche : I = alarme instantanée, **S** = alarme de supervision, **T** = défaut, **vide** = aucune réponse

Types de point : Eau, Temp. élevée, Temp. faible, Type de surveillance de ligne Résistance de fin de ligne double, Sélections de réponse du point

Etat armé	État du circuit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armé	Ouvert/ Court-circuit	T	I	T	I												
Armé	Défaut	I	I	T	T												
Désarmé	Ouvert/ Court-circuit	T	I	T	I												
Désarmé	Défaut	I	I	T	T												

Touche : I = alarme instantanée, **S** = alarme de supervision, **T** = défaut, **vide** = aucune réponse

Types de point : Eau, Temp. élevée, Temp. faible, Résistance de fin de ligne unique avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert	TA	TA	TA	I	T			I	T							
Armé	Court-circuit	I	T	TA	TA	TA	I	T									
Désarmé	Ouvert	TA	TA	TA	I	T			I	T							
Désarmé	Court-circuit	I	T	TA	TA	TA	I	T									
Touche : I = alarme instantanée, **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																	

Types de point : Eau, Temp. élevée, Temp. faible, Résistance de fin de ligne double avec Type de surveillance de ligne d'auto-surveillance, Sélections de réponse du point																
Etat armé	**État du circuit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armé	Ouvert/ Court-circuit	TA	TA	TA	TA												
Armé	Défaut	I	T	TA													
Désarmé	Ouvert/ Court-circuit	TA	TA	TA	TA												
Désarmé	Défaut	I	T	TA													
Touche : I = alarme instantanée, **T** = défaut, **TA** = alarme d'auto-surveillance, **vide** = aucune réponse																

Remarque!
Alarmes de supervision et d'autosurveillance pour les points environnementaux
Pour les points environnementaux, les réponses en cas d'alarme Supervision et alarme d'autosurveillance sont interprétées comme des réponses de point de défaillance.

Réponse du point pour le module d'interface Inovonics SDI2 B820
Lorsque le paramètre Source du point est défini sur Radio et que le paramètre Type de module radio est défini sur Radio Inovonics B820, les points radio :
- envoient Court-circuit pour le défaut de point (quel que soit l'état ouvert/court-circuit de la boucle du capteur)
- envoient Ouvert pour un événement d'auto-surveillance (cache du coffret retiré)

Réponse du point pour le récepteur B810 RADION SD
Lorsque Source de point est défini sur Radio et que le paramètre Type de module radio est défini sur Radio RADION B810, les points radio :
- envoient Ouvert ou Court-circuit pour un défaut de point (état électrique de la boucle de capteur)
- envoie Court-circuit pour le commutateur à lames (aimant non présent)
- envoient Auto-surveillance pour un événement d'auto-surveillance (cache du coffret retiré)

Emplacement dans le menu RPS
Points > Indices de point > Type de point / Réponse / Type de surveillance de ligne

Pour obtenir de plus amples informations
Type de point, page 207
Type de surveillance de ligne, page 226
État normal, page 240

11.3.7 Type de surveillance de ligne

Valeur par défaut : Résistance de fin de ligne unique (1KΩ)
Choix :

- Résistance de fin de ligne unique (1KΩ)
- Résistance de fin de ligne unique (2KΩ)
- Résistance de fin de ligne double (1KΩ)
- Aucun EOL
- Résistance de fin de ligne unique (1KΩ) avec auto-surveillance
- Résistance de fin de ligne unique (2KΩ) avec auto-surveillance
- Résistance de fin de ligne double (1 kΩ) avec auto-surveillance

Sélectionnez le type de surveillance de ligne et la résistance de fin de ligne pour la boucle de détecteur de point.
La sélection Résistance de fin de ligne unique (1KΩ) est valide pour toutes les sources de point.
La sélection Résistance de fin de ligne unique (1KΩ) avec auto-surveillance est valide uniquement pour les sources de point Huit entrées (B208), Intégré, Sortie, Clavier, Caméra IP et Porte.
Les sélections Résistance de fin de ligne unique (2KΩ), Résistance de fin de ligne unique (2KΩ) avec auto-surveillance, Résistance de fin de ligne double (1KΩ), Résistance de fin de ligne double (1 kΩ) avec auto-surveillance et Aucune résistance de fin de ligne sont uniquement valides pour les sources de point Intégré et Huit entrées (B208).

Remarque!
Résistances de fin de ligne pour dispositifs de point ZONEX, radio, POPEX
Lorsque le paramètre POINTS > Affectations de points > Source est défini sur ZONEX, Radio ou POPEX, définissez Type de surveillance de ligne sur Résistance de fin de ligne unique (1KΩ).
Même si Type de surveillance de ligne est défini sur Résistance de fin de ligne unique (1KΩ), **ne remplacez pas** les résistances de fin de ligne fournies avec les dispositifs de point ZONEX, POPEX ou radio par des résistances de fin de ligne 1KΩ.

Remarque!
Exigences de firmware pour la centrale du type de surveillance de ligne
Le paramètre Type de surveillance de ligne n'est pas disponible pour le firmware de centrale version 2.xx.
La sélection de résistance Résistance de fin de ligne double (1KΩ) est disponible pour le firmware de centrale version v3.01 et version ultérieure.
Les sélections Résistance de fin de ligne unique (2KΩ) et Aucune résistance de fin de ligne sont disponibles pour le firmware de centrale version 3.03 et ultérieure.
Les sélections Résistance de fin de ligne unique (1KΩ) avec auto-surveillance, Résistance de fin de ligne double (2KΩ) avec auto-surveillance et Résistance de fin de ligne double (1KΩ) avec auto-surveillance sont disponible pour le firmware de centrale version v3.06 et version ultérieure.

Emplacement dans le menu RPS
Points > Profils de point > Type de point/Réponse/Type de surveillance de ligne

Pour obtenir de plus amples informations
Type de point, page 207
Réponse du point, page 213

11.3.8 Temporisation d'entrée

Valeur par défaut : 30 secondes
Choix : 5 - 600 secondes (incréments de 5 secondes)
Entrez le nombre de secondes de la temporisation d'entrée. La temporisation d'entrée donne aux utilisateurs le temps de désarmer avant que la centrale ne crée d'événement d'alarme.
Si la temporisation d'entrée se termine avant que l'utilisateur ne désarme, la centrale crée un événement d'alarme.
La temporisation d'entrée démarre lorsqu'un utilisateur met en défaut un point avec le paramètre *Type de point, page 207* défini sur Partielle, Intérieur ou Suiveur intérieur et que le paramètre *Réponse du point, page 213* est défini sur 4, 5, 6, 7 ou 8.
Si un autre point de temporisation est en défaut alors que la partition est déjà dans une temporisation d'entrée, la centrale ajuste la temporisation sur le point de temporisation avec une durée de temporisation moins importante.

Remarque!
Exigence UL
Pour être en conformité avec les normes UL, la durée totale entrée dans Temporisation d'entrée et *Annulation d'alarme, page 237* ne doit pas être supérieure à 1 minute.

Remarque!
SIA CP-01 Exigence de réduction des fausses alarmes
Pour être en conformité avec la norme SIA CP-01 Réduction des fausses alarmes, définissez ce paramètre sur une valeur comprise entre 30 et 240 secondes pour tous les profils de point. Pour plus d'informations, consultez la norme SIA CP-01 Vérification.

Emplacement dans le menu RPS
Points > Profils de point > Temporisation d'entrée

11.3.9 Tonalité d'entrée désactivée

Valeur par défaut : Non (pour tous les profils de point)
Choix :
- Oui : la tonalité d'entrée ne démarre pas lorsque ce point démarre une temporisation d'entrée.
- Non : la tonalité d'entrée démarre lorsque ce point démarre la temporisation d'entrée.

Ne définissez pas ce paramètre sur Oui pour les points utilisés pour indiquer à l'utilisateur de désarmer après l'entrée dans les locaux.
Pour supprimer la tonalité d'entrée par clavier, définissez le paramètre Claviers > Affectations de clavier > *Tonalité d'entrée, page 127* sur Non.

Emplacement dans le menu RPS
Points > Profils de point > Tonalité d'entrée désactivée

11.3.10 Sirène silencieuse

Valeur par défaut :

– Profil de point 2 : Oui
– Tous les autres profils de point : Non

Choix :

– Oui : activer la sortie Alarme silencieuse lorsque ce point déclenche une alarme. N'activez pas la sortie Sirène d'alarme ou les sirènes d'alarme du clavier. Ce paramètre n'a aucun effet sur les points Incendie et Gaz.
– Non : ne pas activer la sortie Alarme silencieuse lorsque ce point déclenche une alarme.

Remarque!

La sirène d'alarme s'active au bout de deux tentatives échouées vers le récepteur du centre de télésurveillance

Si vous définissez le paramètre *Sonore après deux échecs, page 228* sur Oui, la *Sirène d'alarme, page 146* s'active au bout de deux échecs d'envoi d'un rapport d'alarme silencieuse au récepteur du centre de télésurveillance.

Emplacement dans le menu RPS

Points > Profils de point > Sirène silencieuse

11.3.11 Réponse d'auto-surveillance

Valeur par défaut : Alarme permanente

Choix :

– Alarme permanente - les alarmes d’auto-surveillance point sont toujours audibles et visibles (par défaut).
– Alarme quand désarmé - les alarmes d’auto-surveillance point sont silencieuses et invisibles tant que la partition du point est désarmée (valeur par défaut du panneau CHI).

Emplacement dans le menu RPS

Points > Profils de point > Option d’auto-surveillance point

11.3.12 Sonnerie jusqu'au rétablissement

Valeur par défaut : Non (pour tous les profils de point)

Choix :

– Oui : les sorties Sirène incendie ou Sirène gaz (et les sirènes de clavier) ne peuvent pas être rendues silencieuses tant que le point n'est pas restauré à l'état normal. Si le point est restauré et que l'alarme n'est pas rendue silencieuse, la sortie continue jusqu'à expiration de la durée incendie ou gaz. Si le point n'est pas rétabli, la sortie se poursuit même après expiration de la durée incendie ou gaz.
– Non : les sorties Sirène incendie ou Sirène gaz (et les sirènes d'alarme du clavier) peuvent être rendues silencieuses que le point soit ou non rétabli à l'état normal. Si la sirène incendie ou la sirène gaz n'est pas rendue silencieuse, la sortie continue jusqu'à expiration de la durée incendie ou gaz.

Utilisez ce paramètre pour que les applications incendie ou gaz pour respecter la norme qui indique que les alarmes sonores ne peuvent pas être rendues silencieuses tant que l'événement de défaut n'est pas effacé.

Emplacement dans le menu RPS

Points > Profils de point > Sonnerie jusqu'au rétablissement

11.3.13 Sonore après deux échecs

Valeur par défaut : Non (pour tous les profils de point)

Choix :
- Oui : pour les points silencieux (paramètre Sirène silencieuse défini sur Oui), la sortie Sirène d'alarme s'active au bout de deux tentatives infructueuses d'envoi d'un rapport au récepteur du centre de télésurveillance.
- Non : pour les points silencieux (paramètre Sirène silencieuse défini sur Oui), la sortie Sirène d'alarme ne s'active pas au bout de deux tentatives infructueuses d'envoi d'un rapport au récepteur du centre de télésurveillance.

Lorsqu'un point silencieux (paramètre *Sirène silencieuse, page 227* défini sur Oui) est en défaut, la Durée intrusion commence immédiatement. Jusqu'à 3 minutes peuvent s'écouler avant l'échec de la deuxième tentative d'envoi d'un rapport au récepteur du centre de télésurveillance. Vérifiez que le paramètre *Durée intrusion, page 111* est défini pour inclure ces 3 minutes plus le nombre de minutes souhaité pour l'activation de la *Sirène d'alarme, page 146*.

Emplacement dans le menu RPS
Points > Profils de point > Sonore après deux échecs

11.3.14 Point invisible

Valeur par défaut :
- Oui : profil de point 2
- Non : tous les autres profils de point

Choix :
- Oui : les claviers n'affichent pas d'événements d'alarme pour ce point. Les claviers émettent la tonalité de l'alarme, affichent les événements de défaut et émettent la tonalité de défaut.
- Non : les claviers affichent les événements d'alarme et les événements de défaut. Les claviers émettent la tonalité d'alarme et la tonalité de défaut pour ce point.

Remarque!
Les points environnementaux Incendie, gaz ne s'appliquent pas
Le paramètre de point invisible ne s'applique pas aux points incendie, gaz ou environnementaux (eau, temp. élevée, temp. faible).

Afin d'éviter le déclenchement de la tonalité d'alarme de clavier et de la *Sirène d'alarme, page 146*, définissez le paramètre *Sirène silencieuse, page 227* sur Oui.

Emplacement dans le menu RPS
Points > Profils de point > Point invisible

11.3.15 Sonnerie de panne

Valeur par défaut :
- 1 : profil de point 9
- 0 : tous les autres profils de point

Choix :
0 : le paramètre Sonnerie de panne est désactivé, tonalité de défaut uniquement si le point est à l'état de défaut.
1 : la tonalité de défaut démarre lorsque le point est en défaut. La tonalité de défaut ne peut être rendue silencieuse jusqu'à ce que le point soit rétabli à l'état normal.
2 : la tonalité de défaut démarre lorsque le point est en défaut. La tonalité de défaut peut être rendue silencieuse avant que le point soit rétabli à l'état normal.

3 : la tonalité de défaut démarre lorsque le point est en défaut. La tonalité de défaut s'arrête automatiquement lorsque le point est rétabli à l'état normal. La tonalité de défaut ne peut pas être rendue silencieuse tant que le point est en défaut.
Les réponses du point Alarme instantanée (I), Défaut (T) et Supervision (S) sont prioritaires sur le paramètre Sonnerie de panne. Si le paramètre Réponse du point est défini sur « vide », seul le paramètre Si le paramètre Sonnerie de panne démarre la tonalité de défaut.
Consultez les paramètres *Réponse du point, page 213* pour une description des types de réponse pour chaque type de point et comment ceux-ci sont liés par l'état armé.
Si un événement d'alarme, de défaut de supervision se produit et est reconnu, les choix 1 et 3 du paramètre Sonnerie de défaut poursuivent la tonalité de défaut jusqu'à ce que le point soit rétabli à l'état normal.

Remarque!
Ce paramètre Sonnerie de panne ne s'applique pas au type de point Fonction personnalisée.

Remarque!
Exigence de la norme UL 985 relative aux unités d'alarme incendie de maison familiale
Réglez ce paramètre sur 1 (la tonalité de défaillance démarre en cas de défaillance du point et la tonalité ne peut pas être désactivée tant que le point n’est pas rétabli à l’état normal) pour répondre aux exigences UL 985.

Emplacement dans le menu RPS
Points > Profils de point > Sonnerie de défaut

11.3.16 Point de détection

Valeur par défaut :
- Oui : profils de point 7 à 8
- Non : tous les autres profils de point

Choix :
- Oui : lorsque la centrale est en mode de détection, ce point démarre la tonalité de détection lorsqu'il est en défaut.
- Non : ce point ne démarre pas la tonalité de détection lorsqu'il est en défaut.

La tonalité de détection retentit pendant 2 secondes et le nom du point apparaît sur l'écran des claviers affectés à la même partition que le point.
Les points de détection sont actifs lorsque la réponse du point est vide (aucune réponse).
Le type de point doit être 24 heures, Part active ou Intérieur.

Emplacement dans le menu RPS
Points > Profils de point > Point de détection

11.3.17 Type de réponse de sortie

Valeur par défaut : 0

Choix :
- 0 : désactivé, l'état du point n'affecte pas le fonctionnement de la sortie associée.
- 1 : le passage de ce point à un état de point anormal active la sortie associée. La sortie se réinitialise automatiquement lorsque le point repasse à l'état normal.
- 2 : lorsque ce point déclenche une alarme, la sortie associée s'active. La sortie reste active jusqu'à ce que l'événement d'alarme soit effacé du clavier.

Utilisez ce paramètre pour configurer les sorties à activer dans un modèle stable lorsqu'un point associé (point avec le même numéro que la sortie, point 8 et sortie 8, par exemple) passe à l'état de point anormal.
Définissez ce paramètre sur 0 lorsque la sortie associée est configurée pour une autre fonction de sortie.

La sortie suit le point
Utilisez les sorties pour définir un point programmé pour Type de réponse de la sortie sur Anormal ou En alarme.

Emplacement dans le menu RPS
Points > Profils de point > Type de réponse de sortie

11.3.18 Affichage en tant que dispositif

Valeur par défaut : Non
Choix :
– Oui : afficher [VÉRIFIER DISPOSITIF] sur les claviers lorsque ce point est anormal.
– Non : ne pas afficher [VÉRIFIER DISPOSITIF] lorsque ce point est anormal.

Utilisez cette fonction pour les points qui sont connectés à une sortie de défaut d'un dispositif.

Emplacement dans le menu RPS
Points > Profils de point > Affichage en tant que dispositif

11.3.19 Local quand désarmé

Valeur par défaut :
– Oui : profil de point 9, 12
– Non : tous les autres profils de point

Choix :
– Oui : alors que la partition est désarmée, la centrale n'envoie pas de rapports d'alarme, de défaut ou de rétablissement pour ce point.
– Non : les centrales envoient des rapports d'alarme, de défaut et de rétablissement pour ce point alors que la partition est désarmée.

Ce paramètre n'a aucun effet sur les points incendie ou gaz.
Ne définissez pas ce paramètre sur Oui pour les types de point Interrupteur à clé maintenu, Interrupteur à clé à impulsion ou Ouverture/Fermeture.
Ne définissez pas ce paramètre sur Oui pour les points 24 heures. Les points 24 heures sont toujours armés.
Au lieu de cela, choisissez un type de point contrôlé et utilisez une réponse du point qui envoie une alarme si le point est armé ou non. Par exemple, les points avec le paramètre *Type de point, page 207* défini sur Partielle et le paramètre *Réponse du point, page 213* défini sur 9 envoient une alarme en cas de défaut ou de court-circuit (I) si la partition est armée ou non.

Remarque!
Un rapport de rétablissement est envoyé même lorsque la partition est désarmée si l'événement d'alarme ou de défaut s'est produit alors que la partition a été armée et est retournée à l'état normal une fois la partition désarmée.

Emplacement dans le menu RPS
Points > Profils de point > Local quand désarmé

11.3.20 Local quand armé

Valeur par défaut : Non

Choix :

– Oui : alors que la partition est armée, la centrale n'envoie pas de rapports d'alarme, de défaut ou de rétablissement pour ce point.
– Non : les centrales envoient des rapports d'alarme, de défaut et de rétablissement pour ce point alors que la partition est armée.

Ce paramètre n'a aucun effet sur les points incendie ou gaz.

Ne définissez pas ce paramètre sur Oui pour les types de point Interrupteur à clé maintenu, Interrupteur à clé à impulsion ou Ouverture/Fermeture.

Ne définissez pas ce paramètre sur Oui pour les points 24 heures. Les points 24 heures sont toujours armés.

Au lieu de cela, choisissez un type de point contrôlé et utilisez une réponse du point qui envoie une alarme si le point est armé ou non. Par exemple, les points avec le paramètre *Type de point, page 207* défini sur Partielle et le paramètre *Réponse du point, page 213* défini sur 9 envoient une alarme en cas de défaut ou de court-circuit (I) si la partition est armée ou non.

Emplacement dans le menu RPS

Points > Profils de point > Local quand armé

11.3.21 Désactiver les rétablissements

Valeur par défaut : Non

Choix :

– Oui : désactiver les rapports de rétablissement de ce point.
– Non : activer les rapports de rétablissement de ce point.

Emplacement dans le menu RPS

Points > Profils de point > Désactiver les rétablissements

11.3.22 Forcer armement retournable

Valeur par défaut : Non

Choix :

– Oui : lorsque ce point repasse à l'état normal après un armement forcé (inhibition de point forcé), il passe automatiquement à l'état armé.
– Non : lorsque ce point repasse à l'état normal après un armement forcé (inhibition de point forcé), il reste à l'état d'inhibition forcée.

Définissez ce paramètre sur Oui pour les points qui sont généralement en défaut lors de l'armement de la partition. Lorsque ce point retourne à l'état normal après un armement forcé (inhibition de point forcé), il passe automatiquement à l'état armé avec les autres points de la partition.

Emplacement dans le menu RPS

Points > Profils de point > Forcer armement retournable

11.3.23 Inhibition retournable

Valeur par défaut : Non

Choix :

– Oui : les points contrôlés qui sont inhibés ou inhibés par défaut se rétablissent automatiquement lorsque la partition est désarmée.

– Non - les points contrôlés qui sont inhibés ou inhibés par défaut doivent être rétablis. Utilisez la fonction de clavier INHIBER ?, les fonctions Rétablir un point ou Rétablir tous les points, ou RPS pour rétablir.

Définissez ce paramètre sur Non pour les points de verrouillage.
Les points contrôlés qui sont armés de force (inhibés) sont toujours rétablis lorsque la partition est désarmée.

Emplacement dans le menu RPS
Points > Profils de point > Inhibition retournable

11.3.24 Inhibable

Valeur par défaut :
– Oui : profils de point 1, 7-13, 20
– Non : profils de point 2-6, 14-19

Choix :
– Oui : les points liés à ce profil peuvent être inhibés et l'armement forcé.
– Non : les points liés à ce profil ne peuvent pas être inhibés ou l'armement forcé.

Même lorsque ce paramètre est défini sur Non :
– Les points contrôlés en défaut sont armés de force à la fin de la période de fermeture lorsque le paramètre Fermeture automatique est défini sur Oui.
– Les points contrôlés en défaut sont armés de force lorsque la partition est armée par une planification.

Lorsqu'un point 24 heures ou environnemental est inhibé, INHIBITION 24 HEURES défile sur le clavier. INHIBITION INCENDIE défile pour les points incendie inhibés. INHIBITION GAZ défile pour les points gaz inhibés.
Pour une réponse d'alarme 24 heures sans le défilement continu d'un point 24 heures inhibé, utilisez un point Partielle avec une *Réponse du point, page 213* de 9 à E.

Emplacement dans le menu RPS
Points > Profils de point > Inhibable

11.3.25 Inhibition automatique

Valeur par défaut : Non

Choix :
– Oui : activer l'inhibition automatique pour ce point. La centrale inhibe automatiquement le point lorsque le nombre d'événements d'alarme de point ou de défaut de point atteint le Nombre de points inhibables.
– Non : désactiver l'inhibition automatique pour ce point.

Avec chaque événement d'alarme de point ou de défaut de point, la centrale ajoute 1 au nombre d'événements. Lorsque la partition est désarmée, la centrale réinitialise le nombre d'événements sur 0.
La centrale envoie des rapports Inhibition automatique lorsque le *Nombre de points inhibables, page 90* est atteint et que le paramètre *Transmission rapport inhibition, page 234* est défini sur Oui.
Il n'est pas nécessaire que le paramètre *Inhibable, page 233* soit défini sur Oui pour que l'inhibition automatique fonctionne.
Si le paramètre *Inhibition retournable, page 232* est défini sur Oui, les points inhibé par défaut sont automatiquement inhibés lorsque la partition est désarmée.

Emplacement dans le menu RPS
Points > Profils de point > Inhibition automatique

11.3.26 Transmission rapport inhibition

Valeur par défaut : Non

Choix :

– Oui : la centrale envoie un rapport d'inhibition au moment où le point est inhibé.
– Non : la centrale n'envoie pas de rapport d'inhibition au moment où le point est inhibé.

Ce paramètre permet à un point de générer un rapport d'INHIBITION DE COMMANDE dès qu'un utilisateur inhibe le point depuis le clavier.

Activez ce paramètre pour tous les points pouvant être inhibés 24 heures sur 24. Vous pouvez également signaler un point inhibé au moment où la partition est armée à l'aide de l'option *Différer le rapport d'inhibition, page 234*.

Emplacement dans le menu RPS

Points > Profils de point > Transmission rapport inhibition

11.3.27 Différer le rapport d'inhibition

Valeur par défaut : Non

Choix :

– Oui - la centrale envoie des rapports d'inhibition avec le rapport de fermeture lorsque le point est inhibé par un utilisateur.
– Non : la centrale n'envoie pas de rapports d'inhibition.

Utilisez ce paramètre pour empêcher que les points qui sont inhibés par l'utilisateur ne soient signalés jusqu'à ce que la partition soit armée.

Une fois que la partition est armée, les points inhibés et tout point inhibé pendant la séquence d'armement se signalent en tant que INHIBITION DE POINT avec le rapport de fermeture.

Pour signaler l'inhibition lors de son occurrence et lorsque la partition est armée, définissez ce paramètre et Rapport d'inhibition à occurrence sur Oui. Un rapport d'INHIBITION DE COMMANDE est envoyé dès qu'il se produit et un rapport d'INHIBITION DE POINT est envoyé avec le rapport de fermeture.

Les rapports de contournement ne sont pas générés lors de l'armement de la partition si le rapport de fermeture est supprimé par les périodes d'ouverture/fermeture ou n'est pas signalé.

Les rapports d'inhibition pour les points 24 heures ne sont pas envoyés si ce paramètre et *Transmission rapport inhibition, page 234* sont tous deux définis sur Non.

Emplacement dans le menu RPS

Points > Profils de point > Différer le rapport d'inhibition

Se reporter à

– *Transmission rapport inhibition, page 234*

11.3.28 Point de croisement

Valeur par défaut : Non

Choix :

– Oui : ce point est un point de croisement.
– Non : ce point n'est pas un point de croisement.

L'option Point de croisement réduit les fausses alarmes. Les points peuvent être programmés de façon à ce que la centrale nécessite une condition Alarme dans un délai programmé (temps de point de croisement) d'au moins deux points dans un groupe de points de croisement avant la génération des événements d'alarme de points de croisement.

Un défait sur un point de croisement démarre la minuterie de points de croisement sur la centrale. S'il existe un défaut sur un autre point de croisement dans le même groupe de points de croisement avant expiration du minuteur de points de croisement, la centrale crée des événements d'alarme de point de croisement pour les deux points.
Si le point de croisement qui démarre le minuteur de point de croisement est rétabli à l'état normal et s'il n'y a pas de défaut sur un autre point de croisement dans le même groupe de points de croisement avant expiration du minuteur de point de croisement, la centrale crée un événement non vérifié (et non un événement d'alarme de point de croisement).
Si le point de croisement qui démarre le minuteur de point de croisement est rétabli à l'état normal, puis s'il est mis en défaut et de nouveau rétabli, et t s'il n'y a pas de défaut sur un autre point de croisement dans le même groupe de points de croisement avant expiration du minuteur de point de croisement, la centrale crée un événement non vérifié (et non un événement d'alarme de point de croisement).
Si le point de croisement qui démarre le minuteur de point de croisement reste en défaut jusqu'à expiration du minuteur de point de croisement et s'il n'y a pas de défaut sur un autre point de croisement dans le même groupe de points de croisement, la centrale crée un événement d'alarme de point (et non un événement d'alarme de point de croisement).
La fonction de point de croisement s'applique uniquement aux événements d'alarme. Elle ne s'applique pas aux événements de supervision ou de défaut.
La fonction de point de croisement exige qu'au moins 2 points du groupe soient des points de croisement.
Les groupes de point de croisement ne peuvent pas être configurés. Il existe 8 points dans chaque groupe de points de croisement. Les points 1-8 sont dans le premier groupe. Les points 9-16 sont le deuxième groupe, et ainsi de suite. Les points de croisement dans les différents groupes de points de croisement n'ont aucune incidence entre eux.
Affectez les points de croisement du même groupe de points de croisement au même profil de point :

1. Définissez le paramètre *Type de point, page 207*. Utilisez un paramètre valide de la liste dans la section suivante de cette rubrique.
2. Définissez le paramètre *Réponse du point, page 213* pour la réponse d'alarme instantanée.

Si vous affectez les points de croisement du même groupe de points de croisement à différents profils de point et si vous souhaitez utiliser la fonction Annulation d'alarme, définissez le paramètre *Annulation d'alarme, page 237* sur Oui pour chaque profil de point.
La définition du paramètre *Inhibable, page 233* sur Oui pour les points de croisement peut éviter les alarmes de point de croisement. Par exemple, si les points 1 et 2 sont des points de croisement, le point 1 est inhibé et le point 2 est en défaut, la centrale ne peut pas créer un événement de point de croisement. Si le point 2 reste en défaut avant expiration du minuteur de points de croisement, la centrale crée un événement d'alarme de point (et non un événement d'alarme de point de croisement). Si le point 2 est en défaut et est rétabli avant expiration du minuteur de points de croisement, lorsque le minuteur arrive à expiration, la centrale crée un événement de point non vérifié (et non un événement d'alarme de point de croisement).

Paramètres de type de point pris en charge

- 24 heures
- Intérieur
- Suiveur intérieur
- Part active
- Temp. élevée

– Temp. faible
– Eau

Emplacement dans le menu RPS
Points > Profils de point > Point de croisement

Pour obtenir de plus amples informations
Minuterie de points de croisement, page 205

11.3.29 Vérification de l'alarme

Valeur par défaut :
– Oui : profil de point 5
– Non : tous les autres profils de point

Choix :
– Oui : activer la vérification d'alarme pour ce point. (Types de point d'incendie et de point gaz uniquement)
– Non : désactiver la vérification d'alarme sur ce point.

Si vous définissez ce paramètre sur Oui, vous devez également définir le paramètre Réinitialisable sur Oui.
Lorsqu'un point incendie ou gaz avec le paramètre Vérification de l'alarme défini sur Oui déclenche une alarme, la centrale démarre la fonction de sortie Réinitialiser les détecteurs pour retirer l'alimentation aux points réinitialisables. Lorsque l'alimentation est rétablie, le contrôle ignore le point pendant la durée définie dans le paramètre Durée de redémarrage. Si le point est en mode alarme dans les 65 secondes suivant la fin de la durée de redémarrage, la centrale crée un événement d'alarme.
La centrale n'utilise pas la durée définie dans le paramètre Durée de redémarrage pour le Test de détection incendie. La durée de redémarrage est de 5 secondes.

Emplacement dans le menu RPS
Points > Profils de point > Vérification de l'alarme

Pour obtenir de plus amples informations
Durée de redémarrage, page 105
Réinitialisable, page 236
Réinitialiser les détecteurs, page 147

11.3.30 Réinitialisable

Valeur par défaut :
– Non : profils de point 1-3, 6-20
– Oui : profils de point 4, 5

Choix :
– Oui : la centrale ignore ce point pendant la durée de réinitialisation de la fonction utilisateur Réinitialiser les détecteurs et la durée de réinitialisation/redémarrage dans la fonction de vérification d'alarme.
– Non : ce point n'est pas réinitialisable.

Le paramètre Réinitialisable est uniquement pour les types de point 24 h, Part active, Intérieur, Panique, Incendie et Gaz.
Définissez ce paramètre sur Oui pour les points qui exigent une interruption de l'alimentation pour la réinitialisation d'un événement d'alarme verrouillé. La fonction de point réinitialisable est généralement utilisée pour les détecteurs de fumée et les détecteurs de bris de verre. Ne mélangez pas les dispositifs intrusion et incendie sur la même boucle sous tension.

Lorsque les points sont réinitialisés à l'aide de la fonction utilisateur Réinitialiser les détecteurs, d'un test de détection ou de RPS, la centrale envoie un rapport de réinitialisation de détecteur au récepteur du centre de télésurveillance.

Pour obtenir de plus amples informations
Vérification de l'alarme, page 236
Durée de redémarrage, page 105
Réinitialiser les détecteurs, page 147

Emplacement dans le menu RPS
Points > Profils de point > Réinitialisable

11.3.31 Annulation d'alarme

Valeur par défaut :
- Oui : profils de point 1, 7-10, 11-16, 20
- Non : profils de point 2-6, 17-19

Choix :
- Oui : si le point déclenche une alarme, la centrale diffère le rapport d'alarme pendant la durée définie dans le paramètre Période d'interruption.
- Non : la centrale ne diffère pas les rapports d'alarme.

Si un utilisateur rend l'alarme silencieuse avant expiration de la durée du paramètre Période d'interruption, l'alarme est annulée. Le rapport d'alarme de point n'est pas envoyé au récepteur du centre de télésurveillance.
Lorsqu'une alarme est annulée, les claviers peuvent afficher un message Alarme non envoyée. Voir *Affichage d'interruption, page 129*.
Ce paramètre ne concerne pas les alarmes incendie ou les alarmes de point invisible.

Remarque!
Pour être en conformité avec les normes UL, le temps total entré dans le paramètre *Temporisation d'entrée, page 227* et le paramètre *Période d'interruption, page 88* ne doivent pas dépasser 1 minute.

Emplacement dans le menu RPS
Points > Profils de point > Annulation d'alarme

11.3.32 Délai de supervision de point radio

Valeur par défaut :
- 24 heures : profils de point 1-2, 7-16
- 4 heures : profils de point 3-6

Choix :
- Aucun : désactiver la supervision de point radio.
- 4 heures, 12 heures, 24 heures, 48 heures, 72 heures : définir la durée en heures pour la supervision de point radio.

Si le récepteur radio ne reçoit pas une transmission du dispositif de point radio dans le délai de supervision de point radio, la centrale crée un événement manquant pour le point.
Le paramètre Délai de supervision de point radio pour les points incendie est défini sur 4 heures et il ne peut pas être modifié.
Le Délai de supervision de point radio s'applique aux télécommandes RADION lorsque celles-ci sont configurées en tant que dispositifs de point.
Il s'agit d'un intervalle de supervision secondaire pour le paramètre *Délai de supervision du système (répéteur), page 294*.

Emplacement dans le menu RPS
Points > Profils de point > Délai de supervision de point radio

11.3.33 Fonction personnalisée

Valeur par défaut : Désactivé
Choix :
- B6512 : désactivé, fonction 128-133
- B5512 : désactivé, fonction 128-131
- B4512 : désactivé, fonction 128-129
- B3512 : désactivé, fonction 128

Sélectionnez la fonction personnalisée à démarrer lorsque le point est en défaut à l'état Court-circuit (S) ou Ouvert (O).

Emplacement dans le menu RPS
Points > Profils de point > Fonction personnalisée

11.3.34 Temps de surveillance

Valeur par défaut : 00:00
Choix : 00:00 (désactivé), 00:01-60:00
Définissez le délai d'attente (MM:SS) observé par une centrale désarmée après un défaut de point avant l'envoi d'un rapport Superviseur Intrusion au centre de télésurveillance. Le point doit être en défaut pendant toute la durée.
Si le point est restauré à un état normal pendant cette période, aucun rapport n'est envoyé. La centrale n'affiche pas les événements de temps de surveillance au niveau des claviers. Utilisez la fonction Temps de surveillance pour surveiller les portes qui ne doivent pas être laissées ouvertes. Par exemple, une porte de compacteur de déchets, une porte de vitrine de bijoux et les portes de congélateur.

Remarque!
Le démarrage d'un test de détection incluant des points contrôlés, ou l'armement de la partition du point, annule le minuteur de point de surveillance. Aucun rapport n'est envoyé à l'expiration de la durée configurée.

Emplacement dans le menu RPS
Points > Profils de point > Temps de surveillance

11.3.35 Délai de réponse, désarmé

Valeur par défaut : 00:00
Choix : 00:00 (désactivé), 00:05-60:00
Ce paramètre définit le délai d'attente (MM:SS) observé par la centrale après un défaut de point désarmé avant l'annonce ou la génération d'un rapport sur le défaut.

Remarque!
Profils de points Panique
Ce paramètre n’est pas configurable (désactivé) pour les profils de points Panique, Eau, Temp. élevée et Temp. faible.

Ce paramètre s'applique uniquement aux types de point suivants lorsqu'ils sont désarmés :
- *Partielle, page 240*
- *Intérieur, page 241*
- *Suiveur intérieur, page 242*

Utilisez cette fonction pour temporiser l'effet des paramètres suivants :
- *Réponse du point, page 213*
  - Alarme instantanée
  - Supervision
- *Sonnerie de panne, page 229*
- *Point de détection, page 230*
- *Type de réponse de sortie, page 230*
- *Affichage en tant que dispositif, page 231*
- *Sortie, page 203*

Remarque!
La réponse du point Alarme de temporisation (D) n'est pas prise en charge par la fonction Délai de réponse. Par conséquent, lorsqu'une alarme de temporisation déclenche une alarme instantanée, l'alarme n'est pas différée par cette fonction.

Emplacement dans le menu RPS
Points > Profils de point > Délai de réponse, Désarmé

11.3.36 Délai de réponse, Armé

Valeur par défaut : 00:00
Choix : 00:00 (désactivé), 00:05-60:00
Ce paramètre définit le délai d'attente (MM:SS) observé par la centrale après un défaut de point armé avant l'annonce ou la génération d'un rapport sur le défaut.

Remarque!
Profils de points Panique
Ce paramètre est configurable (activé) pour les profils de points Panique, Eau, Temp. élevée et Temp. faible.

Ce paramètre s'applique uniquement aux types de point suivants lorsqu'ils sont armés :
- *24 heures, page 240*
- *Partielle, page 240*
- *Intérieur, page 241*
- *Suiveur intérieur, page 242*
- *Point Panique, page 244*
- *Point Eau, page 244*
- *Point Temp. élevée, page 244*
- *Point Temp. faible, page 244*

Utilisez cette fonction pour temporiser l'effet des paramètres suivants :
- *Réponse du point, page 213*
  - Alarme instantanée
  - Supervision
- *Type de réponse de sortie, page 230*
- *Affichage en tant que dispositif, page 231*
- *Sortie, page 203*

Remarque!
La réponse du point Alarme de temporisation (D) n'est pas prise en charge par la fonction Délai de réponse. Par conséquent, lorsqu'une alarme de temporisation déclenche une alarme instantanée, l'alarme n'est pas différée par cette fonction.

Emplacement dans le menu RPS
Points > Profils de point > Délai de réponse, Armé

11.3.37 État normal

Valeur par défaut : ouvert
Choix :
– Ouvert : un circuit de point ouvert est l'état Normal.
– Court-circuit : un circuit de point court-circuit est à l'état Normal.
Ce paramètre définit l'état Normal lorsque le paramètre Type de surveillance de ligne est défini sur Aucune résistance de fin de ligne.

Emplacement dans le menu RPS
Points > Profils de point > Type de point/Réponse/Type de surveillance de ligne

11.4 Descriptions de profil de point

11.4.1 24 heures

Un point 24 heures n'est pas activé et désactivé à partir d'un clavier. Les points 24 heures sont armés tout le temps et ils peuvent être utilisés pour les alertes panique, médicale et de police.
Les points 24 heures peuvent être programmés comme inhibables. Cependant, l'application doit être soigneusement prise en compte avec l'utilisation de l'option inhibable. Les points 24 heures inhibables doivent être programmés sur *Sonnerie de panne, page 229*.
Lorsqu'un point 24 heures est inhibé, le rapport doit envoyé lorsqu'il se produit. Si la partition contient tous les points 24 heures, elle n'est jamais armée ou désarmée ; par conséquent, aucun rapport d'inhibition différé n'est envoyé.
Protection 24 heures pour les portes incendie, les trappes de toit, etc. Au lieu de programmer ce type de protection en tant que point 24 heures, envisagez d'utiliser un type de point périmètre, avec une *Réponse du point, page 213* 9 à E. Les points 24 heures n'affichent pas les défauts lorsqu'une fonction d'armement est entrée, alors que les points périmètre le font. Lors de la programmation de ce type de protection, vous devez envisager d'utiliser les options Sonnerie de défaut et *Local quand désarmé, page 231*.
Dispositifs d'alarme effraction dans les installations UL : le type de point 24 heures doit être utilisé pour les points connectés aux dispositifs d'alarme effraction. Le texte du point doit inclure « effraction ».

11.4.2 Partielle

Lorsqu'un profil de point est configuré avec le type de point Partiel, il devient un profil point Partiel. Les points liés à un profil de point Partiel sont des points Partielle. Les points Partiel sont généralement utilisés pour surveiller les dispositifs dans le périmètre des locaux (portes et fenêtres).
Un profil de point Partiel comprend une temporisation d'entrée configurable. La temporisation d'entrée donne le temps nécessaire aux utilisateurs pour atteindre un clavier et désactiver la partition sans créer d'événement d'alarme. Par exemple, lorsqu'un utilisateur ouvre la porte d'entrée (déclenchement d'un point Partiel), la temporisation d'entrée commence. L'utilisateur doit passer à un clavier et désactiver la partition avant l'expiration de la temporisation de sortie pour éviter un événement d'alarme.

Si la partition est en temporisation d'entrée et qu'un second point Partielle se déclenche, la centrale compare la temporisation d'entrée restante à la temporisation d'entrée programmée pour le second point Partielle. Si la temporisation d'entrée du second point est inférieure au temps restant, cela raccourcit la temporisation d'entrée.

Remarque!
Les points Partielle avec une réponse du point instantanée créent des événements d'alarme immédiats
Les points périmètre programmés pour une *Réponse du point, page 213* instantanée ne démarrent pas la temporisation d'entrée lorsqu'ils sont déclenchés. Ils génèrent un événement d'alarme immédiatement, même pendant une temporisation d'entrée ou de sortie.

Lorsqu'un utilisateur active une partition Tout activé, les points Intérieur et les points Suiveur intérieur sont tous armés.
Lorsqu'un utilisateur active une partition Partielle, seuls les points Partiels sont armés. Les points Intérieur et Suiveur intérieur ne sont pas armés. Dans un système standard, l'activation d'une partition Partielle arme uniquement la protection périmétrique, ce qui permet aux utilisateurs de rester dans les locaux sans déclencher d'événements d'alarme à partir de points intérieurs.

11.4.3 Intérieur

Lorsqu'un profil de point est configuré avec le type de point Intérieur, il devient un profil point Intérieur. Les points liés à un profil de point Intérieur sont des points Intérieurs. Les points Intérieurs sont généralement utilisés pour surveiller les dispositifs de détection intérieurs, tels que des portes intérieures, des détecteurs de mouvement, des faisceaux photoélectriques ou des tapis protecteurs.
Les points intérieurs sont armés uniquement lorsque la partition est Tout activé. Ils ne sont pas armés lorsque la partition est Partielle.
La *Réponse du point, page 213* pour les points intérieurs peut être configurée pour une réponse d'alarme instantanée ou différée.

- Instantané : les points configurés pour une réponse d'alarme instantanée créent des événements d'alarme immédiatement, même pendant la durée de temporisation d'entrée ou de sortie. Les points intérieurs sont généralement configurés pour une réponse d'alarme instantanée.
- Différé : lorsqu'un point intérieur configuré pour une réponse d'alarme différée est déclenché alors que la partition est Tout activé, il démarre une temporisation d'entrée. Il ne crée pas d'événement d'alarme à moins que la temporisation d'entrée n'expire avant que la partition soit désactivée.
  Si la partition est déjà dans la temporisation d'entrée lorsqu'un point intérieur avec réponse d'alarme différée se déclenche, la centrale compare la temporisation d'entrée restante et la temporisation d'entrée programmée pour le point intérieur. Si la temporisation d'entrée du point intérieur est inférieure au temps restant, cela raccourcit la temporisation d'entrée.

Les points différés peuvent également démarrer une tonalité d'entrée sur le clavier (voir *Tonalité d'entrée désactivée, page 227*).

Remarque!
Utilisez le profil *Suiveur intérieur, page 242* **pour une alarme instantanée si la partition n'est pas dans une temporisation d'entrée**
Pour certaines installations, vous pouvez choisir un point intérieur qui suit, mais qui ne peut pas démarrer un jour d'entrée. Le déclenchement d'un point suiveur intérieur alors que la partition est Tout activé crée un événement d'alarme instantanée. Cependant, si un autre point est déclenché au démarrage de la temporisation d'entrée, et qu'un autre point Suiveur intérieur est ensuite déclenché, le point suiveur intérieur diffère la réponse d'alarme jusqu'à expiration de la temporisation de sortie. Si la partition est désactivée avant expiration de la temporisation d'entrée, il n'y a pas de réponse d'alarme.

11.4.4 Suiveur intérieur

Lorsqu'un profil de point est configuré avec le type de point Suiveur Intérieur, il devient un profil point Suiveur Intérieur. Les points liés à un profil de point Suiveur Intérieur sont des points Suiveur Intérieur. Les points Suiveurs Intérieurs sont généralement utilisés pour surveiller les dispositifs de détection intérieurs tels que des portes intérieures, des détecteurs de mouvement, des faisceaux photoélectriques ou des tapis protecteurs.
Les points suiveurs intérieurs sont armés uniquement lorsque la partition est Tout activé. Ils ne sont pas armés lorsque la partition est Partielle.
Les points Suiveurs Intérieurs suivent, mais ne peuvent pas démarrer une temporisation d'entrée. Le déclenchement d'un point Suiveur intérieur alors que la partition est Tout activé crée une réponse d'alarme instantanée. Cependant, si un autre point est déclenché au démarrage de la temporisation d'entrée, et qu'un autre point Suiveur intérieur est ensuite déclenché, le point suiveur intérieur diffère la réponse d'alarme jusqu'à expiration de la temporisation de sortie. Si la partition est désactivée avant expiration de la temporisation d'entrée, il n'y a pas de réponse d'alarme.
Pendant la temporisation de sortie, la neutralisation d'un point Suiveur Intérieur ne crée pas d'événement d'alarme (même si un point Partielle Temporisée n'est pas en défaut pendant la temporisation de sortie).
Les points Suiveurs Intérieurs ne démarrent aucune temporisation d'entrée même s'ils sont configurés pour une réponse d'alarme différée (paramètre *Réponse du point, page 213* défini sur 4, 5, 6, 7 ou 8).

Remarque!
Utilisez le profil *Intérieur, page 241* **et la réponse d'alarme différée pour les points intérieurs qui démarrent une temporisation d'entrée**
Pour certaines installations, vous pouvez choisir un point intérieur qui peut démarrer un jour d'entrée. Le déclenchement d'un point intérieur configuré pour la réponse d'alarme différée (voir *Réponse du point, page 213*) alors que la partition Tout activé démarre la temporisation d'entrée. La réponse d'alarme est différée jusqu'à expiration de la temporisation de sortie. Si la partition est désactivée avant expiration de la temporisation d'entrée, il n'y a pas de réponse d'alarme.

11.4.5 Interrupteur à clé maintenu

Programmez la réponse du point 1. Ne connectez pas des dispositifs d'amorçage à un point d'interrupteur à clé.
- Normal : la partition est désarmée.
- Ouvert : lorsque ce point passe de l'état normal à l'état ouvert, la partition est armée.

– Court-circuit : un court-circuit est un défaut alors que la partition est désarmée. Un court-circuit est une alarme alors que la partition est armée. Lorsque ce point passe de l'état court-circuit à l'état normal ou ouvert, il est rétabli.

Si vous programmez la réponse du point sur 2, le point répond comme suit :
– Normal : lorsque ce point passe de l'état ouvert à l'état normal, la partition est armé.
– Ouvert : la partition est désarmée.
– Court-circuit : un court-circuit est un défaut alors que la partition est désarmée. Un court-circuit est une alarme alors que la partition est armée. Lorsque ce point passe de l'état court-circuit à l'état normal ou ouvert, il est rétabli.

Les rapports de défaut et de rétablissement ne sont pas envoyés si le paramètre *Local quand désarmé, page 231* est défini sur Oui.
Les rapports d'alarme et de rétablissement ne sont pas envoyés si le paramètre *Local quand armé, page 232* est défini sur Oui.

Remarque!
La réponse du point 2 est nécessaire pour les dispositifs Radio Inovonics FA113.

11.4.6 Interrupteur à clé à impulsion

Utilisé pour l'armement et le désarmement de partition. La réponse du point doit être programmée sur 1. Ne connectez pas des dispositifs d'amorçage à un point d'interrupteur à clé.
– N->S->N : lorsque ce point passe momentanément de l'état normal à l'état court-circuit et normal, il active/désactive l'état armé de la partition.
– Ouvert : un état ouvert est un défaut alors que le point est désarmé. Un état ouvert est une alarme alors que le point est armé.

Lorsque ce point passe de l'état ouvert à normal, il est rétabli.
Les rapports de défaut et de rétablissement ne sont pas envoyés si le paramètre *Local quand désarmé, page 231* est défini sur Oui.
Les rapports de défaut et de rétablissement ne sont pas envoyés si le paramètre *Local quand armé, page 232* est défini sur Oui.

11.4.7 Point d'ouverture/de fermeture

Utilisé pour l'armement et le désarmement de point. La réponse du point doit être programmée sur 1. Les sirènes locales sont rendues silencieuses par l'intermédiaire du clavier.
– Normal : le point est armé et il envoie un rapport FERMETURE DE POINT. Le rapport FERMETURE DE POINT n'est pas envoyé si le paramètre *Local quand armé, page 232* est défini sur Oui.
– Ouvert : un état ouvert est une alarme alors que le point est armé. Un état ouvert est un défaut alors que le point est désarmé. Les rapports d'ALARME et de RÉTABLISSEMENT ne sont pas envoyés si le paramètre *Local quand désarmé, page 231* est défini sur Oui.
– Court-circuit : le point est désarmé et envoie un rapport OUVERTURE DE POINT. Un rapport OUVERTURE DE POINT n'est pas envoyé si le paramètre Local armé est défini sur Oui.

11.4.8 Point incendie

Ce type de point génère une alarme incendie. Les alarmes incendie sont les événements dont la priorité est la plus élevée sur la centrale.

11.4.9 Supervision secteur auxiliaire

Ce type de point surveille l'alimentation secteur d'une alimentation auxiliaire. Lorsque le point se trouve dans un état anormal, la centrale observe le temps d'attente programmé dans le paramètre Temps de défaut secteur avant de générer un défaut de point. Ce type de point n'utilise pas de *Réponse du point, page 213* ; par conséquent, aucun événement d'alarme ne se produit.
Si ce type de point est inhibé, POINT INHIBÉ 24 HEURES s'affiche sur les claviers.

11.4.10 Point gaz

Ce type de point surveille les détecteurs de détection de gaz et génère une alarme gaz lorsqu'une réponse d'alarme instantanée est activée (voir la section relative à la réponse du point 24 heures).

11.4.11 Fonction personnalisée

Ce type de point active une fonction personnalisée lorsque la réponse du point de fonction personnalisée (CF) est activée (voir le tableau relatif à la réponse du point de la fonction personnalisée). La fonction personnalisée activée est configurée dans le paramètre Fonction personnalisée.

11.4.12 Point Eau

Utilisez ce type de point environnemental pour surveiller les capteurs d’eau qui peuvent détecter une fuite d’eau. Une alarme instantanée ou une réponse à un point de défaut est signalée comme un événement de fuite d’eau. Les types de point environnementaux ne sont pas contrôlés.

11.4.13 Point Temp. élevée

Utilisez ce type de point environnemental pour surveiller les températures élevées. Une alarme instantanée ou une réponse à un point de défaut est signalée comme un événement de température. Les types de point environnementaux ne sont pas contrôlés.

11.4.14 Point Temp. faible

Utilisez ce type de point environnemental pour surveiller les températures faibles. Une alarme instantanée ou une réponse à un point de défaut est signalée comme un événement de température. Les types de point environnementaux ne sont pas contrôlés.

11.4.15 Point Panique

Le type de point Panique fonctionne de la même façon que le type de point 24 heures et peut être programmé avec ou sans sortie audible Ce type de point est armé à tout moment et est utilisé pour les alarmes de panique.

12 Planifications

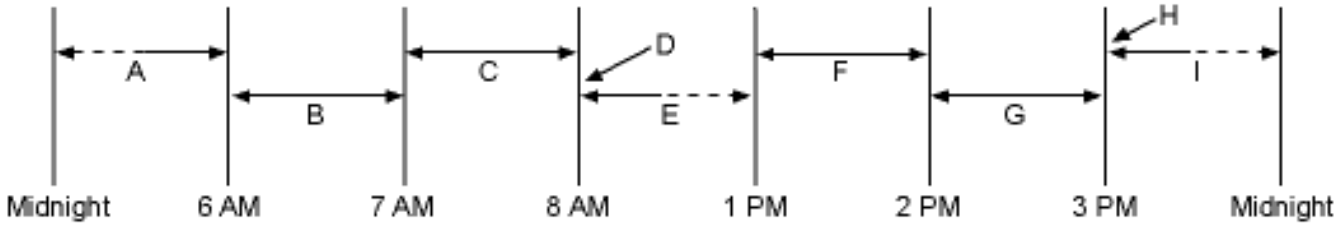
12.1 Périodes d'ouverture/de fermeture

Utilisez ces périodes pour définir des planifications pour le désarmement (ouverture) et l'armement (fermeture). Les périodes d'ouverture et de fermeture peuvent être définies indépendamment. Par exemple, si vous souhaitez uniquement utiliser les fonctions fournies par les périodes de fermeture, laissez les heures vides dans les paramètres des périodes de fermeture et programmez des heures de période de fermeture.
Les planifications d'armement et de désarmement offrent plusieurs fonctionnalités indépendantes :

- Suppression des rapports d'ouverture et/ou de fermeture normaux lorsque le paramètre *Désactiver O/F dans la période, page 114* est défini sur Oui.
- Génération d'un rapport ÉCHEC D'OUVERTURE si la partition n'est pas désarmée conformément à la planification lorsque le paramètre *Échec d'ouverture, page 115* est défini sur Oui.
- Émission d'une tonalité d'avertissement et affichage de [VEUILLEZ FERMER MAINTENANT] sur le clavier lorsqu'il est temps d'armer la partition.
- Génération d'un rapport ÉCHEC DE FERMETURE si la partition n'est pas armée conformément à la planification lorsque le paramètre *Échec de fermeture, page 115* est défini sur Oui.
- Armement automatique de la partition en fin de période de fermeture lorsque le paramètre *Fermeture automatique, page 115* est défini sur Oui.

12.1.1 Chronologie de la période d'ouverture

Exemple d'utilisation de deux périodes d'ouverture le même jour



Les partitions qui sont désarmées entre minuit et 6:00 génèrent des rapports d'ouverture.
Les partitions qui sont désarmées entre 6:00 et 7:00 génèrent des rapports d'ouverture anticipée.
Si la partition est désarmée entre 7:00 et 8:00, des rapports d'ouverture périodiques sont générés.
Si le paramètre Désactiver O/F dans la période est programmé sur « oui », le rapport d'ouverture n'est pas transmis au centre de télésurveillance.
Si la partition n'est pas désarmée avant 8:01, un événement d'échec d'ouverture est généré si le paramètre Échec d'ouverture est défini sur « oui » dans les options Ouverture et Fermeture.
Si l'utilisateur désarme la partition entre 8:01 et 12:59, un événement d'ouverture tardive est généré.
Les partitions qui sont désarmées entre 13:00 et 14:00 génèrent des rapports d'ouverture anticipée.
Si la partition est désarmée entre 14:00 et 15:00, des rapports d'ouverture périodiques sont générés.

Si le paramètre Désactiver O/F dans la période est programmé sur « oui », le rapport d'ouverture n'est pas transmis au centre de télésurveillance.
Si la partition n'est pas désarmée avant 15:01, un événement d'échec d'ouverture est généré si le paramètre Échec d'ouverture est défini sur « oui » dans les options Ouverture et Fermeture.
Si l'utilisateur désarme la partition entre 15:01 et 23:59, un événement d'ouverture tardive est généré.

Programmation de deux périodes d'ouverture le même jour (comme indiqué dans la chronologie)

		Ouvrir			**Fermeture**			
N° période	Jour de la semaine	Ouverture anticipée	Début	Arrêt	Ouverture anticipée	Début	Arrêt	sauf pendant les congés
1	D**LMMJ V**S	06:00	07:00	08:00			23:59	Oui/**Non**
2	D**LMMJ V**S	13:00	14:00	15:00			01:00	Oui/**Non**

Ne programmez pas une seule période pour passer la limite de minuit. L'heure d'arrêt de la période doit être postérieure à l'heure de début de la période. Pour programmer une période qui dépasse la limite de minuit, vous devez programmer deux périodes.
Par exemple, pour programmer des périodes pour une partition qui s'ouvre entre 23:30 et 00:30, cinq jours par semaine, utilisez deux périodes comme illustré dans l'exemple ci-dessous :

Programmation pour la liaison de deux jours via minuit

	Ouvrir			**Fermeture**					
N° période	Ouverture anticipée	Début	Arrêt	Ouverture anticipée	Début	Arrêt	sauf pendant les congés	Index des congés	Partition(s)
1 / Lundi	22:00	23:30	23:59				Oui/**Non**	1234	**1**2345678
2 / Lundi	00:00	00:00	00:30				Oui/**Non**	1234	**1**2345678

12.1.2 Tableau des périodes d'ouverture/de fermeture

Lundi au vendredi, ouverture entre 5:00 et 6:00, fermeture entre 23:00 et 1:00.

		Ouvrir			**Fermeture**			
N° période	Jour de la semaine	Ouverture anticipée	Début	Arrêt	Ouverture anticipée	Début	Arrêt	sauf pendant les congés

		Ouvrir			**Fermeture**			
1	D**LMMJ V**S	04:00	05:00	06:00	20:00	23:00	23:59	Oui/**Non**
2	DL**MMJ V**S				00:00	00:00	01:00	Oui/**Non**

Dimanche, entrée 8:00 et 8:30, sortie entre 14:30 et 17:00.

		Ouvrir		
N° période	Jour de la semaine	Ouverture anticipée	Début	Arrêt
4	DLMMJVS	07:00	08:00	08:30
	Tous les jours doivent être programmés sur NON	Uniquement pendant les congés		

Tableau des périodes d'ouverture/de fermeture
Utilisez ce tableau pour déterminer les entrées appropriées pour votre application.

Jour de la semaine	**La colonne ci-dessous indique brièvement comment activer une fenêtre d'ouverture/de fermeture. Suivez les instructions affichées dans les autres colonnes pour choisir les entrées appropriées.**	**sauf pendant les congés**	**Index des congés**	**Partitions**
Programmer au moins un jour sur OUI	Jour(s) de la semaine	NON	Aucun	Programmer au moins une partition sur OUI
Programmer au moins un jour sur OUI	Jour(s) de la semaine, mais PAS pendant les congés	OUI	Sélectionnez au moins un index	Programmer au moins une partition sur OUI

Jour de la semaine	**La colonne ci-dessous indique brièvement comment activer une fenêtre d'ouverture/de fermeture. Suivez les instructions affichées dans les autres colonnes pour choisir les entrées appropriées.**	**sauf pendant les congés**	**Index des congés**	**Partitions**
Programmer au moins un jour sur OUI	Jour(s) de la semaine, PLUS les jours fériés	NON	Sélectionnez au moins un index	Programmer au moins une partition sur OUI
Tous les jours doivent être programmés sur NON	Uniquement pendant les congés	NON	Sélectionnez au moins un index	Programmer au moins une partition sur OUI

12.1.3 Dimanche au samedi

Valeur par défaut (Dimanche à samedi) : Non

Choix : Oui, Non

Dans les sept paramètres de jour de semaine, sélectionnez les jours de la semaine pendant lesquels les périodes d'ouverture et/ou de fermeture sont actives.

Pour éviter que les périodes ne s'activent certains jours de l'année, définissez le paramètre *sauf pendant les congés, page 255* sur Oui et activez au moins un index de congé. Lorsque le paramètre *sauf pendant les congés, page 255* est défini sur Oui, la période s'exécute les jours de semaine programmés à moins que la date soit définie comme un congé par l'index de congé sélectionné.

Si des périodes d'ouverture et/ou de fermeture sont uniquement nécessaires certains jours de l'année, ne programmez l'exécution de ces périodes pour aucun jour de la semaine. À la place, définissez le paramètre *sauf pendant les congés, page 255* sur Non et sélectionnez un index de congé avec les jours de l'année où vous souhaitez que la période soit active.

Emplacement dans le menu RPS

Planifications > Périodes d'ouverture/de fermeture > Dimanche à samedi

12.1.4 Début d'ouverture anticipée

Valeur par défaut : Désactiver

Choix : Désactivé, HH:MM (heures et minutes) 00:00 à 23:59

Saisissez l'heure la plus tôt possible à laquelle un utilisateur est autorisé à ouvrir (désarmer) une partition.

Ce paramètre est l'un des trois paramètres requis pour créer une période d'ouverture. Pour terminer la programmation d'une période d'ouverture, il est nécessaire de programmer également les paramètres, *Début de période d'ouverture, page 249* et *Fin de période d'ouverture, page 250*.
L'heure indiquée dans ce paramètre est l'heure la plus tôt possible à laquelle un utilisateur est autorisé à ouvrir une partition avant l'heure de *Début de période d'ouverture, page 249*. Si les rapports d'ouverture et de fermeture sont activés, le désarmement de la partition entre minuit et l'heure de Début d'ouverture anticipée génère un rapport d'ouverture.

- Si le paramètre *Désactiver O/F dans la période, page 114* est défini sur Oui et que la partition est désarmée entre l'heure de Début d'ouverture anticipée et l'heure de Début de période d'ouverture, l'événement d'ouverture est envoyé avec un modificateur d'ouverture anticipée. Si l'heure de Début d'ouverture anticipée est identique à l'heure de Début de période d'ouverture, aucun événement d'ouverture n'est envoyé.
- Si le paramètre *Désactiver O/F dans la période, page 114* est défini sur Non et que la partition est désarmée à tout moment, un événement est envoyé sans modificateur d'ouverture anticipée ou modificateur d'ouverture tardive.

Le désarmement de la partition entre l'heure de Début de période d'ouverture et l'heure de Fin de période d'ouverture crée un événement local dans le journal des événements de la centrale, mais il n'envoie pas le rapport d'ouverture au centre de télésurveillance.
Le désarmement de la partition entre l'heure de Fin de période d'ouverture et l'heure de Début d'ouverture anticipée de la période suivante (ou minuit, si elle est antérieure) génère un événement d'ouverture avec un modificateur d'ouverture tardive.
Lorsque vous configurez plusieurs périodes pour le même jour, veillez à ce qu'elles soient ajoutés au système dans l'ordre chronologique. Par exemple, si trois périodes sont programmées pour s'exécuter le mardi, la période 1 (W1) doit se produire avant la période 2 (W2) et la période 2 doit se produire avant la période 3 (W3).

- Évitez de programmer l'heure de Début d'ouverture anticipée avant une heure qui se trouve entre les heures de Début de période d'ouverture et de Fin de période d'ouverture d'une autre période.
- Ne programmez pas une période pour passer la limite de minuit.

L'heure de début des périodes désactivées est 00:00. Si l'entrée de ce paramètre est 00:00, mais que des heures sont programmées pour Début de période d'ouverture et Fin de période d'ouverture, la période est désactivée.
Pour désactiver la période, tous les espaces heures et minutes doivent être 00:00.
Veillez à ce que les valeurs temporelles utilisent une horloge 24 heures. Par exemple, minuit = 00:00 ; 7:00 AM = 07:00 ; 2:45 PM = 14:45 ; 11:59 PM = 23:59.
Si la période doit s'activer le jour où vous la programmez, redémarrez la centrale pour activer la période du jour.

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Début d'ouverture anticipée

12.1.5 Début de période d'ouverture

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes)
Ce paramètre est l'un des trois paramètres requis pour créer une période d'ouverture. Saisissez l'heure à laquelle la centrale doit démarrer la période d'ouverture. La période démarre au début de la minute.
00:00 correspond à minuit, 12:00 à midi. Créez des entrées à l'aide d'une horloge 24 heures (par exemple, 7:00 du matin est entré 7:00, 2:45 de l'après-midi est entré 14:45).

Pour programmer une période d'ouverture, il est nécessaire également de programmer les paramètres Début d'ouverture anticipée et Fin de période d'ouverture.

Pour obtenir de plus amples informations
Début de fermeture anticipée, page 250
Fin de période d'ouverture, page 250

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Début de période d'ouverture

12.1.6 Fin de période d'ouverture

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes)
Saisissez l'heure à laquelle la centrale doit terminer la période d'ouverture. La période s'arrête à la fin de la minute.
00:00 correspond à minuit, 12:00 à midi. Créez des entrées à l'aide d'une horloge 24 heures (par exemple, 7:00 du matin est entré 7:00, 2:45 de l'après-midi est entré 14:45).
Ce paramètre est l'un des trois paramètres requis pour créer une période d'ouverture. Pour programmer une période d'ouverture, il est nécessaire également de programmer les paramètres *Début de fermeture anticipée, page 250* et *Début de période d'ouverture, page 249*.
Si la partition n'est pas désarmée à l'expiration de la *Fin de période d'ouverture, page 250*, la centrale génère un rapport ÉCHEC D'OUVERTURE s'il est activé dans *Échec d'ouverture, page 115*.
Les rapports d'ouverture générés entre les heures de Début de période d'ouverture et de Fin de période d'ouverture peuvent être supprimés en définissant le paramètre *Désactiver O/F dans la période, page 114* sur Oui. Voir Début d'ouverture anticipée pour plus de détails sur les autres fonctions de rapport.
N'utilisez pas l'heure 23:59 comme heure de fin de période à moins qu'une autre période commence le jour suivant à 00:00.
La centrale n'envoie pas de rapports ÉCHEC D'OUVERTURE pour les périodes qui se terminent à 23:59.

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Fin de période d'ouverture

12.1.7 Début de fermeture anticipée

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes) 00:00 à 23:59
Saisissez l'heure la plus tôt possible à laquelle l'utilisateur peut fermer une partition avant l'heure de Début de la période de fermeture.
Ce paramètre est l'un des trois paramètres requis pour créer une période de fermeture. Pour terminer la programmation d'une période de fermeture, il est nécessaire de programmer les paramètres *Début de la période de fermeture, page 251* et *Fin de la période de fermeture, page 252*.
L'heure entrée dans ce paramètre est l'heure la plus tôt possible à laquelle l'utilisateur peut fermer une partition avant l'heure de Début de la période de fermeture. Si les rapports d'ouverture et de fermeture sont activés, l'armement de la partition entre minuit et l'heure entrée dans ce paramètre génère un rapport de fermeture.

Si le paramètre *Désactiver O/F dans la période, page 114* est défini sur Oui et que la partition est armée entre l'heure de Début de fermeture anticipée et l'heure de Début de la période de fermeture, l'événement de fermeture est envoyé avec un modificateur de fermeture anticipée. Si l'heure de Début de fermeture anticipée est identique à l'heure de Début de la période de fermeture, aucun événement de fermeture n'est envoyé.
Si le paramètre Désactiver O/F dans la période est défini sur Non et que la partition est armée à tout moment, un événement de fermeture est envoyé sans les modificateurs de fermeture anticipée et de fermeture tardive.
L'armement de la partition entre les heures de Début de la période de fermeture et de Fin de la période de fermeture crée un événement local dans le journal des événements de la centrale, mais il n'envoie pas le rapport de fermeture au centre de télésurveillance.
L'armement de la partition après l'heure de Fin de la période de fermeture et avant l'heure de Début de fermeture anticipée de la période suivante (ou minuit, si elle est antérieure) génère un événement de fermeture avec un modificateur de fermeture anticipée.
Lorsque vous configurez plusieurs périodes pour le même jour, veillez à ce qu'elles soient ajoutés au système dans l'ordre chronologique. Par exemple, si trois périodes sont programmées pour s'exécuter le mardi, la période 1 (W1) doit se produire avant la période 2 (W2) et la période 2 doit se produire avant la période 3 (W3).
Évitez de programmer l'heure de *Début d'ouverture anticipée, page 248* avant une heure située entre les heures de *Début de période d'ouverture, page 249* et de *Fin de période d'ouverture, page 250* d'une autre période.
L'heure de début des périodes désactivées est 00:00. Si l'entrée de ce paramètre est 00:00, mais que des heures sont programmées pour Début de la période de fermeture et Fin de la période de fermeture, la période est désactivée.
Pour désactiver la période, les espaces heures et minutes doivent être 00:00.
Veillez à ce que les valeurs temporelles utilisent une horloge 24 heures. Par exemple, minuit = 00:00 ; 7:00 AM = 07:00 ; 2:45 PM = 14:45 ; 11:59 PM = 23:59.
Si la période doit s'activer le jour où vous la programmez, redémarrez la centrale pour activer la période du jour.

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Début de fermeture anticipée

12.1.8 Début de la période de fermeture

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes)
Ce paramètre est l'un des trois paramètres requis pour créer une période de fermeture. Saisissez l'heure à laquelle la centrale doit démarrer la période de fermeture. La période démarre au début de la minute.
00:00 correspond à minuit, 12:00 à midi. Créez des entrées à l'aide d'une horloge 24 heures (par exemple, 7:00 du matin est entré 7:00, 2:45 de l'après-midi est entré 14:45).
Pour programmer une période de fermeture, vous devez également programmer les paramètres *Début de fermeture anticipée, page 250* et *Fin de la période de fermeture, page 252*.
Une tonalité d'avertissement retentit et [VEUILLEZ FERMER MAINTENANT] s'affiche sur le clavier si la partition n'est pas armée à l'heure de Début de la période de fermeture. Pour rendre temporairement silencieuse la tonalité, appuyez sur la touche [ÉCHAP] du clavier. La tonalité d'avertissement redémarre 10 minutes plus tard si la partition n'est pas armée.
Voir *Début de fermeture anticipée, page 250* pour plus de détails sur la fonction de rapport.

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Début de la période de fermeture

12.1.9 Fin de la période de fermeture

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes)
Ce paramètre est l'un des trois paramètres requis pour créer une période de fermeture. Saisissez l'heure à laquelle la centrale doit terminer la période de fermeture. La période s'arrête à la fin de la minute.
00:00 correspond à minuit, 12:00 à midi. Créez des entrées à l'aide d'une horloge 24 heures (par exemple, 2:45 de l'après-midi est entré 14:45).
Pour programmer une période de fermeture, vous devez également programmer les paramètres Début de fermeture anticipée et Début de la période de fermeture.
Si la partition n'est pas armée à l'heure d'expiration de Fin de la période de fermeture, la centrale génère un rapport ÉCHEC DE FERMETURE s'il est activé dans Échec de fermeture.
Les rapports de fermeture générés entre les heures de Début de la période de fermeture et de Fin de la période de fermeture peuvent être supprimés en définissant le paramètre Désactiver O/F dans la période sur Oui. Voir Début de fermeture anticipée pour plus de détails sur les autres fonctions de rapport.
N'utilisez pas l'heure 23:59 comme heure de fin de période à moins que la période continue le jour suivant à 00:00. Les rapports ÉCHEC DE FERMETURE ne sont pas envoyés, et la fonction Fermeture automatique ne fonctionne pas pour les périodes qui se terminent à 23:59.
Ne programmez pas une seule période pour passer la limite de minuit. L'heure d'arrêt de la période doit être postérieure à l'heure de début de la période. Pour programmer une période qui dépasse la limite de minuit, vous devez programmer deux périodes.
Par exemple, pour programmer les périodes d'une partition qui ferme entre 23:30 et 00:30, cinq jours par semaine, utilisez deux périodes comme indiqué :

		Ouvrir			**Fermeture**			
N° période	Jour de la semaine	Ouverture anticipée	Début	Arrêt	Ouverture anticipée	Début	Arrêt	sauf pendant les congés
1	**DLMMJ** VS				22:00	23:30	23:59	Oui/**Non**
2	D**LMMJ V**S				00:00	00:00	00:30	Oui/**Non**

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Fin de la période de fermeture

12.1.10 sauf pendant les congés

Valeur par défaut : Non
Choix :
– Oui : ne pas activer cette période pendant les congés.
– Non : un congé n'empêche pas l'activation de cette période.

Ce paramètre vous permet de déterminer si la période est désactivée les jours de congés, ou si elle est active uniquement les jours de congés.
Pour éviter que les périodes ne s'activent certains jours de l'année, définissez le paramètre sauf pendant les congés sur Oui et activez au moins un index de congé. Lorsque le paramètre sauf pendant les congés est défini sur Oui, la période s'exécute les jours de semaine programmés à moins que la date soit définie comme un congé par l'index de congé sélectionné.
Pour pouvoir utiliser ce paramètre, il est nécessaire que la période soit programmée pour s'activer au moins un jour de la semaine et un index de congé doit être activé.
Vous pouvez également effectuer ce choix si les périodes d'ouverture et/ou de fermeture sont nécessaires uniquement certains jours de l'année. Ne programmez pas les périodes pour une exécution les jours de la semaine. En revanche, définissez le paramètre sauf pendant les congés sur Non et sélectionnez au moins un index de congé avec les jours de l'année où vous souhaitez que la période soit active.

Pour obtenir de plus amples informations
Congé n°, page 255

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > sauf pendant les congés

12.1.11 Congé n°

Valeur par défaut (Congé 1) : Non
Choix :
Oui : utiliser l'index de congé sélectionné avec cette période.
Non : ne pas utiliser l'index de congé sélectionné avec cette période.
Ce paramètre permet d'activer jusqu'à quatre index de congés pour une utilisation avec les périodes d'ouverture/de fermeture.
Activez au moins un index de congé si le paramètre *sauf pendant les congés, page 255* est défini sur Oui pour cette période, ou si vous souhaitez que cette période s'active uniquement à des dates spécifiques.

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Congé 1 à 8

12.1.12 Numéro de partition

Valeur par défaut : Non
Choix :
– Oui : activer la période dans le numéro de partition spécifié.
– Non : désactiver la période dans le numéro de partition spécifié.
Ce paramètre détermine si une période particulière s'active dans chacune des partitions de la centrale.

Emplacement dans le menu RPS
Planifications > Périodes d'ouverture/de fermeture > Partition n°

12.2 Périodes de groupe d'utilisateurs

Utilisez les paramètres de cette section pour créer des périodes de groupe d'utilisateurs. Lorsque vous affectez un groupe d'utilisateurs à l'une des périodes, les badges (code, carte d'accès ou jeton et télécommande radio) de chaque utilisateur du groupe d'utilisateurs sont activées pendant la durée entre l'heure d'activation et l'heure de désactivation de la période.

Chaque groupe d'utilisateurs peut être lié à plusieurs périodes de groupe d'utilisateurs sur une période de 24 heures.
Pour plus de détails sur l'affectation d'utilisateurs à un groupe d'utilisateurs, voir Configuration utilisateur > Affectations utilisateur > *Groupe d'utilisateurs, page 164*. Si un utilisateur n'est pas lié à un groupe d'utilisateurs ou si le groupe d'utilisateurs n'est pas lié à une période de groupes d'utilisateurs, les informations d'identification de cet utilisateur sont toujours activées.

12.2.1 Groupe d'utilisateurs

Valeur par défaut : 1
Choix :
– B6512 : 0 à 6
Le choix 0 correspond à Non affecté.
Sélectionnez un groupe d'utilisateurs dans ce paramètre. Les badges de l'utilisateur (code, carte d'accès ou jeton et télécommande radio) des utilisateurs liés au groupe d'utilisateurs sont activées pendant la durée entre l'heure d'activation et l'heure de désactivation de la période du groupe d'utilisateurs.
Vous pouvez lier un groupe d'utilisateurs à plusieurs périodes de groupes d'utilisateurs sur une période de 24 heures, mais les périodes ne doivent pas se chevaucher ou dépasser la limite de minuit.
Si vous avez créé des noms spécifiques pour le paramètre, ce nom s'affiche comme <*Numéro index*> : <*nom descriptif*> dans la sélection de paramètre.

Emplacement dans le menu RPS
Planifications > Périodes de groupes d'utilisateurs > Groupes d'utilisateurs

12.2.2 Dimanche au samedi

Valeur par défaut (Dimanche à samedi) : Non
Choix : Oui/Non
Dans les sept paramètres de jour de la semaine, sélectionnez les jours de la semaine pendants lesquels la période du groupe d'utilisateurs est active.
Pour éviter que les périodes ne s'activent certains jours de l'année, définissez le paramètre sauf pendant les congés sur Oui et activez au moins un index de congé. Lorsque le paramètre sauf pendant les congés est défini sur Oui, la période s'exécute les jours de semaine programmés à moins que la date soit définie comme un congé par l'index de congé sélectionné.
Si des périodes d'ouverture et/ou de fermeture sont uniquement nécessaires certains jours de l'année, ne programmez l'exécution de ces périodes pour aucun jour de la semaine. À la place, définissez le paramètre sauf pendant les congés sur Non et sélectionnez un index de congé avec les jours de l'année où vous souhaitez que la période soit active.

Pour obtenir de plus amples informations
sauf pendant les congés, page 255

Emplacement dans le menu RPS
Planifications > Périodes de groupes d'utilisateurs > Dimanche à samedi

12.2.3 Heure d'activation du groupe

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes)

À partir de l'heure que vous entrez ici, les badges (code, carte d'accès ou jeton et télécommande radio) de chaque utilisateur du groupe d'utilisateurs sont activées. La période commence au début de la minute.
Dans la fenêtre contextuelle **Entrée de l'heure**, entrez l'heure du jour de début de la période. Utilisez le format 24 heures (par exemple, 7:00 du matin est entré 07:00, 2:45 de l'après-midi est entré 14:45).
Si vous sélectionnez **Désactiver** dans la fenêtre contextuelle Entrée de l'heure, Heure d'activation du groupe repasse sur 00:00.
Pour démarrer une période à l'heure que vous entrez ici le jour où vous configurez la centrale, sélectionnez **Réinitialiser la centrale** lorsque vous déconnectez RPS depuis la centrale.

Emplacement dans le menu RPS
Planifications > Périodes de groupes d'utilisateurs > Heure d'activation du groupe

12.2.4 Heure de désactivation du groupe

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes)
L'heure que vous entrez ici est la fin de la période du groupe d'utilisateurs. Les badges (code d'accès, carte d'accès ou jeton et télécommande radio) de chaque utilisateur du groupe d'utilisateurs sont désactivées. La période se termine à la fin de la minute.
Dans la fenêtre contextuelle **Entrée de l'heure**, entrez l'heure du jour de fin de la période. Utilisez le format 24 heures (par exemple, 7:00 du matin est entré 07:00, 2:45 de l'après-midi est entré 14:45).
Si vous sélectionnez **Désactiver** dans la fenêtre contextuelle Entrée de l'heure, Heure de désactivation du groupe repasse sur 00:00.
Pour mettre fin à une période à l'heure que vous entrez ici le jour où vous configurez la centrale, sélectionnez **Réinitialiser la centrale** lorsque vous déconnectez RPS depuis la centrale.

Emplacement dans le menu RPS
Planifications > Périodes de groupes d'utilisateurs > Heure de désactivation du groupe

12.2.5 sauf pendant les congés

Valeur par défaut : Non
Choix : Oui/Non
Ce paramètre vous permet de déterminer si la période est désactivée les jours de congés, ou si elle est active uniquement les jours de congés. Suivez les instructions fournies dans sauf pendant les congés.

Emplacement dans le menu RPS
Planifications > Périodes de groupes d'utilisateurs > sauf pendant les congés

12.2.6 Congé n°

Valeur par défaut : Non
Choix :
Oui : utiliser l'index de congé sélectionné avec cette période.
Non : ne pas utiliser l'index de congé sélectionné avec cette période.
Ce paramètre active jusqu'à quatre index de congés à utiliser avec les Périodes de groupes d'utilisateurs.

Activez au moins un index de congé si le paramètre sauf pendant les congés est défini sur Oui pour cette période utilisateur, ou si vous souhaitez que cette période s'active uniquement à des dates spécifiques.

Emplacement dans le menu RPS
Planifications > Périodes de groupes d'utilisateurs > Congé n°

12.3 Planifications

Utilisez le module PLANIFICATIONS pour programmer la centrale afin qu'elle exécute automatiquement les fonctions qui seraient sinon démarrées par l'utilisateur final au niveau du clavier. Chaque planification peut être programmée pour une exécution à une heure spécifique et à une date ou un jour spécifique de la semaine.
Une planification peut être modifiée à partir du clavier si le paramètre Modification de l'heure est défini sur Oui. La date et l'heure peuvent être modifiées à l'aide de la fonction [Modifier les planifications ?].
Chaque numéro de planification peut être programmé avec l'une des 24 fonctions de la fonction. Une fonction est ce qui est exécuté. Outre la fonction, il est nécessaire de choisir les éléments qui sont liés par la fonction. (Par exemple, lors du choix d'une planification de désarmement, le désarmement est la fonction tandis que les partitions qui sont choisies pour le désarmement représentent les éléments qui sont liés.)
Les fonctions et les paramètres associés sont décrits en détail à la suite du paramètre Fonction.
Chaque planification peut être programmée avec jusqu'à quatre index de congés. Les index de congés peuvent être utilisés pour exécuter la planification pendant les congés en plus de la date et du ou des jours de la semaine. Ils peuvent aussi être utilisés pour éviter que la planification ne s'exécute lors des congés (voir sauf pendant les congés).

12.3.1 Texte du nom de planification

Valeur par défaut : Planification n°
Choix : jusqu'à 32 caractères alphanumériques
Entrez jusqu'à 32 caractères de texte pour décrire la partition.

Emplacement dans le menu RPS
Planifications > Planifications > Texte du nom de la planification

12.3.2 Texte du nom de la planification (deuxième langue)

Valeur par défaut : vide
Choix : jusqu'à 32 caractères alphanumériques
Entrez jusqu'à 32 caractères de texte pour décrire la partition.

Emplacement dans le menu RPS
Planifications > Planifications >Nom du texte de la planification (deuxième langue)

12.3.3 Modification de l'heure

Valeur par défaut : Oui
Choix :
Oui. L'utilisateur peut modifier l'heure de cette planification à partir du clavier, et celle-ci s'affiche sur l'écran MODIFIER LES PLANIFICATIONS.
Non. L'utilisateur ne peut pas modifier l'heure de cette planification depuis le clavier, et celle-ci ne s'affiche pas dans les écrans MODIFIER LES PLANIFICATIONS.

Choisissez si l'utilisateur peut modifier l'heure de cette planification depuis le clavier.

Emplacement dans le menu RPS
Planifications > Planifications > Modification de l'heure

12.3.4 Fonction

Valeur par défaut : Non utilisé
Choix : Consultez la liste des fonctions de planification ci-dessous.
Sélectionnez, dans le menu déroulant, le nom de la fonction qui doit être exécutée par cette planification.
RPS affiche les choix de paramètres disponibles et les champs de portée pour cette fonction. (Par exemple, une liste de cases à cocher s'affiche automatiquement pour les partitions lors de la sélection de la fonction d'armement/de désarmement.)

Remarque!
La fonction Tout activé - Aucune sortie est ignorée lors de l'armement depuis une planification.

Non utilisé : cette fonction est désactivée et aucune fonction après celle-ci ne sera exécutée.
Tout activée Temporisée, page 260
Tout activé Instantané, page 260
Partielle Temporisée, page 260
Partielle Instantané, page 260
Désarmer, page 260
Étendre la fermeture, page 260
Inhiber un point, page 261
Rétablir un point, page 261
Rétablir tous les points, page 261
Activer la sortie, page 261
Désactiver la sortie, page 261
Activer/désactiver la sortie, page 261
Réinitialiser toutes les sorties, page 261
Déverrouiller la porte, page 261
Verrouiller la porte, page 262
Porte sécurisée, page 262
Niveau de contrôle d'accès, page 262
Événements avec accès octroyé, page 262
Événements avec accès refusé, page 262
Connecter vous à RPS, page 262
Port utilisateur du contact RPS, page 263
Envoyer le rapport de statut, page 263
Envoyer le rapport de test, page 263
Envoyer test même si état anormal, page 265
Détection activée, page 265
Détection désactivée, page 265
Afficher la date et l'heure, page 265
Émettre tonalité de détection, page 266
Définir le volume du clavier, page 266
Définir la luminosité du clavier, page 266

Exécuter la fonction personnalisée, page 266

Emplacement dans le menu RPS
Planifications > Planifications > Planification 1-80 > Fonction

12.3.5 Heure

Valeur par défaut : Désactiver
Choix : Désactivé, HH:MM (heures et minutes)
Entrez l'heure à laquelle la planification s'exécute à l'aide d'une horloge 24 heures (par exemple, 2:45 de l'après-midi est entré 14:45).
Les planifications désactivées affichent « Désactivé » dans la cellule.
Procédez comme suit pour programmer une heure :

1. Double-cliquez sur le champ correspondant à la planification dont vous souhaitez programmer l'heure.
2. Si « Désactiver » est sélectionné, désélectionnez-le. Le champ d'heure devient actif.
3. Cliquez dans le champ d'heure et utilisez les flèches haut et bas pour définir l'heure, ou entrez l'heure souhaitée.
4. Cliquez sur OK.

Procédez comme suit pour désactiver une planification :

1. Double-cliquez sur le champ correspondant à la planification que vous souhaitez désactiver.
2. Sélectionnez « Désactiver ».
3. Cliquez sur OK.

Emplacement dans le menu RPS
Planifications > Planifications > Heure

12.3.6 Date

Valeur par défaut : Désactiver
Choix : Désactiver, Jour/Mois (par exemple, 12 juin)
Entrez la date d'exécution de la planification. Les planifications désactivées affichent « Désactivé » dans la cellule Date.

Emplacement dans le menu RPS
Planifications > Planifications > Date

12.3.7 Dimanche au samedi

Valeur par défaut (Dimanche à samedi) : Non
Choix : Oui, Non
Ces paramètres des sept jours de la semaine permettent de sélectionner les jours de la semaine où la planification est active.
Pour éviter que les planifications ne s'activent certains jours de l'année, définissez le paramètre *sauf pendant les congés, page 259* sur Oui et activez au moins un index de congé. Lorsque le paramètre sauf pendant les congés est défini sur Oui, la période s'exécute les jours de semaine programmés à moins que la date soit définie comme un congé par l'index de congé sélectionné.
Si une planification est nécessaire certains jours de l'année, ne programmez pas la planification pour une exécution les jours de la semaine. À la place, définissez le paramètre sauf pendant les congés sur Non et sélectionnez un index de congé avec les dates où vous souhaitez que la période soit active.

Emplacement dans le menu RPS
Planifications > Planifications > Dimanche à samedi

12.3.8 sauf pendant les congés

Valeur par défaut : Non
Choix :
– Oui. Vous pouvez éviter que cette planification s'exécute lors des congés identifiés dans les index de congés spécifiques utilisés avec cette planification. Les index de congés spécifiques sont sélectionnés dans cette section de programmation et programmés dans le module de programmation suivant.
– Non. Cette planification s'exécute lors des congés programmés dans le ou les index de congés utilisés avec cette planification.

Si aucun jour de la semaine n'est programmé, cette planification s'exécute uniquement lors des congés programmés dans le ou les index de congés utilisés avec cette planification. Cette planification s'exécute également si les congés tombent un jour de la semaine qui est programmé.

Emplacement dans le menu RPS
Planifications > Planifications > sauf pendant les congés

12.3.9 Congé n°

Valeur par défaut : Non
Choix :
– Oui : utilisez l'index des congés avec cette Période de groupe d'utilisateurs.
– Non : ne pas utiliser l'index des congés avec cette Période de groupe d'utilisateurs.

Activez au moins un index de congé si le paramètre sauf pendant les congés est défini sur Oui pour cette période utilisateur, ou si vous souhaitez que cette période s'active uniquement à des dates spécifiques.

Emplacement dans le menu RPS
Planifications > Planifications > Congé n°

12.4 Index des congés

12.4.1 Planification

Planification des index de congés
Utilisez ce paramètre pour planifier les congés dans un Index des congés.
Pour chaque Index des congés, vous pouvez planifier jusqu'à 365 (366 pour les années bissextiles) jours de congés.
Cliquez sur l'index de congés pour lequel vous souhaitez planifier des congés. La boîte de dialogue de planning de congés ressemble à un calendrier. Elle présente le mois en cours et l’année par défaut. L'année est fournie à des fins de référence uniquement. Seules les données relatives au mois et au jour sont envoyées à la centrale.
Lorsque vous définissez un jour du calendrier en tant que congé, ce jour est ensuite un congé tous les ans. Pour exemple, si vous définissez le 26 octobre 2019 comme un jour de congé, le 26 octobre est un congé en 2020, 2021, etc. Le jour de la semaine change en fonction de l’année.

Emplacement dans le menu RPS
Planifications > Index des congés > Planification des index de congés

12.5 Descriptions des fonctions de planification

12.5.1 Tout activée Temporisée

Cette fonction simule la fonction de clavier Tout activée Temporisée. Les choix effectués à l'invite du paramètre 1 : Partition n° définissent la ou les partitions qui sont armées par cette planification. La planification peut armer plusieurs partitions. Si un point est en défaut lors de l'exécution de la planification, il est armé de force quelle que soit la valeur du paramètre Forcer armement / inhibition max.

12.5.2 Tout activé Instantané

Cette fonction simule la fonction de clavier Tout activé Instantané. Les entrées du champ Paramètre 1 : partition n° définissent la ou les partitions armées par cette planification. La planification peut armer plusieurs partitions. Si un point est en défaut lors de l'exécution de la planification, il est armé de force quelle que soit la valeur du paramètre Forcer armement / inhibition max.

12.5.3 Partielle Temporisée

Cette fonction simule la fonction de clavier Partielle Temporisée. Les choix effectués à l'invite du paramètre 1 : Partition n° définissent la ou les partitions qui sont armées par cette planification. La planification peut armer plusieurs partitions. Si un point est en défaut lors de l'exécution de la planification, il est armé de force quelle que soit la valeur du paramètre Forcer armement / inhibition max.

12.5.4 Partielle Instantané

Cette fonction simule la fonction de clavier Partielle Instantané. Les choix effectués à l'invite du paramètre 1 : Partition n° définissent la ou les partitions qui sont armées par cette planification. La planification peut armer plusieurs partitions. Si un point est en défaut lors de l'exécution de la planification, il est armé de force quelle que soit la valeur du paramètre Forcer armement / inhibition max.

12.5.5 Désarmer

Cette fonction émule la fonction de clavier de désarmement. Les choix effectués à l'invite du paramètre 1 : Partition n° définissent la ou les partitions qui sont désarmées par cette planification. La planification peut désarmer plusieurs partitions.

12.5.6 Étendre la fermeture

Utilisez cette fonction pour changer l'heure de fermeture attendue de cette zone. La fenêtre ne peut pas être ajustée qu'une fois l'heure de début de la fermeture anticipée passée et la fenêtre de fermeture active.

Remarque!
L'heure de fermeture tardive ne peut pas dépasser minuit. Si elle est activée, elle ne peut pas dépasser l'heure de fermeture la plus tardive configurée d'une zone.

12.5.7 Inhiber un point

Cette fonction émule la fonction de clavier Inhiber un point. L'entrée à l'invite du paramètre 1 : Point n° définit le point inhibé par cette planification. Le point peut être inhibé uniquement si le paramètre Inhibable est programmé sur Oui dans le profil de point lié au point. L'inhibition est indiquée si les rapports d'inhibition sont activés dans le profil de point lié au point. La planification peut inhiber un point.

12.5.8 Rétablir un point

Cette fonction émule la fonction de raccourci clavier Rétablir un point. L'entrée à l'invite du paramètre 1 : Point n° définit le point rétabli par cette fonction. Cette fonction peut inhiber uniquement un point.

12.5.9 Rétablir tous les points

Cette fonction n'est pas disponible en tant que fonction de raccourci clavier. Les partitions sélectionnées à l'invite du paramètre 1 : partition n° définissent les partitions dans lesquelles cette fonction rétablit tous les points.

Remarque!

Les points en défaut 24 heures ne sont pas rétablis

Pour éviter les événements d'alarme de point ou de défaut, les points 24 heures inhibés qui sont en défaut lors de l'exécution de cette fonction ne sont pas rétablis. Ils restent inhibés.

12.5.10 Activer la sortie

Cette fonction émule le raccourci clavier Changer l'état de sortie pour l'activation des sorties.

L'entrée indiquée à l'invite du Paramètre 1 : Sortie n° définit la sortie spécifique activée par cette fonction. La fonction peut activer une sortie.

12.5.11 Désactiver la sortie

Cette fonction émule le raccourci clavier Changer l'état de sortie pour la désactivation des sorties.

L'entrée indiquée à l'invite du Paramètre 1 : Sortie n° définit la sortie spécifique désactivée par cette fonction. La fonction peut désactiver une sortie.

12.5.12 Activer/désactiver la sortie

Cette fonction n'est pas disponible en tant que fonction de raccourci clavier. L'entrée indiquée à l'invite du Paramètre 1 : Sortie n° définit la sortie spécifique activée/désactivée par cette fonction. Si la sortie est activée, elle est désactivée. Si la sortie est désactivée, elle est activée. La fonction n'a d'effet que sur une sortie.

12.5.13 Réinitialiser toutes les sorties

Cette fonction n'est pas disponible en tant que fonction de raccourci clavier. Cette fonction désactive toutes les sorties qui sont activées par une planification ou une fonction personnalisée. Il s'agit d'une fonction de niveau centrale. Aucun autre paramètre ne requiert d'entrée pour cette option.

12.5.14 Déverrouiller la porte

Cette fonction émule la fonction de raccourci clavier Déverrouiller la porte. Cette fonction déverrouille la ou les portes programmées dans le Paramètre 1 : Porte n°.

12.5.15 Verrouiller la porte

Cette fonction émule la fonction de raccourci clavier Verrouiller la porte. Cette fonction retourne la ou les portes programmées dans le Paramètre 1 : Porte n° à leur état normal de verrouillage.

12.5.16 Porte sécurisée

Cette fonction émule la fonction de raccourci clavier Verrouiller la porte. Cette fonction retourne la ou les portes programmées dans le Paramètre 1 : Porte n° à leur état normal de verrouillage.

12.5.17 Niveau de contrôle d'accès

Cette fonction n'est pas disponible en tant que fonction de raccourci clavier et elle détermine si le niveau d'autorité pour l'accès du clé ou de la carte d'un utilisateur est activé ou désactivé.
Lorsque le Paramètre 1 : Niveau d'accès est défini sur Actif, l'accès est accordé aux niveaux d'autorité programmés au Paramètre 2 : Niveau.
Lorsque le Paramètre 1 : Niveau d'accès est défini sur Inactif, l'accès est refusé aux niveaux d'autorité programmés au Paramètre 2 : Niveau.

12.5.18 Événements avec accès octroyé

Cette fonction n'est pas disponible en tant que fonction de raccourci clavier et elle détermine si les événements avec accès octroyé sont enregistrés dans le journal des événements de la centrale.
Lorsque le Paramètre 1 : Niveau d'accès est défini sur Actif, les portes programmées au Paramètre 2 : Porte n° placent leurs événements avec accès octroyé dans le journal des événements de la centrale.
Lorsque le Paramètre 1 : Niveau d'accès est défini sur Inactif, les portes programmées au Paramètre 2 : Porte n° ne placent pas leurs événements avec accès octroyé dans le journal des événements de la centrale.

12.5.19 Événements avec accès refusé

Cette fonction n'est pas disponible en tant que fonction de raccourci clavier et détermine si les événements avec accès refusé sont enregistrés dans le journal des événements de la centrale.
Lorsque le Paramètre 1 : Niveau d'accès est défini sur Actif, les portes programmées au Paramètre 2 : Porte n° placent leurs événements avec accès refusé dans le journal des événements de la centrale.
Lorsque le Paramètre 1 : Niveau d'accès est défini sur Inactif, les portes programmées au Paramètre 2 : Porte n° ne placent pas leurs événements avec accès refusé dans le journal des événements de la centrale.

12.5.20 Connecter vous à RPS

Cette fonction essaie de contacter un service RPS autonome à l'heure configurée. Le compte de la centrale dans RPS contrôle les opérations effectuées en cas de contact réussi.

Remarque!
Évitez d'exécuter plusieurs fonctions en même temps à la même adresse. Les fonctions peuvent être en conflit et l'effet sur la centrale est imprévisible.

Remarque!
Ne programmez pas plusieurs planifications sur le même clavier pendant le même temps d'exécution.

Remarque!
Ne programmez pas des planifications qui s'exécutent à des heures auxquelles un utilisateur est susceptible d'être en train d'exécuter des fonctions au clavier.

12.5.21 Port utilisateur du contact RPS

Cette fonction essaie de contacter le service RPS autonome à l'heure configurée via un dispositif de communication réseau au niveau du port configuré. Le compte de la centrale dans RPS contrôle les opérations effectuées en cas de contact réussi.

12.5.22 Envoyer le rapport de statut

Cette fonction génère un rapport d'état pour chaque partition qui est activée. Le rapport est envoyé aux téléphones programmés pour les rapports de test et les rapports de statut dans le routage de rapport.
Le rapport de statut peut être différé si aucun autre rapport n'a été envoyé depuis le dernier rapport de statut. Pour différer le rapport de statut pendant 24 heures, définissez l'option du Paramètre 1 : Différé sur Oui.

Remarque!
Conflit entre les rapport de planification exécutée
Désactivez les rapports de planification exécutée si vous utilisez des rapports de test différé ou d'état. Ces rapports ne s'exécuteront pas si les rapports de planification exécutée sont activés.

12.5.23 Envoyer le rapport de test

Cette fonction de planification envoie le même rapport de test que la fonction de rapport de test utilisateur.
Vous pouvez envoyer des rapports de test à 1 ou à l'ensemble des destinations qui sont configurées pour un groupe destinataire. Le dispositif de destination principal ainsi que le premier, deuxième et troisième dispositifs de destination de sauvegarde peuvent envoyer des rapports de test manuels et automatiques (programmés).
Si un point dans n'importe quelle partition est anormal (défaut non effacé de l'écran du clavier), la centrale envoie un rapport de test anormal au lieu du rapport de test.
Si le paramètre Paramètres liés à la centrale > Routage des rapports > *Transmission rapport de test, page 33* est défini sur Oui, le rapport de test (ou le rapport de test anormal) est suivi d'un rapport de diagnostic pour chaque état anormal du système. Accédez à Paramètres liés à la centrale > Routage des rapports > *Rapports diagnostiques, page 61* pour obtenir une liste des rapports inclus.

Choix, Paramètre 1 : Différé

- Oui : différer l'envoi des rapports de test pendant 24 heures, si la centrale envoie un autre rapport.
- Non : ne pas différer l'envoi de rapports de test.

Remarque!

Seul l'envoi du rapport de test est différé

Lorsque le Paramètre 1 : Différé est défini sur Oui, seul l'envoi du rapport de test est différé. La planification Envoyer le rapport de test continue de s'exécuter selon la fréquence définie dans le Paramètre 2 : Fréquence.

Choix, Paramètre 2 : Fréquence

- Toutes les heures : la première planification Envoyer le rapport de test s'exécute à l'heure entrée au paramètre Heure de la planification. La planification Envoyer le rapport de test s'exécute ensuite toutes les heures.
- Tous les mois : la première planification Envoyer le rapport de test s'exécute à l'heure entrée au paramètre Heure de la planification, à la date indiquée au paramètre Date. La planification Envoyer le rapport de test s'exécute ensuite tous les mois.
- Planifié - la planification d'envoi du rapport de test est exécutée selon les paramètres d'heure, de date et des jours de la semaine de la planification.

Remarque!

Si le paramètre 2 est défini sur Planifié et qu'une date est saisie dans le paramètre Date, les paramètres des jours de la semaine sont ignorés.

La centrale envoie le rapport de test à la date et à l'heure saisies dans les paramètres Date et Heure de la planification.

Choix, paramètre 3

Lorsque le paramètre 3 est configuré pour n'importe quel Groupe de destinataires (principal, premier, deuxième ou troisième Dispositif de destination de sauvegarde), le paramètre 4 des destinations est activé. Pour plus d'informations sur la configuration des Groupes de destinataires, voir *Communicateur, vue d'ensemble, page 66*.

Choix, paramètre 4

Lorsque Paramètre 4 est activé, toutes les destinations Groupe destinataire configurées sont affichées. Cochez la case en regard du ou des Groupes destinataires que vous souhaitez utiliser comme destination.

Différer les rapports de test

Lorsque le Paramètre 1 : Différé est défini sur Oui, la centrale démarre (ou redémarre) un minuteur de décompte 24 heures chaque fois qu'elle reçoit un accusé de réception du récepteur du centre de télésurveillance pour un rapport.

Si le Paramètre 2 est défini sur Toutes les heures et si la centrale n'a pas reçu d'accusé de réception à l'heure d'exécution de la première planification Envoyer le rapport de test, la centrale envoie le rapport de test. Si la centrale a reçu un accusé de réception, les rapports de test sont différés pendant 24 heures à partir du dernier accusé de réception reçu. La planification Envoyer le rapport de test qui doit s'exécuter Toutes les heures n'envoie pas de rapport de test pendant au moins 24 heures.

Si le Paramètre 2 est défini sur Tous les mois et si la centrale n'a pas reçu d'accusé de réception dans les 24 heures qui suivent l'heure de la première exécution de planification Envoyer le rapport de test, la centrale envoie le rapport de test. Si la centrale reçoit un accusé de réception dans les 24 heures qui suivent l'heure à laquelle une planification mensuelle Envoyer le rapport de test doit s'exécuter, le rapport de test est différé pendant 24 heures à partir du dernier accusé de réception reçu. Si le minuteur de compte à rebours 24 heures arrive à expiration, la centrale envoie le rapport de test différé à ce moment-là.

Si le Paramètre 2 est défini sur Planifiée et si la centrale n'a pas reçu d'accusé de réception dans les 24 heures qui suivent l'heure d'exécution planifiée pour la planification Envoyer le rapport de test, la centrale envoie le rapport de test. Si la centrale reçoit un accusé de réception dans les 24 heures qui suivent l'heure à laquelle une planification Envoyer le rapport de test est planifiée pour exécution, le rapport de test est différé pendant 24 heures à partir du dernier accusé de réception reçu. Si le minuteur de compte à rebours 24 heures arrive à expiration, la centrale envoie le rapport de test différé à ce moment-là.

Remarque!
Conflit entre les rapport de planification exécutée
Désactivez les rapports de planification exécutée si vous utilisez des rapports de test différé ou d'état. Ces rapports ne s'exécuteront pas si les rapports de planification exécutée sont activés.

Configuration du routage des rapports
Pour la configuration du routage des rapports pour les rapports de test, les rapports de test anormaux et les rapports de test étendus, reportez-vous à Paramètres liés à la centrale > Routage des rapports > Rapports de test > *Rapports de test, page 60*.

12.5.24 Envoyer test même si état anormal

Lorsque cette fonction de planification es exécutée et qu'un point dans n'importe quelle partition est anormal (défaut non effacé de l'écran du clavier), la centrale envoie un rapport de test anormal. S'il n'y aucun point anormal lorsque cette planification est exécuté, la centrale n'envoie pas de rapport.
Si le paramètre Paramètres liés à la centrale > Routage des rapports > *Transmission rapport de test, page 33* est défini sur Oui, le rapport de test (ou le rapport de test anormal) est suivi d'un rapport de diagnostic pour chaque état anormal du système. Accédez à Paramètres liés à la centrale > Routage des rapports > *Rapports diagnostiques, page 61* pour obtenir une liste des rapports inclus.

12.5.25 Détection activée

Cette fonction émule le fonctionnement du raccourci clavier Changer le mode de détection en activant le mode de détection pour les partitions programmées au Paramètre 1 : partition n°. Le mode de détection déclenche un carillon sur un clavier dans la portée lorsqu'un point de surveillance est en défaut alors qu'il est désarmé.

12.5.26 Détection désactivée

Cette fonction émule le fonctionnement du raccourci clavier Changer le mode de détection en désactivant le mode de détection pour les partitions programmées au Paramètre 1 : partition n°.

12.5.27 Afficher la date et l'heure

Cette fonction émule le raccourci clavier Afficher la date et l'heure en affichant la date et l'heure en cours sur les claviers SDI2 spécifiés au Paramètre 1 : claviers n°.

Remarque!
Lorsque vous utilisez la fonction Afficher la date et l'heure avec les fonctions Définir le volume du clavier et Définir la luminosité du clavier dans la même fonction personnalisée, elles doivent être séparées d'environ 10 secondes avec une fonction Temporisation.

12.5.28 Émettre tonalité de détection

Cette fonction n'est pas disponible en tant que raccourci clavier. Lorsque cette fonction est activée, les claviers SDI2 spécifiés au Paramètre 1 : claviers n° émettent en continu une tonalité de détection.
Arrêtez la tonalité par n’importe quelle interaction avec le clavier ou désactivation de la tonalité en appuyant sur la touche Echap.

12.5.29 Définir le volume du clavier

Cette fonction définit les claviers configurés indiqués au Paramètre 1 : clavier n° au niveau de volume entré au Paramètre 2 : Niveau de volume. Pour plus de détails sur les paramètres de volume, voir *Volume du clavier, page 130* dans la section relative à la configuration clavier.

12.5.30 Définir la luminosité du clavier

Cette fonction définit les claviers configurés indiqués au Paramètre 1 : clavier n° au niveau de luminosité sélectionné au Paramètre 2 : Niveau de luminosité. Pour plus de détails sur le paramètre de luminosité, voir le paramètre *Luminosité du clavier, page 131* dans la section relative à la configuration clavier.

12.5.31 Exécuter la fonction personnalisée

Cette fonction exécute la fonction personnalisée sélectionné au Paramètre 1 : fonction personnalisée n° à une heure programmée.

13 Accès

13.1 Porte nº

Utilisez les paramètres de cette section pour configurer chaque porte.

13.1.1 Texte du nom de porte

Valeur par défaut : Porte ##
Choix : jusqu'à 32 caractères alphanumériques
La centrale B6512 prend en charge les portes 1 à 4.
Entrez jusqu'à 32 caractères de texte pour décrire la porte.

Emplacement dans le menu RPS
Accès > Portes > Texte du nom de porte

13.1.2 Texte du nom de porte (deuxième langue)

Valeur par défaut : vide
Choix : jusqu'à 32 caractères alphanumériques
La centrale B6512 prend en charge les portes 1 à 4.

Entrez jusqu'à 32 caractères de texte pour décrire la porte.

Emplacement dans le menu RPS
Accès > Portes > Texte du nom de porte (deuxième langue)

13.1.3 Partition d'entrée

Valeur par défaut : 1
Choix :
– B6512 : 1-6
Affectez une partition au contrôleur de porte. Il s'agit de la partition de sortie d'un utilisateur lors de l'initiation une demande de sortie (REX).

Emplacement dans le menu RPS
Accès > Portes > Entrée

13.1.4 Nº du clavier associé

Valeur par défaut : aucun clavier
Choix : 0 à 32
– B6512 : 1 à 12
Ce paramètre définit le contrôleur de porte pour le clavier SDI2 associé à KP# Double authentification. Le paramètre Désactivé désactive également le fonctionnement Double authentification.
Entrez le numéro du clavier (KP#) qui détermine la portée des droits de désarmement de l'ID utilisateur. Les partitions se désarment sur la base de la portée de ce clavier et de son niveau d'autorité.
Aucun clavier : seule la partition liée à la partition d'entrée se désarme pour cette porte.

Emplacement dans le menu RPS
Accès > Portes > Nº du clavier associé

13.1.5 Fonction personnalisée

Par défaut : Désactivé
Choix :

– B6512G : Désactivé, CF128 à CF133

Désactivé : la fonction personnalisée est désactivée.

CF### : numéro de fonction personnalisée qui s'active lorsqu'un ID valide est entré, si le niveau d'accès utilisateur et le niveau d'armement de la partition sont appropriés.

Utilisez ce paramètre pour programmer une fonction personnalisée qui s'active sur le clavier programmé pour la portée.

Cette fonction personnalisée s'active uniquement pour les utilisateurs avec une autorité de niveau fonction qui permet à un ID valide d'exécuter une fonction personnalisée pendant l'état armé ou désarmé.

L'utilisateur auquel la carte ou le clé est lié doit avoir un code.

Le tableau suivant illustre comment cette programmation affecte l'activation de la fonction personnalisée :

Niveau de fonction	Activation de fonction personnalisée
A (armé)	Le clé utilisateur active la fonction personnalisée liée au contrôleur de porte uniquement lorsque la partition d'entrée pour le contrôleur de porte est Tout activé ou Partielle.
D (désarmé)	Le clé utilisateur active la fonction personnalisée liée au contrôleur de porte uniquement lorsque la partition d'entrée pour le contrôleur de porte est désarmée.
C (armé et désarmé)	La clé utilisateur active la fonction personnalisée liée au contrôleur de porte, quel que soit l'état armé de la partition d'entrée.
Vide	La clé utilisateur n'active pas la fonction personnalisée liée au contrôleur de porte.

Emplacement dans le menu RPS

Accès > Portes > Fonction personnalisée n°

13.1.6 Point de porte

Valeur par défaut : 0

Choix : 0 (aucun point lié), 1-96

Utilisez ce paramètre pour lier un point à une porte. Ce point ne peut pas être utilisé pour les autres affectations de point.

Les points de porte doivent être programmés en tant que points Partielle. Si un point de porte requiert un comportement de type de point 24 heures, utilisez le type de point Partielle avec une Réponse du point 9 à C pour la réponse d'alarme instantanée lorsque la partition est active (armée) ou inactive (désarmée).

Si vous sélectionnez un point intégré (points 1-8) comme point de porte, veillez à ce qu'aucune résistance de fin de ligne ne soit connectée à la boucle de détecteur sur la centrale.

N'activez aucun point POPIT (ou point OctoPOPIT) avec le même numéro de point comme point de porte. Si vous utilisez le même numéro de point pour le point de porte et un point POPIT ou OctoPOPIT, un défaut de point supplémentaire est crée.

Emplacement dans le menu RPS
Accès > Portes > Point de porte

13.1.7 Stabilisation du point de porte

Valeur par défaut : 600 ms
Choix :

Stabiliser		
300 ms	1800 ms	3300 ms
600 ms	2100 ms	3600 ms
900 ms	2400 ms	3900 ms
1200 ms	2700 ms	4200 ms
1500 ms	3000 ms	4500 ms

Ce paramètre définit la durée pendant laquelle le module de contrôle d'accès analyse un point de porte avant de déclencher une alarme. Pour les paramètres appropriés, consultez les instructions du fabricant du dispositif connecté au point de porte.

Emplacement dans le menu RPS
Accès > Portes > Stabilisation du point de porte

13.1.8 Point de verrouillage

Valeur par défaut : 0
Choix : 0 (aucun point lié), 1-96
Utilisez ce paramètre pour définir un point en tant que point de verrouillage. Un point de verrouillage ne peut pas être utilisé pour d'autres affectations de point.
Les points de verrouillage doivent être programmés en tant que points Partielle. Si un point de verrouillage requiert un comportement de type de point 24 heures, utilisez le type de point Partielle avec une Réponse du point 9 à C pour la réponse d'alarme instantanée lorsque la partition est active (armée) ou inactive (désarmée).
Lorsqu'un point de verrouillage est en défaut, il empêche le module de contrôle d'accès d'autoriser l'accès pour une lecture d'ID ou une demande de porte valide.
Vous pouvez utiliser le même point en tant que point de verrouillage pour plusieurs modules de contrôle d'accès. Le partage d'un point en tant que point de verrouillage pour plusieurs modules permet à un point en défaut d'éviter que plusieurs modules accordent un accès.
Le point de verrouillage est considéré comme dans un état normal s'il est inhibé, inhibé par défaut ou armé de force. On a ainsi un fonctionnement normal de l'accès même si la porte est laissée ouverte.

Emplacement dans le menu RPS
Accès > Portes > Point de verrouillage

13.1.9 Porte automatique

Valeur par défaut : non
Choix :

– Oui : lorsque la partition liée dans le paramètre Partition d'entrée est désactivée (désarmée), l'état de la porte est automatiquement Déverrouillé.
– Non : lorsque la partition liée dans le paramètre Partition d'entrée est désactivée (désarmée), l'état de la porte n'est pas modifié. L'état précédent de la porte reste le même (verrouillé ou déverrouillé).

Utilisez ce paramètre pour déverrouiller la porte (shuntage verrouillé et gâche) automatiquement lorsque le paramètre Partition d'entrée est définie sur Désactivé (désarmée). La porte se verrouille de nouveau lorsque la partition est définie sur Tout activé ou Partielle (armée).
Ce paramètre n'affecte pas l'état armé de la partition. Lorsque la partition affectée au paramètre Partition d'entrée de porte est armée, Tout act ou Part act, l'état de la porte passe automatiquement à verrouillé, quel que soit la valeur du paramètre Porte automatique (Oui ou Non).

Remarque!
Utilisation d'une porte sécurisée pour remplacer l'état Déverrouillé
Vous ne pouvez remplacer manuellement l'état Déverrouillé. Utilisez le paramètre Porte sécurisée pour remplacer ce paramètre.

Emplacement dans le menu RPS
Accès > Portes > Porte automatique

13.1.10 Déverrouillage en cas d'incendie

Valeur par défaut : non
Choix :
Oui : L'alarme incendie ou gaz de n'importe quelle partition déverrouille la porte.
Non : la porte ne change pas de mode en cas d'alarme incendie ou gaz.
Utilisez ce paramètre pour déverrouiller la sortie du point de gâche de porte et shuntage de porte en cas d'alarme incendie ou gaz. Un événement de déverrouillage de porte est traité. Cette fonctionnalité remplace un état Porte sécurisée, un état Porte verrouillée et un point de verrouillage en défaut. Lorsqu'un déverrouillage incendie se produit, vous devez reverrouiller la porte manuellement à partir d'un clavier.

Remarque!
Cela déverrouille la porte, quel que soit l'état armé.

Remarque!
Vous pouvez faire revenir à un état normal les portes activées par un déverrouillage en cas d'incendie, en appuyant sur 8 - Menu principal > 3 - Actions > 8 - Accès, ou via le clavier avec la commande 46 - Menu Accès.

Remarque!
Pour les contrôleurs de porte configurés pour la double authentification, le paramètre Déverrouillage en cas d'incendie est disponible uniquement si vous configurez le clavier associé avec une Fonction de saisie du code de type Cycle de porte. Toutes les autres fonctions de saisie du code utilisent le lecteur de clé pour l'authentification et empêchent toutes les fonctions de porte y compris le Déverrouillage en cas d'incendie.

Emplacement dans le menu RPS
Accès > Portes > Déverrouillage en cas d'incendie

13.1.11 Désarmer à l'ouverture

Valeur par défaut : Non
Choix :
Oui : la partition se désarme uniquement après qu'un accès a été accordé à un utilisateur avec l'autorité de désarmement, et que le point de porte a été en défaut (la porte a été ouverte).
Non : la partition se désarme lorsqu'un utilisateur avec un niveau de désarmement valide présente un clé/une carte valide, que la porte ait ou non été ouverte.
Utilisez cet élément de programmation pour déterminer si la porte doit être physiquement ouverte avant le désarmement de la partition en cas de demande d'accès valide. L'utilisateur qui initialise la demande d'accès doit avoir les niveaux d'accès qui permettent le désarmement avec ID.

Emplacement dans le menu RPS
Accès > Portes > Désarmer à l'ouverture

13.1.12 Durée de gâche

Valeur par défaut : 10
Choix : 1 - 240 secondes
La gâche s'active pendant la durée programmée.
Entrez la durée pendant laquelle la sortie de la gâche s'active afin de permettre à un utilisateur d'ouvrir la porte. La gâche s'active si le badge (carte), la demande d'entrée (RTE), la demande de sortie (REX) et la fonction [CYCLE DE PORTE ?] du clavier sont valides.

Emplacement dans le menu RPS
Accès > Portes > Durée de gâche

13.1.13 Durée de shuntage

Valeur par défaut : 10
Choix : 0 - 254
La durée de shuntage de porte peut être définie en secondes, minutes ou heures.
Entrez la durée pendant laquelle la porte est shuntée afin de permettre à un utilisateur d'ouvrir la porte sans que le point ne déclenche un défaut, une alarme ou une condition en défaut.

Remarque!
Pour les portes connectées SDI, la centrale applique automatiquement la durée maximale de 240.
Pour les portes connectées SDI2, une centrale dépourvue de firmware prenant en charge les temps de shuntage les plus importants appliquera les entrées au-delà de 240 en secondes.

Choix	Valeur de temps
0-240	0-240 secondes
241	5 minutes
242	10 minutes

243	20 minutes
244	30 minutes
245	40 minutes
246	50 minutes
247	60 minutes
248	2 heures
249	3 heures
250	4 heures
251	5 heures
252	6 heures
253	7 heures
254	8 heures

Emplacement dans le menu RPS
Accès > Portes > Durée de shuntage

13.1.14 Durée de la sonnerie

Valeur par défaut : 2
Choix : 0, 1 - 240 secondes
0 : aucune durée de sonnerie pour cette porte.
1 - 240 : la sonnerie retentit pendant la durée (en secondes) programmée.
Entrez la durée (en secondes) pendant laquelle la sortie de sonnerie s'active pour avertir l'utilisateur que la gâche est activée et que la porte est prête pour l'ouverture. La sonnerie s'arrête lorsque la porte est ouverte.
Une sonnerie distincte est requise.
De nombreux lecteurs comportent une sonnerie interne qui n'est pas liée par le paramètre Durée de la sonnerie.

Emplacement dans le menu RPS
Accès > Portes > Durée de la sonnerie

13.1.15 Durée d'extension

Valeur par défaut : 10
Choix : 0, 1 - 30 secondes
Entrez la durée (1 à 30) pendant laquelle prolonger l'activation de la gâche, de la sonnerie et du shuntage lorsque la durée de shuntage expire et qu'une porte reste ouverte. À la fin de la durée d'extension programmée, la sonnerie continue à retentir jusqu'à ce que la porte se ferme. En outre, s'il est programmé, le point lié à la porte indique un défaut, une alarme ou une défaillance au niveau du clavier.
Quelle que soit la programmation de point de porte, le système génère un événement de défaut Porte laissée ouverte lorsque le système est désarmé et un événement d'alarme Porte laissée ouverte lorsque le système est armé et que la porte est maintenue ouverte au-delà de la durée d'extension Des événements « Porte fermée - Rétablissement » sont générés après que la porte est restée ouverte au-delà de la Durée d'extension et qu'elle est revenue à l'état normal.

Entrez 0 pour désactiver la Durée d'extension. L'événement de défaut Porte laissée ouverte, l'événement d'alarme Porte laissée ouverte et l'avertissement au niveau du clavier sont tous désactivés.

Emplacement dans le menu RPS
Accès > Portes > Durée d'extension

13.1.16 Désactiver à l'ouverture

Valeur par défaut : Oui
Choix :
Oui : la gâche se désactive lorsque le point de porte est en défaut (la porte est ouverte) une fois l'accès accordé.
Non : la gâche reste activée pendant la durée de gâche programmée, ou la gâche se désactive lorsque le point de porte est en défaut (la porte est ouverte) et restauré (fermée) une fois l'accès accordé, selon la première échéance.
Ce paramètre détermine si la gâche se désactive immédiatement lors de l'ouverture physique de la porte (le point de porte est en défaut).
Pour que cette fonction fonctionne, un point doit être lié au paramètre Point de porte.
Afin de réduire les fausses alarmes lorsque la porte « rebondit » ouverte, laissez ce paramètre sur Oui (valeur par défaut).

Emplacement dans le menu RPS
Accès > Portes > Désactiver à l'ouverture

13.1.17 Shuntage RTE uniquement

Valeur par défaut : Non
Choix :
Oui : lorsque la demande d'entrée RTE sur le module de contrôle d'accès est court-circuitée, le point de porte est shunté pendant la Durée de shuntage. La sortie de gâche n'est pas activée.
Non : lorsque la demande d'entrée RTE sur le module de contrôle d'accès est court-circuitée, le point de porte est shunté pendant la Durée de shuntage. La sortie de gâche est activée pendant la Durée de gâche.
Utilisez ce paramètre lorsqu'un utilisateur peut ouvrir une porte manuellement sans compter sur un clé/une carte pour activer la gâche (une « barre poussoir », par exemple).

Remarque!
Aucun événement RTE lorsque le paramètre Shuntage RTE uniquement est défini sur Oui
Lorsque le paramètre Shuntage RTE uniquement est défini sur Oui, la centrale ne consigne ni ne signale aucun événement Demande d'entrée lorsque l'entrée RTE est court-circuitée.

Emplacement dans le menu RPS
Accès > Portes > Shuntage RTE uniquement

13.1.18 Stabilisation d'entrée RTE

Valeur par défaut : 600 ms
Choix :

Stabiliser		
300 ms	1800 ms	3300 ms
600 ms	2100 ms	3600 ms

Stabiliser		
900 ms	2400 ms	3900 ms
1200 ms	2700 ms	4200 ms
1500 ms	3000 ms	4500 ms

Ce paramètre définit la durée pendant laquelle le module de contrôle d'accès analyse l'entrée RTE avant d'initier un événement Demande d'entrée (RTE). Pour les paramètres appropriés, consultez les instructions du fabricant du dispositif connecté à l'entrée RTE.

Emplacement dans le menu RPS
Accès > Portes > Stabilisation d'entrée RTE

13.1.19 Shuntage REX uniquement

Valeur par défaut : Non
Choix :
Oui - la durée de shuntage programmée s'active afin que la porte puisse être ouverte manuellement.
Non-: la demande de sortie (REX) active automatiquement la durée de gâche et de shuntage programmées.
Utilisez cet élément de programmation pour désactiver la gâche, en activant quand même la durée de shuntage programmée en cas de demande de sortie d'une partition.
Utilisez ce paramètre lorsqu'un utilisateur peut ouvrir une porte manuellement sans compter sur un clé/une carte pour activer la gâche (une « barre poussoir », par exemple).
Lorsque ce paramètre Shuntage REX uniquement est défini sur Oui, les événements de demande de sortie ne sont pas consignés ou signalés.

Emplacement dans le menu RPS
Accès > Portes > Shuntage REX uniquement

13.1.20 Stabilisation d'entrée REX

Valeur par défaut : 600 ms
Choix :

Stabiliser		
300 ms	1800 ms	3300 ms
600 ms	2100 ms	3600 ms
900 ms	2400 ms	3900 ms
1200 ms	2700 ms	4200 ms
1500 ms	3000 ms	4500 ms

Ce paramètre définit la durée pendant laquelle le module de contrôle d'accès analyse l'entrée REX avant d'initier un événement Demande de sortie (REX). Pour les paramètres appropriés, consultez les instructions du fabricant du dispositif connecté à l'entrée REX.

Emplacement dans le menu RPS
Accès > Portes > Stabilisation d'entrée REX

13.1.21 Accès octroyé

Valeur par défaut : Oui

Choix :

Oui : les événements ACCÈS OCTROYÉ et DEMANDE D'ACCÈS AUX PORTES sont consignés et signalés.

Non : les événements ACCÈS OCTROYÉ et DEMANDE D'ACCÈS AUX PORTES ne sont ni consignés ni signalés.

Ce paramètre détermine si les événements ACCÈS OCTROYÉ et DEMANDE D'ACCÈS AUX PORTES de ce module de contrôle d'accès sont consignés et signalés par la centrale.

Un événement ACCÈS OCTROYÉ peut être initié par :

- une lecture valide d'un badge (carte ou clé)
- un état de porte valide modifié sur le clavier

Emplacement dans le menu RPS

Accès > Portes > Accès octroyé

13.1.22 Accès refusé

Valeur par défaut : Oui

Choix :

Oui : les événements ACCÈS REFUSÉ sont consignés et signalés.

Non : les événements ACCÈS REFUSÉ ne sont ni consignés ni signalés.

Ce paramètre Aucune entrée détermine si les événements ACCÈS REFUSÉ de ce module de contrôle d'accès sont consignés et signalés par la centrale.

Un événement Aucune entrée (ACCÈS REFUSÉ) peut être généré par :

- un ID utilisateur, un verrouillage ou une porte sécurisée inconnus ou non valides, ou un niveau d'autorité incorrect
- une demande d'entrée/de sortie (RTE/REX) pour une porte en verrouillage ou une porte sécurisée

Emplacement dans le menu RPS

Accès > Portes > Aucune entrée

13.1.23 Demande d'entrée

Valeur par défaut : non

Choix :

Oui : les événements Demande d'entrée (RTE) sont consignés et signalés.

Non : les événements Demande d'entrée (RTE) ne sont pas consignés et signalés.

Ce paramètre détermine si les événements Demande d'entrée (RTE) de ce module de contrôle d'accès sont consignés et signalés par la centrale.

Le format Modem 4 est pris en charge. Le contact ID n’est pas pris en charge. Si Oui est sélectionné, les événements RTE ou REX avec contact ID ne sont pas signalés.

Emplacement dans le menu RPS

Accès > Portes > Demande d'entrée

13.1.24 Demande de sortie

Valeur par défaut : non

Choix :

Oui : les événements Demande de sortie (REX) sont consignés et signalés.

Non : les événements Demande de sortie (REX) ne sont pas consignés et signalés.

Ce paramètre détermine si les événements Demande de sortie (REX) du module de contrôle d'accès sont consignés et signalés par la centrale.

Le format Modem 4 est pris en charge. Le contact ID n'est pas pris en charge. Si Oui est sélectionné, les événements RTE ou REX avec contact ID ne sont pas signalés.

Emplacement dans le menu RPS
Accès > Portes > Demande d'entrée

13.1.25 Mode d'échec

Valeur par défaut : Mode prévention
Choix :
Mode prévention. La porte reste verrouillée pour garantir une sécurité permanente.
Mode sécurité. Le module d'accès libère le mécanisme de verrouillage de porte pour permettre le passage.
Ce paramètre définit le comportement du module d'accès lorsqu'il perd la communication avec la centrale et passe en Mode d'échec.
Cette option de configuration s'applique uniquement aux modules de contrôle d'accès SDI2 B901.

Emplacement dans le menu RPS
Accès > Portes > Mode d'échec

13.1.26 Auto-surveillance du coffret

Valeur par défaut : Non
Choix :
Oui : activer l'entrée d'auto-surveillance (T+).
Non : désactiver l'entrée d'auto-surveillance (T+).

Remarque!
Le paramètre Auto-surveillance du coffret configure l'entrée d'auto-surveillance du lecteur, T +
Pour le module Interface de contrôle d'accès B901, ce paramètre active l'entrée d'auto-surveillance du lecteur (borne T+). Il n'y a pas d'entrée d'auto-surveillance du coffret sur ces modules.

Pour un module D9210C ou B901 sur le bus SDI (Source de la porte = SDI), le raccourcissement de l'entrée d'auto-surveillance (T+) sur commun (COM) crée un événement Point manquant pour le *Point de porte, page 268*.
Pour un module B901 sur le bus SDI2 (Source de la porte = SDI2 (B901)), le raccourcissement de l'entrée d'auto-surveillance (T+) sur commun (COM) crée un événement Point manquant pour le *Point de porte, page 268* et un événement d'auto-surveillance pour le module B901.

Emplacement dans le menu RPS
Accès > Portes > Auto-surveillance du coffret

13.2 Paramètres d'accès global

13.2.1 Type de carte

Valeur par défaut : 26 bits
Choix :
- 26 bits
- MIFARE classic 32 bits

– Corporate 1000 35 bits
– 37 bits, aucun code de site
– 37 bits avec code de site

Ce paramètre spécifie le format de carte et de clé utilisé pour tous les contrôleurs de portes et claviers.

Définissez ce paramètre sur 26 bits si des badges (carte ou clé) sont utilisés avec un clavier B942.

Codes de site par défaut pour les types de carte

26 bits : le code de site par défaut est 255.

32 bits : le code de site par défaut est vide. Le code de site n'est pas configurable (Le paramètre Code de site est grisé).

35 bits : le code de site par défaut est 4095. Entrez le code de site (code d'installation) pendant la configuration d'une carte d'accès utilisateur.

37 bits aucun code de site : le code de site est vide. Le code de site n'est pas configurable (Le paramètre Code de site est grisé).

37 bits avec code de site : le code de site par défaut est 65535.

Emplacement dans le menu RPS

Accès > Paramètres globaux de clavier > Type de carte

13.3 Source de la porte

Valeur par défaut : Désactivé

Choix :

– Désactivé. Le module de porte est désactivé.
– SDI2 (B901)

Utilisez ce paramètre pour lier chaque porte à un type de dispositif.

Emplacement dans le menu RPS

Accès > Portes > Source de la porte

14 Automatisation / App à distance

14.1 Dispositif d'automatisation

Valeur par défaut : Aucun
Choix :
- Aucun. La communication d'automatisation est désactivée.
- Mode 1 avec connexion intégrée sans TLS.
- Mode 1 avec un module B426 à l'adresse 1 de SDI2.
- Mode 1 avec un module B426 à l'adresse 2 de SDI2.
- Mode 1 avec connexion intégrée avec TLS.
- Mode 2 (avec une connexion intégrée ou un module B426 à l'adresse 1-2 de SDI2, avec TLS).

Emplacement dans le menu RPS
Automatisation / App à distance > Dispositif d'automatisation

14.2 Taux du statut

Valeur par défaut : 0
Choix :
- 0 : les informations de statut ne sont jamais envoyées, sauf si demandé.
- 1 - 255 : les informations de statut sont selon l'intervalle programmé.

Ce paramètre définit la fréquence à laquelle les informations de statut par défaut sont envoyées au module d'interface série.
Les informations de statut incluent le statut du point actuel (normal ou anormal), le statut de partition de la centrale (Tout activé, Tout activé Instantané, Partielle Temporisée Armé, Partielle Instantané, Désarmé, Temporisation d'entrée de partition, Partielle Temporisée d'entrée, Temporisation de sortie de partition, Partielle Temporisée de sortie), l'état de la centrale (Défaut secteur, Batterie manquante, Restauration secteur, Batterie faible, et ainsi de suite), ainsi que l'état de sortie (sortie activée ou sortie désactivée).
Les entrées sont définies par incréments de 500 millisecondes. Par conséquent, si la valeur 5 est entrée, les informations d'état sont envoyées toutes les 2 500 ms (ou 2,5 secondes). L'entrée 10 équivaut à 5 secondes. Si le paramètre Taux du statut est défini sur une valeur inférieure à 10 et que entre 1 et 6 dispositifs SDI sont connectés au système, la vitesse d'envoi la plus rapide des informations de statut par la centrale est d'environ 1 seconde. En outre, si plus de 6 dispositifs SDI sont connectés à la centrale, la vitesse d'envoi la plus rapide des informations par la centrale est d'environ 1,5 à 2 secondes.

Emplacement dans l'arborescence de menus de RPS
Automatisation / App à distance > Taux du statut

14.3 Code d'automatisation

Valeur par défaut : Vide
Choix : 6 à 24 caractères.
Ce paramètre définit le code qui doit être entré pour que le logiciel d'automatisation puisse se connecter à la centrale.

Ce paramètre accepte jusqu'à 24 caractères, mais il autorise des codes plus courts. La longueur minimale est de six caractères. Le code est sensible à la casse. Le code d'automatisation doit être saisi pour que d'autres commandes d'automatisation puissent être acceptées par la centrale.

Remarque!
Exigence UL 2610
Pour être conforme à la norme UL 2610, la longueur du mot de passe doit être d'au moins 6 caractères et contenir une combinaison de chiffres, de lettres et de symboles.

Emplacement dans l'arborescence de menus de RPS
Automatisation / App à distance > Code d'automatisation

14.4 Mode 1 Numéro de port Ethernet d'automatisation

Valeur par défaut : 7702
Choix : 1 à 65535
Ce paramètre définit le numéro de port pour le Mode 1 Ethernet d'automatisation.

Emplacement dans le menu RPS
Automatisation / App à distance> Mode 1 Numéro de port Ethernet d'automatisation

14.5 App à distance

Valeur par défaut : Activer
Choix :
- Activé - la centrale peut établir des connexions sécurisées avec les applications à distance.
- Désactivé - la centrale ne peut pas établir des connexions sécurisées avec les applications à distance.

Définissez ce paramètre sur Activer, pour permettre à la centrale d'alarme d'établir des connexions sécurisées avec les applications à distance. L'application Bosch Remote Security Control pour smartphones et tablettes est un exemple d'application à distance.
Définissez ce paramètre sur Désactiver, pour interdire à la centrale d'établir des connexions sécurisées avec les applications à distance.

Emplacement dans le menu RPS
Automatisation / App à distance > Application à distance

14.6 Code d'app à distance

Valeur par défaut : [code de 24 caractères généré de manière aléatoire par RPS]
Choix : 6 à 24 caractères alphanumériques sensibles à la casse :
A-Z, a-z, 0-9,!@#$%^&"()-_+=|` ~,<.>/?;:'"[\{]}

Utilisez ce paramètre pour définir le code de la centrale pour les applications distantes afin d'établir une connexion sécurisée à la centrale. Par exemple, les applications mobiles Bosch Remote Security Control (RSC) et Bosch Security Manager (BSM). Le code est échangé et validé par la centrale d'alarme avant que les autres commandes ou codes utilisateur de centrale ne soient acceptés par la centrale.

Remarque!
Exigence UL 2610
Pour être conforme à la norme UL 2610, la longueur du mot de passe doit être d'au moins 6 caractères et contenir une combinaison de chiffres, de lettres et de symboles.

Lors de la mise à jour d'un code d'application à distance sur la centrale, tous les utilisateurs actuels des applications distantes, telles que RSC ou BSM, perdent la possibilité de se connecter tant que leur application n'a pas reçu un nouveau profil de connexion comprenant le nouveau code d'application à distance.
Pour mettre à jour les utilisateurs de :

- l'application Bosch Security Manager - une mise à jour des services d'installation permet de mettre à jour le profil de connexion de la centrale pour tous les utilisateurs actuels de l'application mobile. RPS met à jour les services d'installation pendant des activités spécifiques s'il est en mesure d'atteindre les services en ligne.
  RPS tente de mettre à jour automatiquement les services d'installation à l'aide des détails de la centrale pendant une nouvelle invitation de l'utilisateur à utiliser l'application Bosch Security Manager et pendant la synchronisation de connexion/ programmation de la centrale.
  Les opérateurs RPS peuvent mettre à jour les services d'installation avec les détails de la centrale à tout moment en accédant à Gestion des utilisateurs de Bosch Security Manager et en sélectionnant Mettre à jour le profil mobile des services d'installation.
- Contrôle de sécurité à distance - utilisez Générer un profil d'accès à distance RPS pour créer un nouveau profil de connexion pour la centrale et le distribuer sur chaque application mobile individuelle.
- Intégration des intrusions SDK - utilisez Générer un profil d'accès à distance RPS pour créer un nouveau profil de connexion pour la centrale et le distribuer à chaque intégrateur.

Remarque!
Désactiver le code d'app à distance pour désactiver la connexion à l'application à distance
Pour éviter qu'un utilisateur d'application à distance (RSC ou BSM) ne se connecte à la centrale, même lorsque le paramètre App à distance est défini sur Activé, définissez le paramètre Code d'app à distance sur Désactivé (toute combinaison de lettres majuscules et minuscules).

Emplacement dans le menu RPS
Automatisation / App à distance > Code d'app à distance

15 Modules SDI2

15.1 Module huit entrées B208

Le module huit entrées B208 comporte des entrées (boucles de capteur) pour 8 points. Le module B208 se connecte au bus SDI2 de la centrale.

Type de centrale	Modules pris en charge
B6512	8

Tableau 15.2: Capacité

Réglages des commutateurs
Consultez Réglages de commutateur matériel > *Réglages de commutateur du module huit entrées B208, page 297*

15.1.1 Auto-surveillance du coffret

Valeur par défaut : Non - Désactiver
Choix :
– Oui : activer l'entrée d'auto-surveillance du coffret
– Non : désactiver l'entrée d'auto-surveillance du coffret
Lorsque l'entrée d'auto-surveillance est activée et connectée à un contact d'auto-surveillance Bosch ICP-EZTS, la centrale crée un événement d'auto-surveillance lorsque la porte du coffret est ouverte, ou lorsque le coffret est arraché du mur.

Emplacement dans le menu RPS
Modules SDI2 > Huit entrées B208 > Auto-surveillance du coffret

15.2 Module huit sorties B308

Le module huit sorties B308 est un dispositif qui se connecte au bus SDI2 de la centrale. Chaque module comporte 8 sorties surveillées de manière indépendante et dont le fonctionnement est similaire à celles des modules de sortie.

Type de centrale	Modules pris en charge
B6512	8

Tableau 15.3: Capacité

Réglages des commutateurs
Voir Réglages de commutateur matériel > *Réglages de commutateur du module huit sorties B308, page 297*

15.2.1 Auto-surveillance du coffret

Valeur par défaut : Non - Désactiver
Choix :
– Oui : activer l'entrée d'auto-surveillance du coffret
– Non : désactiver l'entrée d'auto-surveillance du coffret

Lorsque l'entrée d'auto-surveillance est activée et connectée à un contact d'auto-surveillance Bosch ICP-EZTS, la centrale crée un événement d'auto-surveillance lorsque la porte du coffret est ouverte, ou lorsque le coffret est arraché du mur.

Emplacement dans le menu RPS
Modules SDI2 > Huit sorties B308 > Auto-surveillance du coffret

15.3 Transmetteur IP (B42x)

Connexion du B42x
Connectez le module à la centrale à l'aide du bus SDI2.

Configuration du module
Vous pouvez utiliser un seul ou les deux modules de communication B426/B450 pour la création de rapports du centre de télésurveillance ou les communication RPS. Vous pouvez aussi utiliser l'un des modules B42x pour la communication avec le logiciel d'automatisation.

Remarque!
Pour éviter toute perte de communication, la configuration envoyée à la centrale pour le module B42x ne prend effet qu'une fois RPS déconnecté de la centrale.
Si le module est configuré via l'interface Web de configuration B42x pour désactiver la programmation de centrale (autrement dit, paramètre Programmation de la centrale activé défini sur Non), la programmation RPS du B42x est acceptée par la centrale, mais elle n'est pas appliquée au module B42x. Le paramètre Programmation de la centrale activé n'est pas disponible dans RPS.

15.3.1 Auto-surveillance du coffret du module

Valeur par défaut : Non - Désactiver
Choix :
– Oui : activer l'entrée d'auto-surveillance du coffret
– Non : désactiver l'entrée d'auto-surveillance du coffret
Lorsque l'entrée d'auto-surveillance est activée et connectée à un contact d'auto-surveillance Bosch ICP-EZTS, la centrale crée un événement d'auto-surveillance lorsque la porte du coffret est ouverte, ou lorsque le coffret est arraché du mur.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Auto-surveillance du coffret

15.3.2 Mode IPv6

Valeur par défaut : Non
Choix :
– Oui : utiliser le mode IPv6 (Internet Protocol version 6) pour les communications IP
– Non : utiliser le mode IPv4 (Internet Protocol version 4) pour les communications IP
Lorsque IPv6 activé est défini sur Oui, définissez DHCP/IP automatique activé sur Oui.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Mode IPv6

15.3.3 DHCP IPv6

Valeur par défaut : Activé (Oui)
Choix :

– Activé (Oui) : DHCP définit automatiquement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP. AutoIP permet l'affectation d'adresses IP dynamiques aux dispositifs au démarrage.
– Désactivé (Non) : définissez ce paramètre sur Désactivé s'il n'y a aucun service DHCP. Définissez manuellement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP.

DHCP nécessite un serveur DHCP.

Emplacements dans le menu RPS

SDI2 > Transmetteur IP B42x > DHCP IPv6

15.3.4 DHCP IPv4/IP automatique activé

Valeur par défaut : Activé (Oui)

Choix :

– Activé (Oui) : DHCP définit automatiquement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP. AutoIP permet l'affectation d'adresses IP dynamiques aux dispositifs au démarrage.
– Désactivé (Non) : définissez ce paramètre sur Désactivé s'il n'y a aucun service DHCP. Définissez manuellement l'adresse IP, la passerelle par défaut IP et l'adresse de serveur DNS IP.

DHCP nécessite un serveur DHCP.

Le paramètre n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Emplacement dans le menu RPS

SDI2 > Transmetteur IP B42x > DHCP IPv4/IP automatique activé

15.3.5 Adresse IPv4

Valeur par défaut : 0.0.0.0

Choix : 0.0.0.0 à 255.255.255.255

Si DHCP IPv4/IP automatique activé est défini sur Oui, ce paramètre est grisé (inaccessible).

Si DHCP IPv4/IP automatique activé est défini sur Non, entrez ici l'adresse IPv4.

Ce paramètre n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Emplacement dans le menu RPS

SDI2 > Transmetteur IP B42x > Adresse IPv4

15.3.6 Masque de sous-réseau IPv4

Valeur par défaut : 255.255.255.0

Choix : 0.0.0.0 à 255.255.255.255

Si DHCP IPv4/IP automatique activé est défini sur Oui, ce paramètre est grisé (inaccessible).

Si DHCP IPv4/IP automatique activé est défini sur Non, entrez ici le masque de sous-réseau IPv4.

Le paramètre n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Pour obtenir de plus amples informations

Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS

SDI2 > Transmetteur IP B42x > Masque de sous-réseau IPv4

15.3.7 Passerelle par défaut IPv4

Valeur par défaut : 0.0.0.0
Choix : 0.0.0.0 à 255.255.255.255
Si DHCP IPv4/IP automatique activé est défini sur Oui, ce paramètre est grisé (inaccessible). Si DHCP IPv4/IP automatique activé est défini sur Non, entrez ici l'adresse de passerelle par défaut.
Le paramètre n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Passerelle par défaut IPv4

15.3.8 Adresse IP du serveur DNS IPv4

Valeur par défaut : 0.0.0.0
Choix : 0.0.0.0 à 255.255.255.255
Un serveur de noms de domaine (DNS pour Domain Name Server) utilise les noms de domaine interne ou noms d'hôte pour fournir les adresses IP correspondantes. En mode DHCP, le DNS par défaut du serveur est utilisé. Pour utiliser un serveur DNS personnalisé en mode DHCP, saisissez ici l'adresse IP du serveur DNS personnalisé.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Adresse IP du serveur DNS IPv4

15.3.9 Autre adresse IP du serveur DNS IPv6

Valeur par défaut :
Choix : 0000:0000:0000:0000:0000:0000:0000:0000 à FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Ce paramètre définit l'adresse de serveur DNS IPv6 pour le mode IP statique.
Lorsque cette adresse est définie par le service DHCP, ne la modifiez pas.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Adresse IP du serveur DNS IPv6

15.3.10 UPnP (Universal Plug and Play) activé

Valeur par défaut : Oui
Choix :
Oui (Activé) : utiliser UPnP pour ouvrir un programme d'acheminement de port pour les connexions RPS et RSC (Contrôle de sécurité à distance) entrantes
Non (Désactivé) : ne pas utiliser UPnP
Le paramètre UPnP n'a aucun effet sur la génération de rapport d'événements IP pour un récepteur du centre de télésurveillance.
Le paramètre UPnP n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > UPnP activé

15.3.11 Numéro de port HTTP

Valeur par défaut : 80
Choix : 1 à 65535
Ce paramètre permet la configuration du numéro de port du serveur Web.
Lorsque la sécurité TLS améliorée est activée, HTTPS est appliqué. La valeur par défaut pour HTTPS est 443.
Si la sécurité améliorée n'est pas activée, la valeur HTTP est appliquée.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > Numéro de port HTTP

15.3.12 Délai du cache ARP (secondes)

Valeur par défaut : 600
Choix : 1 à 600 (secondes)
Ce paramètre spécifie le délai des entrées du cache ARP.
Le paramètre n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Délai du cache ARP (secondes)

15.3.13 Accès Web/USB activé

Valeur par défaut : Non
Choix : Oui/Non
Ce paramètre permet aux utilisateurs autorisés d'afficher et de modifier les paramètres de configuration du module via un navigateur Web standard ou un port USB, en fonction des options disponibles.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > Accès Web/USB activé.

15.3.14 Mot de passe d'accès Web/USB

Valeur par défaut : vide
Choix : blanc, caractères ASCII imprimables
Ce paramètre définit un nouveau mot de passe requis pour les connexions directes au moyen d'un accès Web. Le mot de passe doit comporter entre 4 à 10 caractères imprimables ASCII. Les blancs désactivent la vérification de mot de passe.

Remarque!
Exigence UL 2610
Pour être conforme à la norme UL 2610, la longueur du mot de passe doit être d'au moins 6 caractères et contenir une combinaison de chiffres, de lettres et de symboles.

Remarque!
Le code par défaut du module B426 se trouve sur une étiquette apposée sur le module.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP > Mot de passe d'accès Web

15.3.15 Mise à jour du firmware activée

Valeur par défaut : Non

Choix :
Oui : modifier le firmware via l'interface Web.
Non : modifier le firmware via le logiciel de programmation.
Ce paramètre permet de modifier le firmware à l'aide de l'interface Web externe.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > Mise à niveau du firmware activée

15.3.16 Nom d'hôte du module

Valeur par défaut : Vide
Choix : 1-63 caractères, a-z, a-z, 0-9, tiret (-) au format 0000.0000.0000.0000. Notez que le nom d'hôte du module ne peut pas commencer ou finir par un tiret (-).
Le nom d'hôte identifie le communicateur IP (module intégré ou SDI2) sur le réseau. Laissez ce paramètre vide pour utiliser le nom d'hôte par défaut défini en usine.
Le paramètre n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Emplacement dans le menu RPS
SDI2 > IP B42x > Nom d'hôte du module

15.3.17 Description de l'unité

Valeur par défaut : Vide
Choix : : jusqu'à vingt caractères alphanumériques.
Ce paramètre décrit le module (emplacement, attributs, etc.) en 20 caractères au maximum. Utilisez uniquement les caractères suivants : A à Z, 0 à 9, ?, &, @, -, *, +, $, #, /

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > Description de l'unité.

15.3.18 Numéro de port TCP/UDP

Valeur par défaut : 7700
Choix : 0 - 65535
Pour les communications dotées de RPS, de l'automatisation ou du Contrôle de sécurité à distance (RSC) dans les installations standard, conservez le port TCP/UDP par défaut

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > Numéro de port TCP/UDP

15.3.19 Durée de conservation TCP

Valeur par défaut : 4 minutes
Choix : Désactivé - 8 heures
La durée entre les messages d'activité TCP peut être définie en minutes ou en heures. Les messages d'activité permettent de s'assurer qu'une connexion demeure active.
Le paramètre n'a aucun effet sur le fonctionnement de l'interface de communicateur enfichable B450.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Durée de conservation TCP

15.3.20 Adresse de test IPv4

Valeur par défaut : 8.8.8.8
Choix : adresse IPv4 ou nom de domaine

La centrale effectue un ping de l'adresse de test IPv4 afin de vérifier que les paramètres de configuration réseau sont corrects et que le réseau est opérationnel.
L'adresse de test par défaut fonctionne pour la plupart des réseaux.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Adresse de test IPv4

15.3.21 Adresse de test IPv6

Valeur par défaut : 2001:4860:4860::8888
Choix : adresse IPv6 ou nom de domaine
La centrale effectue un ping de l'adresse de test IPv6 afin de vérifier que les paramètres de configuration réseau sont corrects et que le réseau est opérationnel.
L'adresse de test par défaut fonctionne pour la plupart des réseaux.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Adresse de test IPv6

15.3.22 Sécurité Web et d'automatisation

Valeur par défaut : Activer
Choix :
– Désactiver : la sécurité améliorée n'est pas appliquée.
– Activer : la sécurité améliorée est appliquée.

Définissez ce paramètre sur Activer pour une sécurité améliorée pour l'automatisation et l'accès Web du B42x.
Lorsque cette option est activée, HTTPS est appliqué à l'accès Web du B42x, ce qui modifie la valeur par défaut
du paramètre Numéro de port HTTP. Ce paramètre active également la sécurité TLS pour l'automatisation.

Emplacement dans le menu RPS
SDI2 > Transmetteur IP > Sécurité Web et d'automatisation

15.3.23 Autre adresse IP du serveur DNS IPv4

Valeur par défaut : 0.0.0.0
Choix : 0.0.0.0 à 255.255.255.255
Si le transmetteur IP ne parvient pas à obtenir une adresse à partir du serveur principal, il essaie avec le serveur DNS secondaire. Saisissez l'adresse IP du serveur DNS IPv4 secondaire.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Autre adresse IP du serveur DNS IPv4

15.3.24 Autre adresse IP du serveur DNS IPv6

Valeur par défaut :
Choix : 0000:0000:0000:0000:0000:0000:0000:0000 à
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Si le communicateur IP ne parvient pas à obtenir une adresse à partir du serveur principal, il essaie avec le serveur DNS secondaire. Saisissez l'adresse IP du serveur DNS IPv6 secondaire.

Pour obtenir de plus amples informations
Formats de l'adresse IP et du nom de domaine, page 303

Emplacement dans le menu RPS
SDI2 > Transmetteur IP B42x > Autre adresse IP du serveur DNS IPv6

15.4 B450 Cellulaire

15.4.1 SMS entrant

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : Oui
Choix :
– Activé (Oui) - vous pouvez utiliser des messages de texte SMS entrants pour configurer le module.
– Désactivé (Non) - le module ne traite pas les messages de texte SMS entrants.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > SMS entrant

15.4.2 Durée de conservation de la session (minutes)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : 0
Choix : 0 (désactivé) à 1000 (minutes) (0 (disable) to 1000 (minutes))
Temps en minutes entre les messages d'activité. Les messages d'activité permettent de s'assurer qu'une connexion demeure active.
Modifiez uniquement la valeur par défaut pour les installations commerciales homologuées UL1610 haut niveau de sécurité.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Durée de conservation de la session

15.4.3 Délai d'inactivité (minutes)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : 0
Choix : 0 (désactiver) à 1000 (minutes) (0 (disable) to 1000 (minutes))
– 0 (désactivé) (0 (disabled)) - la centrale ne surveille pas le trafic de données.
– 1 à 1 000 (1 to 1000) - délai sans trafic de données avant que la centrale ne mette fin à une session.

Modifiez uniquement la valeur par défaut pour les installations commerciales homologuées haute sécurité UL 1610 qui nécessitent une notification de signal faible.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > SMS entrant

15.4.4 Délai de signalisation de signal de faible puissance (secondes)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : 0 (désactivé) (0 (disabled))
Choix : 0 (désactivé) (0 (disabled), 1 - 3600 (secondes) (1 - 3600 (seconds))
Durée de signal faible (LED rouge sur le transmetteur cellulaire) avant que la centrale ne déclenche un événement Signal faible cellulaire.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Signalisation de délai de signal de faible puissance (secondes)

15.4.5 Signalisation de délai de signal de faible puissance (secondes)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : 0
Choix : 0 (désactivé) - 3600 (secondes) (0 (disabled) - 3600 (seconds))
Conservez la valeur par défaut de ce paramètre, sauf instruction contraire du support Bosch. Lorsque le module enfichable cellulaire ne détecte qu'une seule tour pendant les secondes définies au niveau de ce paramètre, la centrale enregistre un événement Tour unique. Lorsque le transmetteur cellulaire détecte au moins deux tours pendant les secondes définies au niveau de ce paramètre, la centrale enregistre un événement Rétablissement Tour unique.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Signalisation de délai de tour unique

15.4.6 Délai de signalisation d'absence de tour (secondes)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : 0
Choix : 0 (désactivé) - 3600 (secondes) (0 (disabled) - 3600 (seconds))
Lorsque le module enfichable cellulaire ne détecte aucune tour pour les secondes définies par ce paramètre, la centrale enregistre un événement Absence de tour (No Towers) et un événement Pas d'adresse IP (No IP Address).
La centrale enregistre un événement Rétablissement cellulaire aucune tour disponible (Cellular No Tower Available Restoral) lorsque le module enfichable cellulaire détecte une ou plusieurs tours pendant les secondes définies par ce paramètre.
La centrale enregistre un événement Rétablissement Pas d'adresse IP (No IP Address restoral) lorsque le module cellulaire enfichable enregistre une ou plusieurs tours et reçoit une adresse IP dans les 60 secondes.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Signalisation de délai d'absence de tour

15.4.7 Longueur SMS sortant

Valeur par défaut : 160
Choix : 0 (désactivé) à 3 600 (caractères)
Les fournisseurs cellulaires définissent la limite pour la longueur de message SMS à 160 caractères (par défaut). Les fournisseurs rejettent les messages SMS au-dessus de cette limite.

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Longueur du SMS sortant

15.4.8 PIN SIM

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : Vide
Choix : 0-9 (minimum 4 chiffres, minimum 8 chiffres)
Utilisez ce paramètre uniquement lorsqu'un code PIN est nécessaire pour les cartes ICCID. Si aucun code PIN SIM n'est nécessaire, laissez ce champ à blanc.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > PIN SIM

15.4.9 Nom du point d'accès réseau (APN)

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : eaaa.bssd.vzwentp
Choix : 0-9, A-Z, a-z, **-** , **:** , **.** (jusqu'à 60 caractères)
Pour modifier le nom du point d'accès (APN) défini sur la valeur par défaut, entrez jusqu'à 60 caractères. Le champ est sensible à la casse.

Firmware de centrale version 3.07 ou ultérieure
Avec le firmware de centrale version 3.07 ou ultérieure, lorsque le paramètre APN est vide, la centrale utilise une liste interne des valeurs de Network Access Point Name (APN). Lorsqu'un transmetteur cellulaire enfichable B442, B443 ou B444 est branché, la liste interne comprend :
– Iotst.aer.net
– gne
– wyless.apn (valide uniquement pour les versions antérieures à RPS 6.07)
– wyless.com.attz
– bosch.vzwentp
Lorsqu'un transmetteur cellulaire enfichable B444-V est branché, la liste interne comprend :
– bssd.vzwentp
Lorsqu'un transmetteur cellulaire enfichable B444-A est branché, la liste interne comprend :
– bssd.attentp

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Nom du point d'accès réseau (APN)

15.4.10 Nom d'utilisateur du point d'accès réseau

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : Blanc
Choix : Caractères ASCII (jusqu'à 30)
Entrez jusqu'à 30 caractères ASCII pour le nom d'utilisateur du Point d'accès réseau.
Le nom d'utilisateur est sensible à la casse.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Nom de l'utilisateur du point d'accès réseau

15.4.11 Mot de passe du point d'accès réseau

Remarque!
Informations de configuration importantes pour la communication cellulaire
Consultez *Configuration du service Cellulaire, page 300* pour une présentation et des informations sur la configuration.

Valeur par défaut : Blanc
Choix : Caractères ASCII (jusqu'à 30 caractères)
Entrez jusqu'à 30 caractères ASCII pour le mot de passe de Point d’accès réseau.
Le mot de passe est sensible à la casse.

Emplacement dans le menu RPS
Modules SDI2 > Transmetteur IP > B450 Cellulaire > Mot de passe du point d'accès réseau

15.5 Alimentation auxiliaire B5xx

L'alimentation auxiliaire B5xx se connecte au bus SDI2 de la centrale. Elle offre une alimentation 12 volts CC 2,5 A supervisée.

Type de centrale	Modules pris en charge
B6512, B5512	4
B4512	2
B3512	2

Réglages des commutateurs
Voir Réglages de commutateur matériel > Dispositifs SDI2 > *Réglages de commutateur de l'alimentation auxiliaire B5xx, page 298*

15.5.1 Module activé

Valeur par défaut : Non
Choix :
– Oui : superviser le module SDI2.
– Non : ne pas superviser le module SDI2.

Emplacement dans le menu RPS
SD12 > Alimentation B520 > Module activé

15.5.2 Auto-surveillance du coffret du module

Valeur par défaut : Non - Désactiver
Choix :
– Oui : activer l'entrée d'auto-surveillance du coffret
– Non : désactiver l'entrée d'auto-surveillance du coffret
Lorsque l'entrée d'auto-surveillance est activée et connectée à un contact d'auto-surveillance Bosch ICP-EZTS, la centrale crée un événement d'auto-surveillance lorsque la porte du coffret est ouverte, ou lorsque le coffret est arraché du mur.

Emplacement dans le menu RPS
SDI2 > Alimentation auxiliaire B520 > Auto-surveillance du coffret

15.5.3 Une ou deux batteries

Valeur par défaut : Un
Choix :
– Un : une batterie est connectée aux bornes BATT 1 du B5xx.
– Deux : deux batteries sont connectées au B5xx. Une batterie est connectée aux bornes BATT 1 et une batterie est connectée aux bornes BATT 2.

Emplacement du menu RPS
Modules SDI2 > Alimentation auxiliaire B5xx > Une ou deux batteries

15.6 Récepteur radio

La centrale prend en charge deux types de modules d'interface radio SDI2.
- RADION récepteur SD B810
- Interface de bus SDI2 Inovonics B820

Vous pouvez utiliser un seul module radio à la fois.

Remarque!
Choisissez le type de module radio **avant** d'ajouter des points, des utilisateurs ou des répéteurs au système. Lorsque vous modifiez des types radio, RPS réinitialise toutes les informations radio à leurs valeurs par défaut définies en usine. Toutes les informations radio précédemment configurées sont effacées.

Réglages des commutateurs
Voir les *Réglages de commutateur matériel, page 296* du B810/B820

15.6.1 Type de module radio

Valeur par défaut : Radio RADION B810
Choix :
- Non lié
- Radio RADION B810
- Radio Inovonics B820

Ce paramètre configure le système pour un module radio RADION ou Inovonics.
Non lié. Vous ne pouvez pas utiliser de dispositif radio. La radio n'est pas une sélection valide pour le paramètre Source pour tous les points. Vous ne pouvez pas enregistrer les télécommandes radio pour un utilisateur.

Capacité radio B820 Inovonics
Dispositifs : 350 (sans inclure les répéteurs)
Répéteurs : 4
Vous pouvez lier des dispositifs radio Inovonics aux points.
Vous pouvez lier les télécommandes Inovonics aux utilisateurs.

Capacité radio RADION B810
Télécommandes : 1000
Points : 504 (numéros de point valides : 9 à 96)
Répéteurs : 8
Lorsque ces limites sont atteintes, RPS affiche un message d'avertissement. Pour ajouter un autre dispositif de ce type, supprimez un ou plusieurs des dispositifs existants.
Emplacement dans le menu RPS
Modules SDI2 > Récepteur radio > Type de module radio

15.6.2 Auto-surveillance du coffret du module

Valeur par défaut : Non - Désactiver
Choix :
- Oui : activer l'entrée d'auto-surveillance du coffret
- Non : désactiver l'entrée d'auto-surveillance du coffret

Lorsque l'entrée d'auto-surveillance est activée, la centrale crée un événement d'auto-surveillance lorsque le coffret est ouvert ou lorsque le coffret est retiré du mur.

Emplacement dans le menu RPS
SDI2 > Récepteur radio > Auto-surveillance du coffret

15.6.3 Délai de supervision du système (répéteur)

Valeur par défaut : 12 heures
Choix :
– Aucun : désactiver la supervision du répéteur radio.
– 4, 12, 24, 48, 72 heures
Ce paramètre définit le délai de supervision de tous les répéteurs radio configurés. Si le récepteur radio n'a aucune nouvelle d'un répéteur dans le délai (nombre d'heures) défini par ce paramètre, la centrale crée un événement de répéteur manquant.

Remarque!
Délai de supervision de point radio
Configurez le délai de supervision radio pour les points non incendie en utilisant le paramètre Profils de point / *Délai de supervision de point radio, page 237*. Le délai de supervision de point radio pour les points incendie est fixé à 4 heures.

Remarque!
Délai de supervision Télécommande radio
Activez ou désactivez le délai de supervision radio pour les télécommandes à l'aide du paramètre Affectations utilisateur/*Supervisé, page 167*. Lorsque la supervision est activée, le délai de supervision Télécommande radio est fixé à 4 heures.

Emplacement dans le menu RPS
SDI2 > Récepteur radio > Délai de supervision du système

15.6.4 Avertissement de batterie faible

Valeur par défaut : Ne jamais retentir
Choix : Ne jamais retentir, 4 heures, 24 heures
Ce paramètre est global pour tous les points non incendie. La centrale définit automatiquement le paramètre Avertissement de batterie faible sur 24 heures pour les points incendie.
Emplacement dans le menu RPS
Modules SDI2 > Récepteur radio > Avertissement de batterie faible

15.6.5 Détection de brouillage activée

Valeur par défaut : Oui
Choix :
– Oui : activer la détection de brouillage (interférences) radio.
– Non : désactiver la détection de brouillage (interférences) radio.
Pour le module radio Inovonics B820, la détection de brouillage (interférences) radio est toujours activée, même lorsque ce paramètre est défini sur Non.
Emplacement dans le menu RPS
Modules SDI2 > Récepteur radio fil > Détection de brouillage activée

15.7 Répéteur radio

Les répéteurs radio ne sont pas physiquement connectés au bus SDI2. Vous devez configurer un module d'interface radio dans le cadre du système.
La centrale prend en charge deux types de modules d'interface radio SDI2 :

– Radio RADION B810
– Radio Inovonics B820

Le type de répéteur radio doit correspondre au type de récepteur. Choisissez le type de récepteur radio avant de configurer des répéteurs. La centrale prend en charge jusqu'à 8 répéteurs simultanément. Tous les répéteurs doivent être du même type.

15.7.1 Auto-surveillance du coffret du module

Valeur par défaut : Non - Désactiver

Choix :

– Oui : activer l'entrée d'auto-surveillance du coffret
– Non : désactiver l'entrée d'auto-surveillance du coffret

Lorsque l'entrée d'auto-surveillance est activée, la centrale crée un événement d'auto-surveillance lorsque le coffret est ouvert ou lorsque le coffret est retiré du mur.

Emplacement dans le menu RPS

SDI2 > Répéteur radio > Auto-surveillance du coffret

15.7.2 RFID RADION (B810)

Valeur par défaut : 0

Choix : 0, 11 - 167772156

Le numéro RFID est un numéro unique lié aux dispositifs radio en usine. Le numéro RFID se trouve sur l'étiquette du produit.

Étant donné que les répéteurs radio sont à la fois des récepteurs et des transmetteurs, un numéro RFID leur est lié.

Emplacement dans le menu RPS

Modules SDI2 > Récepteur radio > RFID (radio RADION B810)

15.7.3 RFID Inovonics (B820)

Valeur par défaut : N/A

Portée : 0 - 99999999

Le numéro RFID est un numéro unique lié aux dispositifs radio en usine. Le numéro RFID se trouve sur l'étiquette du produit.

Étant donné que les répéteurs radio sont à la fois des récepteurs et des transmetteurs, un numéro RFID leur est lié.

Emplacement dans le menu RPS

Modules SDI2 > Répéteur radio > RFID (Radio Inovonics B820)

16 Réglages de commutateur matériel

16.1 Adresse du clavier

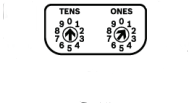
Réglages de commutateur d'adresse du clavier de base B91x

Adresse	Interrupteurs					
	1	2	3	4	5	6
1	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT	ÉTEINT	ÉTEINT
2	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT	ÉTEINT
3	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT	ÉTEINT
4	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT
5	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT
6	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT
7	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT
8	ÉTEINT	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT
9	ALLUMÉ	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT
10	ÉTEINT	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT
11	ALLUMÉ	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT
12	ÉTEINT	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT
13	ALLUMÉ	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT
14	ÉTEINT	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT
15	ALLUMÉ	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT
16	ÉTEINT	ÉTEINT	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT
17	ALLUMÉ	ÉTEINT	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT
18	ÉTEINT	ALLUMÉ	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT
19	ALLUMÉ	ALLUMÉ	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT
20	ÉTEINT	ÉTEINT	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT
21	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT
22	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT
23	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT	ALLUMÉ	ÉTEINT
24	ÉTEINT	ÉTEINT	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT
25	ALLUMÉ	ÉTEINT	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT
26	ÉTEINT	ALLUMÉ	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT
27	ALLUMÉ	ALLUMÉ	ÉTEINT	ALLUMÉ	ALLUMÉ	ÉTEINT
28	ÉTEINT	ÉTEINT	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT
29	ALLUMÉ	ÉTEINT	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT

Adresse	Interrupteurs					
	1	**2**	**3**	**4**	**5**	**6**
30	ÉTEINT	ALLUMÉ	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT
31	ALLUMÉ	ALLUMÉ	ALLUMÉ	ALLUMÉ	ALLUMÉ	ÉTEINT
32	ÉTEINT	ÉTEINT	ÉTEINT	ÉTEINT	ÉTEINT	ALLUMÉ

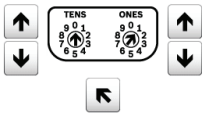
Réglages de commutateur d'adresse du clavier à deux lignes B92x/clavier de type Distributeur de billets B93x

Réglez les commutateurs d'adresse selon la configuration de la centrale. Si plusieurs claviers SDI2 se trouvent sur le même système, chaque clavier SDI2 doit avoir une adresse unique. Pour les adresses à un seul chiffre de 1 à 9, définissez le commutateur des dizaines sur 0. La figure ci-dessous illustre le réglage du commutateur d'adresse pour l'adresse 1.



Réglages de commutateur d'adresse du clavier à écran tactile B94x

Pour définir l'adresse, utilisez les flèches haut et bas à droite de l'image des commutateurs afin de modifier le chiffre des unités, et les flèches situées sur la gauche pour modifier le chiffre des dizaines. Appuyez sur la flèche en diagonale sous les commutateurs pour enregistrer le réglage et revenir à l'écran de mise sous tension.



16.2 Réglages de commutateur du module huit entrées B208

Le tableau suivant décrit la relation entre les réglages de commutateur du module et la plage d'adresses de point qui correspond au réglage. Les valeurs de la plage de points répertoriés dans cette table font référence à POINTS > Affectations de point.
Terminez les entrées B208 inutilisées avec une résistance de fin de ligne.

16.3 Réglages de commutateur du module huit sorties B308

Le tableau suivant décrit la relation entre les réglages de commutateur du module et la plage de numéros de sortie qui correspond au réglage.

16.4 Réglages de commutateur du module de communication Ethernet B426

Ce tableau décrit la relation entre les réglages du commutateur de module et le type de communication de centrale qui correspond au réglage.

Réglage du commutateur B426	Adresse	Type de bus	Fonction
1	1	SDI2	Automatisation, programmation à distance, création de rapports

16.5 Réglages de commutateur du module cellulaire B450

Ce tableau décrit la relation entre les réglages du commutateur de module et le type de communication de centrale qui correspond au réglage.

Réglage du commutateur B450	Adresse	Type de bus	Fonction
0	-	-	paramètre de configuration locale
1	1	SDI2	Automatisation, programmation à distance, création de rapports

16.6 Réglages de commutateur de l'alimentation auxiliaire B5xx

La plage de commutateur d’adresse rotatif pour l’alimentation auxiliaire B5xx est comprise entre 1 et 4 pour les centrales d’alarme B6512 et B5512, entre 1 et 2 pour la centrale d’alarme B4512, et entre 1 et 2 pour la centrale d’alarme B3512. Les plages d'adresse 00 et 05-99 ne sont pas valides sur le bus de dispositif SDI2. Le réglage par défaut en usine est 01. Lorsque vous utilisez plusieurs alimentations, affectez chacune d'elles à un réglage de commutateur différent.

Réglages de commutateur B5xx valides
01
02
03
04

16.7 Réglages de commutateur du récepteur radio RADION B810

Les commutateurs d'adresse B820 et B810 fournissent un réglage à un seul chiffre pour l'adresse du module. Le module utilise l'adresse 1. Les adresses 0 et 2 à 9 ne sont pas valides.

16.8 Réglages de commutateur du récepteur radio Inovonics B820

Les commutateurs d'adresse Inovonics B820 fournissent un réglage à un seul chiffre pour indiquer l'adresse du module. Le module utilise les adresses 1 à 4. Les adresses 0 et 5 à 9 ne sont pas valides.
Seule l'adresse 1 est valide pour ces centrales.

16.9 Réglages de commutateur du module d'accès B901

Deux commutateurs d'adresse déterminent l'adresse pour le module de contrôle d'accès B901. La
centrale utilise l'adresse pour les communications.
Insérez un tournevis plat pour régler les commutateurs d'adresse.

Adresse	Désignation
0,0	Désactivé
0,1 à 0,4	Portes 1 à 4

17 Configuration du service Cellulaire

Inscrivez-vous d'abord au Service Cellulaire Bosch

Avant de pouvoir utiliser la communication cellulaire pour les rapports, les notifications personnelles, les connexions RPS ou RSC, vous devez contacter votre support technique Bosch régional pour configurer ou obtenir les détails de votre compte.

Configuration de RPS pour le service cellulaire

La configuration de RPS pour le service cellulaire est simple et rapide avec l'Assistant de configuration :

1. Cliquez sur Config pour ouvrir le menu de configuration.
2. Sélectionnez Ouvrir l'assistant de configuration.

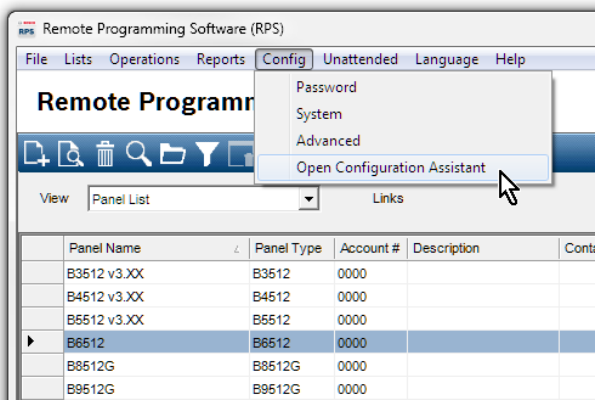


Figure 17.1:

Configuration RPS manuelle pour le service cellulaire

Si vous choisissez de ne pas utiliser l'Assistant de configuration, procédez comme suit pour configurer RPS pour le service cellulaire :

1. Cliquez sur Config pour ouvrir le menu de configuration, puis sélectionnez Système.
2. Cliquez sur l'onglet Connectivité.
3. Cliquez sur Cellulaire.
4. RPS tente d'utiliser les informations ICCID pour créer automatiquement une connexion VPN à la centrale lors de l'utilisation d'un module cellulaire. Si les détails de votre service cellulaire ne peuvent pas être automatiquement récupérés et requièrent une connexion VPN manuelle, entrez les détails de la connexion dans l'onglet VPN. RPS utilisera ces informations pour créer automatiquement votre VPN Windows pendant chaque connexion de la centrale, et pour le supprimer lors de la déconnexion.

Configurez le compte de centrale pour le service cellulaire

La configuration d'un compte de centrale pour le service cellulaire est simple et rapide avec l'Assistant de compte :

1. Dans la Liste de centrales, cliquez avec le bouton droit sur le compte de la centrale que vous souhaitez configurer pour le service cellulaire.
2. Sélectionnez Ouverture de l'Assistant de compte.

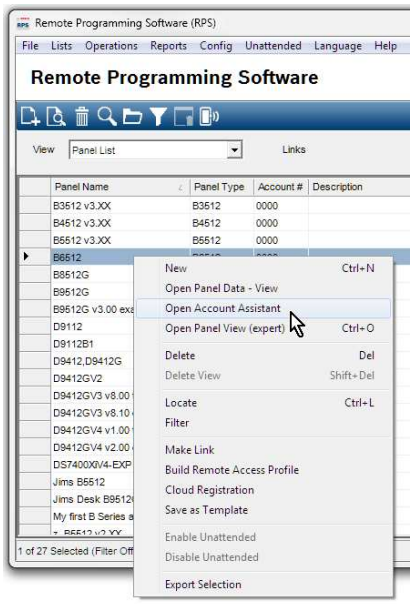


Figure 17.2:

Si vous choisissez de ne pas utiliser l'Assistant de compte, vous pouvez configurer manuellement un compte de centrale pour le service cellulaire en procédant comme suit :

1. Dans la liste de centrales, cliquez sur le compte de centrale pour lequel vous voulez configurer un service cellulaire, puis cliquez sur Ouvrir les données de centrale - Vue.
2. Cliquez sur l'onglet Cellulaire.
3. Entrez les informations dans les champs de connectivité cellulaire. RPS utilise le numéro ICCID pour récupérer et stocker l'adresse IP liée, le numéro de téléphone et le plan attribué pour les utiliser pendant les connexions.

– Lors de la connexion à cette centrale via le réseau cellulaire, RPS récupère les informations de service nécessaires à la création automatique de votre connexion VPN Windows, à l'établissement de la connexion à la centrale, puis au retrait automatique de VPN Windows après déconnexion de la centrale.
– Si votre service cellulaire nécessite une connexion VPN manuelle pour les connexions cellulaires, entrez les détails de la connexion dans Configuration du système RPS > Connectivité > onglet VPN. RPS utilisera ces informations pour créer automatiquement la connexion VPN Windows pendant chaque connexion de la centrale, et pour le supprimer lors de la déconnexion.

4. Lorsque vous avez terminé, cliquez sur OK.
5. Pour définir les paramètres de centrale, cliquez avec le bouton droit sur le compte de centrale sur lequel vous avez cliqué à l'étape 1, puis sélectionnez Ouvrir la vue de centrale.
6. Paramètres liés à la centrale > *Module enfichable cellulaire, page 39* : conservez les valeurs par défaut de ces paramètres. Effectuez uniquement des modifications pour les installations commerciales homologuées UL1610 qui nécessitent une notification de signal faible.
7. Paramètres liés à la centrale > *Communicateur, vue d'ensemble, page 66* > Dispositif de destination principal (Dispositif de destination de sauvegarde) : pour l'envoi des rapports d'un groupe destinataire via un transmetteur cellulaire, sélectionnez une destination Cellulaire (enfichable) comme destination principale (ou de sauvegarde).

8. Paramètres liés à la centrale > *Communication améliorée, page 71* : définissez ici les destinations de rapport, ainsi que les paramètres de polling/supervision. Assurez-vous que les taux de polling cellulaires suivent les paramètres recommandés et sont alignés sur votre plan cellulaire.
9. Paramètres liés à la centrale > Notification personnelle > *Destinations de notification personnelle, page 95* : définissez les numéros de téléphone pour les messages SMS, les adresses e-mail pour les messages électroniques. Définissez la méthode sur SMS cellulaire enfichable, SMS cellulaire de l'élément de bus, E-mail cellulaire enfichable ou E-mail élément de bus.

Se reporter à

- *Module enfichable cellulaire, page 39*
- *Communicateur, vue d'ensemble, page 66*
- *Communication améliorée, page 71*
- *Destinations de notification personnelle, page 95*

18 Formats de l'adresse IP et du nom de domaine

Format d'adresse IPv4

Les adresses IPv4 sont au format décimal ASCII, xxx.xxx.xxx.xxx (xxx = 0 à 255). Les quatre octets (xxx) de l'adresse sont séparés par des points.

Correct : 12.3.145.251

Incorrect : C.17.91.FB

Format d'adresse IPv6

Les adresses IPv6 se composent de huit groupes de 4 chiffres hexadécimaux séparés par des deux points, xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, x = 0 à F.

Format du nom de domaine qualifié complet

Le nom de domaine qualifié complet permet de définir l'adresse exacte d'un dispositif dans la hiérarchie DNS. Il comprend le nom d'hôte unique du dispositif et le sous-réseau sur lequel le dispositif se situe, séparés par des points.

Exemple : receiver01.your-alarm-company.com

Chaque libellé au sein du nom doit être conforme à la norme RFC-921, « Planification de mise en œuvre du système de noms de domaine ».

Seulement les lettres (A-Z), les chiffres (0 à 9) et le signe moins (-) sont autorisés dans les libellés de texte du nom de domaine qualifié complet.

Le point (.) est autorisé uniquement pour délimiter les libellés de texte qui comprennent le nom de domaine qualifié complet.

Avant d'entrer un nom de domaine qualifié complet, assurez-vous que le dispositif adressé est correctement enregistré auprès des serveurs DNS disponibles pour le transmetteur IP. Cette vérification peut être effectuée à l'aide d'un outil ping.

Informations supplémentaires

Des informations sur les noms d'hôtes et les formats de nom de domaine qualifié complets sont disponibles sur le site Web « The Internet Engineering Task Force (IETF) » à l'adresse http://www.ietf.org/

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Pays-Bas
www.boschsecurity.fr

Des solutions pour les bâtiments au service d’une vie meilleure

202409091557