Guide de l’administrateur Synergis™ Cloud Link 3.1.2

Cliquez ici pour obtenir la dernière version de ce document.

Dernière mise à jour du document : 4 septembre 2024

Mentions légales

Informations sur le documents

Titre du document : Guide de l'administrateur Synergis[MC] Cloud Link 3.1.2

Numéro du document d'origine : EN.702.043-V3.1.2(1)

Numéro de document : FR.702.043-V3.1.2(1)

Date de mise à jour du document : 4 septembre 2024

Vous pouvez envoyer vos commentaires, corrections et suggestions concernant ce guide à l'adresse documentation@genetec.com.

À propos de ce guide

Ce guide décrit la configuration de l'appareil Synergis Cloud Link pour une utilisation avec Security Center, ainsi que l'intégration de toutes les unités tierces compatibles avec l'appareil. Il suppose que vous connaissez la plateforme Security Center, et en particulier le système de contrôle d'accès Synergis.

Ce guide est proposé en complément de la documentation suivante :

- *Guide de l'administrateur Security Center*
- *Guide d'installation du matériel Synergis^{MC} Cloud Link*
- *Guide d'intégration Synergis^{MC} Softwire*

Pour en savoir plus, voir le TechDoc Hub.

Ce guide ne couvre pas les informations disponibles dans les documentations de fournisseurs tiers, comme les détails des entrées et sorties de vos modules d'interface. Il ne décrit pas non plus les logiciels tiers.

Terminologie

Dans la plupart des contextes, les termes *unité Synergis^{MC}* (ou *appareil*) et *unité Synergis Cloud Link* (ou *appareil*) sont utilisés de manière interchangeable. Le mot *appareil* est préféré lorsque l'accent est mis sur l'appareil lui-même, et le mot *unité* est préféré lorsque l'accent est mis sur l'inscription de l'appareil dans Security Center.

Notes et avertissements

Les avis et avertissements suivants peuvent être utilisés dans ce guide :

- **Conseil :** Suggère une manière d'appliquer les informations d'un thème ou d'une étape.
- **Note :** Décrit un dossier particulier, ou développe un point important.
- **Important :** Souligne une information critique concernant un thème ou une étape.
- **Attention :** Indique qu'une action ou étape peut entraîner la perte de données, des problèmes de sécurité ou des problèmes de performances.
- **Avertissement :** Indique qu'une action ou une étape peut entraîner des dommages physiques, ou endommager le matériel.

IMPORTANT : Le contenu de ce guide peut faire référence à des informations publiées sur des sites Web de tiers qui étaient correctes au moment de leur publication. Toutefois, ces informations peuvent changer sans notification préalable de la part de Genetec Inc.

Table des matières

Partie I

Introduction

Cette section comprend les chapitres suivants:

1

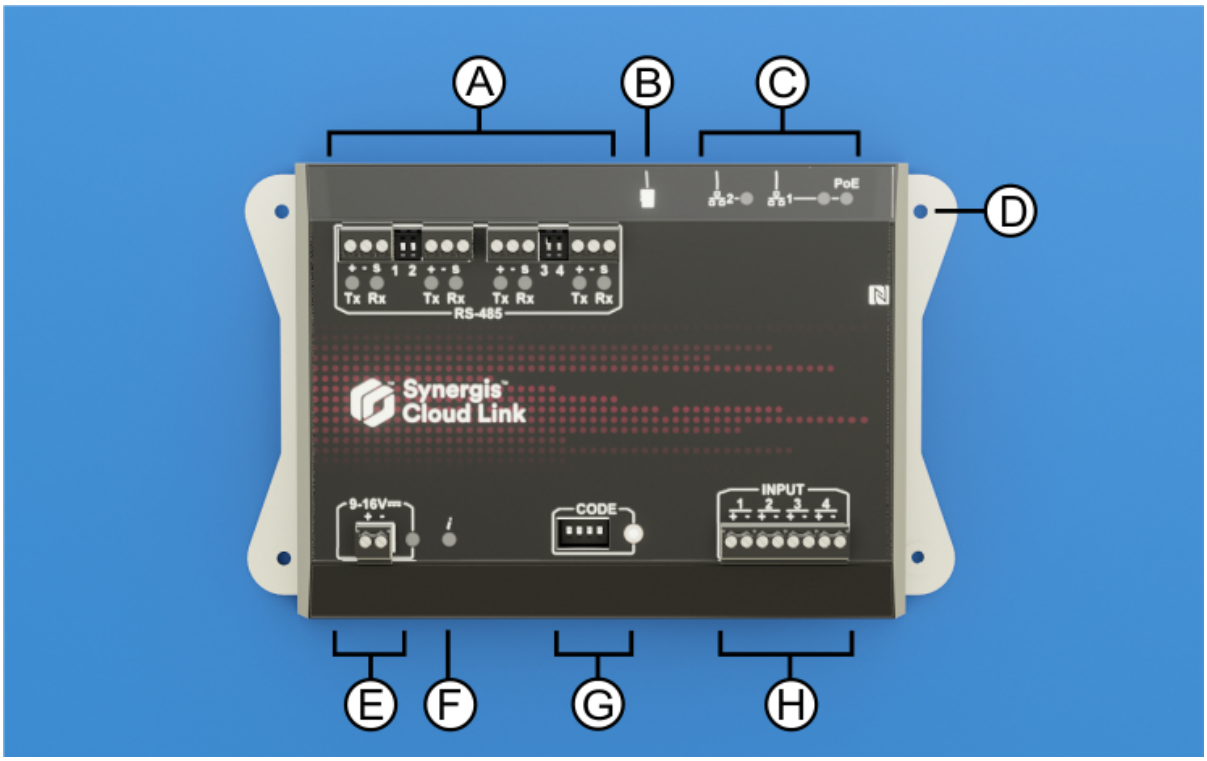
Présentation de Synergis Cloud Link

Cette section aborde les sujets suivants:

Qu’est-ce que la technologie Synergis Cloud Link ?

Synergis[MC] Cloud Link est une passerelle IdO compatible PoE conçue pour répondre à la demande d'une solution de contrôle d'accès non propriétaire.

Synergis Cloud Link fournit une prise en charge native de modules de sécurité non propriétaires populaires, qu'il s'agisse de contrôleurs intelligents Mercury Security, HID Global et Axis Communications ou de verrous électroniques ASSA ABLOY, Allegion ou SimonsVoss, qui nécessitent un contrôleur Mercury.



	Caractéristiques matérielles	Ce que vous devez savoir
A	Ports RS-485	Synergis Cloud Link comprend quatre canaux de communication RS-485. Le nombre de modules que vous pouvez connecter à chaque port RS-485 dépend du type de modules d'interface que vous installez.
B	Carte Micro SD	Utilisation future
C	Ports Ethernet	Deux ports Ethernet sont fournis pour la connexion au réseau IP. **REMARQUE :** Le port Ethernet 1 peut être utilisé pour alimenter l'appareil en utilisant l'alimentation PoE (Power over Ethernet).
D	Trous de fixation	Vous pouvez fixer l'appareil à une surface appropriée à l'aide des trous de fixation ou sur un rail DIN à l'aide du support de fixation pour rail DIN en option.
E	Alimentation	Connectez l'appareil à une alimentation 12 VCC (nominale).
F	LED d'information (*i*)	La LED fournit des informations sur l'état du système.

	Caractéristiques matérielles	Ce que vous devez savoir
G	Commutateurs DIP à code de commande	Les quatre commutateurs DIP à code vous permettent d'exécuter des commandes qui peuvent, par exemple, réinitialiser certaines configurations de l'appareil.
H	Entrées de surveillance	L'appareil comprend quatre entrées que vous pouvez utiliser pour surveiller les événements externes du système de contrôle d'accès.

Rubriques connexes

À propos de Synergis Cloud Link 312, page 6

Exécution des codes de commande du commutateur DIP

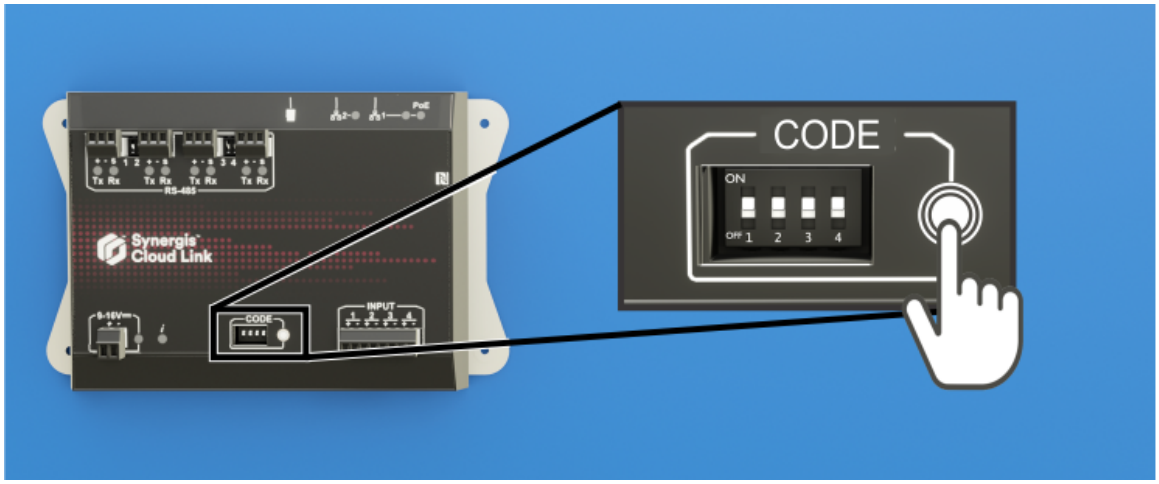
comprend quatre commutateurs DIP à code en façade. Ils vous permettent d'exécuter des codes de commande, afin d'appliquer certaines configurations et de réinitialiser des paramètres.

Procédure

1 Sélectionnez un code de commande à exécuter. Pour en savoir plus, voir Codes de commande des commutateurs DIP , page 5.

2 Entrez le code sur les commutateurs DIP de l'appareil.

3 Appuyez sur le bouton de code de commande pendant 1 seconde.



La LED d'information (*i*) confirme que le code a été reconnu.

Nom de la DEL	Couleur de la DEL	Description
Information (*i*)	Orange : fixe 3 secondes	Code du commutateur DIP reconnu
	Rouge : 3 clignotements	Code du commutateur DIP non reconnu

4 Pour éviter un changement de configuration accidentel, réglez les quatre commutateurs DIP sur ON ON ON ON.

REMARQUE : Aucune action n'est associée à ce code, ce qui en fait un état sûr lorsque la configuration est terminée.

Codes de commande des commutateurs DIP

En activant ou désactivant les quatre commutateurs DIP à code, vous pouvez appliquer une configuration à l'appareil .

Commandes des commutateurs DIP

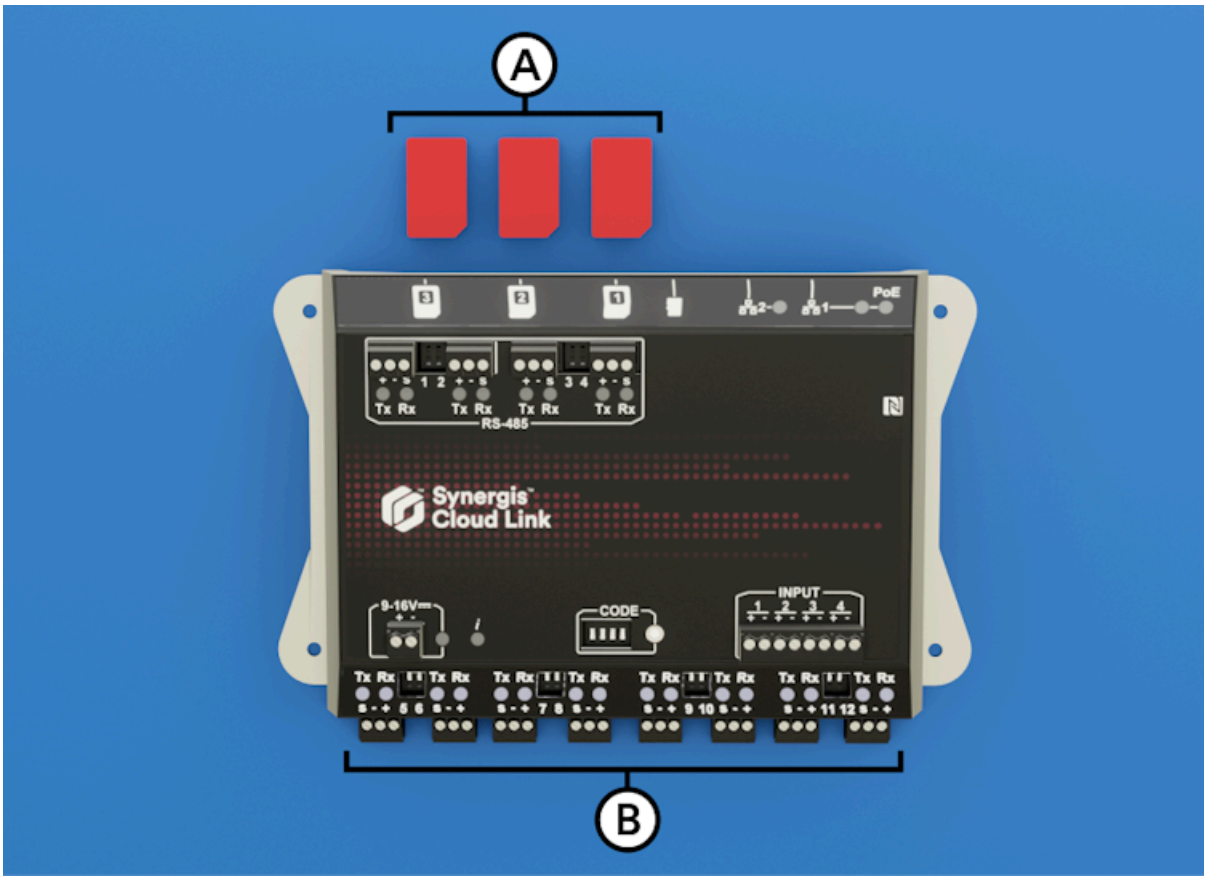
S1	S2	S3	S4	Description de la commande
ON	ON	ON	ON	Aucun code : Après l'exécution d'un code de commande, réglez les commutateurs DIP sur ON ON ON ON pour éviter une modification accidentelle de la configuration.
ON	OFF	OFF	OFF	Réinitialisation partielle aux réglages d'usine. Cette commande a les effets suivants : • Réinitialise le mot de passe de connexion de Synergis[MC] Appliance Portal sur la valeur d'usine (logiciel). • Supprime l'unité du Gestionnaire d'accès SaaS hébergé • Réinitialise le mode d'adressage réseau sur DHCP • Réinitialise le port de découverte sur 2000 • Supprime toutes les configurations matérielles (modules d'interface connectés) • Supprime toutes les configurations de titulaires de cartes (identifiants et règles d'accès) • Réinitialise l'ensemble des réglages de l'unité • Efface toutes les options de journalisation. **REMARQUE :** Le micrologiciel de l'unité n'est pas affecté par cette commande.
ON	OFF	OFF	ON	Réinitialise tous les réglages aux valeurs par défaut et supprime les certificats SSL.
OFF	OFF	ON	OFF	Rétablit la possibilité de modifier les états des sorties depuis la page *Diagnostic d'E/S* du Synergis[MC] Appliance Portal.

Rubriques connexes

Désactiver les contrôles de sorties, page 38

À propos de Synergis Cloud Link 312

Comparé au Synergis[MC] Cloud Link standard, le modèle 312 de l'appareil intègre huit ports RS-485 supplémentaires et trois emplacements de cartes SAM.



Lettre	Caractéristiques matérielles	Ce que vous devez savoir
A	Emplacements de cartes SAM	Vous pouvez utiliser des cartes SAM (Secure Access Module) pour le stockage de clés de chiffrement.
B	RS-485	Le Synergis Cloud Link 312 fournit 8 ports RS-485 supplémentaires au système, pour un total de 12 ports.

REMARQUE : L'appareil Synergis Cloud Link 312 n'a pas été évalué pour la conformité UL/ULC et ne doit pas être utilisé dans les installations qui exigent cette conformité.

Pour en savoir plus sur l'appareil Synergis Cloud Link 312, voir les spécifications sur Synergis Cloud Link 312.

Rubriques connexes

Qu'est-ce que la technologie Synergis Cloud Link ?, page 3

2

Premiers pas avec Synergis Appliance Portal

Cette section aborde les sujets suivants:

Présentation du Synergis Appliance Portal

Synergis[MC] Appliance Portal est l'outil d'administration Web utilisé pour configurer et gérer l'appareil Synergis[MC], et pour mettre à niveau son micrologiciel.

Les tâches suivantes ne peuvent pas être effectuées sur le portail :

- Modifier le mot de passe exigé pour se connecter à l'appareil Synergis[MC] Cloud Link .
- Configurer les paramètres réseau sur l'appareil pour qu'il fonctionne avec votre système.
- Inscrire et configurer les modules d'interface connectés à l'appareil.

  REMARQUE : Les contrôleurs Mercury et Honeywell (PW6K1IC, PRO32IC, PW7K1IC et PRO42IC) doivent être inscrits et configurés sur la page *Périphériques* de l'unité de contrôle d'accès dans Config Tool.
- Configurer le comportement de contrôle d'accès de l'appareil en mode en ligne et hors ligne.
- Tester et diagnostiquer les lecteurs, E/S et connexions des modules d'interface à l'appareil .
- Configurer les réglages spécifiques des contrôleurs Mercury et des contrôleurs en aval.
- Configurer les paramètres de la DEL et du signal sonore du lecteur grâce à la prise en charge de l'exportation et de l'importation de la configuration.
- Configurer MIFARE DESFire sur les lecteurs OSDP et STid.
- Activer la cryptographie basée sur la carte SAM sur l'appareil Synergis Cloud Link 312.
- Gérer les certificats X.509.
- Afficher et exporter l'état et la configuration de l'appareil .
- Afficher les fonctionnalités et l'état des contrôleurs Mercury.
- Mettre à niveau le micrologiciel de l'appareil et du module d'interface.
- Redémarrer le matériel ou le logiciel de l'appareil .

Tâches à effectuer dans Config Tool

Les tâches suivantes ne peuvent pas être effectuées avec le portail. Utilisez plutôt Security Center Config Tool pour les effectuer.

- Affecter des appareils (contacts numériques, lecteurs) aux portes et aux zones.
- Configurer les propriétés individuelles des portes et des zones.
- Configurer les liens E/S.
- Configurer les lecteurs de type *Carte et code PIN* afin qu'une carte et un code PIN soient exigés pour obtenir l'accès.

Pour en savoir plus sur le déploiement de Synergis, voir les chapitres suivants du *Guide de l'administrateur Security Center* :

- Pour configurer les portes et les lecteurs de type *Carte et code PIN*, voir Secteurs, portes et ascenseurs.
- Pour configurer les zones et les liens d'E/S, voir Zones et détection d'intrusions.

Connexion à l'appareil Synergis Cloud Link

Pour configurer votre appareil Synergis[MC] Cloud Link, connectez-vous à l'appareil via le Synergis[MC] Appliance Portal.

Avant de commencer

Les informations suivantes sont nécessaires lors de la première connexion :

- **Nom d'hôte ou adresse IP de l'appareil :** Le nom d'hôte par défaut comprend SCL (pour Synergis Cloud Link), suivi de l'adresse MAC de l'appareil. Par exemple, SCL0010F32CF482. L'adresse MAC se trouve sur l'étiquette de l'appareil.

  Pour obtenir l'adresse IP, effectuez un test ping sur l'appareil. Pour obtenir les adresses IP IPv6, vous devez retirer les deux derniers chiffres de la valeur entre crochets renvoyée par le test ping. L'adresse IPv6 comprend les crochets. Par exemple, [fe80::ebf:15ff:xxxx:xxxx].
- **Nom d'utilisateur et mot de passe par défaut :** Le nom d'utilisateur et le mot de passe par défaut sont *admin* et *softwire*. Vous êtes obligé de changer le mot de passe lors de la première connexion.

À savoir

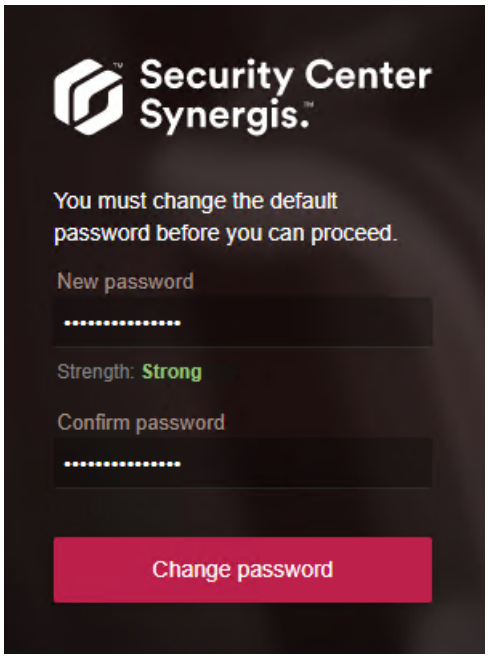
- À compter du micrologiciel Synergis Cloud Link 2.0.3, si vous n'utilisez pas DHCP, vous pouvez vous connecter via une adresse lien-local. Avant la version 2.0.3, IPv6 est requis pour utiliser une adresse lien-local.
- Si vous n'utilisez pas DHCP, les connexions réseau alternatives empêchent le chargement de Synergis Appliance Portal.

Procédure

1. (Première connexion) Reliez le connecteur **LAN 1** de l'appareil à votre réseau local.
2. Ouvrez un navigateur Web et entrez `https://` suivi du nom d'hôte ou de l'adresse IP de l'appareil.
   Exemple : L'adresse suivante utilise le nom d'hôte : `https://SCL0010F32CF482`

   L'adresse suivante utilise le format d'adresse IP IPv6 : `https://[fe80::ebf:15ff:xxxx:xxxx]`
3. Si vous démarrez une nouvelle session avec votre navigateur pour vous connecter à l'appareil, vous recevrez une erreur de certificat. Suivez les instructions du navigateur à l'écran pour vous connecter au site Web.
4. Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.
   Si vous avez déjà modifié le mot de passe par défaut, la page d'accueil est affichée. Si vous n'avez pas encore modifié le mot de passe par défaut, vous devez le changer avant de vous connecter.

5 Entrez un mot de passe *fort* ou *très fort*, confirmez-le, puis cliquez sur **Modifier le mot de passe**.
REMARQUE : Le mot de passe doit comprendre au moins 15 caractères.

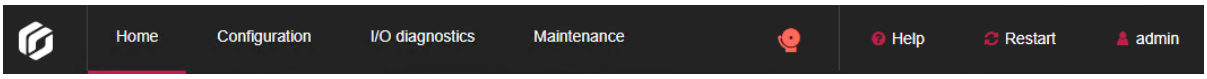


Le mot de passe est mis à jour pour l'utilisateur, et vous devez vous connecter avec le nouveau mot de passe.

Visite guidée de l'interface de Synergis Appliance Portal

La page d'accueil de Synergis[MC] Appliance Portal est divisée en une barre de menu en haut et une zone d'accès rapide avec icônes permettant d'accéder à des tâches fréquemment utilisées. La page d'accueil est dynamique et les icônes affichées dépendent du contexte.

Le menu principal est composé des éléments suivants :



- **Accueil :** Revenir à la page d'accueil.
- **Configuration :** Ouvrir la page *Matériel*, vous permettant de configurer les modules d'interface associés à l'unité Synergis[MC] Cloud Link . Les sous-pages suivantes sont accessibles depuis la page *Configuration* :
  - *Paramètres de l'unité*
  - *Journalisation Synergis Softwire*
  - *Réseau*
  - *Utilisateurs*
  - *Réglages de contrôleur Mercury*
  - *Procédures et déclencheurs Mercury*
  - *Réglages du témoin LED et de l'avertisseur sonore*
  - *Paramètres de contrôleurs Synergis IX*
  - *Moteur d'automatisation*
  - *Réglages de contrôleurs en aval*
  - *Magasin de clés Synergis*
  - *MIFARE DESFire*
  - *OSDP avancé*
  - *Certificats*
  - *Carte SAM* (pour unité Synergis Cloud Link 312 uniquement)
  - *Connexion au nuage* (pour les unités avec Cloud Agent)
- **Diagnotic d'E/S :** Ouvrir la page *Canaux* où vous pouvez surveiller le changement d'état des contacts, et les identifiants lus par les lecteurs lorsque vous les déclenchez. Les sous-pages suivantes sont accessibles depuis la page *Diagnostic d'E/S* :
  - *Appareils*
  - *Canaux*
  - *Interfaces*
  - *Portes*
  - *Ascenseur*
  - *Zones matérielles*
  - *Zones d'E/S*
- **Maintenance :** Ouvrir la page *État du système* où vous pouvez afficher un instantané de l'état de l'unité et du réseau. Vous pouvez également télécharger les fichiers de configuration à partir de cette page. Les sous-pages suivantes sont accessibles depuis la page *Maintenance* :

  - *Rapport de capacité*
  - *Visionneur de journaux*
  - *Télécharger les journaux de diagnostic*
  - *Diagnostic de ping*
  - *Capture réseau* (utilisé par l'assistance technique Genetec)
  - *Mise à niveau de l'interface*
  - *Mise à jour du micrologiciel*
  - *Stockage*
  - *Peer-to-peer*
  - *Télécharger la sauvegarde Synergis IX*
- **Notifications :** Affiche les alertes de dysfonctionnement du système.
- **Aide :** Ouvre un menu déroulant contenant deux éléments :
  - *Aide* ouvre le *Guide de l'administrateur Synergis^{MC} Cloud Link* dans une fenêtre de navigateur distincte.
  - *À propos* affiche la version du micrologiciel de l'appareil Synergis Cloud Link et les informations de copyright.
- **Redémarrer :** Ouvre un menu déroulant dans lequel vous faites votre choix entre **Redémarrer le logiciel** ou **Redémarrer le système** pour redémarrer le matériel ou le logiciel d'une unité Synergis Cloud Link.
- **Administrateur :** Ouvre un menu déroulant dans lequel vous pouvez mettre l'unité hors tension ou sélectionner *Configuration des utilisateurs*, pour modifier la langue de l'interface du portail.

Partie II

Configuration générale

Cette section comprend les chapitres suivants:

3

Configuration de Synergis Cloud Link

Cette section aborde les sujets suivants:

Préparer la configuration de l’unité Synergis Cloud Link

Avant de configurer une unité Synergis[MC] Cloud Link , vous devez effectuer certaines tâches préalables.

- Lisez les *Notes de version Synergis[MC] Cloud Link* pour prendre connaissance d'éventuels problèmes connus et d'autres informations.
- Munissez-vous d'un ordinateur équipé d'une carte réseau, d'un câble Ethernet et d'un navigateur web.
- (Facultatif) Demandez à votre service informatique d'affecter une adresse IP à votre unité Synergis Cloud Link .
- Réglez les paramètres matériels (commutateurs DIP, molettes d’adresse, et ainsi de suite) à leur position définitive sur les modules d’interface.
- Connectez les modules d'interface à l'unité Synergis Cloud Link en utilisant les canaux de communication adaptés.

  REMARQUE : Chaque fabricant de matériel utilise un protocole de communication distinct, ce qui signifie que tous les modules d’interface connectés à un même canal RS-485 doivent provenir du même fabricant.
- Connectez les appareils physiques (REX, capteurs de porte, et ainsi de suite), ou utilisez des LED et des commutateurs de test durant la phase de configuration.

  Pour en savoir plus, voir le *Guide d’installation du matériel Synergis[MC] Cloud Link*.
- Téléchargez le dernier pack Synergis Cloud Link sur la page *Téléchargement de produits* de GTAP.
- Installez et configurez Security Center avec au moins un rôle Access Manager.

  Pour en savoir plus sur le déploiement de Synergis[MC], voir le *Guide de l'administrateur Security Center*.

Lorsque vous avez terminé

Configurez votre unité Synergis Cloud Link .

Configuration de l'unité Synergis Cloud Link

Vous pouvez configurer l'unité Synergis[MC] Cloud Link une fois les tâches de configuration préalable effectuées.

Avant de commencer

Effectuez les tâches de configuration préalables.

Procédure

1. Toutes les unités Synergis Cloud Link sont livrées avec un nom d'hôte attribué en usine. Si votre réseau ne prend pas en charge le DHCP, vous devez affecter une nouvelle adresse IP à l'appareil.
2. (Facultatif) Changez le certificat X.509 par défaut de l'unité.
3. Installez la dernière version du micrologiciel de l'appareil Synergis[MC].
4. Connectez physiquement les modules d'interface à l'unité Synergis Cloud Link.
   Pour en savoir plus, voir le *Guide d'installation du matériel Synergis[MC] Cloud Link* sur TechDoc Hub.
5. Établissez la communication entre l'unité Synergis Cloud Link et ses modules d'interface connectés via le Synergis[MC] Appliance Portal.
6. Testez les connexions matérielles et la configuration et apportez toute modification nécessaire.
7. Configurez le comportement de contrôle d'accès de l'unité Synergis Cloud Link.
8. Ajoutez l'unité Synergis Cloud Link à un rôle Gestionnaire d'accès afin de l'intégrer à votre système Security Center.

Configuration des propriétés réseau

Pour que votre unité Synergis[MC] Cloud Link soit accessible sur le réseau de votre système Security Center, vous devez configurer les propriétés réseau de l'unité.

À savoir

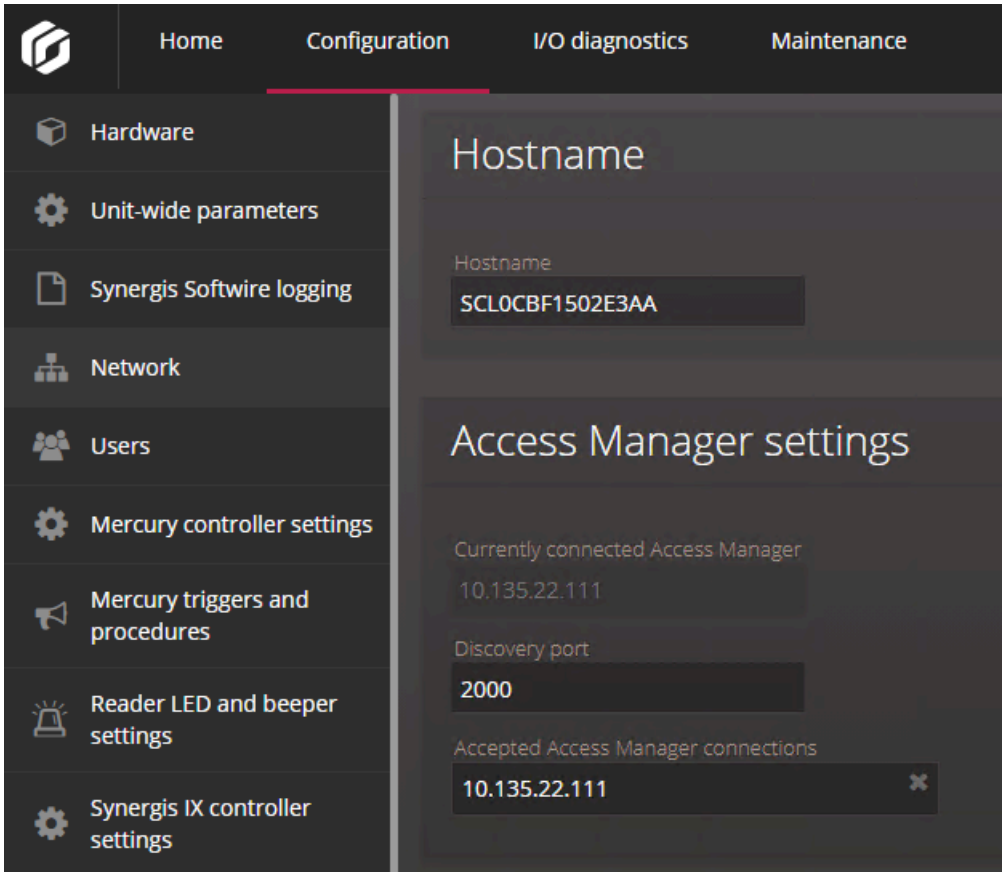
L'unité Synergis Cloud Link est livrée avec un nom d'hôte attribué en usine. Si votre réseau ne prend pas en charge le DHCP, vous devez affecter une nouvelle adresse IP à l'unité.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Réseau**.

3 (Facultatif) Dans la section *Nom d'hôte*, modifiez le **Nom d'hôte** si nécessaire.



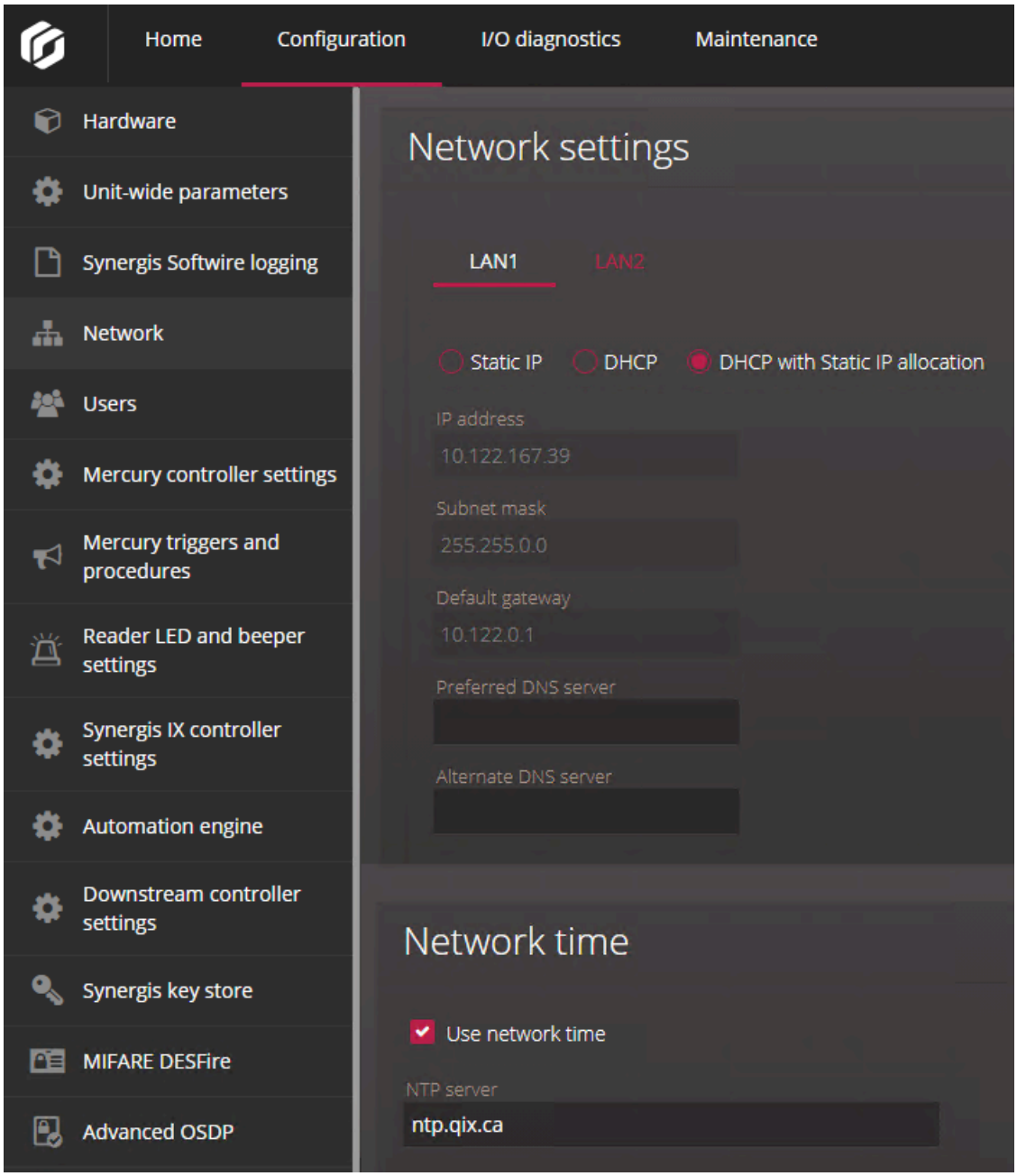
BONNE PRATIQUE : Les noms d'hôtes doivent être uniques sur un réseau, et le nom d'hôte par défaut est garanti unique. Nous vous recommandons donc de conserver le nom d'hôte par défaut, qui se trouve sur l'étiquette de l'appareil.

4 Dans la section *Réglages du Gestionnaire d'accès*, modifiez le cas échéant le **Port de découverte**.

5 Dans la section *Paramètres réseau*, sélectionnez la carte réseau **LAN1** ou **LAN2** pour connecter l'unité Synergis Cloud Link à son Gestionnaire d'accès, puis configurez l'adresse IP et les propriétés réseau de l'unité Synergis Cloud Link.

IMPORTANT : Pour éviter les problèmes de réseau, des règles strictes doivent être suivies lors de la configuration des propriétés réseau de l'unité :

- Si l'unité ne se trouve pas sur le même segment de réseau que le Gestionnaire d'accès, alors l'adresse IP de l'unité doit être définie sur **IP statique** ou **DHCP avec affectation d'IP statique**.
- **LAN1** et **LAN2** ne doivent pas se trouver sur le même sous-réseau. Si c'est le cas, seul l'un d'entre eux doit être configuré avec une passerelle par défaut.



6 Dans la section *Temps réseau*, configurez le serveur NTP (Network Time Protocol) s'il en existe un.

a) Cliquez sur **Utiliser l'heure du réseau** et entrez le nom du **serveur NTP**.

BONNE PRATIQUE : Un serveur NTP offre une plus grande précision temporelle que le protocole intégré qui synchronise les unités Synergis Cloud Link avec leur gestionnaire d'accès. Par conséquent, utilisez l'heure du réseau lorsqu'un serveur NTP est disponible sur votre réseau. Tous les serveurs et postes de

travail Security Center doivent être synchronisés sur le même serveur NTP que vos appareils Synergis Cloud Link.

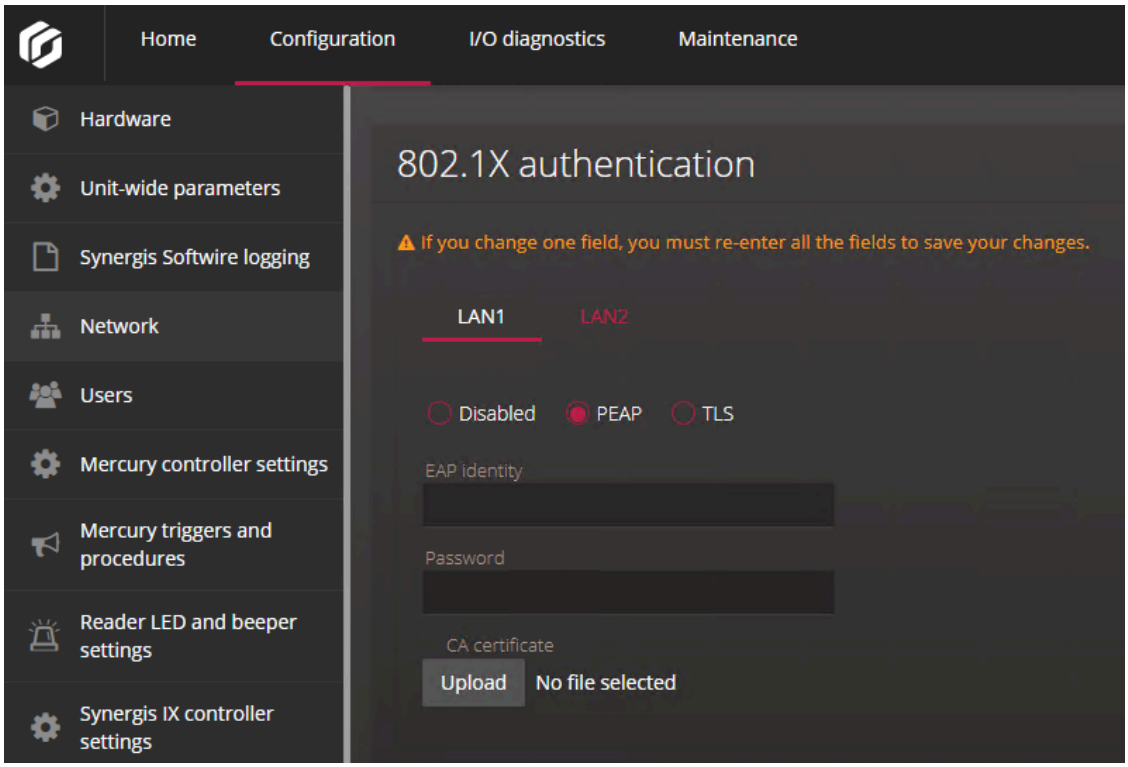
7 Dans la section *Authentification 802.1X* section, sélectionnez le réseau local que vous souhaitez utiliser pour l'authentification 802.1X et sélectionnez le mode d'authentification.

REMARQUE : Si vous avez déjà configuré ces paramètres par le passé, leurs valeurs actuelles sont affichées. Si vous devez modifier une valeur, vous devez saisir à nouveau toutes les valeurs. Dans le cas contraire, les modifications apportées ne seront pas enregistrées.

- **Désactivé :** L'authentification 802.1X est désactivée par défaut.
- **PEAP :** Utilisez le protocole PEAP (Protected Extensible Authentication Protocol).

  Saisissez l'**identité EAP** (nom d'utilisateur) et le **mot de passe**, puis chargez le **certificat du CA**.

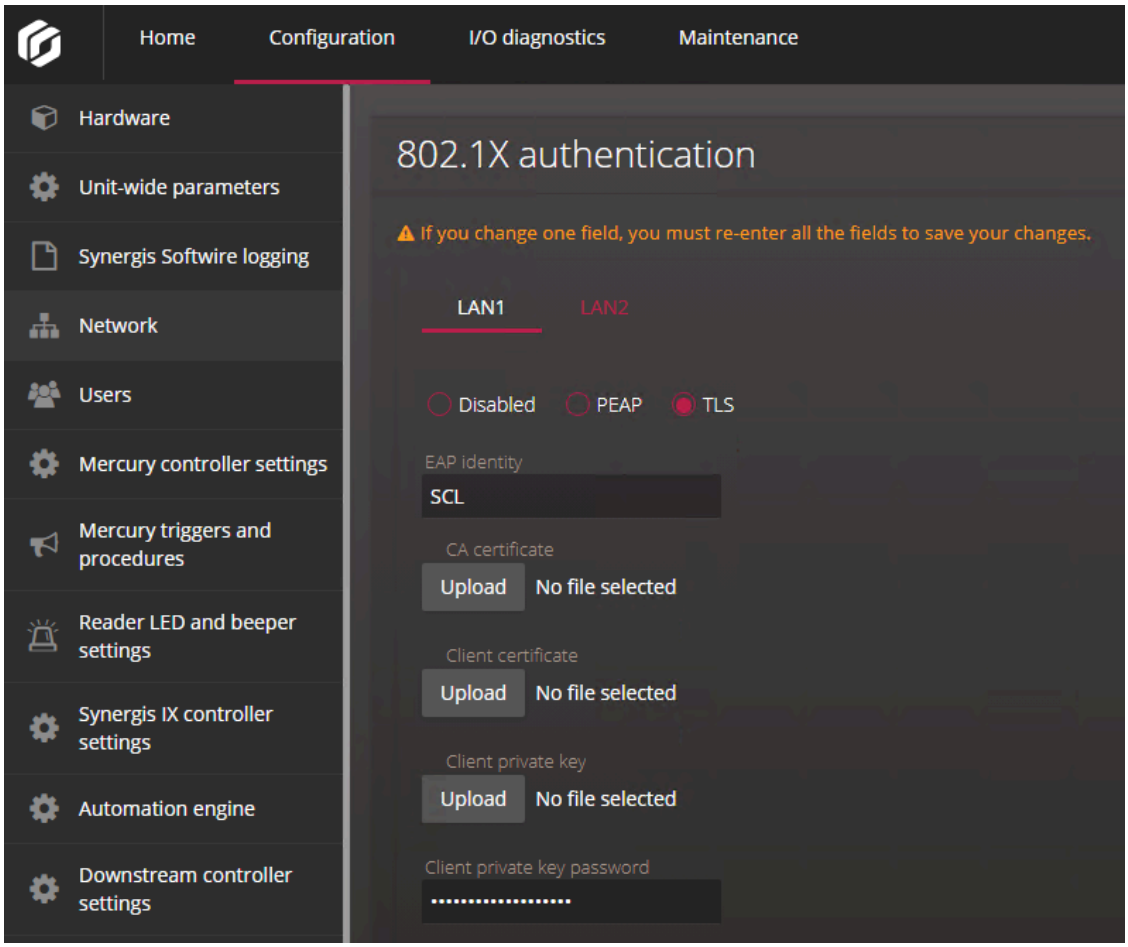
  REMARQUE : Le certificat CA doit être un fichier PEM ou DER.



- **TLS :** Utilisez le protocole TLS (Transport Layer Security).

Saisissez l'**identité EAP** (nom d'utilisateur), chargez le **certificat de CA**, le **certificat client** et la **clé privée du client**, puis saisissez le **mot de passe de la clé privée du client**.

REMARQUE : Le certificat CA doit être un fichier PEM ou DER.



8 Cliquez sur **Enregistrer**.

L'unité Synergis Cloud Link redémarre, et vous êtes automatiquement redirigé vers la nouvelle adresse IP de l'unité.

Si vous avez activé l'heure réseau, l'unité se synchronise avec le serveur NTP 45 secondes après l'activation du paramètre, puis toutes les 15 minutes.

Rubriques connexes

Exécution des codes de commande du commutateur DIP, page 4

Utilisation de certificats auto-signés

Un Synergis[MC] Cloud Link est livré avec un certificat X.509 généré en usine. Remplacez le certificat par défaut pour augmenter la sécurité en générant un nouveau certificat auto-signé.

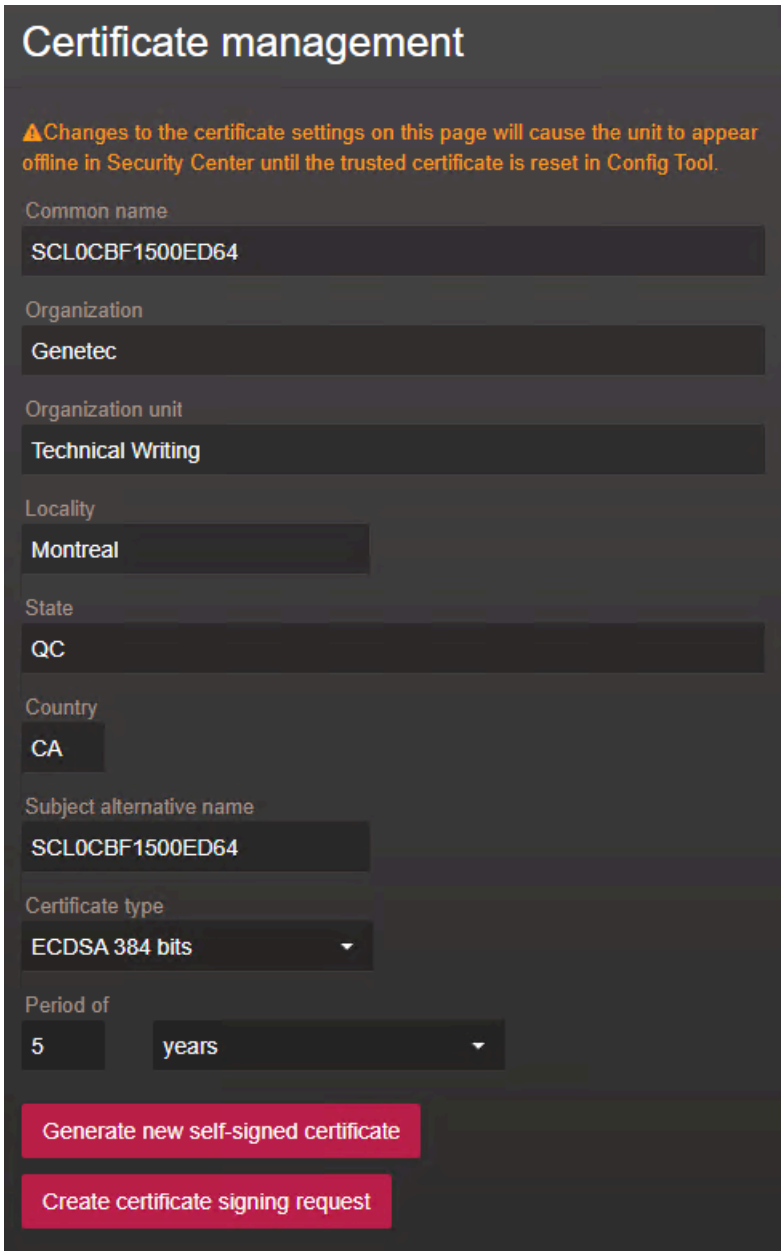
Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Certificats**.

3 Dans la section *Gestion des certificats*, renseignez les champs d'identification.

REMARQUE : Les champs **Nom commun**, **Autre nom de l'objet** et **Pays** sont obligatoires.



4 Dans la liste **Type de certificat**, sélectionnez l'une des combinaisons d'algorithme et de longueur de clé suivantes :
   - ECDSA 256 bits
   - ECDSA 384 bits
   - RSA 2048 bits
   - RSA 3072 bits
   - RSA 4096 bits

5 Cliquez sur **Générer un nouveau certificat auto-signé**, puis relancez votre navigateur et reconnectez-vous à l'unité.

   Le certificat est désormais généré sur l'unité .

6 Installez le certificat dans le magasin de certificats du navigateur.
   a) Cliquez sur **Configuration** > **Certificats**.
   b) Dans la section *Certificats actuels*, cliquez sur **Télécharger**.
   c) Dans Windows, suivez les instructions dans l'*Assistant Importation du certificat* pour importer le certificat dans le dossier *Autorités de certification racines de confiance* à l'aide de l'option **Ordinateur local**.

      Installez le certificat sur tous les postes qui doivent se connecter à l'unité Synergis Cloud Link mise à jour.

      REMARQUE : Le fichier de certificat est nommé avec le nom d'hôte et un suffixe *.cer*.

7 Relancez votre navigateur et reconnectez-vous à l'unité.

Votre unité n'affichera plus d'erreur de sécurité dans la barre d'adresses lors de la connexion avec le nom d'hôte.

Lorsque vous avez terminé

Si l'unité a déjà été inscrite dans Security Center, le Gestionnaire d'accès n'approuve pas le nouveau certificat ou ne se connecte pas à l'unité, et vous devez alors réinitialiser le certificat approuvé dans Config Tool.

Pour en savoir plus, voir Réinitialiser le certificat de confiance .

Utilisation de certificats approuvés

L’authenticité du certificat auto-signé fourni avec l’unité par défaut ne peut pas être vérifiée par la méthode habituelle en exploitant l’infrastructure à clés publiques. Pour renforcer la sécurité, vous pouvez utiliser à la place un certificat signé par une autorité de certification.

À savoir

L'utilisation de certificats signés par une autorité de certification est plus adaptée pour les configurations où plusieurs ordinateurs et navigateurs accèdent à l'unité Synergis[MC] Cloud Link car vous n'avez pas besoin de configurer chaque navigateur pour reconnaître ces certificats approuvés.

Procédure

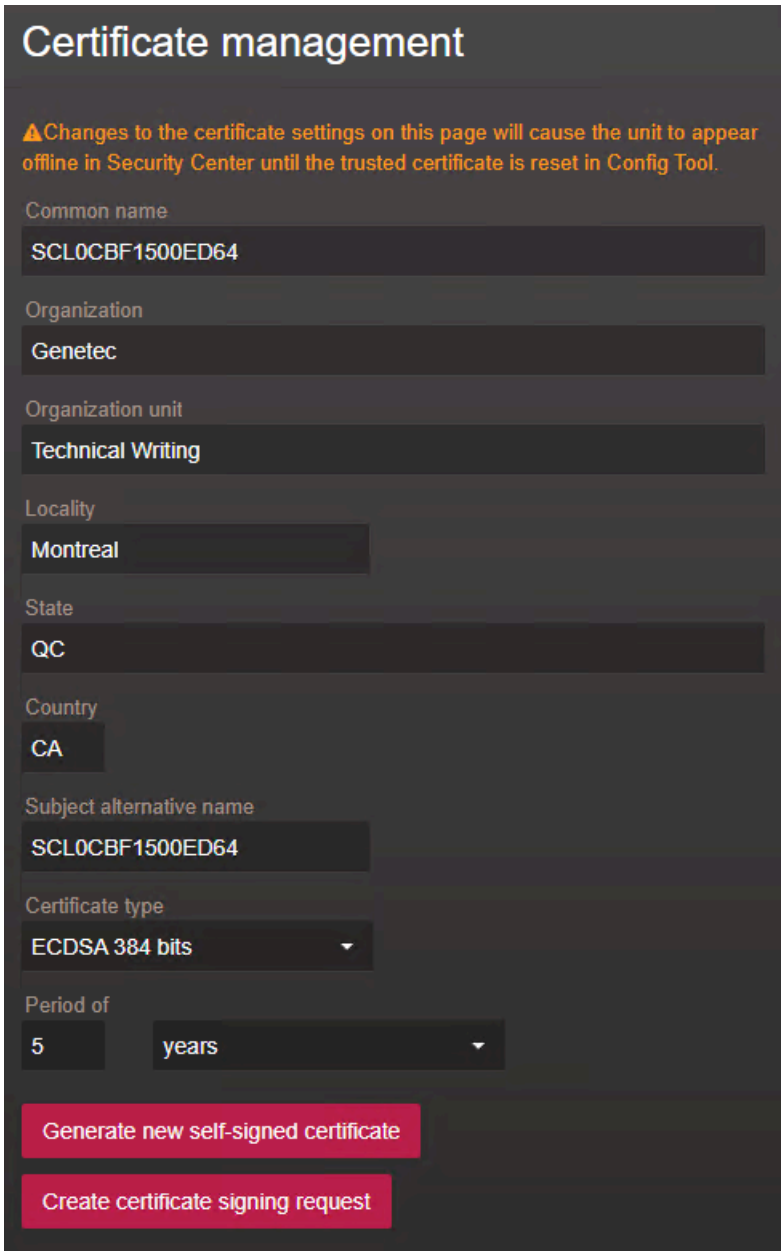
1 Connectez-vous à l’unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Certificats**.

3 Dans la section *Gestion des certificats*, renseignez les champs d'identification.

Le champ **Nom commun** contient le nom d'hôte par défaut de l'unité. Le champ **Autre nom de l'objet** contient également le nom d'hôte par défaut, mais il peut contenir une liste d'entrées DNS séparées par des virgules.

REMARQUE : Les champs **Nom commun**, **Autre nom de l'objet** et **Pays** sont obligatoires.



4 Dans la liste **Type de certificat**, sélectionnez l'une des combinaisons d'algorithme et de longueur de clé suivantes :

- ECDSA 256 bits
- ECDSA 384 bits
- RSA 2048 bits
- RSA 3072 bits
- RSA 4096 bits

5 Cliquez sur **Créer une demande de signature de certificat**.

Un fichier *.req* est généré, contenant la partie publique du certificat. Le fichier ne contient pas la clé privée et n'est donc pas confidentiel.

6 Dans l'Explorateur Windows, naviguez jusqu'à votre dossier Téléchargements, puis copiez le fichier *.req* de demande de signature et envoyez-le à une autorité de certification.

Après vérification, l'autorité de certification signe la partie publique du certificat avec sa propre clé privée.

7 Lorsque vous avec reçu les certificats de l'autorité de certification, importez le certificat signé.

a) Reconnectez-vous à l'unité, et cliquez sur **Configuration** > **Certificats**.

b) Dans la section *Importer un certificat signé*, cliquez sur **Sélectionner le certificat** et naviguez jusqu'au dossier qui contient les certificats.

c) Sélectionnez le premier certificat, puis cliquez sur **Transférer**. Répétez pour les autres certificats.

REMARQUE : Chaque certificat de la chaîne de certificats doit être transféré individuellement, ou en une fois si vous avez reçu un fichier de collection *.p7b*. Si vous avez reçu un fichier de collection, vous n'avez pas besoin de transférer le certificat racine.

Votre unité n'affichera plus d'erreur de sécurité dans la barre d'adresses lors de la connexion avec le nom d'hôte.

Lorsque vous avez terminé

Si l'unité a déjà été inscrite dans Security Center, le Gestionnaire d'accès n'approuve pas le nouveau certificat ou ne se connecte pas à l'unité, et vous devez alors réinitialiser le certificat approuvé dans Config Tool.

Pour en savoir plus, voir Réinitialiser le certificat de confiance .

Configurer les modules d’interface connectés à l'unité Synergis Cloud Link

Pour établir la communication entre l'unité Synergis[MC] Cloud Link et les modules d'interface connectés, vous devez les configurer sur le Synergis[MC] Appliance Portal .

Avant de commencer

Connectez physiquement les modules d'interface à l’unité Synergis Cloud Link .

À savoir

Un module d'interface est un périphérique de sécurité tiers qui communique avec une unité de contrôle d'accès via une connexion IP ou RS-485, et qui fournit des connexions d'entrée, de sortie et de lecteur supplémentaires à l'unité.

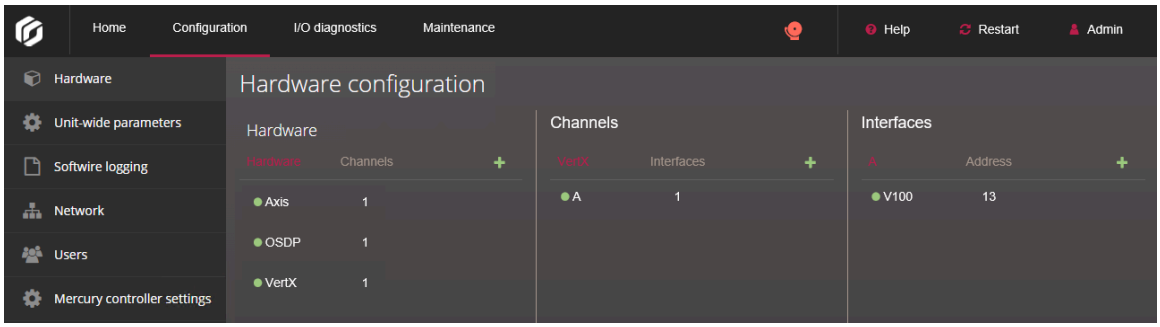
REMARQUE : Les contrôleurs Mercury LP et MP et Honeywell (PW6K1IC, PRO32IC, PW7K1IC et PRO42IC) doivent être inscrits et configurés sur la page *Périphériques* de l'unité de contrôle d'accès dans Security Center Config Tool.

Procédure

1 Connectez-vous à l’unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

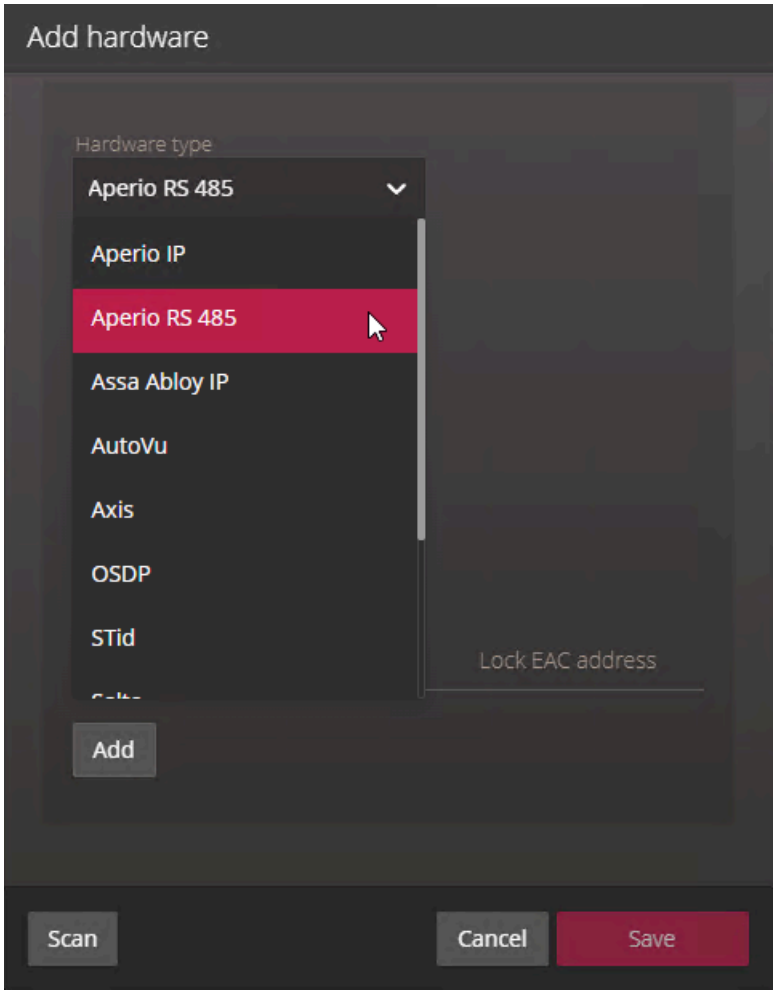
Le portail présente l’arborescence matérielle en trois colonnes. Les informations affichées dans chaque colonne variant en fonction de la sélection dans la colonne précédente :



- **Matériel :** Les fabricants de matériel configurés et le nombre de canaux utilisés. Cliquez sur un fabricant de matériel pour afficher ses canaux dans la deuxième colonne.
- **Canaux :** Les canaux utilisés par le fabricant sélectionné dans la première colonne. Survolez un canal pour afficher les options ( ), cloner ( ) et supprimer ( ).
- **Interfaces :** Les modules d’interface connectés au canal sélectionné dans la deuxième colonne.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** ( ).

4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez le **Type de matériel**, le **Canal** et les autres propriétés du module d'interface, qui varient en fonction du type de matériel sélectionné.



5 Dans la même boîte de dialogue, ajoutez tous les modules d'interface connectés au même canal :

- Pour ajouter les modules d'interface manuellement, cliquez sur **Ajouter**.
- Pour découvrir les modules d'interface, cliquez sur **Analyser**.

  Les modules d'interface d'un même fabricant connectés à un même canal doivent utiliser le même débit en bauds, et être configurés avec des adresses physiques distinctes pour être ajoutés à la liste.

6 Cliquez sur **Enregistrer**.

Le type de matériel, le canal et les modules d'interface que vous venez d'ajouter apparaissent dans l'arborescence matérielle.

7 Sélectionnez chaque module d'interface dans l'arborescence matérielle, cliquez sur , puis configurez ses réglages dans la fenêtre qui s'affiche.

Pour une description des réglages, consultez la documentation du fabricant.

8 Au bas de la page, cliquez sur **Save** (Enregistrer).

Lorsque vous avez terminé

Testez les modules d'interface.

Modifier les réglages par défaut des modules d'interface

Pour simplifier le processus de configuration lorsque vous avez plusieurs modules d'interface d'un même type à configurer, vous pouvez modifier les réglages d'usine et les enregistrer en tant que nouvelles valeurs par défaut pour chaque type de module.

À savoir

L'unité Synergis[MC] Cloud Link est configurée en usine avec des réglages par défaut pour tous les modules d'interface pris en charge.

Procédure

1 Cliquez sur **Configuration** > **Matériel**.

2 À partir de la page *Configuration matérielle*, sélectionnez le fabricant, le canal et l'interface que vous voulez utiliser comme modèle.

3 Dans la boîte de dialogue *Modifier*, apportez les modifications nécessaires aux réglages.

4 Cliquez sur **Définir comme valeur par défaut** et enregistrez.

Vos modifications sont enregistrées comme nouveaux paramètres par défaut. À l'ajout suivant d'un module d'interface du même type, vos nouvelles valeurs par défaut seront utilisées pour initialiser la page *Propriétés*.

Effacer les réglages par défaut personnalisés des modules d'interface

Si vous avez créé des réglages par défaut personnalisés pour les modules d'interface et que vous souhaitez revenir aux réglages d'usine pour l'ajout de modules d'interface, vous pouvez effacer les réglages par défaut personnalisés.

À savoir

IMPORTANT : Ne confondez pas le bouton **Supprimer les réglages par défaut** avec le bouton **Rétablir les valeurs d'usine**.

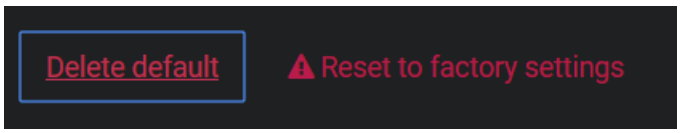
- Le bouton **Supprimer les réglages par défaut** ne fait qu'interrompre l'utilisation de vos réglages par défaut personnalisés, afin que les réglages d'usine soient utilisés lors de l'ajout suivant d'un module d'interface de même type.
- Le bouton **Rétablir les valeurs d'usine** réinitialise les valeurs de la page actuelle sur leurs réglages d'usine lorsque vous enregistrez.

Procédure

1 Cliquez sur **Configuration** > **Matériel**.

2 Sur la page *Matériel*, sélectionnez le module d'interface qui sert de modèle.

3 Dans la boîte de dialogue *Modifier*, cliquez sur **Supprimer les réglages par défaut**.



Cloner les réglages de modules d’interface

Pour gagner du temps lors de la configuration, vous pouvez ajouter des modules d’interface en dupliquant les réglages d’un module existant, puis en modifiant les copies en cas de besoin.

Avant de commencer

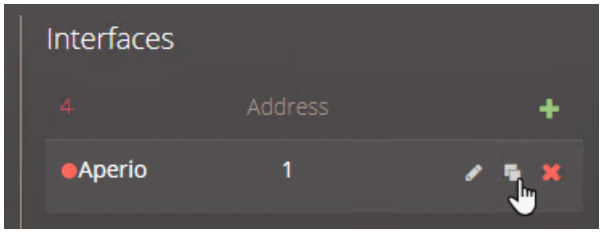
Si vous souhaitez cloner vos modules d’interface, mais que vous en avez déjà créé de nouveaux, supprimez les nouveaux modules.

Procédure

1 Cliquez sur **Configuration** > **Matériel**.

2 Dans la section *Configuration matérielle*, sélectionnez le module d’interface que vous souhaitez cloner dans l’arborescence matérielle.

3 Cliquez sur .



4 Dans la boîte de dialogue *Cloner le matériel*, ajoutez tous les modules d’interface souhaités basés sur le même modèle, puis cliquez sur **Enregistrer**.

Il vous suffit de spécifier l’adresse physique de chaque nouveau module d’interface ainsi que le canal auquel il est connecté. Tous les autres réglages sont copiés depuis le module d’interface modèle.

Lorsque vous avez terminé

Modifiez les réglages des modules d’interface clonés.

Tester les modules d’interface connectés

Vous pouvez tester les connexions matérielles et votre configuration en surveillant les réponses en temps réel sur la page *Diagnotic d'E/S* du Synergis[MC] Appliance Portal .

Avant de commencer

Configurez les modules d’interface.

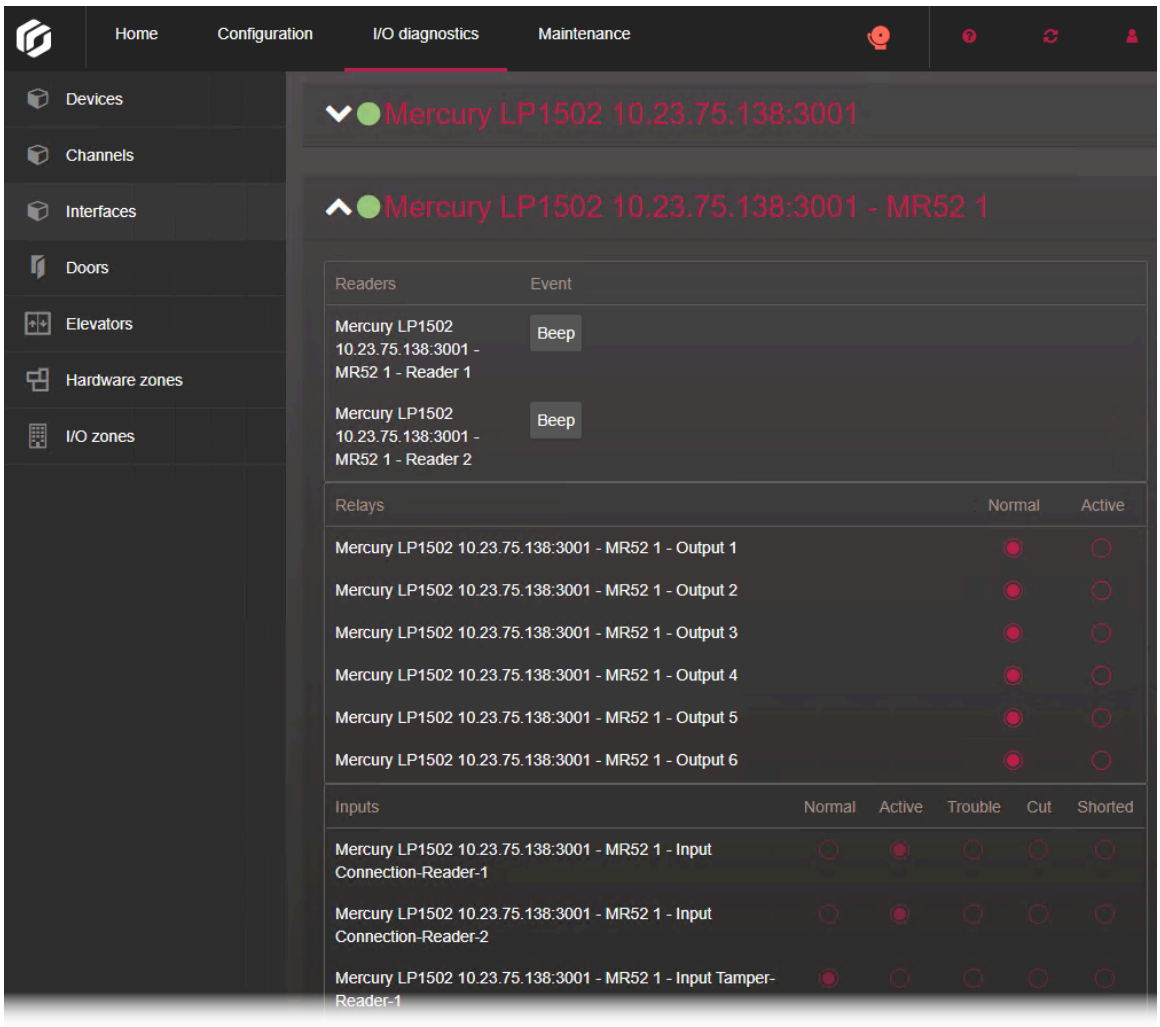
À savoir

Vous pouvez personnaliser la page pour afficher les éléments que vous souhaitez surveiller.

Procédure

1 Connectez-vous à l’unité Synergis Cloud Link.

2 Cliquez sur **Diagnostics d’E/S** > **Interfaces**.



3 Cliquez sur pour développer l’interface que vous voulez surveiller.

4 Activez les périphériques (lecteurs de cartes, capteurs de porte, verrous de porte, et ainsi de suite) connectés à l'unité Synergis Cloud Link par le biais des modules d'interface.

S’ils ne se comportent pas comme prévu, vérifiez les connexions et la configuration du module d’interface.

Configuration des paramètres de l'unité

Tous les modules d'interface connectés à une même unité Synergis[MC] Cloud Link ont généralement les mêmes comportements. Vous pouvez configurer ces paramètres sur la page *Paramètres de l'unité* du Synergis[MC] Appliance Portal.

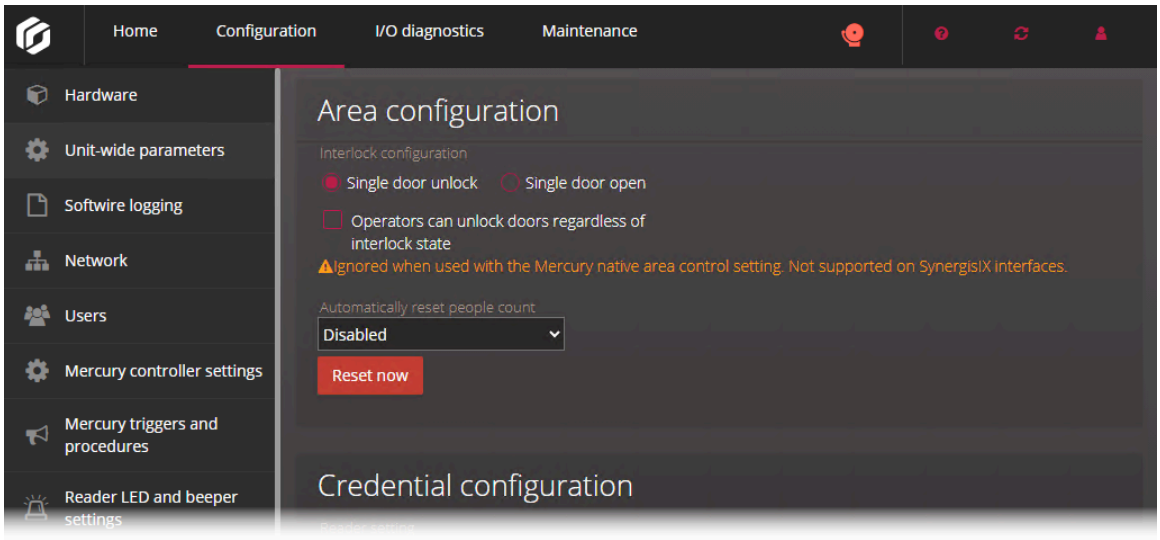
À savoir

La procédure suivante décrit toutes les options de la page *Paramètres de l'unité*. Configurez-les en fonction des besoins de votre système.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Paramètres de l'unité**.



3 Dans la section *Configuration de secteur*, configurez les options suivantes :

- **Configuration de sas :** Un sas est un système composé de plusieurs portes, et pour lequel une seule porte peut être ouverte à un instant donné. Vous avez deux options :
  - **Déverrouillage de porte unique :** Ne déverrouiller qu'une seule porte à la fois.
  - **Ouverture de porte unique :** Dès qu'une porte est ouverte, verrouiller toutes les autres.
  - **Les opérateurs peuvent déverrouiller les portes quel que soit l'état du sas :** Permet de déverrouiller les portes manuellement à l'aide du bouton **Déverrouiller** du widget *Porte*, y compris si la porte fait partie d'un sas. Vous pouvez utiliser ce réglage avec les réglages de sas **Déverrouillage de porte unique** et **Ouverture de porte unique**.
    Ce paramètre doit être configuré pour chaque unité Synergis Cloud Link qui contrôle des portes configurées dans un sas, et la modification de ce paramètre nécessite un redémarrage du logiciel.

REMARQUE : Ce paramètre n'est pas supporté avec les intégrations de Synergis^{MC} IX et il est ignoré lorsqu'il est utilisé avec l'une des fonctionnalités natives Mercury suivantes :
- Antiretour
- Capacité maximale
- Sas

- **Réinitialiser automatiquement le nombre d'individus :** Réinitialiser le nombre d'individus quotidiennement ou hebdomadairement. Désactivé par défaut.

4 Dans la section *Configuration d'identifiants*, configurez les options suivantes :
- **Réglages du lecteur :** Ne s'applique qu'aux lecteurs de type Carte et code PIN. Vous avez deux options :
  - **Carte ou code PIN :** La carte ou le code PIN peuvent servir à obtenir l'accès.
  - **Carte seule :** Seule la carte sert à accorder l'accès.

  REMARQUE : Pour appliquer le mode *Carte et code PIN* qui nécessite l'utilisation d'une carte et la saisie d'un code PIN pour obtenir l'accès, vous devez configurer les paramètres du lecteur dans Config Tool. Le mode *Carte et code PIN* fonctionne uniquement pendant les horaires du lecteur. En dehors de ces horaires, le lecteur fonctionne soit en mode *Carte uniquement*, soit en mode *Carte ou code PIN*, selon le réglage du lecteur effectué dans le Synergis Appliance Portal .
- **Longueur maximale du code PIN :** S'applique aux modules d'interface qui prennent en charge les lecteurs en mode-00. L'unité Synergis Cloud Link traite le code PIN en cours de saisie dès qu'il atteint le nombre de chiffres maximal, sans attendre la saisie de la touche '#'.

  REMARQUE : Certaines intégrations ne prennent pas en charge cette fonctionnalité. Pour en savoir plus, voir le *Guide d'intégration de Synergis^{MC} Softwire*.

5 Dans la section *Contrôles de sorties*, configurez l'option suivante :
- **Désactiver les contrôles de sorties :** Cliquez pour désactiver la possibilité de modifier l'état des sorties depuis la page *Diagnostic d'E/S* du portail de l'appareil Synergis.

6 Dans la section d'inscription au *Security Center SaaS*, configurez l'option suivante :
- **Communiquer avec le nuage pour l'inscription :** Assurez-vous que cette option est sélectionnée avant d'inscrire votre unité Synergis dans le Security Center SaaS. Une fois que votre unité est inscrite, l'option est automatiquement supprimée.

7 Cliquez sur **Enregistrer**.

Les modifications sont appliquées après un redémarrage logiciel.

Rubriques connexes

Codes de commande des commutateurs DIP, page 5
Versionnement des clés pour les cartes SAM, page 48
Désactiver les contrôles de sorties, page 38

Configuration des paramètres des LED et du signal sonore du lecteur

Vous pouvez configurer le comportement des DEL et du signal sonore du lecteur pour communiquer différents états de contrôle d'accès à la personne se trouvant devant une porte. Par exemple, vous pouvez faire en sorte que la DEL clignote en couleur ambre lorsque le système attend la saisie d'un code PIN.

Avant de commencer

Pour l'instant, cette fonctionnalité n'est prise en charge que pour les lecteurs contrôlés par Mercury.

À savoir

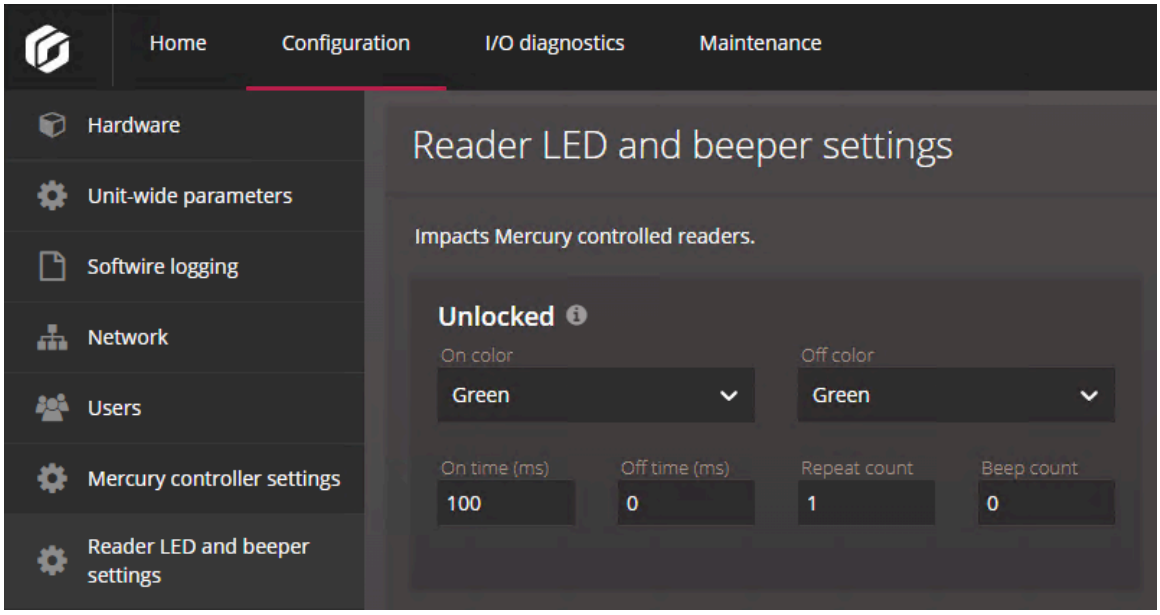
Vous pouvez indiquer par un comportement unique de la DEL du lecteur et du signal sonore les états de contrôle d'accès suivants :

- **Déverrouillé :** La porte est déverrouillée pour maintenance, sur horaire ou temporairement sur contournement d'horaire.
- **Désactivé :** Le lecteur est shunté (désactivé).
- **Carte seule :** La porte est verrouillée lorsque le lecteur fonctionne en mode *Carte uniquement*.
- **Carte et code PIN :** La porte est verrouillée lorsque le lecteur fonctionne en mode *Carte et code PIN*.
- **Carte ou code PIN :** La porte est verrouillée lorsque le lecteur fonctionne en mode *Carte ou code PIN*.
- **Accès refusé :** Une demande d'accès est refusée.
- **Accès accordé :** Une demande d'accès est accordée ou la porte est déverrouillée manuellement.
- **Demander le code PIN :** Le système attend la saisie d'un code PIN. Pour cela, le lecteur doit fonctionner en mode *Carte et code PIN*.
- **Demander le deuxième titulaire de cartes :** Le système attend la présentation d'un deuxième identifiant. Cela se produit lorsqu'une règle de deux personnes ou une règle d'escorte des visiteurs est en vigueur.
- **Alarme de porte :** L'alarme *Porte ouverte trop longtemps* ou l'alarme *Porte forcée* a été déclenchée.
- **Attendre :** Le système attend qu'un identifiant biométrique soit présenté ou qu'un système externe valide un identifiant.

Procédure

1 Connectez-vous à l'unité Synergis[MC] Cloud Link.

2 Cliquez sur **Configuration** > **Paramètres des DEL et du signal sonore du lecteur**.



3 Pour chaque état de porte, configurez la façon dont vous voulez que le lecteur se comporte :

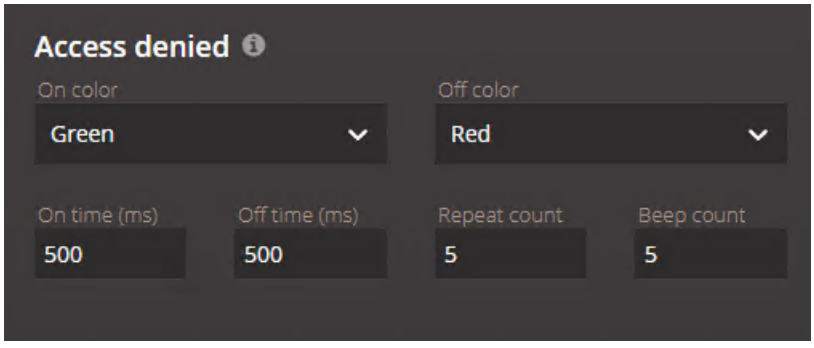
- **Couleur d'activation :** Couleur de la DEL lorsque la porte passe dans cet état.
- **Temps d'allumage (ms) :** Temps en millisecondes pendant lequel la DEL reste dans la couleur 'On'.
- **Couleur de désactivation :** Couleur alternée de la DEL.
- **Temps d'extinction (ms) :** Temps en millisecondes pendant lequel la DEL reste dans la couleur 'Off'.
- **Nombre de répétitions :** Nombre de fois que la DEL passe par le cycle couleur 'On' - couleur 'Off'.
- **Nombre de bips :** Nombre de fois que le lecteur doit émettre un signal sonore.

LA DEL et le signal sonore s'allument en même temps. Le comportement de la DEL dure *((Temps d'allumage + Temps d'extinction) x Nombre de répétitions)* millisecondes. Ce comportement est interrompu lorsque la porte passe à un autre état.

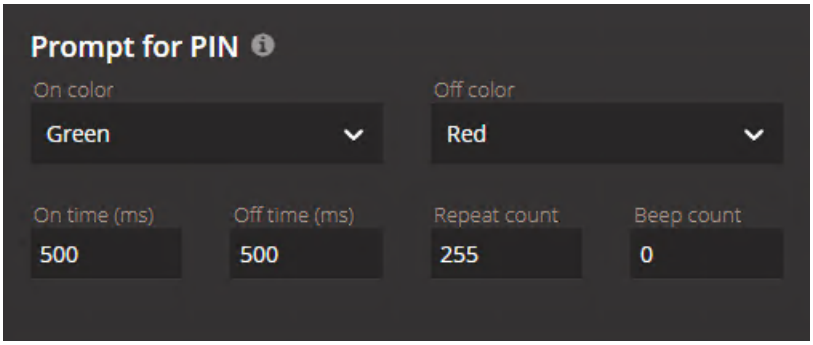
REMARQUE : Le volume et la durée du signal sonore ne peuvent pas être contrôlés.

4 Cliquez sur **Enregistrer**.

- **Exemple 1 :** Pour que la DEL clignote en rouge et vert pendant 5 secondes maximum et émette cinq bips lorsque l'accès est refusé à une porte, utilisez les paramètres suivants.



- **Exemple 2 :** Pour inviter l'utilisateur à saisir un code PIN en faisant clignoter rapidement la DEL en couleur ambre jusqu'à ce que le code PIN soit saisi sans émettre de signal sonore, utilisez les paramètres suivants.


Prompt for PIN
On color
Green
Off color
Red
On time (ms)
500
Off time (ms)
500
Repeat count
255
Beep count
0

Copie des paramètres de la DEL du lecteur et du signal sonore d'une unité Synergis à l'autre

Vous pouvez exporter les paramètres des LED et des signaux sonores d'une unité Synergis[MC] Cloud Link et les importer dans d'autres unités Synergis Cloud Link.

Avant de commencer

Configurez les paramètres des LED et du signal sonore du lecteur pour une première unité Synergis Cloud Link.

À savoir

Les paramètres de la DEL du lecteur et du signal sonore sont des paramètres propres à l'unité. Toutefois, pour l'instant, seuls les lecteurs contrôlés par Mercury sont pris en charge.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link à partir de laquelle vous souhaitez effectuer la copie.

2 Cliquez sur **Configuration** > **Paramètres des DEL et du signal sonore du lecteur**.

3 Cliquez sur **Exporter**.

Les paramètres des LED et du signal sonore sont enregistrés dans un fichier nommé *LedConfig<Hostname>_yyyy-mm-dd_hh_mm_ss.xml*, où *<Hostname>* est le nom d'hôte de l'unité Synergis Cloud Link, dans votre dossier *Téléchargements*.

4 Connectez-vous à l'unité Synergis Cloud Link vers laquelle vous souhaitez effectuer la copie.

5 Cliquez sur **Configuration** > **Paramètres des DEL et du signal sonore du lecteur**.

6 Cliquez sur **Importer**.

Une fenêtre du navigateur de fichiers s'ouvre.

7 Naviguez vers votre dossier *Téléchargements*, sélectionnez le fichier XML que vous voulez, puis cliquez sur **Ouvrir**.

Les paramètres de la LED du lecteur et du signal sonore lus dans le fichier sont appliqués à votre unité Synergis Cloud Link.

8 Cliquez sur **Enregistrer**.

Désactiver les contrôles de sorties

Pour éviter que les portes puissent être déverrouillées par Synergis[MC] Appliance Portal , vous pouvez désactiver le contrôle des états de sorties.

À savoir

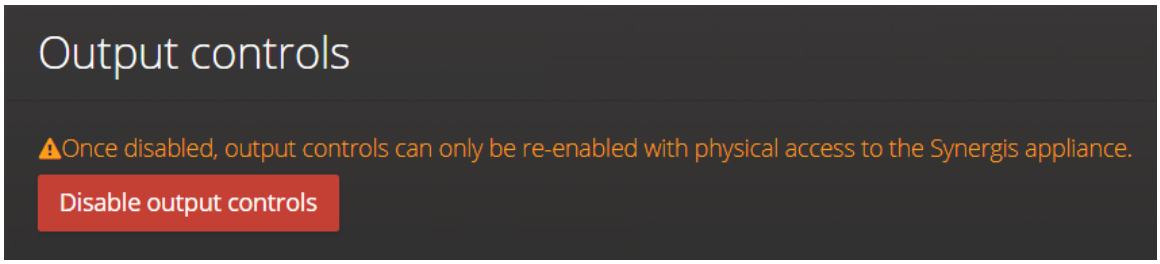
- Si vous désactivez les contrôles de sorties, vous pouvez afficher l'état des sorties, mais vous ne pouvez plus les modifier sur la page *Diagnostic d'E/S*.
- Vous ne pouvez réactiver les contrôles de sorties qu'en exécutant une commande de commutateur DIP sur l'appareil Synergis[MC] Cloud Link .

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Paramètres de l'unité**.

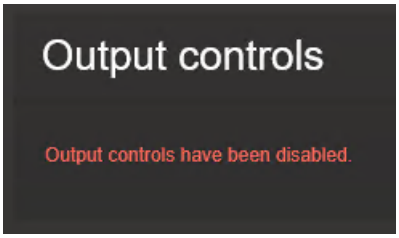
3 Dans la section *Contrôles de sorties*, cliquez sur **Désactiver les contrôles de sorties**.



La boîte de dialogue *Contrôles de sorties* apparaît et vous inviter à continuer.

4 Cliquez sur **OK**.

Le bouton **Désactiver les contrôles de sorties** disparaît et le message suivant est affiché : *Les contrôles de sorties ont été désactivés.*



Rubriques connexes

Codes de commande des commutateurs DIP, page 5

À propos de la fonctionnalité Moteur d'automatisation

Le moteur d'automatisation est la fonctionnalité du Synergis[MC] Softwire qui exécute des règles, comme les associations événement-action dans Security Center. Le moteur d'automatisation fonctionne même lorsque l'unité Synergis[MC] est déconnectée de son rôle Gestionnaire d'accès.

REMARQUE : Une règle de moteur d'automatisation ne génère aucune action si l'unité Synergis Cloud Link et les appareils en aval ne parviennent pas à communiquer.

Les règles de moteur d'automatisation font partie des fichiers de configuration de l'unité Synergis Cloud Link . Il est recommandé de télécharger ces fichiers lorsque vous avez terminé de configurer les règles, afin de pouvoir restaurer la configuration en cas de remplacement de l'unité.

Configuration requise

- Synergis Cloud Link 3.0.2

REMARQUE : Avant Synergis Cloud Link 3.0.2, la fonction de *moteur d'automatisation* était appelée *règle primitive*. Les règles primitives configurées dans les versions précédentes de Synergis Cloud Link sont affichées automatiquement sur la page *Moteur d'automatisation* du portail de l'appareil Synergis[MC] après la mise à niveau vers la version 3.0.2 ou ultérieure.

Limitations

Tenez compte des limitations suivantes du moteur d'automatisation :

- L'outil Copier la configuration ne s'applique pas à cette fonction.
- L'outil Remplacement de l'unité ne s'applique pas à cette fonction.
- Supprimer une porte à laquelle des règles de moteur d'automatisation ont été appliquées ne supprime pas les règles correspondantes.
- L'unité Synergis Cloud Link doit être en ligne pour pouvoir y configurer des règles de moteur d'automatisation.
- Les valeurs décimales ne sont pas prises en charge pour la fréquence des impulsions de l'action *Sortie - Impulsion*.
- Le niveau d'accès minimal configuré pour un secteur dans Security Center remplace le niveau d'accès minimal activé par une règle du moteur d'automatisation.

Configurer les règles du moteur d'automatisation

Pour déclencher des actions lorsqu'un événement de contrôle d'accès se produit, configurez les règles du moteur d'automatisation dans Synergis[MC] Appliance Portal . Par exemple, augmenter la distance de sécurité minimale d'une zone lorsqu'une entrée de porte passe en état de panne.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Moteur d'automatisation**.

3 Cliquez sur **Ajouter une règle**.

4 Dans la section *Événement*, sélectionnez un événement déclencheur dans la liste :

- **Lecteur - Accès autorisé**
- **Porte - Alarme de porte maintenue ouverte**
- **Porte - Alarme d'ouverture forcée**
- **Porte - Accès autorisé**
- **Porte - Accès refusé**
- **Mise à jour de l'état d'entrée**

5 Dans le champ **Nom**, donnez un nom à la règle.

6 En fonction de l'événement que vous avez sélectionné, cliquez sur ✎ en regard du champ **Lecteur**, **Porte** ou **Entrée**.

7 Dans la boîte de dialogue qui apparaît, sélectionnez le lecteur, la porte ou l'entrée, puis cliquez sur **OK**.

REMARQUE : Si vous avez un grand nombre de lecteurs, de portes ou d'entrées, utilisez le champ de recherche en haut de la boîte de dialogue pour les rechercher par nom.

8 Si vous avez sélectionné l'événement *Porte - Accès accordé* ou *Mise à jour de l'état de l'entrée*, configurez les paramètres supplémentaires :

- **Porte - Accès autorisé :** (Facultatif) Pour accorder l'accès à un groupe de titulaires de cartes, récupérez le GUID du groupe dans Config Tool, puis entrez le GUID dans le champ **Groupe de titulaires de cartes**.
- **Mise à jour de l'état d'entrée :** Sélectionnez le ou les états de l'entrée qui doivent déclencher l'action :
  - **Actif**
  - **Normal**
  - **Problème**

9 Dans la section *Actions*, cliquez sur **Ajouter une action**, puis sélectionnez l'une des actions suivantes dans la liste :

- **Sortie - Définir**
- **Sortie - Effacer**
- **Sortie - Impulsion**
- **Secteur - Définir le niveau d'accès minimal**

10 En fonction de l'action que vous avez sélectionnée, cliquez sur ✎ en regard du champ **Sortie** ou **Secteur**.

11 Dans la boîte de dialogue qui apparaît, sélectionnez une sortie ou un secteur, puis cliquez sur **OK**.

REMARQUE : Si vous avez un grand nombre de sorties ou de secteurs, utilisez le champ de recherche en haut de la boîte de dialogue pour les rechercher par nom.

12 Si vous avez sélectionné l'action *Sortie - Impulsion* ou *Secteur - Définir le niveau d'accès minimal*, configurez les paramètres supplémentaires :

- **Sortie - impulsion :** Dans le champ **Secondes**, entrez un nombre pour spécifier la fréquence des impulsions.
- **Secteur - Définir le niveau d'accès minimal :** Dans le champ **Minimum**, entrez une valeur comprise entre 1 et 7 pour spécifier le niveau d'accès minimal pour accéder au secteur.

13 Configurez d'autres actions en fonction de vos besoins.

14 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Téléchargez la configuration de votre unité Synergis Cloud Link sous forme de fichier compacté, afin de pouvoir restaurer les règles du moteur d'automatisation en cas de remplacement de l'unité.

Pour en savoir plus, voir Télécharger le fichier de configuration de votre unité Synergis Cloud Link, page 247.

Récupération des IUG d'entité

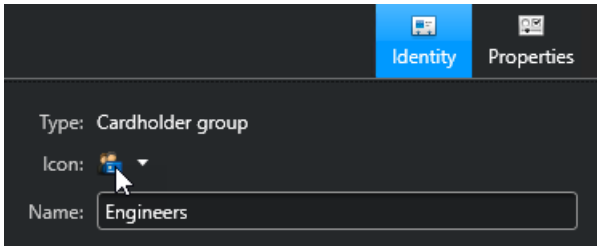
Avant de spécifier un groupe de titulaires de cartes dans une règle du moteur d'automatisation, vous devez récupérer le GUID (globally unique identifier) de l'entité dans Config Tool.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Titulaires de cartes et identifiants**.

2 Sélectionnez le groupe de titulaires de cartes dans l'arborescence des entités.

3 Sur la page *Identité* du groupe de titulaires de cartes, cliquez deux fois sur l'icône de l'entité en maintenant la touche Ctrl enfoncée.



L'IUG est copié dans votre presse-papiers.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

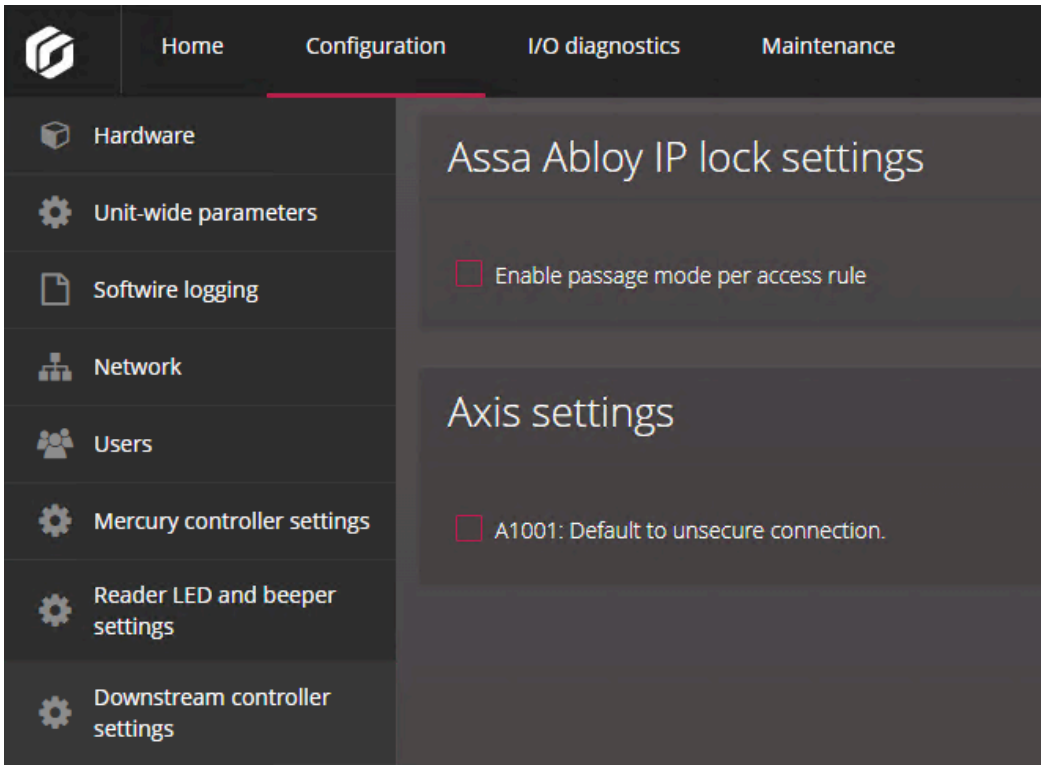
Configuration des paramètres des contrôleurs en aval

Vous pouvez configurer le comportement de tous les modules d'interface connectés à une même unité Synergis[MC] Cloud Link sur la page *Paramètres des contrôleurs en aval* du Synergis[MC] Appliance Portal.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Réglages des contrôleurs en aval**.



3 Dans la section *Réglages des verrous IP Assa Abloy*, configurez l'option suivante :

- **Activer le mode passage par règle d'accès :** Crée le champ personnalisé *PassageMode* nécessaire pour activer le mode passage pour les verrous IP Assa Abloy par règle d'accès.

  Pour en savoir plus, voir Activer le mode passage des verrous IP Assa Abloy, page 90.

4 Dans la section *Réglages Axis*, configurez l'option suivante :

- **A1001 : connexion non sécurisée par défaut :** Sélectionnez cette option afin de pouvoir utiliser Synergis[MC] Softwire pour mettre à niveau le micrologiciel de votre contrôleur AXIS A1001 s'il ne prend pas en charge le protocole HTTPS.

5 Cliquez sur **Enregistrer**.

Les modifications sont appliquées après un redémarrage logiciel.

Configuration de MIFARE DESFire

Pour activer MIFARE DESFire sur votre unité Synergis Cloud Link, vous devez charger le fichier de configuration, puis associer la configuration à vos lecteurs transparents STid SSCP ou OSDP.

Avant de commencer

Configurez des Lecteurs STid SSCP ou des Lecteurs OSDP.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **MIFARE DESFire**.

3 Cliquez sur **Sélectionner le fichier de sites de cartes à puces**, et naviguez jusqu'à votre fichier de configuration personnalisé (*SmartCardsSites.xml*) ou jusqu'au fichier par défaut livré avec votre installation Security Center.

Pour en savoir plus sur le fichier *SmartCardsSites.xml*, voir Configurer MIFARE DESFire dans Security Center.

4 Si vous utilisez la messagerie sécurisée DESFire EV2, activez cette fonction dans votre système.

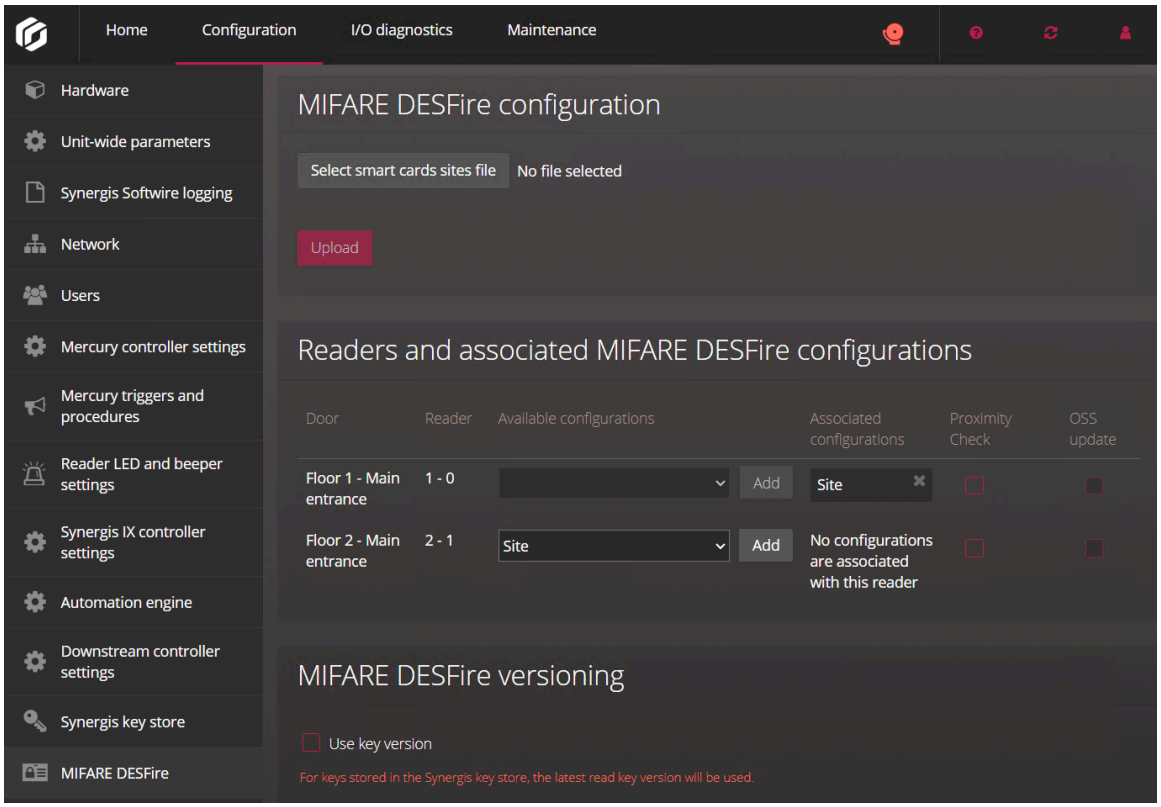
5 Cliquez sur **Transférer**.

Le message suivant est affiché : *Transfert réussi.*

6 Associez les lecteurs et les configurations MIFARE DESFire :

a) Pour chaque lecteur, sélectionnez un site dans la liste **Configurations disponibles**.

b) Cliquez sur **Ajouter**.



7 Si votre système utilise le versionnement des clés, cochez la case **Utiliser la version des clés**.

Deux scénarios doivent être envisagés :

- **Les clés sont stockées dans le magasin de clés Synergis :** Lorsque la case est cochée, le système demande à la carte quelle version de clé elle utilise, puis tente de la trouver dans le magasin de clés. Si la case n'est pas cochée, le système utilise toujours la dernière version. Pour en savoir plus, voir À propos du magasin de clés Synergis, page 49.
- **Les clés sont stockées sur la carte SAM :** Lorsque la case est cochée, le système demande à la carte quelle version de clé elle utilise, puis tente de la trouver sur la carte SAM. Si la case n'est pas cochée, le système utilise toujours la version 0. Pour plus d'informations, voir Versionnement des clés pour les cartes SAM, page 48.

8 Cliquez sur **Enregistrer**.

Rubriques connexes

Configurer et inscrire des lecteurs STid utilisant le protocole SSCP, page 229
Configurer et ajouter des lecteurs OSDP dans Synergis Appliance Portal, page 219

Activation de la messagerie sécurisée DESFire EV2

Pour utiliser la messagerie sécurisée DESFire EV2, vous devez activer l'authentification EV2 sur vos fichiers de configuration DESFire et les exporter vers vos postes de travail et unités Synergis[MC] Cloud Link.

Avant de commencer

Configurez MIFARE DESFire dans Security Center et exportez votre configuration dans un fichier XML.

À savoir

Le fichier de configuration DESFire (*SmartCardsSites.xml*) est créé dans Config Tool à l'aide de la tâche *MIFARE DESFire configuration*. Pour l'instant, cette tâche ne prend pas en charge le mode d'authentification EV2. Par conséquent, vous devez modifier manuellement ce paramètre dans le fichier XML exporté.

Procédure

1 En utilisant un éditeur de texte, ouvrez votre fichier personnalisé *SmartCardsSites.xml*.

2 Repérez <AuthenticationMode> l'étiquette à la fin de chaque configuration et remplacez EV1 par EV2.

```
<AuthenticationMode>
  <EV2 />
</AuthenticationMode>
```

3 Enregistrez vos modifications et fermez le fichier.

4 À l'aide de Config Tool, importez le fichier modifié *SmartCardsSites.xml* avec la tâche *configuration MIFARE DESFire*.

5 Exportez la nouvelle configuration MIFARE DESFire vers vos postes de travail et vos Synergis Cloud Link unités.

Déverrouiller les cartes SAM

Stocker les clés de chiffrement sur des cartes MIFARE SAM (Secure Access Module) plutôt que dans le magasin de clés Synergis[MC] renforce la sécurité, car les clés ne peuvent pas être récupérées. Les cartes SAM doivent être déverrouillées pour interagir avec Synergis[MC] Cloud Link pour les opérations cryptographiques.

Avant de commencer

- Configurez une unité Synergis Cloud Link 312.

  REMARQUE : Vous devez avoir une unité Synergis Cloud Link 312 pour stocker les clés de carte SAM. Pour en savoir plus sur la préparation de Synergis Cloud Link 312, voir Installer des cartes SAM dans un appareil Synergis Cloud Link 312.
- Configurez les cartes SAM avec un outil de production SAM et installez de une à trois cartes.

  REMARQUE : Si vous installez plusieurs cartes SAM, les cartes doivent avoir les mêmes clés. Installer plusieurs cartes SAM permet d'accélérer les lectures et les décisions d'accès sur les unités très sollicitées pour le contrôle d'accès.

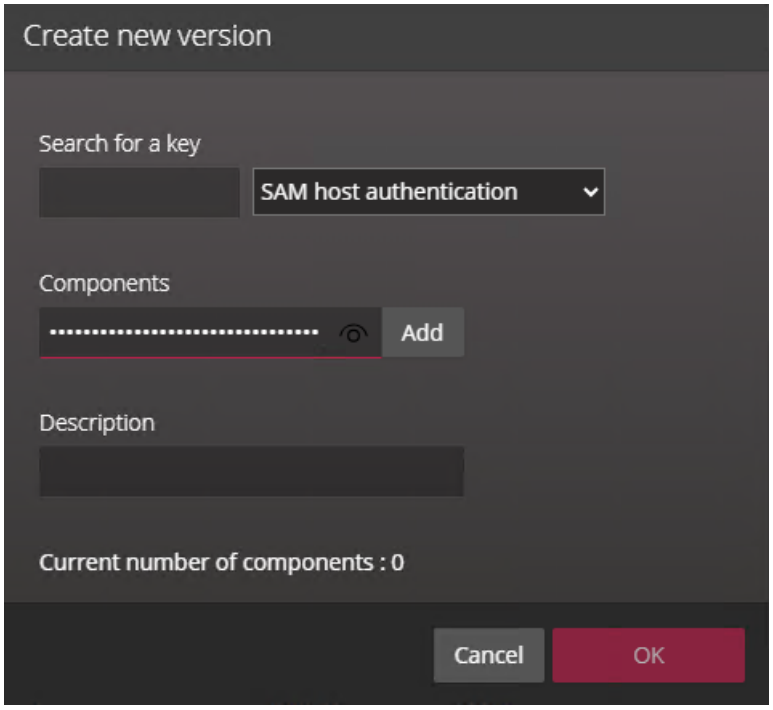
Procédure

1 Connectez-vous à l'unité Synergis Cloud Link 312.

2 Cliquez sur **Configuration** > **Magasin de clés Synergis**[MC].

3 En haut de la liste des clés, cliquez sur ➕.

4 Dans la boîte de dialogue *Créer une nouvelle version*, procédez de la manière suivante :

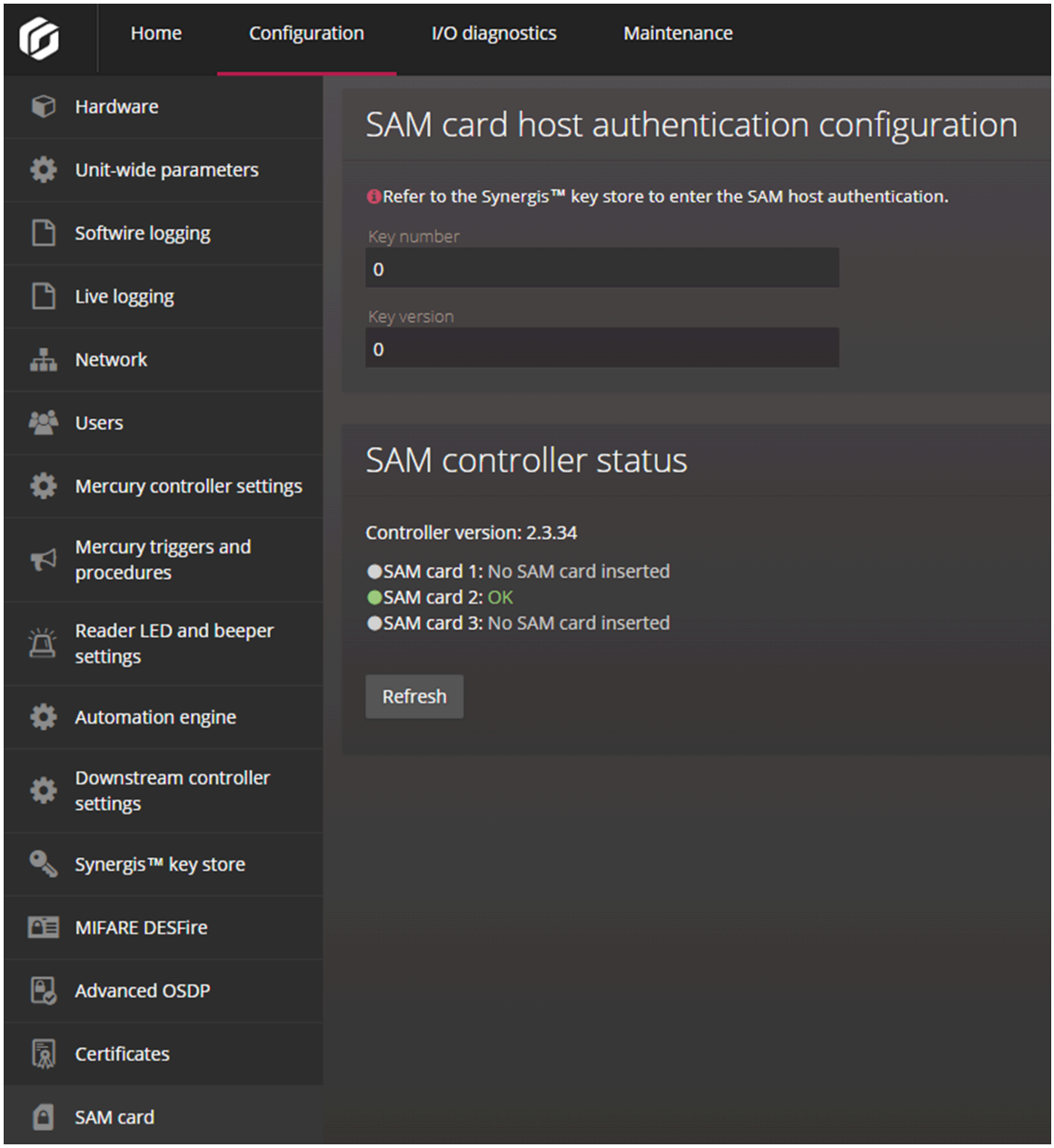


   a) Sélectionnez **Authentification de l'hôte SAM**.

   b) Dans le champ **Composants**, entrez les clés d'authentification de l'hôte que vous avez configurées dans l'outil de production SAM, et cliquez sur **Ajouter**.

   c) Cliquez sur **OK**.

5 Cliquez sur **Configuration** > **Carte SAM**.



6 Dans la section *Configuration de l'authentification de l'hôte SAM*, entrez le numéro et la version de la clé d'authentification de l'hôte stockée sur la carte SAM.

7 Dans la section *État du contrôleur SAM*, vérifiez que les cartes SAM sont insérées et configurées correctement.

Vous pouvez installer jusqu'à trois cartes SAM. Chaque emplacement peut avoir l'un des états suivants :

- **OK :** Une carte SAM est insérée et la clé d'authentification de l'hôte, le numéro de clé et le numéro de version sont valables.
- **Échec de déverrouillage de la carte SAM :** Une carte SAM est insérée, mais la clé d'authentification de l'hôte, le numéro de clé ou le numéro de version ne correspondent pas à ceux qui sont stockés sur la carte.
- **Aucune carte SAM insérée :** Il n'y a pas de carte SAM dans l'emplacement.

Lorsque vous avez terminé

Inscrivez des lecteurs STid ou OSDP, ou configurez les lecteurs inscrits.

Rubriques connexes

Versionnement des clés pour les cartes SAM, page 48
À propos de Synergis Cloud Link 312, page 6

Versionnement des clés pour les cartes SAM

Pour utiliser les versions de clés de lecture de l'application avec vos cartes SAM MIFARE, configurez jusqu'à trois clés pour les cartes à l'aide d'un outil de configuration de cartes SAM, puis activez le versionnement des clés sur le Synergis[MC] Appliance Portal.

Avant de commencer

- Configurez jusqu'à trois clés pour vos cartes SAM à l'aide d'un outil de production SAM.
- Installez les cartes SAM dans une unité Synergis[MC] Cloud Link 312. Pour en savoir plus, voir Installer des cartes SAM dans un appareil Synergis Cloud Link 312.

À savoir

Par défaut, Security Center ne prend pas en charge les cartes SAM avec les versions de clés de lecture de l'application autre que la version 0 ; l'activation du versionnement des clés permet d'utiliser des cartes pré-codées dont les versions de clés sont différentes de 0. La fonctionnalité s'exécute avec les protocoles OSDP et SSCP et offre une gestion des clés flexible aux administrateurs qui souhaitent incrémenter leur version de clé régulièrement.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link 312.

2 Cliquez sur **Configuration** > **MIFARE DESFire**.

3 Dans la section *Versions MIFARE DESFire*, cochez la case **Utiliser la version de clé**.

Lorsque la case est cochée, le système demande à la carte quelle version de clé elle utilise, puis tente de la trouver sur la carte SAM. Si la case n'est pas cochée, le système utilise toujours la version de clé 0.

4 Cliquez sur **Enregistrer**, puis redémarrez l'unité.

Rubriques connexes

Déverrouiller les cartes SAM, page 45

À propos de Synergis Cloud Link 312, page 6

À propos du magasin de clés Synergis

Le magasin de clés Synergis[MC] sert à configurer et stocker les clés de chiffrement.

Clés dans le magasin de clés Synergis

Chaque clé de chiffrement est constituée d'un ou de plusieurs composants. Pour une sécurité renforcée, une clé peut être constituée de plusieurs composants, afin de pouvoir la scinder et la distribuer à plusieurs intervenants sans que personne ne possède la clé complète.

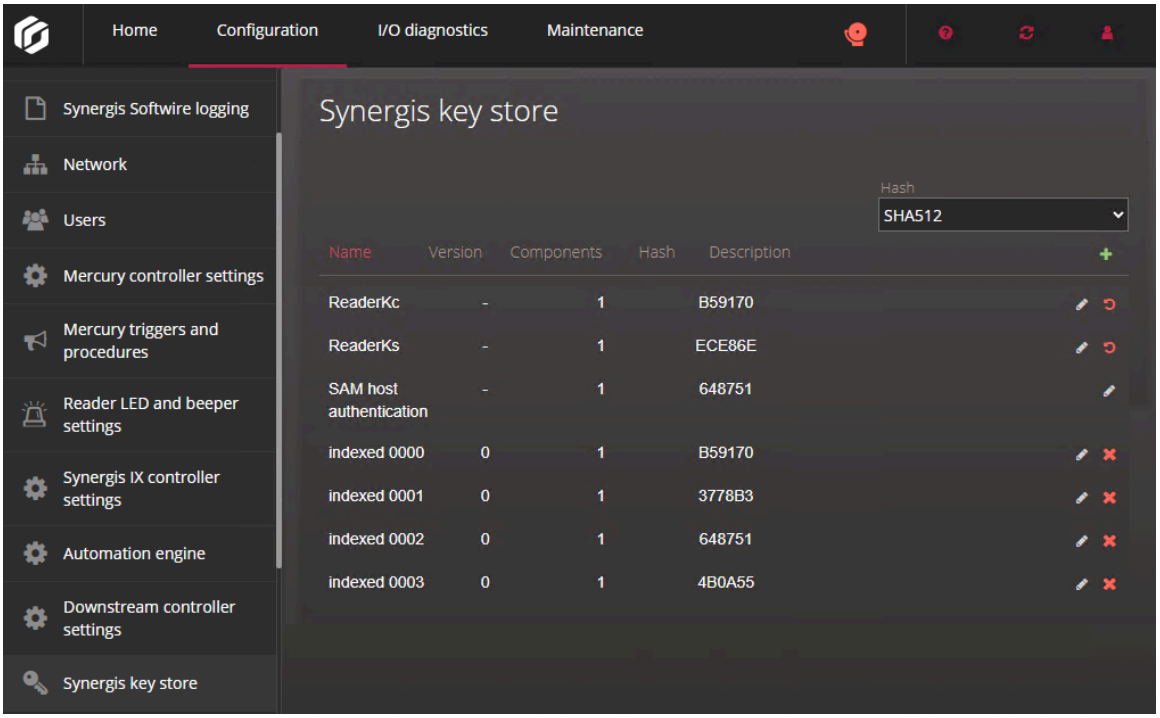
Dans le magasin de clés Synergis, la version, le nombre actuel de composants et le hachage sont affichés pour chaque clé.

- **Version :** Le numéro de version de la clé. Chaque version de la clé que vous créez est une nouvelle clé.

  Plusieurs versions de la même clé sont répertoriées si la case **Utiliser la version de la clé** de la page Configuration MIFARE DESFire est cochée. Lorsque la case est cochée, le système interroge la carte pour savoir quelle version de la clé elle utilise, puis il tente de la trouver dans le magasin de clés. Les clés indexées 00 à 31 peuvent avoir jusqu'à trois versions à la fois. Si la case n'est pas cochée, le système utilise toujours la dernière version.

  Par exemple, si vous activez le versionnement des clés, puis que vous ajoutez les versions *1*, *2*, puis *3* pour la clé *indexed 01*, puis que vous décochez cette case, seule la version *3* est affichée dans le magasin de clés Synergis pour cette clé. Si vous créez version *4*, puis cochez à nouveau la case, les versions *2*, *3* et *4* sont affichées.

  REMARQUE : Les clés ReaderKc, ReaderKs et authentification de l'hôte SAM ne prennent pas en charge les versions de clés. Les dernières modifications sont incrémentées automatiquement.
- **Composants :** Le nombre de composants qui forment actuellement la clé. Chaque composant est une valeur hexadécimale de 32 caractères.
- **Hachage :** Le hachage de clé utilisé pour vérifier la validité de la clé que vous avez saisie dans le magasin de clés Synergis. La clé est valable si elle correspond au hachage d'autres unités, la carte SAM ou l'outil de production de cartes à puce avec lequel vous voulez comparer. Pour en savoir plus, voir Utilisation du hachage de clés dans le magasin de clés Synergis, page 51.



Les clés de chiffrement MIFARE DESFire peuvent être exportées depuis Security Center vers une ou plusieurs unités Synergis[MC] Cloud Link de votre système. Les clés sont ensuite mises à jour automatiquement sur la page *Magasin de clés Synergis* du Synergis[MC] Appliance Portal. Pour en savoir plus, voir Exporter les clés MIFARE DESFire vers les unités Synergis Cloud Link.

Cas d'utilisation des différentes clés

Chaque type de clé dans le magasin de clés Synergis est utilisée dans un contexte particulier :

- **ReaderKc et ReaderKs :** Sert à configurer les clés de communication pour les lecteurs STid. Pour en savoir plus, voir Modifier les clés de communication RS-485 par défaut pour les lecteurs STid utilisant le protocole SSCP, page 236.
- **SAM host authentication :** Sert à déverrouiller les cartes SAM pour pouvoir utiliser les clés de chiffrement qu'elles stockent. Pour en savoir plus, voir Déverrouiller les cartes SAM, page 45.
- **Indexed 00 à 31 :** Sert à créer les clés de chiffrement pour accéder à l'identifiant sécurisé d'une carte MIFARE DESFire. Pour en savoir plus, voir Activer MIFARE DESFire pour les lecteurs OSDP transparents, page 222 et Activer le mode transparent sur les lecteurs STid utilisant le protocole SSCP, page 233.

Utilisation du hachage de clés dans le magasin de clés Synergis

Vous pouvez utiliser le hachage de clés pour comparer les clés du magasin de clés Synergis à d'autres unités, ou à la carte SAM ou à l'outil de création de cartes utilisé pour créer les clés.

À savoir

Les clés enregistrées dans le magasin de clés Synergis ne peuvent pas être récupérées, mais elles peuvent être vérifiées à l'aide du hachage de clés.

Procédure

1 Connectez-vous à l'unité Synergis[MC] Cloud Link.

2 Cliquez sur **Configuration** > **Magasin de clés Synergis**.

3 Dans la liste **Hachage**, sélectionnez l'algorithme utilisé par l'outil de création de cartes tiers ou l'unité Synergis Cloud Link :

- **KCV** : Key Checksum Value
- **SHA1** : Secure Hash Algorithm 1
- **SHA256** : Version 256 bits de Secure Hash Algorithm 2
- **SHA384** : Version 384 bits de Secure Hash Algorithm 2
- **SHA512** : Version 512 bits de Secure Hash Algorithm 2

Dans la colonne **Hachage**, le hachage de clé de 6 caractères (24 bits) est affiché, quel que soit l'algorithme utilisé.

4 Vérifiez que le hachage de clé dans le magasin de clés Synergis correspond au hachage d'autres unités, de la carte SAM ou de l'outil de production de cartes à puce avec lequel vous voulez comparer.

5 Vérifiez que le hachage de clé dans le magasin de clés Synergis correspond au hachage d'autres unités, de la carte SAM ou de l'outil de production de cartes à puce avec lequel vous voulez comparer.

Modifier le délai de saisie du code PIN pour les portes

Lorsque des codes PIN longs sont utilisés, vous pouvez modifier le délai de saisie du code PIN pour donner plus de temps aux titulaires de cartes pour la saisie.

À savoir

Le délai par défaut est de 5 secondes.

Procédure

1 Connectez-vous à Security Center avec Config Tool.

2 Dans la tâche *Vue secteur*, sélectionnez la porte dont vous souhaitez prolonger le délai de saisie du code PIN.

3 Cliquez sur l'onglet **Matériel**.

4 En regard du lecteur *Carte et code PIN* affecté à la porte, cliquez sur **Paramètres du lecteur** ( ).

5 Dans la boîte de dialogue *Paramètres du lecteur*, activez **Utiliser la carte et le code PIN** si nécessaire.

6 Spécifiez le **Délai d'accès**, puis cliquez sur **Enregistrer** > **OK**.

7 Si le réglage souhaité est *Carte ou code PIN*, procédez de la manière suivante :

a) Cliquez sur **Paramètres du lecteur** ( ), et désactivez **Utiliser la carte et le code PIN**.

b) Cliquez sur **Enregistrer**.

8 Cliquez sur **Appliquer**.

Configurer la journalisation des événements sur l’unité Synergis Cloud Link

L'unité Synergis[MC] Cloud Link peut conserver des journaux détaillés pour le dépannage et l'assistance. Toutefois, ces journaux sont désactivés par défaut. Activez-les si vous souhaitez consulter le rapport de dépannage ou télécharger les journaux pour l’assistance.

À savoir

- Activez la journalisation uniquement si l'assistance technique Genetec[MC] vous y invite.
- Les erreurs *critiques* sont toujours écrites dans les journaux, quel que soit le niveau de journalisation défini.
- Vous pouvez télécharger les journaux sur la page *Télécharger les journaux de diagnostic* du Synergis[MC] Appliance Portal .
- Vous pouvez également configurer les journaux pour qu'ils soient stockés dans le cloud via Azure Application Insights.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Configuration** > **Journalisation Synergis Softwire**.

3 Dans la section *Journalisation Synergis Softwire*, sélectionnez un **Niveau de journalisation**.

4 Si vous sélectionnez le niveau de journalisation **Débogage** ou **Trace**, entrez le nombre de jours pour lesquels vous souhaitez récupérer les journaux du niveau sélectionné dans le champ **Rétablir le niveau de journalisation Infos après (jours)**.

Exemple: Si vous sélectionnez **Débogage** comme niveau de journalisation et saisissez **10** dans le champ **Rétablir le niveau de journalisation Info après (jours)**, les journaux de niveau *Critique*, *Erreur*, *Avertissement*, *Info* et *Débogage* sont consignés pendant dix jours. Après dix jours, seuls les journaux de niveau *Critique*, *Erreur*, *Avertissement* et *Info* sont consignés.

5 Cliquez sur **Enregistrer**.

Configurer la journalisation des événements auxiliaires dans le cloud pour l'unité Synergis Cloud Link

Configurez votre unité Synergis[MC] Cloud Link pour qu'elle se connecte à une ressource Azure Application Insights, afin que les journaux puissent être stockés dans le cloud en plus d'être stockés sur l'unité elle-même. Cela peut simplifier l'analyse des journaux et l'utilisation d'outils de surveillance sur ces derniers.

Avant de commencer

Une ressource Application Insights doit être créée et configurée.

À savoir

- L'unité Synergis Cloud Link se connecte à la ressource Application Insights par l'intermédiaire de la clé d'appareillage de la ressource.
- Vous pouvez utiliser la clé d'appareillage pour connecter plusieurs unités Synergis Cloud Link à la même ressource Application Insights.
- Vous pouvez configurer différents niveaux de journalisation pour les journaux stockés sur l'unité Synergis Cloud Link et dans le cloud.

  Exemple : Pour économiser de l'espace sur l'unité, vous pouvez la configurer pour stocker uniquement les journaux de niveau *Critique*, en envoyant tous les autres journaux vers le cloud.

Procédure

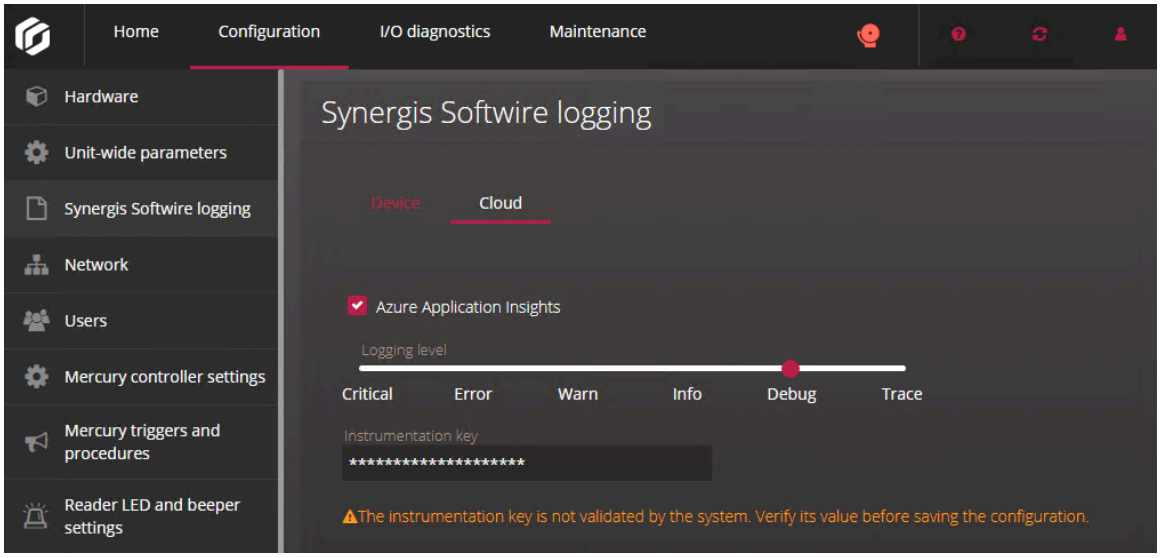
1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Configuration** > **Journalisation Synergis Softwire**.

3 Dans la section *Journalisation Synergis Softwire*, cliquez sur sur la vue **Cloud**, puis sélectionnez **Azure Application Insights**.

4 Sélectionnez un **Niveau de journalisation**.

5 Dans le champ **Clé d'appareillage**, saisissez la clé d'appareillage de la ressource Application Insights à laquelle vous souhaitez envoyer les journaux.



6 Cliquez sur **Enregistrer**.

Configurer la conservation des historiques sur l'unité Synergis Cloud Link

Vous pouvez configurer la durée de conservation des journaux d'historique de l'unité Synergis[MC] Cloud Link avant leur suppression automatique.

À savoir

- Par défaut, les historiques sont conservés 90 jours.
- Les historiques peuvent être téléchargés sur la page *Télécharger les journaux de diagnostic* du portail par l'utilisateur Admin.
- Les éléments suivants sont journalisés :
  - Tentatives de connexion réussies et infructueuses, modifications du mot de passe des utilisateurs et blocages des utilisateurs, qui surviennent après trois tentatives de connexion infructueuses.
  - Modifications de la configuration du Synergis[MC] Appliance Portal .

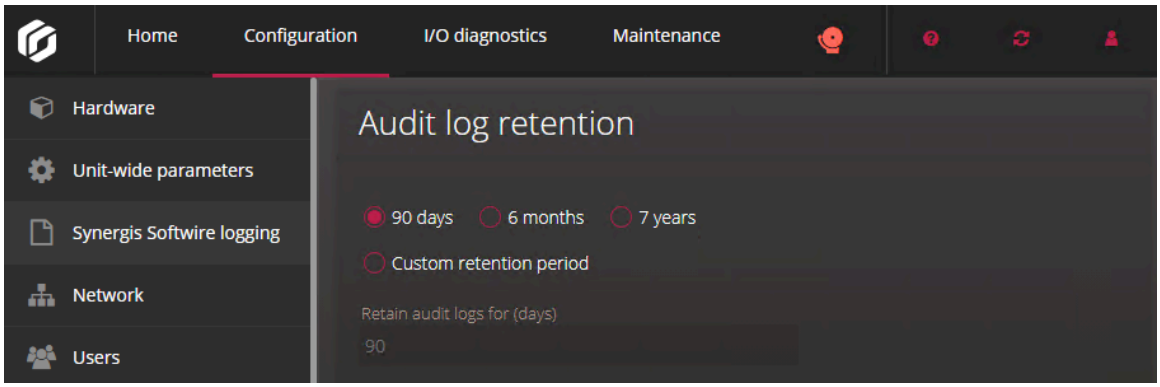
    REMARQUE : Les modifications apportées sur les pages *Matériel* et *Réseau* ne sont pas consignées.
  - Commandes de commutateurs DIP exécutées sur l'appareil Synergis Cloud Link .

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Configuration** > **Journalisation Synergis Softwire**.

3 Dans la section *Rétention des historiques*, sélectionnez une durée de conservation :



- **90 jours**
- **6 mois**
- **7 ans**
- **Période de rétention personnalisée** : Entrez un valeur comprise entre 2 et 2557 pour spécifier la durée en jours de la période de rétention.

4 Cliquez sur **Enregistrer**.

Inscription des unités Synergis Cloud Link à Security Center

Pour inscrire une unité Synergis[MC] Cloud Link dans Security Center, affectez l'unité à un rôle Gestionnaire d'accès.

Avant de commencer

Configurez les propriétés réseau de l'unité Synergis Cloud Link.

À savoir

Lorsque vous créez un rôle Gestionnaire d'accès, l'extension Synergis est ajoutée automatiquement. L'extension est créée avec le port de découverte par défaut 2000. Si vous avez configuré un autre port dans les propriétés réseau de l'unité, vous devez le modifier dans Config Tool en conséquence.

BONNE PRATIQUE : Si vous avez plusieurs rôles Gestionnaire d'accès qui contrôlent des unités Synergis sur le même sous-réseau, veillez à ce qu'ils utilisent des ports de découverte différents. Dans le cas contraire, vous risquez de subir des problèmes de performances.

Procédure

1 Si l'unité n'utilise pas le port de découverte par défaut, modifiez le port de découverte de l'extension Synergis pour qu'il corresponde au port configuré sur l'unité :
   a) Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.
   b) Sélectionnez le Gestionnaire d'accès, et cliquez sur l'onglet **Extensions**.
   c) Sélectionnez l'extension Synergis.
   d) Sélectionnez le port de découverte, puis cliquez sur **Modifier l'élément** ( ).
   e) Dans la boîte de dialogue *Port de découverte*, entrez le numéro de port configuré pour vos unités, et cliquez sur **Enregistrer**.

2 Ajoutez l'unité Synergis[MC] au rôle Gestionnaire d'accès.

Ajout d'unités Synergis Cloud Link à un rôle de Gestionnaire d'accès

Pour contrôler l'accès aux zones sécurisées de votre site et surveiller les événements de contrôle d'accès dans Security Center, vous devez ajouter des unités de contrôle d'accès à un rôle Gestionnaire d'accès.

Avant de commencer

Vérifiez que le port de découverte de l'extension Synergis[MC] correspond au numéro de port sur votre unité.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

2 Cliquez sur **Unité de contrôle d'accès** ( ).

3 Dans la boîte de dialogue *Création d'une unité*, cliquez sur **Type d'unité**, puis sélectionnez **Synergis**.

4 Dans la section *Extrémité réseau*, entrez le nom d'hôte ou l'adresse IP de l'unité, ainsi que les identifiants de connexion d'administrateur.

5 Si la redirection de ports est nécessaire, cliquez sur **Options avancées** et entrez l'URL de base dans le champ **Adresse Web**.

6 Cliquez sur **Suivant**.

7 Sélectionnez une **Partition** à laquelle vous souhaitez ajouter l'unité de contrôle d'accès, et cliquez sur **Suivant**.

Les partitions déterminent quels utilisateurs Security Center ont accès à cette entité. Seuls les utilisateurs autorisés de la partition peuvent afficher ou modifier l'unité de contrôle d'accès.

8 Vérifiez la fenêtre *Résumé de l'opération* et cliquez sur **Créer**.

Le Gestionnaire d'accès tente de se connecter à l'unité, et l'inscrit auprès du système. Lorsque la procédure est terminée avec succès, un message de confirmation est affiché.

9 Cliquez sur **Fermer**, puis sur **Actualiser** ( ).

L'unité nouvellement ajoutée apparaît sous le Gestionnaire d'accès auquel elle a été affectée dans la vue **Rôles et unités**. Le nom par défaut de l'entité est le nom d'hôte de l'unité. Désormais, cette unité ne répondra qu'aux commandes envoyées par ce rôle Gestionnaire d'accès.

REMARQUE : Par la suite, si vous modifiez les paramètres de connexion sur l'unité, vous devrez informer le Gestionnaire d'accès en synchronisant l'unité avec le Gestionnaire d'accès.

10 Si cette unité doit être connectée en tant que pairs à d'autres unités, ajoutez-la au groupe de pairs approprié. Pour en savoir plus, voir Activer le pair-à-pair sur le rôle Gestionnaire d'accès.

Ajouter les unités Synergis Cloud Link à un gestionnaire d'accès du logiciel en tant que service hébergé

Ajouter une unité Synergis^{MC} Cloud Link à votre Gestionnaire d'accès active l'unité pour établir une connexion sécurisée à un déploiement Security Center SaaS Edition (Classic) hébergé.

Avant de commencer

- Vérifiez que le DNS et les autres paramètres réseau de l'unité sont bien configurés.
- Modifiez le mot de passe de connexion par défaut pour l'unité.
- Vérifiez que l'unité Synergis Cloud Link est connectée à Internet.

  Allez sur *https://<adresse IP SCL>/CloudAgent*, et connectez-vous au portail de l'agent Synergis^{MC} SaaS avec les identifiants de connexion que vous utilisez pour vous connecter au portail de l'appareil Synergis^{MC}. L'état de la connexion est disponible sur la page *Activation* de l'unité. Si votre réseau local ne peut se connecter à Internet que via un serveur de proxy, indiquez l'URL du proxy ainsi que le nom d'utilisateur et mot de passe éventuels sur la page *Proxy*.
- Vérifiez que votre poste Config Tool est sur le même réseau que votre unité Synergis Cloud Link.

À savoir

Cloud Agent est préinstallé sur toutes les unités Synergis Cloud Link de nouvelle génération. Cloud Agent est un module logiciel distinct qui établit une connexion sécurisée au cloud. Lorsque l'unité est inscrite à un Gestionnaire d'accès SaaS hébergé, la connexion au cloud est activée.

Procédure

Pour ajouter une unité Synergis Cloud Link à un Gestionnaire d'accès SaaS hébergé :

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

2 Cliquez sur **Unité de contrôle d'accès** ( ).

3 Dans la boîte de dialogue *Création d'une unité*, cliquez sur **Type d'unité**, puis sélectionnez **Synergis^{MC} SaaS**.

4 Dans la zone **Point limite réseau**, saisissez le nom d'hôte ou l'adresse IP de l'unité puis cliquez sur **Valider**.

   Le système vérifie le Synergis Cloud Link et affiche l'adresse MAC de l'unité.

5 Entrez le nom d'utilisateur et mot de passe de l'administrateur.

   Le nom d'utilisateur par défaut est admin. Modifiez le mot de passe par défaut pour inscrire l'unité.

6 Vérifiez la fenêtre *Résumé de l'opération* et cliquez sur **Créer**.

   Config Tool envoie les informations de Synergis Cloud Link au gestionnaire d'accès qui les réexpédie à la passerelle du logiciel en tant que service. Lorsque l'unité est connectée à la passerelle SaaS, un message de confirmation est affiché.

7 Cliquez sur **Fermer**, puis sur **Actualiser** ( ).

   La nouvelle unité de contrôle d'accès apparaît sous le gestionnaire d'accès auquel elle a été affectée dans la vue **Rôles et unités**. Le nom par défaut de l'entité est le nom d'hôte de l'unité Synergis Cloud Link. Désormais, cette unité ne répondra qu'aux commandes envoyées par ce gestionnaire d'accès.

Pour supprimer une unité Synergis Cloud Link d'un Gestionnaire d'accès SaaS hébergé :

1 Dans la vue **Rôles et unités**, sélectionnez l'unité Synergis Cloud Link dans l'arborescence.

2 Cliquez sur **Supprimer** ( ).

3 Dans la boîte de dialogue de confirmation qui apparaît, cliquez sur **Supprimer**.

Synchronisation de l'unité Synergis Cloud Link avec le Gestionnaire d'accès

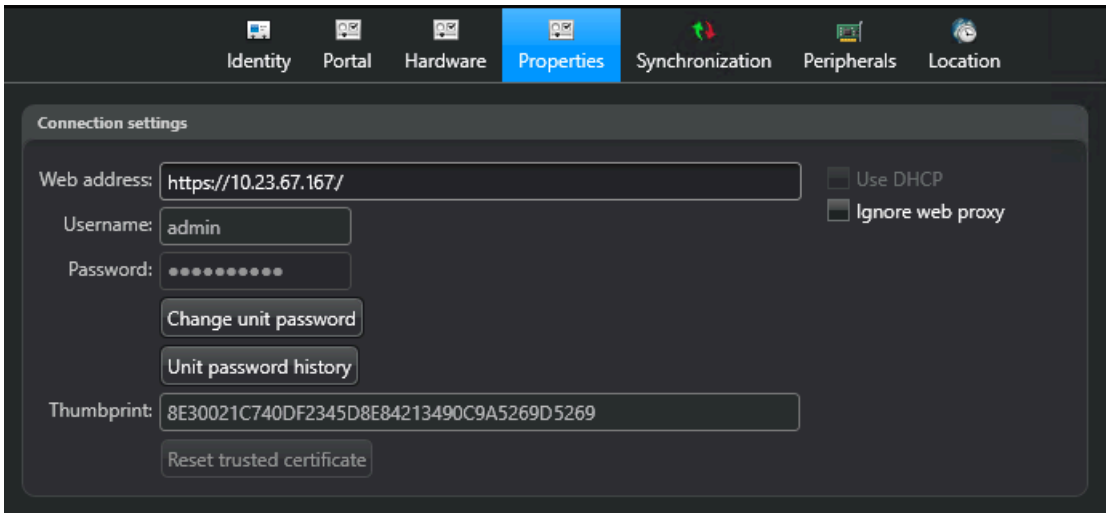
Certains paramètres de l'unité Synergis[MC] Cloud Link ne sont pas automatiquement synchronisés avec le Gestionnaire d'accès. Si vous modifiez des paramètres de l'unité via le Synergis[MC] Appliance Portal, comme le mot de passe de connexion, l'adresse IP ou la manière de répondre aux demandes de connexion, vous devez modifier les paramètres correspondants du Gestionnaire d'accès dans Config Tool.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

2 Dans l'arborescence des entités, sélectionnez l'unité que vous avez modifiée.

3 Cliquez sur l'onglet **Propriétés**.



4 Dans la section *Paramètres de connexion*, modifiez les paramètres pour qu'ils correspondent à ceux de l'unité sur le Synergis[MC] Appliance Portal.

- **Adresse Web :** Adresse Web pour contacter le portail de l'unité Synergis. Si vous modifiez l'adresse web pour utiliser l'adresse IP de l'unité après l'avoir inscrite avec son nom d'hôte, veillez à supprimer l'adresse IPv6 dans la liste **Connexions Gestionnaire d'accès acceptées** sur la page *Réseau* du portail

de l'unité. Si vous ne supprimez pas l'adresse IPv6 de la liste, l'unité ne se reconnectera plus si elle est déconnectée.

- **Nom d'utilisateur et mot de passe :** Nom d'utilisateur et mot de passe.
- **Modifier le mot de passe de l'unité :** Click to update the password.
- **Historique des mots de passe d'unité :** Affiche les détails des cinq dernières tentatives de modification du mot de passe via Security Center, dont la date, le mot de passe précédent et le nouveau mot de passe.
- **Utiliser le DHCP :** Ne modifiez ce paramètre que si un agent d'assistance technique Genetec vous y invite. Ce paramètre est réinitialisé à chaque fois que le Gestionnaire d'accès se reconnecte à l'unité Synergis.
- **Ignorer le proxy Web :** Activez cette option pour indiquer au Access Manager d'ignorer les réglages de Serveur proxy sur le serveur qui héberge actuellement le rôle. Désactivez cette option pour indiquer au Gestionnaire d'accès de respecter les réglages de Serveur proxy (effacé par défaut).
- **Empreinte :** L'empreinte du certificat sur l'unité Synergis. This field is automatically updated to reflect the new certificate when you click the **Reset trusted certificate** button.
- **Réinitialiser le certificat de confiance. :** (Activé lorsque l'unité est hors ligne) Cliquez sur ce bouton pour que le Gestionnaire d'accès oublie le certificat de confiance pour cette unité afin de pouvoir en accepter un nouveau. Utilisez cette fonctionnalité si vous avez changé le certificat numérique de l'entité après son inscription.

5 Cliquez sur **Appliquer**.

Configuration des entrées de surveillance sur l’appareil Synergis Cloud Link

Vous pouvez utiliser les quatre entrées sur l'appareil Synergis[MC] Cloud Link pour surveiller l'installation physique de l'appareil. Vous pouvez par exemple connecter une entrée à un interrupteur de sabotage sur le boîtier qui contient l’appareil.

À savoir

- Vous pouvez définir un comportement spécial pour chaque entrée. Chaque comportement spécial correspond à un événement que vous pouvez recevoir dans la tâche *Surveillance* :

Comportement spécial	Événement de Security Center
Problème d’alimentation	Panne de courant
Interrupteur de sabotage	Sabotage matériel
Problème de batterie	Panne de batterie

- Vous pouvez voir les changements d’état des entrées sur la page *Diagnotic d’E/S* dans le Synergis[MC] Appliance Portal.

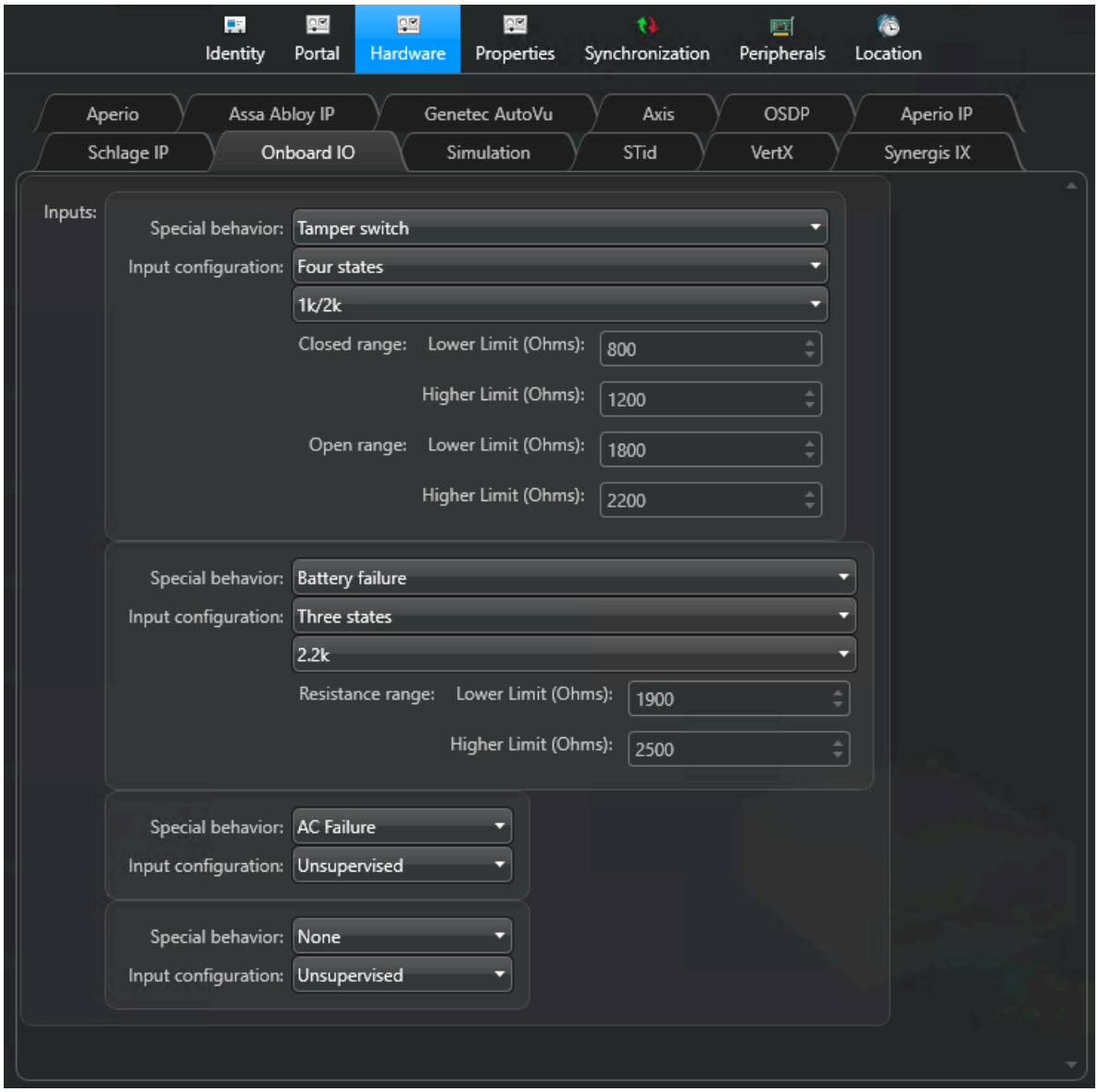
Procédure

1 Sur la page d’accueil de Config Tool, ouvrez la tâche *Contrôle d’accès*, puis cliquez sur la vue **Rôles et unités**.

2 Sélectionnez votre unité Synergis Cloud Link et cliquez sur l’onglet **Matériel**.

3 Cliquez sur l'onglet **ES embarquées**, puis configurez les entrées :

Exemple :



- **Comportement spécial :** Les comportements spéciaux déterminent l'événement que vous recevez dans la tâche *Surveillance* lorsque l'entrée est dans un état anormal. Par défaut, le comportement spécial est réglé sur **Aucun**. Sélectionnez l'une des options suivantes :
  - **Problème d'alimentation**
  - **Interrupteur de sabotage**
  - **Problème de batterie**
- **Configuration des entrées :** Sélectionnez l'une des options suivantes :
  - **Non supervisé :** Les entrées sont non supervisées par défaut.
  - **Trois états :** Sélectionnez l'une des options préconfigurées qui sélectionnent la **Plage de résistance**, ou sélectionnez **Personnalisé** et entrez la **Limite inférieure (Ohms)** et la **Limite supérieure (Ohms)** vous-même.
  - **Quatre états :** Sélectionnez l'une des options préconfigurées qui sélectionnent la **Plage si fermé** et la **Plage si ouvert**, ou sélectionnez **Personnalisé** et entrez la **Limite inférieure (Ohms)** et la **Limite supérieure (Ohms)** vous-même.

4 Cliquez sur **Appliquer**.

5 Cliquez sur l’onglet **Périphériques**, puis cliquez deux fois sur l’entrée que vous avez configurée sur la page *Matériel*.

6 (Facultatif) Dans la boîte de dialogue *Modifier l’entrée*, entrez un nouveau nom et ID logique.

7 Spécifiez le **Type de contact** :

   a) Sélectionnez **Non supervisé**, **Supervisé à 3 états** ou **Supervisé à 4 états** en fonction de la valeur que vous avez sélectionnée pour **Configuration des entrées** sur la page *Matériel*.

   b) Sélectionnez **Normalement ouvert** ou **Normalement fermé**.

8 Cliquez sur **Enregistrer**.

Lorsqu'une entrée est en état anormal, l'unité Synergis Cloud Link devient jaune, et vous recevez un avertissement d'entité. Si vous surveillez l'unité Synergis Cloud Link et les événements de comportement spécial, vous recevez l'événement correspondant au comportement spécial de l'entrée dans la tâche *Surveillance*.

Partie III

Configuration spécifique pour les intégrations

Cette section comprend les chapitres suivants:

4

Verrous sans fil Allegion Schlage

Cette section aborde les sujets suivants:

Inscription de verrous sans fil Allegion Schlage sur l'unité Synergis

Les verrous Allegion Schlage LE, NDE et Control (FE410 et BE467F) peuvent être intégrés à la plate-ENGAGE sans contrôleurs Mercury.

À savoir

L'intégration ENGAGE IP prend en charge jusqu'à 10 verrous par passerelle et jusqu'à 32 passerelles par unité Synergis[MC], avec un maximum of 200 verrous par unité. Vous devez disposer d'un accès en ligne pour effectuer cette tâche.

Procédure

1 Créez un compte partenaire ENGAGE sur *portal.allegionengage.com*.

IMPORTANT : Ne créez pas votre compte ENGAGE depuis l'application mobile Allegion ENGAGE.

2 Téléchargez la dernière version de Genetec[MC] Allegion Site Configurator depuis la page Téléchargement de produit *GTAP* :

a) Dans la liste **Download Finder**, sélectionnez votre version de **Synergis[MC] Cloud Link**.

b) Téléchargez Genetec Allegion Site Configurator.

3 Utilisez Genetec Allegion Site Configurator pour créer le site qui doit accueillir le matériel de contrôle d'accès.

Ce processus crée automatiquement une clé de site. Notez la clé de site et stockez-la en lieu sûr.

4 Téléchargez l'app mobile Allegion ENGAGE sur l'App Store ou sur Google Play.

5 Ouvrez l'application mobile Allegion ENGAGE pour vous connecter à votre compte partenaire ENGAGE.

6 Utilisez l'application mobile Allegion ENGAGE pour ajouter les passerelles et les verrous au site et pour les relier.

7 Connectez-vous à l'unité Synergis Cloud Link.

8 Cliquez sur **Configuration** > **Matériel**.

9 En haut de la colonne **Matériel**, cliquez sur **Ajouter** (➕).

10 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **Schlage IP** dans la liste **Type de matériel**, puis entrez l'adresse IP de la passerelle ENGAGE et la clé de site créée avec Genetec Allegion Site Configurator.

11 Cliquez sur **Enregistrer**.

Les identifiants de connexion à la passerelle sont automatiquement saisis, et les verrous connectés sont affichés dans l'arborescence matérielle.

IMPORTANT : Assurez-vous que la clé du site est correctement saisie. En cas de saisie incorrecte, aucun identifiant n'est synchronisé avec le verrou.

12 (Facultatif) Ajoutez chacune des autres passerelles ENGAGE.

13 Inscrivez les identifiants dans Security Center.

REMARQUE : Vous ne pouvez pas inscrire des identifiants par saisie automatique sur le verrou. Vous pouvez utiliser le lecteur Allegion Schlage MT20 Enrollment Reader en mode Keystroke Emulator.

Ré-inscription de verrous sans fil Allegion Schlage sur une unité Synergis

Vous pouvez ré-inscrire les verrous Allegion Schlage depuis la page *Matériel* de l'unité Synergis[MC] dans Config Tool afin d'éviter d'avoir à rétablir les paramètres d'usine sur la passerelle ENGAGE et ses verrous et d'utiliser l'application mobile Allegion ENGAGE pour le processus de ré-inscription.

À savoir

- La passerelle ENGAGE ne doit pas avoir été réinitialisée aux paramètres d'usine avant d'être ré-inscrite via Config Tool.
- Vous pouvez uniquement utiliser le Synergis[MC] Appliance Portal pour inscrire la passerelle ENGAGE pour la première fois, ou pour l'inscrire après l'avoir réinitialisée aux paramètres d'usine.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

2 Dans l'arborescence des entités, sélectionnez l'unité Synergis pour laquelle vous souhaitez ré-inscrire la passerelle ENGAGE.

3 Cliquez sur **Matériel** > **Schlage IP**.

4 Cliquez sur **Ajouter** (), puis spécifiez les informations suivantes :

- **IP :** L'adresse IP de la passerelle ENGAGE.
- **Nom d'utilisateur :** Le nom d'utilisateur de la passerelle ENGAGE.
- **Mot de passe :** Le mot de passe de la passerelle ENGAGE.
- **Clé de site :** La clé de site que vous avez créée à l'aide de Genetec[MC] Allegion Site Configurator lors de l'inscription initiale de la passerelle ENGAGE.

REMARQUE : Vous pouvez utiliser l'URL suivante pour accéder au nom d'utilisateur et au mot de passe : *https://<IP SCL>/SchlageIP/Bus/<IP passerelle>/RevealCredentials* , où *<IP SCL>* est l'adresse IP de l'unité Synergis et *<IP passerelle>* est l'adresse IP de la passerelle ENGAGE.

5 Cliquez sur **Appliquer**.

Les verrous sont ajoutés sur la page *Périphériques* de l'unité Synergis dans Config Tool. Cette opération peut prendre plusieurs minutes.

5

Verrous Assa Abloy compatibles Aperio

Cette section aborde les sujets suivants:

Associer les verrous compatibles Aperio avec le concentrateur AH30

Si vous utilisez des verrous compatibles Aperio avec un concentrateur AH30, vous devez jumeler les verrous avec le concentrateur à l'aide de l'application Aperio Programming Application (APA) avant d'inscrire les verrous sur votre unité Synergis[MC].

Avant de commencer

Vous devez disposer des éléments suivants :

- Le manuel Aperio Online Programming Application
- Aperio Programming Application (APA)
- Clé USB
- TriBee Bootloader, qui comprend le pilote du dongle USB
- Micrologiciel pris en charge
- Un ordinateur pour exécuter APA.
- Une carte compatible avec le lecteur.
- Fichier de clé de chiffrement fourni par ASSA ABLOY

Procédure

1 Réglez l'adresse EAC (1 à 15) sur le concentrateur à l'aide des commutateurs DIP.

IMPORTANT : Jusqu'à huit concentrateurs peuvent être connectés en guirlande sur un canal RS-485, mais ils doivent tous utiliser une adresse EAC différente.

2 Allumez le concentrateur.

3 Branchez le dongle USB sur votre ordinateur et installez les éléments suivants :

- TriBee Bootloader (pilote du dongle USB)
- Aperio Programming Application (APA)

4 Ouvrez APA, puis ouvrez ou créez une installation.

REMARQUE : Chaque installation est liée à un fichier de clé de chiffrement. Contactez ASSA ABLOY pour obtenir ce fichier de clé pour créer une installation.

5 Scannez pour détecter le concentrateur, et associez les verrous avec le concentrateur.

Pour en savoir plus, voir le *Manuel Aperio Online Programming Application*.

6 Avec APA, faites la mise à niveau du micrologiciel du concentrateur et des verrous.

Pour en savoir plus, voir Verrous compatibles Aperio pris en charge.

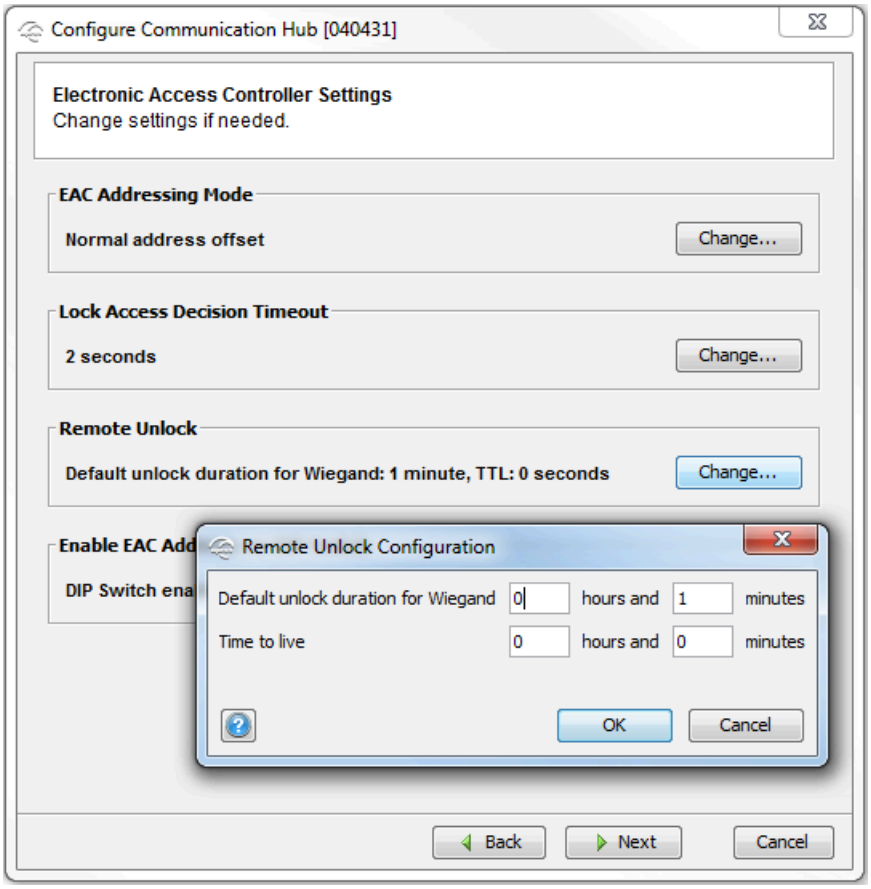
BONNE PRATIQUE : Faites toujours la mise à niveau du concentrateur avant la mise à niveau les verrous ou capteurs. Vérifiez que le commutateur DIP est réglé sur la bonne adresse EAC. Si le DIP 5 (mode association) est réglé sur actif durant une mise à niveau, le concentrateur démarrera avec une autre adresse EAC.

7 Configurez le concentrateur.

8 Si le micrologiciel du concentrateur de communication est antérieur à la version 2.6.5, activez l'option **Déverrouillage à distance** pour utiliser les horaires de déverrouillage de Security Center.

Avec le micrologiciel version 2.6.5 ou ultérieure, cette option est activée par défaut.

9 Dans la boîte de dialogue *Remote Unlock Configuration* (Configuration du déverouillage à distance), entrez une valeur dans **Time to live** (Durée de vie) et cliquez sur **OK**.



Ce délai indique la durée de la présence de la commande **Remote unlock** (grantAccessSequence) sur le concentrateur. Ce réglage doit toujours être supérieur à la valeur de **Status Report Interval** (Fréquence de signalement de l'état) définie sur le verrou.

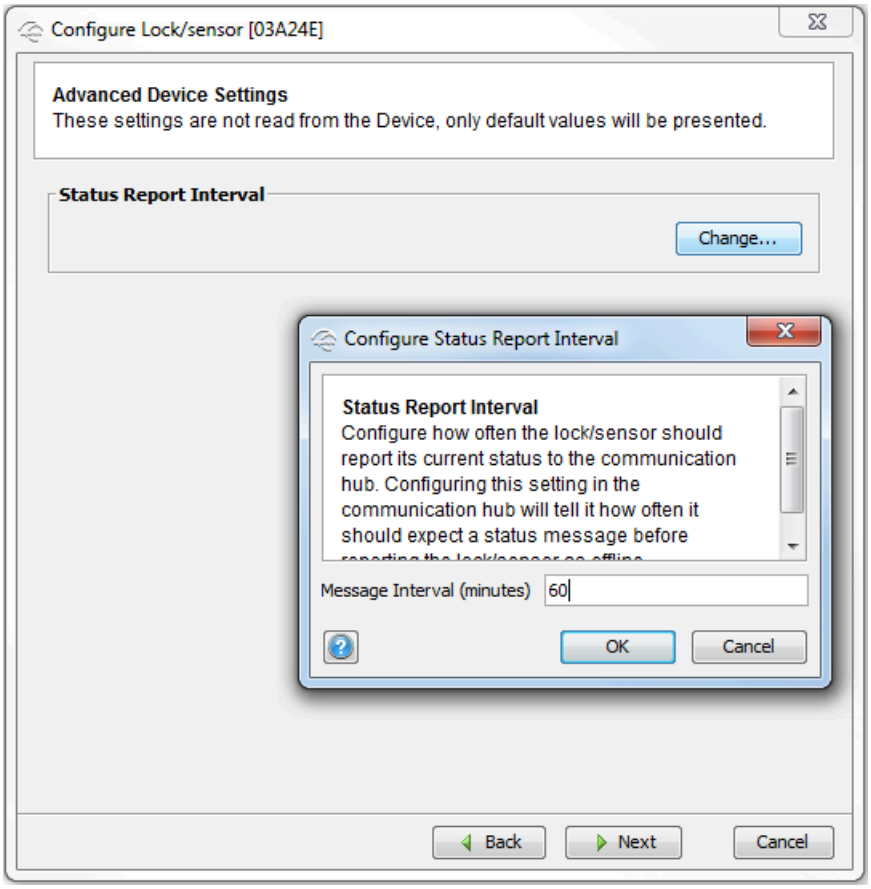
Vous pouvez ignorer la valeur **Default unlock duration for Wiegand** (Durée de déverrouillage par défaut pour Wiegand).

10 Si les horaires de déverrouillage sont utilisés, entrez une valeur de **Status Report Interval** de 5 à 15 minutes.

La diminution de la valeur de fréquence de signalement de l'état diminue l'autonomie du produit. Toute modification de cet intervalle doit être appliquée sur le verrou et sur le concentrateur de communication. S'il n'y a qu'un seul verrou associé au concentrateur de communication, c'est automatique. Si plusieurs

verrous sont associés au commutateur de communication, vous devez régler **Status Report Interval** via le concentrateur.

REMARQUE : Sur les verrous v3, le réglage **Status Report Interval** ne sert qu'à signaler l'état de connectivité du verrou. Il s'agit de l'intervalle d'interrogation **Polling Interval** qui sert à diminuer le décalage à l'activation et la désactivation des horaires.



11 Associez chaque verrou sans fil :

a) Faites un clic droit sur **Communication hub** et sélectionnez **Pair with lock or sensor** (Associer au verrou ou capteur).

Le processus d'association démarre.

b) Laissez l'identifiant sur le verrou, ou activez l'aimant pour que le capteur associe le matériel au concentrateur.

Le concentrateur attribue automatiquement une adresse EAC au verrou.

c) Notez l'adresse EAC (1 à 127) affectée au verrou.

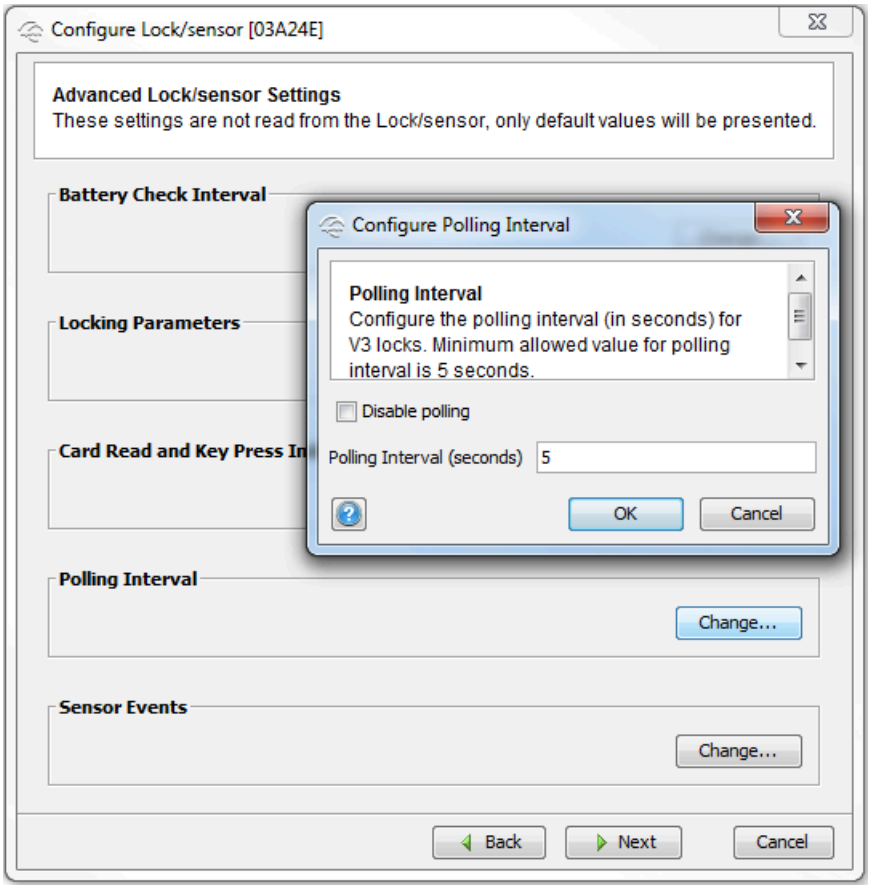
L'adresse EAC du concentrateur est intégrée à celle du verrou. Pour obtenir l'adresse EAC du concentrateur à partir de celle du verrou, appliquez une des formules suivantes :

- *Adresse EAC du concentrateur* = *Adresse EAC du verrou* **modulo** 16
- *Adresse EAC du concentrateur* = (**reste de** *l'Adresse EAC du concentrateur*) **divisé par** 16

12 Si vous utilisez des verrous v3, réglez **Polling Interval** sur 5 secondes.

Cela permet de limiter le décalage à l'activation et la désactivation des horaires, qui diminue la réactivité des verrous. Cela permet également aux commandes de déverrouillage envoyées depuis Security Desk d'être prises en compte sous 5 secondes. Il est déconseillé d'utiliser les commandes de déverrouillage

manuelles sur les verrous autres que v3, car la commande ne fonctionne qu'au bout d'une minute ou plus, selon la valeur de **Status Report Interval**.



13 Une fois que tous les verrous sont associés, sélectionnez l'utilisation de la communication radio sécurisée sur le concentrateur.

Lorsque vous avez terminé

Inscrivez les verrous sur l'unité Synergis.

Inscrire des verrous compatibles Aperio connectés à un concentrateur AH30

Pour que l'unité Synergis[MC] Cloud Link puisse communiquer avec les verrous compatibles Aperio, vous devez les inscrire sur le Synergis[MC] Appliance Portal.

Avant de commencer

- Associez les verrous compatibles Aperio avec le concentrateur.
- Connectez le hub à l'un des canaux RS-485 (1 - 4) :
  - Connectez le connecteur A du concentrateur au « + » du canal.
  - Connectez le connecteur B du concentrateur au « - » du canal.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** (➕).

4 Dans la boîte de dialogue *Ajouter du matériel*, dans la liste **Type de matériel**, sélectionnez **Aperio RS 485** .

5 Sélectionnez le **Canal** (1 - 4) .

REMARQUE : Si vous avez l'unité Synergis Cloud Link 312, vous avez jusqu'à 12 canaux. Pour en savoir plus, voir À propos des ports RS-485 du Synergis Cloud Link.

6 Dans la liste **Type de module d'interface**, sélectionnez **Aperio**.

7 Indiquez les verrous que vous souhaitez inscrire en procédant de l'une des manières suivantes :

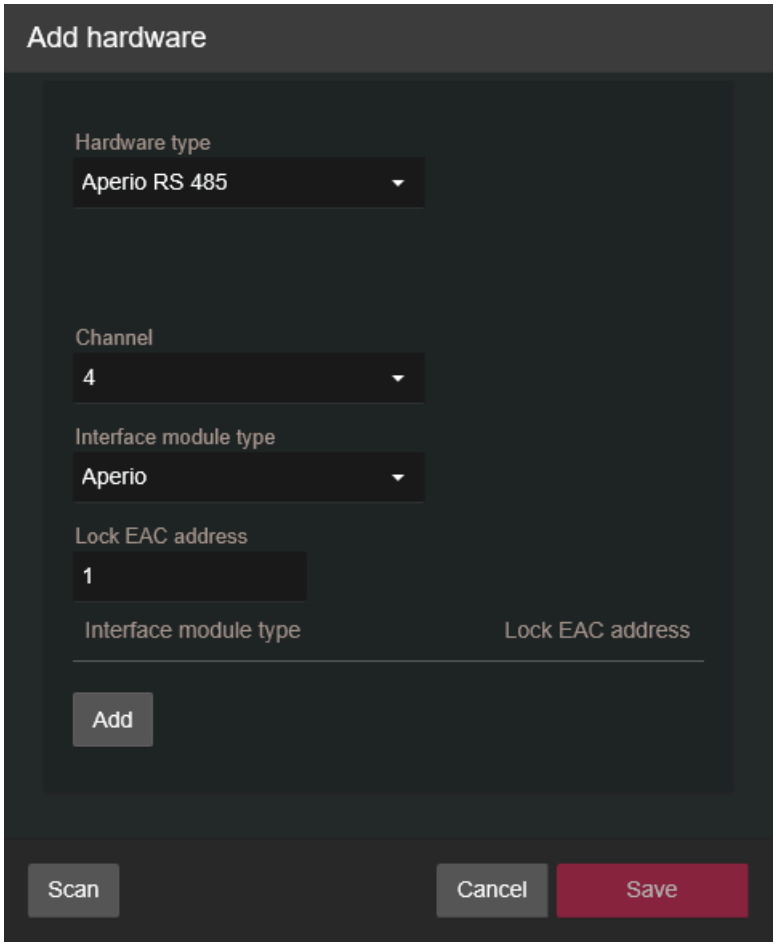
- Pour les inscrire automatiquement, cliquez sur **Analyser**.

  La fonction d'analyse détecte tous les modules d'interface d'un même fabricant connectés au même canal.

  Si le Synergis[MC] Appliance Portal ne détecte pas tous les modules d'interface connectés, essayez l'inscription manuelle.
- Pour inscrire un verrou manuellement, entrez son adresse EAC (1 à 127) que vous avez notée lorsque vous l'avez associée au concentrateur, et cliquez sur **Ajouter**.

Répétez pour configurer tous les modules connectés au même canal.

CONSEIL : Si vous inscrivez peu de verrous et connaissez leurs adresses EAC, l'inscription manuelle est plus rapide.



8 Cliquez sur **Enregistrer**.

Le type de matériel, le canal et le module d'interface que vous venez d'ajouter sont répertoriés sur la page *Configuration matérielle*.

9 Sélectionnez un verrou pour afficher ses propriétés dans le volet de droite.

Les adresses EAC du concentrateur et du verrou sont indiquées.

10 Sélectionnez chaque module d'interface sur la page *Configuration matérielle*, puis configurez ses réglages.

Pour une description des réglages, consultez la documentation du fabricant. Apportez les modifications nécessaires.

11 Testez la connexion de votre module d'interface et votre configuration à partir de la page *Diagnostics d'E/S*.

Lorsque vous avez terminé

- Inscrivez l’unité Synergis dans Security Center.
- Configurez les portes équipées des verrous compatibles Aperio.

Associer des verrous compatibles Aperio à un concentrateur IP AH40

Si vous utilisez des verrous compatibles Aperio avec un concentrateur AH40, vous devez configurer le concentrateur avec l'application Aperio Programming Application (APA) avant d'inscrire les verrous sur votre unité Synergis[MC].

Avant de commencer

Vous devez disposer des éléments suivants :

- Le manuel Aperio Online Programming Application
- Aperio Programming Application (APA)
- Clé USB
- TriBee Bootloader, qui comprend le pilote du dongle USB
- Micrologiciel pris en charge
- Un ordinateur pour exécuter APA.
- Une carte compatible avec le lecteur.
- Fichier de clé de chiffrement fourni par ASSA ABLOY

Procédure

1 Allumez le concentrateur.

2 Branchez le dongle USB sur votre ordinateur et installez les éléments suivants :

- TriBee Bootloader (pilote du dongle USB)
- Aperio Programming Application (APA)

3 Ouvrez APA, puis ouvrez ou créez une installation.

REMARQUE : Chaque installation est liée à un fichier de clé de chiffrement. Contactez ASSA ABLOY pour obtenir ce fichier de clé pour créer une installation.

4 Utilisez APA pour configurer le concentrateur :

a) Faites la mise à niveau du micrologiciel du concentrateur et des verrous.

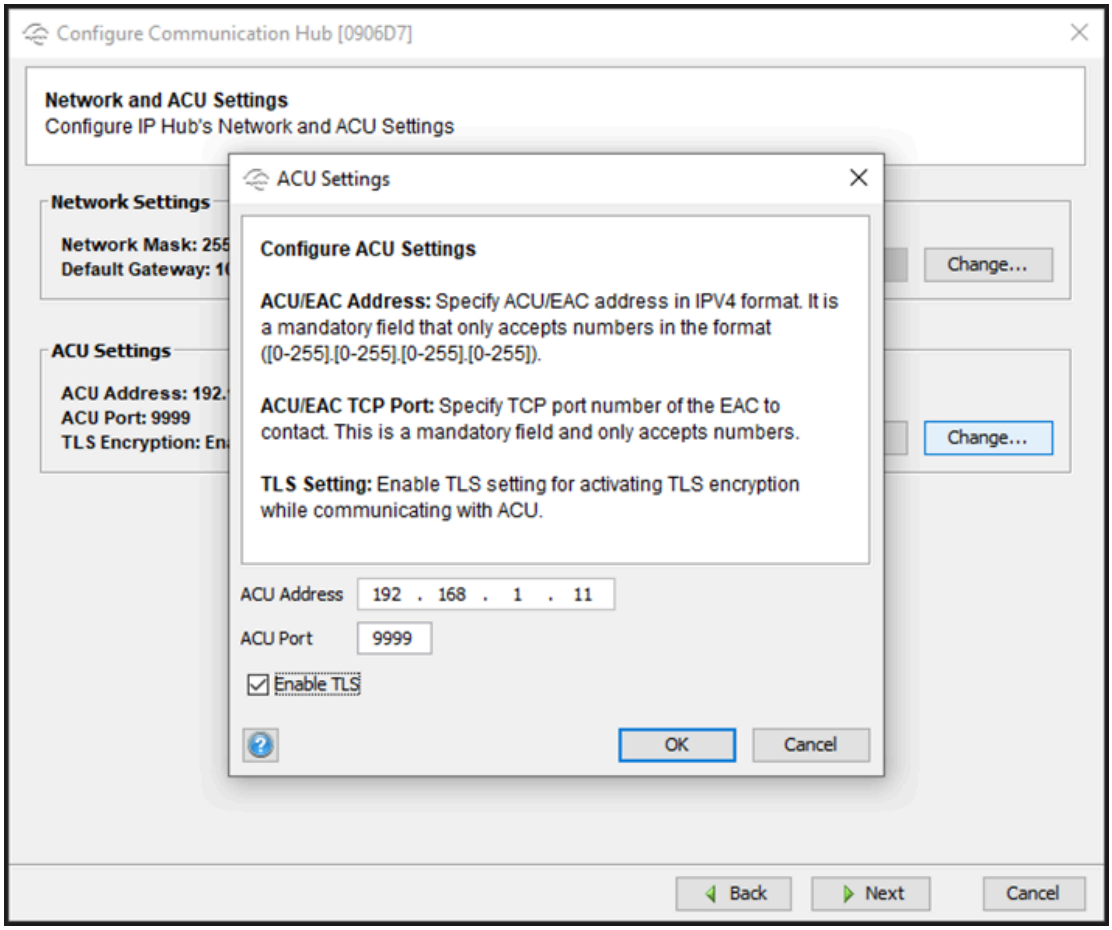
BONNE PRATIQUE : Exécutez toujours la mise à niveau du concentrateur avant celle des verrous ou capteurs.

b) Associez le concentrateur avec les lecteurs.

Sélectionner le concentrateur AH40 IP dans APA associe automatiquement le concentrateur aux lecteurs.

REMARQUE : Notez le numéro de port. Vous en aurez besoin pour inscrire le concentrateur sur le Synergis[MC] Appliance Portal.

c) Spécifiez l'adresse IP de l'unité Synergis en tant qu'adresse ACU.



Inscrire des verrous compatibles Aperio connectés à un concentrateur IP AH40

Pour que l'unité Synergis[MC] puisse communiquer avec les verrous compatibles Aperio, vous devez les inscrire sur le Synergis[MC] Appliance Portal.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** ( ).

4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **Aperio IP** en tant que **Type de matériel**, et entrez le numéro de port du concentrateur dans le champ **Port**. Le port par défaut est 9999.

5 Cliquez sur **Enregistrer**.

6 Cliquez sur **Modifier** ( ) dans l'interface Aperio IP.

La boîte de dialogue de configuration du canal apparaît.

7 Dans la boîte de dialogue de configuration, cochez la case **Inscrire** du concentrateur que vous souhaitez inscrire.

REMARQUE : Si vous avez configuré plusieurs concentrateurs AH40 sur le même port, tous les concentrateurs connectés et leur adresse MAC sont affichés.

8 Cliquez sur **Enregistrer**.

Les verrous connectés au concentrateur AH40 inscrit apparaissent dans l'arborescence matérielle et s'affichent en vert. Ce processus peut prendre jusqu'à 2 minutes.

Configurer les portes équipées d'un verrou compatible Aperio

Pour éviter de recevoir des événements *Porte verrouillée* et *Porte déverrouillée* en double dans Security Desk, vous devez désactiver l'option **Autoriser automatiquement la demande de passage** pour toutes les portes équipées d'un verrou compatible Aperio.

Avant de commencer

- Inscrivez l'unité Synergis Cloud Link dans Security Center.
- Selon le concentrateur que vous utilisez, procédez de l'une des manières suivantes :
  - Sur un concentrateur RS-485 AH30, jumelez vos verrous avec le concentrateur AH30 et inscrivez les verrous compatibles Aperio sur l'unité Synergis.
  - Pour les concentrateurs IP AH40 jumelez vos verrous avec le concentrateur AH30 et inscrivez les verrous compatibles Aperio sur l'unité Synergis.

À savoir

Les verrous Aperio utilisent un REX mécanique. Ce n'est pas l'unité Synergis Cloud Link qui contrôle le déverrouillage de la porte lorsque le REX est déclenché. Lorsque **Autoriser automatiquement les demandes de passage** est activé dans la configuration de la porte, les événements *Porte verrouillée* et *Porte déverrouillée* sont reçus deux fois dans Security Desk.

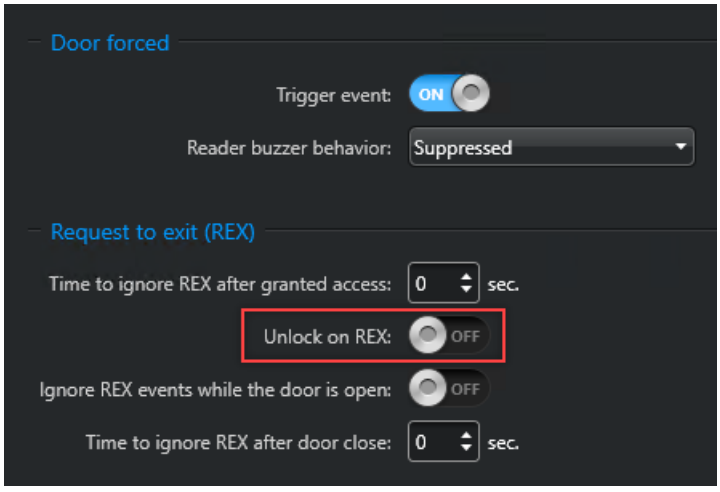
Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Vue secteur*.

2 Dans l'arborescence des entités, sélectionnez la porte équipée du verrou compatible Aperio.

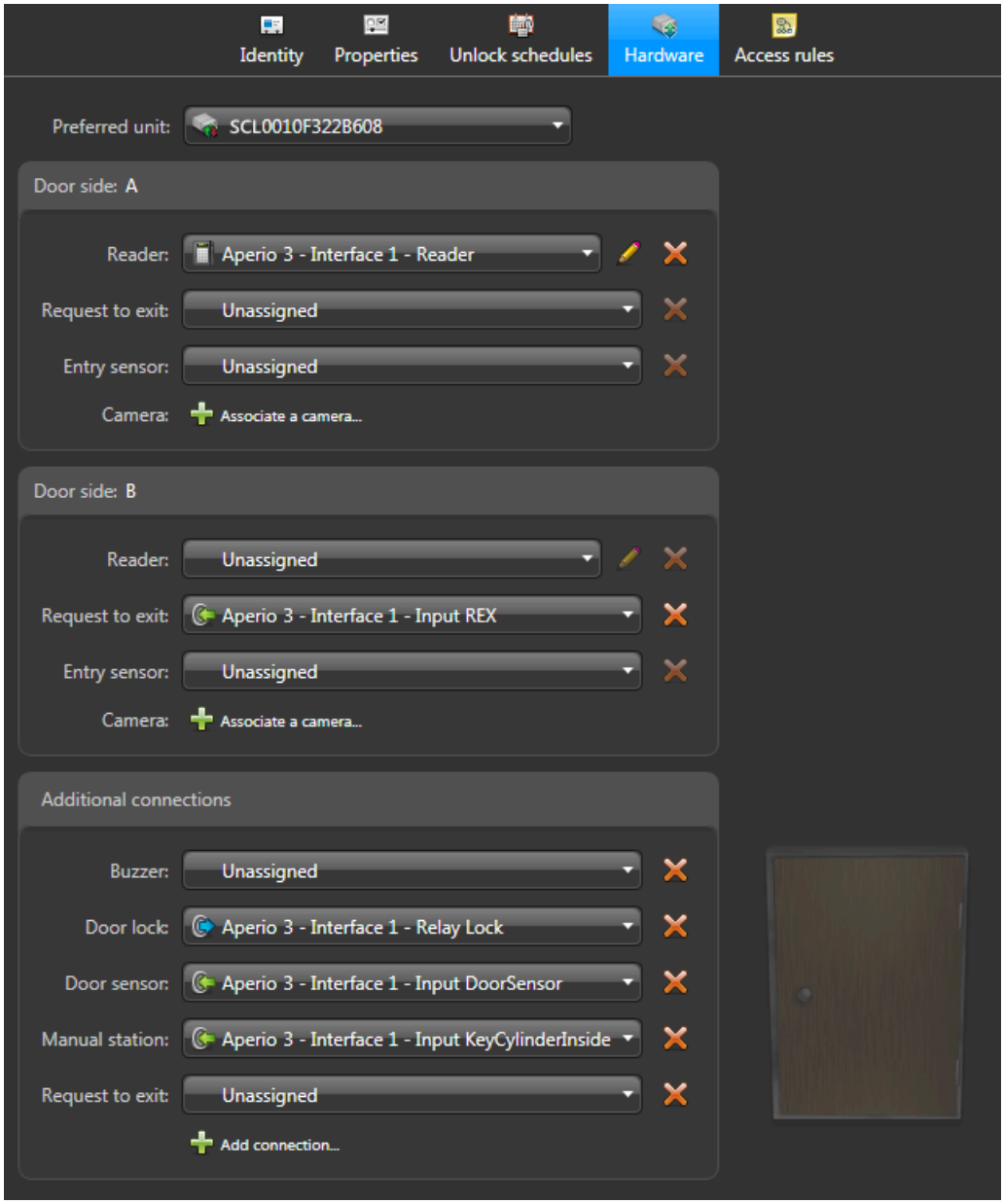
3 Cliquez sur l'onglet **Propriétés**.

4 Dans la section *Demande de passage (REX)*, désactivez l'option **Déverrouillage sur REX**.



5 Cliquez sur l'onglet **Matériel**, puis sélectionnez l'unité Synergis qui contrôle le verrou.

Tous les périphériques qui correspondent au même verrou ont le même préfixe « Aperio X - Interface n », où X correspond au numéro de canal (1 - 4) , et n correspond à l'adresse EAC du verrou.



6 Dans la section *Côté de porte (entrée)*, affectez le lecteur correspondant à la porte.

7 Dans la section *Côté sortie (sortie)* de la porte, affectez le capteur REX correspondant à la porte.

8 Dans la section *Connexions supplémentaires*, appliquez les réglages suivants :

- Affectez le relais de verrouillage à **Verrou**, et
- Affectez l'entrée du capteur de porte à **Capteur de contact**.
- Affectez *KeyCylinderInside* ou *KeyCylinderOutside* à **Station manuelle**, le cas échéant.

9 Si le lecteur doit fonctionner en mode *Carte et code PIN*, veillez à configurer un délai suffisamment long pour que le titulaire de cartes ait le temps de saisir le code.

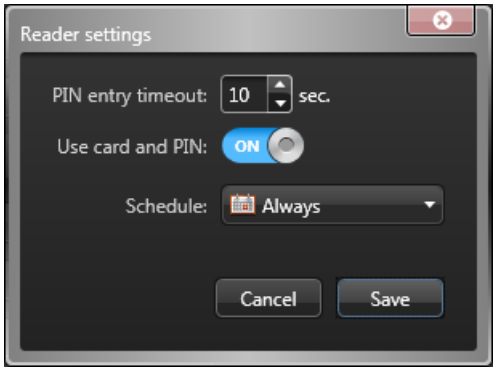
Le délai par défaut de 5 secondes est insuffisant pour les verrous Aperio. Une fois que le titulaire de cartes a présenté son identifiant à la porte, il doit attendre que le témoin DEL passe au vert avant de saisir son code. Ce processus prend systématiquement plus de 5 secondes.

a) Cliquez sur **Paramètres du lecteur** (🖉) en regard du **Lecteur**.

b) Dans la boîte de dialogue *Paramètres du lecteur*, activez l'option **Utiliser la carte et le code PIN**.

c) Modifiez le **Délai de saisie de code PIN**.

Nous recommandons 10 secondes.



d) Cliquez sur **Enregistrer**.

10 Cliquez sur **Appliquer**.

6

Verrous IP Assa Abloy

Cette section aborde les sujets suivants:

Présentation de la configuration des verrous IP Assa Abloy

Pour configurer le fonctionnement des verrous IP Assa Abloy avec une unité Synergis[MC], vous devez d'abord configurer les verrous avec l'outil Lock Configuration Tool (LCT), puis associer les verrous à l'unité Synergis à l'aide de Synergis[MC] Appliance Portal.

Le tableau suivant résume le processus de configuration du verrou IP.

Phase	Description	Voir
1	Vérifiez que le micrologiciel du verrou IP est à jour et pris en charge par votre version de Synergis[MC] Softwire.	• *Guide de démarrage rapide de l'installation des verrous IP* livré avec le verrou. • « Verrous IP Assa Abloy pris en charge » dans le *Guide d'intégration Synergis[MC] Softwire* .
2	Configurez le verrou IP avec l'outil LCT. • Configurez l'adresse d'hôte sur le verrou IP pour qu'elle corresponde à l'adresse IP de l'unité Synergis. • Configurez le port de communication du verrou IP qui sera utilisé par l'unité Synergis en tant que port de découverte pour la détection des verrous (par défaut=2571). • Si le chiffrement est nécessaire, configurez la clé AES dans le profil du verrou. Vous aurez besoin de cette clé après avoir associé le verrou IP à l'unité Synergis.	• *Le manuel Network & Lock Configuration Tool User Manual* fourni avec votre verrou.
3	Établissez la communication entre l'unité Synergis et les verrous IP connectés sur le Synergis[MC] Appliance Portal.	• Inscription de verrous IP Assa Abloy connectés à l'unité Synergis, page 93.

À propos de la fonctionnalité événements Réveil par radio des verrous Assa Abloy WiFi

Événements de réveil par radio est une fonctionnalité de tous les verrous Assa Abloy WiFi qui permet de sélectionner les événements que les verrous doivent immédiatement signaler par connexion WiFi.

Fonctionnement

Par défaut, les événements *Porte forcée* et *Porte entrebâillée trop longtemps* réveillent la radio WiFi du verrou pour signaler ces événements lorsqu'ils surviennent. Utilisez l'option **Événements de réveil** sur chaque verrou individuel pour sélectionner les événements qui activent la radio WiFi. Les événements qui ne sont pas sélectionnés pour réveiller la radio WiFi sont signalés lors du réveil suivant de la radio WiFi.

Limiter l'utilisation de la batterie sur les verrous WiFi

Dans le cadre de certaines installations, l'autonomie des verrous peut être raccourcie par les nombreux événements *Porte tenue ouverte* qui réveillent la radio WiFi. Leur autonomie peut être prolongée s'il est acceptable de signaler les événements *Porte tenue ouverte* lors du réveil planifié suivant de la radio. Pour prolonger l'autonomie, ne réglez l'option **Événements de réveil** que sur *Porte forcée*. Les événements *Porte forcée* réveillent alors la radio WiFi tandis que les événements *Porte tenue ouverte* sont rapportés lors du réveil suivant de la radio WiFi.

Configurer la fonctionnalité événements Réveil par radio des verrous Assa Abloy WiFi

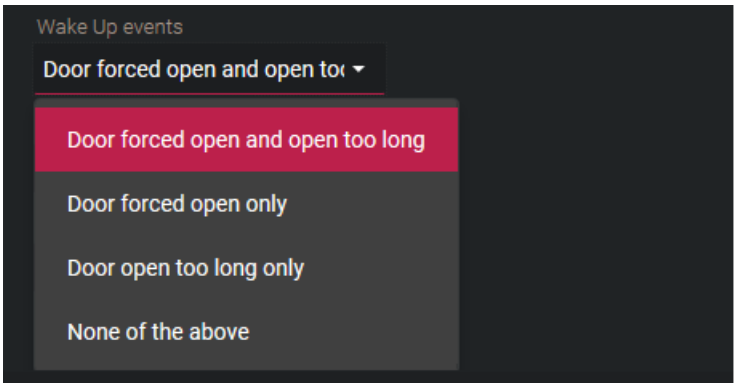
Vous pouvez configurer les verrous Assa Abloy WiFi individuels pour qu'ils contactent le contrôleur par radio WiFi en cas d'événements de réveil particuliers.

Avant de commencer

Inscrivez le verrou Assa Abloy IP.

À savoir

Vous pouvez configurer un Événement de réveil pour chaque verrou Assa Abloy WiFi.



Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.
2 Cliquez sur **Configuration** > **Matériel**.
3 Sélectionnez **Assa Abloy IP**, puis sélectionnez le canal et le verrou Assa Abloy.
4 Réglez l'option **Événements de réveil** pour le verrou.
5 Cliquez sur **Appliquer**.

Activer le mode fuite et retour sur les verrous IP Assa Abloy de type 8200 avec pêne dormant surveillé

Pour activer le *mode fuite et retour* sur les portes contrôlées par des verrous IP Assa Abloy, vous devez créer un champ personnalisé booléen nommé Escape Return pour les portes, et le régler sur VRAI pour les portes pour lesquelles vous souhaitez activer cette fonctionnalité.

Avant de commencer

Les verrous IP Assa Abloy qui prennent en charge la fonctionnalité *fuite et retour* sont les modèles au format de type 8200 avec pêne dormant surveillé.

Exemple :

- Verrous encastrés IN120 et IN220 8200 avec pêne dormant. Aucun autre verrou IN120 ou IN220 ne prend en charge cette fonctionnalité.
- Verrou encastré Passport 1000 P2 avec pêne dormant. Aucun autre verrou Passport 1000 P2 ne prend en charge cette fonctionnalité.

À savoir

Le code de prévention des incendies au Canada stipule qu'une porte ne doit jamais se reverrouiller automatiquement. Dès lors, lorsque la fonctionnalité fuite et retour est activée, les fonctionnalités suivantes sont désactivées.

- Horaires de déverrouillage
- Mode maintenance
- Déverrouillage manuel depuis Security Desk
- Contourner temporairement les horaires de Security Desk

Lorsque la fonctionnalité de fuite et retour est activée et qu'un titulaire de cartes sort par une porte, la porte reste déverrouillée après fermeture jusqu'à ce que le titulaire présente sa carte d'accès pour verrouiller la porte. Si le titulaire de cartes ne présente pas sa carte pour verrouiller la porte, celle-ci reste déverrouillée en son absence. Lorsque le titulaire de cartes revient, il doit présenter sa carte d'accès pour ouvrir la porte. Une fois à l'intérieur, il doit actionner le pêne dormant pour verrouiller la porte.

Procédure

1 Créez un champ personnalisé de type booléen pour les entités portes, et nommez-le Escape Return.

Respectez scrupuleusement cette orthographe, y compris les majuscules et minuscules, sans oublier l'espace.

2 Ouvrez la tâche *Vue secteur* et réglez le champ personnalisé **Escape Return** sur VRAI pour toutes les portes pour lesquelles vous souhaitez activer cette fonctionnalité.

CONSEIL : Si vous voulez activer cette fonctionnalité sur de nombreuses portes, nous vous conseillons d'utiliser l'*Outil Copie de configuration*.

3 (Verrous WiFi seulement) Déclenchez un réveil par radio pour activer la fonctionnalité fuite et retour sur le verrou.

Vous pouvez déclencher un réveil par radio en ouvrant le boîtier et en appuyant sur le bouton, ou en présentant un identifiant refusé.

4 Effectuez les tâches du cycle du *mode fuite et retour* une première fois en sortant par une porte, puis en présentant un identifiant valable après sa fermeture.

Le système crée alors les événements personnalisés que vous pouvez utiliser pour configurer les associations événement-action.

Deux événements personnalisés sont ajoutés à votre système :

- **Escape Return Mode Start (Début du mode fuite et retour) :** Porte déverrouillée en sortant ou en entrant avec un identifiant valable.
- **Escape Return Mode End (Fin du mode fuite et retour) :** Porte verrouillée avec un identifiant valable ou en actionnant le pêne dormant de l'intérieur.

Configurer un numéro de série Persona pour les verrous IN120 et IN220

Pour pouvoir utiliser le mode passage sur les verrous SARGENT et Corbin Russwin Cx IN120 et IN220, vous devez les configurer avec un numéro de série PERSONA.

Procédure

1 Connectez le verrou à un poste de travail, puis ouvrez le fichier de configuration du verrou avec l'outil LCT.

2 Sur la page *Configuration du verrou*, cliquez sur l'icône **Réglages**.

3 Cliquez sur l'onglet **Serial Number Setup** (Configuration du numéro de série).

4 Réglez **Manufacturer** (Fabricant) et **Board Type** (Type de carte) sur *Persona*.

5 Appliquez les modifications et suivez les instructions à l'écran.
Le verrou est à présent doté d'un nouveau numéro de série.

6 Avec LCT, appliquez à nouveau la configuration au verrou.

7 Si le verrou a déjà été ajouté à l'unité Synergis[MC], procédez de la manière suivante :
   a) Supprimez le verrou puis ajoutez-le à nouveau avec le nouveau numéro de série.
   b) Reconfigurez l'entité porte matérielle avec le nouveau verrou.

À propos du mode passage pour les verrous IP Assa Abloy

Le mode passage est une fonctionnalité disponible sur tous les verrous IP Assa Abloy. Elle permet aux titulaires de cartes autorisés à garder les verrous en état déverrouillé en passant leur badge une ou deux fois sur le lecteur, selon le modèle et la marque du contrôleur. La même procédure rétablit l'état normal du verrou.

Mode passage déclenché par un seul balayage

Ce qui suit concerne les verrous SARGENT Cx, les verrous Corbin Russwin Cx IN120 et IN220 et tous les verrous Sx.Lorsque le lecteur est en mode *Carte ou code PIN* ou *Carte et code PIN*, le mode passage est activé et désactivé des manières suivantes :

- **Carte ou code PIN :** Passez le badge une fois ou entrez le code PIN.
- **Carte et code PIN :** Passez d'abord le badge, puis entrez le code PIN.

REMARQUE : Les titulaires de cartes doivent avoir un niveau d'accès supérieur à 7.

Mode passage déclenché par un double balayage

Les informations suivantes concernent des verrous particuliers :

- Tous les verrous Px
- Verrous Sx exécutant le micrologiciel Hx
- Verrous SARGENT Cx Passport 1000 P1 et P2
- Verrous Corbin Russwin Cx Access 700 PIP1 et PWI1
- Verrous SARGENT et Corbin Russwin Cx IN120 et IN220 avec un numéro de série PERSONA

REMARQUE : Les verrous IN120 et IN220 peuvent être commandés ou configurés manuellement.

- **Carte ou code PIN :** Passez le badge deux fois pour lancer le mode passage. Le code PIN ne peut pas être utilisé.
- **Carte et code PIN :** Passez le badge une fois, entrez le code PIN, puis badgez une deuxième fois pour lancer le mode passage.

Mode passage activé par porte ou par règle d'accès

Vous pouvez activer la fonctionnalité mode passage en utilisant un champ personnalisé de porte ou de règle d'accès. L'utilisation des deux champs personnalisés à la fois est déconseillée. Lorsque le mode passage est activé via un champ personnalisé de porte, quiconque a accès à la porte peut utiliser le mode passage. Lorsque le mode passage est activé via un champ personnalisé de règle d'accès, vous pouvez restreindre la fonction à certaines portes et certains titulaires de cartes.

Activer le mode passage des verrous IP Assa Abloy

Pour activer le mode passage sur les portes contrôlées par des verrous IP Assa Abloy, vous devez créer un champ personnalisé booléen intitulé *PassageMode* pour les portes ou pour les règles d'accès.

Avant de commencer

- En savoir plus sur le mode passage.
- Configurez un numéro de série Persona pour les verrous IN120 et IN220.

Procédure

Pour activer la fonctionnalité mode passage par porte :

1 Dans Config Tool, créez un champ personnalisé de type booléen pour les entités porte, et nommez-le `PassageMode`.

REMARQUE : Respectez scrupuleusement cette orthographe, y compris les majuscules et minuscules.

2 Ouvrez la tâche *Vue secteur*.

3 Depuis le navigateur d'entités, sélectionnez une porte, puis cliquez sur l'onglet **Champs personnalisés**.

4 Sélectionnez le champ personnalisé **PassageMode**, puis cliquez sur **Appliquer**.

5 Répétez les deux étapes précédentes pour toutes les portes pour lesquelles vous souhaitez activer le mode passage.

Pour activer la fonctionnalité mode passage par règle d'accès :

1 Connectez-vous à l'unité Synergis[MC].

2 Cliquez sur **Configuration** > **Réglages des contrôleurs en aval**.

3 Dans la section *Réglages des verrous IP Assa Abloy*, sélectionnez l'option **Activer le mode passage par règle d'accès**.

4 Cliquez sur **Enregistrer**.

5 Redémarrez votre unité Synergis.

Le champ personnalisé *PassageMode* pour les règles d'accès est créé automatiquement dans Security Center.

6 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Règles d'accès**.

7 Depuis le navigateur d'entités, sélectionnez une règle d'accès, puis cliquez sur l'onglet **Champs personnalisés**.

8 Sélectionnez le champ personnalisé **PassageMode**, puis cliquez sur **Appliquer**.

9 Répétez les deux étapes précédentes pour toutes les règles d'accès pour lesquelles vous souhaitez activer le mode passage.

Activer le mode confidentialité sur les verrous IP Assa Abloy sans pêne dormant surveillé

Pour activer le *mode confidentialité* depuis Config Tool sur les portes contrôlées par des verrous IP Assa Abloy, vous devez créer un champ personnalisé booléen nommé Privacy Mode pour les portes, et le régler sur VRAI pour les portes pour lesquelles vous souhaitez activer cette fonctionnalité.

Avant de commencer

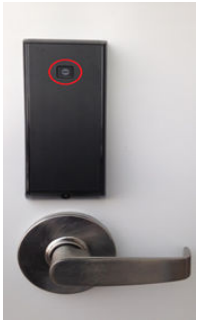
Les verrous IP Assa Abloy qui prennent en charge le mode confidentialité sont les verrous PoE et WiFi de type Cx.

À savoir

Le mode confidentialité est une fonctionnalité des verrous IP Assa Abloy qui n'accorde l'accès qu'aux superviseurs (*ignorer les titulaires de cartes*). Cette option est désactivée par défaut.

Les informations suivantes présentent le fonctionnement de cette option. Pour activer le mode confidentialité, appuyez sur le *bouton confidentialité* situé sur le côté intérieur de la porte lorsqu'elle est fermée. Le témoin DEL sur le bouton clignote lentement pendant environ 2 minutes pour indiquer que le mode confidentialité est en vigueur. Cette action correspond à l'activation du pêne dormant sur les verrous équipés d'un pêne dormant surveillé.

REMARQUE : Si le lecteur émet un bip et clignote cinq fois en violet lorsque vous appuyez sur le *bouton confidentialité*, le mode confidentialité ne peut pas être activé car la porte est ouverte.



Tous les titulaires de cartes avec une valeur de niveau d'accès inférieure à sept opèrent en tant que superviseurs. Le mode confidentialité est désactivé lorsque la porte est ouverte de l'intérieur, ou lorsqu'un superviseur entre avec son badge.

Procédure

1 Créez un champ personnalisé de type booléen pour les entités portes, et nommez-le Privacy Mode.

Respectez scrupuleusement cette orthographe, y compris les majuscules et minuscules, sans oublier l'espace.

2 Ouvrez la tâche *Vue secteur* et réglez le champ personnalisé **Privacy Mode** sur VRAI pour toutes les portes pour lesquelles vous souhaitez activer cette fonctionnalité.

CONSEIL : Si vous voulez activer cette fonctionnalité sur de nombreuses portes, nous vous conseillons d'utiliser l'*Outil Copie de configuration*.

Deux événements personnalisés sont ajoutés à votre système :

- **Pêne dormant engagé :** Cet événement est déclenché lorsque le mode confidentialité est activé sur une porte

- **Pêne dormant rétracté :** Cet événement est déclenché lorsque le mode confidentialité est désactivé sur une porte

Inscription de verrous IP Assa Abloy connectés à l'unité Synergis

Pour que l'unité Synergis[MC] puisse communiquer avec les verrous IP Assa Abloy connectés, vous devez les associer sur le Synergis[MC] Appliance Portal en utilisant le *mode jumelage de verrous*.

Avant de commencer

Configurez les verrous IP avec l'outil Lock Configuration Tool (LCT). Si le chiffrement est activé, notez la valeur de clé **Lock AES Key**.

À savoir

Pendant que le mode association de verrous est actif, tous les verrous IP connectés à l'unité Synergis sur les ports de communication spécifiés sont détectés. Une fois le jumelage terminé, l'unité Synergis se reconnecte au Gestionnaire d'accès dans Security Center et ajoute les verrous IP jumelés.

REMARQUE : Les étapes et instructions de *Renforcement* sont facultatives, mais protègent votre système contre les cyberattaques.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

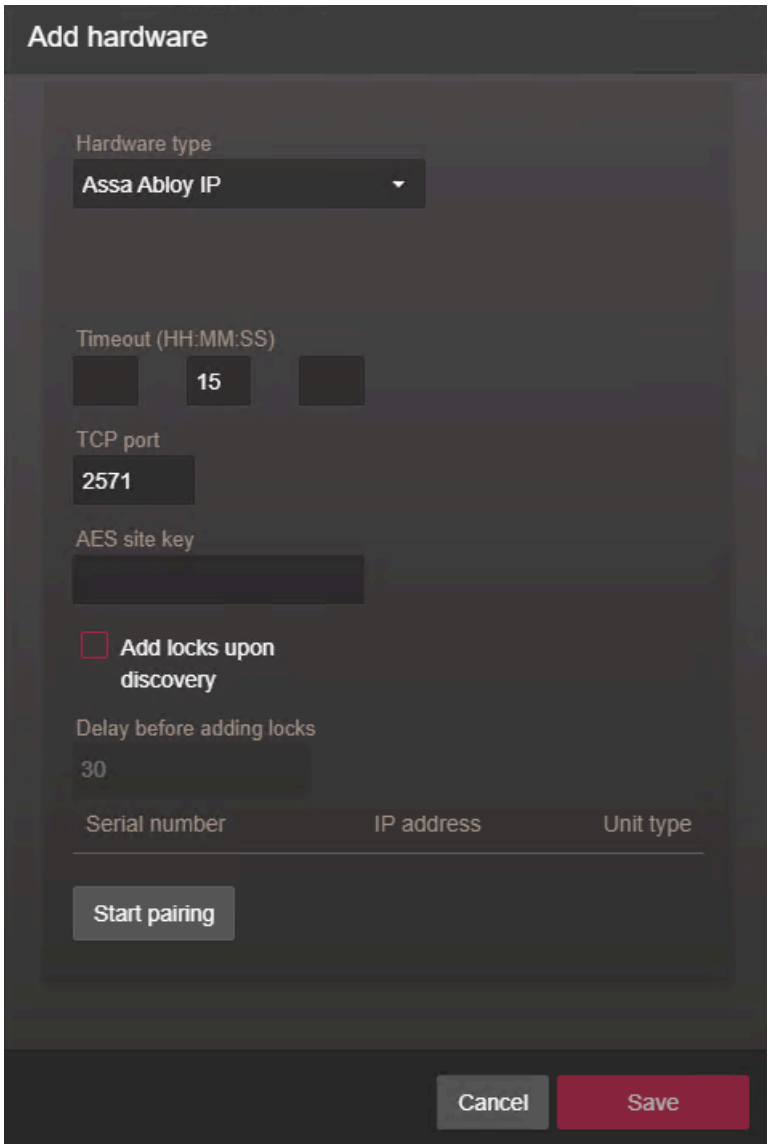
2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** ( ).

4 Dans la liste **Type de matériel**, sélectionnez **Assa Abloy IP**.

5 (Facultatif) Dans le champ **Délai d'expiration**, sélectionnez la durée d'activation du mode association de verrous. Les connexions aux nouveaux verrous IP ne sont associées que durant le laps de temps spécifié.

REMARQUE : Sauvegardez le fichier de configuration de l'unité Synergis au cas où vous auriez besoin de remplacer l'appareil à un moment donné, surtout si vous avez plusieurs verrous WiFi, car ils sont plus longs à réinscrire.



6 Si vous utilisez un port autre que le port 2571 par défaut, dans la boîte de dialogue *Port TCP*, tapez le numéro du port de communication que vous avez configuré sur les verrous IP.

7 Si vous avez activé le chiffrement via LCT, dans le champ *Clé AES du site*, tapez la clé AES (chaîne hexadécimale de 32 caractères) configurée pour votre verrou.

REMARQUE : Vous pouvez modifier ou supprimer la clé AES sur la page *Matériel* de l'unité Synergis dans Config Tool.

8 (Facultatif) Si vous souhaitez que les verrous IP soient ajoutés lorsqu'ils sont découverts, procédez de la manière suivante :

a) Sélectionnez l'option **Ajouter les verrous découverts**.

IMPORTANT : Lorsque cette option est sélectionnée, l'unité Synergis se reconnecte au Gestionnaire d'accès après l'ajout de chaque groupe de verrous IP. Cette option n'est conseillée que si vous devez lancer la configuration des verrous IP avant que le mode association soit terminé.

b) Dans l'option **Délai avant l'ajout des verrous**, sélectionnez le nombre de secondes qui doivent s'écouler avant que les verrous déjà découverts soient ajoutés.

9 Cliquez sur **Démarrer l'association**.

IMPORTANT : Pour les verrous WiFi, appuyez sur le bouton COM ou Reset à l'arrière du verrou pour déclencher la connexion à l'unité Synergis.

Les verrous IP sont détectés et ajoutés au tableau.

Si vous rencontrez des problèmes de jumelage du verrou à l'unité Synergis, testez la connexion entre le verrou IP et l'unité.

10 Procédez de l'une des manières suivantes :

- Pour arrêter le mode association de verrous et ajouter les verrous détectés, cliquez sur **Arrêter et enregistrer**.
- Pour annuler le mode association de verrous, cliquez sur **Annuler**.

  REMARQUE : Si l'option **Ajouter les verrous découverts** est sélectionnée, certains verrous auront parfois déjà été ajoutés.
- Patientez jusqu'à l'expiration du mode association de verrous.

L'unité Synergis se reconnecte au rôle Gestionnaire d'accès, et les verrous découverts sont ajoutés.

11 Cliquez sur **Configuration** > **Matériel**.

Les verrous IP ajoutés apparaissent dans l'arborescence de configuration matérielle. Lorsque vous sélectionnez un verrou, le type d'unité, le numéro de série et l'adresse IP du verrou IP sélectionné sont affichés sous *Propriétés*.

12 En l'absence d'informations sous *Propriétés*, actualisez la page.

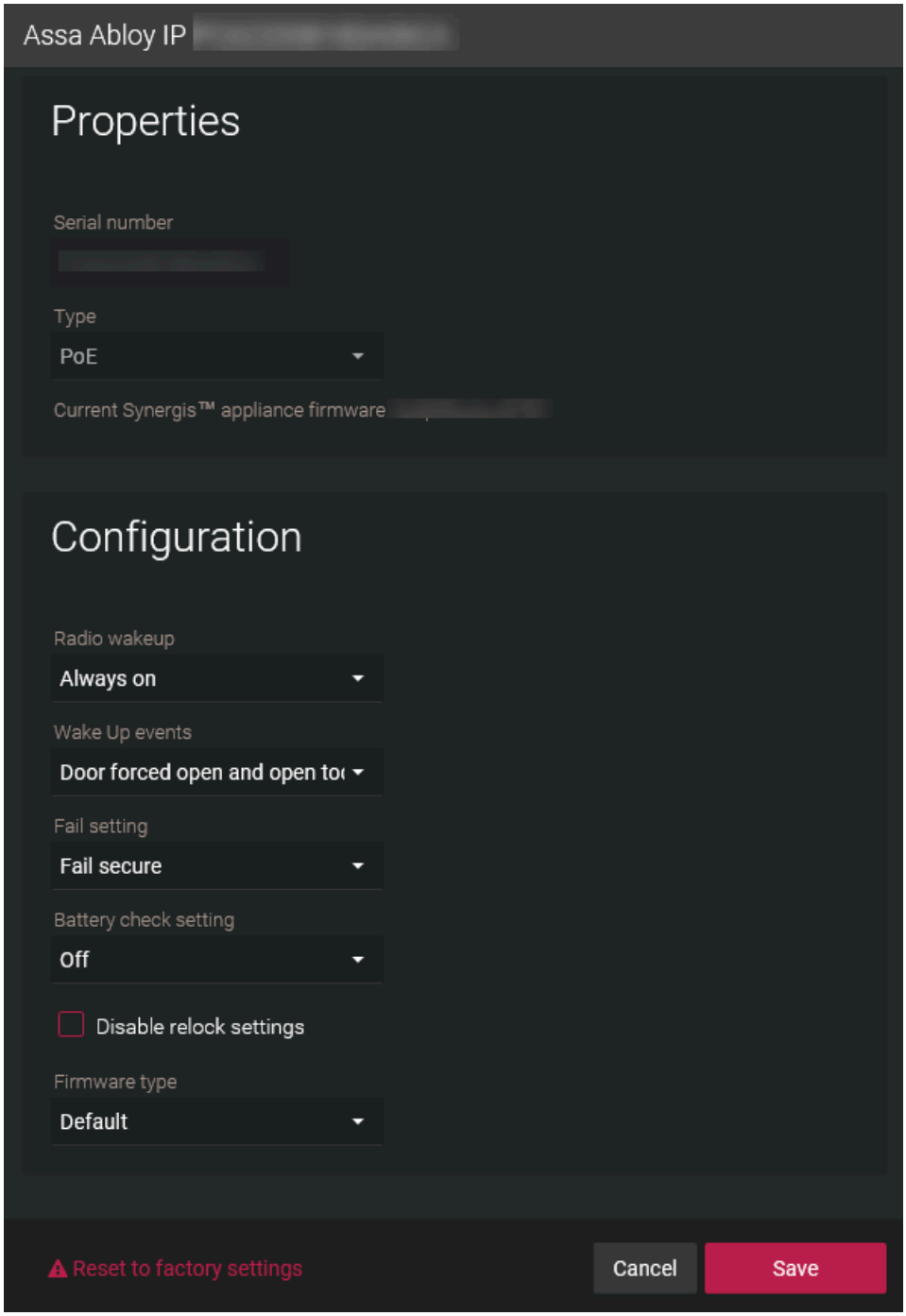
Pour les verrous Wi-Fi, il peut s'écouler jusqu'à 2 minutes avant que les informations soient affichées sous *Propriétés*. Les verrous WiFi sont affichés en rouge dans l'arborescence matérielle, car ils ne sont pas connectés en permanence à l'unité Synergis.

a) Pour les verrous PoE : Sous *Propriétés*, vérifiez que l'option **Réveil par radio** est réglée sur **Toujours activé** afin qu'aucun événement *Accès accordé* ne soit manqué dans Security Desk, et réglez **Vérification de la batterie** sur **Désactivé**.

b) Pour les verrous WiFi : Sous *Propriétés*, vérifiez que **Réveil par radio** est réglé sur **Tous les jours**, et entrez l'horaire (**Heure** et **Minute**) souhaité.

Sélectionnez **Heure locale** si vous voulez que l'heure du réveil par radio tienne compte du fuseau horaire de l'unité Synergis. Si vous ne sélectionnez pas cette option, la valeur UTC est utilisée par défaut.

c) Modifiez les autres réglages de verrous selon vos besoins.



13 Cliquez sur **Enregistrer**.

Tester la connexion entre le verrou IP et l'unité Synergis

Si vous rencontrez des problèmes d'association de l'unité Synergis[MC] et du verrou IP, vous pouvez tester la connexion entre le verrou et l'unité à l'aide de l'outil Lock Configuration Tool (LCT).

Procédure

1 Pour les verrous PoE, reportez-vous à la commande **Ping Test** dans LCT.
2 Pour les verrous Wi-Fi, reportez-vous à la commande **Verify Connection to Host** dans LCT.

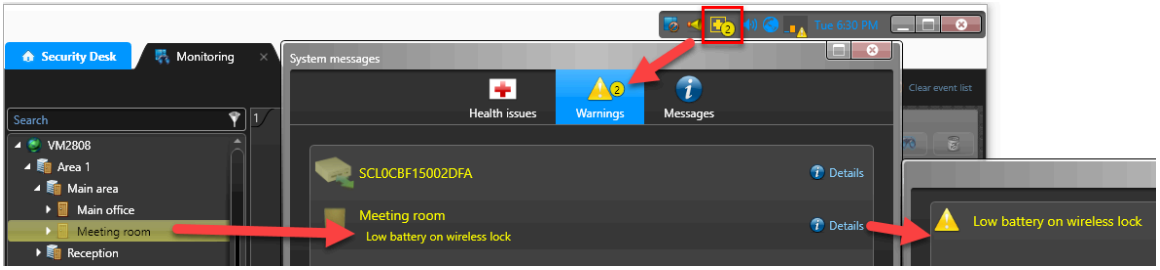
Vérifier l’état de la batterie des verrous Wi-Fi

Pour vérifier l’état de la batterie d’un verrou IP WiFi Assa Abloy, vous pouvez surveiller l’événement *Panne de batterie* sur l’unité Synergis[MC] à laquelle le verrou est connecté.

À savoir

Pour chaque verrou WiFi, Security Center crée une entrée virtuelle appelée *Input BatteryFail* qui indique *Actif* dans l’onglet **Surveillance** et qui est affiché avec une alerte jaune sur l’icône **Messages système** dans la zone de notification lorsque la batterie est faible.

REMARQUE : *Input BatteryFail* est une entrée logicielle créée pour indiquer l’état de la batterie des verrous Wi-Fi. Vous ne pouvez pas connecter d’appareils physiques à cette entrée.



Procédure

1 Sur la page d’accueil de Security Desk, ouvrez la tâche *État du système*.

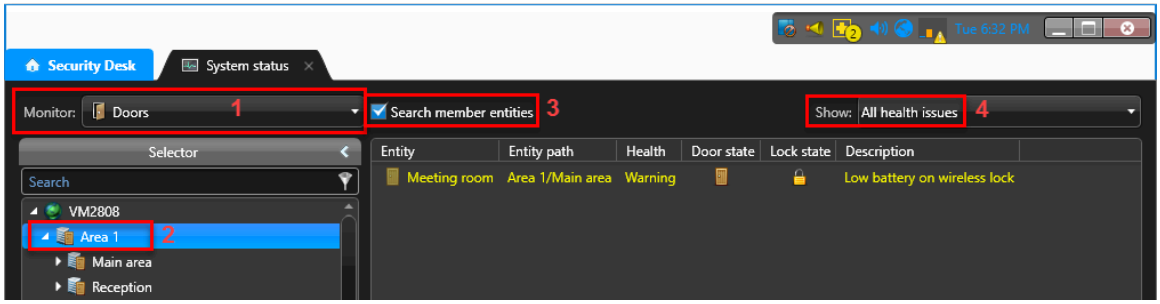
2 Dans la liste **Surveillance**, sélectionnez **Portes**.

3 Dans l’arborescence des entités, sélectionnez le secteur parent.

4 Cochez la case **Rechercher les entités membres** pour afficher tous les verrous dans les sous-secteurs.

5 Dans la liste **Afficher**, sélectionnez **Tous les dysfonctionnements** pour afficher les portes avec avertissements.

REMARQUE : L’entrée **Input BatteryFailed** indique *Actif* pour les verrous Wi-Fi qui ont un problème de batterie.



6 Prévoyez le remplacement de la batterie des verrous WiFi qui affichent l’avertissement de batterie faible.

7

Caméras AutoVu SharpV

Cette section aborde les sujets suivants:

Inscription de caméras AutoVu SharpV sur l'unité Synergis

Pour que l'unité Synergis[MC] puisse communiquer avec la caméra SharpV, vous devez inscrire la caméra auprès de l'unité Synergis dans Security Center.

Avant de commencer

- Configurez la caméra SharpV pour utiliser la communication HTTPS. Pour en savoir plus, voir le *Guide de déploiement* ou le *Manuel* de la caméra que vous installez.
- Installez le certificat auto-signé Genetec[MC] ou un certificat signé par une autorité de certification de confiance.
- Si vous inscrivez une caméra SharpV, connectez-vous au portail Web de la SharpV et modifiez le mot de passe par défaut.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** ( ).

4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **AutoVu** dans la liste **Type de matériel**.

5 Sélectionnez un **Canal**.

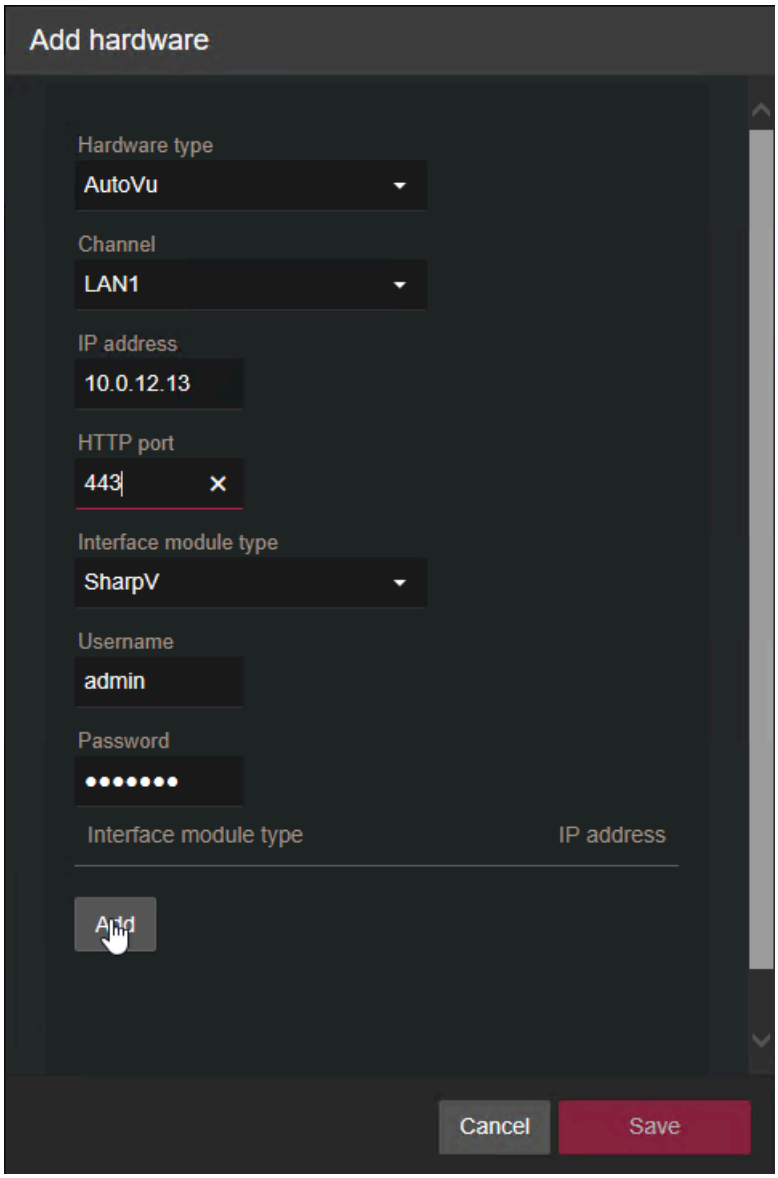
6 Entrez l'**adresse IP** de la caméra.

7 Saisissez le **Port** de la caméra.
La SharpV utilise le **Port** 443 pour la communication HTTPS avec Security Center.

8 Dans la liste **Type de module d'interface**, sélectionnez **SharpV**.

9 Entrez le **Nom d'utilisateur** et **Mot de passe** qui sert à accéder au portail Web SharpV.
REMARQUE : Pour les caméras SharpV, vous ne pouvez pas utiliser le mot de passe par défaut.

10 Cliquez sur **Ajouter**, puis sur **Enregistrer**.



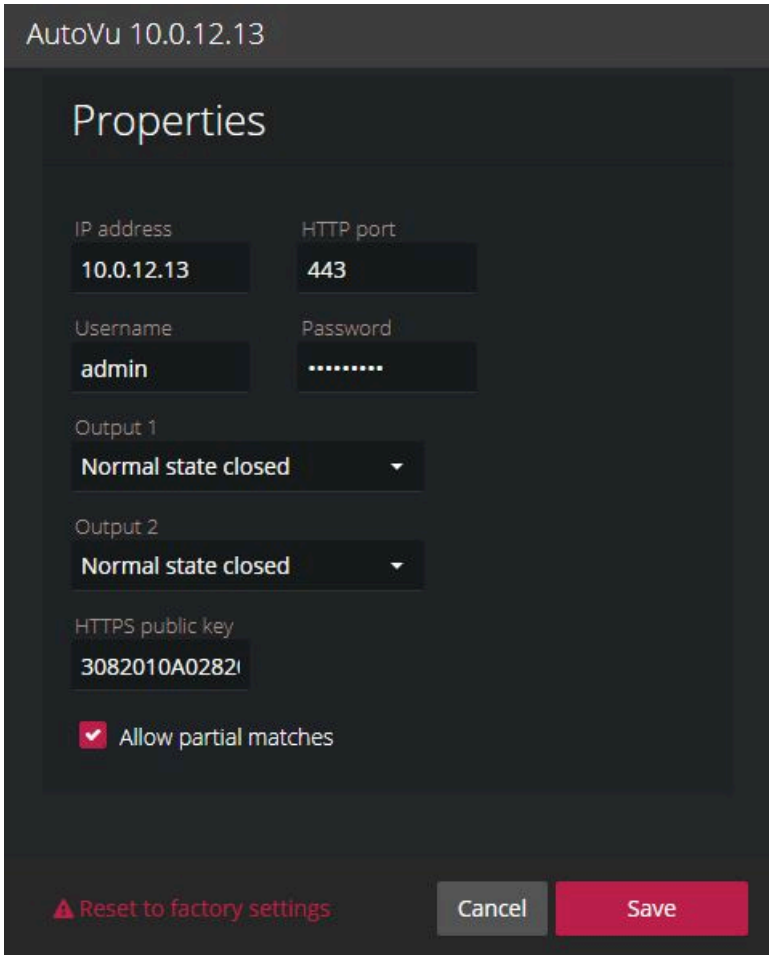
11 Sur la page *Configuration matérielle*, cliquez sur la caméra AutoVu[MC] inscrite, puis cliquez sur son canal et son interface pour afficher ses propriétés.

12 Si vous utilisez les sorties de la SharpV pour contrôler une barrière d'accès pour véhicules, sélectionnez *Normalement ouvert* ou *Normalement fermé* pour les sorties.

13 Laissez le champ **Clé publique HTTPS** vide. Cette information est ajoutée automatiquement en fonction du certificat de la caméra.

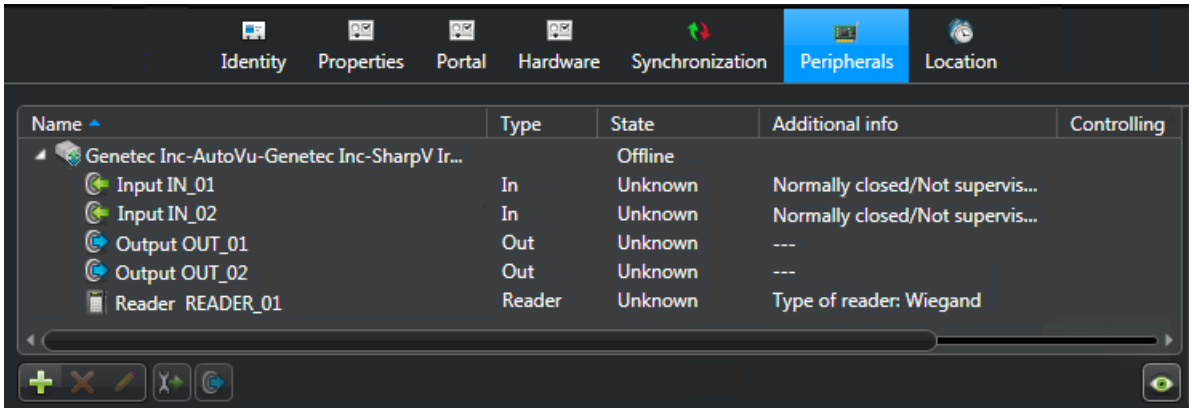
14 La case **Autoriser les correspondances partielles** est cochée par défaut. Cette fonctionnalité accepte les lectures de plaques avec une différence d'un caractère avec un identifiant de plaque d'immatriculation configuré. Il peut s'agir de l'insertion, de la suppression ou de la suppression d'un seul caractère,

n'importe où dans le numéro de plaque. Lorsque cette fonctionnalité est activée, les lectures de plaques sales ou endommagées sont plus susceptibles d'être acceptées.



15 Cliquez sur **Enregistrer**.

Dans Config Tool, la caméra SharpV est affichée sur la page *Périphériques* de l'unité Synergis, et les entrées et sorties sont affichées sous la caméra SharpV.



Configuration d'une caméra SharpV pour contrôler une barrière d'accès pour véhicules

Pour utiliser une caméra SharpV pour contrôler une barrière d'accès pour véhicules, la barrière doit être configurée en tant que porte dans Security Center.

Avant de commencer

- Connectez physiquement la barrière à l'appareil Synergis[MC]. Pour en savoir plus, voir le *Guide d'installation matérielle* de l'appareil de contrôle d'accès que vous installez.
- Inscrivez l'unité Synergis dans Security Center.
- Inscrivez la caméra SharpV sur l'unité Synergis.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Vue secteur*.

2 Sélectionnez le secteur auquel vous souhaitez ajouter la barrière.

3 Cliquez sur **Ajouter une entité** (), et sélectionnez **Porte**.

4 Dans l'assistant **Création d'une porte**, entrez le nom et la description de la barrière d'accès pour véhicules.

5 Dans la liste **Emplacement**, sélectionnez le secteur dans lequel la porte sera créée, puis cliquez sur **Suivant**.

6 Sur la page *Informations sur la porte*, affectez des noms aux côtés de porte.

Exemple: Entrée/sortie.

7 Pour associer la barrière à l'unité de contrôle d'accès sur laquelle elle est câblée :

a) Dans la liste **Unité de contrôle d'accès**, sélectionnez l'unité Synergis.

b) Dans la liste **Module d'interface**, sélectionnez la caméra SharpV.

8 Cliquez sur **Suivant**.

9 Examinez la page *Résumé de l'opération* , et cliquez sur **Créer** > **Fermer.**

La barrière est affichée dans l'arborescence des entités.

10 Sélectionnez la barrière et cliquez sur l'onglet **Propriétés**.

11 Configurez le comportement de contrôle d'accès général de la barrière. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*.

12 Cliquez sur **Appliquer**.

13 Cliquez sur l'onglet **Matériel** et décrivez le câblage entre l'unité de contrôle d'accès et la barrière à Security Center. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*.

14 Créez des titulaires de cartes en utilisant leur plaque d'immatriculation en tant qu'identifiant. Pour en savoir plus sur la création de titulaires de cartes, voir le *Guide de l'utilisateur de Security Center*.

Lors de l'affectation d'identifiants aux titulaires de cartes, sélectionnez l'option **Plaque d'immatriculation**.

15 Sélectionnez les personnes qui ont accès à la porte. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*.

8

Contrôleurs Axis

Cette section aborde les sujets suivants:

Inscription de contrôleurs Mercury sur l'unité Synergis

Pour que l'unité Synergis[MC] puisse communiquer avec les contrôleurs Axis, vous devez inscrire les contrôleurs à l'aide du Synergis[MC] Appliance Portal ou de Config Tool.

Avant de commencer

- Munissez-vous du numéro de série ou de l'adresse IP de vos contrôleurs Axis. Consultez la documentation Axis pour trouver ces informations.
- Connectez vos contrôleurs Axis à l'unité Synergis.

À savoir

Lorsque l'unité Synergis inscrit un contrôleur, elle applique une configuration par défaut à tous les contacts d'entrée et relais de sortie Axis. Axis et Synergis utilisent une terminologie distincte pour décrire leurs paramètres.

REMARQUE : Seule l'inscription via le Synergis[MC] Appliance Portal est décrite ici, mais vous pouvez également inscrire un contrôleur Axis dans **Config Tool** > **Contrôle d'accès** > **Rôles et unités**.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

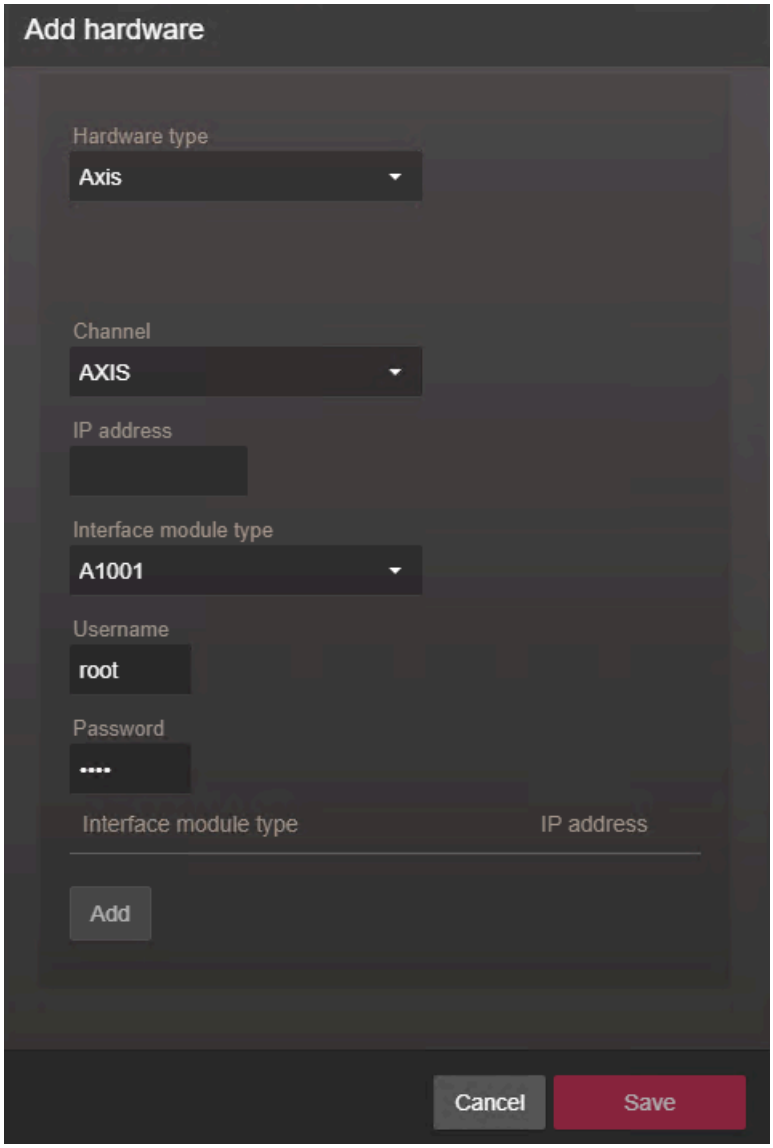
3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** (➕).

4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **Axis** sous **Type de matériel**.

5 Sélectionnez le canal IP où le contrôleur Axis est connecté.

6 Entrez les paramètres de connexion requis pour connecter le contrôleur Axis.

- **Adresse IP :** Utilisez l'adresse IP du contrôleur Axis.
- **Type de module d'interface :** Sélectionnez le type d'unité Axis que vous inscrivez. A1001 est la valeur par défaut.
- **Nom d'utilisateur et mot de passe :** Le nom d'utilisateur et le mot de passe par défaut sont `root` et `pass`.



7 Cliquez sur **Ajouter**.

8 Activez **Mode autonome** .

9 (Facultatif) Répétez les étapes 3 à 8 pour ajouter un autre contrôleur Axis.

10 Cliquez sur **Enregistrer**.

Le type de matériel, le canal et le module d'interface que vous venez d'ajouter sont affichés sur la page *Configuration matérielle*. Il peut falloir jusqu'à 1 minute pour que le module Axis se connecte en ligne.

11 Si vous n'avez pas la dernière version du micrologiciel, faites la mise à niveau de l'une des manières suivantes :

- Recommandé pour Security Center 5.10 ou version ultérieure : Mettez à jour le micrologiciel à l'aide de la tâche *Inventaire matériel* dans Config Tool. Pour en savoir plus, voir Mettre à niveau la plate-forme et le micrologiciel des unités de contrôle d'accès et le micrologiciel des modules d'interface.
- Mettez à jour le micrologiciel à l'aide du Synergis[MC] Appliance Portal.

12 Testez la connexion de votre module d'interface et votre configuration à partir de la page *Diagnostics d'E/S*.

REMARQUE : Pour utiliser le protocole HTTPS, le contrôleur AXIS A1001 doit utiliser le micrologiciel 1.65.2 ou ultérieur, et les interfaces A1601 doivent utiliser le micrologiciel 1.83.1.1 ou ultérieur.

Lorsque vous avez terminé

Ajoutez l'unité Synergis à un rôle Gestionnaire d'accès afin de l'intégrer à votre système Security Center.

Activer le mode autonome sur les contrôleurs Axis

Pour configurer vos unités Axis afin qu'elles prennent des décisions d'accès indépendamment d'une unité Synergis[MC], activez le *mode autonome* sur le Synergis[MC] Appliance Portal.

À savoir

En situation de latence élevée, le *Mode autonome* améliore le délai entre la lecture d'une carte et l'événement *Porte déverrouillée* en désactivant l'autorisation à distance. L'unité Axis envoie l'information à l'unité Synergis après la prise de décision.

REMARQUE : Puisque le *Mode autonome* ne contacte pas l'unité Synergis pour les décisions de contrôle d'accès, l'utilisation de ce mode implique certaines limitations :

- Les fonctionnalités avancées de Security Center sont désactivées.
- La modification des identifiants, comme la révocation d'un accès, prennent plus longtemps à appliquer, puisqu'elles doivent être transmises à l'unité Axis pendant la synchronisation.

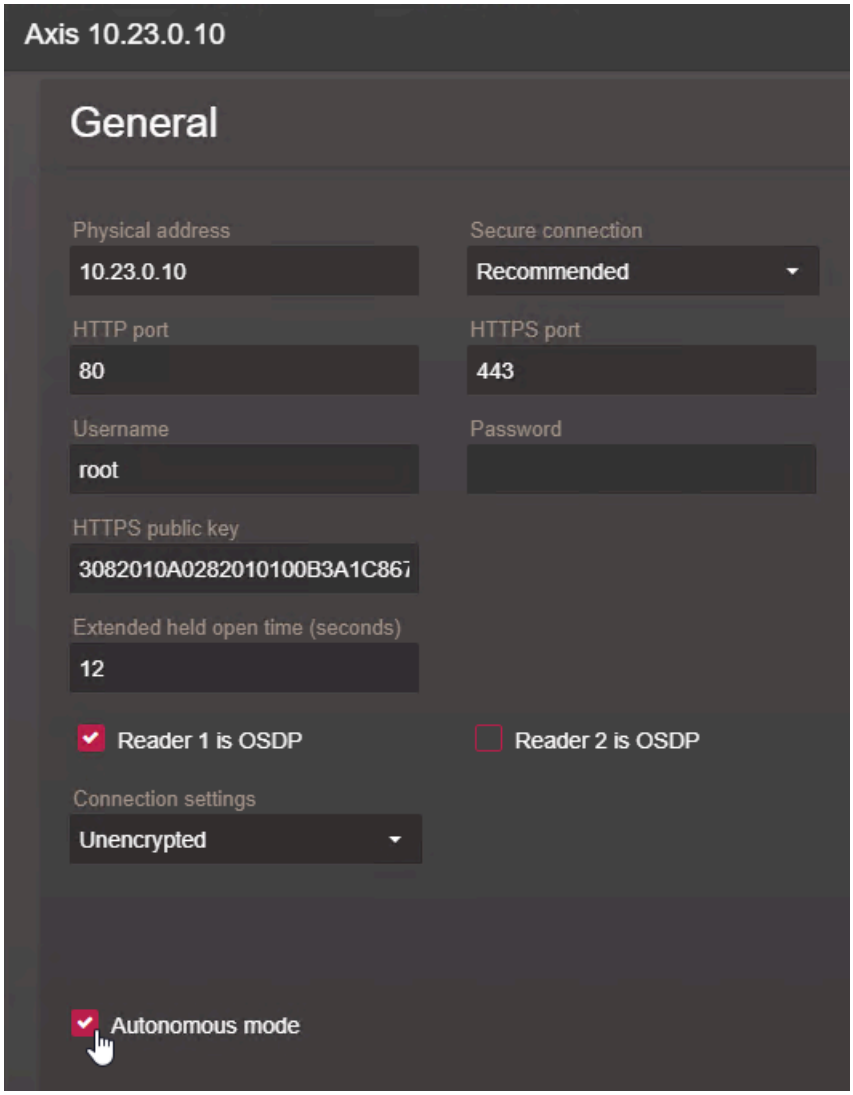
Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 Dans l'arborescence matérielle, sélectionnez l'unité Axis que vous souhaitez exécuter en *mode autonome*.
La fenêtre de configuration apparaît.

4 Cochez la case **Mode autonome**.



5 Cliquez sur **Enregistrer**.

6 (Facultatif) Répétez les étapes pour toutes les unités Axis que vous souhaitez exécuter en *Mode autonome*.

L'unité Axis prend les décisions d'accès indépendamment, puis envoie des informations de contrôle d'accès à l'unité Synergis.

Renforcer les contrôleurs Axis

Il est recommandé d'activer le filtrage des adresses IP sur le contrôleur Axis pour autoriser les adresses IP de l'unité Synergis[MC] et du poste de l'administrateur à se connecter au contrôleur.

Avant de commencer

Procédure

1 Connectez-vous au portail web du contrôleur Axis.

Pour en savoir plus, voir la documentation Axis.

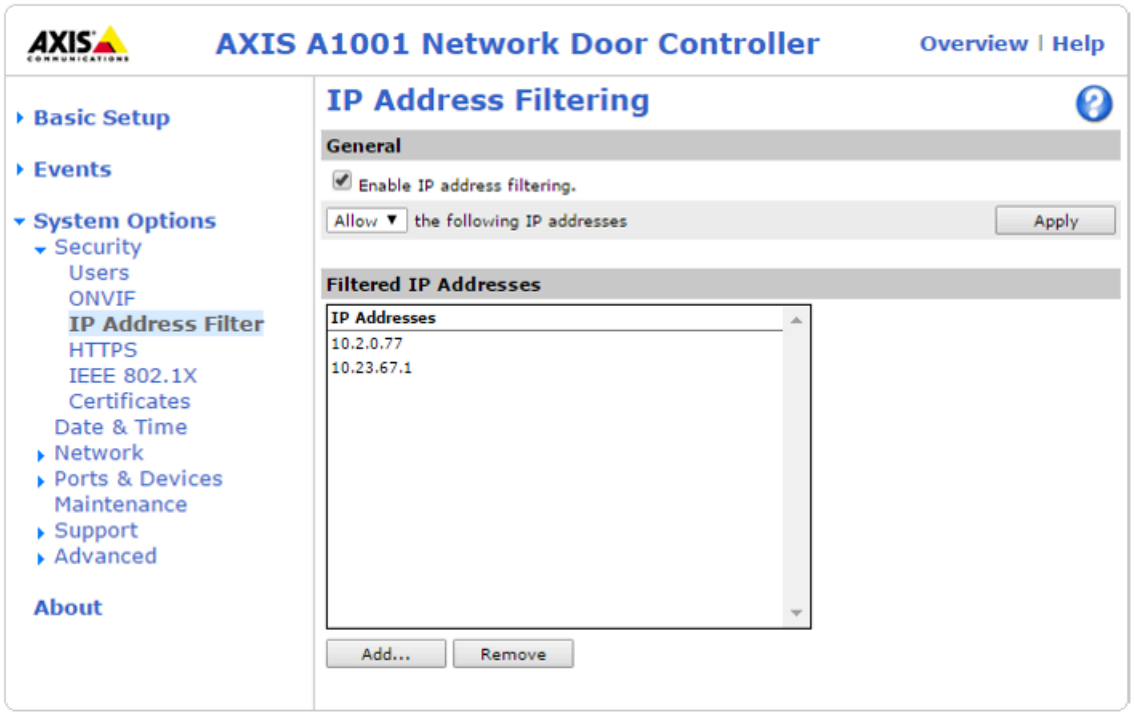
2 Cliquez sur **Setup** > **Additional Controller Configuration** > **System Options** > **Security** > **IP Address Filter** (Configuration, Configuration supplémentaire du contrôleur, Options système, Sécurité, Filtrage des adresses IP).

3 Activez l'option **Activer le filtrage des adresses IP des recommandations de sécurité du produit d'Axis Communications** puis sélectionnez **Autoriser** dans la liste.

4 Cliquez sur **Appliquer**.

5 Dans la liste *Filtered IP Addresses* (Adresses IP filtrées), ajoutez l'adresse IP de l'unité Synergis et celle du poste d'administration qui doit se connecter au portail Web du contrôleur Axis.

Exemple :



6 Sous **System options**, cliquez sur **Network** > **TCP/IP** > **Advanced**, et désactivez les options **FTP server** et **RTSP server**.

Elles ne sont pas utilisées par Synergis[MC] Softwire.

7 Cliquez sur **Enregistrer**.

Configurer les périphériques de contrôleurs Axis

Pour configurer les contacts d'entrée, relais de sortie et lecteurs connectés au contrôleur Axis, vous devez effectuer les modifications dans Config Tool et sur le Synergis[MC] Appliance Portal.

Avant de commencer

- Inscrivez le contrôleur Axis sur l'unité Synergis[MC].
- Ajoutez l'unité Synergis à un rôle Gestionnaire d'accès.

À savoir

- Les relais de sortie et les lecteurs sont configurés sur la page *Matériel* de l'unité Synergis sur le Synergis[MC] Appliance Portal ou dans Config Tool.
- Les contacts d'entrée sont configurés sur la page *Matériel* et sur la page *Périphériques* de l'unité Synergis dans Config Tool.

Procédure

Pour configurer les réglages de sortie d'un contrôleur Axis :

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 Sur les contrôleurs A1601, configurez les ports d'E/S auxiliaires en tant qu'entrées ou sorties, selon vos besoins.

4 Sur les contrôleurs A1001, configurez les réglages selon vos besoins.

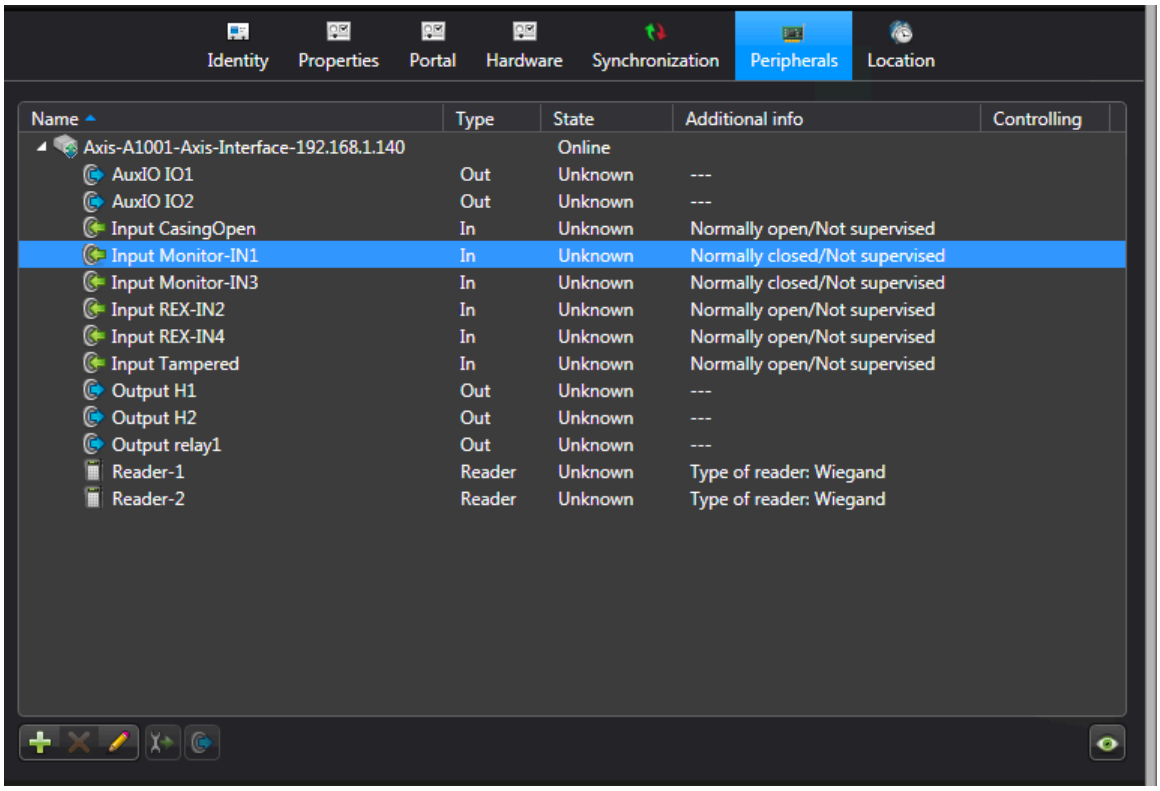
Pour en savoir plus sur chaque réglage, consultez la documentation Axis.

Pour configurer les réglages d'entrée d'un contrôleur Axis :

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

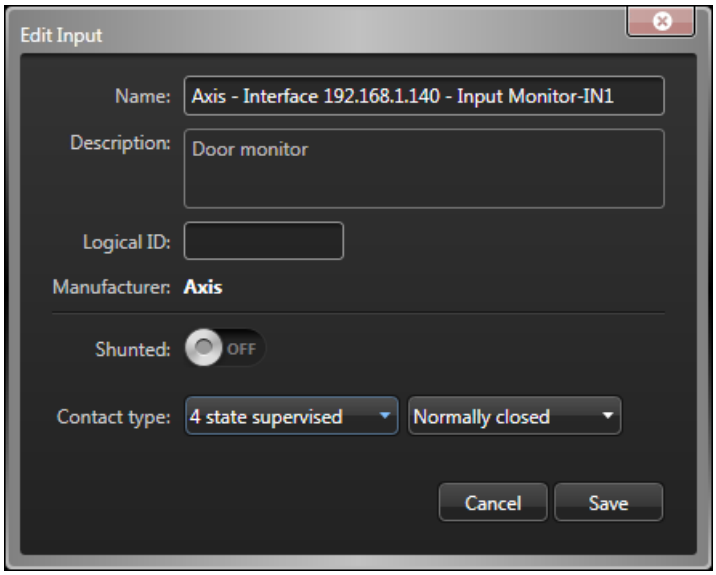
2 Dans l'arborescence des entités, sélectionnez l'unité Synergis, puis cliquez sur l'onglet **Périphériques**.

3 Développez le contrôleur Axis que vous souhaitez modifier, sélectionnez une entrée, puis cliquez sur **Modifier** ( ).



4 Effectuez les modifications nécessaires dans la boîte de dialogue *Modifier l'entrée*.

Exemple :



REMARQUE : Les réglages disponibles dépendent de l'entrée sélectionnée. Sur les unités A1601, les E/S 1, 2, 3, 4, 13 et 14 ne peuvent pas être supervisées lorsqu'elles sont configurées en tant qu'entrées.

- **Nom :** Nom de l'appareil en entrée.
- **ID logique :** Doit être unique parmi les périphériques connectés à l'unité.
- **Désactivé :** Sélectionnez cette option pour ignorer les entrées. Une fois contourné, l'état de l'entrée affiche *Normal*, quelle que soit la manière de la déclencher.

REMARQUE : Si l'ouverture de la porte est forcée, l'événement *Ouverture de porte forcée* est toujours généré dans Security Center, même si l'entrée de porte est désactivée.

- **Type de contact :** Spécifiez l'état *Normal* du contact d'entrée et son mode de supervision.
  - **Non supervisé/normalement fermé :** L'état normal du contact de l'entrée est fermé, et l'unité de contrôle d'accès ne signale pas que l'entrée est en état anormal.
  - **Non supervisé/normalement ouvert :** L'état normal du contact de l'entrée est ouvert, et l'unité de contrôle d'accès ne signale pas si l'entrée est en état anormal.
  - **4 - état supervisé/normalement fermé :** L'état normal du contact de l'entrée est fermé, et l'unité de contrôle d'accès signale si l'entrée est en état anormal.
  - **4 - état supervisé/normalement ouvert :** L'état normal du contact de l'entrée est ouvert, et l'unité de contrôle d'accès signale si l'entrée est en état anormal.

5 Cliquez sur **Enregistrer**, puis sur **Appliquer**.

Configurer les ports d'E/S auxiliaires d'un contrôleur AXIS A1601

Vous pouvez configurer les ports d'E/S auxiliaires des contrôleurs AXIS A1601 afin qu'ils servent d'entrées ou de sorties à l'aide du Synergis[MC] Appliance Portal.

À savoir

- Si une E/S auxiliaire est déjà utilisée dans une configuration et que vous modifiez son type, l'E/S bascule hors ligne, et vous devez mettre à jour cette E/S manuellement dans la configuration dans Security Center.
- Par défaut, les E/S auxiliaires 1 et 2 sont des sorties, et les E/S auxiliaires 3, 4, 13 et 14 sont des entrées. Lorsqu'elles sont configurées en tant qu'entrées, elles ne peuvent pas être supervisées.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

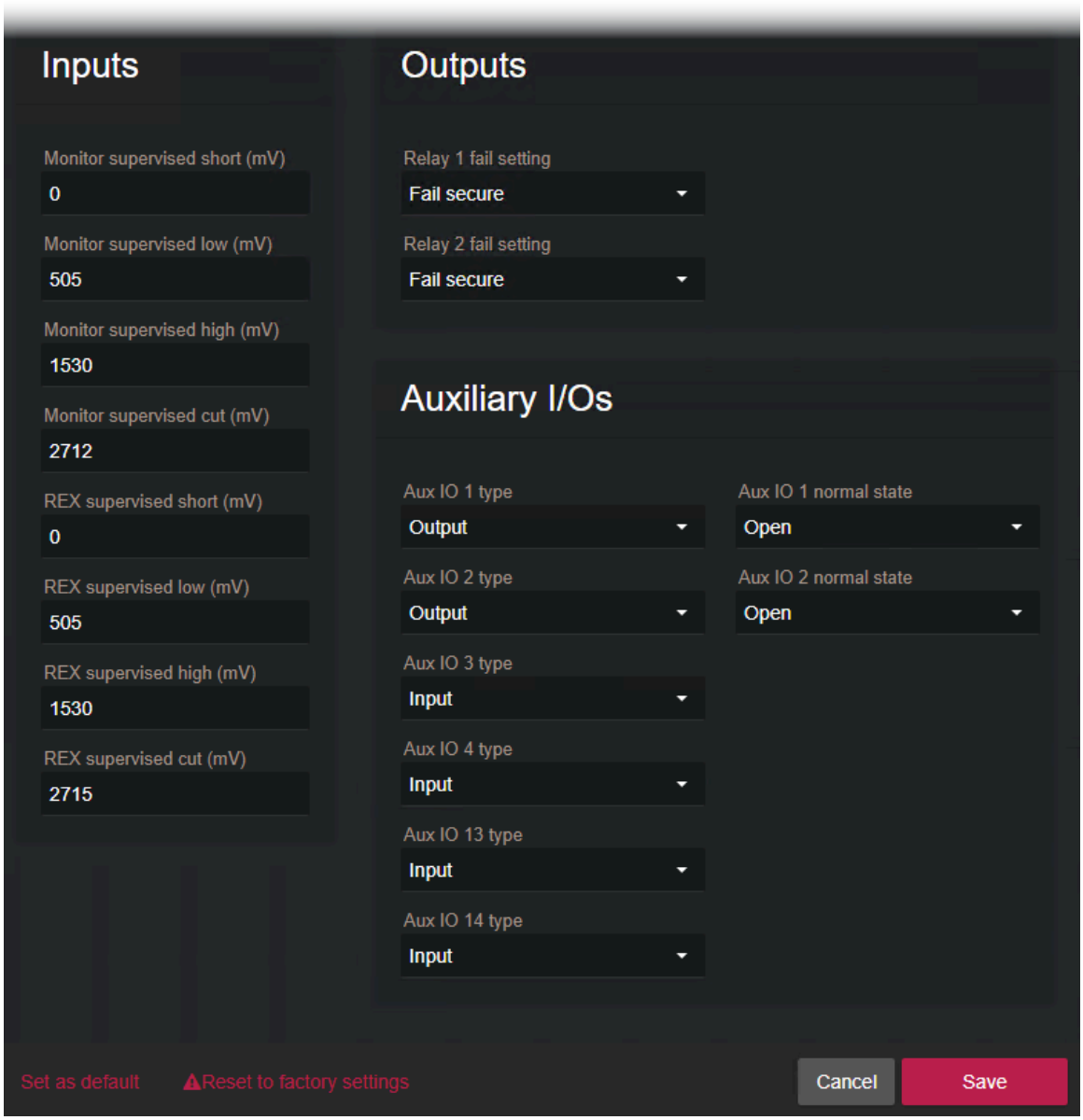
2 Cliquez sur **Configuration** > **Matériel**.

3 Cliquez sur l'unité Axis dans la colonne *Matériel*, puis dans la colonne *Canaux*.

4 Dans la colonne *Interfaces*, cliquez sur l'unité pour ouvrir ses réglages.

5 Faites défiler la page jusqu'à la section *E/S auxiliaires*, et modifiez les **Types d'E/S aux.** selon vos besoins.

REMARQUE : Si vous modifiez le type pour créer une sortie, vous devez configurer l'état normal sur **Ouvert** ou **Fermé**. Vous ne pouvez configurer l'état normal d'une entrée que dans Config Tool.



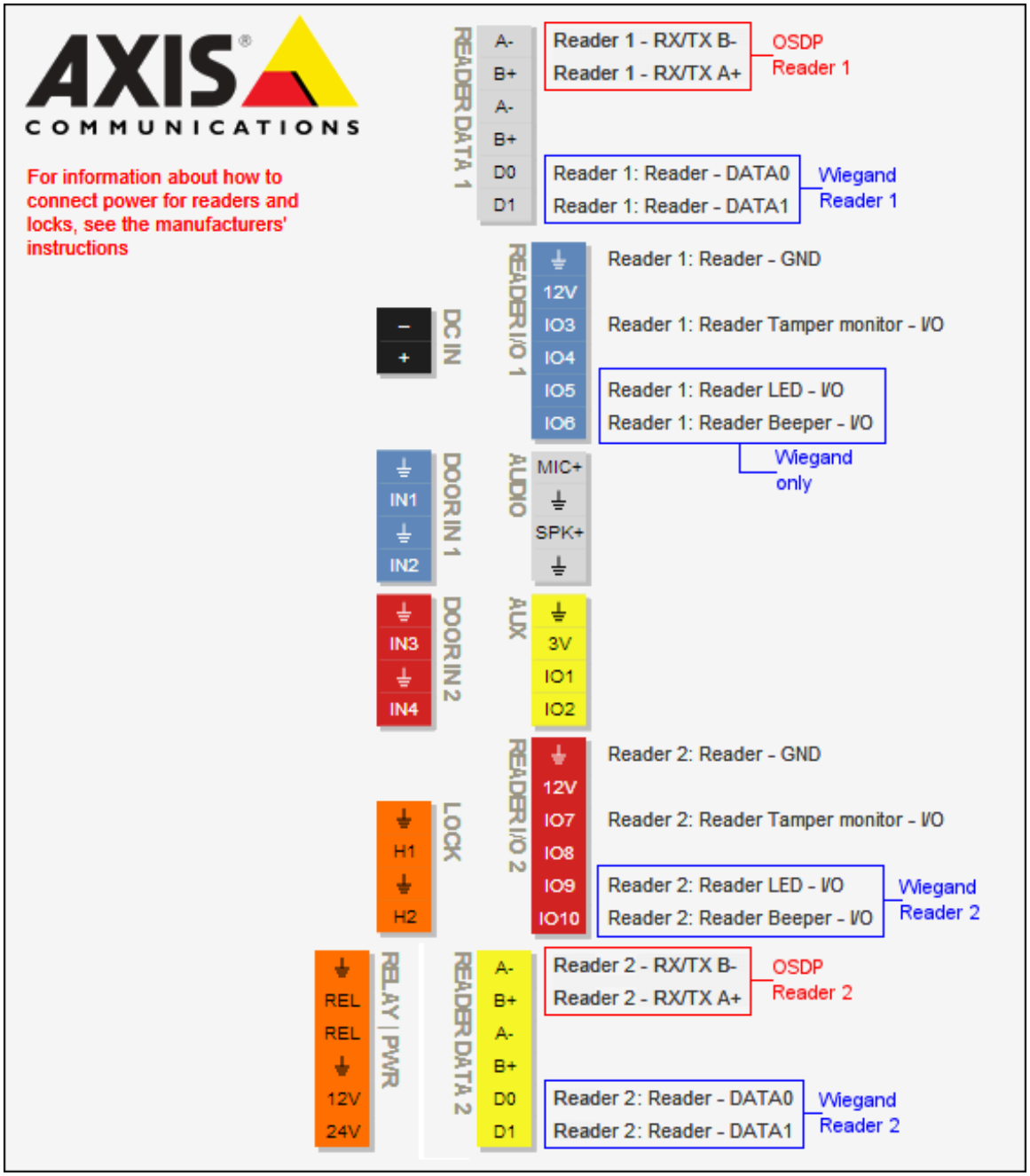
6 Cliquez sur **Enregistrer**.

Connexions des lecteurs sur le contrôleur AXIS A1001

Chaque contrôleur AXIS A1001 prend en charge deux lecteurs appelés *Reader 1* et *Reader 2* dans Security Center Config Tool. Les lecteurs peuvent utiliser le protocole Wiegand (par défaut) ou OSDP. Pour OSDP, le lecteur doit être câblé sur le premier jeu de données de lecteur **A-/B+**.

Le schéma suivant répertorie les ensembles de connecteurs correspondant au lecteur sur le contrôleur Axis.

REMARQUE : Ce schéma de broches n'apparaît que si le contrôleur Axis est déconnecté de l'unité Synergis[MC].



Connexions des lecteurs sur le contrôleur AXIS A1601

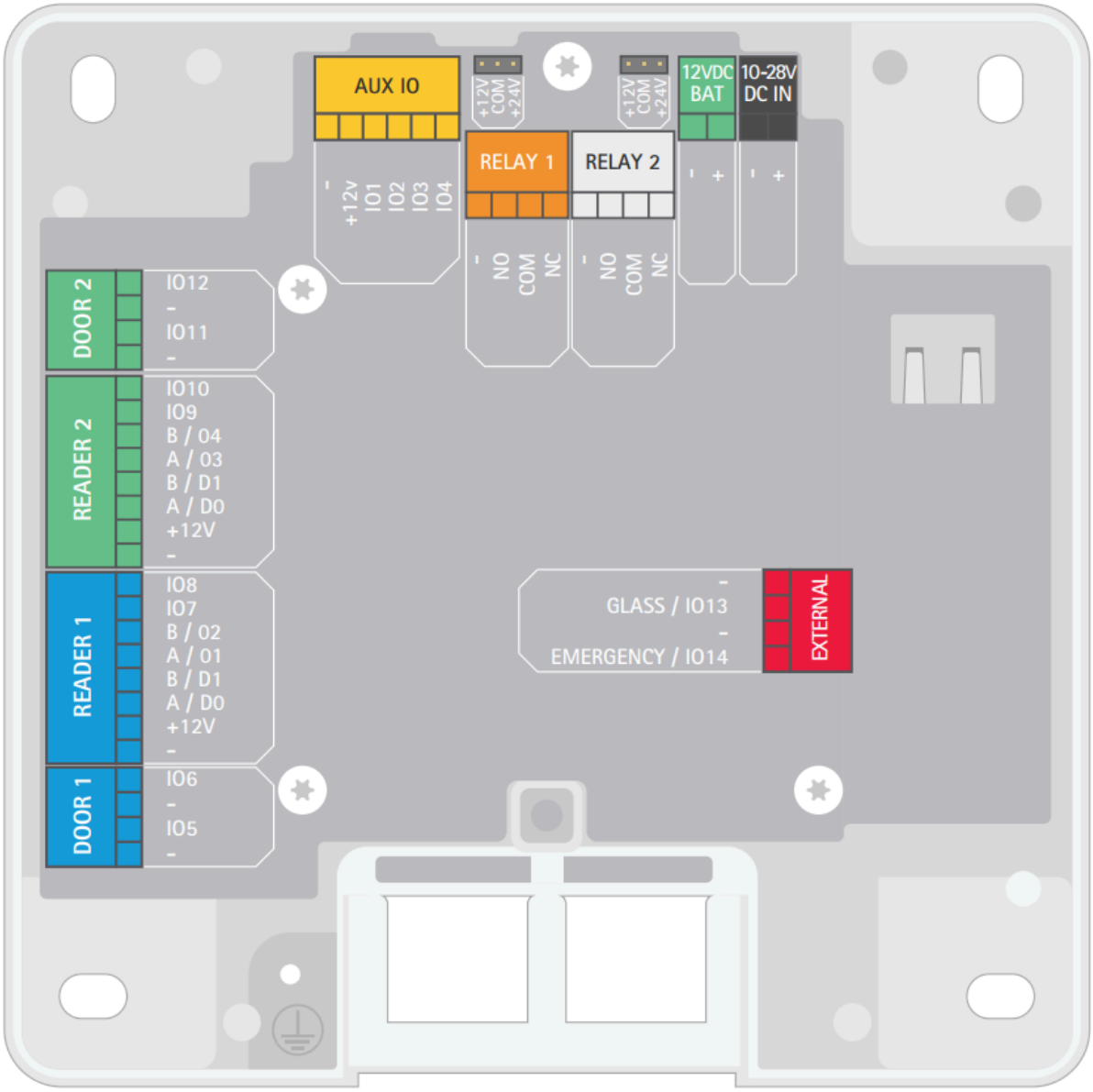
Chaque contrôleur AXIS A1601 prend en charge deux lecteurs appelés *Reader 1* et *Reader 2* dans Security Center Config Tool.

Le schéma suivant répertorie les ensembles de connecteurs correspondant au lecteur sur le contrôleur Axis.

Par défaut, le contrôleur A1601 est représenté dans Security Center de la manière suivante :

- Huit entrées : deux capteurs de porte, deux REX, quatre entrées auxiliaires (E/S 3, 4, 13 et 14)
- Quatre sorties : deux relais de verrouillage, deux sorties auxiliaires (E/S 1 et 2).

REMARQUE : Les E/S auxiliaires peuvent être configurées en tant qu'entrées ou sorties.



Activer des lecteurs OSDP (Secure Channel) sur un contrôleur AXIS A1601

Vous pouvez utiliser OSDP avec Secure Channel entre un contrôleur AXIS A1601 et ses lecteurs OSDP pour obtenir un chiffrement de bout en bout.

À savoir

Les contrôleurs A1601 nécessitent le micrologiciel 1.84.4 ou ultérieur.

Procédure

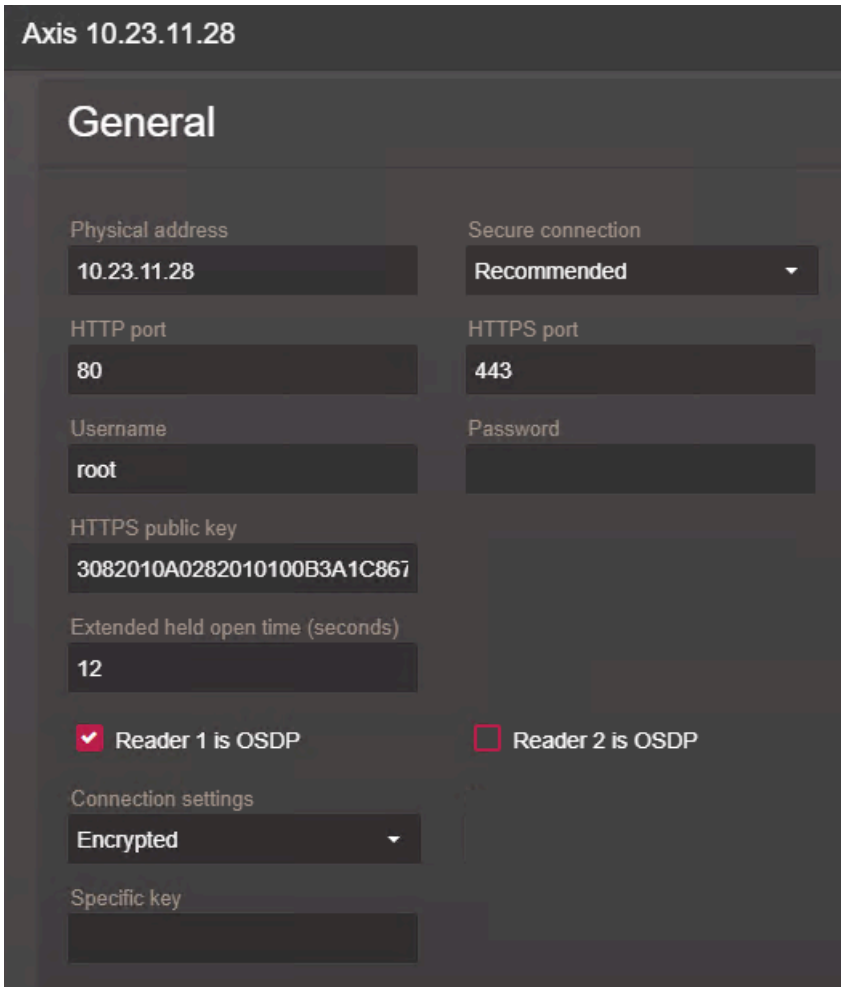
1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 Dans l'arborescence matérielle, sélectionnez l'unité Axis à laquelle vous souhaitez ajouter des lecteurs OSDP (Secure Channel).

La fenêtre de configuration apparaît.

4 Cochez la case **Le lecteur est OSDP** pour le lecteur qui vous intéresse.



5 Dans la liste **Réglages de connexion**, sélectionnez **Chiffré**.

6 Dans le champ **Clé spécifique**, entrez la clé 128 bits (32 caractères hexadécimaux).

Si le lecteur a été précédemment configuré pour une communication sécurisée, copiez-collez la clé existante. Sinon, définissez le lecteur en mode d'installation (voir la documentation du fabricant du lecteur) et copiez-collez la clé de votre choix.

7 Cliquez sur **Enregistrer**.

La clé est ajoutée au magasin de clés Axis, et sert à communiquer avec le lecteur.

9

Contrôleurs DDS

Cette section aborde les sujets suivants:

Inscrire un contrôleur RS-485 DDS

Pour que l'unité Synergis[MC] puisse communiquer avec les contrôleurs DDS connectés à son interface RS-485, vous devez les inscrire avec le Synergis[MC] Appliance Portal.

Avant de commencer

Connectez les modules DDS aux canaux RS-485 (A, B, C ou D) de l'unité Synergis de la manière suivante :

- Connectez Rx\L du module DDS au « - » du canal.
- Connectez Tx\H du module DDS au « + » du canal.
- Connectez 0v du module DDS au « G » du canal.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** ().

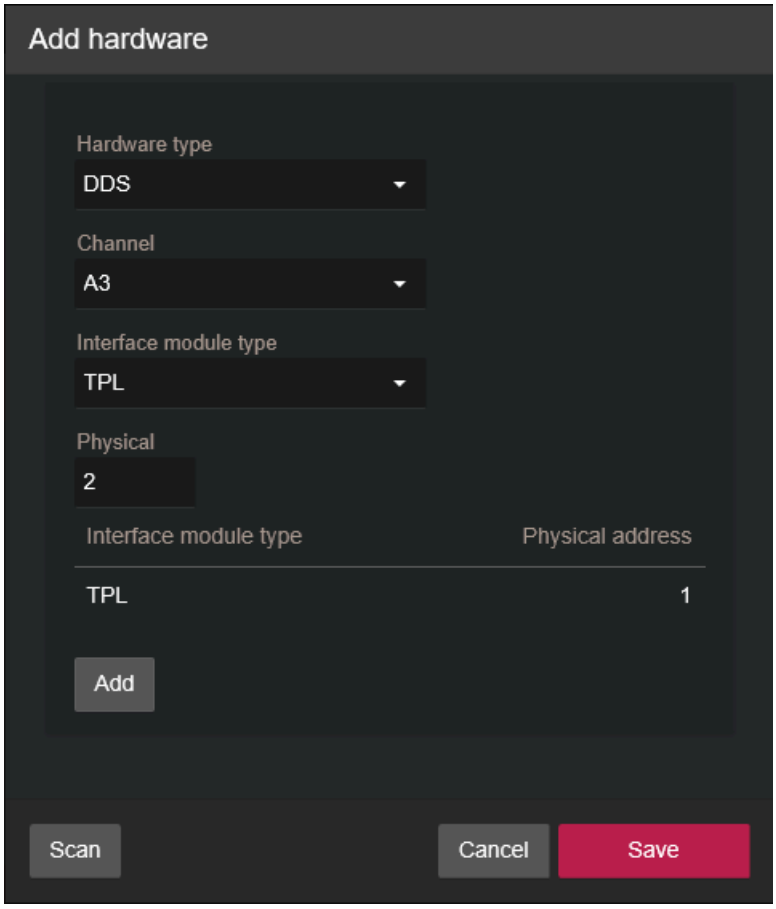
4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **DDS** sous **Type de matériel**.

5 Sélectionnez le **Canal** (A, B, C ou D).
Tous les modules d'interface connectés à un même canal doivent provenir d'un même fabricant.

6 Dans la même boîte de dialogue, ajoutez tous les modules d'interface connectés au même canal.

Procédez de l'une des manières suivantes :

- Pour l'inscrire manuellement, entrez l'adresse physique (0 à 31) configurée sur le module DDS et cliquez sur **Ajouter** (➕). Sélectionnez ensuite le type de module précis.



Répétez pour configurer tous les modules connectés au même canal.

- Pour les inscrire automatiquement, cliquez sur **Analyser**.

  La fonction d'analyse détecte tous les modules d'interface d'un même fabricant connectés au même canal.

  Si le contrôleur ne détecte pas tous les modules d'interface connectés, vérifiez qu'ils ont tous une adresse physique distincte.

  Lorsque vous cliquez sur **Ajouter**, l'adresse dans le champ **Physique** bascule vers l'adresse disponible suivante.

7 Cliquez sur **Enregistrer**.

Le type de matériel, le canal et le module d'interface que vous venez d'ajouter sont répertoriés sur la page *Configuration matérielle*.

8 Sélectionnez chaque module d'interface sur la page *Configuration matérielle*, puis configurez ses réglages.

Pour une description des réglages, consultez la documentation du fabricant. Apportez les modifications nécessaires.

9 Cliquez sur **Enregistrer**.

10 Testez la connexion de votre module d'interface et votre configuration à partir de la page *Diagnostics d'E/S*.

Lorsque vous avez terminé

Inscrivez l’unité Synergis dans Security Center.

Définir l’adresse physique d’un contrôleur de porte TPL

Chaque module TPL connecté à un même canal RS-485 ou détecté sur le même réseau local doit utiliser une adresse physique distincte.

À savoir

L’adresse physique d’un contrôleur de porte TPL est définie par deux ensembles de commutateurs DIP : DS2 et JP4. Si une carte d’extension TCP/IP est connectée à la carte du contrôleur TPL, vous devez la retirer pour accéder aux commutateurs DIP.

Procédure

1 Réglez DS2/1 sur 1 ou ON.

2 Réglez l’adresse physique sur JP4 en fonction des tableaux suivants.

JP4/1:	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
JP4/2:	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
JP4/3:	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
JP4/4:	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
JP4/5:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

JP4/1:	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
JP4/2:	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
JP4/3:	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
JP4/4:	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
JP4/5:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

REMARQUE : JP4 (6, 7, 8) servent à définir le protocole de communication du lecteur. Par exemple, pour Wiegand avec lecture jusqu’à 50 bits sans vérification de parité, réglez JP4/7 sur 1 ou ON, et DS2/4 sur 1 ou ON. Pour en savoir plus, consultez la documentation de DDS correspondant à votre matériel spécifique.

10

Sous-tableaux HID VertX

Cette section aborde les sujets suivants:

Inscrire les sous-tableaux HID VertX connectés à l'unité Synergis

Pour établir la communication entre l'unité Synergis[MC] et les modules d'interface connectés, vous devez configurer les modules d'interface dans Synergis[MC] Appliance Portal.

Avant de commencer

Connectez les modules HID VertX aux canaux (1 - 4) de votre unité Synergis Cloud Link .

REMARQUE : Si vous avez l'unité Synergis Cloud Link 312, vous avez jusqu'à 12 canaux. Pour en savoir plus, voir À propos des ports RS-485 du Synergis Cloud Link.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** ( ).

4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **VertX** en tant que **Type de matériel**.

5 Sélectionnez le **Canal** (1 - 4) .

Tous les modules d'interface connectés à un même canal doivent provenir d'un même fabricant.

6 Dans la même boîte de dialogue, ajoutez tous les modules d'interface connectés au même canal.

Vous pouvez inscrire les modules d'interface automatiquement ou manuellement.

CONSEIL : Si vous inscrivez peu de modules et connaissez leurs adresses physiques, l'inscription manuelle est plus rapide.

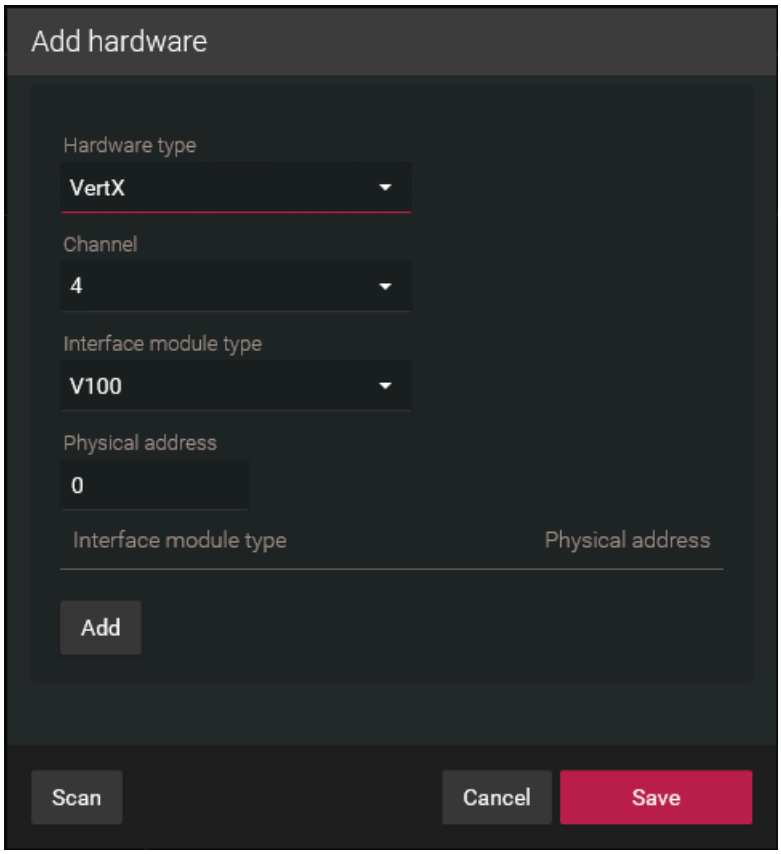
Procédez de l'une des manières suivantes :

- Pour les inscrire automatiquement, cliquez sur **Analyser**.

La fonction d'analyse détecte tous les modules d'interface d'un même fabricant connectés au même canal.

Si le contrôleur ne détecte pas tous les modules d'interface connectés, vérifiez qu'ils ont tous une adresse physique distincte.

- Pour l'inscription manuelle, entrez l'adresse physique (0 à 15) configurée sur l'appareil d'interface HID, sélectionnez le type de modèle, puis cliquez sur ✚.



Répétez pour configurer tous les modules connectés au même canal.

7 Cliquez sur **Enregistrer**.

Le type de matériel, le canal et le module d'interface que vous venez d'ajouter sont répertoriés sur la page *Configuration matérielle*.

8 Sélectionnez chaque module d'interface sur la page *Configuration matérielle*, puis configurez ses réglages.

Pour une description des réglages, consultez la documentation du fabricant. Apportez les modifications nécessaires.

9 Cliquez sur **Enregistrer**.

10 Testez la connexion de votre module d'interface et votre configuration à partir de la page *Diagnostics d'E/S*.

Lorsque vous avez terminé

Inscrivez l'unité Synergis dans Security Center.

Activer la supervision des lecteurs sur HID VertX V100

Pour recevoir *les événements Porte hors* ligne lorsque le lecteur connecté à un tableau VertX V100 est déconnecté ou éteint, vous devez configurer le réglage de lecteur Je suis vivant **dans** Config Tool et programmer le lecteur avec la carte de configuration appropriée.

Avant de commencer

Inscrivez le tableau VertX V100 sur l'unité Synergis[MC].

À savoir

La supervision de lecteur n'est prise en charge que pour les lecteurs connectés à un tableau VertX V100 contrôlé par une unité Synergis.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.

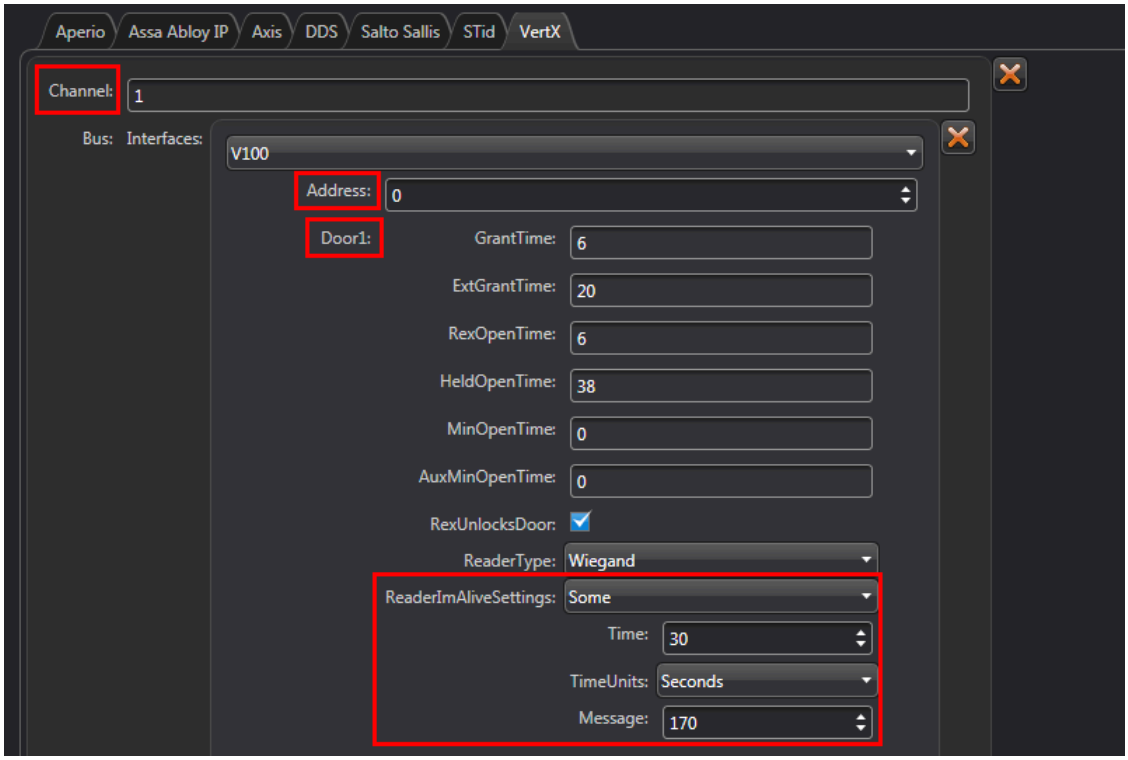
2 Cliquez sur **Rôles et unités**, puis cliquez sur l'unité Synergis.

3 Cliquez sur **Matériel**, puis faites défiler la page jusqu'au tableau V100 auquel le lecteur est connecté.

Si votre unité Synergis contrôle plusieurs tableaux V100, veillez à identifier le bon lecteur en fonction de son **Canal**, son **Adresse** physique et son numéro de porte (**Porte1** ou **Porte2**).

4 Sous la porte sélectionnée, cliquez sur **ReaderImAliveSettings**, et modifiez la valeur sur **Some**.

Time doit être égal ou supérieur à la valeur **Je suis vivant** située sur la carte de configuration du lecteur, et **Message** doit correspondre au message **Je suis vivant** (170 est l'équivalent décimal de AA en hexadécimal).



5 Cliquez sur **Appliquer**.

6 Configurez le lecteur avec la carte de programmation (également appelée carte de configuration) adaptée.

Lorsque le lecteur est éteint ou déconnecté du tableau V100, vous recevrez désormais l'événement *Porte hors ligne : L'appareil est hors ligne* pour la porte associée.

11

Contrôleurs Mercury

Cette section aborde les sujets suivants:

Réglages des lecteurs Mercury

Il s'agit de la liste complète des réglages des lecteurs Mercury. Ces réglages correspondent à des lecteurs matériels spécifiques. La majorité des lecteurs utilisés de nos jours exploitent la norme Wiegand. Pour utiliser des cartes à puce ou pour configurer des lecteurs Secure OSDP2, reportez-vous aux notes techniques des lecteurs correspondants.

Fonction	Description
Type du lecteur	
Wiegand standard	• Règle **Mode de pavé numérique** sur **HID** • Règle **Mode lecteur DEL** sur **Bicolore** • Règle **Impulsions Wiegand** sur **ON**
Piste magnétique standard	• Règle **Mode de pavé numérique** sur **Aucun** • Règle **Mode lecteur DEL** sur **Bicolore** • Règle **Rogner les bits zéro** sur **ON** • Règle **Convertir en ensemble de semioctets** sur **ON** • Règle **Autoriser le décodage Mag bidirectionnel** sur **ON** • Règle **Supervisé** sur **ON** • Règle **Entrées provenant du lecteur** sur **ON**
OSDP standard	• Active le **Mode OSDP** • Règle **Mode de pavé numérique** sur **HID** • Règle **Mode lecteur DEL** sur **OSDP**
OSDP 2	• Active le **Mode OSDP** • Règle **Mode de pavé numérique** sur **HID** • Règle **Mode lecteur DEL** sur **OSDP personnalisé** Ce mode permet également la configuration du débit binaire, Traçage, Carte à puce, adresse et des Communications sécurisées sur le port du lecteur.
F2F standard	• Règle **Mode de pavé numérique** sur **HID** • Règle **Mode lecteur DEL** sur **Bicolore** • Règle **Convertir en ensemble de semioctets** sur **ON** • Règle Sets **Casi F2F 1 fil** to **ON**
F2F supervisé	• Règle **Mode de pavé numérique** sur **HID** • Règle **Mode lecteur DEL** sur **Bicolore** • Règle **Convertir en ensemble de semioctets** sur **ON** • Règle Sets **Casi F2F 1 fil** to **ON** • Règle **Supervisé** sur **ON**

Fonction	Description
F2F supervisé avec entrées	• Règle **Mode de pavé numérique** sur **Aucun** • Règle **Mode lecteur DEL** sur **Bicolore** • Règle **Convertir en ensemble de semioctets** sur **ON** • Règle Sets **Casi F2F 1 fil** to **ON** • Règle **Supervisé** sur **ON** • Règle **Entrées provenant du lecteur** sur **ON**
Personnalisé	Permet à l'utilisateur de configurer n'importe quel Mode de pavé numérique et d'autres réglages en fonction du lecteur matériel.
Mode de pavé numérique[1]	
Aucun	Aucun mode particulier n'est activé.
MR20	Mode de pavé numérique 8 bits MR20 avec sabotage.
HID	Format de pavé numérique 4 bits HID.
Indala	Format Motorola/Indala 8 bits constitué d'un code 4 bits et du même code inversé.
MR20 sans sabotage	Mode de pavé numérique 8 bits MR20 sans sabotage.
4 bits, valable 60 secondes	Format de pavé numérique 4 bits avec prise en charge du mode HID I'm Alive réglé sur 60 secondes.
8 bits, valable 60 secondes	Format de pavé numérique 8 bits avec prise en charge du mode HID I'm Alive réglé sur 60 secondes.
4 bits, valable 10 secondes	Format de pavé numérique 4 bits avec prise en charge du mode HID I'm Alive réglé sur 10 secondes.
8 bits, valable 10 secondes	Format de pavé numérique 8 bits avec prise en charge du mode HID I'm Alive réglé sur 60 secondes.
Mode lecteur DEL	
Bicolore	Circuit de commande bicolore à trois états générique à 1 fil.
2 fils	Circuits rouge et vert distincts sans avertisseur.
Dorado-780	Circuit à deux fils sans conversion de couleur.
LCD	Active le circuit de l'écran LCD sur les lecteurs équipés d'un LCD.
Bioscrypt	Active l'interface Bioscrypt.
OSDP	Imite le comportement du DEL et de l'avertisseur Wiegand sur les lecteurs OSDP.
SNET	Active SNET sur les contrôleurs Honeywell.

Fonction	Description
OSDP personnalisé	Autorise l'utilisateur à définir des réglages OSDP personnalisés.
Autres commandes	
Impulsions Wiegand	Active les impulsions Wiegand Data 1/Data 0.
Rogner les bits zéro	Supprime les zéros de remplissage.
Convertir en tableau de demi octets	Utilisé par les pistes magnétiques.
Autoriser le décodage Mag bidirectionnel	Envoie des données décodées quelle que soit la direction de balayage de la carte.
Autoriser le décodage Northern Mag	Décode les données Wiegand 32 bits de certaines cartes Northern.
Casi F2F 1 fil	Avec le type de communication Casi F2F 1 fil, utilise un fil pour la communication au lieu de deux.
Supervisé	Active la supervision. Utilisé uniquement avec le drapeau F2F.
Entrées provenant du lecteur	Indique que les entrées doivent provenir du lecteur. Utilisé uniquement avec le drapeau F2F.

[1] Mercury ne prend pas en charge les lecteurs de clavier émettant un code PIN en mode Wiegand 26bits (mode HID-14).

Préparer l’inscription du contrôleur Mercury

Avant d’inscrire le contrôleur Mercury sur l’unité Synergis[MC], affectez une adresse IP statique au contrôleur.

Avant de commencer

Vous devez disposer des éléments suivants :

- **Guide d'installation et de configuration Mercury :** Manuel d’utilisation pour la connexion au portail Web du contrôleur Mercury et la configuration de son adresse IP, parmi d’autres réglages.
- **Adresse IP statique :** Adresse IP statique affectée au contrôleur par votre service informatique.
- **Adresses physiques :** Chaque module d’interface connecté à un même port RS-485 d’un même contrôleur Mercury doit avoir une adresse physique unique (configurée par micro-interrupteur DIP).

BONNE PRATIQUE : Si vous avez de nombreux contrôleurs Mercury à inscrire sur une même unité Synergis, il est conseillé de les inscrire tous en même temps. Chaque contrôleur que vous ajoutez ou supprimez de l’unité Synergis entraîne le redémarrage de l’unité. Durant le redémarrage, l’unité est hors ligne pendant environ 30 secondes.

À savoir

Les contrôleurs Mercury inscrits sur une même unité Synergis ne peuvent pas être affectés à différentes partitions dans Security Center. Si vous devez affecter des contrôleurs à différentes partitions, inscrivez-les sur différentes unités Synergis, puis affectez les unités Synergis aux différentes partitions.

REMARQUE : Les étapes et instructions de *Renforcement* sont facultatives, mais protègent votre système contre les cyberattaques.

Procédure

1 Sur la carte du contrôleur Mercury, réglez l’interrupteur DIP *S1-1* en position **ON**.

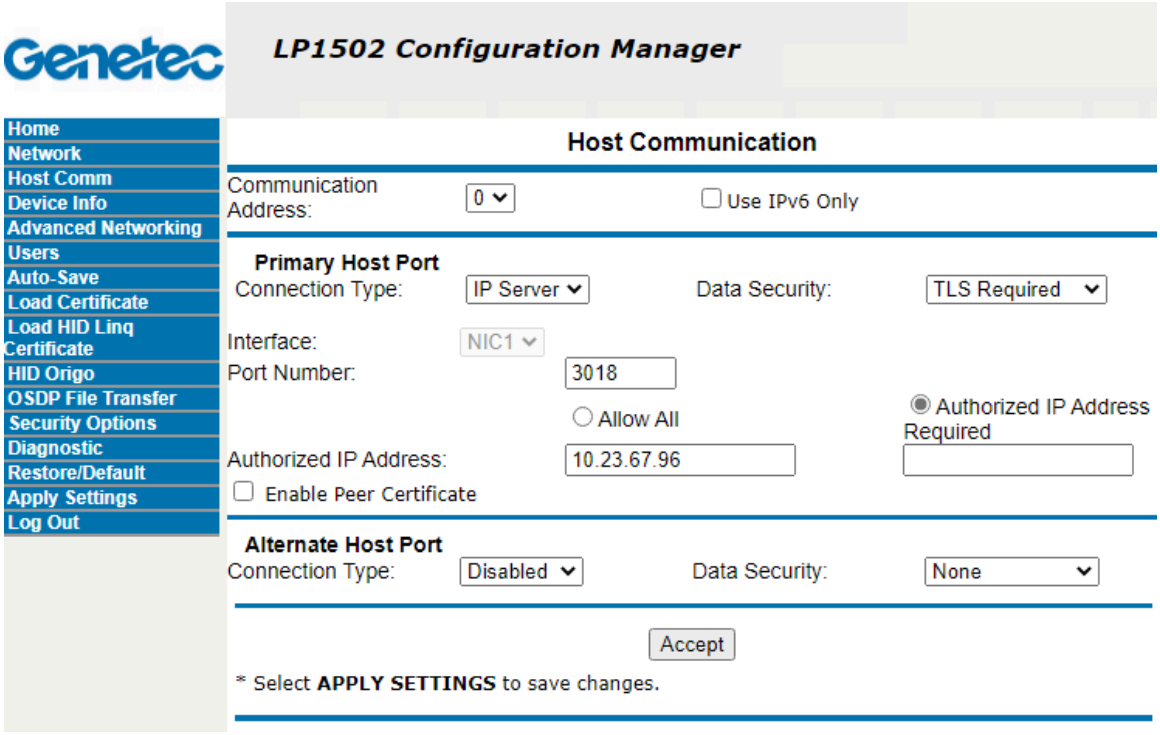
Vous disposez alors d’une fenêtre de 5 minutes pour vous connecter avec les réglages d’usine par défaut.

2 Connectez-vous au contrôleur Mercury via sa page web *Configuration Manager* Utilisez l’adresse IP (192.168.0.251) et les identifiants (admin/password) par défaut. Pour en savoir plus, voir la documentation du fabricant.

3 Sélectionnez **Network** (Réseau) dans le menu, configurez l’**adresse IP** du contrôleur Mercury, et cliquez sur **Accept**.

4 Sélectionnez **Host Comm** dans le menu.

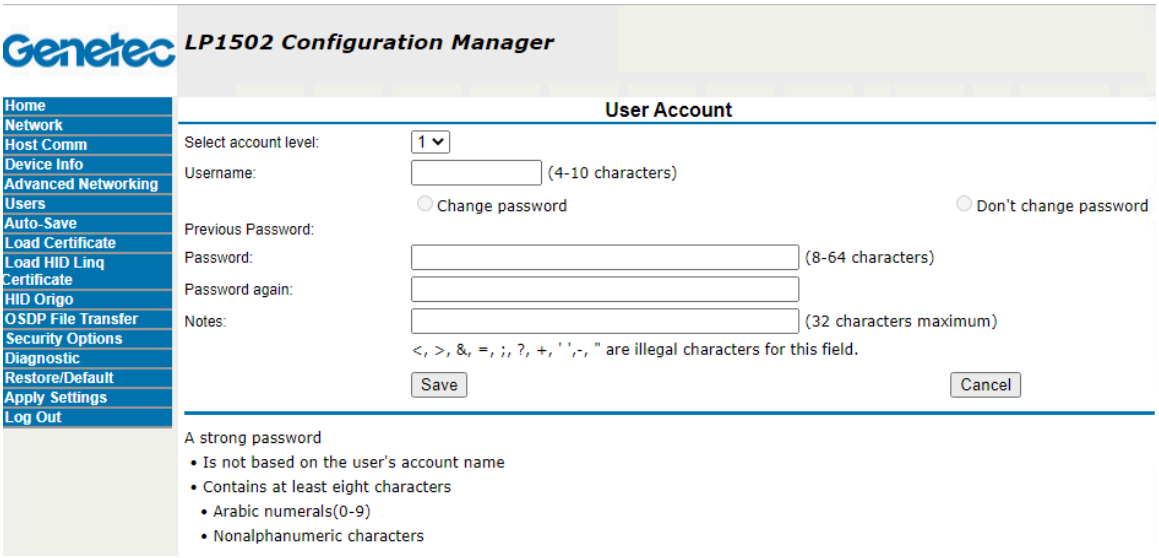
5 Sur la page *Host Communication*, configurez les réglages suivants, puis cliquez sur **Accept**.



- **Communication Address :** Régler sur **0**.
  IMPORTANT : À ne pas confondre avec **Canal** qui doit être unique lorsque vous inscrivez le contrôleur Mercury sur l'unité Synergis.
- **Numéro de port :** Numéro de port utilisé par l'unité Synergis pour communiquer avec le contrôleur Mercury (3001 par défaut),
- **Authorized IP Address Required :** (*Renforcement*) Sélectionnez cette option, puis réglez **Adresse IP autorisée** sur l'adresse de l'unité Synergis.
- **Sécurité des données :** Régler sur **TLS Required**.
  IMPORTANT : Si TLS n'est pas sélectionné, le contrôleur Mercury reste hors ligne.

6 Sélectionnez **Users** (Utilisateurs) dans le menu, puis cliquez sur **New User** (Nouvel utilisateur).

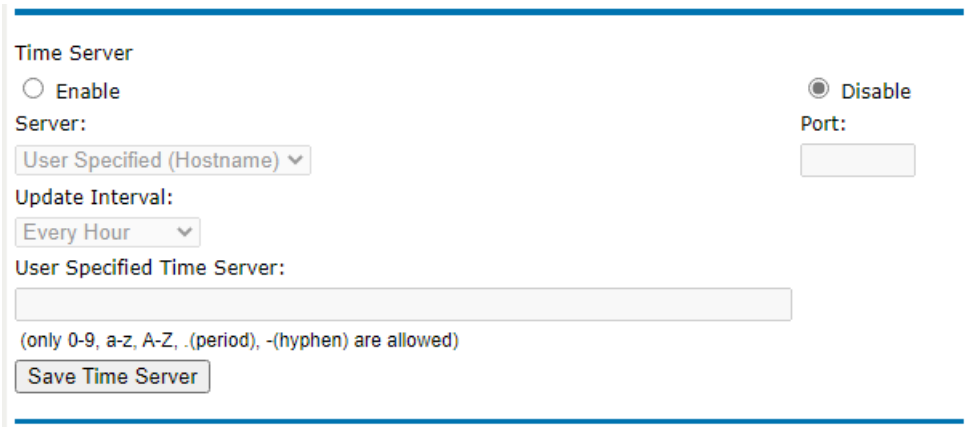
Créer un compte utilisateur sur le contrôleur Mercury vous évite d'accéder physiquement à l'unité pour régler l'interrupteur DIP *S1-1* sur **ON** pour modifier la configuration du contrôleur.



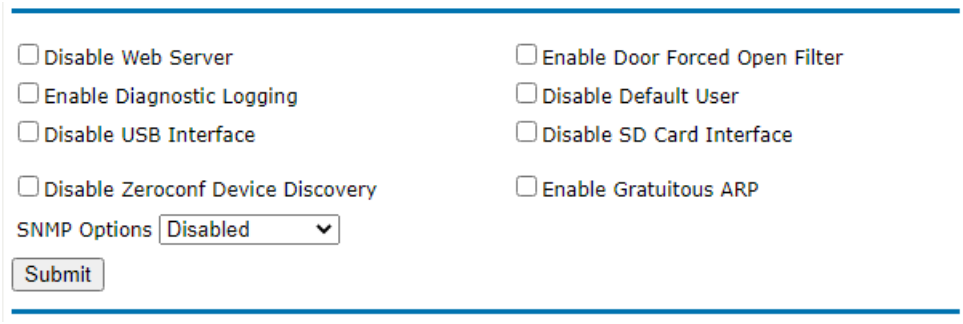
7 (*Renforcement*) Sur la page *User Account* (Compte utilisateur), entrez le **Username** (Nom d'utilisateur) et un mot de passe fort dans **Password**, confirmez le mot de passe, puis cliquez sur **Save** (Enregistrer).

8 Sur la page *Utilisateurs*, désactivez **Time Server** (Serveur d'horloge).

Le Serveur d'horloge n'est pas requis. Synergis[MC] Softwire surveille et règle automatiquement l'heure sur les unités Mercury.



9 (*Renforcement*) Sur la page *Utilisateurs*, désactivez **SNMP Options** et cliquez sur **Submit** (Envoyer).



10 Sélectionnez **Apply Settings** (Appliquer les réglages), puis cliquez sur **Apply Settings, Reboot** (Appliquer les réglages, Redémarrer).

11 Sur la carte du contrôleur Mercury, réglez l'interrupteur DIP *S1-1* en position **OFF** pour rétablir le fonctionnement normal.

   Vous empêchez ainsi l'utilisation des réglages d'usine par défaut pour la connexion au contrôleur.

12 Lorsque vous êtes invité à continuer, sélectionnez **I understand and wish to proceed** (Je comprends et je souhaite continuer), puis cliquez sur **Yes**.

Lorsque vous avez terminé

Inscrivez le contrôleur Mercury sur l'unité Synergis.

Inscrire un contrôleur Mercury sur l’unité Synergis

Pour que l’unité Synergis[MC] puisse communiquer avec les contrôleurs Mercury qui y sont connectés, vous devez les inscrire avec Security Center Config Tool.

Avant de commencer

Préparez le contrôleur Mercury à l’inscription.

À savoir

Mercury controllers enrolled on a Synergis[MC] unit are not visible from the Synergis[MC] Appliance Portal *Hardware* page.

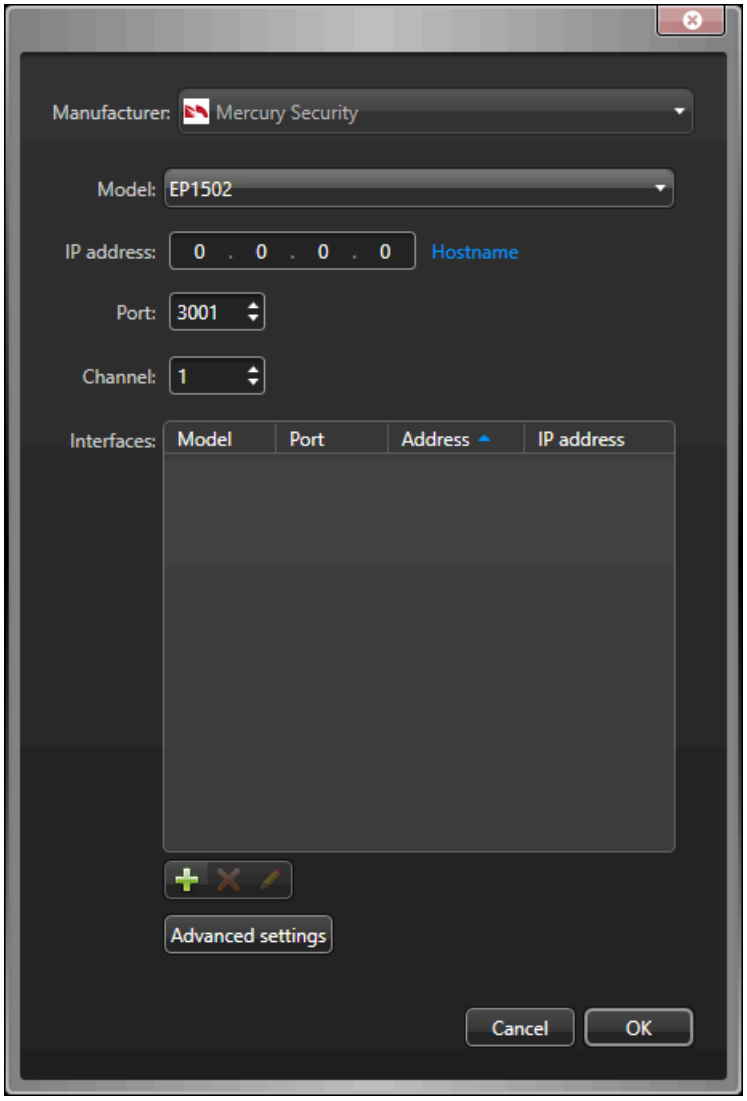
Sur l’unité Synergis, un ID de canal unique doit être affecté à chaque contrôleur Mercury. Tous les contrôleurs Mercury ont des bus RS-485 sur lesquels les modules d’interface (MR50, MR52, MR16IN et MR16OUT) sont connectés. Chaque module d’interface connecté à un même bus RS-485 ou Ethernet doit avoir une adresse physique unique.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.

2 Cliquez sur **Rôles et unités**, puis cliquez sur l’unité Synergis.

3 Cliquez sur **Périphériques**, puis sur **Ajouter un élément** ( ).



4 Saisissez les informations suivantes :

- **Modèle :** Modèle du contrôleur.
- **Adresse IP :** Adresse IP statique affectée au contrôleur par votre service informatique.
- **Nom d'hôte :** Cliquez sur le lien bleu pour identifier le contrôleur par son nom d'hôte. Cette option n'est disponible que si vous exécutez Security Center 5.12.0.0 ou ultérieur.

  REMARQUE : Lorsque vous inscrivez un contrôleur Mercury avec son nom d'hôte, vous devez lui adjoindre `.local` si le contrôleur n'utilise pas le DHCP et le DNS sur le réseau.
- **Port :** Port de communication. La valeur par défaut est 3001. Le port doit correspondre à la valeur configurée sur la page web Mercury Device Manager.
- **Canal :** ID de canal correspondant à ce contrôleur. L'ID de canal peut être compris entre 0 et 63, et doit être unique sur l'unité Synergis. Une fois qu'il est affecté, vous ne devez pas le modifier.

5 Si le modèle de contrôleur sélectionné prend en charge les sous-tableaux, ajoutez-les.

REMARQUE : Prenez en compte les considérations suivantes :

- Ajoutez les tableaux MR51e PoE après l'inscription du contrôleur.
- Pour les contrôleurs EP1501, LP1501, ne dépassez pas la limite de huit sous-tableaux par contrôleur, conformément aux recommandations de Mercury.
- Le tableau M5-20IN occupe deux adresses consécutives sur le bus de communication. Pour disposer de 20 entrées du tableau M5-20IN, vous devez ajouter deux tableaux M5-20IN à votre contrôleur M5-IC dans Config Tool. L'adresse du premier tableau doit correspondre à l'adresse physique du tableau M5-20IN, et l'adresse du second tableau doit être égale à l'adresse du premier tableau plus un.
- Les unités MR62e peuvent avoir une adresse IPv6, mais elles ne peuvent pas communiquer avec les contrôleurs Mercury par IPv6.

a) Sous la liste *Interfaces*, cliquez sur **Ajouter un élément** ( ).

b) Dans la boîte de dialogue qui apparaît, sélectionnez le **Modèle**, le **Port**, l'**Adresse** (0 - 31) et le cas échéant l'adresse IP du tableau en aval.

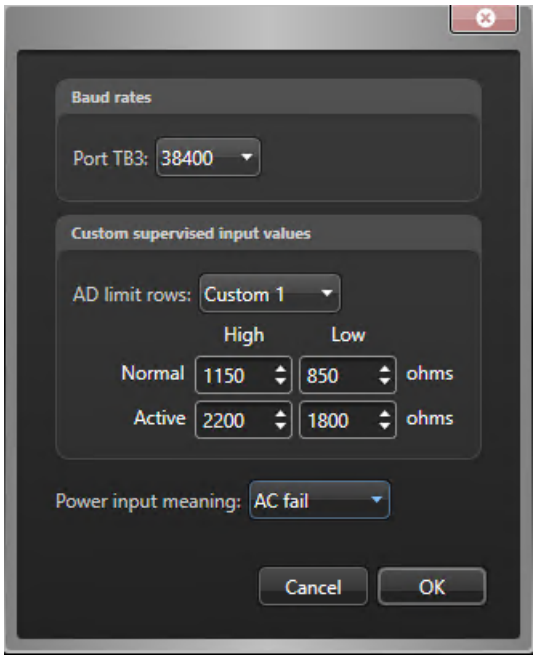
Tous les tableaux connectés à un même port doivent utiliser une adresse différente.

c) Cliquez sur **OK**.

d) Répétez l'opération selon vos besoins.

6 (Facultatif) Cliquez sur **Options avancées** pour modifier les réglages avancés.

Les réglages disponibles dépendent du modèle de contrôleur sélectionné. Vous pouvez généralement modifier le débit en bauds du port série disponible, les valeurs personnalisées d'entrées supervisées et la configuration d'événement d'entrée d'alimentation.

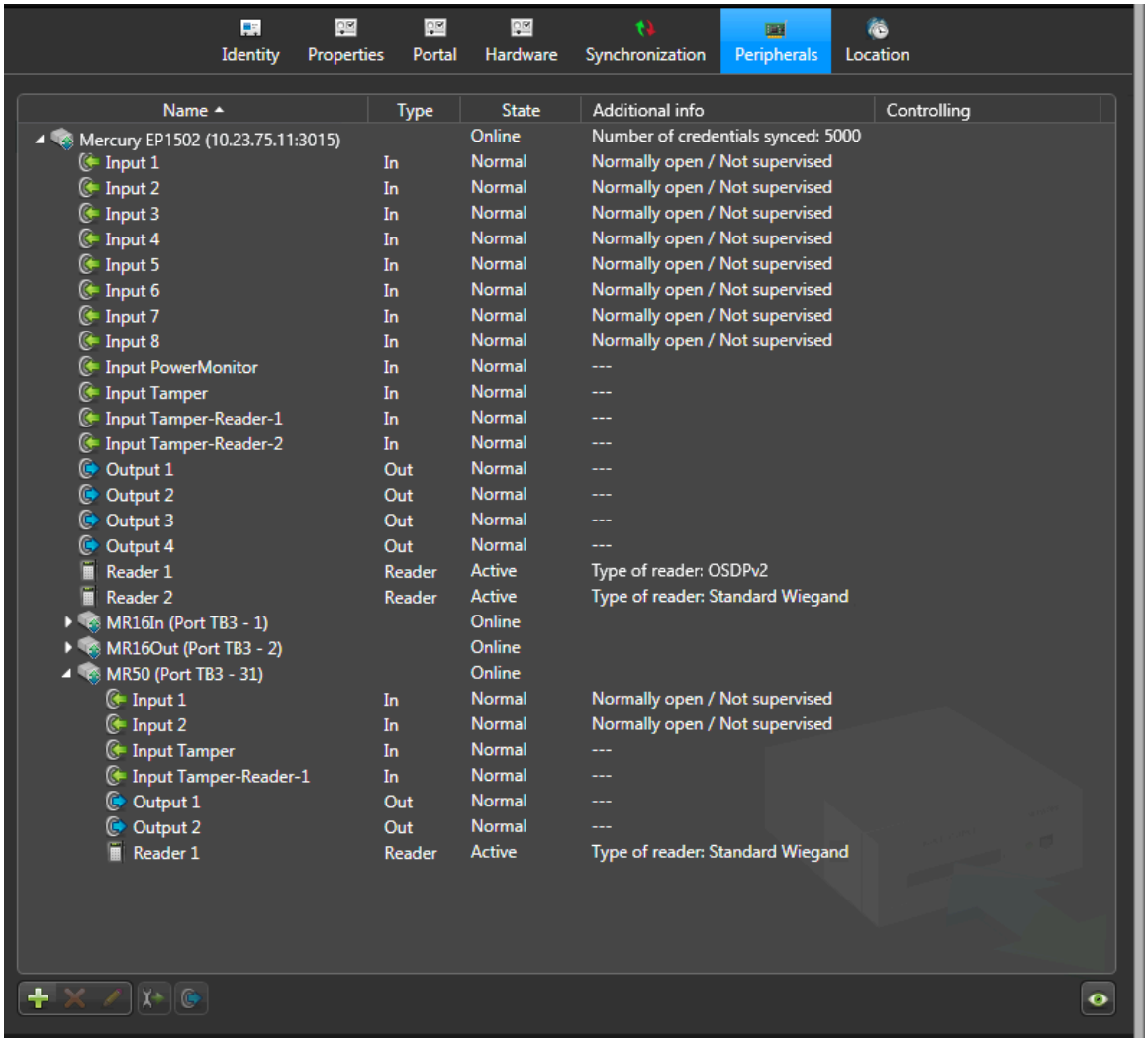


REMARQUE : Vous pouvez configurer quatre préréglages personnalisés différents sur les entrées de votre contrôleur Mercury. Pour les utilisateurs qui passent d'une version antérieure de Security Center et qui ont configuré une valeur personnalisée, le préréglage apparaît sous **Personnalisé 1** dans la liste **Lignes de limites AD**.

7 Cliquez sur **OK** au bas de la boîte de dialogue.

8 Cliquez sur **Appliquer**.

Le contrôleur Mercury ainsi que tous ses sous-tableaux et périphériques connectés sont affichés dans la page *Périphériques*.



L'ajout de modules d'interface à l'unité Synergis entraîne un redémarrage logiciel de l'unité. Durant ce processus, l'unité Synergis et tous les périphériques associés sont affichés hors ligne (en rouge).

9 Sélectionnez chaque appareil d'E/S et lecteur découvert, et configurez leurs propriétés au besoin.

Pour les lecteurs OSDP (Secure Channel), voir Ajouter des lecteurs OSDP (Secure Channel) à un contrôleur Mercury, page 162.

10 Testez le câblage et la configuration en déclenchant les entrées et sorties.

L'état de l'E/S déclenchée change en temps réel à l'écran.

REMARQUE : L'activité des lecteurs n'est pas affichée sur la page *Périphériques*.

Lorsque vous avez terminé

Le cas échéant, ajoutez les tableaux MR51e au contrôleur Mercury, puis reproduisez le câblage physique des modules d'interface aux portes et zones dans Security Center.

Configurer les réglages des contrôleurs Mercury dans Synergis Appliance Portal

Vous pouvez configurer les paramètres de vos contrôleurs Mercury sur le Synergis[MC] Appliance Portal.

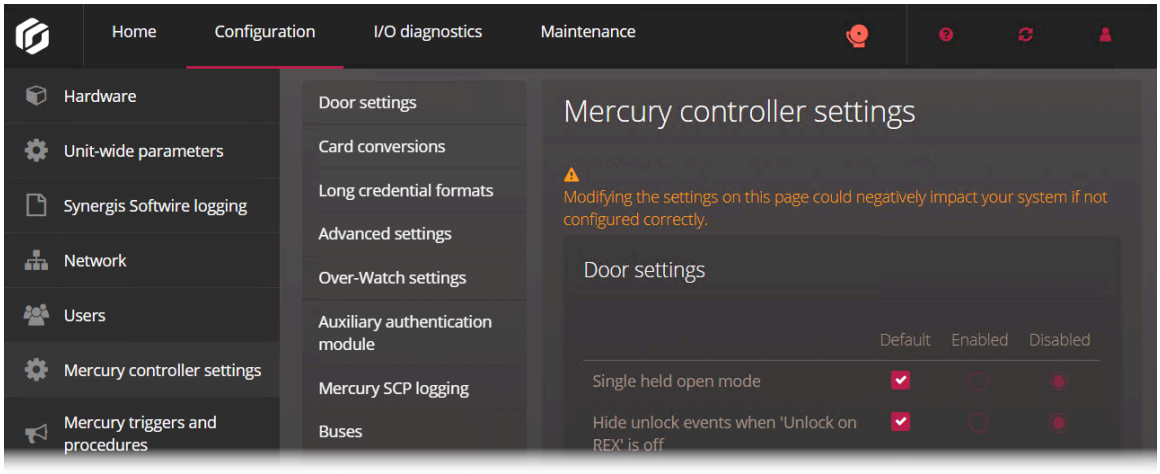
À savoir

Tout le matériel affecté à une porte ou à un ascenseur doit être contrôlé par le même contrôleur Mercury sous la même unité Synergis[MC] Cloud Link pour qu'il puisse fonctionner lorsque l'unité Synergis Cloud Link est hors ligne.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Réglages de contrôleur Mercury**.



3 Cliquez sur l'onglet **Réglages de porte** dans le menu latéral, et configurez les réglages suivants selon vos besoins :

- **Mode un seul entrebâillement :** Ignorez les événements *Porte entrebâillée trop longtemps* qui surviennent après le premier événement tant que la porte reste ouverte.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.
- **Masquer les événements de déverrouillage lorsque 'Déverrouillage sur REX' est désactivé :** Le contrôleur Mercury envoie des événements de déverrouillage sur activation REX, que la porte soit déverrouillée ou non. Activez ce réglage pour masquer ces événements de déverrouillage. L'activation de ce réglage retarde la réception de tous les événements, afin que les faux événements de déverrouillage puissent être filtrés.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.
- **Désactiver le transfert de décision de l'hôte (mode hors ligne) :** Ce réglage est désactivé par défaut, ce qui signifie que le transfert de décision de l'hôte Mercury est activé, et que l'unité Synergis Cloud Link prend les décisions de contrôle d'accès. Lorsque ce réglage est activé, le transfert de décision de l'hôte Mercury est désactivé, ce qui signifie que les contrôleurs Mercury prennent leurs propres décisions comme s'ils étaient déconnectés de l'unité Synergis Cloud Link . Dans ce cas, certaines fonctionnalités avancées et les cartes qui ne sont pas encore synchronisées avec le contrôleur Mercury ne fonctionnent pas, mais la porte devient bien plus réactive.

  BONNE PRATIQUE : N'activez pas le réglage **Désactiver le transfert de décision de l'hôte (mode hors ligne)**, sauf en cas de mauvaise connexion réseau entre l'unité Synergis Cloud Link et les

contrôleurs Mercury. Pour en savoir plus, voir Différences entre l'activation et la désactivation du transfert de décision de l'hôte, page 146.

- **Accès accordé silencieux :** Les lecteurs ne bipent pas lorsque l'accès est accordé.
- **Accès refusé silencieux :** Les lecteurs ne bipent pas lorsque l'accès est refusé.
- **Inhiber les événements Porte forcée :** Les événements *Porte forcée* sont désactivés.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.
- **Inhiber les événements « Défaut moteur » sur les verrous Schlage :** Les événements *Défaut moteur* des verrous Schlage sont désactivés.

  REMARQUE : Ce réglage n'affecte pas les événements *Défaut moteur* provenant d'autres appareils.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.
- **Inhiber les événements 'Perte RF' des verrous Schlage :** Les événements *Perte RF* des verrous Schlage sont désactivés.

  REMARQUE : Ce réglage n'affecte pas les événements *Perte RF* provenant d'autres appareils.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.
- **Témoin LED du lecteur éteint lorsque verrouillé :** Les témoins LED des lecteurs OSDP sont désactivés lorsque la porte associée est en état verrouillé normal.
- **Contrôle de secteur natif Mercury :** Active les fonctions natives Mercury d'antiretour, de capacité maximale et de sas sur le contrôleur Mercury. Pour en savoir plus, voir Limitations du contrôle de secteur natif Mercury, page 148.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.
- **Mode REX délai d'accès prolongé :** Les portes restent déverrouillées tant que l'entrée REX est active, et durant le délai d'accès normal qui suit. En l'absence d'un capteur de porte, la porte reste déverrouillée tant que l'entrée REX est active ou durant le délai d'accès normal, selon la durée qui est la plus longue.

  Cela permet d'éviter que les portes contrôlées par un capteur de mouvement se verrouillent et

  déverrouillent plusieurs fois par minute. Cette fonctionnalité nécessite le micrologiciel Mercury 1.29.1 ou ultérieur.

  REMARQUE : Vous pouvez également configurer ce réglage au niveau de chaque porte.
- **Événements « Demande de sortie » en direct :** Change la manière dont Synergis[MC] Softwire traite les événements *Demande de sortie* sur les contrôleurs Mercury LP et MP, afin que les horodatages des événements soient référencés avec précision. Ce réglage est activé par défaut.
- **Programmer les procédures LED de l'alarme de porte :** Fait en sorte que les lecteurs associés aux contrôleurs Mercury suivent les séquences Synergis Softwire de témoins LED et d'avertisseur sonore au lieu de celles de Mercury pour les alarmes de porte.

  REMARQUE : Lorsque ce réglage est désactivé et que des événements *Porte forcée* et *Porte entrebâillée trop longtemps* sont générés, les témoins LED sur les lecteurs associés ne clignotent pas.

  Effectuez un redémarrage du logiciel, puis réinitialisez les contrôleurs Mercury si vous modifiez ce réglage.
- **Recevoir les événements de contrainte lorsque la contrainte est désactivée :** Entraîne le déclenchement des événements *Accès refusé : Code PIN non valable* et *Code PIN de contrainte saisi* dans Security Center si quelqu'un saisit un code PIN de contrainte lorsque le réglage **Code PIN de contrainte** est désactivé dans Config Tool.

4 Cliquez sur l'onglet **Conversions de cartes**, dans le menu latéral et configurez les réglages suivants selon vos besoins :

Effectuez un redémarrage du logiciel si vous modifiez l'un de ces réglages.

- **Casi M5 56 -> 40**
- **Ambiguous HID 1441 -> 56**
- **Conversion avec perte pour les identifiants de plus de 52 bits :** Corrige un bug dans les versions de Synergis Softwire antérieures à la 10.10 qui pouvait entraîner des problèmes avec les identifiants de 52 à 64 bits.
- **FASC-N 200 bits vers 128 bits :** Toutes les cartes se rapportent à la version 128 bits. Ce réglage est utilisé avec les dispositions de bases de données FICAM ou Identifiants longs.
- **Ajouter un traducteur F2F vers Wiegand :** Ajoutez ou configurez d'autres traducteurs.

5 Cliquez sur l'onglet **Formats d'identifiants longs** dans le menu latéral, puis configurez l'option suivante :

- **Longueur de format Wiegand (bits) :** Les formats d'identifiants longs pour les contrôleurs Mercury ne sont pas configurés automatiquement dans Security Center. Configurez le format manuellement en entrant une valeur entre 64 et 240, puis en cliquant sur **Ajouter**. Ce réglage est utilisé avec les dispositions de bases de données FICAM ou Identifiants longs.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.

6 Cliquez sur l'onglet **Options avancées** dans le menu latéral, et configurez les réglages suivants selon vos besoins :

Effectuez un redémarrage du logiciel si vous modifiez l'un de ces réglages.

- **Contrôle du chiffrement SIO :** Active le chiffrement sur le bus RS-485 entre les contrôleurs EP ou Honeywell et leurs cartes SIO en aval, ou entre les contrôleurs LP et les cartes SIO plus anciennes. Les contrôleurs LP avec cartes SIO S3 utilisent le chiffrement du canal indépendamment de ce réglage.

  BONNE PRATIQUE :

  - Limitez les mises à niveau en masse à 10 cartes SIO pour un même contrôleur EP.
  - Avant de mettre à niveau plusieurs cartes SIO, désactivez le réglage **Contrôle du chiffrement SIO**.
- **Pas de LCA sans porte :** Les lecteurs ne sont pas préconfigurés lorsque les unités SIO sont ajoutées, et les diagnostics d'E/S ne signalent pas les lectures provenant de lecteurs non associés. Ce réglage élimine les problèmes liés à l'inscription de plus de 64 ports de lecteurs sur un contrôleur Mercury ou à l'utilisation de portes sans lecteur dépassant également ce seuil.
- **Deux lecteurs OSDP par port de lecteur :** Permet à une unité LP1502, LP4502, MP1502, MP4502, MR50-S3 et MR52-S3 de prendre en charge deux lecteurs OSDP par port.

  - Pour les unités LP1502, LP4502, MR50-S3 et MR52-S3, cela nécessite Security Center 5.10.4.0 ou une version ultérieure.
  - Pour les unités MP1502 et MP4502, cela nécessite Security Center 5.12.1.0 ou une version ultérieure.
- **Prise en charge de la piste magnétique :** Ce réglage est activé par défaut, et permet la prise en charge de huit formats de carte Wiegand par contrôleur Mercury. Pour chacun des huit formats de carte Wiegand, des formats de carte à piste magnétique correspondants sont créés automatiquement. Lorsque le réglage est désactivé, chaque contrôleur Mercury peut prendre en charge jusqu'à 16 formats de carte Wiegand, et aucun format de carte à piste magnétique n'est créé automatiquement.

7 Cliquez sur l'onglet **Réglages Over-Watch** dans le menu latéral, puis sélectionnez le réglage **Module externe LP4502 Over-Watch** pour activer le module externe Over-Watch sur tous les contrôleurs LP4502 sous l'unité Synergis Cloud Link . Le module externe Over-Watch n'est nécessaire que pour l'intégration BEST Wi-Q via Mercury.

Pour en savoir plus, voir Configurer le module externe Over-Watch pour l'intégration BEST Wi-Q, page 190.

8 Cliquez sur l'onglet **Module d'authentification auxiliaire** dans le menu latéral, et sélectionnez **Désactivé**, **PivClass** ou **TIEntryPoint**.

Ce réglage est utilisé avec la disposition de base de données FICAM et le module externe adapté pour le contrôleur LP4502.

9 Cliquez sur l'onglet **Journalisation Mercury SCP** dans le menu latéral, cliquez sur **Démarrer la journalisation** pour des options de journalisation propres à Mercury, puis entrez la durée en jours de la journalisation.

10 Cliquez sur l'onglet **Bus** dans le menu latéral, et cliquez sur **Réinitialiser** pour chaque contrôleur ou sur **Réinitialiser tout** pour que les nouveaux réglages soient envoyés à tous les contrôleurs.

11 Cliquez sur l'onglet **Réglages de disposition de base de données** dans le menu latéral, puis configurez les options suivantes :

a) Sélectionnez une disposition de base de données dans la liste.

La disposition **Fonctionnalités enrichies (valeur par défaut)** est adaptée à la plupart des cas. Les autres dispositions de bases de données répondent à des exigences particulières. Réinitialisez les contrôleurs lorsque vous modifiez la disposition de base de données.

Pour en savoir plus sur les différentes dispositions de bases de données, voir Dispositions de bases de données pour les contrôleurs Mercury, page 150.

b) Configurez la longueur maximale du code PIN.

Longueur maximale du code PIN par défaut est sélectionné par défaut. La valeur par défaut pour toutes les dispositions est de **6**. Pour modifier cette valeur, sélectionnez **Longueur maximale du code PIN personnalisée**, puis entrez une nouvelle valeur dans le champ **Longueur maximale du code PIN**.

REMARQUE : La diminution de cette valeur sert généralement à éviter d'avoir à appuyer sur la touche # à la fin des codes PIN à quatre chiffres, lorsque le système n'utilise que des codes PIN à quatre chiffres. La définition de la **Longueur maximale du code PIN** sur une valeur supérieure à celle prise en charge par la disposition de base de données sélectionnée entraîne l'arrêt de vos contrôleurs Mercury, et les codes PIN dépassant la **Longueur maximale du code PIN** ne fonctionnent pas.

Effectuez un redémarrage du logiciel si vous modifiez ce réglage.

12 Cliquez sur l'onglet **Réglages de code PIN** dans le menu latéral, puis configurez les options suivantes :

- **Inclure et ajouter des zéros de remplissage aux codes PIN :** Pour ajouter des zéros à vos codes PIN, sélectionnez **Personnalisé**, puis entrez une valeur dans **Longueur du code PIN après l'ajout des zéros de remplissage**. Par exemple, la longueur maximale du code PIN est de six chiffres, et vous entrez la valeur **4** dans **Longueur du code PIN après l'ajout des zéros de remplissage**. Si le code PIN d'origine est **9**, le code devient **0009**. Si le code PIN d'origine est **123**, le code devient **0123**.

  Effectuez un redémarrage du logiciel si vous modifiez ce réglage.

  Pour en savoir plus, voir À propos de la configuration des codes PIN avec zéros de remplissage pour les intégrations Mercury, page 154.

13 Cliquez sur l'onglet **Réglages spécifiques aux lecteurs OSDP** dans le menu latéral, puis configurez les réglages suivants :

- **Correction LED Nexus et Verint OSDP :** Corrige un problème de témoin LED associé à certains lecteurs OSDP Nexus et Verint.
- **Ignorer la programmation des LED :** Résout un problème sur les lecteurs OSDP où la LED s'éteint pendant quelques secondes lorsque la porte se verrouille à nouveau après avoir été ouverte.

14 Cliquez sur l'onglet **Règle d'escorte de visiteur et règle de deuxième personne** dans le menu latéral, puis configurez l'option suivante :

- **Délai maximal entre présentations de la carte :** S'applique à toutes les portes gérées par les contrôleurs Mercury.

  Effectuez un redémarrage du logiciel, puis réinitialisez les contrôleurs Mercury si vous modifiez ce réglage.

15 Cliquez sur l'onglet **Comportement des portes pour les cartes SIO hors ligne** dans le menu latéral et sélectionnez l'une des options suivantes :

Ce paramètre s'applique uniquement aux portes dont le lecteur et le verrou se trouvent sur la même carte Mercury SIO. Les portes sans lecteur ne sont pas concernées. Lorsque la porte est déverrouillée en

raison de ce réglage, le comportement du témoin LED du lecteur ne correspond pas aux différents états de verrouillage de la porte.

IMPORTANT : Les événements qui surviennent pendant que la carte SIO est déconnectée du contrôleur Mercury ne sont pas enregistrés.

- **Par défaut (verrouillé) :** Lorsque la carte SIO perd la connexion au contrôleur Mercury, les portes qu'elle contrôle sont verrouillées, peu importe leur état avant la perte de connexion.
- **Déverrouillé :** Lorsque la carte SIO perd la connexion au contrôleur Mercury, les portes qu'elle contrôle sont déverrouillées, peu importe leur état avant la perte de connexion.
- **Verrouillé :** Lorsque la carte SIO perd la connexion au contrôleur Mercury, les portes qu'elle contrôle sont verrouillées, peu importe leur état avant la perte de connexion.
- **Code d'installation :** Lorsque la carte SIO perd la connexion au contrôleur Mercury, seuls les identifiants configurés avec les formats de cartes et codes d'installation peuvent accéder aux portes. Si aucun format de carte ou code d'installation n'est configuré, les portes contrôlées par la carte SIO sont verrouillées, peu importe leur état avant la perte de connexion.

  Pour en savoir plus, voir Configurer les cartes SIO Mercury hors ligne pour accorder l'accès via les codes d'installation, page 156.

  Effectuez un redémarrage logiciel si vous sélectionnez le réglage **Code d'installation**.

16 Pour rétablir toutes les valeurs par défaut, à l'exception des réglages de disposition de base de données, cliquez sur **Rétablir les valeurs par défaut**.

IMPORTANT : Il n'est pas possible de récupérer les réglages antérieurs.

17 Cliquez sur **Enregistrer**.

Différences entre l'activation et la désactivation du transfert de décision de l'hôte

Le comportement de votre système de contrôle d'accès diffère selon que la fonctionnalité de transfert de décision d'hôte Mercury est activée ou désactivée.

Vous pouvez activer ou désactiver le transfert de décision de l'hôte depuis Synergis[MC] Appliance Portal. Accédez à **Configuration** > **Réglages de contrôleur Mercury** > **Réglages de porte**, puis configurez le paramètre **Désactiver le transfert de décision de l'hôte (mode hors ligne)**. Ce paramètre est désactivé par défaut. Le transfert de décision de l'hôte est donc activé et c'est l'unité Synergis[MC] Cloud Link qui prend les décisions de contrôle d'accès.

Reportez-vous au tableau qui suit pour savoir dans quelles circonstances le système de contrôle d'accès se comporte différemment, selon que le transfert de décision de l'hôte est activé ou désactivé.

	Transfert de décision de l'hôte activé (par défaut)	Transfert de décision de l'hôte désactivé
Décisions de contrôle d'accès prises par	Synergis Cloud Link	Contrôleur Mercury
Lecture de carte pour l'heure de déverrouillage des portes	0 à 5[1] secondes	Inférieure à 1 seconde
Supprimer un titulaire de cartes ou un identifiant dans Security Center • Versions antérieures à 5.11.3.5 • 5.12.0.0	Rapide	Jusqu'à 1 heure pour propager les modifications
Supprimer un titulaire de cartes ou un identifiant dans Security Center • 5.11.3.6 ou ultérieure • 5.12.1.0 ou ultérieure	Pas de différence dans le comportement	

	Transfert de décision de l'hôte activé (par défaut)	Transfert de décision de l'hôte désactivé
Désactiver un titulaire de cartes ou un identifiant manuellement ou automatiquement à sa date d'expiration	Pas de différence dans le comportement	
Révoquer l'accès en supprimant un titulaire de cartes d'un groupe titulaires de cartes ou d'une règle d'accès, en modifiant des horaires, etc. **REMARQUE :** Révoquer l'accès en supprimant ou désactivant un titulaire de cartes non inclus.	Rapide	Jusqu'à 1 heure pour propager les modifications
Sas, antiretour, et occupation max.	Pris en charge	L'option **Contrôle de secteur natif Mercury** doit être activée.

[1] Cette opération peut prendre jusqu'à 5 secondes, en fonction des conditions de réseau.

Activer la prise en charge des identifiants longs sur les contrôleurs Mercury

Avant d'utiliser des identifiants jusqu'à 240 bits avec vos contrôleurs Mercury, vous devez activer la prise en charge des identifiants longs sur votre unité Synergis[MC] Cloud Link .

Avant de commencer

Vérifiez les points suivants :

- Votre unité Synergis Cloud Link exécute Synergis[MC] Softwire 11.0 ou ultérieur, et elle est en ligne et connectée à votre réseau.
- Les contrôleurs Mercury avec lesquels vous souhaitez utiliser les identifiants longs sont équipés du micrologiciel 1.29.1 ou ultérieur.

À savoir

Comme les identifiants de 64 bits ou plus ne sont pas automatiquement synchronisés avec Mercury, vous devez les activer manuellement.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Réglages de contrôleur Mercury**.

3 Cliquez sur **Réglages de disposition de base de données** dans le menu latéral, puis sélectionnez la disposition de base de données **Identifiants longs** dans la liste.

4 Cliquez sur l'onglet **Formats d'identifiants longs** dans le menu latéral, et entrez la longueur d'identifiant que vous souhaitez utiliser.

La valeur doit être comprise entre 64 et 240.

5 Cliquez sur **Ajouter**.

Vous pouvez ajouter jusqu'à huit formats d'identifiants différents.

6 Cliquez sur **Enregistrer**.

7 Effectuez un redémarrage logiciel :
   a) Dans le menu du haut, cliquez sur **Redémarrer** > **Redémarrer le logiciel**.
8 Après le redémarrage logiciel, reconnectez-vous à l'unité Synergis Cloud Link .
9 Sur la page *Réglages de contrôleur Mercury*, cliquez sur l'onglet **Bus** dans le menu latéral.
10 Cliquez sur **Réinitialiser** pour les contrôleurs qui doivent prendre en charge les identifiants longs.

Vous pouvez à présent utiliser les nouveaux formats d'identifiants que vous avez activés avec vos contrôleurs Mercury.

Limitations du contrôle de secteur natif Mercury

Le contrôle de secteur natif Mercury, qui concerne les sas, la capacité maximale et l'antiretour, présente certaines limites.

- **Antiretour souple :** L'événement *Violation antiretour* pour l'antiretour souple est généré lorsque la porte s'ouvre, et pas lorsque l'accès est accordé.

  Si vous configurez l'antiretour souple sur une porte sans capteur de porte, les événements *Violation antiretour* ne sont jamais générés, car la porte ne s'ouvre jamais.

  L'antiretour souple sur les appareils Mercury ne prend pas en charge un délai de présence.
- **Antiretour physique :** Mercury ne prend pas en charge les éléments suivants :
  - L'antiretour physique qui n'est pas également réglé sur **Strict**.
  - L'antiretour physique et strict quand le réglage **Activer l'antiretour global** est activé dans le rôle Gestionnaire d'accès de Config Tool.
- **Délai d'antiretour :** Mercury prend en charge un délai d'expiration pour l'antiretour strict et physique. Si un **Délai de présence** est configuré pour un secteur, l'antiretour physique refuse l'accès au titulaire de cartes jusqu'à l'expiration du délai, puis lui accorde à nouveau l'accès au secteur.

  Cela déclenche un événement *Violation antiretour* pour l'antiretour souple, puis l'antiretour physique s'applique à nouveau au titulaire de cartes jusqu'à expiration du délai. Cette configuration n'est pas compatible avec les secteurs contrôlés par Synergis^{MC} Softwire.
- **Modèle « un pour un » de Mercury pour les titulaires de cartes et les identifiants :** Si un titulaire de cartes dans Security Center a plusieurs identifiants de type carte, Mercury considère que chaque identifiant appartient à un titulaire de cartes distinct.

  Cela signifie que chaque identifiant peut servir à pénétrer une fois dans un secteur sans déclencher de violation antiretour. De même, si le titulaire de cartes utilise deux identifiants différents pour entrer dans un secteur avec des restrictions antiretour et de capacité maximale, le titulaire de cartes compte pour deux personnes dans le calcul de capacité maximale.
- **Contourner l'antiretour :** Aucun événement *Violation antiretour* n'est généré pour les titulaires de cartes pour qui l'option **Contourner les règles d'antiretour** est activée.
- **Sas et antiretour :** Les sas et l'antiretour ne fonctionnent que si toutes les portes configurées pour le secteur utilisant ces fonctionnalités sont gérées par le même contrôleur Mercury.

  Un contrôleur Mercury peut avoir des portes dans de nombreux secteurs et qui utilisent toute combinaison de ces fonctionnalités, ou aucune d'elles. Dans les secteurs où vous n'utilisez pas ces fonctionnalités, les portes peuvent être gérées par plusieurs contrôleurs Mercury.

  Une porte gérée par un contrôleur Mercury ne peut être utilisée en tant qu'entrée et sortie que d'un seul secteur avec un sas ou avec l'antiretour, bien que dans Security Center, vous puissiez configurer plusieurs secteurs pour une même porte.
- **Sas :** Si une partie du sas est hors ligne en raison de la panne d'une seule carte SIO, le sas empêche le déverrouillage ou l'ouverture des autres portes qui composent le sas.

  Lorsque le sas natif est activé, les options **Contourner** et **Confinement** dans Config Tool ne sont pas prises en charge. Elles peuvent être configurées, mais n'ont aucun effet.

- **Antiretour sur horaire :** L'antiretour sur horaire n'est pas pris en charge au niveau Mercury. Synergis Softwire active et désactive l'antiretour sur horaire tant que les contrôleurs Mercury sont connectés ou lorsque qu'ils se reconnectent, et l'horaire est réglé sur *Toujours*. L'état Mercury n'est pas modifié par l'horaire en lui-même, et il conserve donc son état au moment de la déconnexion.
- **Divergences de comptage d'individus :** Puisque Mercury suit ses propres secteurs, le comptage d'individus peut parfois diverger entre votre Synergis[MC] Cloud Link, la tâche *Comptage d'individus* de Security Desk et le contrôleur Mercury. Pour éviter que ces divergences créent des problèmes, il est recommandé de réinitialiser régulièrement le comptage d'individus en procédant de la manière suivante :
  - Sur le Synergis[MC] Appliance Portal, accédez à **Configuration** > **Paramètres de l'unité** > **Configuration de secteur**, puis programmez une réinitialisation quotidienne ou hebdomadaire.
    Le compteur d'individus est alors réinitialisé sur le Synergis Cloud Link et sur les contrôleurs Mercury qu'il gère.
  - Dans Config Tool, réinitialisez le compteur dans la tâche *Comptage d'individus* en utilisant l'action *Réinitialiser le comptage d'individus* dans les tâches planifiées ou dans les associations événement-action pour chaque secteur que vous souhaitez réinitialiser.

Configurer le mode REX délai d'accès prolongé Mercury par porte

Avant de pouvoir activer le mode REX délai d'accès prolongé sur des portes particulières, vous devez créer un champ personnalisé de porte dans Security Center.

À savoir

- Cette fonctionnalité nécessite le micrologiciel Mercury 1.29.1 ou ultérieur.
- Lorsque le mode REX avec délai d'accès prolongé est activé, la porte reste déverrouillée tant que l'entrée REX est active, et durant le délai d'accès normal qui suit. Cela permet d'éviter que les portes contrôlées par un capteur de mouvement se verrouillent et déverrouillent plusieurs fois par minute.
- Tenez compte des limitations suivantes :
  - En cas de redémarrage du contrôleur Mercury, la porte revient à son état normal tant que le REX n'est pas à nouveau déclenché.
  - En l'absence d'un capteur de porte, la porte reste déverrouillée tant que l'entrée REX est active ou durant le délai d'accès normal, selon la durée qui est la plus longue.
  - La porte se verrouille à la fin d'un horaire de déverrouillage indépendamment de l'état du REX.
- Si vous souhaitez contrôler toutes les portes gérées par Mercury sous un même Synergis[MC] Cloud Link en même temps, vous pouvez configurer le paramètre du **Mode REX délai d'accès prolongé** sur le portail de l'appareil Synergis[MC] Appliance Portal.

  REMARQUE : Si vous créez le champ personnalisé dans Security Center, le paramètre sur les unités Synergis Cloud Link inscrites auprès du système concerné est ignoré.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Système* et cliquez sur la vue **Paramètres généraux**.

2 Cliquez sur l'onglet **Champs personnalisés**, puis cliquez sur **Ajouter un élément** ().

3 Dans la boîte de dialogue *Ajouter un champ personnalisé*, configurez les options suivantes :

- **Type d'entité :** Sélectionnez **Porte**.
- **Type de donnée :** Sélectionnez **Booléen**.
- **Nom :** Entrez `Mode REX délai d'accès prolongé`.
- **Valeur par défaut :** Sélectionnez cette option si vous souhaitez que les portes utilisent par défaut le mode REX délai d'accès prolongé.

4 Cliquez sur **Enregistrer et fermer**, puis sur **Appliquer**.

Dispositions de bases de données pour les contrôleurs Mercury

Différentes dispositions de bases de données sont disponibles pour vos contrôleurs Mercury.

Reportez-vous aux tableaux suivants pour savoir quelle disposition de base de données répond à vos besoins.

Disposition de base de données enrichie (par défaut)

Modèle	Nombre maximal de titulaires de cartes
EP1501, EP1502	145 000

Modèle	Nombre maximal de titulaires de cartes
EP2500	370 000
M5-IC, MS-ICS	370 000
EP4502	419 000
LP1501, LP1502	200 000
LP2500	419 000
LP4502	500 000
MP1502	200 000
MP4502	500 000

Fonctionnalités prises en charge	Pris en charge
Longueur de code PIN par défaut	6
Longueur maximale du code PIN	10
Contrôle de secteur natif (antiretour, sas et capacité maximale)	Oui
Règle de deuxième personne et escorte de visiteurs	Oui
Longueur maximale des identifiants (en bits)	64
Ascenseurs	Oui

Disposition de base de données pour identifiants longs

Modèle	Nombre maximal de titulaires de cartes
EP1501, EP1502	80 000
EP2500	210 000
M5-IC, MS-ICS	214 000
EP4502	210 000
LP1501, LP1502	111 000
LP2500	222 000
LP4502	444 000
MP1502	111 000
MP4502	444 000

Fonctionnalités prises en charge	Pris en charge
Longueur de code PIN par défaut	6
Longueur maximale du code PIN	10
Contrôle de secteur natif (antiretour, sas et capacité maximale)	Oui
Règle de deuxième personne et escorte de visiteurs	Oui
Longueur maximale des identifiants (en bits)	240
Ascenseurs	Oui

Disposition de base de données pour codes PIN longs

Modèle	Nombre maximal de titulaires de cartes
EP1501, EP1502	80 000
EP2500	300 000
M5-IC, MS-ICS	300 000
EP4502	300 000
LP1501, LP1502	150 000
LP2500	350 000
LP4502	500 000
MP1502	150 000
MP4502	500 000

Fonctionnalités prises en charge	Pris en charge
Longueur de code PIN par défaut	15
Longueur maximale du code PIN	15
Contrôle de secteur natif (antiretour, sas et capacité maximale)	Oui
Règle de deuxième personne et escorte de visiteurs	Oui
Longueur maximale des identifiants (en bits)	64
Ascenseurs	Oui

Disposition de base de données à grande échelle

Modèle	Nombre maximal de titulaires de cartes
EP1501, EP1502	250 000
EP2500	560 000
M5-IC, MS-ICS	560 000
EP4502	600 000
LP1501, LP1502	250 000
LP2500	600 000
LP4502	600 000
MP1502	250 000
MP4502	600 000

Fonctionnalités prises en charge	Pris en charge
Longueur de code PIN par défaut	6
Longueur maximum du code PIN	6
Contrôle de secteur natif (antiretour, sas et capacité maximale)	Non
Règle de deuxième personne et escorte de visiteurs	Non
Longueur maximale des identifiants (en bits)	64
Ascenseurs	Non

Disposition de base de données FICAM

N'utilisez la disposition de base de données FICAM que si vous souhaitez respecter la norme Federal Information Processing Standard 201 (FIPS 201) de l'administration américaine avec des identifiants PIV (Personal Identity Verification), PIV-I (Personal Identity Verification-Interoperable) ou CIV (Commercial Identity Verification). Cette disposition de base de données n'est conçue que pour une utilisation avec les contrôleurs Mercury LP4502.

Pour en savoir plus, voir le Guide de l'utilisateur de HID pivClass pour Security Center ou la Note technique Utiliser l'authentification TI EntryPoint sur Mercury LP4502.

Modèle	Nombre maximal de titulaires de cartes
EP1501, EP1502	98 000
EP2500	180 000
M5-IC, MS-ICS	100 000
EP4502	180 000

Modèle	Nombre maximal de titulaires de cartes
LP1501, LP1502	139 000
LP2500	279 000
LP4502	500 000

Fonctionnalités prises en charge	Pris en charge
Longueur de code PIN par défaut	6
Longueur maximum du code PIN	6
Contrôle de secteur natif (antiretour, sas et capacité maximale)	En ligne
Règle de deuxième personne et escorte de visiteurs	Oui
Longueur maximale des identifiants (en bits)	240
Ascenseurs	Oui

À propos de la configuration des codes PIN avec zéros de remplissage pour les intégrations Mercury

Avant de configurer les codes PIN avec des zéros de remplissage pour votre intégration Mercury sur le portail de l'appareil Synergis[MC], examinez les exigences et la manière dont les réglages **Longueur maximale du code PIN** et **Longueur du code PIN après l'ajout des zéros de remplissage** affectent vos codes PIN.

Conditions

Prérequis pour l'utilisation des identifiants de type code PIN avec les intégrations Mercury :

- Security Center 5.7 SR2 ou ultérieur est requis pour utiliser les codes PIN à six chiffres avec zéros de remplissage. Dans la 5.7 SR1 et les versions antérieures, les codes PIN à six chiffres avec zéros de remplissage ne fonctionnent pas. L'accès est accordé, mais vous ne recevez pas d'événement *Accès accordé* dans Security Center.
- Chaque titulaire de cartes doit avoir un badge et un seul identifiant de type code PIN.
- Si l'unité est réglée sur **Carte ou code PIN** alors que le titulaire de cartes n'a qu'un identifiant à code PIN, l'identifiant n'est pas synchronisé avec le contrôleur Mercury et ne fonctionne pas.

  Contournement : Créez et attribuez au titulaire de carte un faux identifiant carte.
- Les lecteurs à pavé numérique HID doivent prendre en charge l'option mode-00.

À propos de la longueur maximale du code PIN avec zéros de remplissage

Pour configurer des zéros de remplissage pour les codes PIN, modifiez le réglage **Longueur du code PIN après l'ajout des zéros de remplissage** sur la page *Réglages de contrôleur Mercury* du portail de l'appareil Synergis. Les réglages **Longueur du code PIN après l'ajout des zéros de remplissage** et **Longueur maximale du code PIN** s'influencent mutuellement des manières suivantes :

- Les codes PIN ne fonctionnent plus si la **Longueur du code PIN après l'ajout des zéros de remplissage** est supérieure à la **Longueur maximale du code PIN**.

- Des zéros de remplissage sont ajoutés aux codes PIN trop courts jusqu'à ce qu'ils atteignent la **Longueur du code PIN après l'ajout des zéros de remplissage**, pas la **Longueur maximale du code PIN**.
- Les codes PIN dont la longueur est supérieure ou égale à la **Longueur du code PIN après l'ajout des zéros de remplissage** sont valables dès lors qu'ils ne dépassent pas la **Longueur maximale du code PIN**.

La **Longueur maximale du code PIN** est réglée sur **6**. La **Longueur du code PIN après l'ajout des zéros de remplissage** est réglée sur **4**.

- Si le code PIN d'origine est **9**, le code devient **0009**.
- Si le code PIN d'origine est **123**, le code devient **0123**.
- Si le code PIN d'origine est **12345**, le code reste inchangé.

À propos des autorisations d'accès par le biais de codes d'installation avec les cartes Mercury SIO hors ligne

Découvrez la manière dont les décisions d'accès sont affectées lorsque vous configurez l'accès pour ne l'accorder qu'aux identifiants qui utilisent certains formats de carte et codes d'installation lorsque la carte SIO perd la connexion au contrôleur Mercury.

- Par défaut, Synergis Softwire prend en charge jusqu'à huit formats de carte par contrôleur Mercury. Chaque code d'installation que vous ajoutez compte comme un format de carte, même si les codes d'installation sont configurés pour le même format de carte.

  REMARQUE : Pour faire passer le nombre de formats de carte pris en charge à 16, vous pouvez désactiver l'option **Prise en charge de la piste magnétique** dans la section *Options avancées* de la page *Réglages de contrôleur Mercury*. La piste magnétique n'est pas prise en charge lorsque l'option **Code d'installation** est sélectionnée en tant que comportement de porte pour les cartes SIO hors ligne, même si l'option **Prise en charge de la piste magnétique** est activée.
- Lorsque la carte SIO perd la connexion au contrôleur Mercury et qu'aucun format de carte ou code d'installation n'est ajouté au portail de l'appareil Synergis[MC], les portes contrôlées par la carte SIO sont verrouillées, indépendamment de leur état avant la perte de connexion.
- Voici ce qui se produit lorsqu'un identifiant est valable dans Security Center, mais que son code d'installation n'a pas été ajouté sur le portail de l'appareil Synergis :
  - Si le contrôleur Mercury se déconnecte de l'unité Synergis Cloud Link, l'accès est refusé.
  - Si le contrôleur Mercury est connecté à l'unité Synergis Cloud Link, l'accès est accordé.

Contrôle de secteur natif Mercury, transfert de décision de l'hôte et antiretour

Lorsque vous configurez le comportement des portes quand les cartes SIO sont hors ligne pour utiliser les codes d'installation pour accorder l'accès, les décisions d'accès varient en fonction des autres fonctionnalités activées et de leurs interactions.

Voici les hypothèses utilisées dans cet exemple :

- L'option **Code d'installation** est sélectionnée en tant que comportement des portes pour les cartes SIO hors ligne sur le portail de l'appareil Synergis.
- Le titulaire de cartes 1 a un identifiant avec un code d'installation qui a été ajouté au portail de l'appareil Synergis.
- Le titulaire de cartes 2 a un identifiant avec un code d'installation qui n'a *pas* été ajouté au portail de l'appareil Synergis.
- L'antiretour est appliqué aux secteurs auxquels les titulaires de cartes veulent accéder.
- Le contrôleur Mercury est déconnecté de l'unité Synergis Cloud Link.

Réglage sur le portail de l'appareil Synergis		
Contrôle de secteur natif Mercury	Désactiver le transfert de décision de l'hôte (mode hors ligne)	Décision d'accès après un deuxième passage de badge

Réglage sur le portail de l'appareil Synergis		
Désactivé	Désactivé	• Le titulaire de cartes 1 reçoit une violation antiretour. • Le titulaire de cartes 2 reçoit une violation antiretour.
Désactivé	Activé	• L'antiretour ne fonctionne pas.
Activé	Désactivé	• Le titulaire de cartes 1 reçoit une violation antiretour. • Le titulaire de cartes 2 se voit refuser l'accès.
Activé	Activé	• Le titulaire de cartes 1 reçoit une violation antiretour. • Le titulaire de cartes 2 se voit refuser l'accès.

Configurer les cartes SIO Mercury hors ligne pour accorder l'accès via les codes d'installation

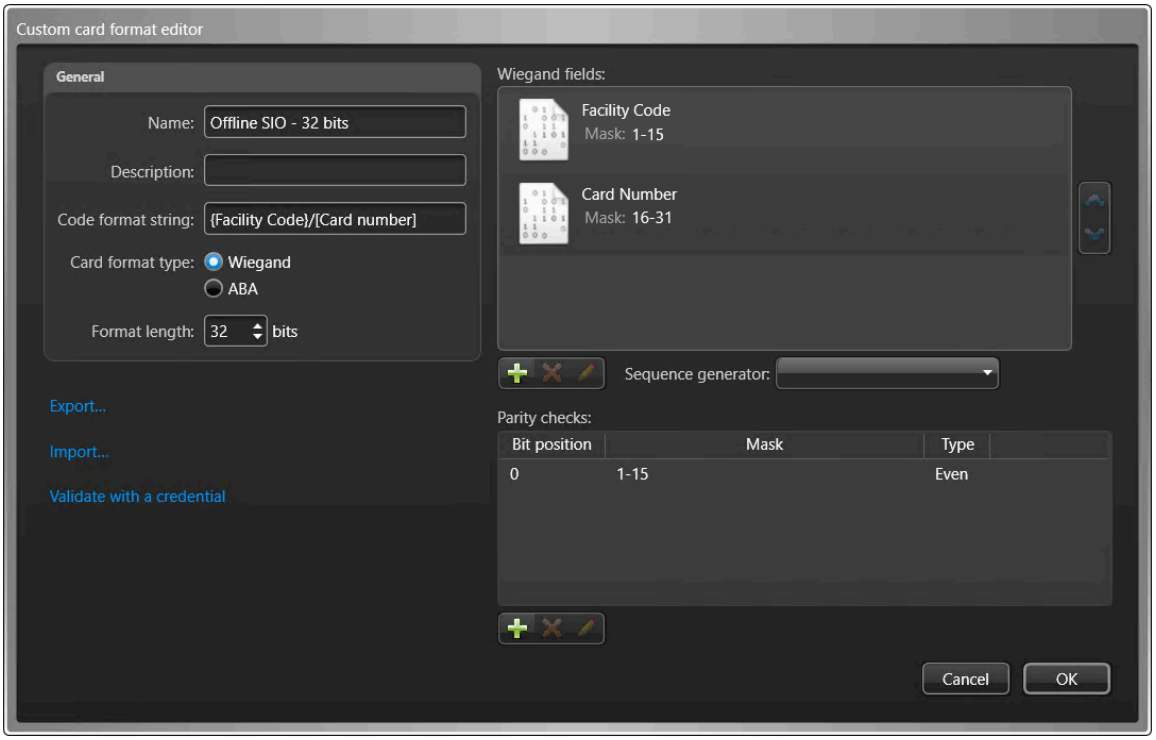
Vous pouvez configurer l'accès afin de ne l'accorder qu'aux identifiants dotés de certains formats de carte et codes d'installation ou de certains formats de carte bruts lorsque la carte SIO perd la connexion au contrôleur Mercury.

Avant de commencer

- **ATTENTION :** Configurer l'accès pour qu'il soit accordé par code d'installation ou format de carte lorsque la carte SIO perd la connexion au contrôleur Mercury diminue considérablement la sécurité de votre système. Lorsque cette option est configurée, aucun historique d'activité n'est disponible. Les événements qui surviennent pendant que la carte SIO est déconnectée du contrôleur Mercury ne sont pas enregistrés.
- Découvrez comment accorder l'accès via les formats de cartes et codes d'installation affecte les décisions d'accès.
- Pour utiliser un format de carte Wiegand personnalisé, créez-le dans Config Tool, puis exportez-le dans un fichier XML. Le format de carte personnalisé doit être configuré avec un champ Wiegand intitulé

`Facility` Code (Code d'installation). Le masque du champ Wiegand doit être une séquence ascendante de bits, d'une longueur maximale de 63 bits.

Exemple :



Pour en savoir plus, voir Créer un format de carte personnalisé.

Procédure

Pour accorder l'accès via un format de carte et un code d'installation :

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Réglages de contrôleur Mercury**.

3 Cliquez sur l'onglet **Comportement des portes pour les cartes SIO hors ligne** dans le menu latéral, puis sélectionnez **Code d'installation**.

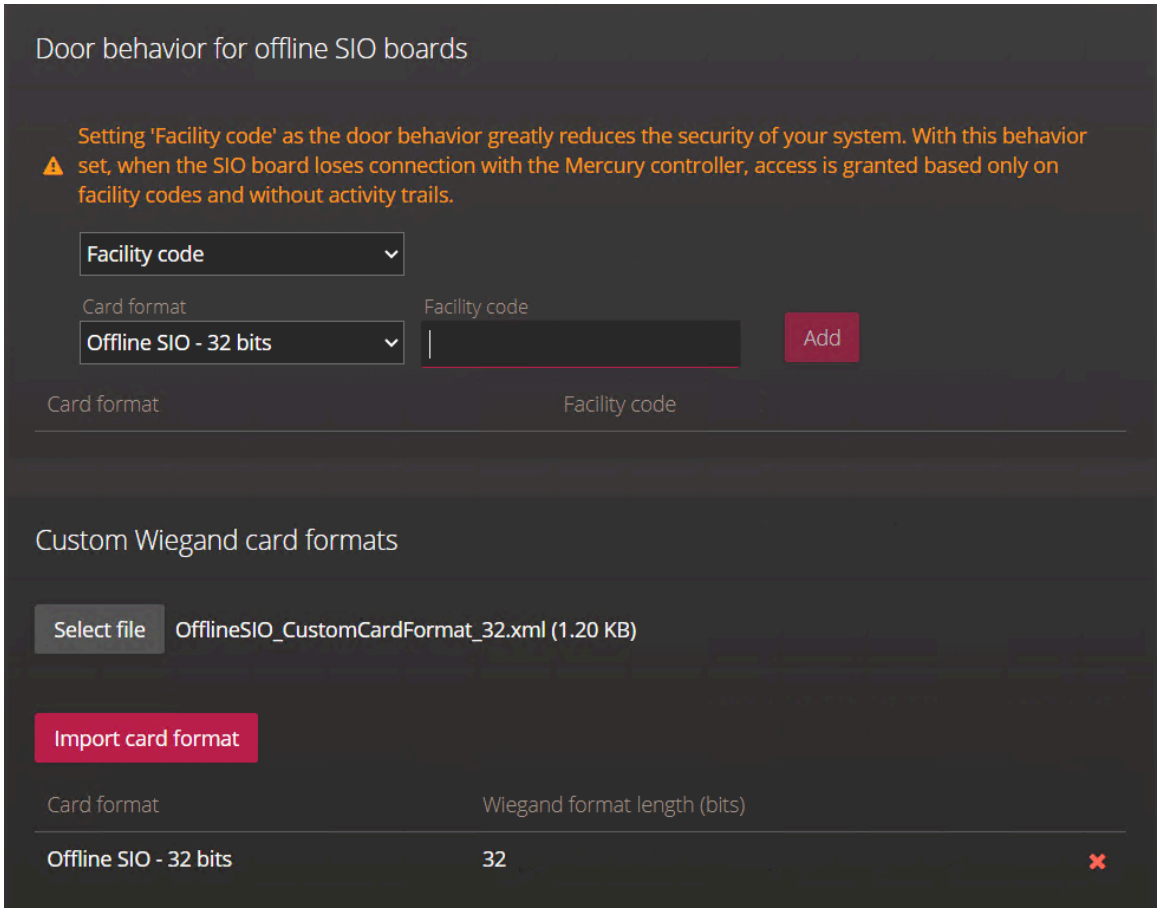
4 (Facultatif) Pour utiliser un format de carte personnalisé, procédez de la manière suivante :

a) Dans la section *Formats de carte Wiegand personnalisés*, cliquez sur **Sélectionner un fichier**, puis sélectionnez le fichier XML que vous avez exporté depuis Config Tool.

b) Cliquez sur **Importer un format de carte**.

Le format de carte personnalisé apparaît dans la section *Formats de carte Wiegand personnalisés*, et peut à présent être sélectionné dans la liste déroulante **Format de carte** de la section *Comportement des portes pour les cartes SIO hors ligne*.

Exemple :



5 Sélectionnez un format de carte dans la liste **Format de carte**, puis entrez une valeur dans le champ **Code d'installation**.

6 Cliquez sur **Ajouter**.

Le format de carte et le code d'installation configurés sont ajoutés à la liste.

7 Cliquez sur **Enregistrer**, puis effectuez un redémarrage logiciel.

L'accès n'est accordé qu'aux identifiants qui correspondent à la fois au format de carte et au code d'installation.

Pour accorder l'accès via un format de carte personnalisé brut :

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Réglages de contrôleur Mercury**.

3 Ajoutez le format de carte personnalisé en procédant de la manière suivante :

a) Cliquez sur l'onglet **Formats d'identifiants longs** dans le menu latéral, et entrez la longueur d'identifiant que vous souhaitez utiliser.

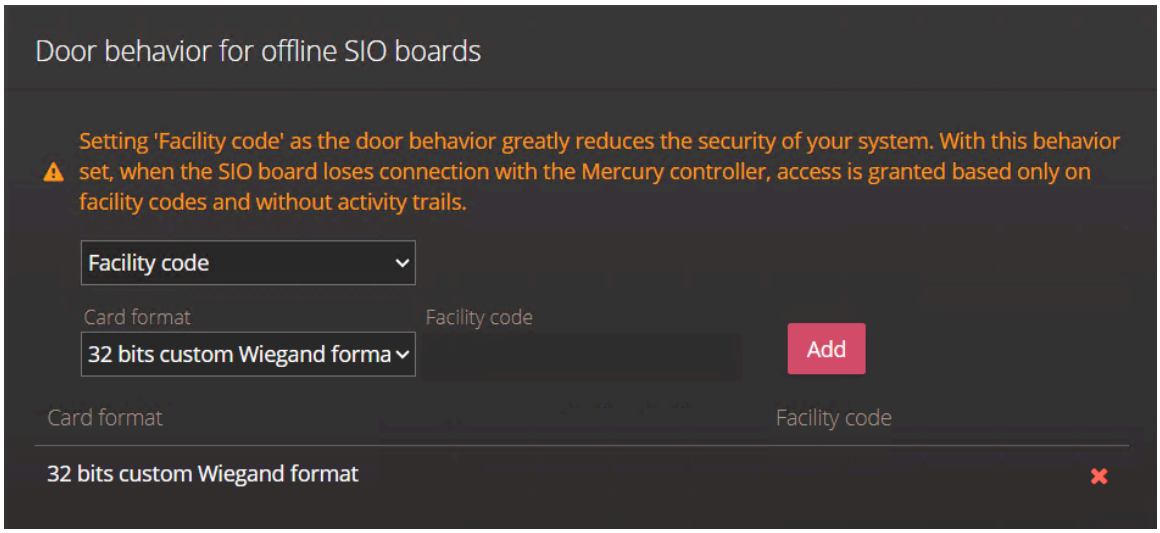
b) Cliquez sur **Ajouter**.

Vous pouvez désormais sélectionner le format de carte personnalisé dans la liste déroulante **Format de carte** de la section *Comportement des portes pour les cartes SIO hors ligne*.

4 Cliquez sur l'onglet **Comportement des portes pour les cartes SIO hors ligne** dans le menu latéral, puis sélectionnez **Code d'installation**.

5 Sélectionnez le format de carte personnalisé dans la liste déroulante **Format de carte**, puis cliquez sur **Ajouter**.

Exemple :



6 Cliquez sur **Enregistrer**, puis effectuez un redémarrage logiciel.

L'accès n'est accordé qu'aux identifiants qui correspondent au format de carte, indépendamment du code d'installation.

Considérations relatives à l'installation du lecteur OSDP avec Mercury

Il y a plusieurs points à prendre en considération avant d'ajouter des lecteurs OSDP à vos contrôleurs Mercury.

Limites

L'état de la connexion des lecteurs OSDP et OSDP 2 sur les contrôleurs Mercury n'est pas actualisé si le lecteur n'est pas affecté à une porte ou un ascenseur.

REMARQUE : Cette limitation concerne également les lecteurs Out lorsque vous utilisez deux lecteurs OSDP par port.

Lecteurs OSDP embarqués pris en charge avec les contrôleurs Mercury

Reportez-vous au tableau suivant pour savoir combien de lecteurs OSDP Synergis[MC] Softwire prend en charge avec Mercury :

Modèle	Ports du lecteur embarqués	Lecteurs OSDP embarqués maximum par panneau
MR50-S2[1]	1	1
MR50-S3	1	2 (deux sur un port)[2]
MR52-S2[1]	2	2 (un par port)
MR52-S3	2	4 (deux par port)[2]
MR51e	2	2 (deux sur un port uniquement)
MR62e	1	4 (quatre sur un port)
EP1501	2	2 (deux sur un port uniquement)
EP1502	2	2 (un par port)
EP4502	2	2 (un par port)
LP1501	2	2 (deux sur un port uniquement)
LP1502	2	4 (deux par port)[2]
LP4502	2	4 (deux par port)[2]
MP1502	2	4 (deux par port)[2]
MP4502	2	4 (deux par port)[2]

REMARQUE : Les contrôleurs Mercury EP2500 et LP2500 ne sont pas répertoriés, car ils ne disposent pas de ports de lecteur embarqué. Ils prennent en charge des lecteurs OSDP via les modules d'interface énumérés dans le tableau.

[1] Les appareils Series 2 MR50 et Series 2 MR52 ne prennent pas en charge OSDP Secure Channel ni deux lecteurs OSDP par port.

[2] Deux lecteurs OSDP par port sont pris en charge via le paramètre **Deux lecteurs OSDP par port de lecteur**. Ce paramètre est configuré dans la page *Réglages de contrôleur Mercury* dans Synergis[MC] Appliance Portal.

Instructions de câblage des lecteurs OSDP

En fonction de la révision de l'assemblage et de la révision PCB de votre module d'interface Mercury et des contrôleurs EP, LP ou MP, des conditions d'installation spécifiques doivent être respectées :

- Une résistance de rappel de 1K ohm doit être ajoutée entre les lignes Mercury DAT/D0 et GND des modules d'interface et des contrôleurs EP, LP ou MP.
- La résistance de rappel doit être installée sur le panneau.
- Pour garantir un fonctionnement correct, l'installation ne doit présenter aucun défaut de la masse. Vérifiez que la terre DC (retour d'alimentation) n'est pas reliée à la terre.
- Il est possible de réutiliser le câblage de Wiegand pour OSDP. Toutefois, il est possible que les câbles Wiegand standard ne respectent pas les recommandations de paire torsadée RS-485.
- Un câblage en forme d'étoile n'est pas recommandé.

Pour savoir si vous devez ajouter une résistance de rappel 1K ohm entre D0 et GND, voir KBA-78953.

Pour en savoir plus sur le câblage des lecteurs OSDP, voir Connecter les modules d'interface Mercury dans Synergis Cloud Link.

Résistances de terminaison

Les consignes suivantes sont particulièrement importantes si vous utilisez un débit en bauds élevé, comme 115 200 bauds :

- Pour des câbles OSDP plus longs que 200 pieds (61 m) ou avec interférence EMF, installez une résistance 120 ohm sur les deux extrémités de la disposition de chaîne des données RS-485.
- Pour des câbles Wiegand plus longs que 32 pieds (10 m) ou avec interférence EMF, installez une résistance 120 ohm sur les deux extrémités de la disposition de chaîne des données RS-485.

En cas d'erreur de communication, vous pouvez diminuer le débit de baud, ajouter des résistances de terminaison ou les deux.

Ajouter des lecteurs OSDP (Secure Channel) à un contrôleur Mercury

Pour ajouter un lecteur OSDP (Secure Channel) à un contrôleur Mercury LP ou MP, vous devez d'abord configurer le lecteur sur le contrôleur avec Config Tool, puis associer le lecteur au contrôleur sur le Synergis[MC] Appliance Portal.

Avant de commencer

Inscrivez le contrôleur et ses sous-tableaux sur l'unité Synergis[MC].

À savoir

- Pour ajouter un lecteur OSDP (Secure Channel) à un contrôleur Mercury, vous devez jumeler le lecteur (échange de clés) avec le contrôleur auquel il est connecté. Pour pouvoir associer un lecteur en mode sécurisé à un autre port de lecteur lorsqu'il est déjà associé à un port de lecteur en mode sécurisé, rétablissez les réglages d'usine du lecteur.
- À compter de Synergis[MC] Softwire 11.2, les lecteurs OSDP connectés ne répondent pas lors d'un passage de badge, sauf s'ils sont configurés pour contrôler une porte ou un ascenseur dans Security Center.
- Les adresses valides pour les lecteurs OSDP contrôlés par Mercury sont 0 à 3.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

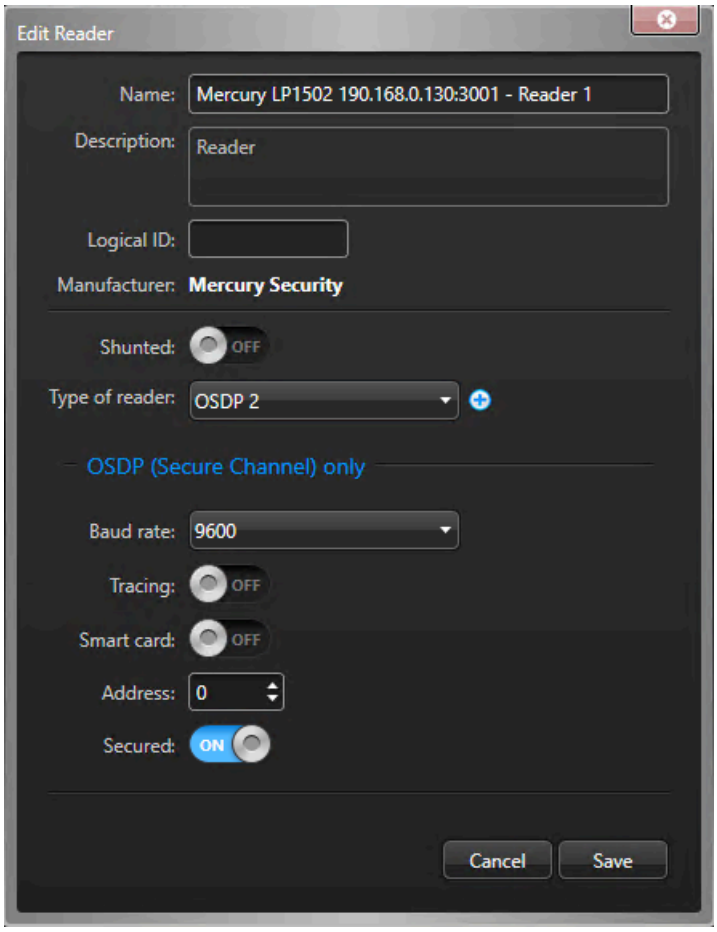
2 Dans l'arborescence des entités, sélectionnez l'unité Synergis, puis cliquez sur l'onglet **Périphériques**.

3 Le cas échéant, développez le contrôleur pour voir les sous-tableaux et périphériques MR.

4 Cliquez sur le lecteur ( ) que vous souhaitez configurer et cliquez sur **Modifier** ( ).

5 Dans la boîte de dialogue *Modifier le lecteur*, sélectionnez **OSDP 2** dans la liste **Type de lecteur**.

Exemple:



REMARQUE : L'option **Sécurisé** doit être activée.

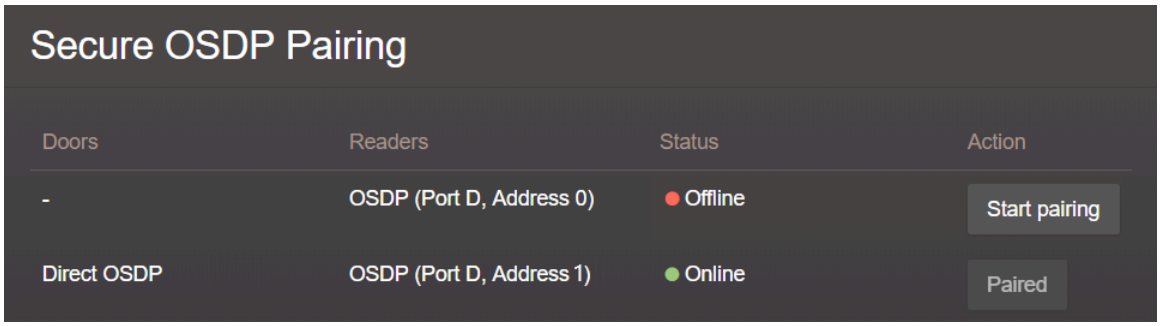
6 Configurez les autres réglages dans la section *OSDP (Secure Channel) seulement* selon vos besoins, puis cliquez sur **Enregistrer**.

7 Connectez-vous à l'unité Synergis Cloud Link.

8 Cliquez sur **Configuration** > **OSDP avancé**.

9 Repérez la ligne avec le port, le lecteur et la porte associée, et cliquez sur **Démarrer l'association**.

Les clés sont partagées et les lecteurs rebasculent en ligne. Le lecteur est à présent sécurisé. Tout lecteur qui refuse la clé reste déconnecté.



10 Répétez l'étape 9 pour les autres lecteurs.

Les clés sont partagées et les lecteurs rebasculent en ligne. Les lecteurs sont maintenant sécurisés. Tout lecteur qui refuse la clé reste déconnecté.

Une fois le processus de jumelage terminé, le lecteur apparaît en ligne dans Config Tool.

Configurer deux lecteurs OSDP par appareil Mercury

Les appareils Mercury suivants peuvent chacun prendre en charge deux lecteurs OSDP : EP1501, LP1501, et MR51e. Pour activer cette fonctionnalité, vous devez configurer les deux lecteurs pour utiliser le premier port de lecteur sur l'appareil Mercury.

Avant de commencer

Configurez les lecteurs OSDP.

À savoir

- Sur les contrôleurs Mercury EP1501, LP1501, le premier port est le bornier TB2.
- Sur les panneaux en aval du Mercury MR51e, le premier port est le bornier TB3.
- Lorsque vous configurez deux lecteurs OSDP sur le premier port, vous ne pouvez pas utiliser le second port.
- Les contrôleurs Mercury EP1501, LP1501 doivent être inscrits sans cartes d'extension pour que le premier port de lecture soit disponible pour les deux lecteurs OSDP.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

2 Dans l'arborescence des entités, sélectionnez l'unité Synergis, puis cliquez sur l'onglet **Périphériques**.

3 Cliquez deux fois sur **Lecteur 1**, puis configurez les réglages suivants :

- **Type du lecteur :** Sélectionnez **OSDP 2**.
- **Débit en bauds :** Sélectionnez un débit binaire.
- **Address :** Sélectionnez l'adresse que vous avez configurée pour le premier lecteur.

4 Répétez l'étape 3 pour **Lecteur 2**, en utilisant l'adresse configurée pour le deuxième lecteur.

Sélectionner **OSDP 2** pour les deux lecteurs affecte automatiquement les deux lecteurs au premier port.

5 (Facultatif, lecteurs compatibles seulement) Vérifiez que l'option **Sécurisé** est **ACTIVÉE**.

Configuration des périphériques Mercury pour utiliser deux lecteurs OSDP par port

Les appareils Mercury suivants peuvent prendre en charge deux lecteurs OSDP sur chacun de leurs ports de lecteur intégrés : LP1502, LP4502, MP1502, MP4502, MR50-S3 et MR52-S3. Vous devez activer cette fonctionnalité dans le Synergis[MC] Appliance Portal[MC] avant de configurer les lecteurs dans Config Tool.

À savoir

- La prise en charge de deux lecteurs OSDP par port sur LP1502, LP4502, MR50-S3 et MR52-S3 nécessite Security Center 5.10.4.0 ou une version ultérieure.
- La prise en charge de deux lecteurs OSDP par port sur Mercury MP1502 et MP4502 nécessite Security Center 5.12.1.0 ou une version ultérieure.
- Si l'option **Deux lecteurs OSDP par port de lecteur** est activée dans le Synergis Appliance Portal et que vous ne configurez qu'un des lecteurs OSDP sur une porte, vérifiez que le lecteur configuré est le lecteur principal, sinon la porte renverra un avertissement, même si elle fonctionne.

Procédure

1 Sur le Synergis Appliance Portal, activez l'option **Deux lecteurs OSDP par port de lecteur** sur la page *Paramètres de contrôleur Mercury* .

REMARQUE : Lorsque cette option est activée, l'option **Carte à puce** configurée sur le lecteur OSDP dans Config Tool est activée par défaut et reste activée en arrière-plan, même si vous la désactivez.

2 Redémarrez Synergis Softwire.

3 Ajoutez deux lecteurs OSDP sur le port de lecteur d'un contrôleur Mercury :

a) Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Rôles et unités**.

b) Dans l'arborescence des entités, sélectionnez l'unité Synergis^{MC}, puis cliquez sur l'onglet **Périphériques**.

c) Cliquez deux fois sur **Lecteur 1**, puis configurez les réglages suivants :

- **Type du lecteur :** Sélectionnez **OSDP 2**.
- **Débit en bauds :** Sélectionnez un débit binaire.
- **Address :** Sélectionnez l'adresse que vous avez configurée pour le premier lecteur.

d) Cliquez sur **Enregistrer**.

e) Cliquez deux fois sur **Sortie Lecteur 1**, et sélectionnez l'adresse que vous avez configurée pour le deuxième lecteur.

REMARQUE : Il suffit de configurer l'adresse, car *Lecteur 1* et *Sortie Lecteur 1* utilisent la même configuration (à l'exception de l'adresse).

4 Affectez les lecteurs à une porte.

Exemple : *Lecteur 1* et *Sortie Lecteur 1* doivent être affectés à une même porte, et *Lecteur 2* et *Sortie Lecteur 2* doivent être affectés à une même porte.

5 Si le contrôleur a un deuxième port de lecteur, vous pouvez répéter l'étape 3 pour configurer *Lecteur 2* et *Sortie Lecteur 2* sur le deuxième port.

Lorsque vous avez terminé

Jumelez les lecteurs OSDP sur le Synergis^{MC} Appliance Portal. Si vous utilisez OSDP 2, vous devrez parfois désactiver le *Mode installation* sur le lecteur après son jumelage si ce mode n'est pas désactivé après le jumelage.

Ajouter des tableaux MR51e à un contrôleur Mercury

Le MR51e est un tableau PoE pour une seule porte qui doit être contrôlé par un contrôleur Mercury. Pour que le tableau MR51e puisse communiquer avec le contrôleur, vous devez configurer le tableau afin qu'il utilise le mode d'adressage DHCP public (recommandé) ou IP statique.

Avant de commencer

Les conditions suivantes sont requises :

- Si ce n'est pas déjà fait, chargez la version prise en charge du micrologiciel des tableaux MR51e.
- Inscrivez le contrôleur EP sur l'unité Synergis[MC].
- Si les tableaux MR51e utilisent le mode d'adressage IP statique, téléchargez l'utilitaire *MSC MR51e Address Configuration Tool* sur le site Web de Mercury.

À savoir

Pour l'intégration Mercury via Synergis[MC] Softwire, seuls deux modes d'adressage sont compatibles avec le tableau MR51e : DHCP public et IP statique.

REMARQUE : Le port Lecteur 1 sur le tableau MR51e peut prendre en charge jusqu'à deux lecteurs OSDP.

Procédure

1 Procédez de l'une des manières suivantes :

- Configurez le tableau MR51e pour l'utilisation du DHCP public (recommandé).
- Configurez le tableau MR51e pour l'utilisation d'une IP statique.

2 Dans Config Tool, ouvrez la tache *Contrôle d'accès*, et cliquez sur **Rôles et unités**.

3 Sélectionnez l'unité Synergis, et ajoutez les tableaux MR51e.

Pour en savoir plus, voir les étapes pour l'ajout de tableaux en aval dans Inscrire un contrôleur Mercury sur l'unité Synergis, page 138.

Configurer le MR51e pour l'utilisation du mode d'adressage DHCP public

Si votre réseau prend en charge le DHCP, il est conseillé de régler vos tableaux MR51e afin qu'ils utilisent le DHCP public.

Procédure

1 Sur le tableau MR51e, réglez **S1** (commutateurs DIP de configuration) sur **0001**.

Réglez les commutateurs DIP 4, 3 et 2 sur OFF, et le commutateur DIP 1 sur ON.

2 Appuyez sur **S2** (commutateur de réinitialisation).

Configurer le MR51e pour l'utilisation du mode d'adressage IP statique

Si votre réseau ne prend pas en charge le DHCP, configurez vos tableaux MR51e afin qu'ils utilisent l'adressage IP statique.

Avant de commencer

Téléchargez l'utilitaire MSC MR51e Address Configuration Tool et installez-le sur votre ordinateur. Vérifiez que le tableau MR51e est relié au même sous-réseau que votre ordinateur.

Procédure

1 Sur le tableau MR51e, réglez **S1** (commutateurs DIP de configuration) sur **0011**.

Réglez les commutateurs DIP 4 et 3 sur OFF, et les commutateurs DIP 2 et 1 sur ON.

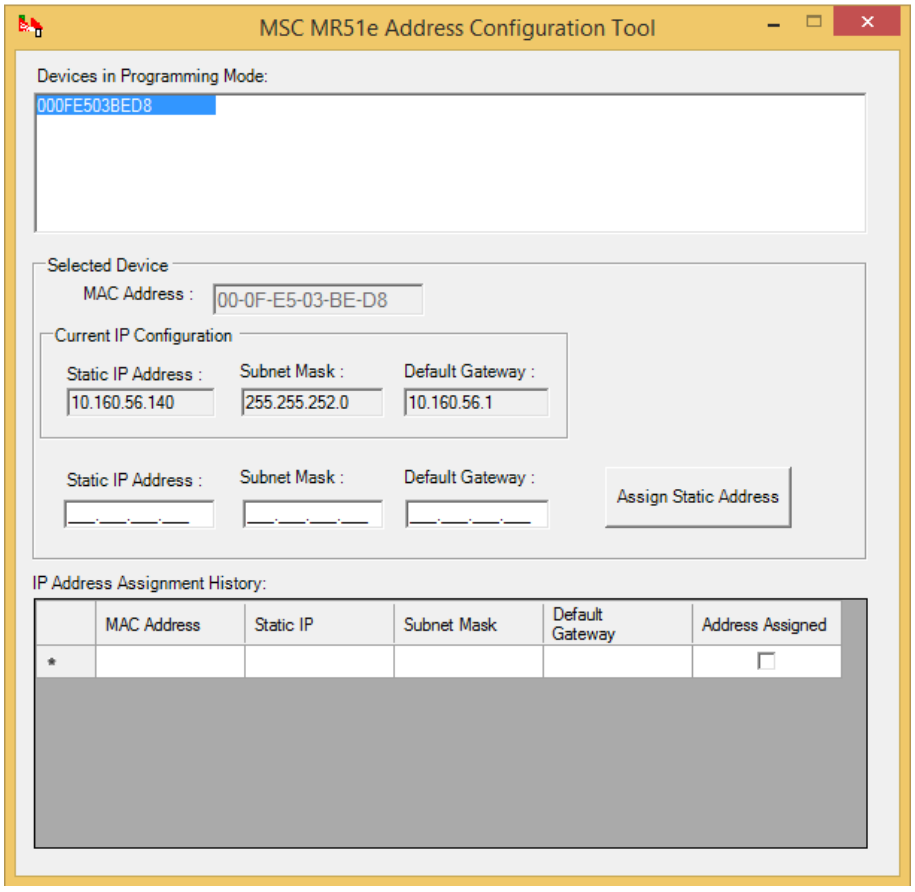
2 Ouvrez l'utilitaire MSC MR51e Address Configuration Tool.

3 Appuyez sur **S2** (commutateur de réinitialisation).

Une fois détectée, l'adresse MAC du tableau MR51e apparaît dans la liste **Devices in Programming Mode** (Appareils en mode programmation).

4 Sélectionnez le panneau MR51e que vous souhaitez programmer dans la liste **Devices in Programming Mode**.

L'adresse MAC du tableau MR51e sélectionné apparaît dans le champ **Selected Device** (Appareil sélectionné).



5 Entrez les valeurs de **Static IP Address** (Adresse IP statique), **Subnet Mask** (Masque de sous-réseau) et **Default Gateway** (Passerelle par défaut), puis cliquez sur **Assign Static Address** (Affecter une adresse statique).

   Les valeurs saisies apparaissent dans le groupe **Current IP Configuration** (Configuration IP actuelle) et dans la liste **IP Address Assignment History** (Historique d'affectation d'adresses IP).

6 Sur le tableau MR51e, réglez **S1** (commutateurs DIP de configuration) sur **0010**.

   Réglez les commutateurs DIP 4, 3 et 1 sur OFF, et le commutateur DIP 2 sur ON.

7 Appuyez sur **S2** (commutateur de réinitialisation).

Configurer le MR62e pour l'utilisation du mode d'adressage IP statique

Avant d'ajouter le tableau Mercury MR62e ou le contrôleur Mercury sur l'unité Synergis[MC], vous devez affecter une adresse IP statique à l'unité.

Avant de commencer

Vous devez disposer des éléments suivants :

- **Guide d'installation et de configuration Mercury :** Manuel d'utilisation pour la connexion au portail Web du contrôleur Mercury et la configuration de son adresse IP, parmi d'autres réglages.
- **Adresse IP statique :** Adresse IP statique affectée au contrôleur par votre service informatique.

Procédure

1 Connectez-vous à la page Internet du panneau MR62e.

2 Dans le champ **IP statique**, saisissez une adresse IP.

3 Cliquez sur **Enregistrer**.

Configuration de l'adresse du lecteur Mercury pour le tableau MR62e

Les lecteurs connectés au tableau en aval MR62e sont utilisés par paires spécifiques et doivent être configurés avec des adresses prédéfinies, fournies par Mercury pour fonctionner.

Le tableau suivant indique la configuration requise de l'adresse du lecteur :

Numéro de lecteur (adresse)	Configuration d'une porte	Tourniquets et ascenseurs Mercury
0	**Porte 1** : lecteur latéral intérieur	Oui
1	**Porte 2**: lecteur latéral intérieur	Oui
2	**Porte 1** : lecteur latéral extérieur	Non
3	**Porte 2**: lecteur latéral extérieur	Non

REMARQUE : Pour utiliser le MR62e afin de contrôler une seule porte *d'entrée/sortie de carte*, utilisez les adresses 0 et 2.

Pour utiliser le MR62e afin de contrôler des portes *d'entrée de carte/sortie avec demande de passage*, utilisez les adresses 0 et 2.

Déconnecter les tableaux MR d’un contrôleur Mercury

Pour déconnecter un tableau Mercury MR d’un contrôleur Mercury inscrit dans Security Center, vous pouvez supprimer le tableau du contrôleur dans Config Tool.

À savoir

Les tableaux Mercury MR doivent être hors ligne dans Security Center avant de les supprimer.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.

2 Cliquez sur **Rôles et unités**, sélectionnez votre unité Synergis[MC] et cliquez sur l’onglet **Périphériques**.

3 Si le tableau MR contrôle des portes ou des zones, déconnectez-les.

4 Déconnectez le tableau :

- Déconnectez l’alimentation du tableau et attendez qu’il bascule hors ligne dans Config Tool.
- Cliquez sur l’onglet **Périphériques**, sélectionnez le tableau, cliquez sur **Modifier**, puis modifiez l’**adresse** du tableau pour qu’il se déconnecte du contrôleur et bascule hors ligne dans Config Tool.

5 Cliquez sur l’onglet **Périphériques**, sélectionnez le tableau, cliquez sur **Supprimer**, puis cliquez sur **Appliquer**.

À propos des déclencheurs et procédures Mercury

Les déclencheurs et procédures Mercury sont comparables aux associations événement-action dans Security Center. Vous pouvez configurer des déclencheurs et des procédures sur le portail de l'appareil Synergis qui exécutent directement des règles sur un contrôleur Mercury.

Fonctionnement des déclencheurs et procédures Mercury sur le portail de l'appareil Synergis

- Les déclencheurs et procédures Mercury fonctionnent de concert pour créer une règle. Le déclencheur détermine le *quand* en fonction d'un événement, tandis que la procédure détermine le *quoi* à l'aide d'une ou de plusieurs actions. Chaque déclencheur est associé à une procédure, mais chaque procédure peut être utilisée par plusieurs déclencheurs.
- Si les entités utilisées au sein des déclencheurs et procédures basculent dans un état inattendu, vous pouvez rétablir leur état d'origine à l'aide du bouton **Rétablir les valeurs par défaut** sur la page *Déclencheurs et procédures Mercury*.

  REMARQUE : Ce bouton sert également a restaurer les déclencheurs et procédures Mercury après la restauration des fichiers de configuration d'une unité Synergis Cloud Link.

Bonnes pratiques

Pour une performance optimale des déclencheurs et procédures Mercury, vérifiez que les réglages suivants sont activés sur la page *Réglages de contrôleur Mercury* sur le portail de l'appareil Synergis[MC] :

- **Événements « Demande de passage » en direct :** Activez ce réglage si vous créez des déclencheurs avec des événements REX.
- **Contrôle de secteur natif Mercury :** Activez ce réglage si vous créez des déclencheurs associés à des secteurs.

À propos de la surveillance des procédures et déclencheurs Mercury

Dans Security Center 5.12 et ultérieur, les déclencheurs et procédures Mercury génèrent des événements personnalisés qui peuvent être exploités par le mécanisme événement-action.

- **Surveillance des événements :** Vous pouvez surveiller les événements personnalisés dans la tâche *Surveillance* de Security Desk en ajoutant l'unité Synergis Cloud Link à la liste *Surveillance des événements*.
- **Rapports d'événements :** Vous pouvez créer des rapports sur les événements personnalisés à l'aide de la tâche *Événements d'unité de contrôle d'accès* dans Security Desk et Config Tool, et en filtrant par l'unité Synergis Cloud Link.
- **Capacité :** Sur la page *Rapport de capacité* du portail de l'appareil Synergis, les lignes *Déclencheurs personnalisés* et *Procédures personnalisées* de la section *Capacité* indiquent le nombre de déclencheurs et procédures créées sur le contrôleur Mercury sélectionné.

Limitations des procédures et déclencheurs Mercury

Les procédures et déclencheurs Mercury du portail de l'appareil Synergis ont les limitations connues suivantes :

Limitations générales

- Chaque contrôleur Mercury peut contenir jusqu'à 3 000 déclencheurs et 3 000 procédures. Les procédures et déclencheurs au-delà cette limite sont ignorés.

Limitations associées à la configuration

- Vous pouvez activer une sortie en fonction de la modification d'une entrée. Toutefois, il n'y a pas d'option pour rétablir l'état initial de la sortie.

  Contournement : Pour réinitialiser la sortie, créez une procédure distincte pour rétablir l'état d'origine de la sortie avec un déclencheur basé sur un changement d'entrée.
- Les entrées et sorties affectées aux portes et aux ascenseurs ne peuvent pas servir de déclencheurs de points de surveillance ou de contrôle.
- Les commandes de comportements de témoins LED envoyées par Synergis[MC] Softwire à Mercury remplacent les comportements actifs. Cela concerne le basculement du témoin LED sur rouge en cas de reverrouillage et sur vert lorsqu'une porte adopte un horaire d'accès libre.
- La remise sous tension du contrôleur Mercury annule les procédures *Contourner le mode de lecteur* configurées avec une durée **Indéfinie**.
- La configuration du mode de lecteur temporaire des procédures *Contourner le mode de lecteur* remplace toute modification manuelle apportée au mode de lecteur.

  Exemple : Si vous basculez un lecteur en mode *Carte et code PIN* alors qu'une procédure *Contourner le mode de lecteur* active est configurée pour régler le mode de lecteur sur *Verrouillé*, la porte reste verrouillée. Toutefois, à l'expiration de la procédure, le lecteur rebascule en mode *Carte et code PIN*.
- Lorsqu'un titulaire de cartes passe son badge sur un lecteur désactivé par une procédure *Contourner le mode de lecteur*, l'événement *Accès refusé* dans Security Center n'intègre pas de motif de refus.
- Pour les procédures *Définir un point de contrôle* configurées avec une commande **Périodique**, vous ne pouvez voir que le premier et le dernier changement de sortie dans Config Tool.

Limitations associées aux horaires

- Les horaires ne sont synchronisés avec l'unité Synergis Cloud Link que s'ils sont associés à une entité contrôlée par l'unité concernée. Pour utiliser des horaires réservés aux déclencheurs et procédures, vous devez ajouter une fausse porte à l'unité Synergis Cloud Link et lui appliquer les horaires.
- Vous ne pouvez créer que 255 horaires dans Security Center, y compris les horaires de déverrouillage et les horaires réservés aux procédures et déclencheurs Mercury.
- Mercury impose une limite de 12 intervalles horaires. Pour en savoir plus, voir Limitations Mercury relatives aux horaires de déverrouillage de portes.

Types d'actions pour les procédures Mercury

Chaque procédure Mercury doit inclure une ou plusieurs des actions suivantes.

Action	Description
Armer/désarmer une zone	Armer ou désarmer une zone matérielle : • **Désarmer :** Masquez toutes les entrées de la zone. Les entrées activées ne basculent pas en état d'alarme. • **Armer :** Si aucune entrée n'est active, armez la zone et démasquez toutes les entrées. • **Forcer l'armement :** Armez la zone, mais ne démasquez que les entrées inactives. Les entrées déjà actives restent masquées. • **Contourner l'armement :** Armez la zone et démasquez toutes les entrées.

Action	Description
Procédure de contrôle	Contrôler une procédure Mercury : • **Exécuter :** Exécutez les actions dans la procédure sélectionnée. • **Abandon retardé :** Si la procédure est en attente en raison d'une action *Délai*, abandonner la procédure sans effectuer les actions suivantes. • **Reprise retardée :** Si la procédure est en attente en raison d'une action *Délai*, ignorer l'attente pour que les actions suivantes puissent être exécutées.
Délai	Demandez à la procédure d'attendre le nombre de secondes configuré avant d'exécuter les actions suivantes.
Ignorer les portes forcées	Désactivez les alarmes porte forcée pour la porte.
Ignorer les portes maintenues ouvertes	Désactivez les alarmes porte maintenue ouverte pour la porte.
Ignorer les alarmes de points de surveillance	Masque l'entrée, l'empêchant de basculer en état d'alarme en cas d'activation.
Contourner la LED du lecteur	Appliquez une séquence LED temporaire au lecteur. Configurez les options suivantes : • **Couleur d'activation** • **Couleur de désactivation** • **Temps d'allumage (ms)** • **Temps d'extinction (ms)** • **Répétition (0 à 255)** • **Nombre de bips (0 à 15)**
Contourner le mode de lecteur	Contournez le mode du lecteur pour la durée indiquée avec l'un des modes de lecteur suivants : • **Désactivé :** Les lectures de cartes et les demandes de passage sont désactivées et la porte reste verrouillée. • **Déverrouillé :** La porte est déverrouillée. • **Verrouillé :** Les lectures de cartes sont désactivées, mais les demandes de passage sont honorées. • **Carte seule :** Seules les cartes sont des identifiants d'accès valables. • **Carte et code PIN :** Une carte et un code PIN sont requis pour obtenir un accès. • **Carte ou code PIN :** Les identifiants d'accès Carte ou code PIN sont valables. • **Code PIN seul :** Seuls les codes PIN sont des identifiants d'accès valables.
Définir un point de contrôle	Activez une sortie qui n'est pas affectée à un pêne de porte.
Déverrouiller momentanément la porte	Déverrouillez la porte pour la durée configurée.

Types d'événements pour les déclencheurs Mercury

Les événements déterminent le moment où un déclencheur Mercury est déclenché.

Événement	Description
Accès refusé : Format de carte non valable	L'accès est refusé si le format de carte n'a pas été synchronisé avec le contrôleur Mercury.
Accès refusé : Demande rejetée par le contrôleur	L'accès est refusé pour l'un des motifs suivants : • Le lecteur est en mode *Verrouillé*. • Un identifiant inconnu est utilisé. • La décision d'accorder l'accès de Mercury est supplantée par Synergis Softwire. • Restriction de sas.
Accès refusé : Titulaire de cartes non autorisé	L'accès est refusé pour l'un des motifs suivants : • La règle d'accès associée à ce titulaire de cartes ne s'applique pas à lors de la date ou de l'heure de l'horaire. • Un code PIN non valable est saisi. • Violation antiretour native. • Une carte connue sans accès est utilisée sur ce lecteur. • Deux titulaires de cartes doivent présenter leurs identifiants dans un délai donné et le délai a expiré. • La limite de capacité du secteur est atteinte. • La règle d'escorte de visiteur est en vigueur et le visiteur a badgé avant l'hôte. • Une carte et un code PIN sont requis pour accéder au secteur, et le titulaire de cartes n'a pas saisi de code PIN dans le temps imparti.
Accès refusé : Identifiant inconnu	L'accès est refusé si le format de carte est reconnu, mais que l'identifiant n'a pas encore été synchronisé avec le contrôleur Mercury.
Accès accordé	L'accès est accordé dans les cas suivants : • Le titulaire de cartes ouvre la porte. • Le délai pour entrer expire et la porte se reverrouille. • La porte est dénuée de capteur de porte et l'entrée est supposée.
Accès accordé : Entrée détectée	L'accès est accordé lorsque le passage est détecté.
Accès accordé : Déverrouillé	L'accès est accordé lorsqu'une porte est déverrouillée.
Porte fermée	La porte est fermée.
Porte forcée	La porte est forcée.
Porte maintenue ouverte	La porte est maintenue ouverte.
Porte ouverte (pas forcée)	La porte est ouverte, mais pas forcée.
Porte reverrouillée après REX	La porte est reverrouillée après une demande de passage.

Événement	Description
Porte reverrouillée après déverrouillage manuel	Porte reverrouillée après un déverrouillage manuel
Porte reverrouillée après déverrouillage manuel ou REX	La porte est reverrouillée après un déverrouillage manuel ou une demande de passage.
Porte déverrouillée par REX	La porte est déverrouillée par une demande de passage.
Code PIN de contrainte saisi	Un code PIN de contrainte est entré sur le lecteur. L'événement est généré même si l'option **Code PIN de contrainte** est désactivée pour le secteur et que l'accès est refusé.
Capacité maximale stricte atteinte	La capacité maximale stricte est atteinte.
Taux d'occupation strict descendu à zéro	La capacité maximale stricte est revenue à zéro.
Point de surveillance : Alarme (active)	L'entrée démasquée devient active. Les entrées des zones désarmées sont masquées.
Point de surveillance : Défaillance (problème)	L'entrée bascule en état *Problème*.
Point de surveillance : Sécurisé (inactif)	L'entrée bascule en état *Inactif*.
Mode de lecteur : Carte et code PIN	Le mode du lecteur bascule vers *Carte et code PIN*.
Mode de lecteur : Carte seule	Le mode du lecteur bascule vers *Carte seule*.
Mode de lecteur : Carte ou code PIN	Le mode du lecteur bascule vers *Carte ou code PIN*.
Mode de lecteur : Désactivé	Le mode du lecteur bascule vers *Désactivé*.
Mode de lecteur : Verrouillé	Le mode du lecteur bascule vers *Verrouillé* (lecteur contourné).
Mode de lecteur : Code PIN seul	Le mode du lecteur bascule vers *Code PIN seul*.
Mode de lecteur : Déverrouillé	Le mode du lecteur bascule vers *Déverrouillé* (mode maintenance).

Configurer les déclencheurs Mercury sur le portail de l'appareil Synergis

Configurez un déclencheur pour spécifier quand une procédure doit être exécutée.

Avant de commencer

Configurez les procédures Mercury sur le portail de l'appareil Synergis[MC].

À savoir

La couleur du nom du déclencheur indique s'il existe un problème de configuration :

- **Orange :** La configuration a été enregistrée, mais un problème a empêché son analyse et sa synchronisation avec le contrôleur Mercury. Cela peut se produire lorsque des entités associées n'existent plus ou ne sont pas correctement synchronisées avec le contrôleur. Le contrôleur Mercury doit être en ligne pour que cette couleur soit affichée.
- **Rouge :** Des informations requises pour la configuration sont manquantes ou non valables.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Déclencheurs et procédures Mercury**.

3 Dans la liste **Sélectionner un contrôleur**, sélectionnez le contrôleur pour lequel vous souhaitez créer un déclencheur.

4 Cliquez sur **Ajouter un déclencheur**.

5 Dans le champ **Nom**, donnez un nom descriptif au déclencheur.

6 En regard du champ **Horaire**, cliquez sur . Dans la boîte de dialogue qui apparaît, sélectionnez un horaire dans la liste, puis cliquez sur **OK**.

7 En regard du champ **Événement**, cliquez sur . Dans la boîte de dialogue qui apparaît, sélectionnez un événement dans la liste, puis cliquez sur **OK**.

Pour la liste et la définition des événements, voir Types d'événements pour les déclencheurs Mercury, page 174.

En fonction de l'événement sélectionné, l'un des champs suivants est affiché :

- **Entrée :** Seules les entrées qui ne sont pas affectées à une entité dans Security Center sont affichées, sauf pour les entrées de zones.
- **Lecteur :** Tous les lecteurs sous le contrôleur Mercury sélectionné sont affichés.
- **Porte :** Seules les portes contrôlées par le contrôleur Mercury sélectionné sont affichées. Sélectionnez le côté de porte.
- **Secteur :** Seuls les secteurs contrôlés par le contrôleur Mercury sélectionné sont affichés.
- **Zone :** Seules les zones matérielles contrôlées par le contrôleur Mercury sélectionné sont affichées.

8 En regard du champ affiché, cliquez sur . Dans la boîte de dialogue qui apparaît, sélectionnez une entité dans la liste, puis cliquez sur **OK**.

9 En regard du champ **Procédure**, cliquez sur . Dans la boîte de dialogue qui apparaît, sélectionnez une procédure dans la liste, puis cliquez sur **OK**.

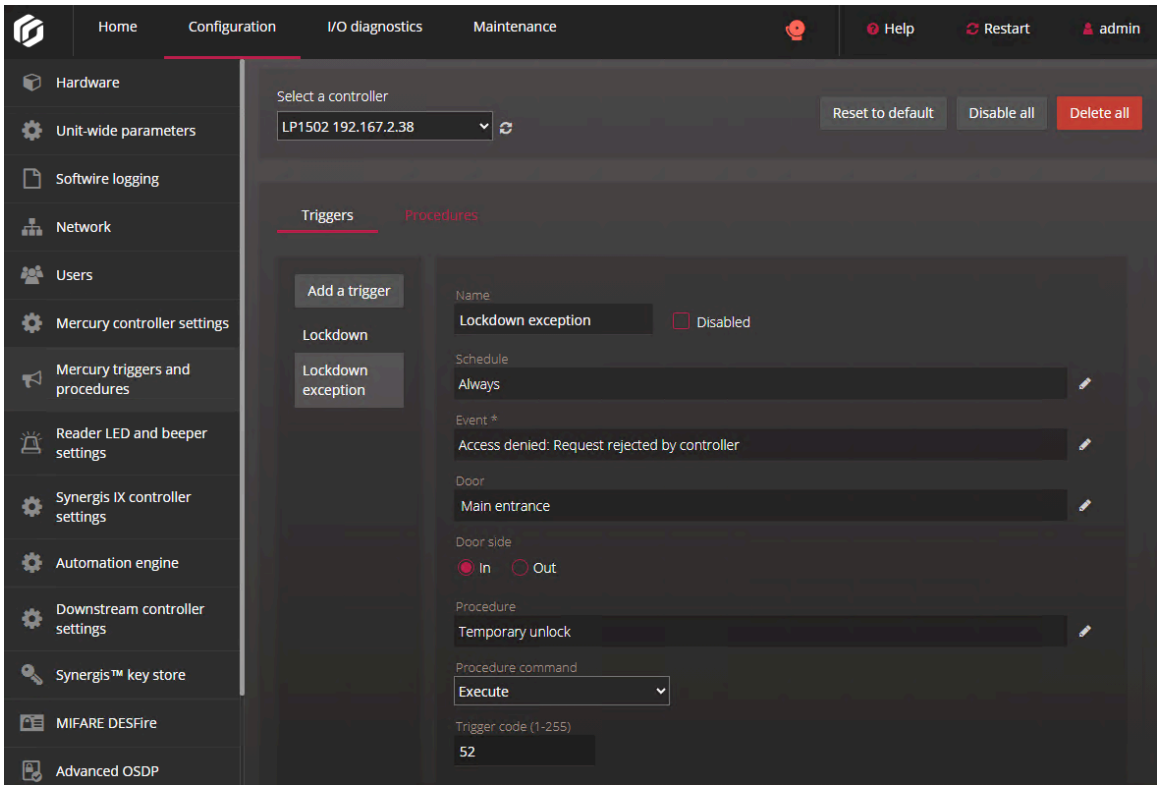
10 Dans la liste **Commande de procédure**, sélectionnez l'un des éléments suivants :

- **Exécuter :** Exécutez les actions dans la procédure sélectionnée.
- **Abandon retardé :** Si la procédure est en attente en raison d'une action *Délai*, abandonner la procédure sans effectuer les actions suivantes.
- **Reprise retardée :** Si la procédure est en attente en raison d'une action *Délai*, ignorer l'attente pour que les actions suivantes puissent être exécutées.

11 (Facultatif) Le champ **Code de déclenchement (1-255)** est affiché, en fonction de l'événement que vous avez sélectionné. Vous pouvez donner une valeur de 1 à 255 au code de déclenchement pour un titulaire de cartes ou un visiteur dans Security Center 5.12 et ultérieur. Un même code de déclenchement peut être utilisé pour plusieurs titulaires de cartes et visiteurs. Il n'y a pas de hiérarchie dans les codes de déclenchement.

12 Cliquez sur **Enregistrer**.

Ce déclencheur est configuré pour exécuter la procédure *Déverrouillage temporaire* lorsque l'accès à la porte *Entrée principale* est refusée à un titulaire de cartes doté du code de déclenchement 52.



Configurer les procédures Mercury sur le portail de l’appareil Synergis

Vous devez configurer une procédure pour définir les actions à exécuter lorsqu’un événement déclencheur survient.

Avant de commencer

Inscrivez un contrôleur Mercury sur l'unité Synergis Cloud Link .

À savoir

La couleur du nom de la procédure indique s'il existe un problème de configuration :

- **Orange :** La configuration a été enregistrée, mais un problème a empêché son analyse et sa synchronisation avec le contrôleur Mercury. Cela peut se produire lorsque des entités associées n’existent plus ou ne sont pas correctement synchronisées avec le contrôleur. Lorsque la procédure est orange, les déclencheurs associés le sont aussi. Le contrôleur Mercury doit être en ligne pour que cette couleur soit affichée.
- **Rouge :** Des informations requises pour la configuration sont manquantes ou non valables.

Procédure

1 Connectez-vous à l’unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Déclencheurs et procédures Mercury**.

3 Dans la liste **Sélectionner un contrôleur**, sélectionnez le contrôleur pour lequel vous souhaitez créer une procédure.

4 Cliquez sur l’onglet **Procédures**.

5 Cliquez sur **Ajouter une procédure**.

6 Dans le champ **Nom**, donnez un nom descriptif à la procédure.

7 Cliquez sur **Ajouter une action** .

Un menu déroulant est affiché dans la colonne *Action*.

8 Cliquez sur la liste déroulante et sélectionnez une action.

Pour la liste des actions et leur description, voir Types d'actions pour les procédures Mercury, page 172.

Différents champs et boutons sont affichés dans les colonnes *Source* et *Réglages* en fonction de l'action sélectionnée.

9 Si un champ est affiché dans la colonne *Source*, cliquez sur en regard du champ, puis sélectionnez une source dans la liste de la boîte de dialogue qui apparaît.

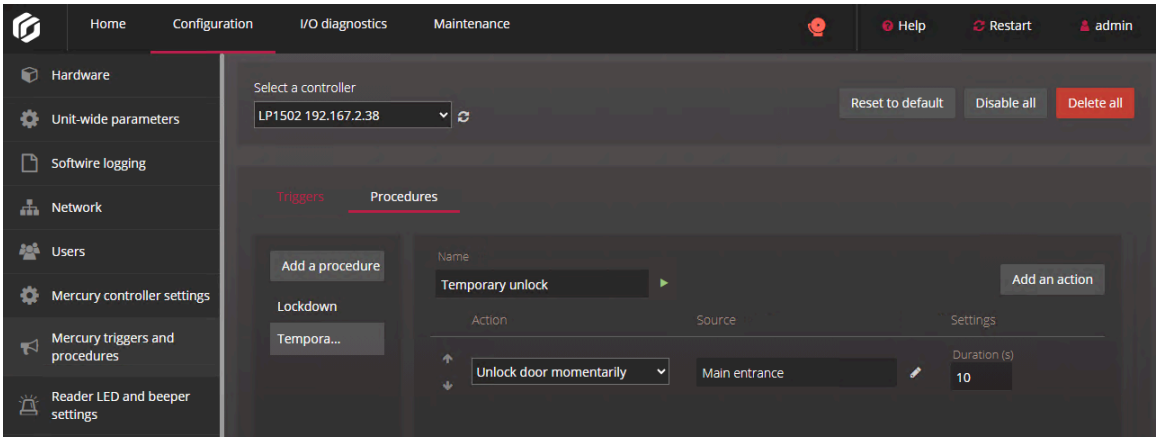
10 Dans la section *Réglages*, configurez les options selon vos besoins.

11 (Facultatif) Ajoutez des actions selon vos besoins.

12 (Facultatif) Modifiez l’ordre des actions avec les flèches haut et bas. Les actions sont exécutées dans l'ordre d'affichage de la configuration de la procédure.

13 Cliquez sur **Enregistrer**.

Cette procédure est configurée avec l’action *Déverrouiller momentanément la porte*, qui déverrouille la porte *Entrée principale* pendant 10 secondes après activation du déclencheur.



Lorsque vous avez terminé

- Testez la procédure avant de l'associer à un déclencheur en cliquant sur ▶ en regard du champ **Nom** de la procédure. Si la procédure contient une action *Délai*, vous pouvez cliquer sur ■ pour interrompre la procédure pendant le délai d'attente et annuler la procédure.

  REMARQUE : Les boutons ne sont affichés que lorsque la procédure a été synchronisée avec succès avec le contrôleur Mercury. Les boutons sont masqués si le contrôleur est hors ligne ou s'il existe des champs non définis dans la configuration de la procédure. Cliquez sur ⟳ en regard du champ du contrôleur pour actualiser la page.
- Configurez les déclencheurs Mercury sur le portail de l’appareil Synergis.

Désactiver les déclencheurs et procédures Mercury sur le portail de l’appareil Synergis

Pour empêcher l’exécution d'une procédure, vous pouvez désactiver le déclencheur associé à la procédure.

À savoir

Désactiver un déclencheur le désynchronise du contrôleur Mercury, sans pour autant perdre sa configuration. Cette option est utile pour désactiver un déclencheur à titre temporaire. Vous pouvez également dépanner un comportement inattendu en désactivant tous les déclencheurs, puis en les activant un par un pour identifier la source du problème.

Procédure

1 Connectez-vous à l’unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Déclencheurs et procédures Mercury**.

3 Procédez de l'une des manières suivantes :

- Pour désactiver un seul déclencheur, sélectionnez-le dans la liste, puis cochez la case **Désactiver** en regard du champ **Nom**. Cliquez sur **Enregistrer**.
- Pour désactiver tous les déclencheurs pour le contrôleur Mercury sélectionné, cliquez sur **Désactiver tout** en haut de la page *Déclencheurs et procédures Mercury*. Dans la boîte de dialogue qui vous demande de confirmer votre choix, cliquez sur **Désactiver tout**.

Les déclencheurs désactivés sont grisés.

Lorsque vous avez terminé

Pour réactiver un déclencheur, sélectionnez-le, puis décochez la case **Désactiver**, ou cliquez sur **Activer tout** si tous les déclencheurs ont été désactivés. Cliquez sur **Enregistrer**.

12

Verrous Allegion Schlage via Mercury

Cette section aborde les sujets suivants:

Inscription des verrous Allegion Schlage AD et les modules PIM sur l'unité Synergis

Comme l'unité Synergis[MC] ne communique pas directement avec les verrous Allegion Schlage AD ou les modules PIM400, vous devez inscrire ces appareils par l'intermédiaire d'un contrôleur Mercury EP, LP, MP ou Honeywell, à l'aide de Config Tool.

Avant de commencer

- Configurez une adresse RS-485 distincte sur chaque appareil Schlage (verrou AD Series et module PIM400) à l'aide de l'appareil portable Schlage Pidion, puis connectez le verrou et le module à votre contrôleur Mercury. Pour en savoir plus, voir le Guide de l'utilisateur des utilitaires Shlage.
- Configurez l'adresse IP statique attribuée sur le contrôleur Mercury.

À savoir

Mercury controllers enrolled on a Synergis[MC] unit are not visible from the Synergis[MC] Appliance Portal *Hardware* page.

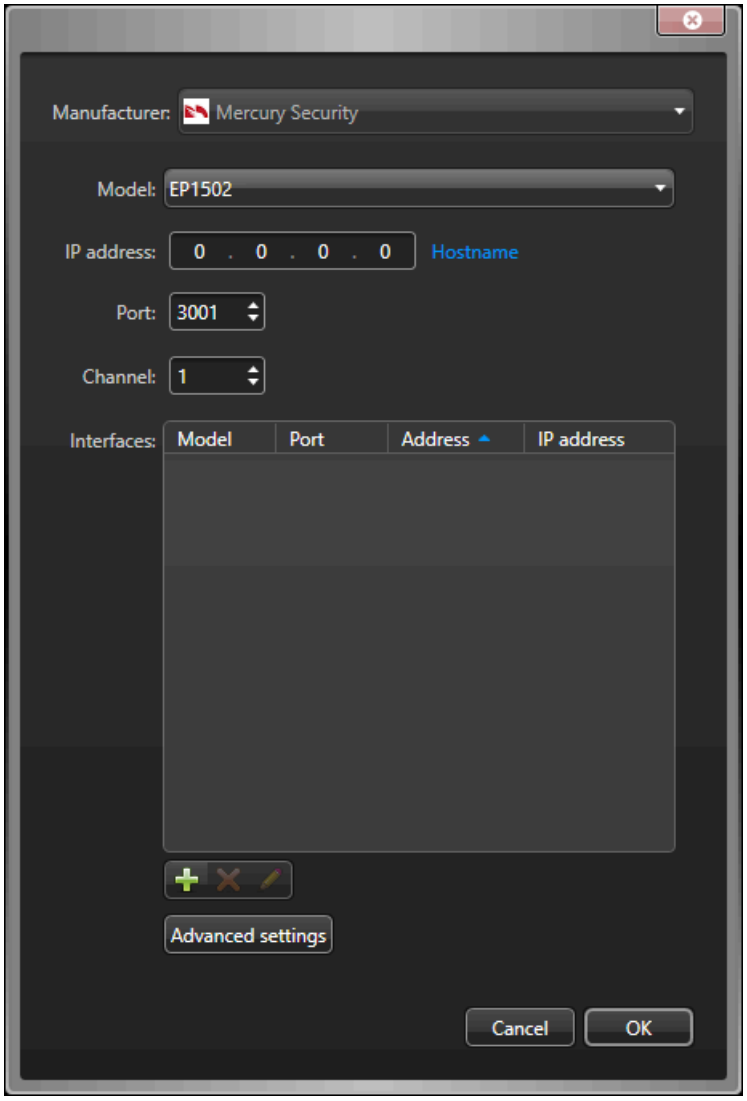
Sur l'unité Synergis, un ID de canal unique doit être affecté à chaque contrôleur Mercury. Tous les contrôleurs Mercury ont des bus RS-485 auxquels les appareils Schlage (AD-300 et PIM400) sont connectés. Chaque appareil Schlage connecté à un même bus RS-485 doit avoir une adresse RS-485 unique.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.

2 Cliquez sur **Rôles et unités**, puis cliquez sur l'unité Synergis.

3 Cliquez sur **Périphériques**, puis sur **Ajouter un élément** ( ).



4 Saisissez les informations suivantes :

- **Modèle :** Modèle du contrôleur.
- **Adresse IP :** Adresse IP statique affectée au contrôleur par votre service informatique.
- **Nom d'hôte :** Cliquez sur le lien bleu pour identifier le contrôleur par son nom d'hôte. Cette option n'est disponible que si vous exécutez Security Center 5.12.0.0 ou ultérieur.

  REMARQUE : Lorsque vous inscrivez un contrôleur Mercury avec son nom d'hôte, vous devez lui adjoindre `.local` si le contrôleur n'utilise pas le DHCP et le DNS sur le réseau.
- **Port :** Port de communication. La valeur par défaut est 3001. Le port doit correspondre à la valeur configurée sur la page web Mercury Device Manager.
- **Canal :** ID de canal correspondant à ce contrôleur. L'ID de canal peut être compris entre 0 et 63, et doit être unique sur l'unité Synergis. Une fois qu'il est affecté, vous ne devez pas le modifier.

5 Ajoutez les appareils Allegion Schlage qui sont connectés à votre contrôleur Mercury.

a) Sous la liste *Interfaces*, cliquez sur **Ajouter un élément** (➕).

b) Dans la boîte de dialogue qui apparaît, sélectionnez le **Modèle** (AD-300 ou PIM400), le **Port** et l'**Adresse** (0 à 31).

c) (PIM400 seulement) Dans **Min**, entrez le premier numéro de porte associé au PIM400, et dans **Nombre**, entrez le nombre de portes associées au PIM400.

Tous les numéros de porte, de **Min** à **Min**+**Nombre** doivent correspondre à un verrou sans fil AD-400.

d) Cliquez sur **OK**.

e) Répétez l'opération selon vos besoins.

6 (Facultatif) Cliquez sur **Options avancées** pour modifier les réglages avancés.

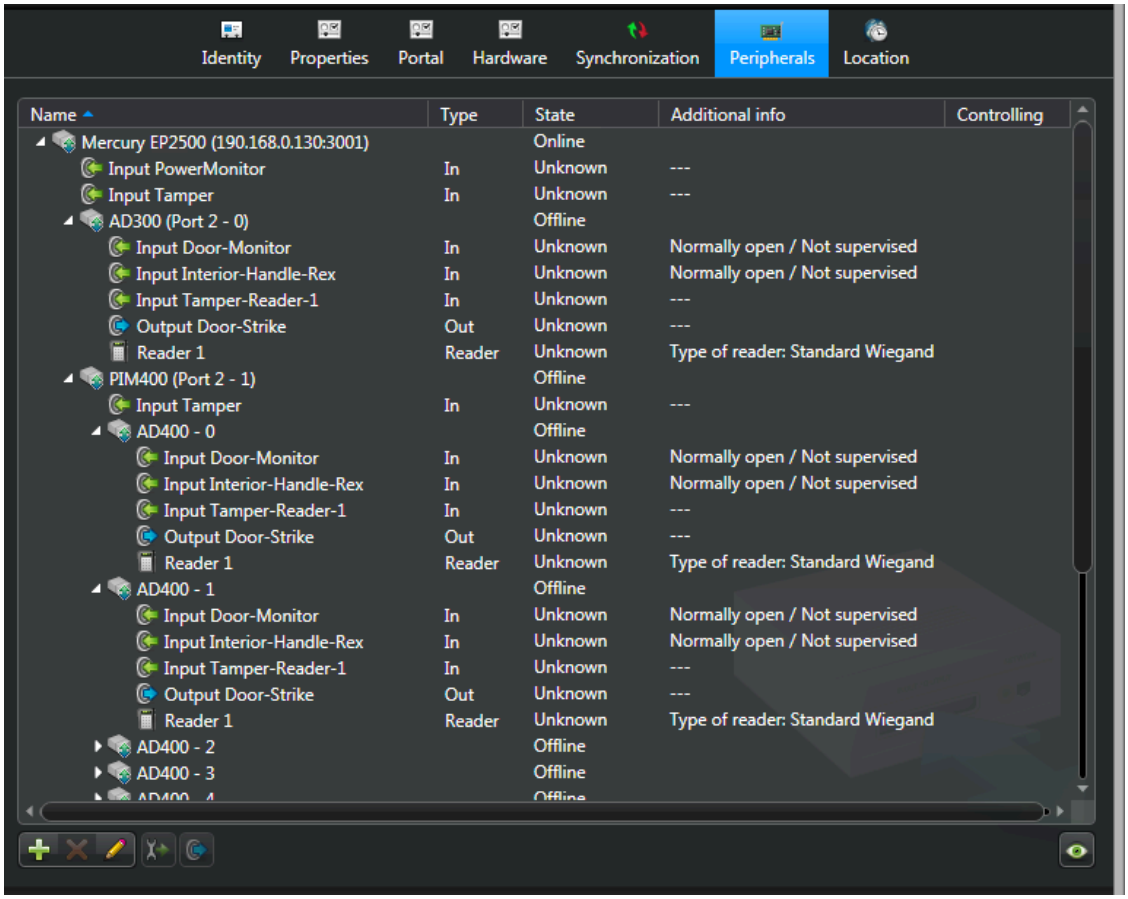
Les réglages disponibles dépendent du modèle de contrôleur sélectionné. Vous pouvez généralement modifier le débit en bauds du port série disponible, les valeurs personnalisées d'entrées supervisées et la configuration d'événement d'entrée d'alimentation.

REMARQUE : Vous pouvez configurer quatre préréglages personnalisés différents sur les entrées de votre contrôleur Mercury. Pour les utilisateurs qui passent d'une version antérieure de Security Center et qui ont configuré une valeur personnalisée, le préréglage apparaît sous **Personnalisé 1** dans la liste **Lignes de limites AD**.

7 Cliquez sur **OK** au bas de la boîte de dialogue.

8 Cliquez sur **Appliquer**.

Le contrôleur Mercury ainsi que tous ses sous-tableaux et périphériques connectés sont affichés sur la page *Périphériques*.



L'ajout de modules d'interface à l'unité Synergis entraîne un redémarrage logiciel de l'unité. Durant ce processus, l'unité Synergis et tous les périphériques associés sont affichés en rouge.

Inscrire des verrous Allegion Schlage LE et NDE compatibles ENGAGE via des contrôleurs Mercury

Avec la plateforme ENGAGE d'Allegion Schlage, vous pouvez stocker vos identifiants sur des cartes et sur des téléphones mobiles compatibles. Pour ce faire, vous devez intégrer les verrous Allegion Schlage LE et NDE via la plateforme ENGAGE en inscrivant un contrôleur Mercury EP, LP ou MP dans Config Tool et en ajoutant la Passerelle ENGAGE comme interface.

Avant de commencer

La configuration initiale et l'association du verrou à la passerelle ENGAGE sont effectués avec l'app mobile Allegion ENGAGE, disponible pour appareils Android et iOS. Touchez **Connect**, puis touchez le signe plus dans l'angle et suivez les instructions. Puis enregistrez les verrous dans Config Tool.

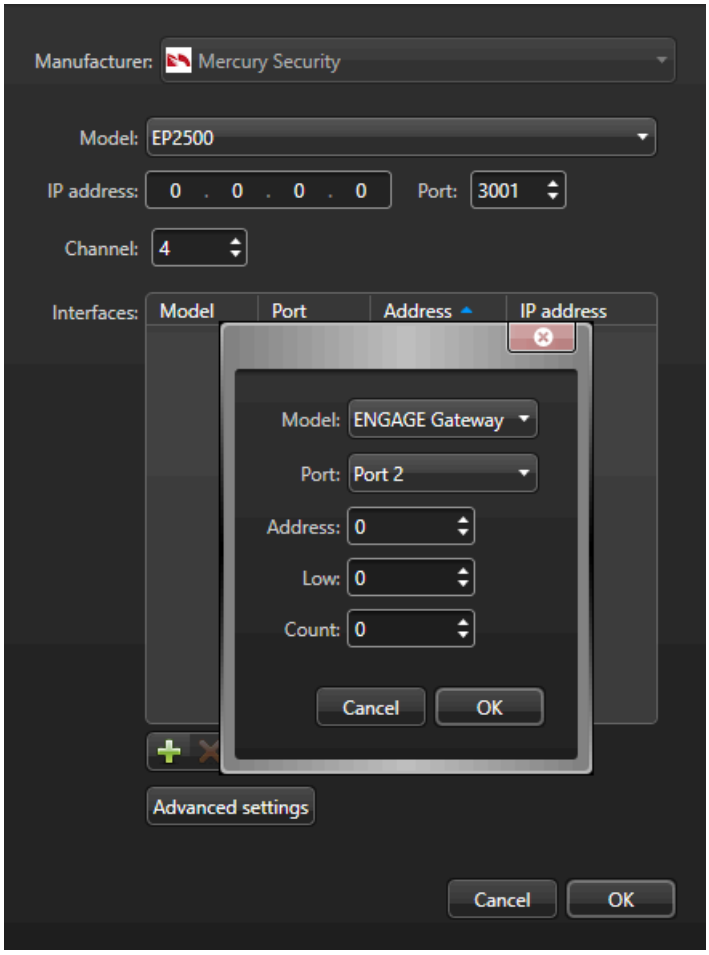
À savoir

Le processus d'inscription de verrous Allegion Schlage NDE et LE avec intégration ENGAGE dans Config Tool est le même que pour l'inscription du module PIM400, sauf que vous devez sélectionner **ENGAGE Gateway** lorsque vous configurez l'interface.

Procédure

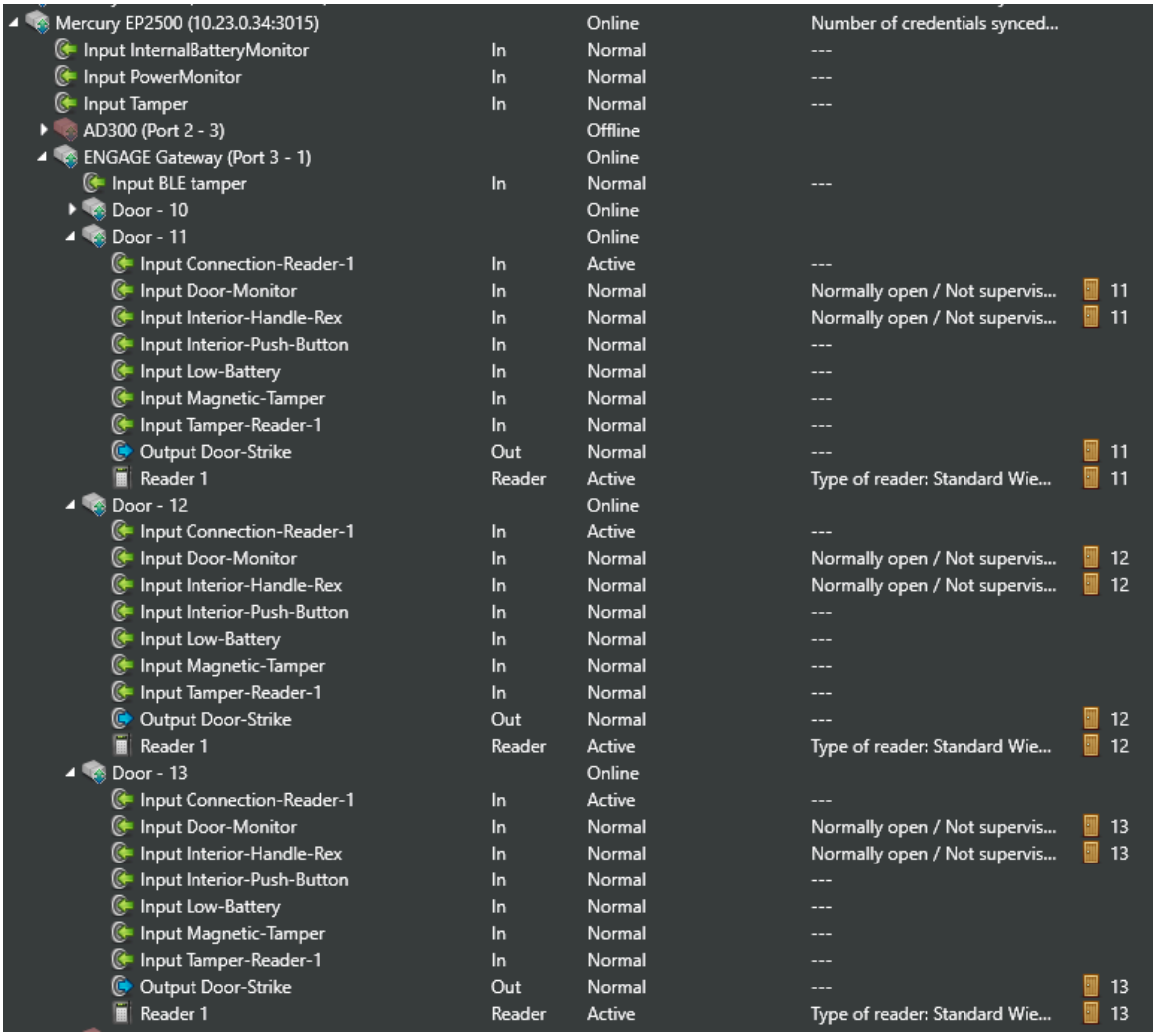
1 Inscrivez les verrous Allegion Schlage NDE ou LE comme indiqué dans Inscription des verrous Allegion Schlage AD et les modules PIM sur l'unité Synergis, page 182.

2 À l'étape 5, sélectionnez Passerelle ENGAGE dans le menu déroulant **Modèle** après avoir cliqué sur **Ajouter un élément** (➕) dans la liste *Interfaces*.



La passerelle ENGAGE ainsi que tous les sous-tableaux et périphériques apparaissent dans l'onglet *Périphériques*.

Exemple :


Mercury EP2500 (10.23.0.34:3015) Online Number of credentials synced...
Input InternalBatteryMonitor In Normal ---
Input PowerMonitor In Normal ---
Input Tamper In Normal ---
AD300 (Port 2 - 3) Offline
ENGAGE Gateway (Port 3 - 1) Online
Input BLE tamper In Normal ---
Door - 10 Online
Door - 11 Online
Input Connection-Reader-1 In Active ---
Input Door-Monitor In Normal Normally open / Not supervis... 11
Input Interior-Handle-Rex In Normal Normally open / Not supervis... 11
Input Interior-Push-Button In Normal ---
Input Low-Battery In Normal ---
Input Magnetic-Tamper In Normal ---
Input Tamper-Reader-1 In Normal ---
Output Door-Strike Out Normal --- 11
Reader 1 Reader Active Type of reader: Standard Wie... 11
Door - 12 Online
Input Connection-Reader-1 In Active ---
Input Door-Monitor In Normal Normally open / Not supervis... 12
Input Interior-Handle-Rex In Normal Normally open / Not supervis... 12
Input Interior-Push-Button In Normal ---
Input Low-Battery In Normal ---
Input Magnetic-Tamper In Normal ---
Input Tamper-Reader-1 In Normal ---
Output Door-Strike Out Normal --- 12
Reader 1 Reader Active Type of reader: Standard Wie... 12
Door - 13 Online
Input Connection-Reader-1 In Active ---
Input Door-Monitor In Normal Normally open / Not supervis... 13
Input Interior-Handle-Rex In Normal Normally open / Not supervis... 13
Input Interior-Push-Button In Normal ---
Input Low-Battery In Normal ---
Input Magnetic-Tamper In Normal ---
Input Tamper-Reader-1 In Normal ---
Output Door-Strike Out Normal --- 13
Reader 1 Reader Active Type of reader: Standard Wie... 13

13

Verrous BEST Wi-Q via Mercury

Cette section aborde les sujets suivants:

Configurer le module externe Over-Watch pour l'intégration BEST Wi-Q

Avant d'inscrire des verrous BEST Wi-Q dans Security Center, vous devez configurer le module externe Over-Watch pour les contrôleurs Mercury LP4502.

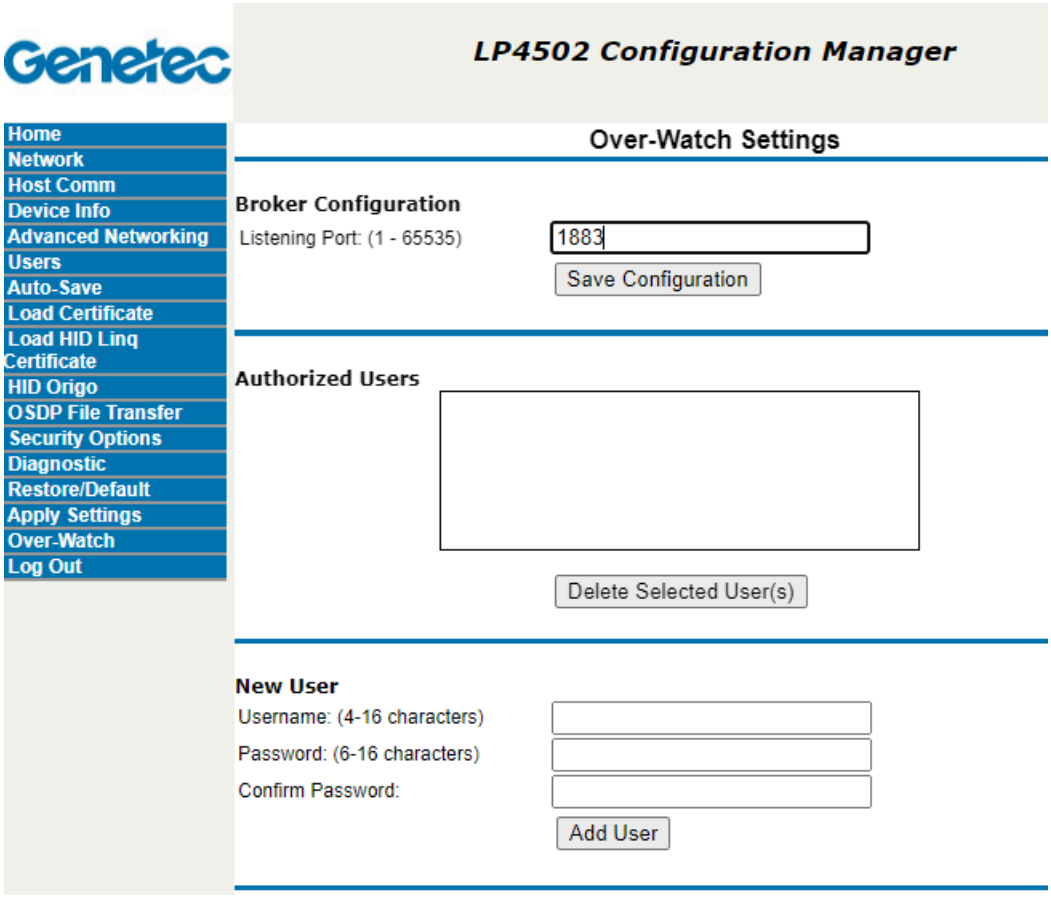
À savoir

- Tous les contrôleurs LP4502 sous une même unité Synergis[MC] Cloud Link doivent être configurés avec le même nom d'utilisateur, mot de passe et port d'écoute.
- Si vous souhaitez déplacer une unité Mercury LP4502 utilisée pour l'intégration BEST Wi-Q d'un Synergis Cloud Link vers un autre, le module externe Over-Watch doit être activé sur le Synergis Cloud Link cible avant le déplacement de l'unité.

Procédure

1 Chargez le module externe Over-Watch sur le contrôleur Mercury.
   a) Sur la page *Téléchargements de produits* de GTAP, sélectionnez **Synergis[MC] Cloud Link Legacy** dans la liste **Download Finder**, puis recherchez le dernier micrologiciel Mercury LP4502.
   b) Enregistrez le fichier *.sfw* sur votre lecteur local.
   c) Mettre à jour le contrôleur Mercury via le Synergis[MC] Appliance Portal .
      Le contrôleur Mercury redémarre après l'installation du micrologiciel.
   d) Connectez-vous à la page Web des options avancées de l'unité Synergis Cloud Link sur https://<Adresse IP>/MercuryEP/FirmwareVersions, puis cliquez sur l'option **Installer le pack Over Watch** affichée sous le contrôleur Mercury LP4502.
   Le contrôleur Mercury redémarre après l'installation du module externe.

2 Configurez l'utilisateur du module externe Over-Watch sur le contrôleur Mercury.
   a) Connectez-vous au contrôleur Mercury via sa page web *Configuration Manager*
   b) Dans le menu latéral, cliquez sur **Over-Watch**.
   c) Sur la page *Réglages Over-Watch*, entrez un numéro de port dans le champ **Port d'écoute**.
   Le port recommandé est le 1883.



   d) Dans la section *Nouvel utilisateur*, entrez un nom d'utilisateur et un mot de passe, confirmez le mot de passe, puis cliquez sur **Ajouter un utilisateur**.
   e) Dans le menu latéral, cliquez sur **Appliquer les réglages**, puis cliquez sur **Appliquer les réglages, Redémarrer**.

3 Configurez les réglages Mercury sur la passerelle BEST Wi-Q.
   a) Connectez-vous à la passerelle BEST Wi-Q.
   b) Dans le menu supérieur, cliquez sur l'onglet **Interface**.
   c) Sur la page *Mercury interface configuration*, sélectionnez l'option **Enable Mercury Mode**, puis entrez l'adresse IP du contrôleur Mercury.
   d) Dans les champs **Port**, **Mercury Username** et **Mercury Password** , entrez les informations (port, nom d'utilisateur et mot de passe) saisies à la création de l'utilisateur du module externe Over-Watch sur le contrôleur Mercury.
   e) Sélectionnez l'option **Enable SSL** (Activer le SSL), puis cliquez sur **Use Mercury certificate** (Utiliser le certificat Mercury).
   f) Cliquez sur **Mettre à jour.**

   L'état de la connexion est affiché en jaune.

4 Activez le module externe Over-Watch sur l'unité Synergis Cloud Link.
   a) Connectez-vous à l'unité Synergis Cloud Link.
   b) Cliquez sur **Configuration** > **Réglages de contrôleur Mercury**.
   c) Cliquez sur l'onglet **Réglages Over-Watch** dans le menu latéral.
   d) Sélectionnez l'option **Module externe LP4502 Over-Watch**, puis entrez le **Nom d'utilisateur**, **Mot de passe** et **Port** que vous avez configurés à la création de l'utilisateur du module externe Over-Watch sur le contrôleur Mercury.
   e) Cliquez sur **Enregistrer**.
   f) Redémarrez Synergis[MC] Softwire.

Lorsque vous avez terminé

Inscrivez une passerelle BEST Wi-Q sur l'unité Synergis[MC].

Inscription de passerelles BEST Wi-Q sur l'unité Synergis via un contrôleur Mercury

Vous devez inscrire les passerelles BEST Wi-Q par l'intermédiaire d'un contrôleur Mercury LP4502 dans Config Tool avant de pouvoir ajouter des verrous ou des contrôleurs d'accès sans fil BEST Wi-Q.

Avant de commencer

Configurez le module externe Over-Watch sur le contrôleur Mercury et activez-le sur l'unité Synergis[MC].

À savoir

Mercury controllers enrolled on a Synergis[MC] unit are not visible from the Synergis[MC] Appliance Portal *Hardware* page.

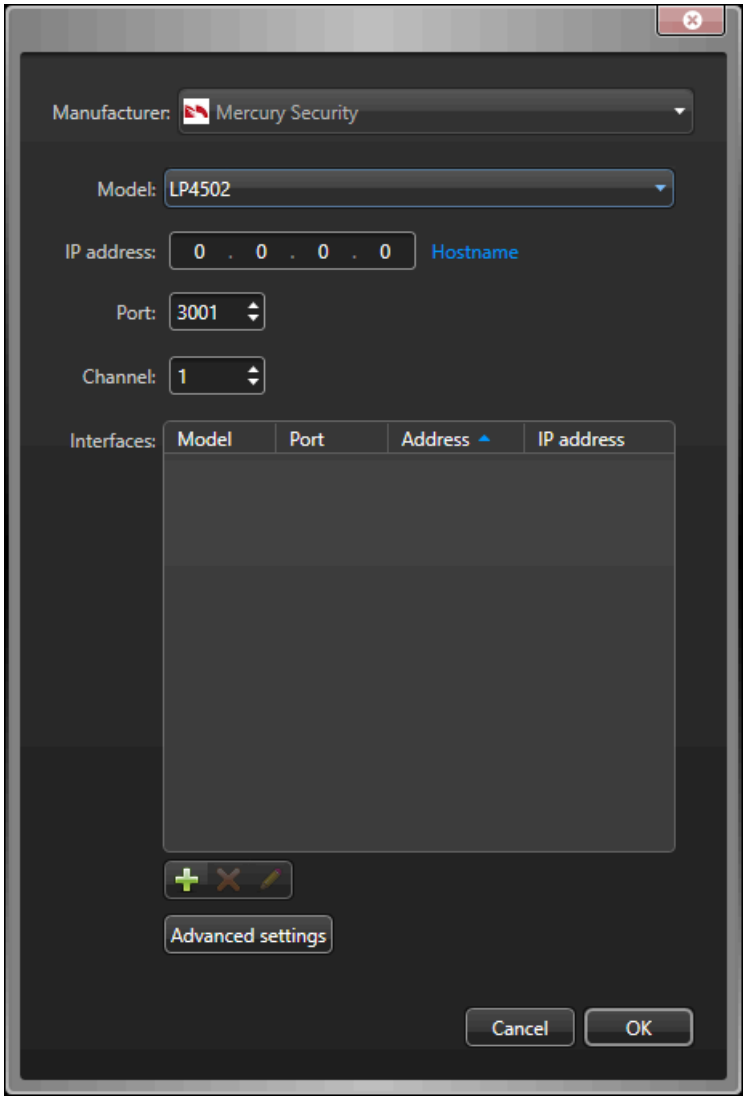
Procédure

1 Inscrivez le contrôleur Mercury LP4502 dans Config Tool.

a) Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.

b) Cliquez sur **Rôles et unités**, puis cliquez sur l'unité Synergis.

c) Cliquez sur **Périphériques**, puis sur **Ajouter un élément** ( ).



d) Saisissez les informations suivantes :

- **Modèle :** Sélectionnez LP4502.
- **Adresse IP :** Adresse IP statique affectée au contrôleur par votre service informatique.
- **Nom d'hôte :** Cliquez sur le lien bleu pour identifier le contrôleur par son nom d'hôte. Cette option n'est disponible que si vous exécutez Security Center 5.12.0.0 ou ultérieur.
- **Port :** Port de communication (3001 par défaut). Le port doit correspondre à la valeur configurée sur la page web Mercury Device Manager.
- **Canal :** ID de canal correspondant à ce contrôleur. L'ID de canal peut être compris entre 0 et 63, et doit être unique sur l'unité Synergis. Une fois qu'il est affecté, vous ne devez pas le modifier.

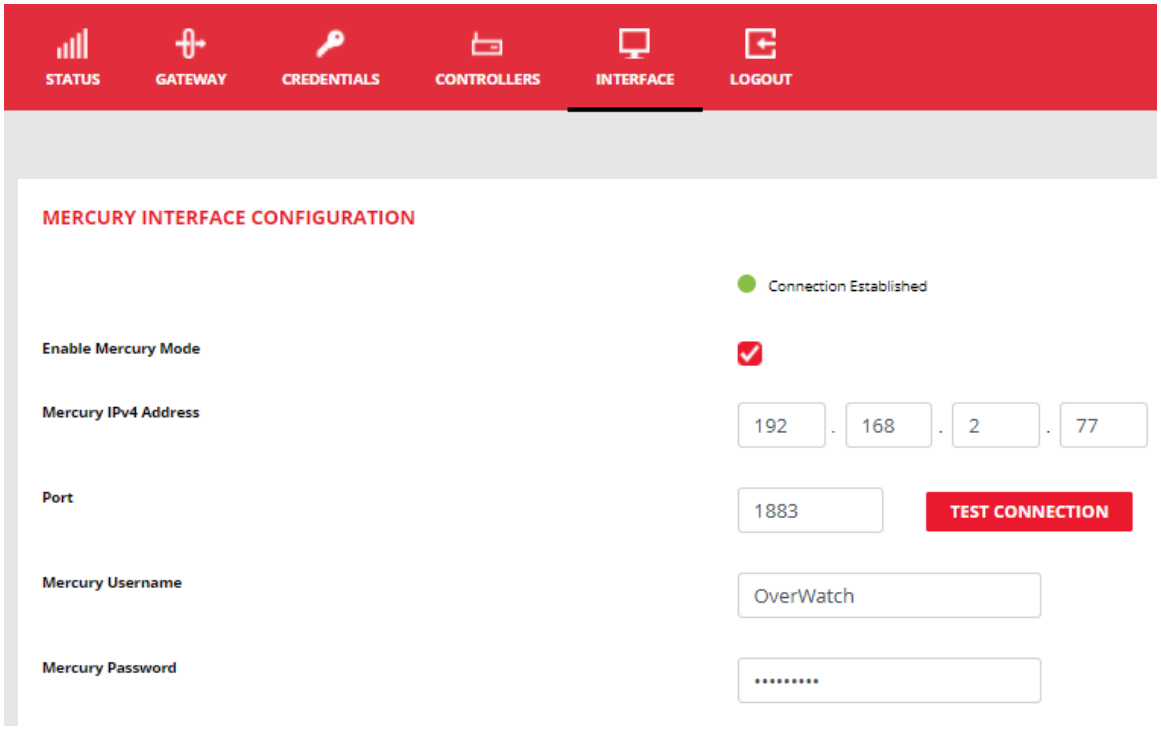
2 Ajoutez la passerelle BEST Wi-Q en tant qu'interface du contrôleur Mercury.

a) Sous la liste *Interfaces*, cliquez sur **Ajouter un élément** (➕).

b) Dans la boîte de dialogue qui apparaît, sélectionnez **Passerelle BEST Wi-Q** en tant que **Modèle**, et entrez l'**Adresse MAC**.

REMARQUE : L'adresse MAC doit être saisie en majuscules, compter 12 caractères, et ne doit pas contenir de points, de deux-points ou de tirets. Par exemple, *A1B2C3D4E5F6*.

Vérifiez que le contrôleur Mercury et la passerelle BEST Wi-Q sont en ligne sur la page **Périphériques** de l'unité Synergis[MC] Cloud Link dans Config Tool, et que la connexion est établie sur la page Web de la passerelle BEST Wi-Q.



Lorsque vous avez terminé

Jumelez les verrous ou contrôleurs d'accès sans fil BEST Wi-Q avec la passerelle BEST Wi-Q, puis affectez-leur des ID ACR (access control reader) depuis la page Web de la passerelle, afin de pouvoir les ajouter plus tard dans Config Tool. Pour en savoir plus sur le jumelage d'appareils avec la passerelle, voir la documentation BEST Wi-Q.

Ajouter des verrous et des contrôleurs d’accès sans fil BEST Wi-Q à la passerelle

Vous devez ajouter des verrous et des contrôleurs d’accès sans fil BEST Wi-Q à la passerelle dans Config Tool.

Avant de commencer

Jumelez les verrous ou contrôleurs d’accès sans fil BEST Wi-Q à la passerelle BEST Wi-Q, puis affectez-leur des ID ACR (access control reader) depuis la page Web de la passerelle, afin de pouvoir les ajouter dans Config Tool. Pour en savoir plus sur le jumelage d’appareils avec la passerelle, voir la documentation BEST Wi-Q.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.

2 Cliquez sur **Rôles et unités**, puis cliquez sur l’unité Synergis[MC].

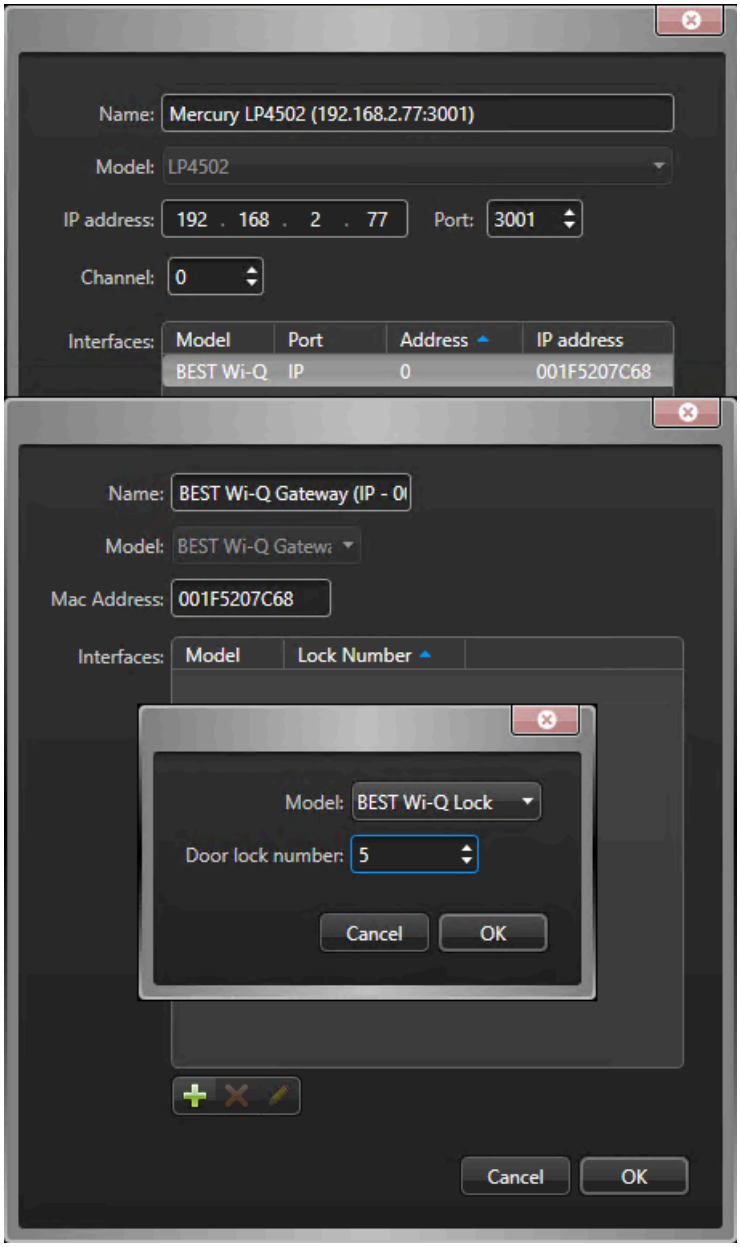
3 Cliquez sur l’onglet **Périphériques**, puis cliquez deux fois sur le contrôleur Mercury LP4502.

4 Dans la boîte de dialogue qui apparaît, cliquez deux fois sur la passerelle BEST Wi-Q dans la liste *Interfaces*.

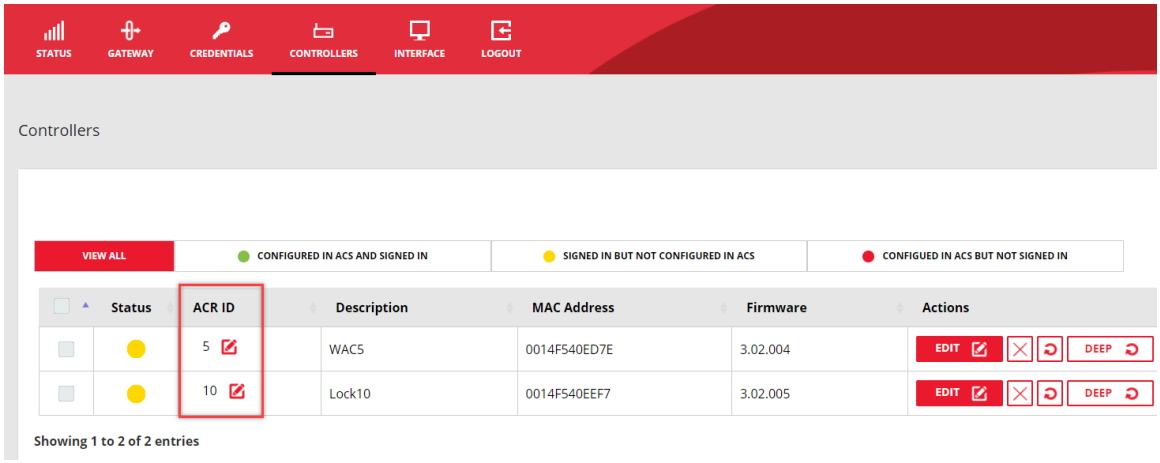
5 Dans la boîte de dialogue qui apparaît, cliquez sur **Ajouter un élément** ( ) sous la liste *Interfaces*.

Une boîte de dialogue apparaît, dans laquelle **Verrou BEST Wi-Q** est sélectionné en tant que **Modèle**. Cette option est utilisée pour les verrous et les contrôleurs d’accès sans fil.

6 Entrez le **Numéro de verrou de porte** du verrou ou du contrôleur sans fil, puis cliquez sur **OK**.



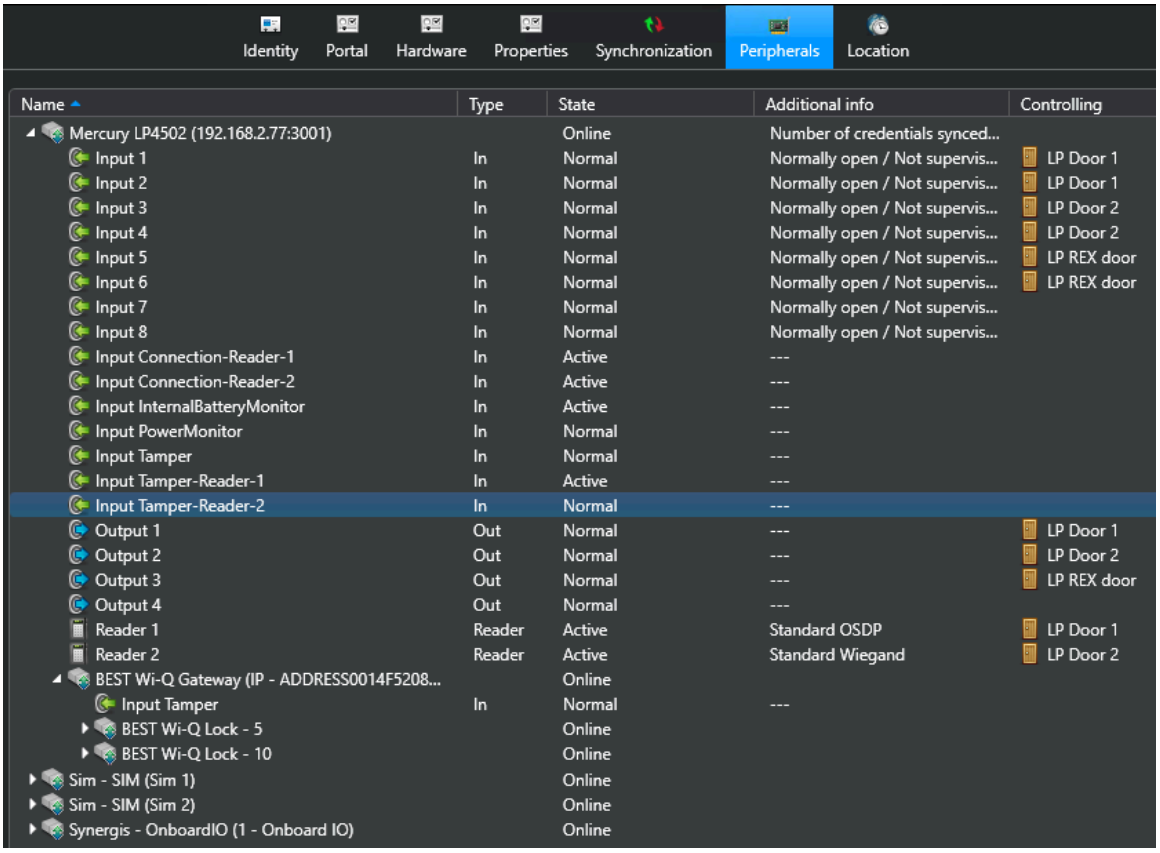
REMARQUE : Le numéro de verrou de porte doit correspondre à l'ID ACR affecté au verrou ou au contrôleur sans fil sur la page Web de la passerelle BEST Wi-Q.



7 Cliquez sur **OK** > **OK**.

8 Cliquez sur **Appliquer**.

Le contrôleur Mercury, la passerelle et les verrous BEST Wi-Q sont affichés sur la page *Périphériques*.

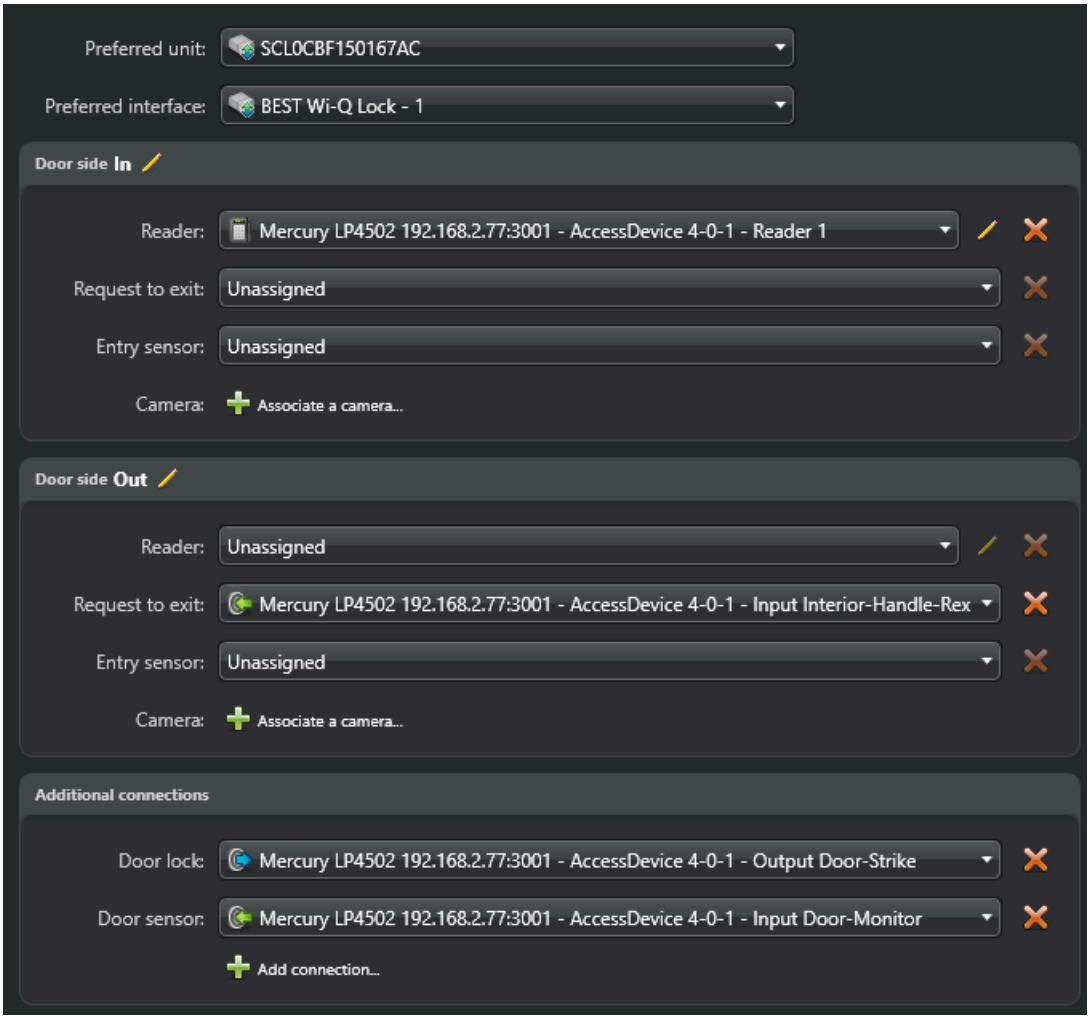


Sur la page Web de la passerelle BEST Wi-Q, l'état du verrou ou du contrôleur sans fil que vous avez ajouté dans Config Tool devient vert.

Lorsque vous avez terminé

Affectez les E/S du verrou ou du contrôleur sans fil aux portes dans Config Tool. Vous pouvez utiliser le modèle de porte *Contrôle unidirectionnel* pour simplifier la configuration.

Exemple : L'image suivante illustre une configuration typique sur la page *Matériel* d'une porte.


Preferred unit:
SCL0CBF150167AC
Preferred interface:
BEST Wi-Q Lock - 1
Door side In
Reader:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Reader 1
Request to exit:
Unassigned
Entry sensor:
Unassigned
Camera:
Associate a camera...
Door side Out
Reader:
Unassigned
Request to exit:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Input Interior-Handle-Rex
Entry sensor:
Unassigned
Camera:
Associate a camera...
Additional connections
Door lock:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Output Door-Strike
Door sensor:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Input Door-Monitor
Add connection...

À propos du mode passage BEST Wi-Q

Les appareils BEST Wi-Q ont leur propre fonction de mode passage, également appelée *mode salle de classe* ou *double badge*, qui permet aux utilisateurs de badger deux fois sur le lecteur pour déverrouiller une porte, puis la reverrouiller.

Activer et configurer cette fonctionnalité

Le mode passage BEST Wi-Q est activé via le champ personnalisé de porte *DoubleSwipe*, comme pour l'activation de la fonction d'activation du double badge dans Security Center.

Pour en savoir plus, voir les rubriques suivantes dans le *Guide de l'administrateur Security Center* :

- À propos de l'activation à double balayage
- Activer l'activation à double balayage
- Configurer une porte pour l'activation à double balayage

Pour qu'un titulaire de cartes puisse utiliser la fonction de mode passage, il doit appartenir à tous les groupes de titulaires de cartes configurés pour l'utilisation du champ personnalisé *DoubleSwipe* sur toutes les portes BEST Wi-Q sous un même contrôleur Mercury LP4502. Pour simplifier la configuration, il est donc recommandé de n'autoriser qu'un seul groupe de titulaires de cartes à utiliser cette fonctionnalité sur ces portes.

Une fois que la fonction est configurée, passer deux fois son badge sur le lecteur génère l'événement *Double balayage activé*, et déverrouille la porte. Badger à nouveau deux fois sur le même lecteur génère l'événement *Double balayage désactivé*, et reverrouille la porte.

Limitations

Les portes équipées de verrous BEST Wi-Q ne prennent pas en charge les fonctions d'avertisseur sonore Mercury.

14

Verrous SimonsVoss SmartIntego via Mercury

Cette section aborde les sujets suivants:

Préparer l'inscription des verrous SimonsVoss SmartIntego

Avant d'inscrire les verrous SmartIntego sur l'unité Synergis[MC], vous devez jumeler le nœud Gateway avec les verrous SmartIntego.

À savoir

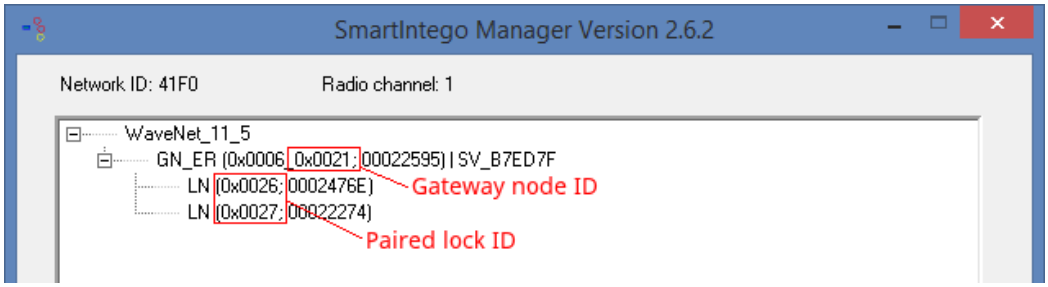
Les étapes et instructions de *Renforcement* sont facultatives, mais protègent votre système contre les cyberattaques.

Procédure

1 Suivez la documentation livrée avec vos appareils SmartIntego et jumelez le nœud Gateway avec vos verrous SmartIntego.

2 Notez les informations suivantes :

- L'adresse IP du nœud Gateway.
- Les ID des appareils indiqués dans la fenêtre de *SmartIntego Manager*.

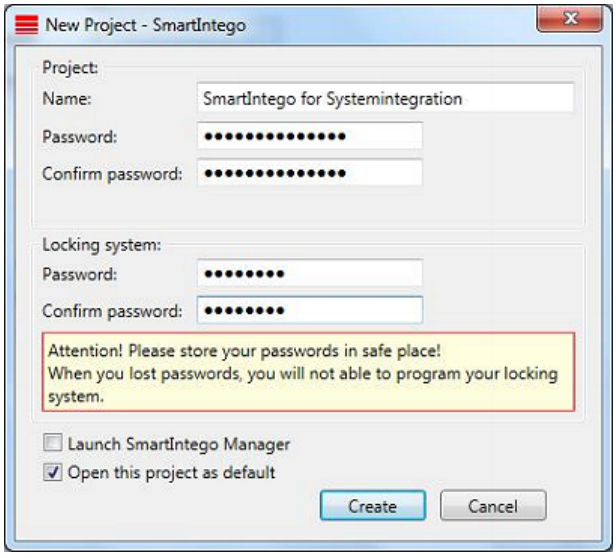


L'ID du nœud Gateway est le deuxième numéro hexadécimal après GN_ER.

L'ID du verrou est le premier numéro hexadécimal après LN.

3 (*Renforcement*) Suivez la documentation livrée avec vos appareils SmartIntego et configurez la clé de chiffrement des communications pour vos verrous.

Le logiciel SmartIntego ne permet pas le jumelage d'un verrou au concentrateur sans mot de passe. Utilisez un mot de passe fort pour le système de verrouillage.



Inscription de verrous SimonsVoss SmartIntego sur une unité Synergis

Comme l'unité Synergis[MC] ne communique pas avec les appareils SimonsVoss SmartIntego, vous devez inscrire ces appareils par l'intermédiaire d'un contrôleur Mercury EP, LP, MP ou Honeywell, en utilisant Config Tool.

Avant de commencer

Jumelez le nœud Gateway avec vos verrous SmartIntego.

À savoir

Les contrôleurs Mercury inscrits sur une unité Synergis ne sont pas visibles sur la page *Matériel* du portail de l'appareil Synergis[MC].

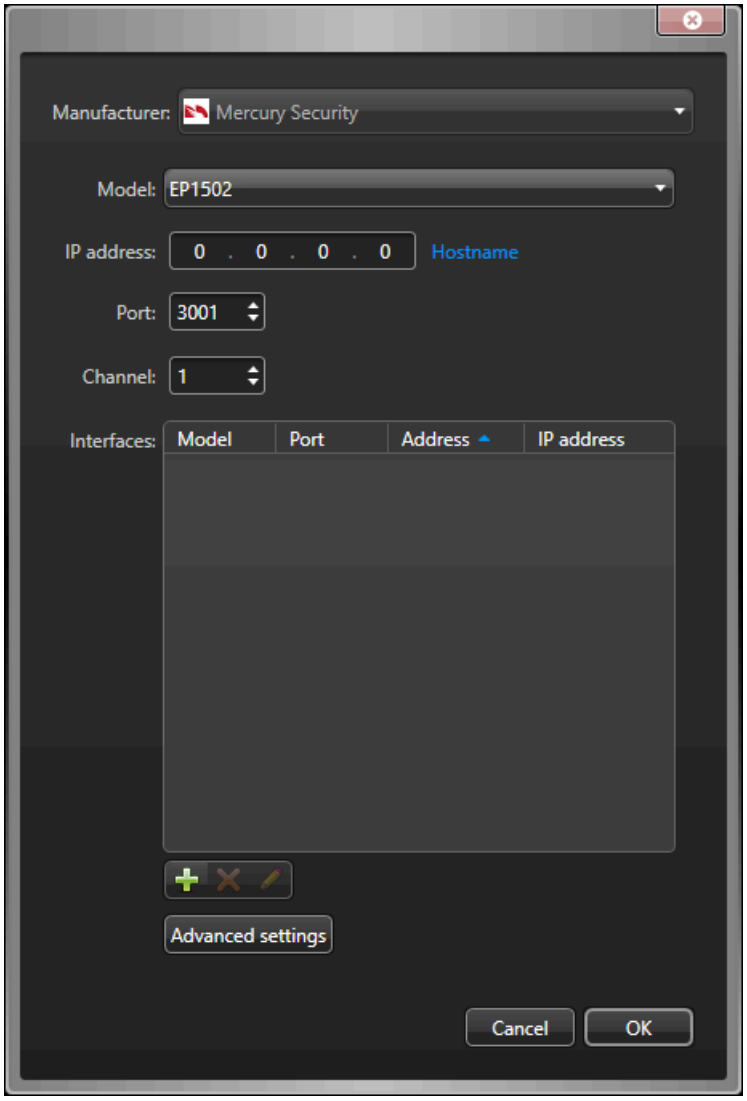
Sur l'unité Synergis, un ID de canal unique doit être affecté à chaque contrôleur Mercury. Le contrôleur communique avec les nœuds Gateway SmartIntego par IP. Les adresses IP ne peuvent pas se chevaucher sur un même réseau.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.

2 Cliquez sur **Rôles et unités**, puis cliquez sur l'unité Synergis.

3 Cliquez sur **Périphériques**, puis sur **Ajouter un élément** ( ).



4 Saisissez les informations suivantes :

- **Modèle :** Modèle du contrôleur.
- **Adresse IP :** Adresse IP statique affectée au contrôleur par votre service informatique.
- **Nom d'hôte :** Cliquez sur le lien bleu pour identifier le contrôleur par son nom d'hôte. Cette option n'est disponible que si vous exécutez Security Center 5.12.0.0 ou ultérieur.

  REMARQUE : Lorsque vous inscrivez un contrôleur Mercury avec son nom d'hôte, vous devez lui adjoindre `.local` si le contrôleur n'utilise pas le DHCP et le DNS sur le réseau.
- **Port :** Port de communication. La valeur par défaut est 3001. Le port doit correspondre à la valeur configurée sur la page web Mercury Device Manager.
- **Canal :** ID de canal correspondant à ce contrôleur. L'ID de canal peut être compris entre 0 et 63, et doit être unique sur l'unité Synergis. Une fois qu'il est affecté, vous ne devez pas le modifier.

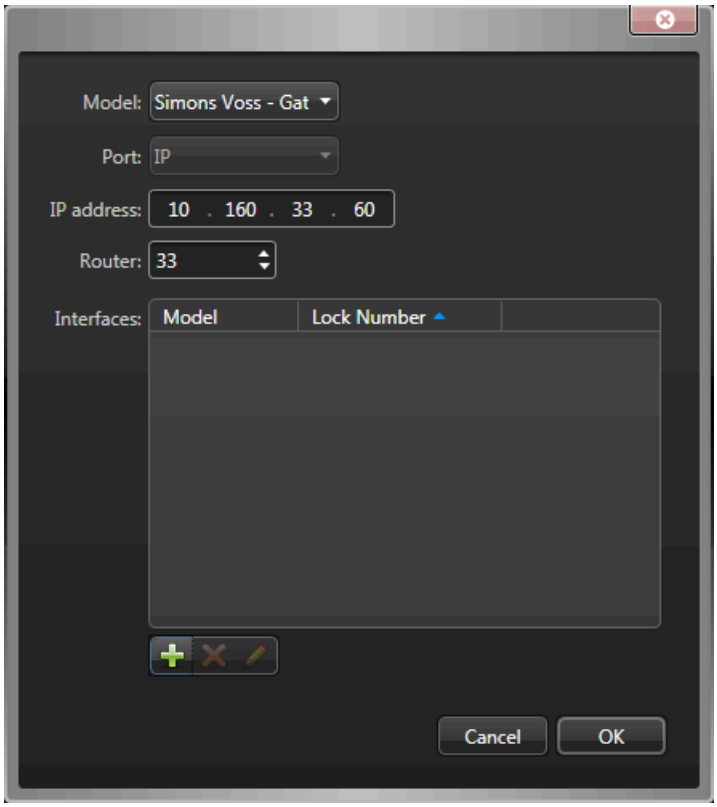
5 Au bas du groupe *Interfaces*, cliquez sur **Ajouter un élément** (➕) pour ajouter le nœud Gateway SmartIntego qui doit communiquer avec le contrôleur.

a) Dans la boîte de dialogue qui apparaît, cliquez sur **Modèle** et sélectionnez **Nœud Gateway SimonsVoss**.

b) Dans **adresse IP**, entrez l'adresse IP du nœud Gateway.

c) Dans **Routeur**, entrez la valeur décimale de l'ID du nœud Gateway.

Par exemple, si l'ID du nœud Gateway est 0x0021, entrez 33 (= 2 x 16 + 1).

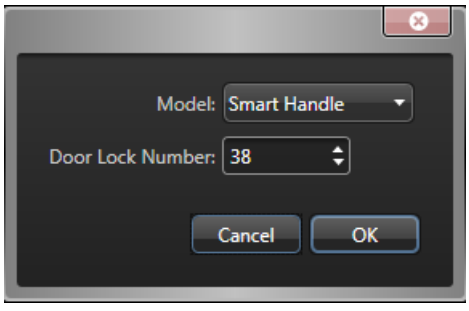


6 Au bas du groupe *Interfaces*, cliquez sur **Ajouter un élément** (➕) pour ajouter les verrous jumelés avec le nœud Gateway.

a) Dans la boîte de dialogue qui apparaît, cliquez sur **Modèle** et sélectionnez le modèle de verrou (Smart Handle, Padlock, Cylinder, et ainsi de suite).

b) Dans **Numéro de verrou**, entrez la valeur décimale de l'ID du verrou.

Par exemple, si l'ID du verrou est 0x0026, entrez 38 (= 2 x 16 + 6)



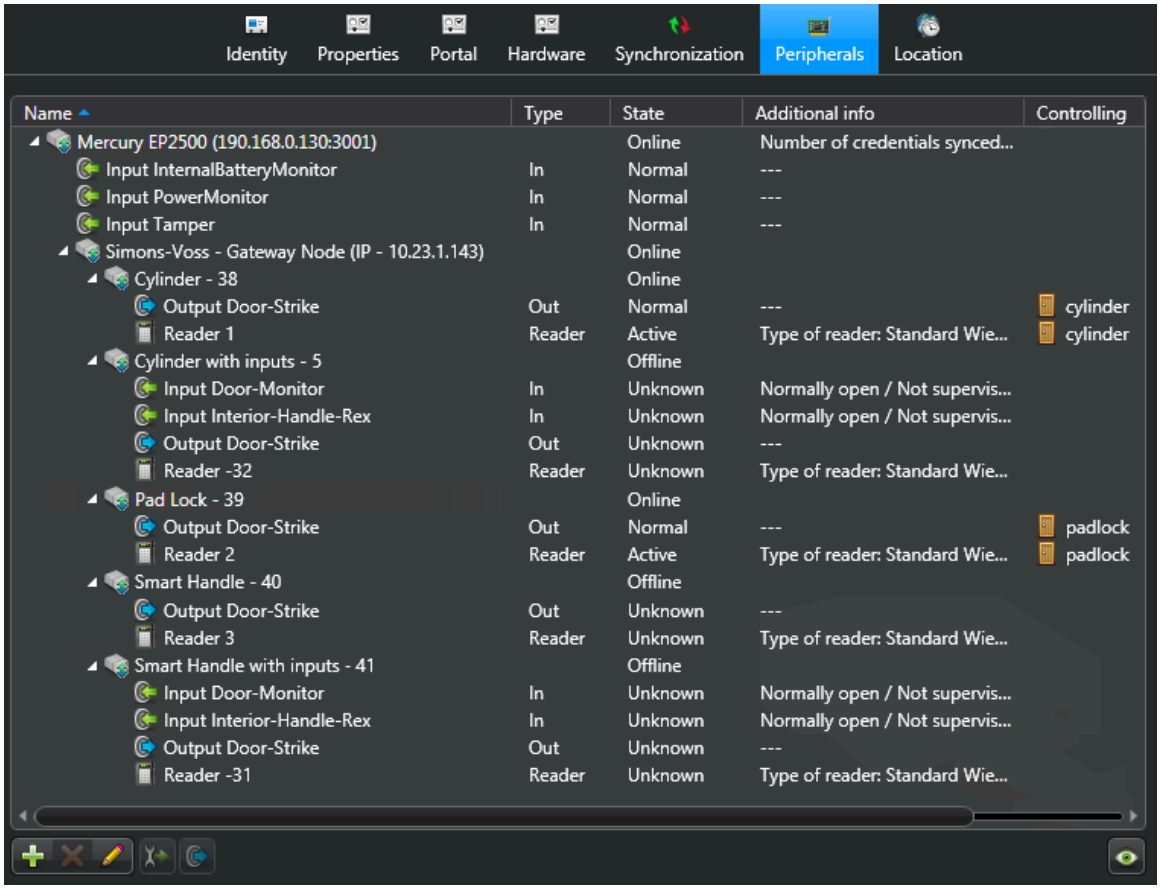
c) Cliquez sur **OK**.

d) Répétez pour les autres verrous à ajouter.

e) Cliquez sur **OK**.

7 Cliquez sur **OK** > **Appliquer**.

Le contrôleur Mercury ainsi que tous ses sous-tableaux et périphériques connectés sont affichés sur la page *Périphériques*.



REMARQUE : L'ajout de modules d'interface à l'unité Synergis entraîne un redémarrage logiciel de l'unité. Durant ce processus, l'unité Synergis et tous les périphériques associés sont affichés en rouge.

8 Testez votre configuration en déclenchant les sorties.

L'état de la sortie déclenchée change en temps réel à l'écran.

REMARQUE : L'activité des lecteurs n'est pas affichée sur la page *Périphériques*.

15

Verrous sans fil SALTO SALLIS

Cette section aborde les sujets suivants:

Inscrire des verrous SALTO SALLIS locks

Pour que l'unité Synergis[MC] puisse communiquer avec les verrous SALTO SALLIS, vous devez les inscrire dans Security Center à l'aide du Synergis[MC] Appliance Portal.

Avant de commencer

Configurez votre infrastructure SALTO SALLIS (routeurs, nœuds et verrous sans fil) en suivant les instructions du *Guide d'installation et de maintenance SALLIS*.

Définissez d'abord les nœuds et les portes avec l'application SALLIS, puis mettre à jour les routeurs et initialiser les verrous avec le PPD (Portable Programmer Device). Ce faisant, notez les informations suivantes :

- **Routeur IP :** Adresse IP et numéro de port.
- **Routeur RS-485 :** Canal de l'unité Synergis auquel le routeur est connecté (1 - 4) .
- **Verrou :** Routeur, ID de verrou et porte concernée.

  Utilisez des noms de porte descriptifs, comme *Débarras du premier étage*. Si vous avez déjà créé les entités porte dans Security Center, utilisez les mêmes noms pour simplifier les choses.

À savoir

Les étapes et instructions de *Renforcement* sont facultatives, mais protègent votre système contre les cyberattaques.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

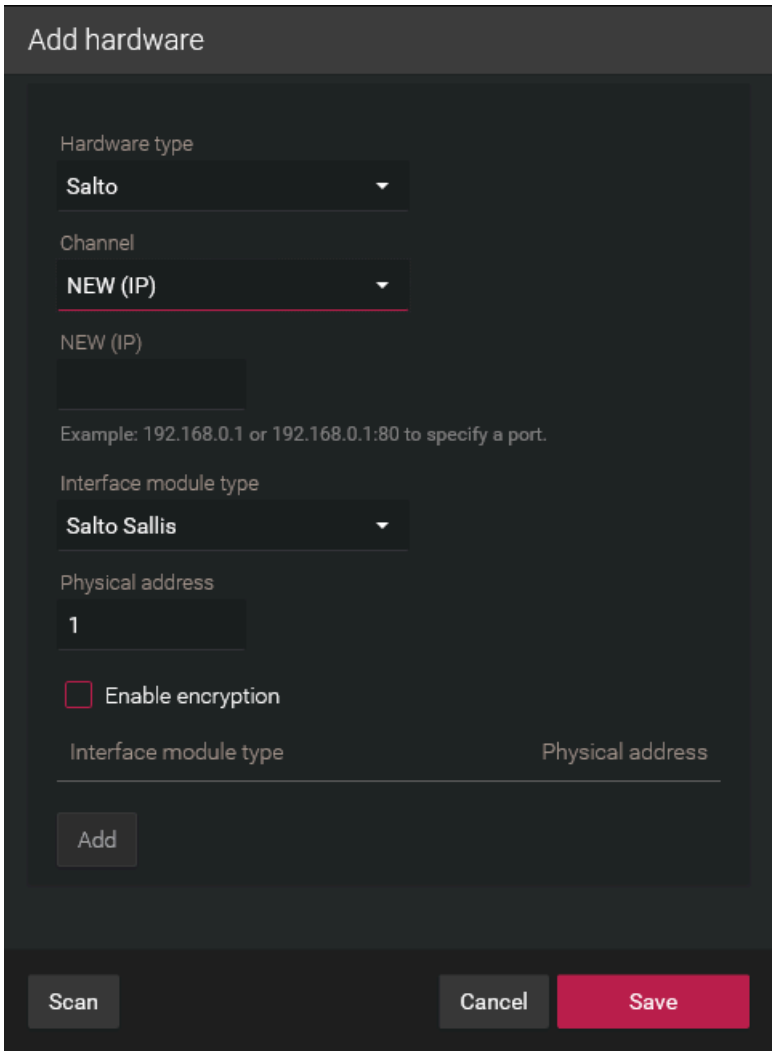
2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** (➕).

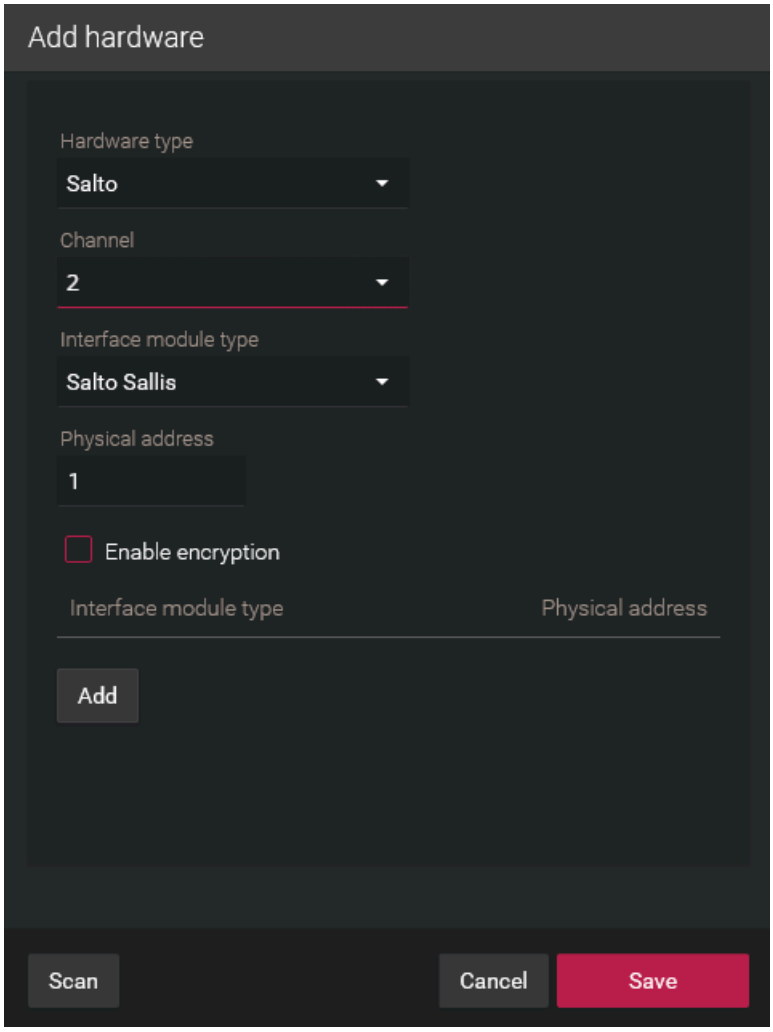
4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **Salto** en tant que **Type de matériel**.

5 Identifiez le canal auquel est connecté le routeur SALLIS, et procédez de l'une des manières suivantes :

- Sélectionnez le canal IP et entrez l'adresse IP et le numéro de port du routeur.

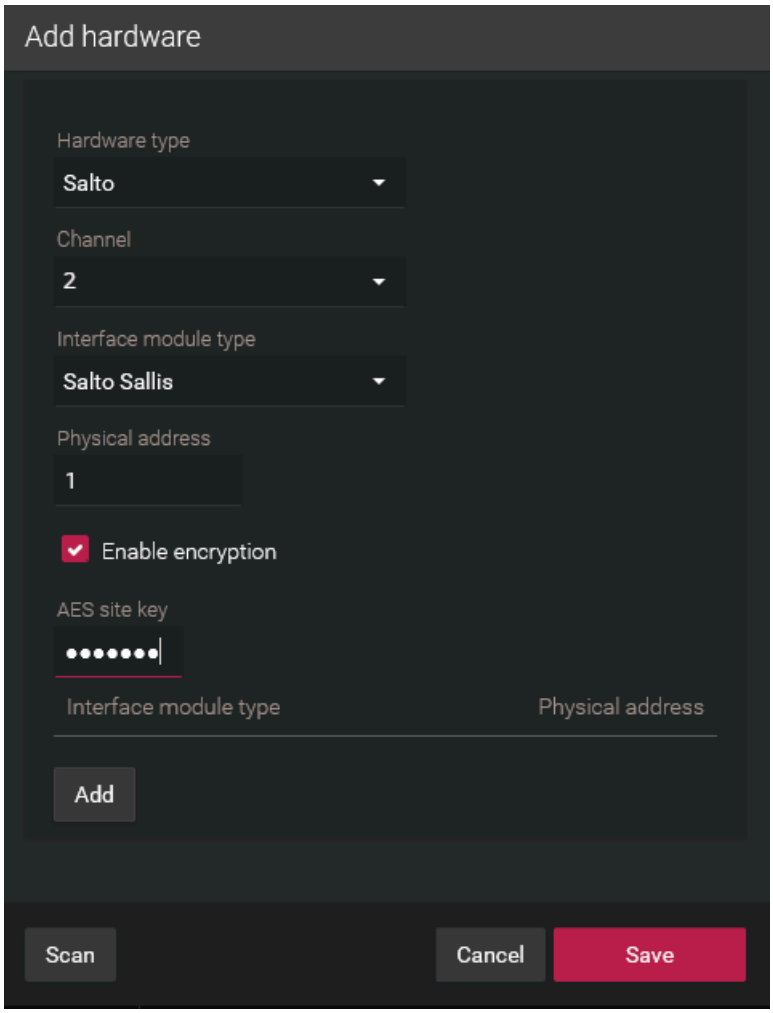


- Sélectionnez un canal RS-485 (1 - 4) . Tous les modules d'interface connectés à un même canal RS-485 doivent provenir d'un même fabricant.


Add hardware
Hardware type
Salto
Channel
2
Interface module type
Salto Sallis
Physical address
1
Enable encryption
Interface module type
Physical address
Add
Scan
Cancel
Save

6 (Renforcement) Pour utiliser le chiffrement, sélectionnez **Activer le chiffrement** et entrez la **clé de site AES**.

REMARQUE : Vous ne pouvez pas modifier les réglages de chiffrement depuis la boîte de dialogue *Ajouter du matériel* sur un canal existant. Pour activer le chiffrement lorsque le canal a déjà été créé, modifiez la configuration du canal sur le Synergis[MC] Appliance Portal.



7 Dans la même boîte de dialogue, ajoutez tous les modules d'interface connectés au même canal.

Vous pouvez inscrire les modules d'interface automatiquement ou manuellement.

CONSEIL : Si vous connaissez les ID de verrous (adresses physiques) et que vous inscrivez peu de modules, l'inscription manuelle est plus rapide.

- Pour les inscrire automatiquement, cliquez sur **Analyser**.

  La fonction d'analyse détecte tous les modules d'interface d'un même fabricant connectés au même canal.

  Si le contrôleur ne détecte pas tous les modules d'interface connectés, vérifiez qu'ils ont tous une adresse physique distincte.
- Pour l'inscription manuelle, entrez l'ID de verrou en tant qu'**Adresse physique**, et cliquez sur **Ajouter** (➕).

  REMARQUE : Les ID de verrou valables sont 1 à 16 pour les routeurs RS-485, et 1 à 64 pour les routeurs PoE.

  Répétez pour configurer tous les verrous sans fil connectés au même canal.

8 Cliquez sur **Enregistrer**.

Le type de matériel, le canal et le module d'interface que vous venez d'ajouter sont répertoriés sur la page *Configuration matérielle*.

9 Testez la connexion de votre module d'interface et votre configuration à partir de la page *Diagnostics d'E/S*.

Lorsque vous avez terminé

Associez vos portes aux verrous SALLIS dans Security Center.

Activer le chiffrement sur un routeur SALLIS existant

Le chiffrement est une propriété de canal sur le Synergis[MC] Appliance Portal. Vous pouvez activer le chiffrement ou modifier le mot de passe de chiffrement sur un routeur SALLIS en modifiant la configuration du canal sur le Synergis[MC] Appliance Portal.

À savoir

Vous ne pouvez pas modifier les réglages de canal tout en ajoutant un verrou à un canal existant. Une fois le canal créé, toutes les modifications des propriétés du canal doivent être effectuées depuis la page de propriétés du canal. Une fois que le chiffrement est activé, vous ne pouvez pas le désactiver uniquement sur le Synergis[MC] Appliance Portal. Vous devez également désactiver le chiffrement en vous connectant directement au routeur.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 Sélectionnez le canal SALTO.

4 Sélectionnez l'option **Activer le chiffrement**, puis entrez la **clé de site AES**.

5 Cliquez sur **Enregistrer**.

Désactiver le chiffrement sur un routeur SALLIS

Pour désactiver le chiffrement sur un routeur SALLIS, vous devez le désactiver à la fois sur le Synergis[MC] Appliance Portal et sur le routeur lui-même.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** (➕).

4 Sélectionnez le canal SALTO, puis décochez l'option **Activer le chiffrement**.

5 Cliquez sur **Enregistrer**.

Dans l'arborescence des appareils, tous les verrous SALLIS sous le canal sélectionné sont affichés en rouge (inactifs).

6 Sur un routeur RS-485, procédez de la manière suivante :

a) À l'aide de l'application SALLIS, téléchargez la configuration du routeur sur le PPD.

b) Sur le PPD, sélectionnez **Update router** (Mettre à jour le routeur).

c) Connectez le PPD au routeur.

7 Sur un routeur PoE, procédez de la manière suivante :

REMARQUE : Si vous avez plusieurs routeurs, vous devez les mettre à jour un par un.

a) Ouvrez le boîtier du routeur PoE, puis appuyez sur le bouton **CLR** pendant 5 secondes.

Le témoin DEL du routeur PoE devient orange.

b) Avec un navigateur web, connectez-vous au portail web du routeur.

Saisissez http://192.168.0.234 dans la barre d'adresse du navigateur.

REMARQUE : Votre poste doit être sur le même sous-réseau que le routeur pour pouvoir vous connecter à son portail web.

c) Dans le navigateur, sous **Chiffrement du routeur** > **Revenir au mode simple ?**, sélectionnez **Oui**.

d) Cliquez sur **Envoyer**.

Le message *Configuration envoyée avec succès* apparaît dans le navigateur. Dans l'arborescence des appareils, tous les verrous SALLIS figurant sous le canal sélectionné sont affichés en noir (actifs).

16

Lecteurs OSDP connectés aux ports Synergis Cloud Link RS-485

Cette section aborde les sujets suivants:

Créer un canal pour configurer les lecteurs OSDP dans Synergis Appliance Portal

Avant d'utiliser les lecteurs OSDP, vous devez configurer leurs adresses et leur débit binaire RS-485. Vous pouvez configurer vos lecteurs directement sur le Synergis[MC] Appliance Portal en créant un canal OSDP avec le mode Programmation activé.

À savoir

- Pour les lecteurs OSDP que vous souhaitez connecter à une unité Mercury, cette procédure, suivie de la définition de l'adresse physique du lecteur dans Synergis Appliance Portal remplace l'utilisation d'une carte de configuration pour définir le débit en bauds et l'adresse physique du lecteur.
- Lorsque le mode Programmation est activé, vous ne pouvez avoir qu'un seul lecteur en ligne connecté au canal RS-485 à la fois.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** (➕).

4 Dans la boîte de dialogue *Ajouter du matériel*, sélectionnez **OSDP** en tant que **Type de matériel**.

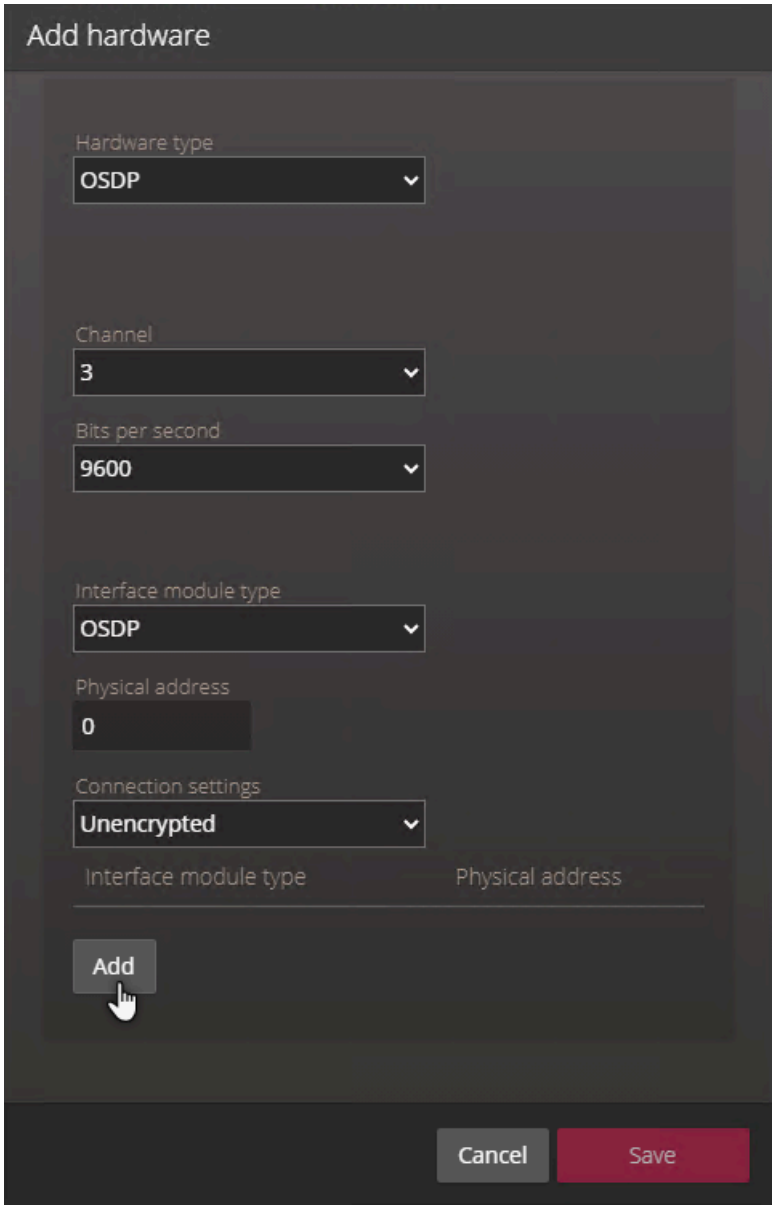
5 Sélectionnez le **Canal** (1 - 4) .

REMARQUE : Si vous avez l'unité Synergis Cloud Link 312, vous avez jusqu'à 12 canaux. Pour en savoir plus, voir À propos des ports RS-485 du Synergis Cloud Link.

6 Dans la liste **Bits par seconde**, sélectionnez le débit binaire que vous souhaitez utiliser sur votre appareil.

REMARQUE : Sélectionnez **Autre** dans la liste pour entrer un débit binaire personnalisé.

7 Sous **Type de module d'interface**, cliquez sur **Ajouter**.

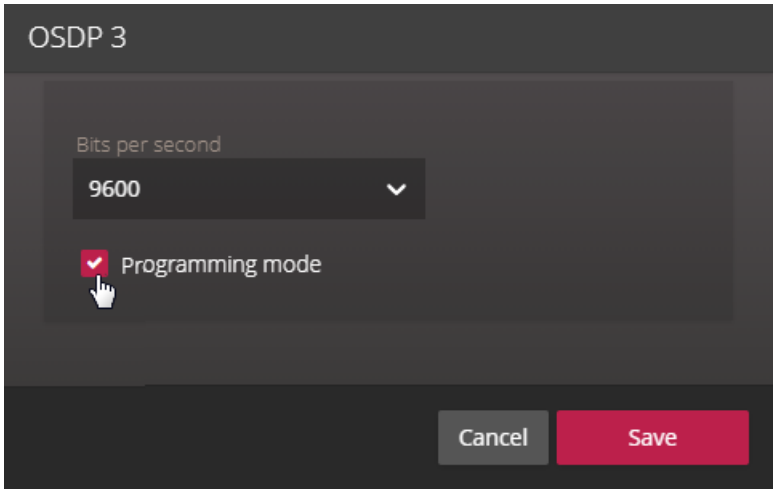


8 Cliquez sur **Enregistrer**.
Le canal et l'interface sont créés.

9 Dans l'arborescence matérielle, sélectionnez le canal OSDP que vous avez créé et cliquez sur **Modifier** ( ).

10 Si vous ajoutez un lecteur, cochez la case **Mode programmation**.

Si vous avez une carte de configuration, vous pouvez l'utiliser à la place du **Mode programmation**. Voir la documentation fournie avec votre carte.



11 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Configurer les lecteurs OSDP

Configurer et ajouter des lecteurs OSDP dans Synergis Appliance Portal

Pour ajouter des lecteurs OSDP à une unité Mercury ou Synergis[MC], configurez les lecteurs sur le Synergis[MC] Appliance Portal.

Avant de commencer

Créez un canal OSDP avec le mode Programmation activé.

À savoir

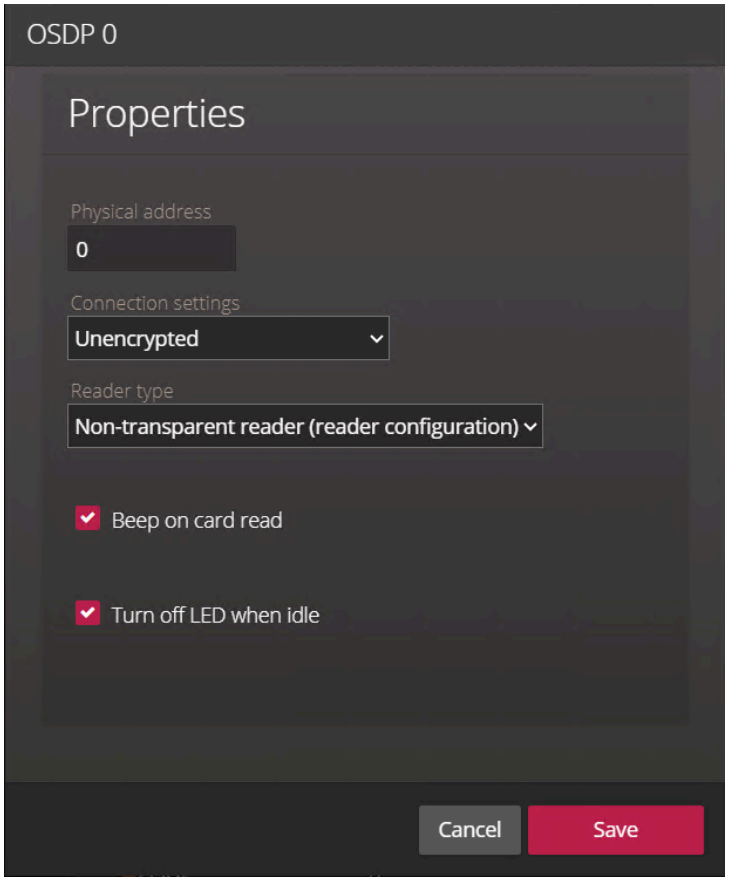
- Tous les lecteurs connectés à un même canal RS-485 doivent être configurés avec des adresses différentes.
- Avant de connecter des lecteurs OSDP à une unité Mercury, vous devrez parfois spécifier le débit en bauds et l'adresse du lecteur. Définir le débit en bauds dans Synergis Appliance Portal, puis suivre cette procédure remplace l'utilisation d'une carte de configuration.
- Lorsque le mode Programmation est activé, vous ne pouvez connecter qu'un seul lecteur à la fois au canal RS-485.

BONNE PRATIQUE : Si vous installez des lecteurs OSDP sur des tourniquets adjacents, il est déconseillé de connecter plus de deux lecteurs à un même canal RS-485, car le délai de réponse du contrôleur sera plus long, et que les chances que deux cartes seront présentées en même temps sont élevées. Pour les portes ordinaires, vous pouvez installer jusqu'à quatre lecteurs par bus.

Procédure

1 Dans l'arborescence matérielle, sélectionnez le lecteur OSDP que vous avez ajouté en créant le canal OSDP, et cliquez sur **Modifier** ( ).

2 Dans la boîte de dialogue *Propriétés*, saisissez l'adresse physique que vous voulez définir pour le lecteur et configurez les options **Signal sonore pour carte lue** et **Éteindre la LED en cas d'inactivité**, si nécessaire.



3 Cliquez sur **Enregistrer**.

4 Connectez et allumez le lecteur.

Le débit binaire et l'adresse physique configurés sont envoyés au lecteur, qui bascule en ligne une fois qu'il les a acceptés.

5 Déconnectez ou éteignez le lecteur.

6 Répétez les étapes 1 à 5 pour les autres lecteurs.

7 Dans l'arborescence matérielle, sélectionnez le canal OSDP et cliquez sur **Modifier** (), puis décochez la case **Mode programmation** cochée durant la création du canal.

8 Ajoutez les lecteurs configurés :

a. En haut de la colonne *Adresse*, cliquez sur **Ajouter** ().

b. Dans la boîte de dialogue *Ajouter du matériel*, cliquez sur **Ajouter** pour ajouter les lecteurs aux adresses que vous avez programmées.

9 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Activez le mode sécurisé sur les lecteurs.

Activer le jumelage sécurisé sur les lecteurs OSDP dans Synergis Appliance Portal

Par défaut, les lecteurs OSDP sont inscrits en état non chiffré. Activer le jumelage sécurisé renforce la sécurité des points d'accès.

Avant de commencer

Configurez les lecteurs OSDP.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 Dans l'arborescence matérielle, sélectionnez le lecteur OSDP et cliquez sur **Modifier** ( ).

4 Dans la liste **Réglages de connexion**, sélectionnez **Chiffré**.

5 Dans la liste **des clés du canal sécurisé OSDP**, sélectionnez l'une des options suivantes :

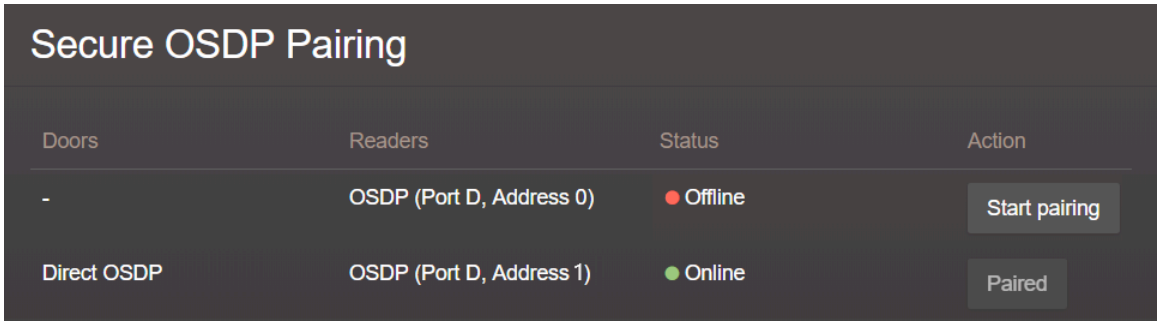
- **Clé aléatoire :** Génère une clé aléatoire de 128 bits (32 caractères hexadécimaux)
- **Clé par défaut :** Utilise la clé par défaut de l'unité. Ce choix est moins sûr.
- **Clé spécifique :** Cette option vous permet de spécifier votre propre clé de 128 bits (32 caractères hexadécimaux).

6 Cliquez sur **Enregistrer**.

7 Cliquez sur **Configuration** > **OSDP avancé**.

8 Repérez la ligne avec le port, le lecteur et la porte associée, et cliquez sur **Démarrer l'association**.

Les clés sont partagées et les lecteurs rebasculent en ligne. Le lecteur est à présent sécurisé. Tout lecteur qui refuse la clé reste déconnecté.



Activer MIFARE DESFire pour les lecteurs OSDP transparents

Les lecteurs OSDP en mode transparent vous obligent à stocker les clés sur votre unité Synergis[MC] Cloud Link ou sur des cartes SAM (Secure Access Module) si vous avez le modèle Synergis Cloud Link 312.

Avant de commencer

Configurez les clés MIFARE DESFire sur votre unité Synergis Cloud Link.

À savoir

Le mode *Carte ou PIN* n'est pas pris en charge avec les lecteurs OSDP configurés en mode DESFire (mode transparent).

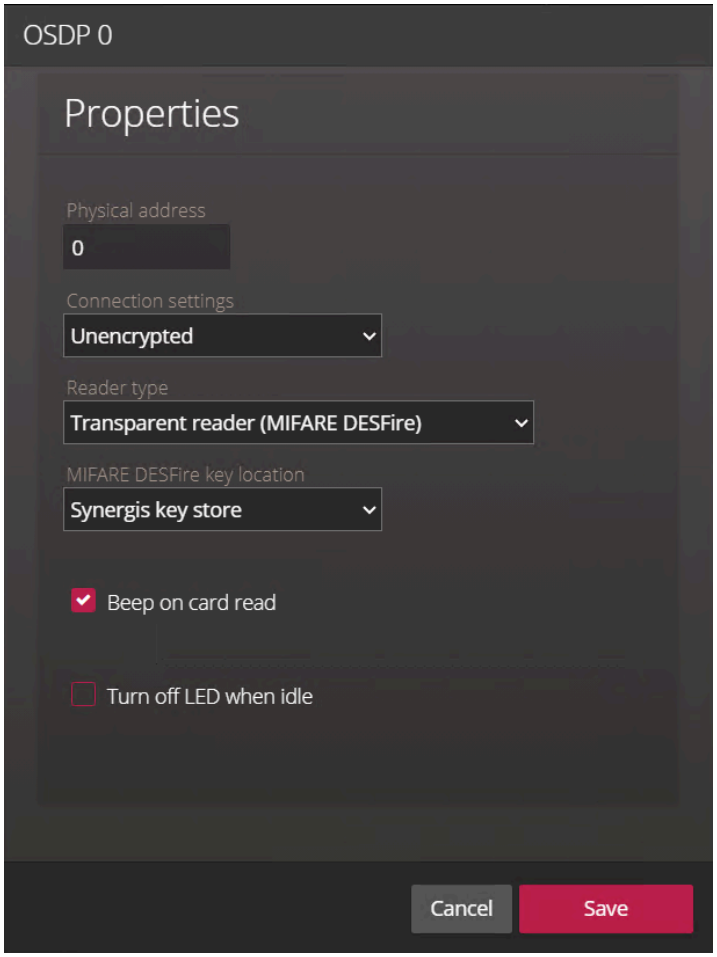
Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

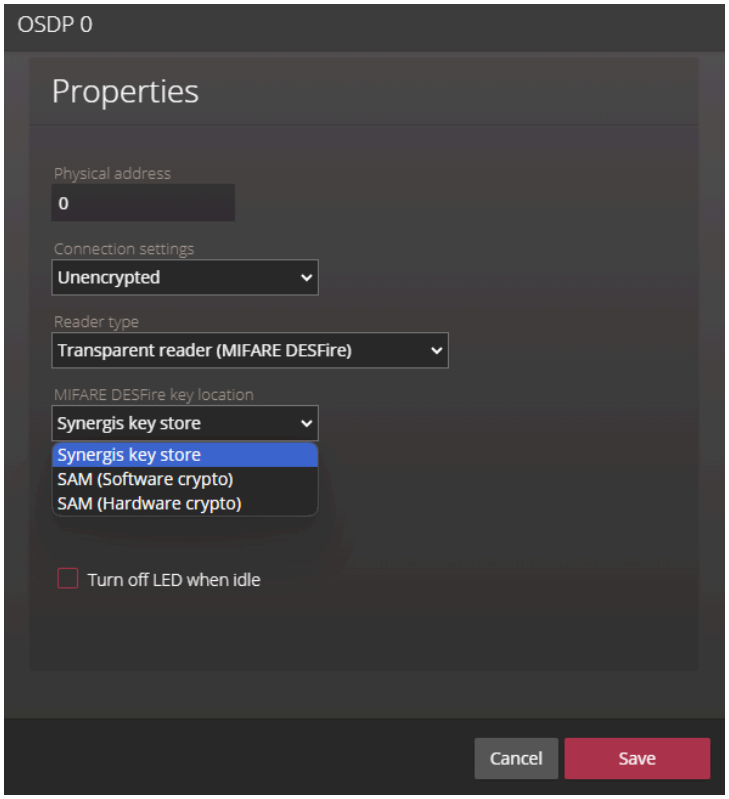
2 Cliquez sur **Configuration** > **Matériel** et sélectionnez un lecteur OSDP inscrit.

3 Cliquez sur **Modifier** ( ) sur l'interface du lecteur sélectionné.

4 Dans la liste **Type de lecteur**, sélectionnez **lecteur transparent MIFARE DESFire**.



5 Dans la liste **Emplacement des clés MIFARE DESFire**, sélectionnez un des éléments suivants :



- **Magasin de clés Synergis :** La clé pour déchiffrer les identifiants est stockée sur l'unité Synergis. Cette option ne nécessite pas de carte SAM.
- **SAM (cryptographie logicielle) :** Option SAM la plus rapide, mais qui nécessite l'activation de l'option **SessionDumpKey** durant le processus de configuration SAM. Pour en savoir plus, voir la documentation fournie avec le logiciel de configuration de votre carte SAM.
- **SAM (cryptographie matérielle) :** Cette option n'exige pas l'activation de **SessionDumpKey** durant le processus de configuration SAM.

REMARQUE : Les options SAM ne sont disponibles que si vous avez le modèle Synergis Cloud Link 312.

6 Cliquez sur **Enregistrer**.

7 Si vous sélectionnez l'option **Magasin de clés Synergis**, utilisez le Synergis[MC] Appliance Portal pour accéder au *Magasin de clés Synergis* et entrer les clés :

a. Sélectionnez un index.

b. Cliquez sur **Créer une nouvelle version**, puis entrez une clé hexadécimale de 32 caractères dans le champ texte.

c. Cliquez sur **Ajouter**.

Le fichier de configuration MIFARE DESFire utilisé pour les clés indexées est compatible avec les lecteurs transparents ou non pour le logiciel.

Limitation : Les lecteurs transparents pour les logiciels ont deux limitations :

- Les lecteurs transparents ne peuvent pas actuellement coder de cartes.
- Les cartes prennent environ 100 ms de plus à lire lorsque le mode transparent est activé.

Lorsque vous avez terminé

Configurez MIFARE DESFire.

Rubriques connexes

À propos de Synergis Cloud Link 312, page 6

Configuration des lecteurs OSDP pour prévenir les attaques par relais

Empêchez les attaques par relais sur les lecteurs OSDP pris en charge en configurant un délai maximum pour l'authentification de la carte.

À savoir

Lors d'une attaque par relais, le système prend plus de temps que la normale pour authentifier une carte, car les pirates doivent se transférer les messages. C'est la raison pour laquelle il est possible de prévenir efficacement les attaques par relais en fixant un délai maximum pour l'authentification des cartes. Lorsque le délai maximum est dépassé pendant la lecture d'une carte, l'unité Synergis[MC] Cloud Link ne prend pas de décision d'accès et la porte reste verrouillée.

REMARQUE : Aucun évènement *Accès refusé* n'est généré lorsque le délai maximum est dépassé.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **MIFARE DESFire**.

3 Dans la section *Lecteurs et configurations MIFARE DESFire*, sélectionnez l'option **Contrôle de proximité** à côté d'un ou plusieurs lecteurs OSDP.

4 Pour chaque lecteur avec **le contrôle de proximité**activé, entrez une valeur en millisecondes pour définir le délai maximum d'authentification de la carte dans le champ **ms**.

CONSEIL : La prévention des attaques par relais est activée pour chaque lecteur. Compte tenu de la variabilité des temps de lecture entre les lecteurs, il convient de déterminer le temps moyen nécessaire au lecteur pour authentifier un badge légitime et d'ajouter une petite marge d'erreur pour calculer le délai maximal. La marge d'erreur suggérée est de 40 millisecondes.

Pour déterminer le temps nécessaire à l'authentification d'une carte, cliquez sur **Visionneur de journaux** > **de maintenance**. Dans le menu déroulant **du journal**, sélectionnez **Syslog**, et entrez `SmartCard` dans le champ **Filtrer par expression régulière**. Pour l'heure d'authentification, vérifiez le préfixe *SmartCard* dans les journaux.

5 Cliquez sur **Enregistrer**.

Transférer des fichiers vers les lecteurs OSDP dans Synergis Appliance Portal

Vous pouvez mettre à niveau le micrologiciel ou la configuration des lecteurs OSDP en transférant des fichiers vers les lecteurs via le Synergis[MC] Appliance Portal.

À savoir

- La procédure suivante ne s'applique qu'aux lecteurs OSDP qui se connectent directement à l'unité Synergis[MC] Cloud Link.
- Utilisez les fichiers de micrologiciel et de configuration fournis par votre fabricant.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

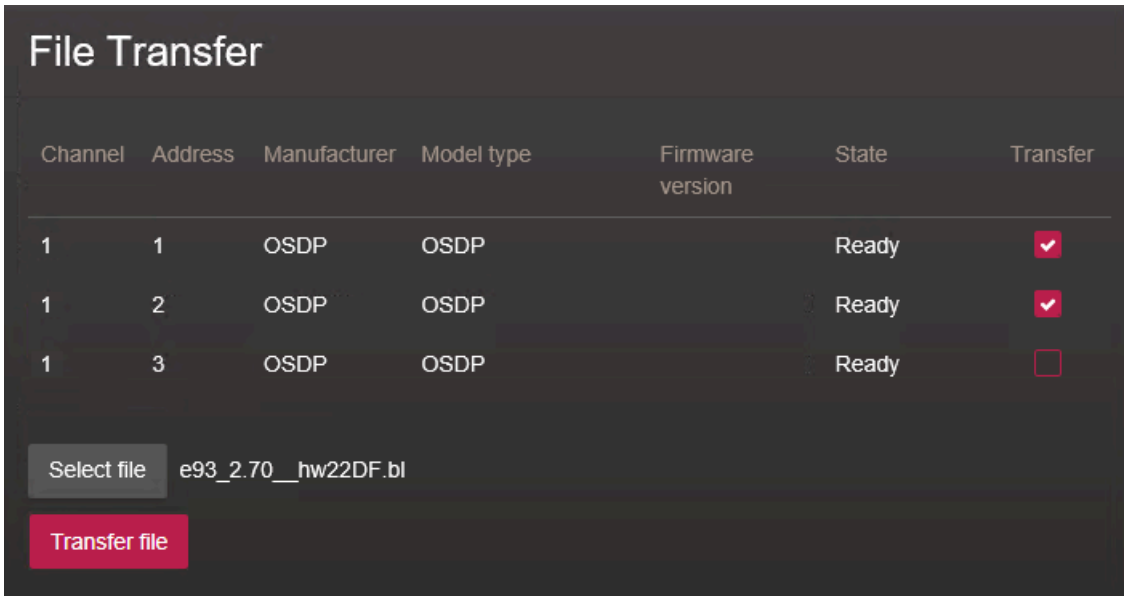
2 Cliquez sur **Configuration** > **OSDP avancé**.

3 Dans la section *Transfert de fichiers*, cochez la case de la colonne **Transférer** des lecteurs auxquels vous voulez transférer le fichier.

4 Cliquez sur **Sélectionner le fichier**.

5 Dans le navigateur de fichiers, sélectionnez le fichier de micrologiciel ou de configuration puis cliquez sur **Ouvrir**.

6 Cliquez sur **Transférer le fichier**.



Le micrologiciel ou la configuration est appliqué après le redémarrage des lecteurs sélectionnés.

17

Lecteurs STid à l’aide du protocole SSCP

Cette section aborde les sujets suivants:

Configurer et inscrire des lecteurs STid utilisant le protocole SSCP

Pour que l'unité Synergis[MC] puisse communiquer avec les lecteurs STid connectés, vous devez les configurer et les inscrire sur le Synergis[MC] Appliance Portal.

Avant de commencer

Vérifiez que le micrologiciel du lecteur STid est à jour et pris en charge par Synergis[MC] Softwire.

À savoir

Si vous installez des lecteurs STid sur des tourniquets adjacents, il est déconseillé de connecter plus de deux lecteurs à un même canal RS-485, car le délai de réponse du contrôleur sera plus long, et que les chances que deux cartes seront présentées en même temps sont élevées. Pour les portes ordinaires, vous pouvez installer jusqu'à quatre lecteurs par bus.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Matériel**.

3 En haut de la colonne **Matériel**, cliquez sur **Ajouter** ( ).

4 Dans la boîte de dialogue *Ajouter du matériel* , sélectionnez **SSCP** sous **Type de matériel**.

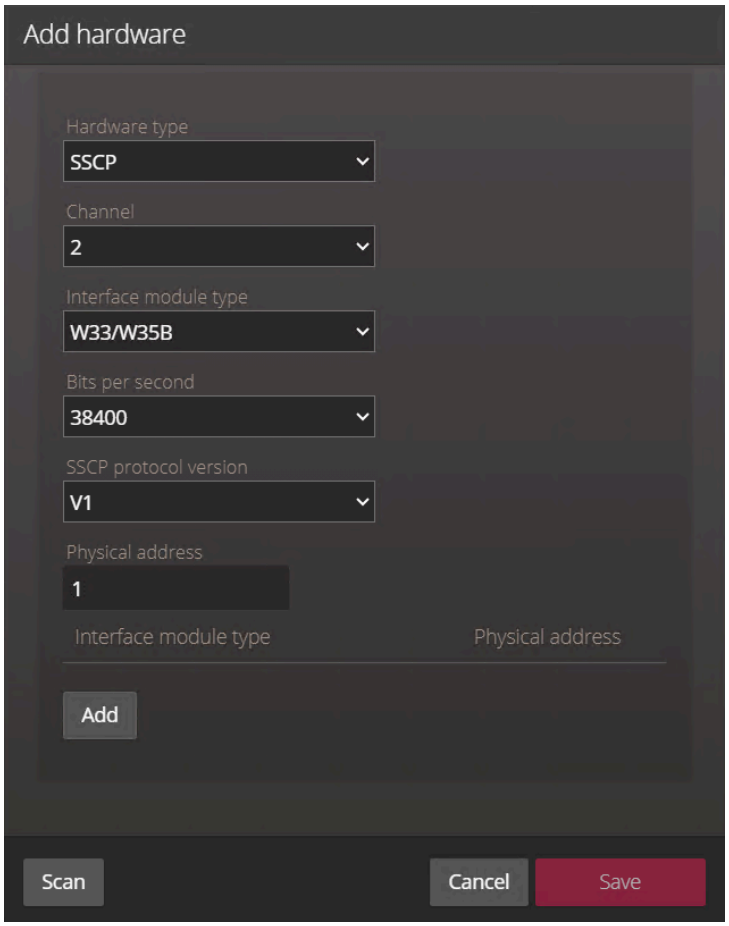
5 Sélectionnez le **Canal** (1 - 4) .

REMARQUE : Si vous avez l'unité Synergis Cloud Link 312, vous avez jusqu'à 12 canaux. Pour en savoir plus, voir À propos des ports RS-485 du Synergis Cloud Link.

6 Sous **Version du protocole SSCP**, sélectionnez **V1** ou **V2**, en fonction du protocole pris en charge par le lecteur.

7 Spécifiez les **Bits par seconde** et l'**Adresse physique** (de 1 à 127).

Le débit en **Bits par seconde** est une propriété du canal, qui est réglée sur le débit binaire du dernier module d'interface ajouté au canal. Le débit par défaut est de 38 400 bit/s. Un débit plus élevé améliore la vitesse de lecture des cartes aux dépens de la distance de câblage maximale.



8 Cliquez sur **Ajouter**.

Le port, le débit binaire et l'adresse physique du lecteur sont configurés dans Synergis Softwire.

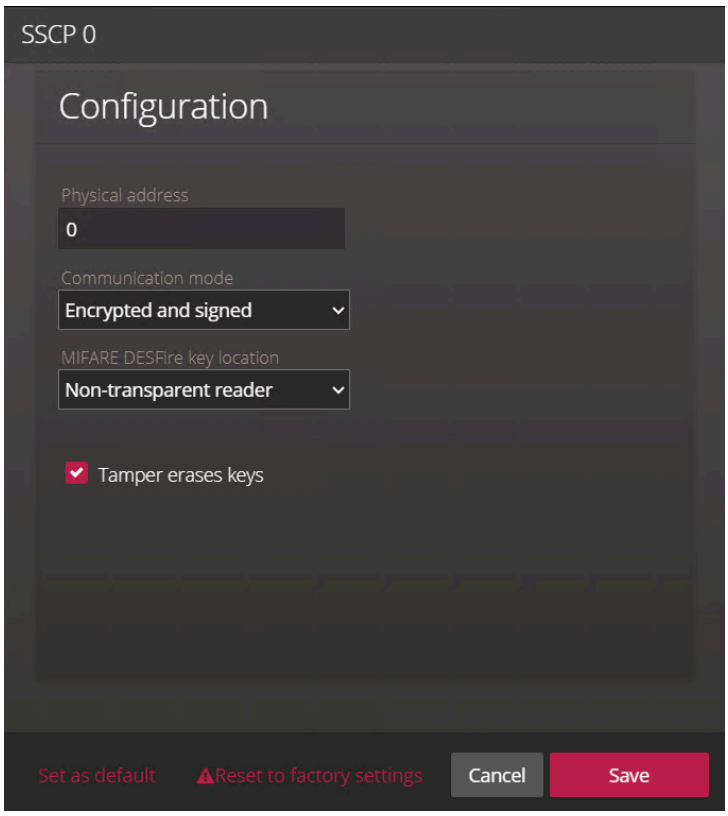
9 (Facultatif) Si vous utilisez le protocole version **V1**, sélectionnez un mode de communication :

a) Sélectionnez le lecteur à l'adresse que vous avez configuré et cliquez sur **Modifier** ( ).

b) Dans la liste **Mode de communication**, sélectionnez un mode :

- *Simple* (mode par défaut)
- *Chiffré* (communication privée)
- *Signé* (communication authentifiée)
- *Chiffré et signé* (communication privée et authentifiée)

REMARQUE : Si vous utilisez **V2**, alors seule l'option **Chiffré et signé** est disponible.



L'option **L'altération efface les clés** est active par défaut, et elle efface toutes les clés embarquées en cas d'altération de l'unité.

c) Cliquez sur **Enregistrer**.

10 Dans l'arborescence matérielle, sélectionnez l'interface que vous avez configurée et cliquez sur **Modifier** ( ).

11 Dans la boîte de dialogue qui apparaît, cochez la case **Mode programmation** et cliquez sur **Enregistrer**.

Le système programme le lecteur avec l'adresse physique et le débit binaire que vous avez configurés.

12 Sélectionnez l'interface et cliquez sur **Modifier** ( ).

13 Décochez la case **Mode programmation** et cliquez sur **Enregistrer**.

14 Répétez la procédure pour ajouter les lecteurs suivants, un lecteur à la fois et avec un lecteur par port.

REMARQUE : Si vous ajoutez plusieurs lecteurs à un port, utilisez un port libre pour les configurer individuellement avant de les connecter au port définitif.

15 Testez la connexion de votre module d'interface et votre configuration à partir de la page *Diagnostics d'E/S*.

Lorsque vous avez terminé

BONNE PRATIQUE : (*Renforcement*) Modifier les clés de chiffrement par défaut du fabricant renforce la sécurité.

Activer le mode transparent sur les lecteurs STid utilisant le protocole SSCP

Les lecteurs MIFARE DESFire utilisent des clés de chiffrement pour accéder aux identifiants sécurisés d’une carte. Lorsque les lecteurs sont configurés pour fonctionner en mode transparent, ces clés sont chargées dans le magasin de clés Synergis[MC] ou sur une carte SAM (Secure Access Module).

Avant de commencer

La porte doit être équipée d'un lecteur STid avec une référence se terminant par AA ou AD.

REMARQUE : Les lecteurs STid transparents avec une référence se terminant par BB ne peuvent pas être utilisés dans ce scénario. Pour une liste des lecteurs qui peuvent être utilisés comme lecteurs transparents, voir Lecteurs STid pris en charge qui utilisent le protocole SSCP.

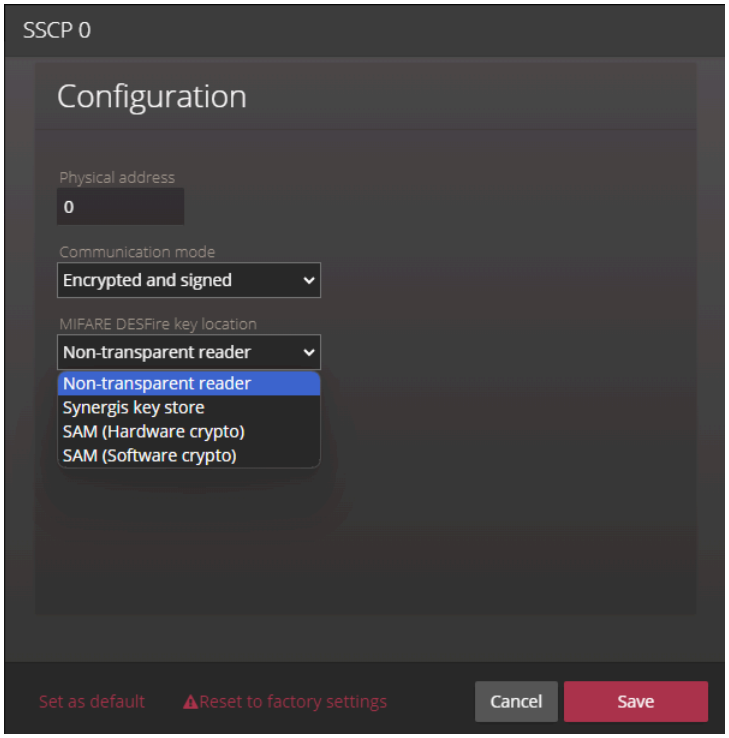
Procédure

1 Connectez-vous à l'unité Synergis[MC] Cloud Link.

2 Cliquez sur **Configuration** > **Matériel** puis sélectionnez **SSCP**.

3 Cliquez sur **Modifier** ( ) sur l’interface du lecteur.

4 Dans la boîte de dialogue de configuration du lecteur, sélectionnez un des éléments suivants dans la liste **Emplacement des clés MIFARE DEFire** :



- **Magasin de clés Synergis :** La clé pour déchiffrer les identifiants est stockée sur l'unité Synergis. Cette option ne nécessite pas de carte SAM.
- **SAM (cryptographie logicielle) :** Option SAM la plus rapide, mais qui nécessite l'activation de l'option **SessionDumpKey** durant le processus de configuration SAM. Pour en savoir plus, voir la documentation fournie avec le logiciel de configuration de votre carte SAM.
- **SAM (cryptographie matérielle) :** Cette option n'exige pas l'activation de **SessionDumpKey** durant le processus de configuration SAM.

REMARQUE : Les options SAM ne sont disponibles que si vous avez le modèle Synergis Cloud Link 312.

5 Si vous sélectionnez l'option **Magasin de clés Synergis**, utilisez le portail Synergis[MC] Appliance pour accéder au magasin de clés Synergis et entrez les clés :

a. Sélectionnez un index.
b. Cliquez sur **Créer une nouvelle version**, puis entrez une clé hexadécimale de 32 caractères dans le champ texte.
c. Cliquez sur **Ajouter**.

Le fichier de configuration MIFARE DESFire utilisé pour les clés indexées est compatible avec les lecteurs STid transparents ou non pour le logiciel.

Limitation : Les lecteurs transparents pour les logiciels ont deux limitations :

- Les lecteurs transparents ne peuvent pas actuellement coder de cartes.
- Les cartes prennent environ 100 ms de plus à lire lorsque le mode transparent est activé.

Lorsque vous avez terminé

Les 32 clés indexées dans le magasin de clés Synergis renforcent la sécurité en permettant de saisir des clés dans les composants. Cliquer sur **Ajouter** entre des composants permet de ne communiquer que la partie de la clé requise à chacun des intervenants.

Rubriques connexes

À propos de Synergis Cloud Link 312, page 6

Modifier les clés de communication RS-485 par défaut pour les lecteurs STid utilisant le protocole SSCP

Vous pouvez modifier les clés de signature et de chiffrement utilisées pour chiffrer et signer les échanges avec les lecteurs STid.

Avant de commencer

Modifiez les clés de *Signature* et de *chiffrement* par défaut des lecteurs STid pour une meilleure sécurité.

À savoir

Modifier les clés de signature et de chiffrement par défaut nécessite la modification des valeurs de clés RS-485 *ReaderKs* et *ReaderKc* sur le lecteur et sur la page *Magasin de clés Synergis* sur le Synergis^{MC} Appliance Portal. Le lecteur STid offre aussi la possibilité de stocker les clés sur l'un de ses index de clés embarqués.

Les lecteurs SSCP V2 n'utilisent que la clé *ReaderKc*.

REMARQUE : Si vous utilisez les clés indexées, en cas d'altération d'un lecteur STid, la porte bascule hors ligne dans Config Tool et le témoin LED du lecteur clignote en orange. Dans ce cas, présentez la carte SKB pour charger les clés RS-485 dans le lecteur. Une fois les clés chargées, le lecteur revient en ligne (le témoin DEL passe au rouge).

Procédure

1 Connectez-vous à l'unité Synergis.

2 Cliquez sur **Configuration** > **Magasin de clés Synergis**.

3 Appliquez les nouvelles valeurs de chiffrement, *ReaderKc* pour la clé de chiffrement et *ReaderKs* pour la clé de signature.

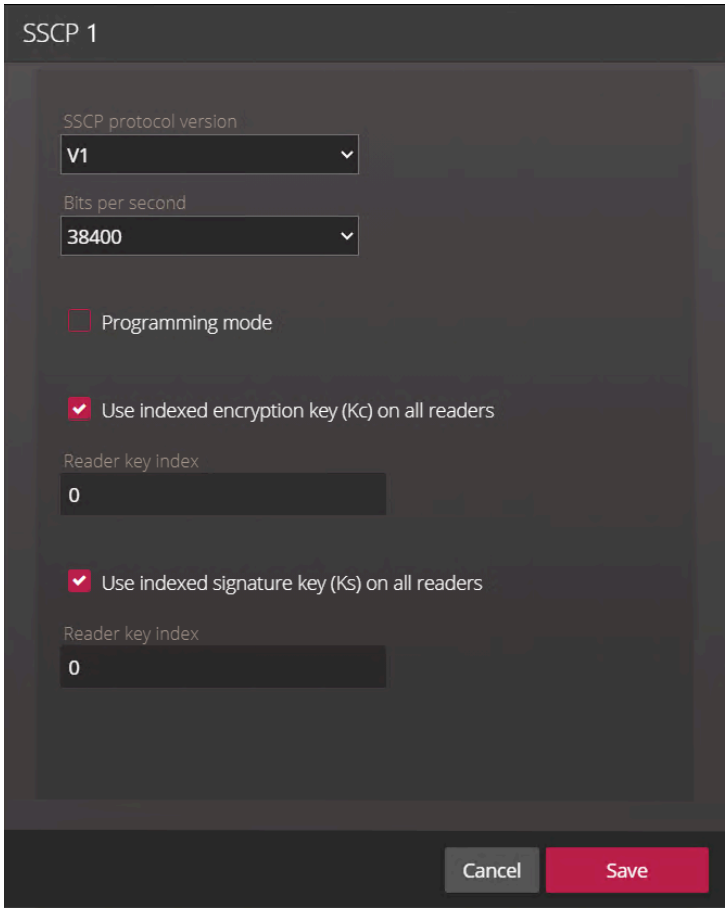
4 Configurez les clés :

   a) Cliquez sur **Configuration** > **Matériel** puis sélectionnez **SSCP**.

   b) Cliquez sur **Modifier** ( ) sur le canal du lecteur.

   c) Si les valeurs *ReaderKc* et *ReaderKs* ont été configurées sur le lecteur, ne cochez pas les options **Utiliser la clé (Kc) de chiffrement indexée sur tous les lecteurs** et **Utiliser la clé (Kc) de signature indexée sur tous les lecteurs**. Si le lecteur clé utilise des clés de signature et de chiffrement indexées, cochez

les options **Utiliser la clé (Kc) de chiffrement indexée sur tous les lecteurs** et **Utiliser la clé (Kc) de signature indexée sur tous les lecteurs**, et entrez les valeurs appropriées des index de clés.



5 Dans le cas de lecteurs qui utilisent des clés indexées, présentez la carte SKB pour charger les clés RS-485 sur le lecteur.

Configuration des lecteurs STid utilisant le protocole SSCP pour prévenir les attaques par relais

Prévenir les attaques par relais sur les lecteurs STid pris en charge en permettant au système de détecter les retards dans les échanges de communication RF entre les cartes et les lecteurs, et de rejeter les demandes d'accès provenant des cartes qui prennent trop de temps à communiquer.

Avant de commencer

- Cette procédure ne s'applique qu'aux lecteurs STid utilisant le protocole SSCP ou SSCP V2 et fonctionnant avec le micrologiciel v21 ou ultérieur.
- Activer la messagerie sécurisée DESFire EV2 :.

À savoir

Une attaque par relais utilise deux appareils malveillants pour transmettre les messages entre un lecteur et une carte, ce qui permet aux pirates de déverrouiller les portes sans que la carte ne soit physiquement près du lecteur. Dans de tels scénarios, le système prend plus de temps que la normale pour authentifier une carte, car les pirates doivent se transférer les messages.

L'activation d'un contrôle de proximité sur les lecteurs STid garantit que seules les demandes d'accès provenant de cartes qui se situent dans une plage horaire configurée sont autorisées.

Procédure

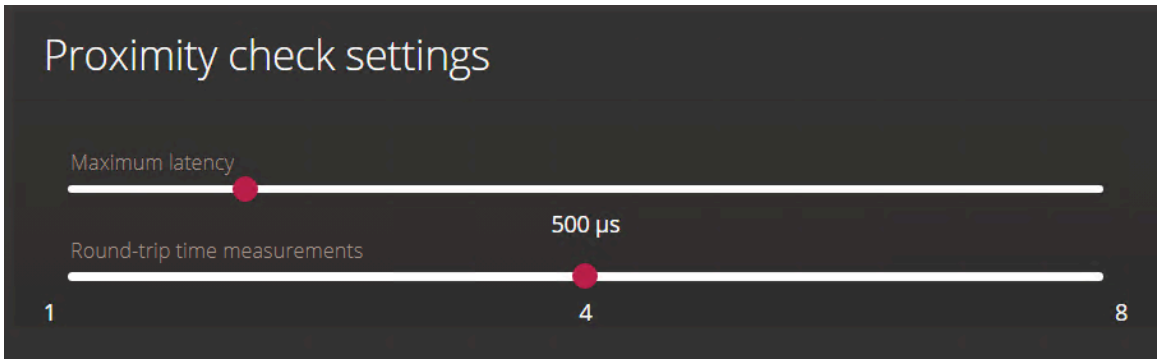
1 Connectez-vous à l'unité Synergis^{MC} Cloud Link .

2 Cliquez sur **Configuration** > **MIFARE DESFire**.

3 Dans la section *Lecteurs et configurations MIFARE DESFire associées*, sélectionnez l'option **Contrôle de proximité** à côté d'un ou plusieurs lecteurs STid.

4 (Facultatif) Dans la section *Réglages du contrôle de proximité*, configurez les réglages suivants :

REMARQUE : Il est conseillé de conserver les paramètres par défaut. L'abaissement de la latence maximale peut entraîner l'échec du contrôle de proximité pour certaines cartes. L'augmentation de la latence maximale peut accroître les chances de réussite d'une attaque par relais.



- **Latence maximale :** Le seuil en microsecondes d'un échange entre la carte et le lecteur. La valeur par défaut est de 500 microsecondes.
- **Mesures du délai aller-retour :** Le nombre d'échanges entre le lecteur et la carte utilisé pour calculer si la lecture de la carte est valide. Chaque échange ne doit pas dépasser la **latence maximale configurée**.

5 Cliquez sur **Enregistrer**.

Si les **Mesures du délai aller-retour** sont réglées sur quatre, lorsqu'un lecteur dont le réglage **Contrôle de proximité** est activé reçoit une demande d'accès, un contrôle de proximité est effectué, conformément à la configuration de la section *Réglages du contrôle de proximité*. Le contrôle de proximité calcule quatre fois la durée de l'échange entre la carte et le lecteur.

Le contrôle de proximité aboutit à l'un des résultats suivants :

- Si le temps calculé pour chacun des quatre échanges est compris dans la **latence maximale**, la carte réussit le contrôle de proximité. Synergis Cloud Link L'unité accorde ou refuse l'accès en fonction des droits d'accès de la carte, et la porte se déverrouille ou reste verrouillée en conséquence.
- Si au moins l'un des échanges prend plus de temps que la **latence maximale**, la carte échoue au contrôle de proximité. L'unité Synergis Cloud Link ne prend pas de décision d'accès et la porte reste verrouillée.

  REMARQUE : Aucun évènement *Accès refusé* n'est généré lorsqu'un contrôle de proximité échoue.

Codage d’un identifiant sur une carte RFID dans Security Desk

Vous pouvez coder un identifiant sur une carte RFID avec Security Desk.

À savoir

Les lecteurs-codeurs USB STid sont contrôlés par Security Desk. Pour en savoir plus, voir Activer les appareils de contrôle d'accès externes.

Partie IV

Maintenance et dépannage

Cette section comprend les chapitres suivants:

18

Maintenance et dépannage des unités Synergis Cloud Link

Cette section aborde les sujets suivants:

Affichage des informations du système sur l'unité Synergis Cloud Link

Vous pouvez afficher l'état de l'unité Synergis[MC] Cloud Link et des fichiers de configuration à des fins de dépannage.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Maintenance** > **État du système**.

3 Cliquez sur **Unité** pour afficher les informations sur le matériel et le micrologiciel de l'unité .

4 Cliquez sur **Réseau** pour afficher la configuration et l'état du réseau de l'unité .

Lorsque vous avez terminé

Téléchargez les fichiers de configuration de l'unité.

Informations sur votre unité Synergis Cloud Link

L'onglet *Unité* de la page *État du système* du Synergis[MC] Appliance Portal affiche des informations sur le matériel et le micrologiciel de l'unité Synergis[MC] Cloud Link.

Nom de la propriété	Valeur de la propriété
Nom d'hôte	Nom d'hôte de l'unité Synergis Cloud Link. Le nom d'hôte par défaut est constitué des lettres « SCL » suivies de l'adresse MAC de l'unité. L'adresse MAC est la première adresse sur l'étiquette collée sur l'unité. Par exemple, si l'étiquette indique 0010F32CF482, le nom d'hôte par défaut est SCL0010F32CF482.
Type de matériel	Appareil Genetec Synergis.
Type de produit	Synergis Cloud Link G2
Version du micrologiciel	La version du micrologiciel Synergis Cloud Link exécutée sur l'unité.
Version de Synergis Softwire	Version de Synergis Softwire incluse dans le micrologiciel de Synergis Cloud Link.
Date de publication	La date de publication du micrologiciel.
Date de mise à niveau	La date de mise à jour du micrologiciel vers la version actuelle.
RAM	La mémoire utilisée et la mémoire totale.
Stockage	Le stockage utilisé et le stockage total.
Température interne	La température interne de l'unité. Lorsque le seuil de température inférieur ou supérieur est franchi, cette valeur vire au rouge et un avertissement est affiché dans les notifications du portail. Pour en savoir plus, voir les spécifications sur Synergis Cloud Link.

Nom de la propriété	Valeur de la propriété
Tension de la batterie RTC	Le niveau de la batterie RTC en volts. Lorsque le seuil inférieur est franchi, un avertissement est affiché dans les notifications du portail et dans Security Center.
Source d'alimentation	La source d'alimentation de l'unité.
Environnement d'exécution	Version de la structure logicielle installée.
Port de découverte	Le port de découverte utilisé par les rôles Gestionnaire d'accès pour communiquer avec cette unité Synergis Cloud Link. **REMARQUE :** L'adresse IP du Gestionnaire d'accès doit également être connue de l'unité Synergis pour que les deux puissent communiquer.
Disponibilité du système	Temps écoulé depuis le dernier redémarrage matériel.
Disponibilité du service	Temps écoulé depuis le dernier redémarrage logiciel.
Gestionnaire d'accès actuellement connecté	Adresse IP du Gestionnaire d'accès qui contrôle cette unité.
Nombre d'événements hors ligne	Nombre d'événements consignés qui n'ont pas encore été synchronisés avec le rôle Gestionnaire d'accès lorsque l'unité est hors ligne. Affiche zéro quand l'unité est en ligne. **REMARQUE :** Il s'agit des événements génériques signalés au Gestionnaire d'accès. À ne pas confondre avec les journaux de dépannage propres à l'unité Synergis Cloud Link.
Nombre de canaux configurés	Nombre de canaux de communication configurés avec des modules d'interface. L'unité Synergis Cloud Link est dotée de deux types de canaux : IP et RS-485.
Numéro de série	Le numéro de série de l'unité.
Nombre de pairs connectés à cette unité	Nombre d'unités Synergis Cloud Link connectées à cette unité en tant que pairs.

Modification du mot de passe de connexion de l'appareil Synergis Cloud Link

Il est recommandé de modifier régulièrement le mot de passe de connexion de l'appareil Synergis[MC] Cloud Link.

À savoir

- Le nouveau mot de passe doit comporter au moins 15 caractères, être unique et aléatoire. Le bouton **Enregistrer** n'est affiché que lorsque le système estime que la fiabilité du mot de passe est *élevée* ou *très élevée*.
- Si l'appareil Synergis Cloud Link était déjà inscrit dans Security Center, il est recommandé de modifier le mot de passe à l'aide de la tâche *Inventaire matériel* de Config Tool au lieu de Synergis[MC] Appliance Portal. Security Center 5.10.1 est la version minimale requise pour ce faire.

  Pour en savoir plus, voir Modifier les mots de passe des unités de contrôle d'accès dans Config Tool.

Procédure

1 Connectez-vous à l'appareil Synergis Cloud Link.

2 Cliquez sur **Configuration** > **Utilisateurs**.

3 Sur la page *Utilisateurs*, sélectionnez un utilisateur.

4 Entrez l'ancien mot de passe, puis entrez et confirmez le nouveau mot de passe.

5 Cliquez sur **Enregistrer**.

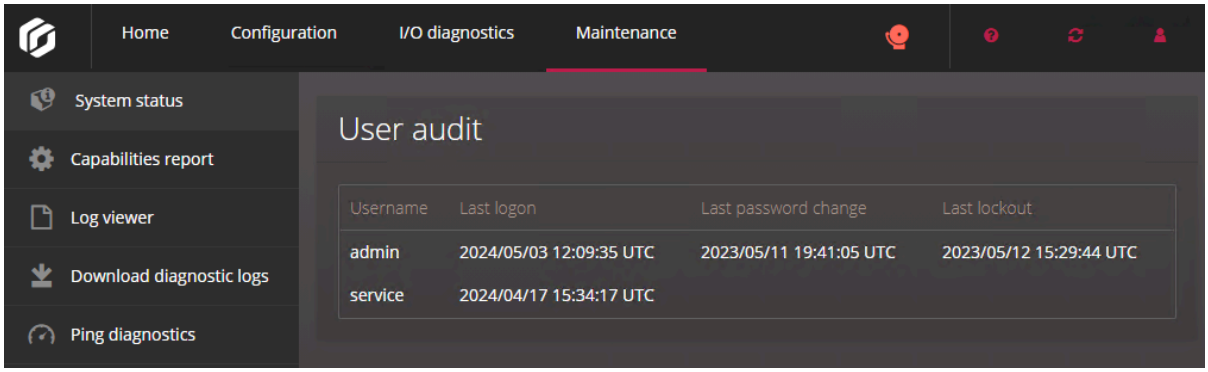
6 Pour les appareils déjà inscrits dans Security Center, modifiez le mot de passe dans Config Tool pour synchroniser l'appareil avec le rôle Gestionnaire d'accès auquel il est connecté.

Le nouveau mot de passe est immédiatement appliqué.

Audits utilisateur Synergis Cloud Link

Pour examiner l'activité des utilisateurs dans Synergis[MC] Appliance Portal , vous pouvez voir quand les utilisateurs se sont connectés à l'unité Synergis[MC] Cloud Link quand ils ont modifié leur mot de passe et quand ils ont été bloqués après trois tentatives de connexion infructueuses.

Allez dans **Maintenance** > **État du système** pour trouver la section *Audits des utilisateurs*. L'horodatage de toutes les activités des utilisateurs est en UTC.



Télécharger le fichier de configuration de votre unité Synergis Cloud Link

Vous pouvez télécharger la configuration de votre unité Synergis[MC] Cloud Link sous forme de fichier compressé pour restaurer la configuration sur une autre unité lors d'un remplacement d'unité.

À savoir

Le fichier de configuration contient des réglages matériels, comme le RIO et les valeurs d'entrées supervisées, ainsi que les règles d'automation engine. Le fichier n'intègre pas les réglages réseau de l'unité, le mot de passe administrateur ni les données de magasin de clés Synergis.

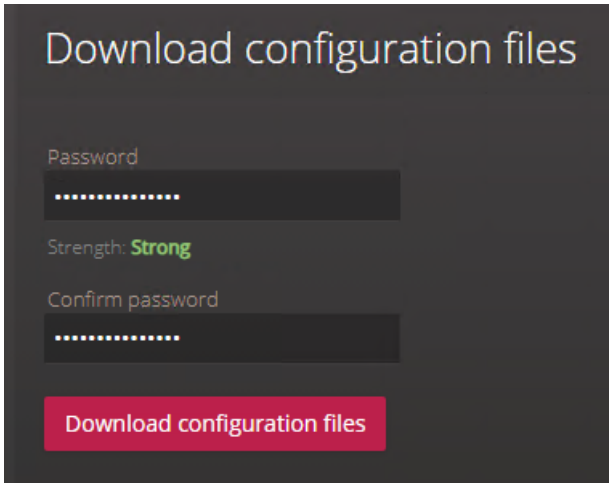
Procédure

1 Connectez-vous à l'unité Synergis Cloud Link.

2 Cliquez sur **Maintenance** > **État du système**.

3 Dans la section *Télécharger les fichiers de configuration*, entrez un mot de passe fiable et confirmez-le.

REMARQUE : Le mot de passe doit comprendre au moins 15 caractères.



4 Cliquez sur **Télécharger les fichiers de configuration**.

REMARQUE : Ce bouton reste grisé si le mot de passe n'est pas assez fiable ou si la confirmation ne concorde pas.

5 Cliquez sur **Enregistrer**.

Transfert du fichier de configuration de votre unité Synergis Cloud Link

Lorsque vous remplacez une unité Synergis[MC] Cloud Link, vous pouvez télécharger les fichiers de configuration de l'ancienne unité, puis les charger sur l'unité de remplacement pour restaurer la configuration.

Avant de commencer

Téléchargez le fichier de configuration de l'unité Synergis Cloud Link.

À savoir

Le fichier de configuration contient des réglages matériels, comme le RIO et les valeurs d'entrées supervisées, ainsi que les règles d'automation engine. Le fichier n'intègre pas les réglages réseau de l'unité, le mot de passe administrateur ni les données de magasin de clés Synergis.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link de remplacement.

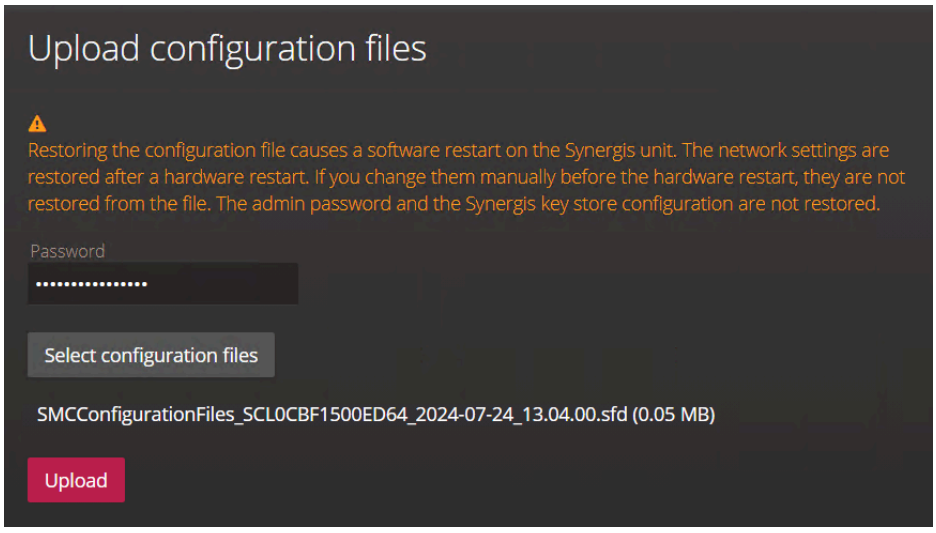
2 Cliquez sur **Maintenance** > **État du système**.

3 Dans la section *Transférer les fichiers de configuration*, cliquez sur **Sélectionner les fichiers de configuration**.

4 Naviguez jusqu'au pack de configuration téléchargé sur votre disque local et cliquez sur **Ouvrir**.

5 Si vous avez défini un mot de passe lorsque vous avez téléchargé les fichiers de configuration, entrez-le dans le champ **Mot de passe**.

6 Cliquez sur **Transférer**.



Le pack de configuration est transféré et l'unité Synergis Cloud Link redémarre.

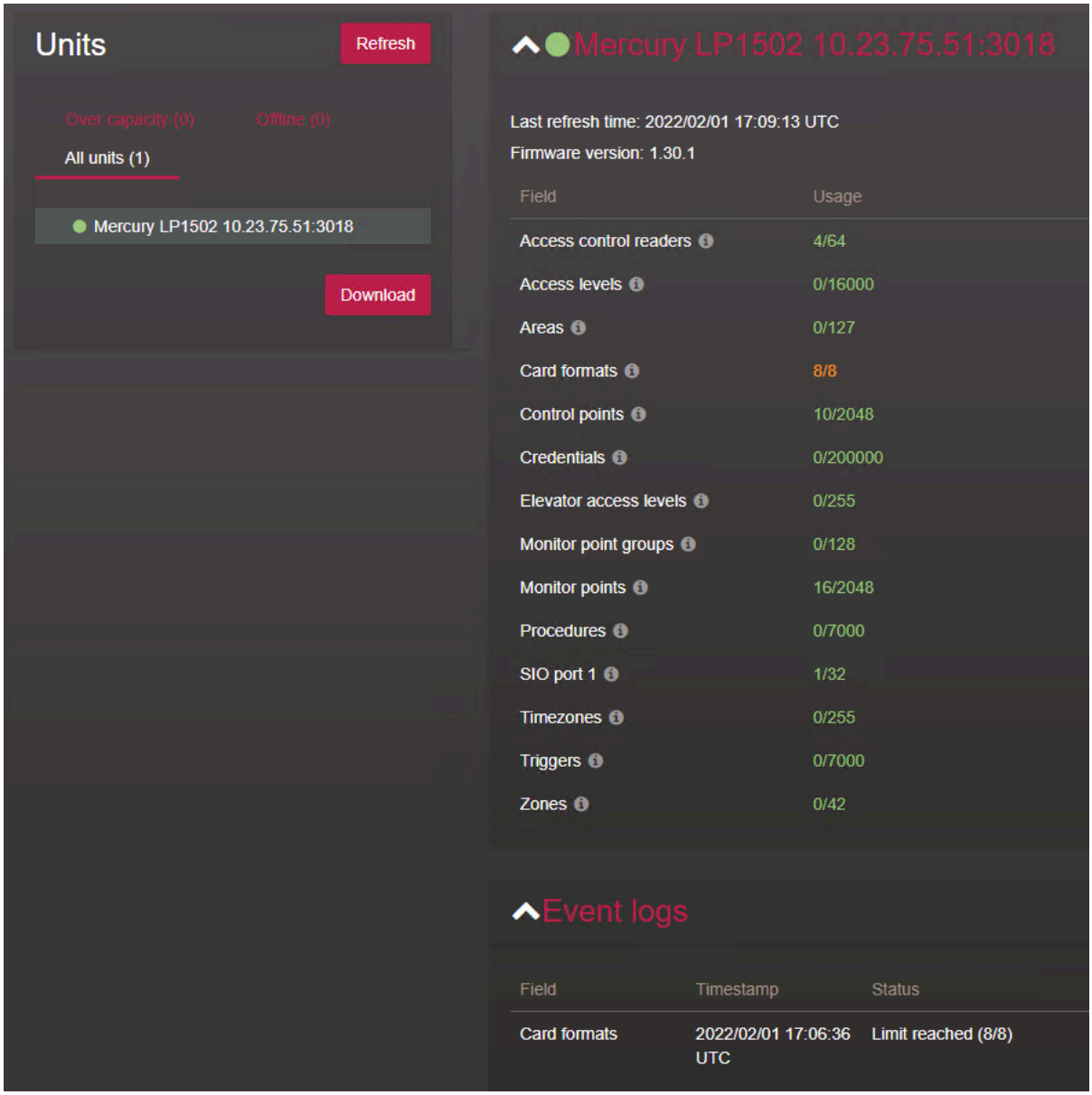
Lorsque vous avez terminé

- Reconfigurer manuellement le mot de passe de l'administrateur et la configuration du magasin de clés Synergis car ils ne sont pas inclus dans le fichier de configuration.

- Pour restaurer les paramètres réseau à partir du fichier de configuration, redémarrez le matériel.

À propos de la page Rapport de capacité

Pour simplifier le dépannage des contrôleurs Mercury inscrits dans votre système, vous pouvez consulter la page *Rapport de capacité* sur le Synergis[MC] Appliance Portal. Cette page présente l'état, les fonctionnalités utilisées et les journaux des événements de chacun de vos contrôleurs.



Seuls les utilisateurs dotés des droits d'administrateur peuvent accéder au *Rapport de capacité*. La page est divisée en plusieurs sections :

- **Unités :** Dresse la liste de tous les contrôleurs Mercury inscrits sur l'unité Synergis[MC] Cloud Link. Cette section doit être actualisée manuellement. Trois vues différentes sont disponibles pour afficher les contrôleurs :
  - Capacité dépassée
  - Hors ligne
  - Toutes les unités

Sélectionnez une unité pour afficher les sections Capacité et *Journaux des événements* correspondantes. Cliquez sur **Télécharger** pour générer un fichier CSV contenant les unités et leur capacité actuelle.

- **Section Capacité pour l'unité sélectionnée. :** Cette section est nommée d'après l'unité sélectionnée dans la section *Unités*. Elle contient les informations suivantes :
  - **Dernière actualisation :** L'horodatage de la dernière récupération des données.
  - **Version du micrologiciel :** La version du micrologiciel de l'unité.
  - **Capacité :** Tableau des fonctionnalités prises en charge par l'unité, et l'utilisation actuelle de chaque fonctionnalité. Par exemple, *2/64* dans la ligne *Lecteurs de contrôle d'accès* indique que l'unité peut encore accepter 62 lecteurs supplémentaires. Survolez l'icône ℹ en regard de chaque fonctionnalité pour afficher les concepts Security Center équivalents.
    Les valeurs de capacité utilisent le code couleur suivant :
    - Le rouge indique que la capacité est dépassée.
      REMARQUE : Si une réinitialisation matérielle se produit alors que les capacités sont dépassées, la fonctionnalité de porte hors ligne et les lectures OSDP ne fonctionnent pas tant que les capacités sont dépassées.
    - L'orange indique que la capacité est atteinte.
    - Le vert indique qu'il reste de la capacité.
- **Journaux des événements :** Affiche les 10 derniers événements critiques pour l'unité sélectionnée depuis le dernier démarrage du micrologiciel, comme des événements de capacité atteinte ou dépassée.

Télécharger les informations d'assistance pour votre unité Synergis Cloud Link

Pour simplifier le dépannage de votre unité Synergis[MC] Cloud Link , vous pouvez télécharger un fichier unique qui contient toutes les informations sur le Synergis[MC] Appliance Portal dont l'assistance technique Genetec[MC] aura besoin.

À savoir

Le fichier d'ingénierie est un fichier .gen chiffré qui ne peut être déchiffré que par l'assistance technique Genetec. Le fichier d'archive contient tous les journaux ainsi qu'une sauvegarde de la configuration de l'unité.

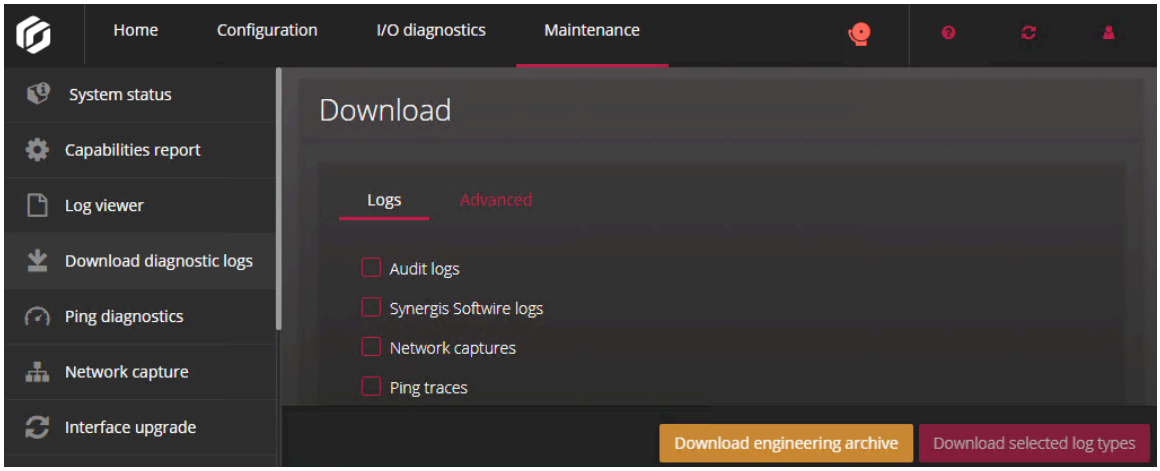
Procédure

1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Maintenance** > **Télécharger les journaux de diagnostic**.

3 Procédez de l'une des manières suivantes :

- Cliquez sur **Télécharger l'archive d'ingénierie**.
- Dans la section *Journaux*, sélectionnez les catégories de journaux à télécharger, puis cliquez sur sur **Télécharger les types de journaux sélectionnés**.
- Cliquez sur l'onglet **Avancé**, développez les catégories, sélectionnez les journaux particuliers à télécharger, puis cliquez sur **Télécharger les fichiers journaux sélectionnés**.



Le fichier est téléchargé.

4 Enregistrez le fichier à envoyer à l'assistance technique Genetec.

Ping des modules d'interface depuis le Synergis Appliance Portal

Vous pouvez effectuer un ping des modules d'interface et de leurs interfaces descendantes depuis le Synergis[MC] Appliance Portal pour vérifier si l'installation de votre unité a réussi, ainsi que pour résoudre des problèmes réseau ou de perte de paquets.

À savoir

- Vous pouvez effectuer deux types de ping depuis le portail :
  - **Ping court :** Prend moins de 10 secondes. Les résultats sont affichés sous l'appareil sélectionné.
  - **Ping à long terme :** Effectue un ping toutes les secondes pendant la durée sélectionnée. Il est possible d'effectuer des pings sur plusieurs modules d'interface à la fois. Un fichier tar.gz contenant le résultat du ping peut être téléchargé sur la page *Télécharger les journaux de diagnostic* du portail.
- Vous ne pouvez pas faire un ping des unités ASSA ABLOY et RIO.
- Les unités Synergis[MC] IX nécessitent le micrologiciel 4.00_1143_M036 ou version ultérieure pour pouvoir faire l'objet d'une requête ping.
- Il se peut que le ping ne fonctionne pas, selon les paramètres de votre pare-feu.

Procédure

1 Connectez-vous à l'unité Synergis[MC] Cloud Link.

2 Cliquez sur **Maintenance** > **Diagnostic ping**.

La liste de tous les modules d'interface et de toutes les interfaces descendantes connectés à votre unité Synergis Cloud Link s'affichent.

3 Démarrer le ping :

- Pour un ping court : sélectionnez un module d'interface et cliquez sur **Ping**.
- Pour un ping long : sélectionnez un ou plusieurs modules d'interface, puis une **Durée de ping long**, puis cliquez sur **Démarrer le ping**.

Les résultats du ping court sont répertoriés sous le module d'interface soumis au ping. Les résultats du ping sur la durée sont disponibles sur la page *Télécharger les journaux de diagnostic*.

Mettre à niveau le micrologiciel Synergis Cloud Link

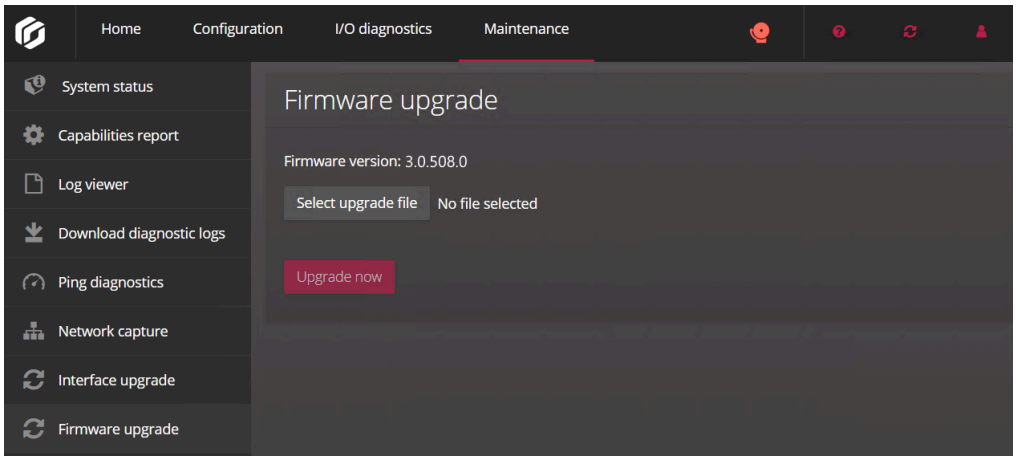
Pour bénéficier des derniers correctifs de sécurité et améliorations, veillez à garder votre unité Synergis[MC] Cloud Link à jour en installant la dernière version du micrologiciel.

Procédure

1 Téléchargez le dernier micrologiciel depuis la page *Téléchargement de produits* de GTAP.
   a) Dans la liste **Download Finder**, sélectionnez **Synergis[MC] Cloud Link**, puis recherchez votre micrologiciel.
   b) Enregistrez le fichier *.sfw* sur votre lecteur local.

2 Connectez-vous à l'unité Synergis Cloud Link.

3 Cliquez sur **Maintenance** > **Mettre à niveau le micrologiciel**.



4 Cliquez sur **Select upgrade file** (Sélectionner le fichier de mise à niveau).

5 Dans le navigateur de fichiers qui s'ouvre, sélectionnez le fichier de micrologiciel *.sfw*, puis cliquez sur **Ouvrir**.

6 Cliquez sur **Mettre à niveau**.

La mise à niveau peut prendre plusieurs minutes, après quoi l'unité redémarre.

Revenir en arrière après la mise à niveau du micrologiciel de l’unité Synergis Cloud Link

Après la mise à niveau du micrologiciel Synergis[MC] Cloud Link , vous disposez de sept jours pour annuler la mise à niveau sur le Synergis[MC] Appliance Portal .

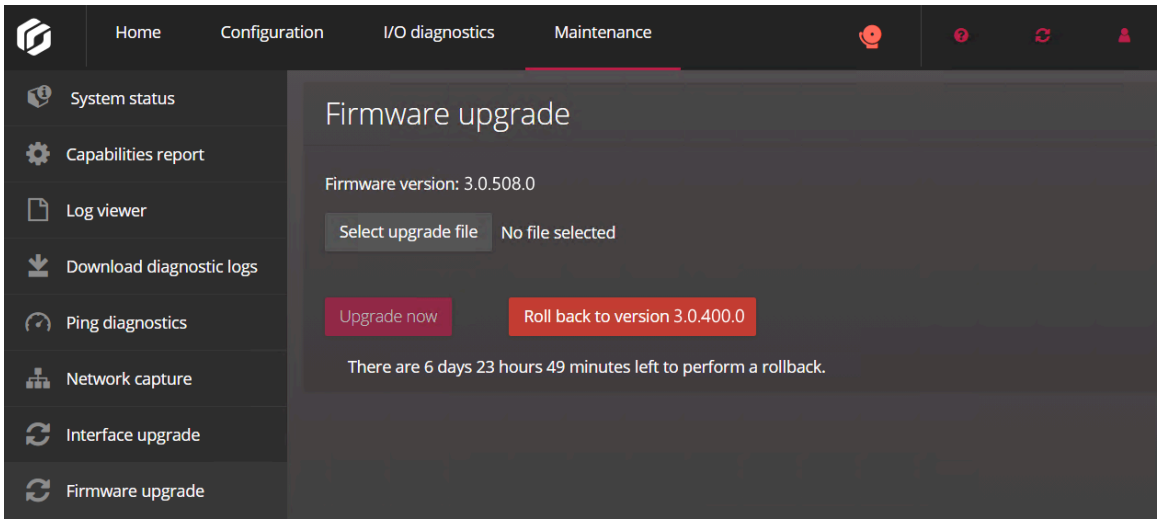
À savoir

- L'annulation rétablit l’état de l'unité avant la dernière mise à niveau. Le micrologiciel ainsi que toute modification de la configuration effectuée après la mise à niveau sont annulés.
- Le bouton **Revenir à la version X.Y.Z** n’est pas affiché dans les cas suivants :
  - Sept jours se sont écoulés depuis la mise à niveau.
  - Espace insuffisant sur l’unité pour enregistrer la sauvegarde temporaire après la mise à niveau.
  - Vous avez déjà annulé la mise à niveau.

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Maintenance** > **Mettre à niveau le micrologiciel**.



3 Cliquez sur **Revenir à la version X.Y.Z**.

Une boîte de dialogue affiche le message suivant : *L'état de la configuration avant la dernière mise à niveau sera rétabli*.

4 Cliquez sur **OK**.

L'unité redémarre. Une fois le rétablissement terminé, le message suivant est affiché : *Rétablissement terminé avec succès. La page sera actualisée automatiquement lorsque l’unité sera disponible.*

Mise à niveau du micrologiciel du module d’interface via Synergis Appliance Portal

Les unités Synergis[MC] Cloud Link fonctionnent de manière optimale lorsque tous les modules d'interface connectés sont dotés du micrologiciel recommandé. Les versions du micrologiciel recommandées sont certifiées par Genetec Inc.

Avant de commencer

- Il est recommandé de mettre à jour le micrologiciel des modules d’interface à l’aide de la tâche *Inventaire matériel* dans Config Tool plutôt que sur le Synergis[MC] Appliance Portal, car vous pouvez effectuer les opérations suivantes dans la tâche *Inventaire matériel* :
  - Mettre à niveau les modules d’interface individuellement ou par lots.
  - Programmer les mises à niveau et configurer la notification par e-mail en cas d’échec.
  - Afficher la progression des mises à niveau et le micrologiciel installé sur chaque module d’interface.
  - Mettre à niveau les interfaces et les modules Mercury SIO.

  Pour en savoir plus, voir Mettre à niveau la plate-forme et le micrologiciel des unités de contrôle d'accès et le micrologiciel des modules d'interface.
- Si vous décidez d’effectuer la mise à niveau via Synergis Appliance Portal, vérifiez que votre module d’interface le permet.

À savoir

Si les versions du micrologiciel de vos modules d'interface sont plus récentes que les versions recommandées, elles sont rétrogradées, sauf pour les verrous IP ASSA ABLOY.

Procédure

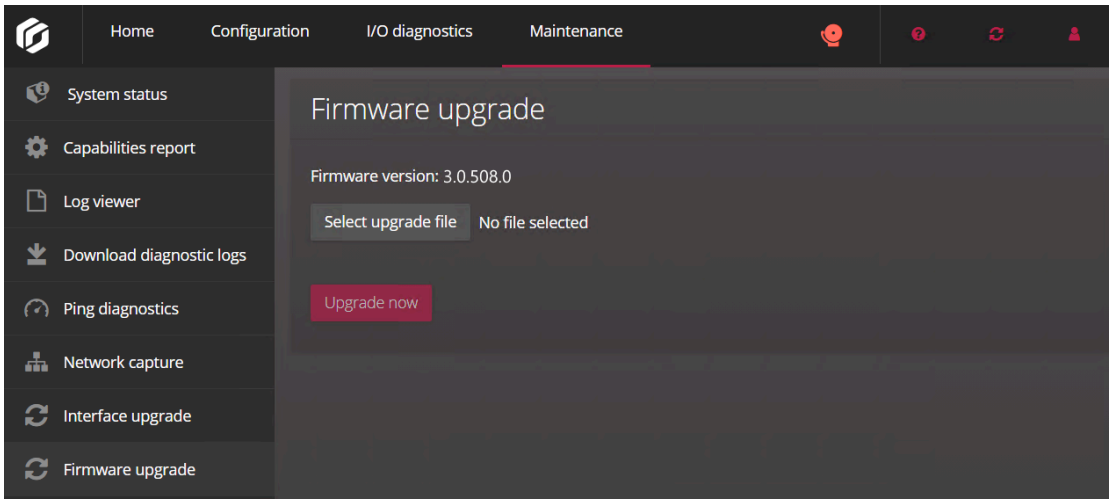
1 Téléchargez le micrologiciel sur l'unité Synergis Cloud Link :

a) Sur la page *Téléchargements de produits* de GTAP, sélectionnez **Synergis^{MC} Cloud Link** dans la liste **Download Finder**, puis recherchez le micrologiciel de votre module d'interface.

b) Enregistrez le fichier *.sfw* sur votre lecteur local.

c) Connectez-vous à l'unité Synergis Cloud Link.

d) Cliquez sur **Maintenance** > **Mettre à niveau le micrologiciel**.



e) Cliquez sur **Select upgrade file** (Sélectionner le fichier de mise à niveau).

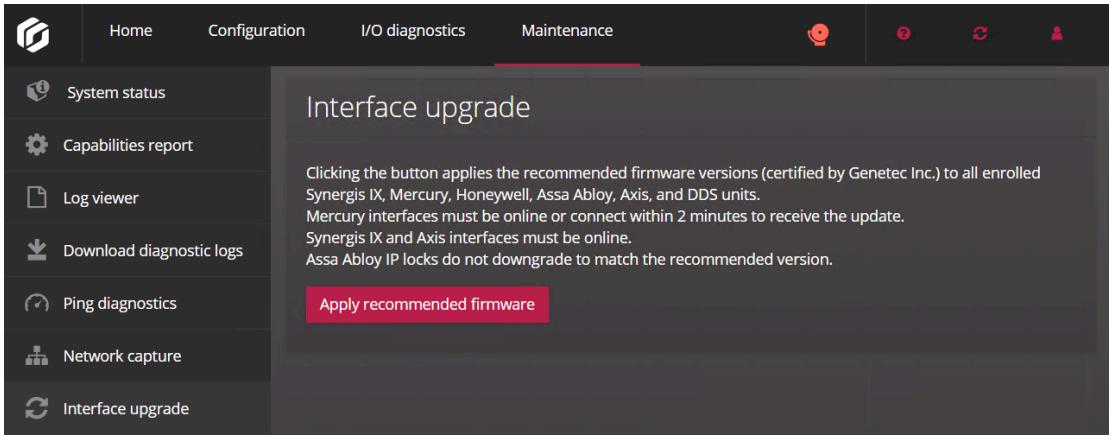
f) Dans le navigateur de fichiers qui s'ouvre, sélectionnez le fichier de micrologiciel *.sfw*, puis cliquez sur **Ouvrir**.

g) Cliquez sur **Mettre à niveau**.

Le micrologiciel est téléchargé sur l'unité Synergis Cloud Link.

2 Envoyer le micrologiciel aux modules d'interface :

a) Cliquez sur**Maintenance** > **Mettre à niveau le micrologiciel**.



b) Cliquez sur **Appliquer un micrologiciel recommandé**.

Le message de confirmation suivant s'affiche : *Mise à niveau terminée avec succès*.

Appareils en aval pris en charge pour la mise à niveau via Synergis Appliance Portal

Vous pouvez mettre à niveau le micrologiciel d'appareils spécifiques dans le Synergis[MC] Appliance Portal. Pour les fabricants qui ne sont pas pris en charge, vous devrez parfois utiliser le logiciel du fabricant pour appliquer le micrologiciel recommandé.

Les appareils suivants peuvent être mis à niveau dans Synergis Appliance Portal :

- **Mercury :**
  - EP1501, EP1502, EP2500, EP4502
  - LP1501, LP1502, LP2500, LP4502
  - MP1502, MP4502
  - M5-IC
  - MS-ICS
- **Honeywell :**
  - PRO32IC
  - PRO42IC
  - PW6K1IC
  - PW7K1IC
- **ASSA ABLOY :**
  - Ensembles de verrous IP Corbin Russwin et SARGENT (contrôleurs CX, PoE et Wi-Fi)
- **Axis :**
  - A1001
  - A1601
- **DDS :**
  - TPL
  - JET
- **Lecteurs OSDP :**
  - Deister
  - WaveLynx
- **Contrôleurs Synergis[MC] IX :**
  - SY-SIX-CTRL-DIN
  - SY-SIX-CTRL-DIN-1D

Nettoyer le stockage sur l’appareil Synergis Cloud Link .

Vérifiez que vous disposez de suffisamment d’espace sur votre appareil Synergis[MC] Cloud Link avant d'installer des mises à jour ou un nouveau micrologiciel. Vous pouvez consulter l’espace disponible et effectuer un nettoyage de votre appareil depuis la page *Stockage* du Synergis[MC] Appliance Portal .

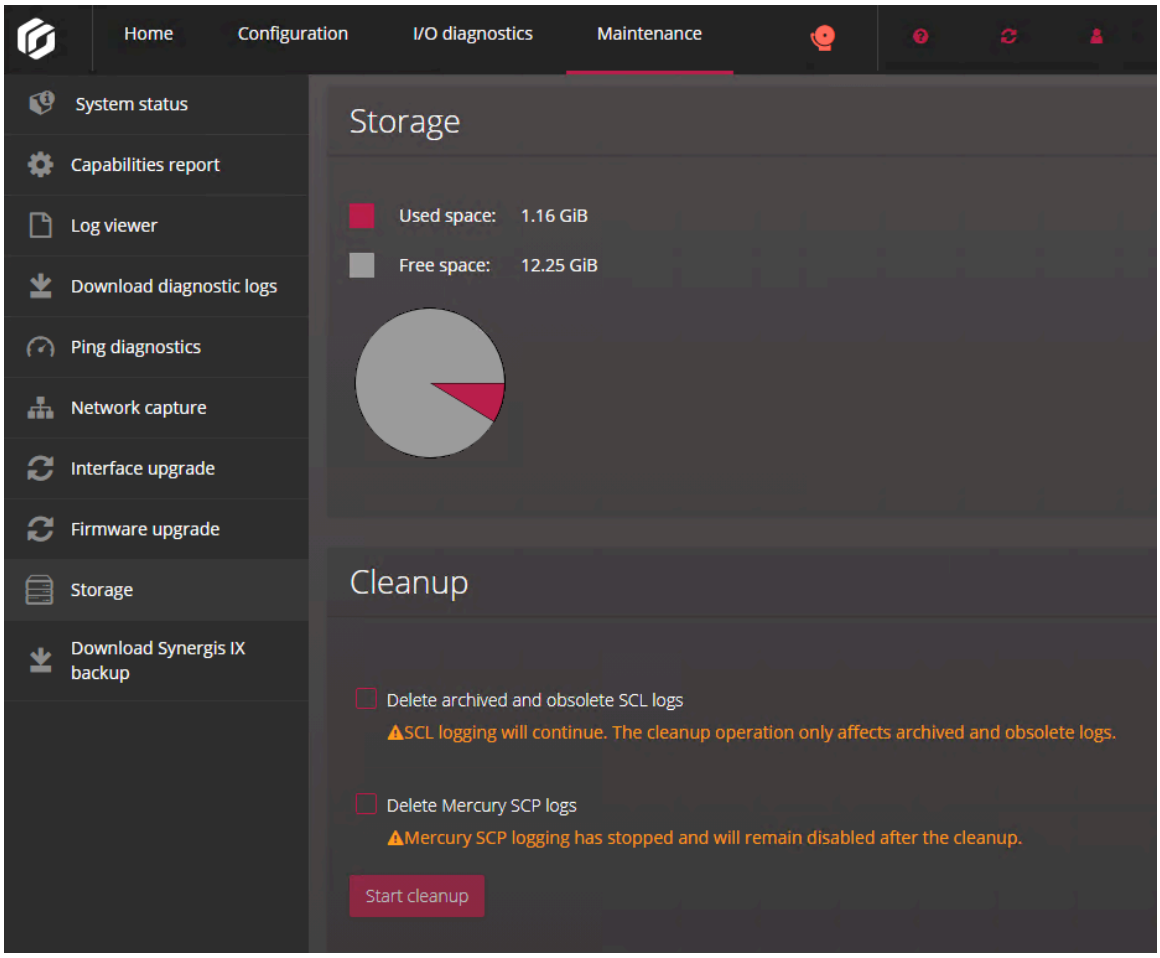
À savoir

IMPORTANT : Lorsqu’un nettoyage est en cours, la mise à jour du micrologiciel et le redémarrage du système sont bloqués sur l’appareil Synergis Cloud Link .

Procédure

1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Maintenance** > **Stockage**.



3 Sélectionnez l'une des options suivantes :

- **Supprimer les journaux archivés et obsolètes :** Lorsque vous lancez ce nettoyage, les journaux Synergis Softwire archivés et obsolètes sont supprimés.
- **Supprimer les journaux Mercury SCP :** Lorsque vous lancez ce nettoyage, tous les journaux Mercury SCP archivés sont supprimés.

4 Cliquez sur **Démarrer le nettoyage**.

Afficher les informations pair-à-pair d'une unité Synergis Cloud Link

Pour résoudre les problèmes liés aux unités connectées en tant que pairs à l'unité Synergis[MC] Cloud Link et vérifier qu'elles peuvent toutes communiquer entre elles, vous pouvez afficher leur état et d'autres informations les concernant depuis Synergis[MC] Appliance Portal .

À savoir

- Lorsque l'option **Activer le pair-à-pair** est désactivée sur la page *Propriétés* du rôle Gestionnaire d'accès dans Config Tool, la ligne *Nombre de pairs connectés* et la page *Pair-à-pair* ne sont pas affichées dans le Synergis Appliance Portal .
- Pour que deux unités soient connectées en tant que pairs, elles doivent appartenir au même groupe de pairs. Jusqu'à 15 unités peuvent appartenir au même groupe. Pour en savoir plus, voir Activer le pair-à-pair sur le rôle Gestionnaire d'accès.
- Pour que les informations d'antiretour global restent fiables (titulaires ayant accès à quels secteurs), au moins une unité doit toujours être alimentée. Ces informations ne sont stockées nulle part, ce qui signifie que si toutes les unités sont désactivées, elles seront perdues.
- Les unités inscrites sur un rôle Gestionnaire d'accès hébergé doivent utiliser le **DHCP** ou le **DHCP avec IP statique** pour que le pair-à-pair puisse fonctionner. Les unités qui utilisent une **IP statique** ne peuvent pas communiquer entre elles. Vous pouvez configurer les réglages réseau en allant dans **Configuration** > **Réseau** dans le Synergis Appliance Portal .

Procédure

Pour afficher le nombre de pairs connectés à l'unité Synergis Cloud Link :

1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Maintenance** > **État du système**.

3 Cliquez sur **Unité**.

Dans la ligne *Nombre de pairs connectés*, le nombre de pairs en ligne par rapport au nombre total de pairs est répertorié. Par exemple, *10/12* indique qu'il y a 12 unités autres que la vôtre sous le même rôle Gestionnaire d'accès, mais qu'il n’y en a que 10 qui sont connectées à votre unité.

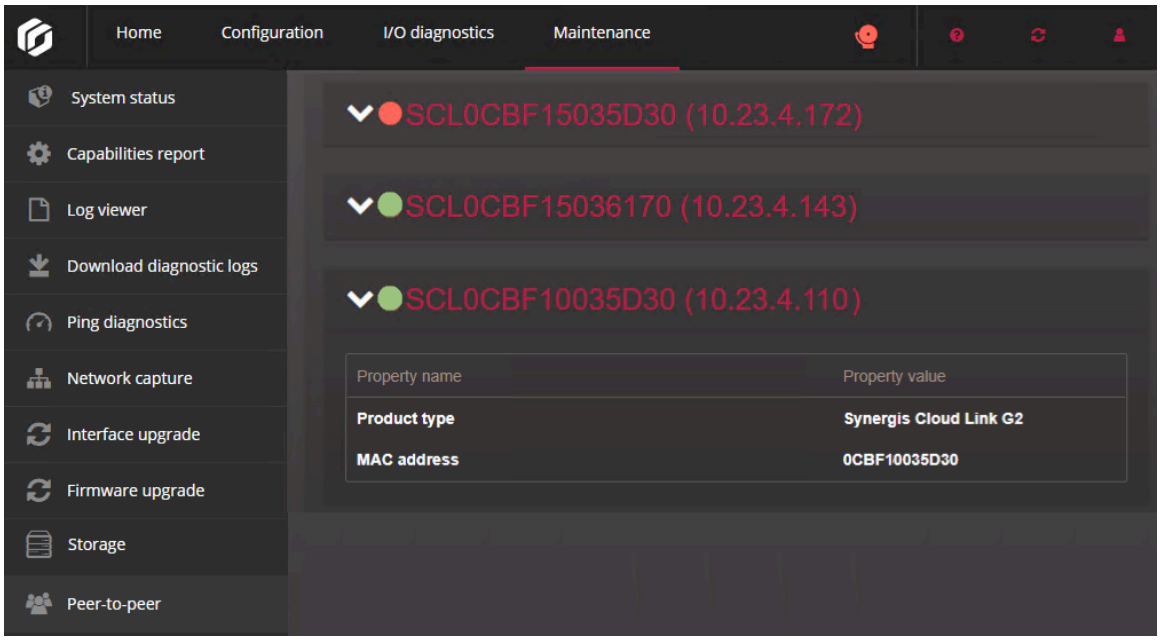
Pour afficher les détails sur les pairs connectés à l'unité Synergis Cloud Link :

1 Connectez-vous à l'unité Synergis Cloud Link .

2 Cliquez sur **Maintenance** > **Pair-à-pair**.

La liste des pairs s’affiche.

3 Cliquez sur une unité pour afficher le type de produit et l'adresse MAC associés.
Exemple :



À propos du compte de service de diagnostic Synergis Cloud Link

Le compte de service de diagnostic fournit des privilèges de diagnostic et de dépannage de base à un titulaire de compte non-administrateur.

Le compte de service de diagnostic permet à une personne sans privilèges d'administrateur de se connecter à l'unité Synergis[MC] Cloud Link et d'effectuer des tâches de diagnostic et de dépannage de base.

L'utilisateur du service de diagnostic a accès à moins de fonctionnalités que l'administrateur. Les pages suivantes du Synergis[MC] Appliance Portal sont accessibles par l'utilisateur du service :

- **Matériel :** Affichez la configuration matérielle.
- **Journalisation Synergis Softwire :** Configurez les niveaux de journalisation et la rétention des historiques.
- **Réseau :** Affichez le nom d'hôte de l'unité, les réglages du Gestionnaire d'accès et les réglages réseau.
- **Utilisateurs :** Faites la mise à jour du mot de passe de l'utilisateur du service.
- **Diagnotic d'E/S :** Affichez les entités contrôlées par l'unité. Contrôlez les sorties si les commandes de sortie sont activées.

  Pour en savoir plus, voir Désactiver les contrôles de sorties , page 38.
- **État du système :** Affichez les propriétés réseau et de l'unité ainsi que l'audit utilisateur.
- **Télécharger les journaux de diagnostic :** Téléchargez les journaux et l'archive d'ingénierie chiffrée pour les fournir à l'assistance technique Genetec[MC].

  REMARQUE : L'utilisateur du service ne peut pas télécharger les historiques.
- **Diagnostic de ping :** Faites un ping des modules d'interface et de leurs interfaces en aval.

Créer le compte de service de diagnostic

Créer un compte de service via le Synergis[MC] Appliance Portal vous permet de fournir un accès de diagnostic et de dépannage de base à quelqu'un qui n'a pas de privilèges d'administrateur.

À savoir

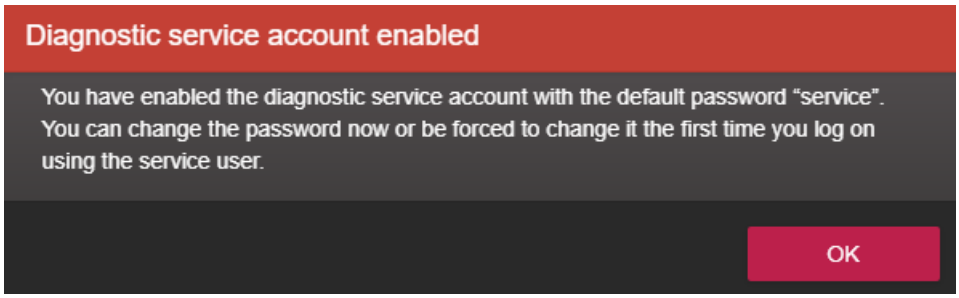
Le nom d'utilisateur et le mot de passe par défaut du compte de service de diagnostic est *service*. Vous pouvez modifier immédiatement le mot de passe par défaut après l'activation du compte, ou être obligé de le modifier lors de la première connexion avec ce compte.

Procédure

1 Connectez-vous à l'unité Synergis[MC] Cloud Link en tant qu'administrateur.

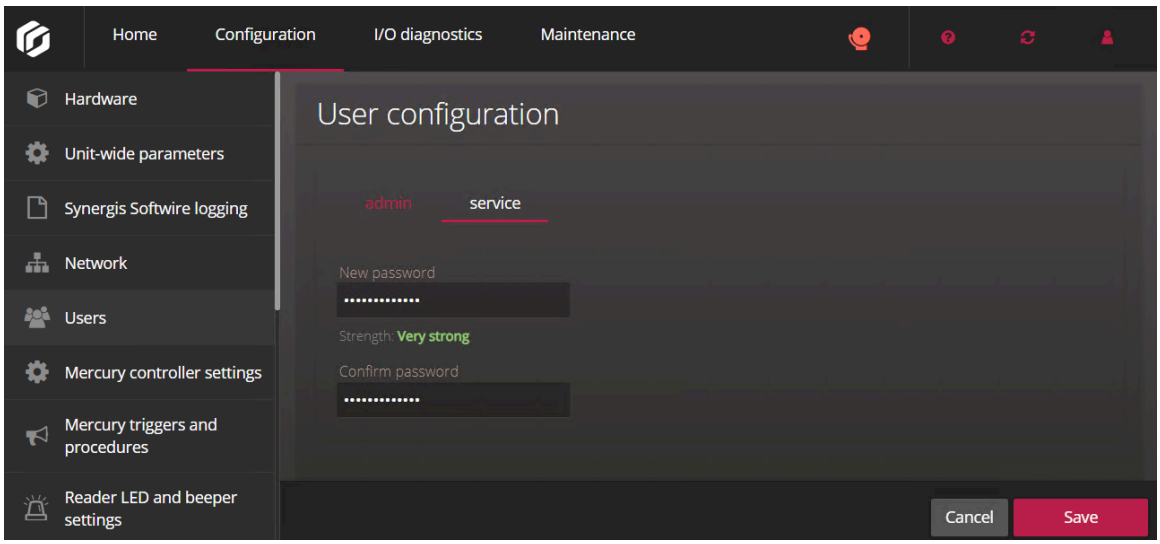
2 Cliquez sur **Configuration** > **Utilisateurs**.

3 Cliquez sur **Activer le compte de service de diagnostic**.
Une boîte de dialogue vous confirme que le compte de service a été activé.



4 Cliquez sur **OK**.

5 Cliquez sur l’onglet **service**, puis remplacez le mot de passe par défaut par un mot de passe fort ou très fort.
REMARQUE : Le mot de passe doit comprendre au moins 15 caractères.



6 Cliquez sur **Enregistrer**.

Redémarrage du matériel ou du logiciel de l'unité Synergis Cloud Link

Durant une séance de dépannage, le technicien d'assistance peut vous demander de faire un redémarrage matériel ou logiciel de l'unité Synergis[MC] Cloud Link.

À savoir

- Un redémarrage matériel, ou *redémarrage système*, est recommandé si vous rencontrez des problèmes matériels.
- Un *redémarrage logiciel* n'est que rarement nécessaire. L'unité Synergis Cloud Link redémarre automatiquement son micrologiciel lorsque vous changez de version du micrologiciel. Le redémarrage manuel du logiciel n’intervient qu’en cas de débogage ou dépannage.

Procédure

1 Connectez-vous à l’unité Synergis Cloud Link.

2 Dans le menu **Redémarrer**, sélectionnez la méthode de redémarrage souhaitée.

- Pour redémarrer le matériel de l’unité, cliquez sur **Redémarrer le système**.
- Pour redémarrer le logiciel de l’unité, cliquez sur **Redémarrer le logiciel**.

Glossaire

activation à double balayage

Avec l'activation à double balayage ou à double passage de badge, un titulaire de cartes autorisé peut déverrouiller une porte et déclencher des actions en passant deux fois son badge. La porte reste déverrouillée et l'action reste active jusqu'à l'événement de double balayage suivant.

admission générale

Appliquée aux secteurs, portes et ascenseurs, la règle admission générale accorde l'accès à tous les titulaires de cartes tout le temps.

antiretour

L'antiretour correspond à une restriction d'accès à un secteur sécurisé empêchant un titulaire de cartes de pénétrer dans un secteur qu'il n'a pas encore quitté, ou inversement.

antiretour global

Fonctionnalité qui étend les restrictions antiretour à des secteurs contrôlés par plusieurs unités Synergis[MC].

antiretour strict

Option de l'antiretour. Lorsque cette option est activée, un événement antiretour est généré lorsqu'un titulaire de cartes tente de quitter un secteur auquel l'accès ne lui a pas été accordé. Lorsqu'elle est désactivée, Security Center ne génère un événement antiretour que lorsqu'un titulaire pénètre dans un secteur qu'il n'a jamais quitté.

appareil Synergis[MC]

Appareil de sécurité en réseau IP fabriqué par Genetec Inc. et dédié aux fonctions de contrôle d'accès. Tous les appareils Synergis[MC] sont livrés avec le logiciel Synergis[MC] Softwire et sont inscrits en tant qu'unités de contrôle d'accès dans Security Center.

aucune admission

La règle aucune admission est une règle d'accès permanente qui refuse l'accès à tous les titulaires de cartes tout le temps, et qui peut servir d'exception aux règles qui accordent l'accès.

certificat X.509

Certificat X.509 et *certificat numérique* sont des synonymes. Dans Security Center, ces deux termes sont utilisés de manière interchangeable.

Gestionnaire d'accès

Le rôle Access Manager gère et surveille les unités de contrôle d'accès du système.

horaire de déverrouillage

Définit les plages de temps durant lesquelles le passage d'un point d'accès (côté de porte ou étage d'ascenseur) est accordé librement.

identifiant

Entité qui représente une carte de proximité, un modèle biométrique ou un code PIN exigé pour accéder à un secteur sécurisé. Un identifiant ne peut être affecté qu'à un titulaire à la fois.

identifiant mobile

Identifiant sur un smartphone qui utilise la technologie Bluetooth ou NFC (Near Field Communication) pour accéder aux secteurs sécurisés.

Liens E/S

Les liens d'entrée/sortie contrôlent un relais de sortie en fonction de l'état combiné (normal, actif ou problème) d'un ensemble d'entrées surveillées. Ils peuvent par exemple servir à déclencher un avertisseur sonore (via un relais de sortie) lorsqu'une fenêtre du rez-de-chaussée d'un immeuble est brisée (si chaque fenêtre est équipée d'un capteur de « bris de glace » relié à une entrée).

Magasin de clés Synergis[MC]

Le magasin de clés Synergis[MC] est une base de données qui contient des clés de lecteur transparent, des clés *ReaderKc* et *ReaderKs* pour les lecteurs STid, et la clé SAM LockUnlock (verrouillage/déverrouillage) pour les unités Synergis[MC] équipées du module d'extension en option. Les clés dans la base de données ne peuvent pas être affichées ou lues, mais elles peuvent être vérifiées par hachage de clés.

mode autonome

Mode de fonctionnement dans lequel le module d'interface prend des décisions autonomes en fonction des réglages de contrôle d'accès préalablement téléchargés depuis l'unité Synergis[MC]. Lorsque le module est en ligne, la création de rapports d'activité est exécutée en direct. Lorsque le module est hors ligne, le rapport d'activité est effectué sur horaire ou lorsque la connexion à l'unité est disponible. Certains modules d'interface ne prennent pas en charge le mode autonome.

mode dégradé

Mode de fonctionnement hors ligne du module d'interface en cas de perte de connexion à l'unité Synergis[MC]. Le module d'interface accorde l'accès à tous les identifiants correspondant à un code d'installation particulier.

mode dépendant

Mode de fonctionnement en ligne du module d'interface, lorsque l'unité Synergis[MC] prend toutes les décisions de contrôle d'accès. Certains modules d'interface ne prennent pas en charge le mode dépendant.

mode supervisé

Mode de fonctionnement en ligne du module d'interface, lorsqu'il prend des décisions en fonction des réglages de contrôle d'accès préalablement téléchargés depuis l'unité Synergis[MC]. Le module d'interface signale son activité en temps réel à l'unité, et permet à l'unité d'ignorer les décisions qui contredisent les réglages actuels de l'unité. Certains modules d'interface ne prennent pas en charge le mode supervisé.

module d'interface

Un module d'interface est un périphérique de sécurité tiers qui communique avec une unité de contrôle d'accès via une connexion IP ou RS-485, et qui fournit des connexions d'entrée, de sortie et de lecteur supplémentaires à l'unité.

moteur d'automatisation

Le moteur d'automatisation est la fonctionnalité du Synergis[MC] Softwire qui exécute des règles, comme les associations événement-action dans Security Center. Le moteur d'automatisation fonctionne même lorsque l'unité Synergis[MC] est déconnectée de son rôle Gestionnaire d'accès.

niveau d'accès

Valeur numérique servant à restreindre l'accès à un secteur lorsqu'un niveau de risque est activé. Un titulaire de cartes ne peut pénétrer un secteur que si son niveau d'accès est supérieur ou égal à celui du secteur.

niveau de risque

Un niveau de risque avertit les utilisateurs du système de l'évolution des conditions de sécurité, telles qu'un incendie ou une fusillade, dans une zone spécifique ou dans l'ensemble du système. Des procédures de traitement spécifiques peuvent être appliquées automatiquement lorsqu'un niveau de risqu est relevé ou annulé.

Protocole F2F

Le protocole F2F est un protocole de lecteur propriétaire de Casi Rusco. Il s'agit d'un protocole à un fil, contrairement aux deux fils des protocoles Wiegand ou OSDP.

règle d'accès

Une entité règle d'accès définit une liste de titulaires de cartes auxquels un accès est accordé ou refusé en fonction d'un horaire. Les règles d'accès peuvent être appliquées aux secteurs sécurisés et aux portes d'entrée et de sortie, ou aux secteurs de détection d'intrusion pour l'armement et le désarmement.

règle d'escorte de visiteur

Restriction d'accès à un secteur sécurisé qui requiert l'accompagnement des visiteurs par un titulaire de cartes durant leur visite. Pour que le passage par un point d'accès soit accordé, le visiteur et son hôte attitré (un titulaire de cartes) doivent tous les deux présenter leurs identifiants dans un délai donné.

règle de deuxième personne

Restriction d'accès à une porte qui oblige deux titulaires de cartes (y compris les visiteurs) à présenter leurs identifiants dans un certain laps de temps afin d'obtenir un accès.

règle de superviseur présent

Restriction d'accès à un secteur sécurisé empêchant quiconque de pénétrer le secteur tant qu'un superviseur n'est pas présent sur site. La restriction peut être appliquée en cas d'accès libre (horaires de déverrouillage des portes) ou d'accès contrôlé (règles d'accès en vigueur).

sas

Un sas est un système qui restreint l’accès à un secteur sécurisé en n’autorisant l'ouverture que d'une seule porte de périmètre à la fois.

secteur sécurisé

Un *secteur sécurisé* est une entité secteur qui représente un site physique auquel l'accès est contrôlé. Un secteur sécurisé est constitué de portes de périmètre (portes servant à pénétrer et à quitter le secteur) et de restrictions d'accès (règles régissant l'accès au secteur).

synchronisation d'une unité

La synchronisation d'une unité correspond au téléchargement des derniers réglages Security Center sur une unité de contrôle d'accès. Ces réglages, comme les règles d'accès, titulaires de cartes, identifiants, horaires de déverrouillage, etc., sont nécessaires pour que l'unité puisse prendre des décisions autonomes fiables indépendamment du Gestionnaire d'accès.

Synergis[MC] Appliance Portal

Synergis[MC] Appliance Portal est l’outil d’administration Web utilisé pour configurer et gérer l’appareil Synergis[MC], et pour mettre à niveau son micrologiciel.

Synergis[MC] Cloud Link

Synergis[MC] Cloud Link est une passerelle IdO compatible PoE conçue pour répondre à la demande d’une solution de contrôle d’accès non propriétaire. Synergis[MC] Cloud Link offre une prise en charge native d’une grande variété de contrôleurs intelligents et de verrous électroniques.

Synergis[MC] Softwire

Synergis[MC] Softwire est le logiciel de contrôle d’accès développé par Genetec Inc. pour divers appareils de sécurité sur IP. Synergis[MC] Softwire permet à ces appareils de communiquer avec des modules d’interface tiers. Un appareil de sécurité qui exécute Synergis[MC] Softwire est inscrit en tant qu’unité de contrôle d’accès dans Security Center.

titulaire de cartes

Une entité titulaire de cartes représente un individu autorisé à pénétrer et à quitter des secteurs sécurisés en fonction de ses identifiants (généralement des cartes d'accès), et dont les activités peuvent être surveillées.

unité de contrôle d'accès

Une entité unité de contrôle d'accès représente un périphérique de contrôle d'accès intelligent, comme un appareil Synergis[MC], un contrôleur de porte Axis Powered by Genetec ou un contrôleur réseau HID, et qui communique directement avec le Gestionnaire d'accès sur un réseau IP. Une unité de contrôle d'accès fonctionne de manière autonome si elle est déconnectée du Gestionnaire d'accès.

unité Synergis[MC]

Appareil Synergis[MC] inscrit en tant qu'unité de contrôle d'accès dans Security Center.

zone

Une zone est une entité qui surveille un ensemble d'entrées et déclenche des événements en fonction de leurs états. Ces événements peuvent servir à contrôler des relais de sortie.

Zone d'E/S

Entité zone qui permet d'étendre les liens d'entrée/sortie à plusieurs unités Synergis[MC], dont l'une agit en tant qu'unité principale. Toutes les unités Synergis[MC] impliquées dans une zone d'E/S doivent être gérées par le même Gestionnaire d'accès. La zone d'E/S fonctionne indépendamment du Gestionnaire d'accès, mais cesse de fonctionner si l'unité principale est inaccessible. Une zone d'E/S peut être armée et désarmée depuis Security Desk, dès lors que l'unité principale est en ligne.

zone matérielle

Une zone matérielle est une entité zone dont les liens d'E/S sont gérés par une seule unité de contrôle d'accès. Les zones matérielles fonctionnent indépendamment du Gestionnaire d'accès et ne peuvent donc pas être armées ou désarmées depuis Security Desk.

Où trouver les informations sur les produits

Vous trouverez la documentation sur les produits aux emplacements suivants :

- **Genetec[MC] TechDoc Hub :** La dernière documentation est disponible sur TechDoc Hub.

  Vous ne trouvez pas ce que vous cherchez ? Envoyez un e-mail à l'adresse documentation@genetec.com.
- **Pack d'installation :** Le guide d'installation et les notes de version sont disponibles dans le dossier Documentation du pack d'installation. Ces documents comportent également un lien de téléchargement direct vers la dernière version du document.
- **Aide :** Les applications client Security Center offrent une aide en ligne qui décrit le fonctionnement du produit et la marche à suivre pour utiliser ses fonctionnalités. Pour accéder à l'aide, cliquez sur **Aide**, appuyez sur F1, ou sélectionnez le point d'interrogation **'?'** dans les différentes applications client.

Assistance technique

Le centre d'assistance technique de Genetec[MC] (GTAC) s'engage à fournir le meilleur service d'assistance technique possible à ses clients du monde entier. En tant que client de Genetec Inc., vous avez accès au TechDoc Hub, où vous pouvez trouver des informations et chercher des réponses à vos questions sur les produits.

- **Genetec TechDoc Hub :** Recherchez des articles, manuels et vidéos répondant à vos questions ou vous aidant à résoudre les problèmes techniques.

  Avant de contacter GTAC ou d'ouvrir un dossier de support, il est recommandé de rechercher dans TechDoc Hub les correctifs potentiels, solutions de contournement ou problèmes connus.

  Pour accéder à TechDoc Hub, connectez-vous au Portail Genetec et cliquez sur TechDoc Hub. Vous ne trouvez pas ce que vous cherchez ? Envoyez un e-mail à l'adresse documentation@genetec.com.
- **Centre d'assistance technique de Genetec (GTAC) :** La procédure pour contacter GTAC est décrite dans la Description de Genetec Advantage.

Formation technique

Que ce soit en classe professionnelle ou depuis votre bureau, nos formateurs qualifiés peuvent vous guider dans la conception, l'installation, le fonctionnement et le dépannage du système. Des services de formation technique sont proposés pour tous les produits et pour différents niveaux d'expérience, et peuvent en outre être personnalisés pour répondre à vos besoins ou objectifs particuliers. Pour en savoir plus, voir http://www.genetec.com/support/training/training-calendar.

Licences

- Pour l'activation ou la réinitialisation des licences, contactez GTAC sur https://portal.genetec.com/support.
- Pour des problèmes de contenu de licences ou de références ou concernant une commande, contactez le service clientèle de Genetec à l'adresse customerservice@genetec.com, ou appelez le 1-866-684-8006 (option 3).
- Pour obtenir une licence de démo ou pour des questions sur les tarifs, contactez le service commercial de Genetec à l'adresse sales@genetec.com, ou appelez le 1-866-684-8006 (option 2).

Problèmes et pannes des produits matériels

Contactez GTAC sur https://portal.genetec.com/support pour tout problème lié aux appareils Genetec ou au matériel acheté auprès de Genetec Inc.