

<b>GAMME DE PRODUITS :</b>	ACCÈS		
<b>PRODUIT :</b>	ACT Enterprise		
<b>MODÈLE/Version :</b>	2.10	<b>CATÉGORIE :</b>	MISE À JOUR
<b>CONTACT :</b>	Support technique local	<b>DATE :</b>	29/10/2019

Ce document s'applique à **ACT Enterprise** version 2.10 ou supérieure.

Il s'agit d'une liste des nouvelles caractéristiques et améliorations intégrées dans la version 2.10 d'**ACT Enterprise**. L'utilisation de certaines caractéristiques impose de mettre à jour les firmwares des contrôleurs concernés. Ces firmwares sont joints dans le package d'installation d'**ACT Enterprise** (remarque : le firmware de la platine de porte ACTpro-100 ne peut pas être mis à jour).

## Table des matières

<b>Lecteurs/identifiants Bluetooth :</b> .....	2
<b>Lecteurs biométriques (ZKTeco) :</b> .....	4
<b>Lecteurs OSDP avec chiffrement :</b> .....	6
<b>Limites d'utilisation :</b> .....	8
<b>Badges vierges :</b> .....	10
<b>Déverrouiller une porte au premier accès :</b> .....	11
<b>Activer des sorties OP2 et OP3 lors d'événements de porte forcée et de porte ouverte trop longtemps :</b> .....	11
<b>Augmenter le nombre d'événements du journal à 20 000 :</b> .....	12
<b>Augmenter le nombre de groupe de personnes à 2 000 :</b> .....	12
<b>Mises à jour en finnois et en suédois</b> .....	12
<b>Blocage d'une personne pendant 5 minutes après saisie d'un code PIN erroné 5 fois :</b> .....	12
<b>Désactivation immédiate du relais lors de l'arrêt de la fonction bascule d'une porte:</b> .....	12
<b>Support pour les verrous Assa Aperio version 2 :</b> .....	13
<b>Amélioration de la licence ACT Enterprise :</b> .....	13
<b>Réinitialiser les compteurs de règles :</b> .....	13

## Lecteurs/identifiants Bluetooth :

**ACT Enterprise** prend en charge l'utilisation d'identifiants Bluetooth via les lecteurs Bluetooth commercialisés par Vanderbilt.

### Prérequis :

- Installer **ACT Enterprise** ou **ACT Enterprise Lite** (version gratuite) version **2.10** ou supérieure.
- Seuls les lecteurs Bluetooth commercialisés par Vanderbilt peuvent être pris en charge.
- Installer des lecteurs Bluetooth Wiegand ou OSDP de Vanderbilt.
- Vérifier que le contrôleur ACTpro-1500 a un firmware version **1.08** ou supérieure.
- Enregistrer la licence relative à l'authentification Bluetooth dans **ACT Enterprise server**. ACT Enterprise est vendu avec une licence gratuite.

### Liste des lecteurs Bluetooth pris en charge :

Référence	Description du matériel
P54508-P124-A100	Licence Bluetooth ACTE-BT
N54504-Z160-A100	Lecteur Bluetooth BLUE-A, Wiegand
N54504-Z161-A100	Lecteur Bluetooth BLUE-B, Wiegand, clavier
N54504-Z162-A100	Lecteur Bluetooth BLUE-C, OSDP
N54504-Z163-A100	Lecteur Bluetooth BLUE-D, OSDP, clavier
*N54504-Z164-A100	Bouton de sortie pour porte BLUE-EX

\* Le bouton de sortie sans contact (REX) BLUE-EX (N54504-Z164-A100) fonctionne avec n'importe quel contrôleur.

### Important :

Veillez prendre connaissance des guides de l'utilisateur **Bluetooth** et **VI Mobile ID** pour avoir une description détaillée sur la façon de configurer et d'utiliser les identifiants Bluetooth.

### Étape 1 : Depuis **ACT Manage > Setting > Bluetooth** (ACT Manage > Paramètres > Bluetooth)

- Cochez la case **Activate Bluetooth Enrolment** (Activer enrégistrement Bluetooth).
- Saisissez l'adresse e-mail de la personne (administrateur) qui sera chargée de gérer et d'ajouter les identifiants Bluetooth.
- Saisissez la durée en heures au cours de laquelle la demande de QR code restera valide avant d'expirer.
- Saisissez le nom de l'organisation.
- Cliquez sur **Save** (Enregistrer).



Étape 2 : Depuis **ACT Manage > Setting > SMTP** (ACT Manage > Paramètres > SMTP)

- Saisissez les informations relatives au serveur de messagerie pour permettre à **ACT Enterprise** d'envoyer des e-mails. Office 365 est utilisé ici dans le cadre de cet exemple.
- Cliquez sur **Save** (Enregistrer).
- Cliquez sur **Send Test Email** (Envoyer E-mail de test) pour vérifier qu'ACT Enterprise est correctement configuré pour envoyer des e-mails.



Étape 3 : Depuis **ACT Manage > Manage > Users > General** (ACT Manage > Gérer > Personnes > Général)

- Saisissez une adresse e-mail valide. Il s'agit de l'adresse e-mail à laquelle une invitation est envoyée pour demander une clé d'enregistrement à partir de l'application « VI Mobile ID ».
- Saisissez un numéro du badge dans le champ **One-to-One** (Un-à-Un). Il s'agit du numéro que les lecteurs Bluetooth transmettront au contrôleur.
- Cliquez sur **Save** (Enregistrer).



Étape 4 : Depuis **ACT Manage > Manage > Users > Bluetooth** (ACT Manage > Gérer > Personnes > Bluetooth)

- Cliquez sur **Invite** (Inviter) pour envoyer un e-mail à la personne concernée pour l'inviter à créer un identifiant Bluetooth.



**Exemples d'e-mails d'invitation :**

*Vous avez été invité à créer des identifiants Bluetooth sur votre téléphone pour **Nom de l'organisation**.*

*Téléchargez l'application VI Mobile ID depuis votre compte du magasin d'applications de Vanderbilt.*

*Aller dans Paramètres – Autorisation.*

*Faites une demande d'autorisation et envoyez-la à cette adresse : [adminuser@domain.com](mailto:adminuser@domain.com)*

Étape 5 : Depuis **ACT Manage > Manage > Users > Bluetooth** (ACT Manage > Gérer > Personnes > Bluetooth)

- L'administrateur saisit le code transmis par l'application mobile.  
Exemple de code pour référence : BTAN#97653612D8DA728CA9401594C6F18088A1CD4F4D00#13
- Cliquez sur **Save** (Enregistrer).



## Lecteurs biométriques (ZKTeco) :

ACT Enterprise prend en charge les lecteurs ZKTeco (MA300 et SF420)

### Prérequis :

- Installer **ACT Enterprise** ou **ACT Enterprise Lite** (version gratuite) version 2.10 ou supérieure.
- Enregistrer la licence relative à l'authentification biométrique. ACT Enterprise est vendu avec une licence gratuite
- Installer des lecteurs biométriques ZKTeco.
- Raccorder le lecteur ZKTeco directement à l'interface Wiegand du contrôleur.
- Paramétrer le même réseau IP que celui du serveur ACT Enterprise (le serveur ACT Enterprise communique directement avec les lecteurs biométriques pour leur transmettre des modèles de données biométriques).
- Installer le pilote du lecteur d'enrôlement USB ZKTeco, puis le lecteur lui-même.

### Liste des lecteurs biométriques pris en charge :

Référence	Description du matériel
P54508-P123-A100	Licence Biométrique ACTE-BIO (par lecteur)
N54504-Z152-A100	Lecteur d'empreintes pour contrôle d'accès MA300 (MF)
N54504-Z151-A100	Lecteur d'empreintes pour contrôle d'accès SF420 (MF)
*N54504-Z150-A100	Lecteur d'empreintes USB Silk ID SLK20R (lecteur d'enrôlement)

\*Le pilote du lecteur SLK20R est vendu avec ACT Enterprise et doit être installé avant de raccorder le lecteur d'enregistrement à un port USB.

Important : Prenez connaissance de la rubrique relative à l'authentification biométrique dans le **guide de l'utilisateur** pour avoir une description détaillée sur la façon de configurer et d'utiliser les lecteurs biométriques.

Étape 1 : Depuis **ACT Install > Settings > Biometrics** (ACT Install > Paramètres > Données biométriques)

**Remarque : Cette étape DOIT être effectuée avant d'ajouter des lecteurs biométriques.**

- Sélectionnez le fabricant de lecteurs biométriques que vous avez choisi.

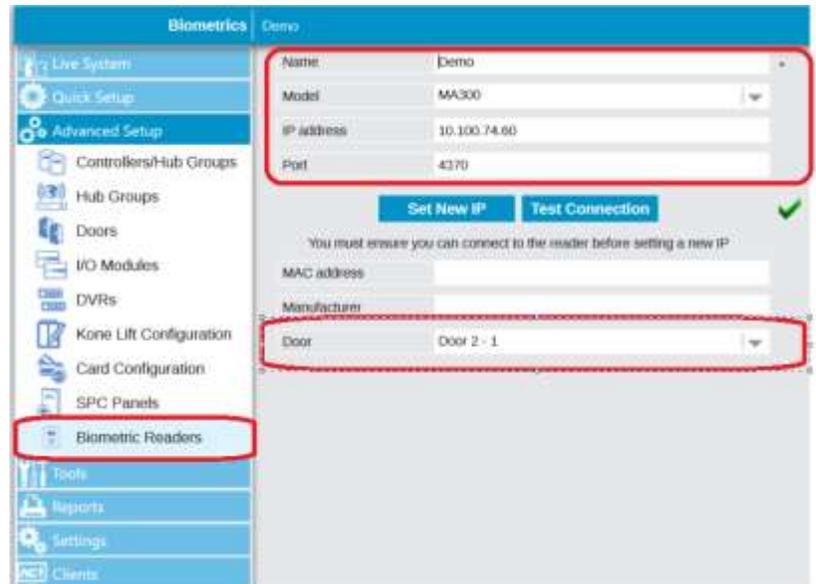
- Saisissez le numéro du badge de l'administrateur dans le champ **Admin Card Number** (Numéro Badge Admin.). Si vous n'en indiquez aucun, les fonctionnalités d'administrateur seront accessibles sur tous les appareils ZKTeco équipés d'un affichage LCD.



- Saisissez le code PIN qui est utilisé pour connecter les lecteurs biométriques à ACT Enterprise.

Étape 2 : Depuis **ACT Install > Advanced Setup > Biometric Readers** (ACT Install > Configuration avancée > Lecteurs biométriques)

- Sélectionnez le modèle du fabricant à partir du menu déroulant **Model** (Modèle). *Remarque : tous les lecteurs biométriques que vous utilisez doivent être conçus par le même fabricant.*
- Saisissez un nom descriptif pour le lecteur dans le champ **Name** (Nom), puis renseignez les valeurs des champs **IP address** (Adresse IP) et Port dont se servira ACT Enterprise pour communiquer avec le lecteur et leur envoyer des modèles de données biométriques.
- Sélectionnez la porte à partir du menu déroulant **Door** (Porte) qui sera associée au lecteur biométrique concerné.



Étape 3 : Depuis **ACT Manage > Manage > Users > General** (ACT Manage > Gérer > Personnes > Général)

- Renseignez des informations au sujet de la personne concernée (nom et groupe de personnes).
- Cliquez sur l'icône en forme d'empreinte digitale à droite du champ **Biometric ID** (ID biométrique), puis suivez les instructions à l'écran.
- Cliquez sur **Save** (Enregistrer).



## Lecteurs OSDP avec chiffrement :

ACT Enterprise version 2.10 ou supérieure prend en charge les lecteurs OSDP de Vanderbilt ainsi que ceux de HID.

### Prérequis :

- Installer **ACT Enterprise** ou **ACT Enterprise Lite** (version gratuite) version 2.10 ou supérieure.
- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500.

### Remarque :

- Si vous mettez à niveau ACT Enterprise à partir d'une version antérieure avec des lecteurs OSDP déjà configurés, il se peut que vous deviez ajouter de nouveau les lecteurs OSDP.
- Les lecteurs OSDP ne sont pris en charge que sur la porte 1 des contrôleurs de la famille des contrôleurs ACT1500.
- Les lecteurs OSDP ne fonctionnent pas avec des contrôleurs plus anciens non équipés de cavalier OSDP. Pour plus d'informations, veuillez consulter le guide d'installation du contrôleur.
- Afin d'éviter des conflits d'adresses, vous devez connecter et configurer les lecteurs OSDP les uns après les autres. Vous ne devez jamais connecter plusieurs lecteurs OSDP avec une adresse identique à un contrôleur.
- Si vous retirez un lecteur OSDP de l'infrastructure ACT Enterprise alors qu'il était configuré pour accepter des communications chiffrées, vous devez le réinitialiser de façon manuelle. Pour plus d'informations sur la réinitialisation des lecteurs OSDP, veuillez consulter la documentation du fabricant qui les a conçus.
- La clé de chiffrement OSDP ne peut pas être modifiée ou supprimée tant que des lecteurs OSDP sont enregistrés dans la base de données.
- **ACT Enterprise** ne prend en charge que les lecteurs OSDP conçus par Vanderbilt et HID.

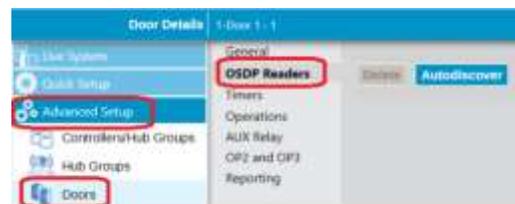
Étape 1 : Depuis **ACT Install > Advanced Setup > Controller > Operations** (ACT Install > Configuration avancée > Contrôleur > Opérations)

- Cochez la case **Support OSDP** (Prise en charge OSDP) du contrôleur. Le contrôleur doit avoir un firmware version 1.08 ou supérieure.
- Cliquez sur **Save** (Enregistrer).



Étape 2 : Depuis **ACT Install > Advanced Setup > Doors > OSDP Readers** (ACT Install > Configuration avancée > Portes > Lecteurs OSDP)

- Cliquez sur **Autodiscover** (Autodécouvrir). Le processus d'autodécouverte peut durer jusqu'à 2 minutes.
- Cochez la case **Support OSDP** (Prise en charge OSDP) du contrôleur OSDP. Le contrôleur doit avoir un firmware version 1.08 ou supérieure.
- Saisissez un nom dans le champ **Name** (Nom) pour chaque lecteur OSDP découvert.



- Sélectionnez la direction du déplacement (Entrée ou Sortie) dans le champ **Direction** pour chaque lecteur OSDP découvert.
- Cliquez sur **Save** (Enregistrer).

**Remarque :**

Si vous mettez à niveau ACT Enterprise à partir d'une version antérieure avec des lecteurs OSDP déjà configurés, vous devez de nouveau renseigner le nom et la direction du déplacement pour chacun des lecteurs OSDP.



## Limites d'utilisation :

Les limites d'utilisation permettent aux organisations de limiter le nombre d'événements d'entrée et de sortie au cours d'une période définie. Cette fonctionnalité peut être utile dans de nombreux scénarios différents. Un scénario d'utilisation quotidien pourrait être, par exemple, celui d'un club pour lequel un utilisateur achèterait 10 accès et verrait son compte être désactivé dès qu'il aurait consommé le dernier.

### Prérequis :

- Installer **ACT Enterprise version 2.10** ou supérieure

Étape 1 : Depuis **ACT Manage > Settings > Usage Limits** (ACT Manage > Paramètres > Limites d'utilisation)

- Cochez la case **Enable Usage Limits** (Valider Limites d'utilisation) et configurez les paramètres souhaités.
- Le champ **Event Window (sec)** (Fenêtre d'événement (sec.)) indique que seul le premier événement qui se produira au cours de la fenêtre d'événement définie sera accepté. Cette configuration permet d'éviter de compter deux fois le passage accidentel d'un badge à deux reprises.



- Paramétrez le groupe de portes qui contient la ou les portes à utiliser pour compter le nombre d'utilisations, celles-ci étant généralement des portes d'entrée ou de sortie.

Étape 2 : Depuis **ACT Manage > Manage > User Groups > Usage Limit Settings** (ACT Manage > Gérer > Groupes de personnes > Paramètres Limites d'utilisation)

Les groupes de personnes ignorent par défaut les limites d'utilisation tant que vous ne décochez pas la case **Usage Limits Ignored** (Limites d'utilisation ignorées). **Une fois la case décochée, toutes les personnes appartenant à ce groupe se verront imposer des limites d'utilisation sauf si vous les désactivez individuellement pour chaque personne.**

Vous pouvez imposer des limites différentes aux personnes en fonction de groupes ou de catégories spécifiques.

- Vous pouvez définir trois catégories de groupes de personnes, par exemple, Or, Argent et Bronze.
- Depuis la rubrique **Usage Limit Settings** (Paramètres Limites d'utilisation), indiquez la valeur du compteur associé à chaque groupe de personnes. L'action prise au moment où la limite d'utilisation est atteinte doit être définie à l'étape 1 ci-dessous.
- Depuis **ACT Manage > Manage > Users** (ACT Manage > Gérer > Personnes), affectez la personne au groupe de personnes approprié.



Étape 3 : Depuis **ACT Manage > Manage > User > Usage Limit Settings** (ACT Manage > Gérer > Personnes > Paramètres Limites d'utilisation)

- Les limites d'utilisation doivent être validées depuis le groupe de personnes. Lorsque vous validez des limites d'utilisation, cette action se répercute à l'ensemble des personnes appartenant à ce groupe sauf si vous décidez de les désactiver individuellement pour chaque personne.
- Vous pouvez faire en sorte d'ignorer des limites d'utilisation pour certaines personnes en cochant la case **Usage Limits ignored** (Limites d'utilisation ignorées).



Étape 4 : Depuis **ACT Manage > Manage > Users > General** (ACT Manage > Gérer > Personnes > Général)

Les limites d'utilisation peuvent être réinitialisées de façon manuelle au niveau de chaque personne. Saisissez une nouvelle valeur dans le champ **Usage Count** (Nombre d'utilisations), puis cliquez sur **Reset** (Réinitialiser).



#### Remarque :

Si vous configurez des compteurs pour décompter un nombre d'entrées donné, par exemple 5 entrées que vous avez accordées à une personne, et que celle-ci les utilise toutes, alors lorsque cette personne essaiera de sortir au bout de la 5<sup>ème</sup> fois, elle se verra refuser la sortie puisque son compte a été configuré pour être désactivé au bout de la 5<sup>ème</sup> entrée. Dans le cadre d'un scénario comme celui-ci dans lequel les personnes doivent s'identifier devant un lecteur pour entrer et pour sortir, nous vous recommandons de paramétrer 10 utilisations et de décrémenter le nombre d'utilisations à chaque événement d'entrée et de sortie. Depuis **ACT Manage > Settings > Usage Limits > Usage event types** (ACT Manage > Paramètres > Limites d'utilisation > Types d'événement d'utilisation), sélectionnez la valeur **Both entry and exit events** (Événements d'entrée et de sortie).



## Badges vierges :

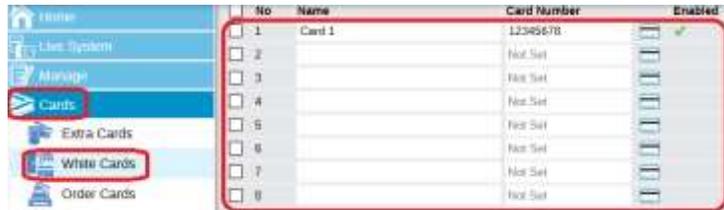
Les badges vierges sont destinés à fournir un accès aux services d'urgence et sont conçus pour contourner toutes les restrictions de contrôle d'accès. Les badges vierges sont téléchargés et stockés directement dans les contrôleurs pour accorder l'accès même lorsque les contrôleurs sont hors ligne.

### Prérequis :

- Installer **ACT Enterprise** version 2.10 ou supérieure
- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500
- Installer un firmware version 1.59 ou supérieure sur le contrôleur ACTpro-4000
- Installer un firmware version 1.25 ou supérieure sur la platine de porte ACTpro-100

Étape 1 : Depuis **ACT Manage > Cards > White Cards** (ACT Manage > Badges > Badges vierges)

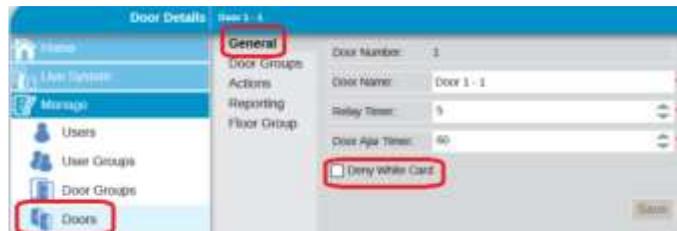
- Vous pouvez ajouter jusqu'à 16 badges vierges pour lesquels vous devez indiquer le nom qui apparaîtra ainsi que le numéro de badge.
- Remarque : Les badges doivent être uniques et ne pas être affectés à des personnes individuelles.
- Cliquez sur **SAVE** (ENREGISTRER)



No	Name	Card Number	Enabled
<input type="checkbox"/>	Card 1	12345678	<input checked="" type="checkbox"/>
<input type="checkbox"/>		Not Set	<input type="checkbox"/>
<input type="checkbox"/>		Not Set	<input type="checkbox"/>
<input type="checkbox"/>		Not Set	<input type="checkbox"/>
<input type="checkbox"/>		Not Set	<input type="checkbox"/>
<input type="checkbox"/>		Not Set	<input type="checkbox"/>
<input type="checkbox"/>		Not Set	<input type="checkbox"/>
<input type="checkbox"/>		Not Set	<input type="checkbox"/>

Étape 2 : Depuis **ACT Manage > Manage > Doors** (ACT Manage > Gérer > Portes)

- Pour exclure des portes du groupe de portes accessibles par des badges vierges, cochez la case **Deny white card** (Refuser badge vierge).
- Cliquez sur **SAVE** (ENREGISTRER)



## Déverrouiller une porte au premier accès :

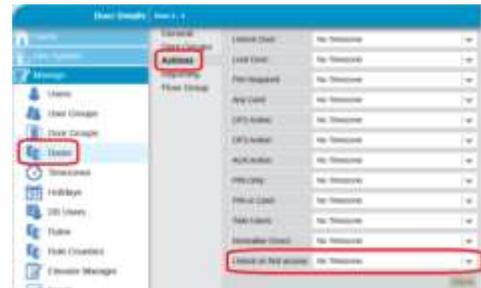
Les portes peuvent être configurées pour être déverrouillées au cours d'une tranche horaire spécifique. Il est possible que certains salariés n'arrivent pas dans les locaux avant le début de la tranche horaire. Lorsque vous configurez cette fonctionnalité, un accès valide doit être autorisé au niveau de la porte concernée avant que celle-ci puisse restée déverrouillée pendant toute la durée de tranche horaire définie.

### Prérequis :

- Installer **ACT Enterprise** version 2.10 ou supérieure
- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500
- Installer un firmware version 1.59 ou supérieure sur le contrôleur ACTpro-4000
- Installer un firmware version 1.25 ou supérieure sur la platine de porte ACTpro-100

Étape 1 : Depuis **ACT Manage > Manage > Doors > Actions** (ACT Manage > Gérer > Portes > Actions)

- Affectez une tranche horaire à l'action **Unlock on first access** (Déverrouiller au premier accès). Vous devez veiller à ne pas configurer des actions contradictoires et des tranches horaires qui se chevauchent. Les actions **Unlock Door** (Déverrouiller Porte) et **Unlock on first access** (Déverrouiller au premier accès) sont contradictoires.



- Cliquez sur **SAVE** (ENREGISTRER)

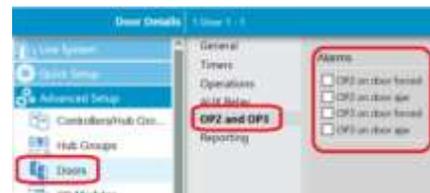
## Activer des sorties OP2 et OP3 lors d'événements de portée forcée et de porte ouverte trop longtemps :

### Prérequis :

- Installer **ACT Enterprise** version 2.10 ou supérieure
- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500
- Installer un firmware version 1.21 ou supérieure sur les platines de porte ACTpro-100

Étape 1 : Depuis **ACT Install > Advanced Setup > Doors > OP2 et OP3** (ACT Install > Configuration avancée > Portes > OP2 et OP3)

- Configurez les sorties OP2 et OP3 en fonction des paramètres souhaités afin qu'elles s'activent lors d'événements de portée forcée ou de porte ouverte trop longtemps.



## Augmenter le nombre d'événements du journal à 20 000 :

Vous pouvez augmenter le nombre d'événements du journal enregistrés dans le contrôleur ACTpro-1500 de 5 000 à 20 000

### Prérequis :

- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500.

## Augmenter le nombre de groupe de personnes à 2 000 :

Vous pouvez augmenter le nombre de groupe de personnes de 1 000 à 2 000

### Prérequis :

- Installer **ACT Enterprise** version 2.10 ou supérieure
- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500
- Installer un firmware version 1.59 ou supérieure sur le contrôleur ACTpro-4000

## Mises à jour en finnois et en suédois

Une mise à jour en finnois et en suédois a été intégrée dans **ACT Enterprise** 2.10

## Blocage d'une personne pendant 5 minutes après saisie d'un code PIN erroné 5 fois :

Lorsque des personnes utilisent un badge et un code PIN, elles se retrouvent temporairement bloquées pendant 5 minutes si elles saisissent un code PIN erroné 5 fois de suite.

### Prérequis :

- Installer **ACT Enterprise** version 2.10 ou supérieure
- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500
- Installer un firmware version 1.25 ou supérieure sur la platine de porte ACTpro-100

## Désactivation immédiate du relais lors de l'arrêt de la fonction bascule d'une porte:

Lorsqu'une porte en mode bascule se referme, l'état du relais est immédiatement modifié en conséquence.

### Prérequis :

- Installer **ACT Enterprise** version 2.10 ou supérieure
- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500
- Installer un firmware version 1.59 ou supérieure sur le contrôleur ACTpro-4000
- Installer un firmware version 1.08 ou supérieure sur la platine de porte ACTpro-100

## Support pour les verrous Assa Aperio version 2 :

Un support est disponible pour les verrous Assa Aperio version 2, lesquels sont remplacés par les verrous Aperio V3 actuels.

### Prérequis :

- Installer un firmware version 1.08 ou supérieure sur le contrôleur ACTpro-1500

### Remarque:

Les verrous Aperio version 2 ne communiquent pas en permanence avec le hub Aperio et nécessitent un déclencheur (présentation d'une carte ou appui sur la poignée) pour établir la communication avec le hub. Lorsqu'une commande ou une action de porte est émise par le logiciel, la demande attend dans le concentrateur Aperio jusqu'à ce que le verrouillage soit déclenchée. Dans ce scénario, la carte présentée est ignorée.

## Amélioration de la licence ACT Enterprise :

**ACT Enterprise** prend en charge des lecteurs OSDP, Bluetooth et biométriques via ZKTeco. **ACT Enterprise** intègre un identifiant Bluetooth gratuit et un identifiant biométrique gratuit.

## Réinitialiser les compteurs de règles :

**ACT Enterprise** 2.10 permet aux opérateurs de paramétrer s'ils souhaitent ou non procéder à la réinitialisation des compteurs chaque nuit. Dans les versions antérieures, les compteurs étaient automatiquement réinitialisés chaque nuit.

### Prérequis :

- Installer **ACT Enterprise** version 2.10 ou supérieure

Depuis **ACT Manage > Setting > Général** (ACT Manage > Paramètres > Général)

Cochez la case Reset rule counters to zero nightly (RAZ compteurs de règles chaque nuit) si vous souhaitez réinitialiser tous les compteurs chaque nuit.



**Remarque :**

Les opérateurs peuvent utiliser le moteur de règles pour réinitialiser des compteurs individuels à la date et l'heure qu'ils décident. Dans le cadre de cet exemple, le compteur CarPark s'incrémente à chaque entrée accordée et se décrémente à chaque sortie accordée. Le compteur CarPark est réinitialisé à minuit chaque vendredi.

