



Notes de version du logiciel Sigur

Révision du 16/07/2026

Table des matières

1.	Version 1.6.8.131 (ajoutée en juillet 2026)	3
2.	Contacts	17

1. Version 1.6.8.131 (ajoutée en juillet 2026)

Système :

- Mise en place d'une protection du serveur contre les attaques DoS et l'usurpation d'adresse IP dans le cadre des attaques par amplification, conformément au protocole DTLSv1.2.
- Correction d'un crash du module serveur lors de l'identification faciale (caméra IP) dans le scénario « Autoriser l'accès uniquement en étant accompagné ».
- Correction d'une erreur au démarrage du module serveur lorsque le mot de passe de la base de données commençait par le caractère \$.
- Résolution d'un problème susceptible de provoquer un crash du module serveur lors de la sauvegarde automatique de la base de données.
- Amélioration de la stabilité du module serveur lorsque la reconnaissance faciale Sigur est active et qu'une connexion au port TLS est établie sans échange de certificats ultérieur.
- Correction d'un blocage du serveur empêchant la connexion des postes clients.
- Correction du fonctionnement de la commande exit dans l'utilitaire AdminCLI.
- Correction d'une erreur d'affichage du nombre maximal d'identifiants autorisés par la licence, qui entraînait un dépassement de seuil intempestif.

Installation et mise à jour du logiciel. Lors d'une désinstallation silencieuse avec le paramètre /S, toutes les fenêtres graphiques sont désormais correctement fermées, et le module serveur ainsi que le serveur de base de données sont automatiquement arrêtés avant la désinstallation.

Logiciel « Client » :

- Amélioration des performances et correction d'erreurs survenant dans l'onglet « Personnel » lors de la génération continue d'un grand volume d'événements.
- Correction d'un problème provoquant l'arrêt du logiciel Client lors du rétablissement de la connexion avec le serveur.
- Correction de l'absence de création des raccourcis dans le menu Démarrer et sur le bureau lors de l'installation du logiciel client sous Windows.
- Correction d'un problème de blocage du logiciel Client lors de la tentative de connexion.
- Correction d'un problème de blocage du système lors de l'utilisation des modes d'accès avec le module « Quarantaine ».
- Correction de problèmes survenant dans le logiciel Client sous Linux lors de l'envoi d'un e-mail de test depuis la configuration du serveur SMTP.

Contrôleurs :

- Ajout de la prise en charge des contrôleurs E2 Lite, E2 Pro, E4 Lite et E4 Pro.
- Dans l'onglet « Périphériques OSDP » des paramètres des contrôleurs, ajout des colonnes « Modèle du périphérique » affichant le modèle du lecteur Sigur connecté, et « Paramètres » permettant d'assigner des fonctions aux modes de

- fonctionnement principal et secondaire du lecteur MK100.
- Refonte du champ « Délai d'armement (ms) » dans les paramètres du contrôleur : la valeur se définit désormais à l'aide d'un curseur plutôt que par saisie manuelle. La valeur maximale est de 60 000 ms. Résolution d'un problème d'enregistrement incorrect du temps d'armement.
 - Ajout, dans le programme d'installation, d'une archive contenant les versions actuelles des micrologiciels des contrôleurs. Il n'est désormais plus nécessaire de télécharger le fichier du micrologiciel depuis le site Web pour les contrôleurs de la gamme récente.
 - Renforcement de la stabilité de la connexion entre le contrôleur et le serveur. Auparavant, des pertes de liaison pouvaient occasionnellement se produire. Désormais, le serveur interroge les contrôleurs toutes les 30 secondes au lieu de 600 secondes.
 - Refactorisation du processus de chargement des données des contrôleurs, permettant d'accélérer la synchronisation et de réduire l'empreinte mémoire.
 - Résolution d'un problème entraînant le remplacement de la configuration utilisateur d'un point d'accès sur un contrôleur doté d'un micrologiciel en version 0.x.x par la configuration par défaut lors de la modification du mode d'armement.
 - Résolution d'un problème susceptible de générer l'erreur « Impossible d'initier la mise à jour » lors de la mise à jour du micrologiciel du contrôleur.
 - Correction d'un problème de lenteur de synchronisation des données dans la mémoire du contrôleur lors de la création d'un nouvel employé.
 - Désormais, lors de la configuration du contrôleur, la liste des sorties pour « Ligne d'indication LED3 du lecteur N » n'affiche que les sorties compatibles avec le modèle de contrôleur concerné.
 - Correction d'un défaut de fonctionnement du bouton de changement de profil de chiffrement.
 - Correction : lors de la sélection de la configuration standard « Deux tourniquets, commande par potentiel » pour le contrôleur E510, les paramètres des boutons de demande d'accès « Entrée » / « Sortie » étaient incorrectement appliqués.
 - Élargissement de l'application du délai d'attente « Temps d'attente pour un accompagnateur » à l'attente du second objet d'accès. Cette modification s'applique aux contrôleurs dont le micrologiciel est en version 1.24.0 ou supérieure.

Lecteurs :

- Ajout de la prise en charge des nouvelles gammes de lecteurs Sigur MK100 et MR100 v2.
- Ajout de la prise en charge du lecteur SR100 EMB en modes USB PC/SC et USB HID.

Indication des lecteurs :

- Correction du comportement de la fenêtre de configuration de l'indication des lecteurs dans le logiciel Client. Désormais, si les modifications ne sont pas enregistrées, les profils d'indication ne disparaissent pas et la fenêtre se ferme

- correctement du premier coup, quel que soit l'onglet.
- Interdiction de créer des profils d'indication personnalisés dont le nom commence par « \$! ».
- Correction d'un dysfonctionnement de l'indication « Changer la couleur » : l'indicateur du lecteur clignotait une fois au lieu de changer de couleur.
- Correction d'une erreur dans la génération du nom de la pièce jointe du profil d'indication lors de l'envoi par e-mail. Auparavant, avec des caractères cyrilliques, le nom du fichier s'affichait encodé dans certains clients de messagerie.

Cartes Mifare :

- Correction d'erreurs de lecture et d'écriture sur certaines cartes Mifare Classic en mode protégé.
- Correction d'un problème de passage de la carte Mifare Plus en mode SL3 via le lecteur ACR1252U.

Personnel :

- Correction d'un problème empêchant la prise en compte des modifications des droits d'accès à un point d'accès lorsque la connexion avec le contrôleur était absente au moment de la modification.
- Sous Windows, ajout d'une limitation de la taille des images importées dans les onglets « Personnel » et « Plans » : seules les résolutions jusqu'à 4K (3840 x 2160) sont désormais prises en charge.
- Correction de la fermeture intempestive de la fenêtre d'import du personnel depuis un tableau MS Excel lorsque le fichier sélectionné contenait des formules.
- Correction d'une erreur survenant après la suppression d'un département, lorsque l'opérateur disposait d'une limite de capacité pour ce département.
- Résolution d'un problème pouvant entraîner une erreur d'accès à la base de données après modification du type d'objet d'accès, sans enregistrement préalable avant de passer à un autre objet.
- Suppression de la possibilité de modifier le type Wiegand pour les QR codes dans l'onglet « Personnel ».
- Désormais, lors du changement du type d'identifiant attribué à un employé vers un QR code, le format défini dans le menu « Fichier » – « Paramètres » – « PIN et QR codes » est automatiquement appliqué. La liste déroulante des formats n'est alors plus modifiable.
- Ajout d'un verrouillage de la liste déroulante des formats lors de l'ajout d'un code PIN.
- Ajout d'une nouvelle propriété pour les badges : « Type de badge ». Cette propriété s'affiche dans la fiche de l'objet d'accès et se sélectionne manuellement lors de la délivrance d'un nouveau badge dans l'interface du logiciel Client. Il est désormais possible d'ajouter des cartes, des identifiants mobiles, des codes PIN et des QR codes pour les employés. Le type de badge peut également être spécifié lors de l'import du personnel depuis un fichier xls.
- Après la mise à jour du logiciel, le type « Carte » sera attribué à tous les badges aux formats W26 / W34 / W36 / W37 / W42 / W58 / W58Dec. Si nécessaire, le

type de badge peut être modifié manuellement, ou bien via l'utilitaire de réattribution massive en fonction du commentaire.

- L'image du QR code d'un employé peut désormais être visualisée et copiée dans l'onglet « Personnel », et également être ajoutée au modèle d'impression des badges.
- Correction d'un problème de tri incorrect des modèles de badges lors de leur création et suppression.
- Résolution d'un problème où, lors de la définition d'une date de validité pour un badge, la date et l'heure précédemment définies pour un autre badge étaient automatiquement reprises.
- Correction d'un problème d'enregistrement incorrect de la photo dans la fiche de l'objet d'accès.
- Correction d'une erreur de sauvegarde des modifications de la date de validité du badge et de la durée d'accès lors d'une édition en masse.
- Correction d'une erreur d'accès à la base de données lors de la tentative d'impression du badge d'un employé.
- Résolution d'un problème où, lors de la création successive de nouveaux objets d'accès, le dernier objet pouvait se voir attribuer le numéro de téléphone du précédent.
- Résolution d'un problème où, lors de la copie d'un modèle graphique de badge, les données n'étaient pas reportées dans le nouveau modèle.
- Correction d'une erreur d'accès à la base de données pouvant survenir lors de l'ajout d'un nouveau poste. Désormais, si une tentative est faite de créer un poste dont le nom ne diffère que par la casse, l'utilisation des lettres « e »/« ë » ou par un espace en fin de chaîne, le système avertit de l'existence de ce poste.
- Correction d'un problème qui laissait actif le bouton « Supprimer l'élément sélectionné » lorsque la racine « Site » était sélectionnée dans l'arborescence des départements.

Vidéosurveillance :

- Reprise de la réception des plaques d'immatriculation reconnues par le serveur ISS (SecurOS) sur les postes clients Sigur sous Linux.
- Correction d'un problème de double enregistrement de l'événement de refus d'accès lors de la reconnaissance d'une plaque d'immatriculation d'un objet dont la durée d'accès est limitée.
- HikCentral : amélioration et optimisation de l'intégration. Publication d'une nouvelle version du service d'intégration – 1.1.0.
- Trassir : correction d'un problème susceptible de provoquer un crash du module serveur lors d'une tentative de passage à un point d'accès en mode identification faciale.
- Macroscop : résolution d'un problème de crash du module serveur lorsque l'intégration est active.
- Domination : correction de l'affichage incorrect dans le logiciel Sigur des canaux provenant du système Domination.
- Correction d'un problème où, lors de la modification de la photo d'un employé via l'API REST, celle-ci n'était pas synchronisée avec le système de vidéosurveillance.
- Correction d'une erreur d'autorisation lors de l'ouverture d'une vidéo archivée

dans l'onglet « Archive » du logiciel Client, survenant lors de la sélection d'un événement lorsque le mot de passe de l'opérateur contenait des caractères spéciaux.

Surveillance :

- Correction d'un problème empêchant l'ouverture du logiciel Client après un redémarrage lorsqu'un élément « Matrice des objets à protéger » était présent dans la vue de supervision.
- Pour l'objet « Localisation des employés » dans l'onglet « Surveillance », ajout de la possibilité d'afficher le département de l'objet d'accès.
- Dans l'onglet « Surveillance » du logiciel Client, suppression du filtre d'événement « Carte présentée » dans la fenêtre modale « Afficher les événements », car cet événement ne s'affiche pas dans cet onglet.
- Correction d'un blocage du logiciel Client lorsque le flux RTSP est inaccessible dans l'onglet « Surveillance ».
- Correction de l'affichage incorrect des informations dans l'onglet « Surveillance » lors de la création d'une vue avec un panneau textuel utilisant un encodage HTML et une liste d'événements.
- Résolution d'un problème où, après avoir cliqué sur le bouton « Actualiser » dans l'onglet « Surveillance », les données du personnel dans la fenêtre « Sélection des employés » ne se mettaient pas à jour lors d'une tentative d'autorisation de passage via le plan.

Modes :

- Ajout d'un filtre par points d'accès dans l'onglet « Modes ».
- Correction de l'affichage incorrect des zones dans les paramètres des modes avec calcul du temps de travail basé sur la présence dans les zones spécifiées.
- Résolution d'un problème d'application incorrecte du mode de niveau 1 lors de l'attribution massive d'un mode via l'onglet « Personnel ».
- Correction de problèmes survenant lors de la copie de modes.
- Suppression de la variable CODEKEY_DESC (« Commentaire du badge ») de la liste des variables disponibles pour la configuration des conditions d'application des modes.

Passages répétés : Résolution d'un problème où, lors de la synchronisation des données pour les nouveaux employés, la règle d'interdiction des passages répétés s'appliquait incorrectement, entraînant leur ajout automatique dans les listes de restriction indépendamment des paramètres.

Archive : L'heure de début de la période couverte est désormais définie comme suit : {date actuelle}, heure De : 00:00.

Rapports :

- Ajout d'un nouveau « Rapport sur la discipline au travail », permettant d'obtenir des informations de base sur les heures d'arrivée et de départ des employés. Il

- est disponible dès la version gratuite du logiciel. Ce rapport peut également être joint à un e-mail lors de l'exécution d'une réponse à un événement.
- Le rapport « Liste du personnel » inclut désormais le type de badge.
 - Le « Rapport sur les cartes non utilisées » est désormais intitulé « Rapport sur les badges non utilisés ».
 - Correction du format des cellules contenant des dates ou des heures dans les modèles de rapports.
 - Correction d'un problème de modification du formatage de l'arrière-plan des cellules dans le rapport exporté.
 - Correction d'un filtrage incorrect par employé lors de l'export du tableau de pointage vers 1C.
 - « Rapport unifié sur le temps de travail » :
 - Résolution d'un problème empêchant la génération du rapport lorsqu'un employé avait deux périodes de travail dans son mode.
 - Correction d'une erreur dans le rapport où, lorsque l'option « Indiquer le jour de la semaine dans les dates » était activée, les valeurs de la colonne « Date » ne s'affichaient pas.
 - « Durée de présence dans les zones d'accès » :
 - Correction d'un calcul incorrect du temps de présence dans la zone courante lors de la génération du rapport.
 - Correction d'un problème où le rapport incluait des lignes avec des dates antérieures à la création de l'employé.
 - « Journal des événements système » :
 - Correction de l'affichage incorrect de l'heure de début dans le rapport.
 - Correction d'un problème où le rapport incluait des objets d'accès auxquels l'opérateur n'avait pas accès.
 - « Journal des actions des opérateurs » :
 - Correction d'un problème où, lors de la génération du rapport, le filtrage par objets d'accès fonctionnait incorrectement. Dans la fenêtre de génération du rapport, le nombre de lignes traitées depuis la base de données et le nombre de lignes incluses dans le rapport final sont désormais affichés.
 - Correction de la génération incorrecte du rapport pour un opérateur ayant des restrictions d'accès aux départements et points d'accès.
 - Résolution d'un problème où la période pour laquelle l'opérateur avait précédemment demandé le « Rapport sur les badges non utilisés » pouvait s'afficher de manière incorrecte.
 - La suppression d'un mode est désormais correctement enregistrée dans le journal des actions des opérateurs.
 - Correction d'une erreur dans le rapport « Journal des événements de sécurité », où les événements liés aux zones de sécurité supprimées apparaissaient dans les résultats.

Opérateurs :

- Mise à jour du texte de l'infobulle pour le droit « Connexion par carte ».

- Le paramètre « Identifiant dans SUDIR » n'est désormais affiché dans les droits de l'opérateur qu'en présence de la licence correspondante.
- Correction d'un problème permettant à un opérateur de modifier le texte des notifications dans l'onglet « Personnel » – « Notifications », même si l'envoi des notifications d'approbation de demande était désactivé.
- Résolution d'un problème empêchant la suppression d'une limite de capacité d'un département dans les paramètres des droits d'un opérateur.
- Suppression de la possibilité de modifier le texte des notifications dans l'onglet « Personnel » – « Notifications » pour les opérateurs ne disposant pas des droits requis.
- Correction d'un problème où les groupes de points d'accès n'apparaissaient pas dans le filtre des points d'accès de l'onglet « Personnel » pour les opérateurs disposant d'une restriction d'accès à ces points.
- Correction d'un problème où un opérateur disposant uniquement d'un droit de visualisation du personnel pouvait attribuer et supprimer des modes d'accès.
- Correction d'un problème où un opérateur sans droit de modification des paramètres du matériel pouvait modifier les paramètres dans l'onglet « Équipement » – « Biométrie ».

Réponse à l'événement :

- Le bouton « Tout sélectionner » fonctionne désormais correctement lors de la sélection d'événements pour la création d'une réponse basée sur un événement unifié.
- Correction d'une erreur empêchant l'action « Définir la date de validité du badge » de s'exécuter lors de la configuration d'une réponse sur les événements de type « Accès accordé » et « Accès refusé ».
- Mise en place d'une vérification des droits de l'opérateur lors de la configuration d'une réponse avec envoi de rapport par e-mail. Désormais, les rapports affichés respectent les restrictions d'accès de l'opérateur. Si l'opérateur ne dispose pas des droits sur les rapports associés à des réponses préexistantes, les événements liés à ces réponses ne s'affichent pas dans l'onglet « Événements ».
- Correction d'un problème susceptible d'affecter l'envoi d'un rapport par e-mail lorsque la langue du poste client différait de celle du serveur.
- Correction d'une erreur où, lors de la suppression d'un événement avec des modifications non enregistrées d'une réponse, la confirmation d'enregistrement appliquait les modifications mais l'événement était tout de même supprimé.
- Correction d'une erreur lors de l'envoi par e-mail du rapport sur la discipline au travail, où le fichier était généré dans un format incorrect.

Gestion des badges temporaires pour visiteurs :

- Résolution d'un problème où la création d'un QR code / badge invité via l'API REST ne définissait pas les points d'accès, rendant impossible l'octroi ultérieur des droits d'accès.
- Résolution d'un problème où les photos supplémentaires et les images n'étaient pas correctement traitées avec les QR codes : les données jointes ne

- s'affichaient ni dans l'onglet « Personnel », ni dans le modèle graphique du badge.
- Résolution d'un problème empêchant l'envoi automatique ou manuel d'un e-mail contenant le QR code invité via les fonctions du logiciel Sigur lorsque l'invité avait été créé via l'API REST.
 - Correction de l'absence de valeur dans le champ « Personne visitée » lors de l'envoi du QR code par e-mail. Auparavant, ce champ pouvait rester vide en l'absence de demande associée.
 - Correction du décalage entre la date de début de validité et la date d'émission effective du QR code par rapport aux valeurs spécifiées dans la demande.
 - Correction d'une erreur de gestion de la durée de validité des badges invités : lors des modifications et des changements en masse du personnel, les modifications de la période de validité et des restrictions étaient appliquées incorrectement, entraînant des incohérences entre les onglets « Visiteurs » et « Personnel ». Des vérifications des badges émis ont été ajoutées et la disponibilité des paramètres de durée de validité a été synchronisée.
 - Correction d'un problème où, lors de la modification de la durée de validité d'un badge invité dans l'onglet « Visiteurs », la trace de son émission disparaissait.
 - Correction d'un problème d'enregistrement des valeurs des paramètres supplémentaires lors de l'émission d'un badge invité en utilisant des informations déjà existantes sur le visiteur.
 - Correction d'un problème où les modifications du nom d'un visiteur avec QR code n'étaient pas synchronisées avec la section « Personnel », même après l'actualisation des onglets ou le redémarrage du logiciel Client.
 - Correction d'un dysfonctionnement de la procédure de suppression des données d'un visiteur sélectionné.
 - Correction d'une erreur survenant lors de la création d'une demande sans spécification du type de document dans le service Web de demandes.
 - Correction de l'affichage incorrect de la version du logiciel dans le service Web de demandes.
 - Résolution d'un problème où la page affichant le numéro de demande et le QR code ne s'ouvrait pas lors de la création d'une demande avec approbation automatique via le service Web.
 - Résolution d'un problème où, lors de la consultation d'une demande créée dans le logiciel Client et contenant plusieurs visiteurs, le service Web n'affichait que le QR code du premier visiteur, même si le numéro de document d'un autre participant à la demande était saisi.
 - Correction d'un problème dans le service Web de demandes où la notification de renvoi du QR code était en anglais.
 - Ajout d'une vérification des données dans les champs « Début de validité » et « Fin de validité » lors de la création d'une demande de visite.
 - Ajout d'une nouvelle valeur système « Non sélectionné » pour le type de document du visiteur.
 - Ajout d'une vérification de l'unicité du nom du document lors de la modification. Les espaces en début et fin de nom sont désormais automatiquement supprimés et ne sont pas enregistrés.
 - Correction de l'affichage incorrect de la valeur du paramètre « Personne visitée » dans la fenêtre d'information du QR code émis pour un visiteur. Désormais, si l'employé visité est licencié ou supprimé du système, son nom s'affiche avec le

préfixe « [Licencié] ».

- Correction d'un problème où, lors de l'émission d'un badge pour un visiteur, le champ E-mail était automatiquement pré-rempli avec la valeur example@ex.com.

Reconnaissance de documents :

- Ajout de la prise en charge de l'intégration avec le produit Content AI PassportReader SDK 1.5.5.
- Rétablissement du fonctionnement avec ABBYY PassportReader SDK. Pour un fonctionnement correct lors de la configuration initiale, il est nécessaire d'exécuter le logiciel Client en tant qu'administrateur.

Terminal mobile Sigur :

- Ajout de la possibilité de scanner des codes-barres au format Code 128, ainsi que des badges de type « QR code » via l'application « Terminal mobile ». À cet effet, un nouveau droit d'opérateur pour l'utilisation de cette fonction a été ajouté dans le logiciel Client, et un nouvel événement « Code scanné : <chaîne scannée> » est désormais enregistré dans l'« Archive » et les rapports.
- L'événement « Accès refusé. Numéro de badge inconnu. » est désormais enregistré dans le logiciel Client lorsqu'une carte inconnue est présentée au terminal hors ligne Sigur.
- Correction d'une erreur où, lors du scan d'un QR code invité dans l'application « Terminal mobile », le message « Numéro de badge inconnu » s'affichait, bien qu'un badge valide ait été émis via le service Web de demandes dans le système.

Synchronisation des données :

- Refactorisation de la fonctionnalité de synchronisation des données depuis des sources externes vers la base de données Sigur, permettant d'accélérer le processus de synchronisation.
- Correction d'erreurs et de blocages du logiciel Client survenant lors de la synchronisation d'objets d'accès dont le format de date était incorrect.
- Correction d'un problème où, lors de la synchronisation depuis des sources externes, un même badge pouvait être attribué à différents objets d'accès.
- Correction d'un problème empêchant la synchronisation depuis une base de données externe lorsque le champ « Date de validité du badge » des employés était vide (NULL).
- Correction d'un problème où un employé dont le champ « Date de validité du badge » était vide (NULL) était supprimé ou déplacé dans le dossier « Licenciés » lors de la synchronisation depuis une base de données externe.

Active Directory : Correction d'un problème où, lors de la configuration du verrouillage des comptes Active Directory, la liste des zones autorisées ne s'affichait pas avant un redémarrage du logiciel Client.

Système de paiement :

- Correction d'un blocage du logiciel Client lors de l'ajout ou de la modification en masse du compte de plusieurs objets d'accès.
- Correction de l'affichage incorrect du montant de la transaction lors de la réception d'une notification de modification de compte.
- Correction d'une erreur d'enregistrement de la valeur du compte de règlement pour un QR code invité.

Alarme intrusion et incendie :

- Correction d'un problème provoquant une longue initialisation du logiciel Client lors d'un grand nombre de points d'accès et lorsque l'opérateur avait accès à l'onglet « Sécurité ».
- Correction d'un problème nécessitant un redémarrage du module serveur pour que le statut d'une nouvelle zone de sécurité s'affiche correctement.
- Ajout de l'affichage de trois nouveaux événements liés aux zones de sécurité Sigur : « Échec de l'armement de la zone. Boucle d'alarme non définie », « ... Lecteur occupé » et « ... Zone en cours d'armement ». Ces événements sont disponibles dans les rapports système, l'« Archive » et l'onglet « Surveillance », et peuvent également être utilisés pour configurer des réponses aux événements.
- Les événements des zones de sécurité des contrôleurs Sigur sont désormais affichés non seulement dans le « Journal des événements de sécurité », mais aussi dans l'« Archive » et le « Journal des événements système ». Ce changement s'applique uniquement aux événements nouvellement enregistrés.
- Correction d'un problème empêchant l'obtention du statut d'une zone de sécurité Sigur et son armement.

Biométrie :

- Correction d'un problème de génération et d'enregistrement des templates de veines de paume Biosmart.
- Correction de l'apparition d'un avertissement concernant des modifications non enregistrées dans les paramètres de biométrie Vzor en l'absence de modifications réelles.
- Correction d'un problème de génération du template biométrique Biosmart Quasar survenant lorsque le nom d'utilisateur du système d'exploitation contenait des caractères cyrilliques.

Intégration avec les terminaux de reconnaissance faciale Suprema :

- Optimisation des performances et de la stabilité du service d'intégration.
- Prise en charge de l'intégration avec les serveurs Sigur sous Debian Linux et RHEL.
- Ajout de la prise en charge de PostgreSQL en tant que base de données externe du système de contrôle d'accès.
- Tests de l'interaction avec les périphériques Suprema via OSDP.
- Correction d'un problème provoquant le blocage du logiciel Client et l'apparition d'erreurs dans les logs après l'activation de l'intégration Suprema dans le menu « Fichier » – « Paramètres » – « Biométrie ».

- Résolution d'un problème où le processus supremaservice ne se terminait pas et où le logiciel Client se bloquait après la désactivation de l'intégration sous Linux.
- Correction d'un problème où l'intégration Suprema continuait de fonctionner après l'expiration de la licence.
- Correction de l'affichage incorrect du champ « Type de code de badge pour la génération » dans le menu « Fichier » – « Paramètres » – « Biométrie » – « Suprema ».
- Correction d'un problème empêchant le chargement des templates biométriques dans les terminaux Suprema lorsque des templates Biosmart Quasar étaient présents dans le système.
- Résolution d'un problème susceptible de provoquer un crash du module serveur lors de la tentative d'ajout d'une empreinte digitale via des périphériques Suprema.
- Correction d'un problème de synchronisation des cartes vers les terminaux Suprema lors de la suppression simultanée de la date de validité des cartes pour plusieurs employés.

Intégration avec les terminaux de reconnaissance faciale Hikvision :

- Optimisation du fonctionnement de l'intégration – réduction de la charge sur le serveur et accélération de la synchronisation des données.
- Correction d'une erreur de synchronisation des données avec les terminaux Hikvision lors de l'utilisation du service d'intégration version 1.5 sous Linux avec PostgreSQL.

Intégration avec BAS-IP :

- Correction d'une erreur empêchant la synchronisation des informations du personnel avec la mémoire des panneaux d'appel.
- Correction d'un problème de synchronisation des badges de type « ID mobile » avec la mémoire des panneaux d'appel.

Intégration avec la boîte à clés Keyguard :

- Suppression de la demande persistante d'enregistrement des modifications lors de la sélection des règles d'accès dans le logiciel Client, qui apparaissait même en l'absence de modifications.
- Correction de l'affichage incorrect de la liste des règles d'accès aux clés lors de l'attribution des droits aux employés.

Intégration avec Dormakaba : Correction d'un problème où la liste des points d'accès et les événements de passage n'étaient pas synchronisés depuis le logiciel Matrix.

Protocole d'intégration WebDel : Correction d'une erreur où, en cas de refus d'accès suite à une décision d'un système externe, l'événement « Accès refusé. Le mode ne permet pas le passage » était généré.

REST API :

- Ajout de nouveaux types d'événements renvoyés en réponse aux requêtes GET /api/v1/events, GET /api/v1/events/types et GET /api/v1/events/parsed :
 - « Changement d'état de l'alimentation du contrôleur » (DC_STATUS).
 - « Changement d'état de la batterie du contrôleur » (BATTERY_STATUS).
 - « Échec du changement de mode du point d'accès » (AP_MODE_DENY).
- Le type d'événement VOLTAGE_STATUS n'est plus utilisé.
- Ajout de l'attribut armingMethod à l'événement « État de la zone de sécurité » (ALARM_LINE_STATUS). Cet attribut est renvoyé lors de la requête GET /api/v1/events/parsed si la zone a été armée à l'aide du lecteur Sigur MK100.
- Ajout de nouvelles causes pour certains types d'événements renvoyés en réponse à la requête GET /api/v1/events/parsed :
- Pour l'événement PASS_DENY :
 - « Access period expired or not started » (« Accès refusé. La période d'accès n'a pas commencé ou est déjà expirée ») ;
 - « Waiting for confirmation of access point mode change » (« Accès refusé. En attente de confirmation du changement de mode du point d'accès »).
- Pour l'événement WAITING_FOR_RULE_STAGE :
 - « Waiting for second access object » (« En attente du second objet pour l'accès ») ;
 - « Waiting for confirmation of access point mode change » (« En attente de confirmation du changement de mode du point d'accès »).
- Pour l'événement MNG_STATE_CHANGED :
 - « PIN », « PIN AND PASS » (changement du mode du point d'accès via un code PIN ou un code PIN avec confirmation par badge).
- Ajout de nouveaux types d'événements renvoyés en réponse aux requêtes GET /api/v1/events, GET /api/v1/events/types et GET /api/v1/events/parsed :
 - « Échec de l'armement de la zone » (ALARM_LINE_DENY) ;
 - « Événement d'état de la zone de sécurité » (ALARM_LINE_STATUS).
- Pour l'événement WAITING_FOR_RULE_STAGE, ajout d'une nouvelle cause : « En attente de confirmation de l'armement de la zone » (« Waiting for confirmation of zone arming »). Ajout de l'attribut alarmZoneId dans l'objet data, et de l'objet alarmZone dans additionalData.
- Ajout de nouveaux endpoints pour la gestion des cartes invitées et des QR codes, la gestion des émissions de cartes invitées, ainsi que la gestion des QR codes et des codes PIN des employés.
- Ajout du champ tabid (numéro du département) dans les paramètres de l'objet departments, accessible également lors de la création et de la modification des départements.
- Ajout de la possibilité d'ajouter, modifier et supprimer le MFUID des cartes.
- Mise à jour des requêtes pour les groupes Employees et Official Vehicles :
 - La période d'accès de l'objet d'accès et le code PIN de vérification peuvent

- désormais être spécifiés lors de la création d'un objet d'accès, et peuvent être modifiés et récupérés via l'API REST (ajout des attributs `accessStartTime`, `accessEndTime` et `verificationPin`) ;
- Ajout de l'objet identifiants dans le corps de certaines requêtes et réponses, contenant tous les identifiants de l'objet d'accès ;
 - Élargissement des filtres disponibles : pour le filtrage par paramètres supplémentaires dans la requête `GET /api/v1/employees`, les opérateurs `IN`, `NEQ`, `IS_NULL`, `IS_NOT_NULL` et `CONTAINS` sont désormais pris en charge.
 - Modification de la logique de gestion des cartes avec l'attribut `guestApplicable=true`.
 - Désormais, les requêtes `GET api/v1/cards` et `GET api/v1/cards/{id}` ne renvoient que les badges de type « Carte ». Pour consulter les identifiants mobiles, QR codes et codes PIN des objets d'accès, il convient d'utiliser les requêtes `GET /api/v1/employees` et `GET /api/v1/employees/{id}`.
 - Optimisation du traitement des requêtes `GET /api/v1/events/parsed` et `GET /api/v1/events` lors de l'utilisation d'un filtre temporel.
 - Correction d'erreurs survenant lors de la génération d'un QR code visiteur avec la requête `PUT /api/v1/guests/{id}/QR`.
 - Correction : dans la réponse à la requête `GET /api/v1/guests`, l'attribut `guestCardId` était présent pour les visiteurs de type « QR », permettant d'obtenir des informations via la requête `GET /api/v1/guestcards/{id}`.
 - Correction de la représentation incorrecte des champs `value` et `formattedValue` dans la réponse à la requête `GET api/v1/guestcards/{id}`.
 - Correction : il était possible de supprimer les modes par défaut via la requête `DELETE /api/v1/accessrules/{id}`.
 - Résolution d'un problème de traitement incorrect de la requête `GET /api/v1/bindings/employees-guestcards` lors de l'utilisation des paramètres `includeFields`, `excludeFields`, `limit` et `offset`.
 - Correction d'une erreur HTTP 500 lors de l'exécution de la requête `GET /api/v1/guestcards` avec les paramètres `value` et `sortBy`. Le tri par les champs `assigned` et `formattedValue` n'est pas pris en charge pour cette requête.
 - Correction d'une erreur HTTP 500 lors de la tentative de suppression d'une valeur de paramètre supplémentaire obligatoire via la requête `PUT /api/v1/employees/{id}`.
 - Correction de la validation des valeurs des cartes lors de leur création via l'API REST. Il n'est désormais plus possible de créer une carte ou un QR code avec un code nul.
 - Résolution d'un problème de traitement des événements qui pouvait entraîner une réponse vide à la requête `GET /api/v1/events/parsed`.
 - Correction d'une erreur HTTP 500 lors de l'exécution de la requête `GET /api/v1/events` sur un serveur de contrôle d'accès sous Linux.
 - Correction : la requête `GET /api/v1/employees` renvoyait tous les employés si un paramètre supplémentaire inexistant était utilisé dans la recherche. Désormais, le serveur renvoie un statut HTTP 422 dans ce cas.
 - Correction d'un problème où le filtrage par `accessObjectId` dans la requête `GET /api/v1/events/parsed` ne fonctionnait pas avec PostgreSQL.
 - Désormais, la requête `GET /api/v1/employees` exécutée par un opérateur ayant une restriction d'accès totale aux départements renvoie une réponse 200 OK

- avec un résultat vide.
- Correction du fonctionnement du filtre par tabid dans la requête GET /api/v1/employees.

Correction d'autres erreurs et optimisation du système :

- Correction d'un problème empêchant le lancement du logiciel « Gestion du serveur ».
- Élimination d'autres causes susceptibles d'entraîner des blocages et une baisse de performance du système.
- Correction d'un problème pouvant provoquer le blocage de l'onglet « Configuration des périphériques » – « Configurer les périphériques IP » dans le logiciel « Gestion du serveur ».
- Correction d'un problème de lenteur de l'onglet « Personnel » lors de l'utilisation de l'intégration avec Biosmart.
- Correction d'erreurs liées à la mise à jour tardive des informations sur la licence chargée dans le logiciel Client.
- Clarification du texte d'aide pour le paramètre « Multiplicateur du résultat de l'alcootest » dans les paramètres des alcootests connectés aux contrôleurs Sigur via l'interface Wiegand.

2. Contacts

Pour toute question ou assistance, veuillez nous contacter en utilisant les informations fournies :

Site web : www.sigur.com

Demandes générales : info@sigur.com

Support technique : support@sigur.com