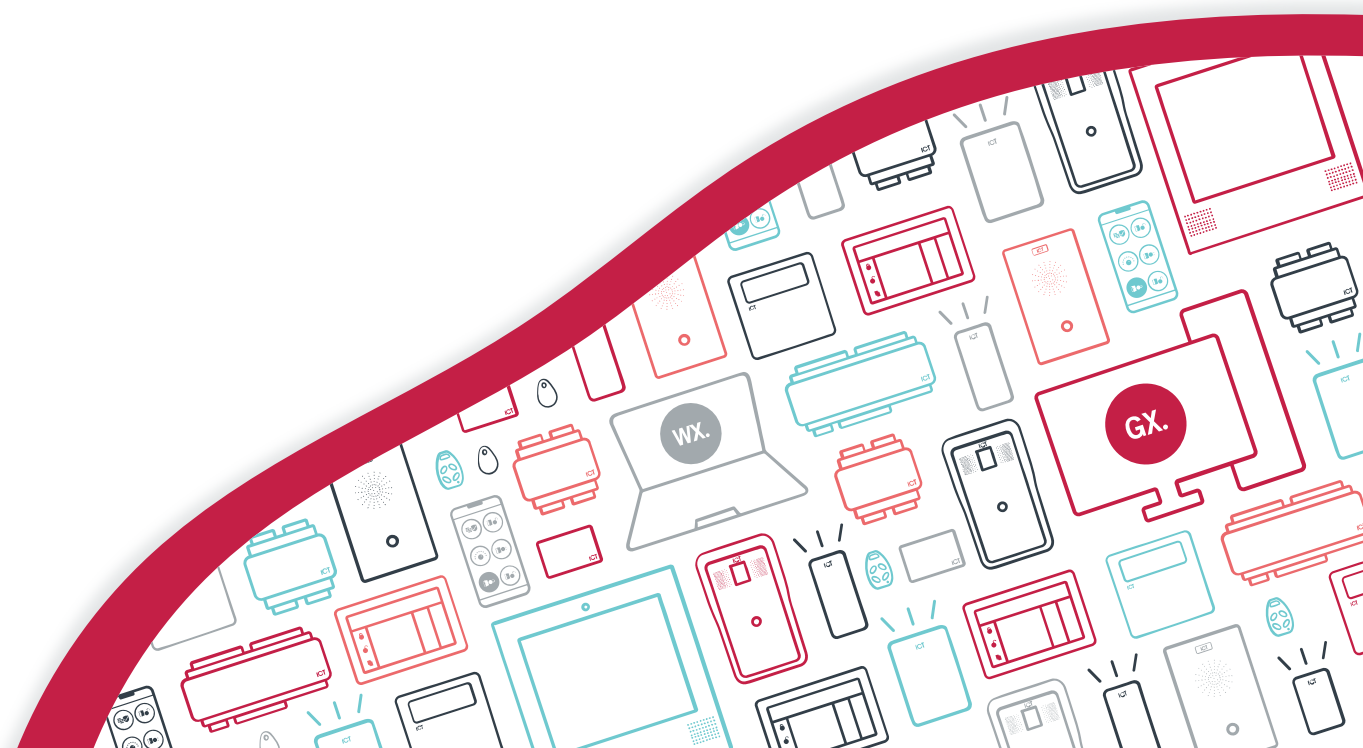
PRT-GX-SRVR

Protege GX

Manuel d'installation



Dernière publication en 06-mars-24 15:28.

Contenu

À propos de ce manuel

Ce que couvre ce manuel

Ce manuel contient des informations et des instructions sur :

- Exigences du système
- Fonctionnalités sous licence
- Installation de Protege GX
- Connexion d'un contrôleur dans Protege GX
- Configuration initiale du site et activation de la licence
- Effectuer des sauvegardes du système

Qui devrait lire ce manuel

Ce manuel est destiné à ceux qui installeront et configureront Protege GX.

Pour obtenir des instructions sur l'utilisation et la programmation de Protege GX, reportez-vous au Manuel d'opération de Protege GX.

Ce que vous devez déjà savoir

Ce manuel suppose que vous avez une connaissance pratique intermédiaire du système d'exploitation Microsoft Windows. Les détails des fonctionnalités de base de Windows sortent du cadre de ce document.

Pour de l'assistance, veuillez contacter l'assistance technique de ICT par courriel ou téléphone. Référez-vous au site Web de ICT (www.ict.co) pour des renseignements supplémentaires.

Avant de commencer

Ce manuel fournit des instructions sur l'installation et la configuration de Protege GX. Il comprend également des informations sur la configuration système requise et les procédures de sauvegarde.

Veuillez prendre un moment pour lire le matériel de cette section avant l'installation.

Exigences du système

Les exigences matérielles suivantes sont basées sur la taille et les exigences de communication de l'installation.

Une installation avec les fonctions de base de Protege GX peut fonctionner sur la machine spécifiée. Une machine plus performante est recommandée lors de l'utilisation de fonctionnalités graphiques, d'identité avec photo et d'automatisation. Utilisez les spécifications de performances adaptées à votre installation.

Installation du contrôleur standard

Une installation standard Protege GX comprend jusqu'à 10 contrôleurs système qui communiquent avec jusqu'à 16 modules chacun. Les contrôleurs sont connectés via Ethernet.

Exigence de matériel de serveur - installation standard

- Machine Intel® Dual Core 2.8 GHz
- 4 Go de RAM
- 40 Go d'espace disque libre
- Souris/clavier
- Ethernet 10/100 MBs

Installation de plusieurs contrôleurs

Une installation à plusieurs contrôleurs se compose de plus de 10 contrôleurs, qui peuvent fonctionner comme plusieurs sites exécutant des contrôleurs individuels, ou comme un site unique exécutant plusieurs contrôleurs. Chaque contrôleur peut avoir un nombre indéfini de modules connectés. La connexion aux contrôleurs peut utiliser tout type de supports de communication et peut communiquer indépendamment ou à la demande.

Pour de meilleures performances, connectez-vous à l'aide d'une connexion Ethernet 10/100MB ou similaire sur un réseau local LAN ou WAN.

Exigences de matériel de serveur - contrôleur multiple

- Intel® Quad Core, 2,8 GHz ou supérieur
- 8 Go de RAM
- 100 Go d'espace disque libre
- Souris/clavier
- Dual Ethernet 10/100 MBs

Systèmes d'exploitation pris en charge

Système opérateur	Édition	Architecture
Microsoft Windows Server 2022	Standard, Datacenter	64 bits
Microsoft Windows Server 2019	Standard, Datacenter	64 bits
Microsoft Windows Server 2016	Standard, Datacenter	64 bits
Microsoft Windows 11	Pro, Business, Enterprise	64 bits
Microsoft Windows 10	Professional, Enterprise	32/64 bits

Environnements de serveur virtuel

Le serveur Protege GX est pris en charge sur les environnements de serveur virtuel. Cependant, ICT se réserve le droit de demander au client la réplication de toute erreur dans un environnement non virtuel.

Lors de l'installation dans des environnements de serveurs virtuels, des précautions particulières doivent être prises pour s'assurer que la configuration système requise (consultez page précédente) est satisfaite par le matériel virtualisé. La machine virtuelle doit être soigneusement examinée en ce qui concerne les ressources et les performances avant de terminer toute installation.

Versions compatibles avec SQL Server

L'application Protege GX utilise un moteur de base de données SQL ouvert non propriétaire pour stocker et partager des informations. Le logiciel est compatible avec SQL 2014, 2016 et 2017 dans les éditions Standard, Express et Enterprise.

L'édition Express est une édition réduite et gratuite de SQL Server qui comprend le moteur et les fonctionnalités essentielles de base de données. La version Express de SQL supporte jusqu'à 10 Gb.

Pour obtenir SQL ou SQL Express, téléchargez le programme d'installation approprié sur le site Web de Microsoft. Il est également recommandé de télécharger SQL Server Management Studio de Microsoft afin de configurer SQL. Téléchargez la dernière version en disponibilité générale (GA) de SSMS à partir du site Web de Microsoft.

Installation de la base de données sur serveur SQL distant

La plate-forme Protege GX prend en charge les installations du serveur SQL à distance. Une attention particulière doit être accordée aux besoins en bande passante, qui sont vitaux pour le bon fonctionnement du système.

Lorsque Protege GX a été installé sur un environnement de serveur SQL distant, l'assistance technique ICT se réserve le droit de demander la réplication client de toute erreur dans un environnement de serveur SQL local.

Configuration requise pour le poste de travail client

Exigence de matériel recommandée - client standard

- Machine Intel® Dual Core 3 GHz
- 4 Go de RAM
- 40 Go d'espace disque libre
- Carte vidéo compatible DirectX 10
- Souris/clavier
- Ethernet 10/100/1000 MBs

Exigences de performance supplémentaires

Lors de la communication avec des sites distants, du matériel supplémentaire peut être nécessaire, comme des modems, des modems fibre ou des routeurs. Celles-ci sortent du cadre de ce document.

La configuration requise pour le serveur et les machines clientes peut varier en fonction de l'utilisation prévue. Lors de l'exécution des fonctions graphiques, d'identité avec photo et d'automatisation à partir du poste de travail client, une machine plus performante peut être nécessaire pour garantir que les plans d'étage et les tâches d'identification avec photo peuvent fonctionner. Lorsque la machine serveur n'est pas utilisée pour la connexion locale avec l'interface utilisateur Protege GX, une configuration de carte vidéo moins performante peut être sélectionnée.

L'interface utilisateur Protege GX prend en charge les résolutions d'écran standard suivantes :

- 1280 x 1024
- 1400 x 1050
- 1600 x 1200
- 1680 x 1050
- 1920 x 1080

La sélection d'autres résolutions d'écran peut produire des résultats d'affichage inattendus.

Intégrations DVR/NVR

Lors de l'intégration avec un système DVR/NVR, il aura sa propre configuration système minimale. Il est important de vérifier auprès du fabricant avant l'installation pour vous assurer que votre machine répond à ces spécifications.

Prérequis

Les composants tiers suivants doivent être installés avant l'installation de Protege GX :

- La dernière version de Microsoft .NET Framework 4.

  Au moment de la rédaction de ce document, la dernière version disponible est Microsoft .NET Framework 4.8.1

- Microsoft SQL Server (requis sur la machine serveur uniquement) : le logiciel est compatible avec SQL 2014, 2016 et 2017 dans les éditions Standard, Express et Entreprise.

  Notez que Microsoft SQL Server possède son propre ensemble de conditions préalables, qui sont spécifiques à la version de Microsoft SQL Server en cours d'installation. Vous devez également vous assurer que la version de SQL Server est compatible avec la version de Windows sur laquelle il sera installé. Veuillez consulter le site Web de Microsoft pour connaître les conditions préalables, les fichiers associés et les instructions d'installation de votre version particulière.

Exigences relatives aux autorisations administratives

Pour terminer l'installation avec succès, vous devez disposer des privilèges administratifs locaux sur le(s) poste(s) de travail sur lequel vous effectuez l'installation. Vous n'avez pas besoin des autorisations d'administration de domaine.

Les autorisations d'administrateur ne sont pas nécessaires pour ouvrir (exécuter) un client qui se connecte au serveur Protege GX. Vous pouvez exécuter l'application cliente en tant qu'utilisateur limité sur n'importe quel poste de travail.

Autorisations de service minimales

Sur certains sites, il n'est pas préférable d'accorder des autorisations administratives complètes aux services Protege GX.

Les services de Protege GX peuvent utiliser un compte de service avec les autorisations minimales suivantes accordées à la fois pour la base de données principale de Protege GX et la base de données d'événements :

- CONNECT
- EXEC
- db_datareader
- db_datawriter

Autorisations de service minimales pour le chiffrement des colonnes

Certaines fonctions de Protege GX utilisent la fonction Toujours chiffré de SQL Server pour chiffrer les colonnes de la base de données :

- Chiffrement du NIP
- Verrouillage sans fil ICT

Pour configurer et utiliser les colonnes chiffrées, vous devez disposer d'autorisations supplémentaires en plus des autorisations minimales indiquées ci-dessus.

Pour plus d'informations, consultez la note d'application 306 : configuration du chiffrement du NIP de l'utilisateur dans Protege GX ou le guide de configuration de la serrure sans fil dans Protege.

- Pour **établir** le chiffrement des colonnes, les autorisations suivantes sont requises :
  - VIEW ANY COLUMN MASTER KEY DEFINITION
  - VIEW ANY COLUMN ENCRYPTION KEY DEFINITION
  - ALTER ANY COLUMN MASTER KEY
  - ALTER ANY COLUMN ENCRYPTION KEY
  - Lisez et écrivez l'accès à la liste de certificats de local machine > Personal
  - Lisez et écrivez l'accès à la liste de certificats de Local machine > Trusted Root Certification Authorities
- Pour **utiliser** le chiffrement des colonnes, les autorisations suivantes sont requises :
  - VIEW ANY COLUMN MASTER KEY DEFINITION
  - VIEW ANY COLUMN ENCRYPTION KEY DEFINITION
  - Lisez l'accès à la liste de certificats de Local machine > Personal

Les autorisations qui ne sont pas requises pour utiliser le cryptage NIP peuvent être désactivées après la configuration initiale.

Licence

Protege GX utilise un modèle de licence modulaire qui est à la fois flexible et évolutif. Cela vous permet d'acheter uniquement les fonctionnalités dont vous avez besoin, mais aussi d'étendre facilement votre système en ajoutant des fonctionnalités supplémentaires quand vous en avez besoin.

Pendant l'installation, vous serez invité à entrer le numéro de série de votre logiciel (SSN). Tous les produits logiciels Protege GX doivent également être enregistrés. Cela s'effectue en se connectant au service d'enregistrement Web à partir du serveur ou en obtenant et en chargeant un fichier de licence (consultez la page 27). Si des fonctionnalités supplémentaires sont achetées à une date ultérieure, répétez simplement le processus de licence.

Éléments et fonctionnalités sous licence

Protege GX propose deux packs de licences distincts et un modèle de licence flexible qui réduit les barrières à l'entrée et évolue à mesure que les sites se développent.

La **Licence de démarrage de Protege GX** est conçue pour rendre la mise en œuvre plus rentable. Cette option est idéale pour les petites organisations qui souhaitent adopter une solution de niveau entreprise tout en conservant la flexibilité d'étendre leur système Protege GX à mesure que leur site se développe. La licence de démarrage est fournie avec 10 portes et est limitée à 100 portes. Pour obtenir une licence pour plus de 100 portes, vous devez passer à une licence standard.

La **Licence standard pour Protege GX** est idéale pour les grandes organisations avec des exigences système plus élevées. La licence standard comprend 50 portes, 1 caméra et 1 connexion d'opérateur simultanée, et ajoute également les actions de calendrier et les courriels sur les fonctionnalités d'événement.

Les deux packs de licences incluent de puissantes fonctionnalités de création de rapports, une , des pages d'état personnalisables, des plans d'étage graphiques et aucune restriction sur le nombre d'utilisateurs, d'événements, de calendriers, de zones ou de modules matériels. Le tableau suivant indique les fonctionnalités et l'étendue incluses dans chaque licence. Pour savoir comment étendre les fonctionnalités et la taille de votre système, reportez-vous à la section Fonctionnalités optionnelles ci-dessous.

Fonctionnalité	Licence de démarrage	Licence standard
Connexions clients simultanées	1	1
Portes *	10	50
Sites	1	Illimité
Contrôleurs	Illimité	Illimité
Utilisateurs	Illimité	Illimité
Caméras	0	1
DVR	N/A	Illimité
Fonctionnalité des actions du calendrier	Désactivé	Activé
Courriel sur la fonctionnalité d'événement	Désactivé	Activé
Fonctionnalité du service Web de SOAP	Activé	Activé
Fonctionnalité client Web	Désactivé	Activé
Opérateurs Web	0	3

* Les serrures sans fil sont considérées comme des portes et sont incluses dans le total des portes.

Des licences supplémentaires pour client, porte et caméra peuvent être achetées pour étendre la configuration originale. Celles-ci ne sont requises qu'en cas de dépassement de la quantité incluse dans la licence actuelle du site.

Une licence de démarrage supportera jusqu'à 100 portes (filaires ou sans fil), les fonctionnalités listées comme « Activées » dans le tableau comparatif et toutes les intégrations non marquées d'un * dans la section des fonctionnalités optionnelles. Pour une extension supplémentaire, y compris l'intégration pour caméras, une mise à niveau vers une licence standard est requise.

Limites maximales

Les portes ont une limite « maximale » de 1000, et une fois cette limite atteinte, le nombre de portes autorisées devient illimité. Cela signifie que le nombre maximum de licences de porte supplémentaires requises (en plus d'une licence standard) serait de 950.

Les caméras ont une limite « maximale » de 500, et une fois cette limite atteinte, le nombre de caméras autorisées devient illimité. Cela signifie que le nombre maximum de licences de caméra supplémentaires requises (en plus d'une licence standard) serait de 499.

Fonctionnalités optionnelles

Des fonctionnalités optionnelles et un modèle de licence flexible vous permettent d'ajouter des fonctionnalités en fonction de l'évolution de vos besoins. Des packs de licences flexibles sont disponibles pour les portes, les caméras et de nombreuses autres fonctionnalités et forfaits d'intégration, vous permettant d'étendre facilement votre système à mesure que votre entreprise se développe.

Code du produit	Description
Extension logiciel de Protege GX	
PRT-GX-CLNT	**Licence client de Protege GX** : Fournit une connexion d'opérateur simultané supplémentaire (client lourd).
PRT-GX-WEB-OPR	**Licence d'opérateur de Protege GX** : Fournit une connexion d'opérateur simultané supplémentaire (client lourd).
PRT-GX-DB-SYNC	**Licence de Service de synchronisation des données ICT** : Permet la synchronisation des données utilisateur à partir de systèmes tiers utilisés pour la gestion des visiteurs, la gestion des ressources humaines, les gymnases et centres de remise en forme, le fret et la livraison et l'éducation.
PRT-GX-AD-OPR	**Licence Protege GX d'intégration d'opérateur d'active Directory** : Permet aux opérateurs de se connecter automatiquement à Protege GX à l'aide de leurs informations d'identification Windows, offrant une authentification centralisée et la commodité de la connexion unique.
PRT-GX-AD-USR	**Licence de Protege GX d'intégration de l'utilisateur d'Active Directory** : Permet aux organisations de créer et de gérer automatiquement les utilisateurs de Protege GX en fonction d'un groupe de sécurité Windows Active Directory défini.
PRT-GX-DOR-10	**Licence de Protege GX pour 10 portes** : Augmente le nombre de portes sous licence sur le serveur de Protege GX de 10 portes supplémentaires.
PRT-GX-DOR-50	**Licence de Protege GX pour 50 portes** : Augmente le nombre de portes sous licence sur le serveur de Protege GX de 50 portes supplémentaires.
PRT-GX-VOIP-10	**Licence de Protege GX pour 10 SIP Station** : Licence pour 10 stations d'interphonie VoIP Protege GX par instance de PRT-GX-SRVR. Chaque station VoIP sous licence est capable de passer des appels vers les stations de travail client Protege GX et de fonctionner comme interphone principal via l'interface utilisateur de la station de travail.
PRT-GX-VIM	**Licence de Protege GX pour module d'intégration des visiteurs** : Permet aux organisations d'enregistrer et de suivre les visiteurs directement à partir de l'interface Protege GX, éliminant ainsi le besoin d'un système de gestion des visiteurs distinct.

Code du produit	Description
PRT-GX-MUST	**Licence de Protege GX pour rapports Assemblement** : Permet aux organisations de créer des rapports Assemblement pour identifier rapidement qui se trouve dans une zone définie en répertoriant tous les utilisateurs qui sont entrés ou sortis via les lecteurs associés à une porte.
PRT-GX-TNA	**Licence de Protege GX pour temps et présence** : Permet aux organisations de créer des rapports de temps et de présence qui utilisent les données d'accès de Protege GX pour fournir des informations sur les mouvements d'entrée et de sortie du personnel, en aidant à la paie et à la gestion des ressources humaines.
PRT-GX-PHOTO	**Protege GX Licence avec photo d'identité** : Permet aux opérateurs de créer et de personnaliser des modèles de photo d'identité et de définir la mise en page et les informations incluses sur la carte ou l'étiquette d'un utilisateur.
PRT-GX-SOAP-SDK	**Kit de développement logiciel de service Web SOAP de Protege GX** : Fournit un moyen simple d'accéder à Protege GX via une plate-forme Web. Créez votre propre application avec une interface personnalisée ou intégrez-la à un appareil physique pour déverrouiller les portes et désarmer les aires. Compatible avec plusieurs plates-formes ou systèmes d'exploitation. L'utilisation du SDK SOAP nécessite la signature d'un accord de non-divulgation.

Les fonctionnalités marquées par un astérisque ***** ne sont pas supportées par la licence de démarrage. Une mise à niveau vers une licence standard est requise pour implémenter ces fonctionnalités optionnelles.

Code du produit	Description
Licences d'intégration de Protege GX	
* PRT-GX-CAM-10	**Licence de Protege GX pour 10 caméras**: 10 caméras supplémentaires, autonomes ou à utiliser avec les systèmes DVR/NVR pris en charge.
* PRT-GX-CAM-50	**Licence de Protege GX pour 50 caméras**: 50 caméras supplémentaires, autonomes ou à utiliser avec les systèmes DVR/NVR pris en charge.
PRT-GX-TPR-IF	**Licence de Protege GX d'interface de lecteur tiers**: Permet l'intégration de lecteurs de cartes tiers et d'autres dispositifs d'identification via Ethernet ou l'interface de lecteur générique. Une licence est requise pour chaque lecteur intelligent configuré.
-	**ICT Licence de lecteur intelligent RS-485**: Permet l'intégration de lecteurs de cartes tiers via l'interface de lecteur RS-485. Une licence est requise pour chaque lecteur intelligent configuré.
PRT-GX-BIO-SP	**Licence de Protege GX d'intégration biométrique Suprema**: Permet l'utilisation de dispositifs Suprema BioEntry pour le contrôle d'accès directement dans Protege GX. Une licence est requise pour chaque lecteur Suprema connecté au système.
PRT-GX-BIO-PR	**Licence de Protege GX d'intégration biométrique de Princeton Identity**: Permet l'intégration avec le système de Pronceton Identity pour l'identification des utilisateurs et un contrôle d'accès intégré. Une licence est requise pour chaque lecteur de Princeton Identity connecté au système.

Code du produit	Description
PRT-GX-DOR-ALEG	**Licence de Protege GX pour porte sans fil IP Allegion**: Permet la connexion d'une porte sans fil Allegion supportée à un contrôleur de système. Une licence est requise pour chaque porte sans fil connectée. Nécessite un concentrateur Allegion RS-485 compatible.
PRT-GX-DOR-AP	**Protege GX Licence Aperio RS-485 pour porte sans fil** : Permet la connexion d'une porte sans fil Aperio supportée à un contrôleur de système. Une licence est requise pour chaque porte sans fil connectée. Nécessite un concentrateur Aperio RS-485 compatible.Nécessite un concentrateur Aperio RS-485 compatible.
PRT-GX-DOR-AP-IP	**Protege GX Licence Aperio IP pour porte sans fil** Permet la connexion d'une porte sans fil Aperio supportée à un contrôleur de système. Une licence est requise pour chaque porte sans fil connectée. Nécessite un concentrateur Aperio RS-485 compatible.
PRT-GX-DSR-DOR	**Licence de Protege GX pour porte sans fil IP ASSA ABLOY DSR**: Permet la connexion d'une porte système ASSA ABLOY DSR prise en charge à un contrôleur système. Une licence est requise pour chaque serrure de porte IP connectée.
* PRT-GX-DOR-IP	**Licence de Protege GX pour porte Salto SHIP**: Permet la connexion d'une porte sans fil Salto SHIP supportée à un contrôleur de système. Une licence est requise pour chaque porte sans fil connectée. Nécessite un concentrateur IP Salto RS-485 compatible.
* PRT-GX-DOR-SL	**Licence de Protege GX pour porte Salto SALLIS**: Permet la connexion d'une porte sans fil Salto SALLIS supportée à un contrôleur de système. Une licence est requise pour chaque porte sans fil connectée. Nécessite un concentrateur IP Salto SALLIS RS-485 compatible.
PRT-GX-INOV	**Licence de Protege GX pour entrée IP Inovonics**: Permet l'intégration avec les dispositifs de détection sans fil Inovonics.
PRT-GX-VING-HLI	**Licence de Protege GX d'intégration ASSA ABLOY VingCard**: Permet l'intégration avec le système VingCard VisiOnline.
* PRT-GX-ELV-HLI-KN	**Licence de Protege GX d'interface de haut niveau pour ascenseur KONE**: Permet l'intégration avec des systèmes d'ascenseur HLI KONE nouveaux ou existants. Une licence est requise par serveur de destination KONE pour être intégrée à Protege GX.
* PRT-GX-ELV-HLI-MCE	**Licence de Protege GX d'interface de haut niveau pour ascenseur MCE**: Permet l'intégration avec des systèmes d'ascenseur HLI MCE nouveaux ou existants. Une licence est requise par serveur de destination MCE pour être intégrée à Protege GX.
* PRT-GX-ELV-MLI-OT	**Licence de Protege GX d'interface de niveau moyen pour ascenseur Otis**: Permet l'intégration avec des systèmes d'ascenseur MLI Otis nouveaux ou existants. Une licence est requise par serveur de destination Otis pour être intégrée à Protege GX.
* PRT-GX-ELV-HLI-OT	**Licence de Protege GX d'interface de haut niveau pour ascenseur Otis**: Permet l'intégration avec des systèmes d'ascenseur HLI Otis nouveaux ou existants. Une licence est requise par serveur de destination Otis pour être intégrée à Protege GX.

Code du produit	Description
* PRT-GX-ELV-EMS-OT	**Licence de Protege GX de système de gestion pour ascenseur Otis**: Permet l'intégration avec des systèmes d'ascenseur EMS Otis nouveaux ou existants. Une licence est requise par serveur de destination Otis pour être intégrée à Protege GX.
* PRT-GX-ELV-HLI-SC	**Licence de Protege GX d'interface de haut niveau pour ascenseur Schindler**: Permet l'intégration avec les systèmes d'ascenseur HLI Schindler PORT Technology nouveaux ou existants. Une licence est requise par serveur de destination Schindler PORT à intégrer avec Protege GX.
* PRT-GX-ELV-HLI-TK	**Licence de Protege GX d'interface de haut niveau pour ascenseur ThyssenKrupp**: Permet l'intégration avec des systèmes d'ascenseur HLI Thyssenkrupp nouveaux ou existants. Une licence est requise par serveur de destination ThyssenKrupp à intégrer avec Protege GX.
PRT-GX-KWI	**Licence de Protege GX d'interface de haut niveau pour KeyWatcher TOUCH**: Permet l'intégration du serveur KeyWatcher TOUCH avec Protege GX, permettant la gestion des utilisateurs, des opérateurs, des horaires et des niveaux d'accès dans les armoires KeyWatcher à partir de Protege GX.
PRT-GX-KSI	**Protege GX Licence d'interface de haut niveau CIC Technology KeySecure**: Permet l'intégration du serveur KeySecure avec Protege GX, permettant la gestion des utilisateurs, des horaires et des niveaux d'accès dans les armoires C.Q.R.iT à partir de Protege GX.
PRT-GX-RED	**Licence de Protege GX de détecteur IP Redwall**: Permet l'intégration avec les détecteurs à balayage laser Optex Redwall.
PRT-GX-BAC-CORE	**Protege GX Licence de service BACnet Core**: Permet l'intégration BACnet avec Protege GX, ce qui permet de surveiller et de contrôler les dispositifs d'automatisation des bâtiments conformes aux normes industrielles. La licence du service de base couvre l'intégration de base et les 32 premiers objets connectés.
PRT-GX-BAC-PL32	**Protege GX Licence BACnet 32 objets**: Chaque licence permet la connexion de 32 objets BACnet supplémentaires en plus de ceux fournis par la licence de base.

Installation

La section suivante décrit les étapes requises pour installer Protege GX afin que vous puissiez être rapidement opérationnel.

1. Installez les prérequis (consultez ci-dessous)
2. Installez le serveur Protege GX (consultez page suivante)
3. Installez le client Protege GX sur n'importe quel poste de travail distant (consultez la page 17)
4. Configurez les paramètres de sécurité recommandés (consultez la page 19)
5. Connectez le contrôleur Protege GX (consultez la page 28)
6. Effectuer la configuration initiale du site (consultez la page 27)

Vous devez disposer des privilèges administratifs locaux sur le serveur et le ou les postes de travail sur lesquels vous effectuez l'installation.

Aperçu de l'installation

Protege GX utilise une architecture client/serveur. Chaque installation comprend un serveur qui contient la base de données principale du système et les services Protege GX. Dans la plupart des cas, le logiciel client sera également installé. L'application cliente peut ensuite être installée sur des postes de travail supplémentaires, ce qui permet à plusieurs opérateurs d'accéder au système. Ces postes de travail se connectent à la base de données et aux services sur le serveur Protege GX.

Installation des prérequis

Avant que Protege GX puisse être installé, le logiciel requis doit être installé.

- Microsoft .NET Framework
- Microsoft SQL Server

Installation de Microsoft .NET Framework

Chaque poste de travail exécutant le logiciel client Protege GX requiert la dernière version de Microsoft .NET Framework 4.

Au moment de la rédaction de ce document, la dernière version disponible est Microsoft .NET Framework 4.8.1

Pour installer Microsoft .NET 4.0 Framework

1. Téléchargez le dernier programme d'installation de .NET Framework 4 sur le site Web de Microsoft.
2. Exécutez le fichier d'installation de .NET Framework. Cela lance le programme d'installation de Microsoft .NET Framework 4.
3. Lisez et acceptez le contrat de licence, puis cliquez sur **Installer**.
4. Suivez les instructions à l'écran pour terminer l'installation.

Il est recommandé de redémarrer la machine une fois l'installation de .NET terminée. Bien qu'un redémarrage ne soit pas essentiel, des composants supplémentaires peuvent être nécessaires pour terminer l'installation, comme l'installation de Windows Image Control.

Installation de Microsoft SQL Server

Il existe plusieurs éditions de SQL Server (les utilisateurs peuvent utiliser SQL Server ou SQL Server Express), allant d'une installation de base de données uniquement à l'installation de bases de données, de services avancés et d'outils de gestion.

Les paramètres avancés dans SQL Server ou la personnalisation de l'installation SQL dans un environnement particulier sortent du cadre de ce document. Si vous avez des questions spécifiques, veuillez contacter votre administrateur système ou l'équipe d'assistance de ICT.

Il est recommandé de ne pas modifier les paramètres par défaut de SQL Server, sauf si cela est spécifié ci-dessous, car ils sont nécessaires au bon fonctionnement de Protege GX.

Pour installer Microsoft SQL Server :

1. Téléchargez le fichier d'installation pour la version requise de SQL Server à partir du site Web de Microsoft. Les étapes de l'installation peuvent différer légèrement en fonction de la version que vous avez choisie.
2. Le fichier d'installation de SQL Server nécessite un accès à Internet pour télécharger les fichiers de support.
   Si le serveur dispose d'un accès à Internet :
   - Exécutez le fichier d'installation de SQL Server sur le serveur.
   - Sélectionnez le type d'installation **Personnalisé**.
   - Définissez l'emplacement d'installation et cliquez sur **Installer** pour télécharger et exécuter les fichiers d'installation.

   Si le serveur n'a pas d'accès à Internet :
   - Exécutez le fichier d'installation de SQL Server sur un autre ordinateur ayant accès à Internet.
   - Sélectionnez **Télécharger les médias**.
   - Définissez l'emplacement de téléchargement et cliquez sur **Téléchargement**.
   - Transférez les fichiers sur le serveur via USB.
   - Exécutez le programme d'installation sur le serveur.
3. Dans le centre d'installation de SQL Server, cliquez sur **Nouvelle installation autonome de SQL Server ou ajouter des fonctionnalités à une installation existante**.
4. Le programme d'installation effectue des vérifications sur le système pour s'assurer que vous disposez des conditions préalables nécessaires et qu'il n'y a pas de problèmes potentiels lors de l'installation. Résolvez les problèmes éventuels et cliquez sur **Suivant**.
5. Définissez le **Type d'installation** sur Réaliser une nouvelle installation de SQL Server. Cliquez sur **Suivant**.
6. Acceptez les termes du contrat de licence et cliquez sur **Suivant**.
7. Sur la page **Caractéristiques**, sélectionnez les éléments suivants et cliquez sur **Suivant** :
   - Services de moteur de base de données
   - Réplication de SQL Server
8. Assurez-vous que **l'Instance nommée** et **l'ID d'instance** sont configurées comme PROTEGEGX, puis cliquez sur **Suivant** pour continuer.
9. Cliquez sur **Suivant** à chaque étape pour accepter les paramètres par défaut.
10. L'installation progressera jusqu'à ce que l'installation de SQL Server soit terminée. Cliquez sur **Fermer** pour quitter l'assistant de configuration.

Installation du serveur de Protege GX

Avant d'installer Protege GX, le moteur de base de données (Microsoft SQL Server) doit être installé séparément.

Vous n'avez pas besoin d'installer SQL Server sur les postes de travail clients (ordinateurs qui se connecteront à distance au serveur Protege GX). Pour terminer l'installation du client, reportez-vous à la section installation de Protege GX du client (consultez page suivante).

Installation des composants du serveur Protege GX :

1. Exécutez le fichier **setup.exe** fourni. Ceci lance l'assistant d'installation Protege GX. Cliquez sur **Suivant** pour continuer.
2. Lisez et acceptez le contrat de licence, puis cliquez sur **Suivant**.
3. Saisissez vos informations d'enregistrement, y compris votre nom, votre société et le numéro de série du produit. Cliquez sur **Suivant** pour continuer.
4. Cliquez sur **Suivant** pour installer dans le dossier par défaut ou sur **Modifier** pour choisir un autre emplacement.
5. Choisissez le **Type de configuration**, puis cliquez sur **Suivant**.
   - **Terminé** : pour installer toutes les fonctionnalités du programme
   - **Personnalisé** : pour choisir les fonctionnalités du programme et l'endroit où elles seront installées. Utilisez cette option si vous ne souhaitez pas installer l'interface client sur le serveur. Cliquez sur l'icône à côté d'une fonctionnalité pour la désactiver. Cliquez sur **Suivant** pour continuer.
6. Cliquez sur **Suivant** pour démarrer les services automatiquement avant la fin de l'installation. Par défaut, les services sont installés à l'aide du compte local. Si vous effectuez une installation à distance, vous devrez personnaliser la connexion et les mots de passe, vous devez donc désactiver cette option et configurer les services manuellement après l'installation.
7. Entrez les détails du serveur de base de données sur lequel la base de données Protege GX sera créée. Si vous avez sélectionné les valeurs par défaut lors de l'installation de SQL Server, ce sera le nom du serveur et Protege GX (où Protege GX est l'instance SQL). Cliquez sur **Suivant** pour continuer.
8. Pour personnaliser les noms et/ou les chemins de la base de données, désactivez le paramètre **Masquer les options de configuration avancées de la base de données** et saisissez les détails appropriés. Il est recommandé que ces paramètres ne soient modifiés que par des utilisateurs avancés. Cliquez sur **Suivant** pour continuer.
9. Cliquez sur **Suivant** pour utiliser le port TCP/IP WCF par défaut ou spécifiez les ports utilisés en saisissant les nouveaux détails.

   Cette option doit être modifiée lorsqu'une autre application sur la machine cible utilise le port par défaut, car cela empêchera les services de démarrer.

   - Pour activer la connexion avec Windows Authentication à l'aide d'Active Directory, l'option **Activer Windows Authentication sur le service de données/les communications client** doit être sélectionnée.
   - S'il n'est pas sélectionné lors de l'installation, pour activer cette fonction à l'avenir, Protege GX devra être désinstallé, puis réinstallé avec cette option sélectionnée.
10. Cliquez sur **Installer** pour commencer l'installation.
11. Cliquez sur **Terminer** pour terminer l'installation et quitter l'assistant d'installation.

Installation du client Protege GX sur des postes de travail distants

Le client Protege GX est automatiquement installé dans le cadre de l'installation du serveur et n'a pas besoin d'être installé si les composants du serveur ont déjà été installés sur la machine. Les étapes suivantes doivent être effectuées sur des postes de travail supplémentaires.

Installation de l'application cliente Protege GX :

1. Exécutez le fichier **setup.exe** fourni. Ceci lance l'assistant d'installation Protege GX. Cliquez sur **Suivant** pour continuer.
2. Lisez et acceptez le contrat de licence, puis cliquez sur **Suivant**.

3. Saisissez vos informations d'enregistrement, y compris votre nom, votre société et le numéro de série du produit. Cliquez sur **Suivant** pour continuer.
4. Cliquez sur **Suivant** pour installer dans le dossier par défaut ou sur **Modifier** pour choisir un autre emplacement.
5. Choisissez la configuration **Personnalisée** et cliquez sur **Suivant**. Cela vous permet de sélectionner les fonctionnalités du programme qui seront installées.
6. Cliquez sur l'option **Serveur** et sélectionnez **Cette fonctionnalité ne sera pas disponible**. Le composant serveur est supprimé de la liste des fonctionnalités à installer.
7. Cliquez sur **Suivant** pour activer ou désactiver Windows Authentication pour les communications serveur/client Protege GX et configurer les ports TCP/IP WCF. Vous pouvez utiliser le port TCP/IP WCF par défaut ou personnaliser le port utilisé en désactivant le paramètre pour utiliser l'option par défaut et en entrant le nouveau port TCP/IP.

   Cette option doit être modifiée lorsqu'une autre application sur la machine cible utilise le port par défaut, car cela empêchera les services de démarrer.
8. Cliquez sur **Installer** pour commencer l'installation.
9. Cliquez sur **Terminer** pour terminer l'installation et quitter l'assistant d'installation.

Paramètres de sécurité recommandés

Il est fortement recommandé que les installations de serveurs Protege GX utilisent des paramètres de sécurité conformes aux meilleures pratiques afin de réduire le risque que le serveur soit exposé à une attaque. Cela inclut :

- Configuration de Protege GX pour utiliser TLS 1.2 (consultez ci-dessous).
- La désactivation des suites de chiffrement et des protocoles non sécurisés (consultez la page 23).

Configuration de Protege GX pour utiliser TLS 1.2

TLS (Transport Layer Security) est un ensemble de protocoles de sécurité mis en œuvre pour protéger les communications et les données transférées. Cependant, plusieurs vulnérabilités connues ont été signalées contre des versions antérieures de TLS. Nous vous recommandons de passer à TLS 1.2 pour une communication sécurisée.

Configuration TLS 1.2

TLS 1.2 est l'option de sécurité par défaut dans le processus d'installation de Protege GX et les éléments requis sont automatiquement configurés dans l'arrière-plan à moins qu'une option différente soit sélectionnée. Si TLS 1.2 n'est pas actuellement activé dans votre installation, vous pouvez l'activer en réinstallant l'application et en vous assurant que TLS 1.2 est sélectionné.

Pour vérifier si TLS 1.2 a été activé lors de l'installation, accédez au répertoire d'installation (C:\Program Files (x86)\Integrated Control Technology\Protege GX) et ouvrez GXSV.exe.config dans un éditeur de texte. Si le fichier contient le texte `sslProtocols="Tls12"`, alors TLS 1.2 a été activé.

Dans le cadre du processus d'installation Protege GX, un certain nombre d'éléments sont installés ou configurés. Ceux-ci incluent :

- Installation de Microsoft .NET Framework 4.6.2.
- Installation de OLE DB Driver 18.
- Création d'un certificat autosigné sur le PC local.
- Ajout d'entrées de configuration dans le répertoire Windows.
- Ajout des entrées de configuration requises dans les fichiers de configuration Protege GX.

En plus de ce qui précède, les étapes manuelles suivantes sont nécessaires pour activer complètement TLS 1.2 pour Protege GX.

Une configuration différente est nécessaire pour utiliser TLS 1.2 avec l'authentification Windows. Pour obtenir des instructions, consultez la Note d'application 277 : Configuration de Protege GX pour utiliser TLS 1.2.

Activer le cryptage forcé et le TCP/IP

1. Ouvrez le gestionnaire de configuration de SQL Server :
   - Appuyez sur **Windows + R** pour ouvrir la boîte de dialogue d'exécution.
   - Tapez sqlservermanager<version>.msc, en remplaçant <version> avec le numéro de la version de l'application correspondant à votre installation de serveur SQL (voir cette page).
   - Cliquer sur **OK**.
2. Ouvrez la section **Configuration réseau de SQL Server** dans le panneau de gauche.
3. Faites un clic droit sur **Protocoles pour ProtegeGX** (ou le nom de l'instance SQL qui contient la base de données de Protege GX), et sélectionnez **Propriétés**.
4. Dans la fenêtre de Propriétés, placez **Cryptage forcé** sur Oui et cliquez sur OK.
5. Ouvrez **Protocoles pour Protege GX**.
6. Double-cliquez sur **TCP/IP** et placez **Activé** sur Oui. Cliquez sur **OK** pour fermer la fenêtre.

7. Ouvrez **Services de serveur SQL** à partir du panneau gauche.
8. Faites un blic droit sur **Serveur SQL (ProtegeGX)** dans le panneau droit et sélectionnez **Redémarrer** pour redémarrer le Service de serveur SQL de Protege GX.
9. Une fois l'opération terminée, fermez le gestionnaire de configuration SQL Server.

Activez la console de gestion IIS

1. Activez la console de gestion IIS en vous dirigeant vers : **Panneau de contrôle > Programmes et fonctionnalités > Activer ou désactiver des fonctionnalités Windows**.
2. Dans la liste de fonctionnalités, allez vers **Internet Information Services > Web Management Tools > IIS Management Console**. Cochez la boîte pour activer cette fonctionnalité.
3. Cliquez sur **OK**.
4. Redémarrez tous les services de Protege GX.

Utilisation d'un certificat personnalisé

Dans certains systèmes, il est préférable d'utiliser un certificat TLS/SSL personnalisé au lieu du certificat auto-signé généré par Protege GX lors de l'installation. Une configuration supplémentaire est nécessaire pour installer le certificat personnalisé.

Ceci est nécessaire lorsque des clients Protege GX se connectent au serveur depuis l'extérieur du routeur/pare-feu et que la redirection de port est en place. Le certificat personnalisé doit faire référence au nom d'hôte externe du serveur Protege GX.

Le processus exact peut varier en fonction de votre système d'exploitation. Consultez votre fournisseur informatique pour des instructions plus détaillées.

Obtenir le certificat de serveur

Un certificat SSL sous la forme d'un fichier.pfx doit être obtenu auprès de votre fournisseur informatique. Celui-ci peut être autosigné ou fournit par une autorité de certification de confiance. Vous aurez également besoin du mot de passe utilisé pour générer le fichier afin d'installer le certificat.

Installation du certificat de serveur

1. Copiez le fichier .pfx sur le serveur Protege GX sur lequel vous installez le certificat.
2. Double-cliquez sur le certificat pour initier **l'assistant d'importation du certificat**.
3. Définissez la **localisation** comme machine locale.
4. Ne pas changer le **fichier à importer**.
5. Entrez le mot de passe utilisé pour générer le fichier .pfx. La personne qui a généré le certificat doit le connaître.
6. Définissez l'emplacement où vous souhaitez stocker le certificat en tant que **dossier personnel**.
7. Finalisez l'importation.

Configurez Protege GX pour utiliser le certificat

Une fois le certificat installé, vous devrez configurer Protege GX pour utiliser ce certificat pour ses connexions.

1. Ouvrez **Microsoft Management Console** en pressant les touches **[WIN + r]**, en tapant mmc et en appuyant sur entrée.
2. Une fois la console ouverte, ouvrez **Ajouter ou Supprimer des Snap-ins** en appuyant sur **[CTRL + m]**, ou via le menu **Fichier**.
3. Double-cliquez sur **Certificats**, sélectionnez **Un compte d'ordinateur** et cliquez sur **Suivant**.
4. Sélectionnez **L'ordinateur local** et cliquez sur **Terminer**.

5. Cliquez sur **OK** pour fermer la fenêtre d'enfichage.
6. Allez vers **Certificats (Ordinateur local) > Personnel > Certificats**.
7. Vous devriez pouvoir voir votre certificat installé ici. Double-cliquez dessus.
8. Trouvez le champ nommé **Thumbprint** et copiez les données en provenant dans un endroit sûr.
9. Ouvrir **GXSV.exe.config**, situé dans le répertoire d'installation (C:\Program Files (x86)\Integrated Control Technology\Protege GX).

   Les fichiers de ce répertoire nécessitent des droits d'administrateur pour être modifiés. Vous devrez peut-être ouvrir le fichier en tant qu'administrateur à l'aide d'une application comme Notepad++, ou faire une copie dans un autre répertoire pour modifier et remplacer l'original.

10. Situez la section suivante dans le XML : /configuration/system.serviceMode1/behaviors/serviceBehaviors/behavior[@name="md"]/serviceCertificate.

    Si cette section n'existe pas, c'est parce que vous n'avez pas installé Protege GX avec TLS activé.

11. Dans l'étiquette `<serviceCertificate>`, changez le `findValue` de l'empreinte du nouveau certificat que vous avez installé. Le résultat ressemblera à ce qui suit :

```
<serviceCertificate
storeLocation="LocalMachine" storeName="My" findValue="CERTIFICATE_
THUMBPRINT" x509FindType="FindByThumbprint" />
```

12. **Sauvegardez** le fichier de configuration et **redémarrez** le service de données pour que les changements fassent effet.Protege GX

Activation de la validation du certificat sur le client

Lorsqu'un certificat de confiance personnalisé est utilisé, il est recommandé d'activer la validation du certificat de service pour renforcer la connexion entre le serveur et le client Protege GX. Cela permet de se protéger contre les attaques de type homme du milieu lors de la connexion initiale.

Cette option n'est disponible que lorsqu'un certificat tiers fourni par une autorité de confiance est utilisé, ou un certificat auto-signé qui a été installé comme certificat de confiance sur les postes de travail clients. Si le même poste client est utilisé pour se connecter à plusieurs serveurs Protege GX, ce paramètre exige que tous les serveurs avec TLS activé utilisent un certificat de confiance.

Pour activer la validation des certificats de service, effectuez la configuration suivante sur tous les postes de travail clients :

1. Ouvrir **GXPI.exe.config**, situé dans le répertoire d'installation (C:\Program Files (x86)\Integrated Control Technology\Protege GX).

   Les fichiers de ce répertoire nécessitent des droits d'administrateur pour être modifiés. Vous devrez peut-être ouvrir le fichier en tant qu'administrateur à l'aide d'une application comme Notepad++, ou faire une copie dans un autre répertoire pour modifier et remplacer l'original.

2. Directement après le noeud `<configSections>`, ajoutez le noeud `<appSettings>` comme indiqué ci-

dessous :

```
<configSections>
    <section
name
="microsoft.scripting"
 type="Microsoft.Scripting.Hosting.Configuration.Section,
Microsoft.Scripting, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=null" requirePermission="false" />
</configSections>
<appSettings>
    <add key="client.validateServiceCertificate" value="true" />
</appSettings>
```

3. Sauvegarder le fichier de configuration.

Le fichier de configuration personnalisé peut être écrasé lors de la mise à jour du logiciel. Vous devrez peut-être ajouter le nœud **<appSettings>** à chaque client après la mise à niveau.

Configuration du service SOAP Protege GX

Cette section décrit la configuration supplémentaire requise pour déployer le service Protege GX Service SOAP pour TLS 1.2.

1. Lorsque vous installez le service SOAP Protege GX, assurez-vous que vous l'installez avec **TLS activé** .
   Sur la page **Personnaliser le port TCP/IP WCF**, faites pointer le service SOAP vers le serveur Protege GX :
   - **Nom du PC installé sur le serveur de données Protege GX** : le nom DNS ou le nom d'hôte du serveur Protege GX.
   - **Port du serveur de données** : 8000 (ou tel que configuré)
   - **Port du serveur de rapports** : 8010 (ou tel que configuré)

   Pour obtenir des instructions sur l'installation du service SOAP, consultez le Manuel d'installation du service SOAP Protege GX .
2. Recherchez et modifiez le fichier suivant : **C:\inetpub\wwwrootProtegeGXSOAPService\Web.config**.
   - Sous **/configuration/system. serviceModel/**, commentez ou supprimez cette ligne : **<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />**.
   - Lors de l'utilisation de la sécurité TLS (recommandé) sur le service de données :
     - Sous **/configuration/system.serviceModel/client/endpoint@address**, définissez le nom d'hôte du point de terminaison sur le nom DNS ou le nom d'hôte du serveur Protege GX.
     - Sous **/configuration/system.serviceModel/client/endpoint/identity/dns@value**, définissez l'identité DNS du point de terminaison sur l'un des « Noms alternatifs des sujets » dans le certificat TLS du service de données.
     - Le nœud suivant ne doit pas exister lors de l'utilisation d'un certificat personnalisé. Supprimer si présent : **/configuration/system.serviceModel/behaviors/endpointBehaviors/behavior[@name=md0]/clientCredentials/serviceCertificate/authentication**.

Renouvellement des certificats TLS

Il est parfois nécessaire de renouveler ou de mettre à jour le certificat TLS associé à une installation Protege GX. Cela peut se produire lorsque :

- Le certificat existant expire.
- L'adresse IP ou le nom d'hôte du serveur change de sorte que le certificat existant n'est plus valide.

Si vous utilisez le certificat auto-signé par défaut généré par votre installation Protege GX, vous devez désinstaller et réinstaller Protege GX pour générer un nouveau certificat auto-signé.

Si vous remplacez un certificat personnalisé, vous devrez installer et configurer le nouveau certificat comme décrit ci-dessus (consultez la page 20). Pour terminer le processus, redémarrez le service de données Protege GX.

Désactiver les suites de chiffrement et les protocoles non sécurisés

Nous vous recommandons de suivre les meilleures pratiques en désactivant les suites de chiffrement et les protocoles de communication anciens et non sécurisés sur le serveur Protege GX et le serveur SOAP. Pour ce faire, vous devez modifier les paramètres du registre sur l'ordinateur où le serveur [Protege GX est installé, ainsi que sur l'ordinateur hébergeant le service SOAP si celui-ci est installé séparément. Pour plus d'informations sur les paramètres pertinents, consultez la Documentation Microsoft et contactez votre fournisseur informatique.

Toujours sauvegarder (exporter) les paramètres du registre avant de le modifier.

IIS Crypto de Nartac Software est un outil utile pour gérer les paramètres de sécurité. Cette option vous permet d'appliquer des paramètres de sécurité au serveur sans avoir à modifier manuellement le registre.

Une installation standard Protege GX a été validée avec les paramètres **PCI 3.2** et les **meilleures pratiques** de IIS Crypto 3.2. PCI 3.2 fournit une sécurité plus stricte et est le paramètre recommandé.

Pour appliquer ces paramètres :

1. Téléchargez IISCrypto.exe à partir du lien ci-dessus.
2. Exécutez le programme et cliquez sur **Oui** pour l'autoriser à apporter des modifications à votre ordinateur.
3. Naviguez vers l'onglet **Modèles**.
4. Sélectionnez le modèle PCI 3.2 dans la liste déroulante, puis cliquez sur **Appliquer**.
5. Redémarrez l'ordinateur pour mettre en oeuvre les nouveaux paramètres.

Protege GX prend en charge un large éventail d'intégrations, qui peuvent ne pas être toutes compatibles avec les paramètres de sécurité des meilleures pratiques. De plus, le matériel plus ancien peut ne pas prendre en charge les protocoles de cryptage les plus récents. Dans certaines situations, il peut être nécessaire d'activer des suites de chiffres et des protocoles de communication moins sécurisés. Il incombe à l'installateur de s'assurer que les paramètres de sécurité appropriés sont appliqués.

Activation du chiffrement transparent des données

Le chiffrement transparent des données (TDE) est une fonctionnalité de SQL Server qui vous permet de chiffrer les bases de données Protege GX « au repos ». Les données sont chiffrées sur le disque, puis déchiffrées lorsqu'une application telle que le logiciel Protege GX y accède. Ainsi, les données ne peuvent pas être lues si un pirate accède aux bases de données ou aux sauvegardes, par exemple en cas de vol du support de stockage physique.

Nous vous recommandons d'implémenter le TDE tant dans la base de données de programmation que dans la base de données d'événements.

Cette fonctionnalité est prise en charge par les éditions suivantes de SQL Server :

- SQL Server Enterprise (à partir de 2008)
- SQL Server Standard (à partir de 2019)

Pour plus d'informations sur le TDE, consultez chiffrement transparent des données (TDE) dans le centre d'aide de Microsoft. Si votre version de SQL Server ne prend pas en charge le TDE, nous vous recommandons d'étudier d'autres méthodes de chiffrement des bases de données au repos.

Remarques importantes

- **Il est essentiel que vous sauvegardiez le certificat utilisé pour chiffrer les bases de données.** Les sauvegardes de bases de données étant également chiffrées, vous aurez besoin du certificat pour restaurer une sauvegarde de base de données sur un nouveau serveur. Si le certificat n'a pas été sauvegardé, il est possible de perdre toutes les données contenues dans les sauvegardes de la base de données.
- Si vous fournissez une sauvegarde de la base de données dans ICT pour la réplication d'un problème, vous devrez également fournir le certificat.
- Le TDE peut avoir un faible impact sur les performances du serveur (3-5 %). Cet impact concerne principalement l'unité centrale.
- Les données déchiffrées peuvent être consultées par toute personne ayant accès à l'instance SQL. Utilisez des contrôles d'accès restrictifs pour empêcher tout accès non autorisé.

Activation du chiffrement transparent des données

1. Ouvrez le composant logiciel enfichable **Services** en suivant les étapes ci-après :
   - Appuyez sur les touches **Windows + R**
   - Tapez **services.msc** dans la barre de recherche et appuyez sur **Entrer**
2. Recherchez le Protege GX Update Service. Faites un clic droit sur le service et cliquez sur **Arrêter**. Cela arrête également les autres services Protege GX.
3. Ouvrir SQL Server Management Studio (SSMS) et se connecter à l'instance Protege GX en tant qu'utilisateur administrateur.
4. Cliquez sur **Nouvelle requête**.
5. Saisissez la requête fournie ci-dessous. SQL Server effectuera alors les opérations suivantes :
   1. Créer une clé principale de base de données protégée par un mot de passe.
   2. Créer un certificat protégé par la clé principale.
   3. Créer une clé de chiffrement de base de données par base de données, protégée par le certificat.
   4. Activer le chiffrement sur chaque base de données.

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
GO
CREATE CERTIFICATE TDECertificate WITH SUBJECT = 'TDE Certificate';
GO
USE ProtegeGX;
GO
CREATE DATABASE ENCRYPTION KEY
    WITH ALGORITHM = AES_256
    ENCRYPTION BY SERVER CERTIFICATE TDECertificate;
GO
ALTER DATABASE ProtegeGX
    SET ENCRYPTION ON;
GO
USE ProtegeGXEvents;
GO
CREATE DATABASE ENCRYPTION KEY
    WITH ALGORITHM = AES_256
    ENCRYPTION BY SERVER CERTIFICATE TDECertificate;
GO
ALTER DATABASE ProtegeGXEvents
```

```
    SET ENCRYPTION ON;
GO
```

Veillez à personnaliser les paramètres suivants :

- **MOT DE PASSE** pour le chiffrement : saisissez un mot de passe solide pour la clé principale de la base de données et sauvegardez-le dans un endroit sûr.
- **SUJET** du certificat TDE : saisissez un nom approprié pour le certificat. Ce nom sera également utilisé pour les paramètres **CERTIFICAT DE SERVEUR**.
- Si vous n'utilisez pas les noms par défaut pour les bases de données ProtegeGX et ProtegeGXEvents, mettez-les à jour.

6. Cliquez sur **Exécuter**. SQL Server travaillera en arrière-plan pour chiffrer les bases de données.
7. Vous pouvez afficher la progression du chiffrement à l'aide de la vue de gestion dynamique des clés de chiffrement des bases de données. Exécutez la requête suivante :

```
SELECT *
FROM sys.dm_database_encryption_keys;
```

8. Une fois le chiffrement terminé, vous devez sauvegarder le certificat de chiffrement et la clé privée à l'aide de la requête suivante :

```
BACKUP CERTIFICATE TDECertificate TO FILE = 'c:\storedcerts\TDE
Certificate'
    WITH PRIVATE KEY ( FILE = 'c:\storedkeys\TDE Key' ,
    ENCRYPTION BY PASSWORD = '<UseAnotherStrongPasswordHere>' );
GO
```

SQL Server va exporter les fichiers de certificat et de clé privée aux emplacements spécifiés.

9. Stockez les sauvegardes du certificat et de la clé privée dans un endroit sûr et enregistrez le mot de passe utilisé pour chiffrer la clé privée.

Si le certificat, la clé privée ou le mot de passe sont perdus, il ne sera pas possible de restaurer les sauvegardes de la base de données sur un autre serveur.

10. Effectuez une sauvegarde complète des deux bases de données en suivant les instructions figurant dans Sauvegarde de votre base de données.
11. Démarrez les services de Protege GX en démarrant le service de données de Protege GX, puis le service de téléchargement de Protege GX.

Activation de l'ASLR obligatoire

L'ASLR (distribution aléatoire de l'espace d'adressage) est un processus de protection de la mémoire qui randomise l'emplacement où les exécutables du système sont chargés en mémoire. Ce processus aide à se prémunir contre les attaques par débordement de tampon en rendant plus difficile pour un attaquant de prédire les adresses cibles et d'exploiter les vulnérabilités de corruption de mémoire.

L'option ASLR obligatoire disponible dans Sécurité Windows peut être utilisée pour garantir que tous les EXE et DLL du système d'exploitation sont randomisés de force au moment de l'exécution. Pour plus d'informations sur l'ASLR obligatoire, consultez la Documentation Microsoft ou contactez votre fournisseur informatique.

Pour maintenir la compatibilité héritée, cette fonction est désactivée par défaut sur tous les systèmes d'exploitation Windows. Nous vous recommandons de suivre les meilleures pratiques en activant la fonctionnalité ASLR obligatoire sur votre serveur Protege GX, votre serveur SOAP et, pour une sécurité maximale, sur tous les postes clients Protege GX.

Vous aurez besoin de droits d'administrateur pour activer cette fonction.

Pour activer l'ASLR obligatoire :

1. Ouvrez **Sécurité Windows**.
2. Naviguez jusqu'à **Contrôle des applications et du navigateur**.
3. Sous la section **Protection contre l'exploitation**, sélectionnez **Paramètres de protection contre l'exploitation**.
4. Sous la section **Paramètres système**, allez à l'option **distribution aléatoire de l'espace d'adressage (ASLR obligatoire)** et changez le paramètre en Activé par défaut.
5. Redémarrez l'ordinateur pour appliquer les nouveaux paramètres.

Autoriser les services à travers le pare-feu de Windows

Il peut être nécessaire d'autoriser les services Protege GX à travers le pare-feu Windows pour éviter que la communication du système soit bloquée.

1. Ouvrez les paramètres du pare-feu Windows dans **Panneau de configuration > Système et sécurité > Pare-feu Windows Defender** .
2. Cliquez sur le lien **Permettre une application ou une fonctionnalité via le pare-feu Windows Defender**, à gauche de l'écran.

   Les logiciels antivirus ou pare-feu tiers peuvent empêcher la modification des règles du Pare-feu Windows. Si tel est le cas, consultez le fabricant tiers pour plus de détails sur l'autorisation des programmes à travers le pare-feu.
3. Sélectionnez **Permettre une autre application...** pour ajouter un programme en tant qu'exception.
4. Cliquez sur **Naviguer**, puis naviguez jusqu'au répertoire d'installation de Protege GX.

   Le fichier est situé dans le répertoire d'installation, par défaut C :\Program Files (x86)\Integrated Control Technology\Protege GX.
5. Sélectionnez (double-cliquez ou sélectionner et **Ouvrir**) l'exécutable que vous voulez autoriser, puis cliquez sur **Ajouter** .

   Ajoutez les exécutables Protege GX suivants, un par un :
   - GXSV.exe
   - GXSV2.exe
   - GXSV3.exe
   - GXPI.exe
   - GXEvtSvr.exe
   - GXDVR1.exe
   - GXDVR2.exe

   Cela permet aux services nécessaires Protege GX d'accéder à travers le pare-feu Windows.

Le processus ci-dessus n'autorisera l'accès qu'à travers votre connexion réseau principale. Si plusieurs réseaux sont connectés, vous devrez autoriser manuellement l'accès (en cochant la case dans la colonne réseau) pour chaque réseau supplémentaire auquel l'exécutable Protege GX doit accéder.

Configuration initiale du site de Protege GX

Après avoir installé Protege GX, le logiciel doit être configuré pour communiquer avec le contrôleur.

Pour des instructions détaillées sur la programmation d'un contrôleur, consultez le Guide de configuration du contrôleur système intégré Protege GX, disponible sur le site Web ICT.

Connectez-vous à Protege GX

1. Double-cliquez sur l'icône Protege GX sur votre bureau ou accédez au programme à partir de votre menu Démarrer de Windows :

   Démarrez > Tous les programmes > ICT > Protege GX > Protege GX

   La fenêtre de connexion s'affiche.
2. Connectez-vous en tant qu'utilisateur avec un accès complet au système. Pour les nouvelles installations, connectez-vous à l'aide du nom d'utilisateur par défaut de l'opérateur administrateur admin avec un mot de passe vide.
3. Si vous vous connectez à un serveur Protege sur une autre machine, entrez les détails du serveur ou l'adresse IP.
4. Cliquez sur **Connexion**.

Il est **fortement recommandé** de remplacer le mot de passe de l'opérateur administrateur par un mot de passe très sécurisé après la première connexion. Pour ce faire, cliquez sur le bouton **Changer le mot de passe** en bas de la page d'accueil.

Création d'un mot de passe sûr

Lorsque vous créez ou modifiez le mot de passe de l'opérateur administrateur, il est **vivement recommandé** de créer un mot de passe très sûr.

À titre indicatif, un mot de passe sécurisé doit inclure les caractéristiques suivantes :

- Minimum huit caractères de longueur
- Combinaison de lettres majuscules et minuscules
- Combinaison de chiffres et de lettres
- Inclusion de caractères spéciaux

Les mots de passe doivent être conformes aux exigences de la politique de mot de passe.

Activation de votre licence

Avant de pouvoir commencer à utiliser Protege GX, vous devez enregistrer et activer votre licence.

Seuls les opérateurs ayant accès à tous les sites du système peuvent activer la licence. Cette procédure doit être effectuée depuis le serveur et non depuis un poste de travail client distant. Vous devez également disposer des privilèges administratifs locaux sur le serveur pour activer correctement la licence.

1. Sur la machine serveur, ouvrez le client Protege GX.
2. À partir du menu principal, sélectionnez **À propos | Licence**.
3. Sélectionnez l'onglet **Mise à jour de licence**.
4. Sélectionnez l'option **Automatique** ou **Manuel** pour télécharger et activer votre licence de Protege GX.
   - Si la machine serveur a un accès Internet, utilisez l'option **Automatique**.
   - Si la machine serveur ne dispose pas d'un accès à Internet, vous devez utiliser l'option **Manuel**.

Les étapes de génération manuelle de la licence et de téléchargement de celle-ci vers Protege GX doivent être exécutées à partir du serveur plutôt que d'un poste de travail client distant, sinon le profil ne correspondra pas et l'activation de la licence échouera.

Pour activer automatiquement votre licence :

1. Cliquez sur **Télécharger la licence**, saisissez les informations requises et sélectionnez **OK**.
2. L'application Protege transmet vos coordonnées au service d'enregistrement Web de ICT, puis active automatiquement votre logiciel.
3. Fermez et redémarrez le client Protege GX pour mettre en oeuvre la nouvelle licence.

Pour activer manuellement votre licence :

1. Cliquez sur **Générer** pour créer un fichier de demande de licence. Lorsque vous y êtes invité, enregistrez le fichier **ICT_LicenceRequest.req** dans un dossier de votre réseau ou sur un lecteur portable.
2. Cliquez sur le lien **Sélectionnez vos options de licence**. Cela ouvre une page Web sur laquelle vous serez invité à entrer les détails de votre site, de l'installateur et du numéro de série (SSN).
3. Accédez au fichier **_LicenceRequest.req** enregistré et cliquez sur **Soumettre**.ICT
4. Vos détails sont ensuite transmis au service d'enregistrement Web de ICT. Une fois l'enregistrement terminé, vous serez invité à télécharger votre fichier de licence (*.lic).
5. Cliquez sur **Naviguer** pour sélectionner le fichier de licence et activer votre licence pour Protege GX.
6. Fermez et redémarrez le client Protege GX pour mettre en oeuvre la nouvelle licence.

Remarque : les étapes 2 à 4 peuvent être effectuées sur n'importe quel poste de travail avec accès à Internet. Les étapes 1 et 5 **doivent être effectuées sur le serveur**.

Ajouter un site

1. Lors de votre première connexion, vous serez invité à ajouter un site.
2. Saisissez un nom pour votre **nouveau site** et cliquez sur **OK**.

Ajout d'un contrôleur

Une fois qu'un site a été ajouté, la fenêtre **Ajouter contrôleur** s'affiche.

1. Saisissez un **nom** pour le contrôleur et définissez le champ **Nombre** sur 1 pour ajouter un seul contrôleur. Sélectionnez le **Type** de contrôleur que vous souhaitez ajouter.
2. Le clavier et les registres de modules d'expansion peuvent alors être ajoutés à partir des sections appropriées.

   Le matériel n'a pas besoin d'être connecté avant la création des registres.
3. Dans la section **Options**, sélectionnez **Créer un groupe de menu d'installation** et **Créer un plan d'étage** si nécessaire.
4. Définissez le type de **carte de rapport CID** par défaut. Le type Grand est recommandé pour la plupart des sites.
5. Dans la section **Portes**, spécifiez le nombre d'enregistrements de porte à créer. Les options suivantes peuvent également être activées ou désactivées :
   - **Assigner aux modules d'expansion de lecteurs**
   - **Assigner les Entrées trouble des portes**
   - **Assigner serrure de lecteur PGM à la configuration de porte**
   - **Assigner Beeper du lecteur à la configuration de l'alarme de porte**
6. Une fois terminé, cliquez sur **Ajouter maintenant**.

7. Allez vers **Sites | Contrôleurs**. Les paramètres définis ci-dessous doivent correspondre à ceux de l'interface Web du contrôleur.
   - **Numéro de série** : le numéro de série du contrôleur.
   - **Adresse IP** : le contrôleur système dispose d'un périphérique Ethernet TCP/IP intégré et doit être programmé avec une adresse TCP/IP valide pour permettre au logiciel de se connecter. Par défaut l'adresse IP est configurée sur 192.168.1.2.
   - **Port de téléchargement** : le port TCP/IP est utilisé pour envoyer des téléchargements au contrôleur. Par défaut c'est le port 21000.
   - **Serveur de téléchargement** : à partir du menu déroulant, sélectionnez le serveur de téléchargement qui doit être utilisé par le contrôleur.
   - **Port pour demande de contrôle et d'état** : le port TCP/IP utilisé pour envoyer les commandes de contrôle au contrôleur. Par défaut il s'agit du port 21001.
8. Cliquez sur **Sauvegarder**.

Vous devrez peut-être redémarrer les services pour mettre le contrôleur en ligne. Sélectionnez l'option **Services** dans le **panneau de contrôle** et redémarrez les **services de Protege GX**.

Sauvegarde du système

Si vous mettez à niveau une installation, il est essentiel d'effectuer une sauvegarde du système avant de terminer la mise à niveau. Le non-respect de cette consigne peut entraîner une perte permanente de données.

Les instructions ci-dessous décrivent comment sauvegarder vos bases de données à partir de SQL Server Management Studio (SSMS). Vous pouvez également effectuer des sauvegardes et configurer des sauvegardes planifiées dans Protege GX sous **Global | Paramètres globaux**.

Compatibilité de la base de données

Lorsque vous sauvegardez ou restaurez une base de données, vous devez prendre note de la **version de la base de données**. Le numéro de version du logiciel (voir **À propos | Version**) indique la version de la base de données comme indiqué ci-dessous :

4	3	264	39
Version majeure	**Version mineure**	**La version de la base de données**	**Élaboration de logiciel**

Les sauvegardes effectuées par le logiciel Protege GX incluent toujours le numéro de version de la base de données dans le nom du fichier. C'est une bonne pratique à suivre lorsque vous effectuez vos propres sauvegardes.

Lorsque vous restaurez une base de données, vous devez vous assurer que la version de la base de données du fichier de sauvegarde est compatible avec celle du logiciel, comme indiqué ci-dessous :

La version de la base de données		Version du logiciel	
265	>	264	✗
264	=	264	✓
264	<	265	✓

- Si la version de la base de données est plus récente que la version du logiciel, il n'est pas possible de restaurer la base de données. Mettez à jour le logiciel avant de la restaurer.
- Si les numéros de version correspondent, la restauration devrait aboutir.
- Si la version de la base de données est plus ancienne que la version du logiciel, la base de données peut être restaurée mais doit être mise à niveau pour correspondre à la version du logiciel. Restaurez la base de données, puis désinstallez et réinstallez le logiciel du serveur pour mettre à niveau la version de la base de données.

Si la version de la base de données et la version du logiciel ne correspondent pas, **le service de données ne démarre pas**.

Sauvegarde de votre base de données

La procédure suivante vous permet d'effectuer une sauvegarde de l'une ou l'autre base de données dans SQL Server Management Studio (SSMS). Les instructions peuvent différer légèrement selon la version de SSMS que vous utilisez.

1. Ouvrez SSMS et connectez-vous au serveur de Protege GX.
2. Développez le nœud Bases de **données**. Faites un clic droit sur le Base de données ProtegeGX ou ProtegeGXEvents et sélectionnez **Tasks > Back Up...**.

3. Si une sauvegarde a été créée précédemment, le fichier sera affiché dans le champ **Destination**. Si vous souhaitez utiliser ce fichier, cliquez sur l'onglet **Options multimédia** et indiquez si vous allez ajouter la sauvegarde actuelle au fichier existant ou remplacer le fichier existant.

   Pour sauvegarder dans un autre fichier, cliquez sur **Supprimer**. Cliquez ensuite sur **Ajouter...** pour saisir le nom et l'emplacement du nouveau fichier de sauvegarde. Cliquez sur **OK**.

   Le fichier de sauvegarde doit être au format .bak. Il est recommandé d'ajouter le numéro de version de la base de données au nom de fichier.

4. Cliquez sur **OK** pour effectuer la sauvegarde.

Restaurer des sauvegardes de la base de données

Il n'est pas possible de restaurer une sauvegarde de base de données dans Protege GX. Ces instructions montrent comment restaurer des sauvegardes à l'aide de SQL Server Management Studio (SSMS).

Avant de restaurer une base de données, sauvegardez votre base de données actuelle afin de pouvoir revenir à un point connu en cas de problème.

1. Si vous restaurez une base de données avec le cryptage transparent des données sur un Serveur différent, vous devez d'abord charger le certificat de cryptage sur le nouveau Serveur.

   Consultez Sauvegarde et restauration avec le chiffrement transparent des données pour obtenir les instructions

2. Vérifiez la version de la base de données que vous restaurez par rapport à la version actuelle du logiciel (**À propos | Version**).

   Si la version de la base de données est supérieure au troisième numéro de la version du logiciel, ne continuez pas (consultez page précédente).

3. Ouvrez le composant logiciel enfichable **Services** en suivant les étapes ci-après :
   - Appuyez sur les touches **Windows + R**
   - Tapez **services.msc** dans la barre de recherche et appuyez sur **Entrer**
4. Recherchez le Protege GX Update Service. Faites un clic droit sur le service et cliquez sur **Arrêter**. Cela arrête également les autres services Protege GX.
5. Ouvrez SSMS et connectez-vous à l'instance Protege GX.
6. Développez le nœud **Bases de données**. Right click the ProtegeGX or ProtegeGXEvents database and select **Tasks > Restore > Database...**.
7. Réglez la **Source** sur **Appareil**, puis cliquez sur le bouton d'ellipse **[...]**.
8. Cliquez sur **Ajouter** pour naviguer vers le fichier de sauvegarde (.bak) que vous allez restaurer. Cliquez sur **OK**.
9. La section **Plan de restauration** affiche le(s) jeu(x) de sauvegarde disponible(s) pour la restauration. S'il y en a plus d'un, utilisez la date de sauvegarde pour déterminer celui qui doit être restauré, puis cochez la case **Restaurer** à côté du jeu de sauvegarde sélectionné.
10. Dans l'onglet **Options**, activez l'option **Écraser la base de données existante**.
11. Cliquez sur **OK** pour lancer le processus de restauration.
12. Si la version de la base de données que vous avez restaurée est antérieure à la version actuelle du logiciel, elle doit être mise à niveau avant que les services ne démarrent. Désinstallez et réinstallez Protege GX pour mettre à jour la base de données.
13. Dans le snap-in **Services**, faites un clic droit sur le Protege GX Data Service et cliquez sur **Commencer**. Si le service de données (data service) démarre, la restauration de la base de données a réussi.

    Le démarrage du service de données démarre également le service d'événements et le service de mise à jour; toutefois, le service de téléchargement doit être démarré manuellement. Il est recommandé de vérifier la configuration avant de lancer le service de téléchargement, car celui-ci commencera à télécharger la programmation vers les contrôleurs.

Sauvegarde et restauration avec le chiffrement transparent des données

Lorsqu'une base de données a un Cryptage transparent des données (CTD) activé, toutes les sauvegardes de cette base de données sont également chiffrées. Si vous devez restaurer la base de données sur un autre serveur, vous devez d'abord créer une clé principale de base de données (DMK) et ajouter le certificat de sauvegarde au nouveau serveur.

Avant de commencer, vous aurez besoin du certificat, de la clé privée et du mot de passe utilisé pour chiffrer la clé privée. Si vous ne disposez pas de sauvegardes de ceux-ci, vous pouvez les exporter à partir du serveur d'origine.

1. Sur le serveur d'origine, cliquez sur **Nouvelle requête** et saisissez la requête suivante :

```
BACKUP CERTIFICATE TDECertificate TO FILE = 'c:\storedcerts\TDE
Certificate'
    WITH PRIVATE KEY ( FILE = 'c:\storedkeys\TDE Key' ,
    ENCRYPTION BY PASSWORD = '<UseAStrongPasswordHere>' );
GO
```

2. Cliquez sur **Exécuter**. SQL Server va exporter les fichiers de certificat et de clé privée aux emplacements spécifiés.

   Vous devez sauvegarder le certificat, la clé privée et le mot de passe utilisé pour chiffrer la clé privée dans un emplacement sécurisé. Si vous les perdez, il ne sera pas possible de restaurer les sauvegardes de la base de données sur un autre serveur.

3. Transférez les fichiers vers le nouveau serveur.

Vous devrez ensuite créer une clé principale de base de données et un certificat sur le nouveau serveur.

1. Ouvrir SQL Server Management Studio (SSMS) et se connecter à l'instance Protege GX en tant qu'utilisateur administrateur.
2. Cliquez sur **Nouvelle requête**.
3. Saisissez la requête suivante :

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
GO
CREATE CERTIFICATE TDECertificate
    FROM FILE = 'c:\storedcerts\TDE Certificate.cer'
    WITH PRIVATE KEY (FILE = 'c:\storedkeys\TDE Key.pvk',
    DECRYPTION BY PASSWORD = '<EnterPrivateKeyPasswordHere>');
GO
```

4. Cliquez sur **Exécuter**. Le certificat sera téléchargé sur le serveur et chiffré à l'aide de la clé principale de base de données.
5. Restaurez les sauvegardes de la base de données comme en temps normal, en suivant les instructions dans Restaurer des sauvegardes de la base de données.

Sauvegarde et restauration avec des colonnes chiffrées

Certaines fonctionnalités de Protege GX utilisent des colonnes de base de données chiffrées pour sécuriser vos données :

- Chiffrement du NIP
- Verrouillage sans fil ICT

Nous vous recommandons de sauvegarder le certificat de chiffrement du service de données pour vous assurer qu'il ne sera pas perdu si le serveur Protege GX tombe en panne. En outre, lorsque vous restaurez la base de données Protege GX sur un autre serveur ou un serveur de téléchargement secondaire, vous devez importer le certificat pour permettre au nouveau serveur d'accéder aux colonnes chiffrées.

Sauvegarde du certificat

Le certificat est créé sur la machine où le service de données est installé, qui peut ne pas être la même machine que l'installation de SQL Server.

1. Pour ouvrir l'outil Gestionnaire de certificats en tant qu'administrateur, appuyez sur les touches **Windows + R**, puis tapez **certlm.msc** dans la barre de recherche et appuyez sur **Contrôle + Maj + Entrée**.
2. Le répertoire de l'outil affichera Certificats : ordinateur local.
3. Ouvrez le dossier **Personnel**, puis cliquez sur le sous-dossier **Certificats**.
4. Dans la fenêtre affichant les certificats, faites défiler jusqu'à la colonne **Nom convivial** et localisez le certificat appelé Certificat de chiffrement du service de données.
5. Cliquez avec le bouton droit de la souris sur le certificat et sélectionnez **Toutes les tâches > Exporter**.
6. L'**assistant d'exportation de certificat** s'ouvre. Cliquez sur **Suivant**.
7. Vous devez sélectionner l'option **Oui, exporter la clé privée**.

   La clé privée est le composant critique du déchiffrement. Si vous n'exportez pas la clé privée, lorsque le certificat sera importé, il ne pourra pas déchiffrer les données chiffrées.

   Cliquez ensuite sur **Suivant**.
8. Assurez-vous que les options **Format de fichier d'exportation** suivantes sont sélectionnées :
   - **Inclure tous les certificats dans le chemin de certification si possible**
   - **Activer la confidentialité des certificats**

   L'option **Supprimer la clé privée si l'exportation est réussie doit être désactivée**.

   Cliquez ensuite sur **Suivant**.
9. Sur la page **Sécurité**, entrez et confirmez un **mot de passe** solide.

   Ce mot de passe doit être sauvegardé en toute sécurité avec les informations importantes du site.
10. Définissez **Chiffrement** sur AES256-SHA256, puis cliquez sur **Suivant**.
11. Spécifiez un **Nom du fichier** d'exportation et un chemin d'accès, puis cliquez sur **Suivant**.
12. Cliquez sur **Terminer** pour terminer l'exportation du certificat.
13. Lorsque l'exportation est terminée, confirmez que le fichier de sauvegarde du certificat .pfx a été exporté dans le chemin d'accès spécifié.
14. Le fichier doit être stocké en toute sécurité dans un endroit distinct afin d'être disponible en cas de besoin.

Vous devez sauvegarder le certificat et le mot de passe utilisé pour chiffrer la clé privée dans un endroit sûr. Si vous les perdez, il ne sera pas possible de restaurer les sauvegardes de la base de données sur un autre serveur.

Restauration du certificat

1. Assurez-vous que le fichier de sauvegarde .pfx est accessible depuis le PC local.
2. Arrêtez tous les services Protege GX avant de lancer l'importation.
3. Pour ouvrir l'outil Gestionnaire de certificats en tant qu'administrateur, appuyez sur les touches **Windows + R**, puis tapez **certlm.msc** dans la barre de recherche et appuyez sur **Contrôle + Maj + Entrée**.

4. Le répertoire de l'outil affichera Certificats: ordinateur local.
5. Ouvrez le dossier **Personnel**.
6. Cliquez avec le bouton droit de la souris sur le sous-dossier **Certificats** et accédez à **Toutes les tâches**, puis sélectionnez **Importer**.
7. L'**assistant d'importation de certificats** s'ouvre. Cliquez sur **Suivant**.
8. Cliquez sur **Naviguer...** et localisez le fichier de sauvegarde .pfx à importer, puis cliquez sur **Suivant**.

   Vous devrez changer le type de fichier en Échange d'informations personnelles (*.pfx;*.p12).
9. Saisissez le **mot de passe** qui a été créé au cours du processus d'exportation.
10. Options d'importation :
    - **Marquez cette clé comme exportable. Vous pourrez ainsi sauvegarder ou transporter vos clés ultérieurement**.
      - Cette option doit être sélectionnée si vous souhaitez pouvoir exporter/sauvegarder la clé privée avec ce certificat à l'avenir. Cette option est légèrement moins sûre.
      - La clé est plus sûre si cette option n'est pas sélectionnée, mais vous ne pourrez pas exporter la clé privée avec le certificat à l'avenir si vous perdez votre fichier de sauvegarde .pfx actuel.
    - Assurez-vous que l'option **Inclure toutes les propriétés étendues** est sélectionnée.
11. Cliquez sur **Suivant**.
12. Assurez-vous que le **magasin de certificats** est défini sur Personnel, puis cliquez sur **Suivant**.
13. Cliquez sur **Terminer** pour terminer l'importation du certificat.
14. Fermez l'outil Gestionnaire de certificats.
15. Redémarrez les services Protege GX.

Sauvegardes planifiées

Les sauvegardes planifiées permettent d'effectuer automatiquement une sauvegarde régulière. Les étapes suivantes décrivent une procédure de sauvegarde planifiée de base. Les scripts fournis peuvent être adaptés selon les besoins en fonction de l'environnement informatique et de la version SQL installée.

Créer une procédure de sauvegarde sauvegardée

La procédure SQL sauvegardée suivante peut générer une sauvegarde complète, différentielle ou du journal des transactions, avec un nom de fichier dynamique basé sur le type de sauvegarde et la date/heure. Vous pouvez créer une procédure sauvegardée en exécutant ce script en tant que requête dans SQL.

Cette procédure sauvegardée doit être modifiée selon les besoins de votre installation.

```
USE MASTER
GO

CREATE PROCEDURE dbo.sp_BackupDatabase
@databaseName sysname, @backupType CHAR(1)
AS
BEGIN
SET NOCOUNT ON;

DECLARE @sqlCommand NVARCHAR(1000)
DECLARE @dateTime NVARCHAR(20)

SELECT @dateTime = REPLACE(CONVERT(VARCHAR, GETDATE(),111),'/','') +
```

```
REPLACE(CONVERT(VARCHAR, GETDATE(),108),':','')

IF @backupType = 'F'
SET @sqlCommand = 'BACKUP DATABASE ' + @databaseName +
' TO DISK = ''C:\Backup\' + @databaseName + '_Full_' + @dateTime + '.bak'''

IF @backupType = 'D'
SET @sqlCommand = 'BACKUP DATABASE ' + @databaseName +
' TO DISK = ''C:\Backup\' + @databaseName + '_Diff_' + @dateTime +
'.bak'' WITH DIFFERENTIAL'

IF @backupType = 'L'
SET @sqlCommand = 'BACKUP LOG ' + @databaseName +
' TO DISK = ''C:\Backup\' + @databaseName + '_Log_' + @dateTime + '.trn'''

EXECUTE sp_executesql @sqlCommand
END
```

Vous devrez peut-être actualiser SSMS avec Ctrl + Maj + R avant que la procédure sauvegardée ne devienne disponible.

Créer un script de sauvegarde

Créez un script SQL pour exécuter la procédure sauvegardée. Enregistrez le script sous le nom dbbackup.sql et sauvegardez-le dans le dossier C:\ Backup.

```
sp_BackupDatabase 'databasename', 'backuptype'
GO
```

Le premier paramètre définit le le nom de la base de données : ProtegeGX ou ProtegeGXEvents. Le deuxième paramètre définit le type de sauvegarde : **F** pour complète, **D** pour différentielle ou **L** pour transactionnelle.

Vous pouvez créer plusieurs scripts pour effectuer les sauvegardes requises sur chaque base de données.

Créer une tâche planifiée Windows

Ces étapes créent une tâche planifiée pour exécuter le script SQL à l'aide de l'utilitaire sqlcmd.

Certaines versions de SSMS n'incluent pas l'utilitaire sqlcmd dans le programme d'installation. S'il n'est pas présent, vous devez télécharger les utilitaires de ligne de commande Microsoft pour SQL Server. Assurez-vous que la version téléchargée correspond à la version de SQL Server utilisée.

L'emplacement d'installation standard de cet utilitaire est C \Program Files(x86)\Microsoft SQL Server\Client SDK\ODBC\XXX\Tools\Binn, où XXX est un numéro basé sur le numéro de version de l'utilitaire. Cependant, notez que l'utilitaire peut être installé sous un numéro de version **antérieur** à celui prévu. Vous pouvez confirmer la version actuelle de l'utilitaire en tapant `sqlcmd -?` dans une invite de commande.

1. Ouvrez le planificateur de tâches de Windows en vous dirigeant vers **Démarrer > Panneau de configuration > Système et sécurité > Outils d'administration** et en sélectionnait **Planificateur de tâches**.
2. Dans le volet **Actions**, sélectionnez **Créer une tâche de base...**.
3. Saisissez un **nom** pour la tâche et une **description** facultative. Cliquez sur **Suivant**
4. Sélectionnez la fréquence et l'heure de la journée auxquelles la tâche doit s'exécuter. Cliquez sur **Suivant**.
5. Sélectionnez **Démarrer un programme**, puis cliquez sur **Suivant**.
6. Cliquez sur **Parcourir...** et accédez à l'emplacement d'installation de sqlcmd comme indiqué ci-dessus.
7. Sélectionnez sqlcmd.exe et cliquez sur **OK**.

8. Entrez la commande suivante dans le champ **Ajouter des arguments (facultatif)** : `-S.\Instancename -E -i C :\Backup\dbBackup.sql`.

   Cette commande se décompose comme suit :

   - `-S` (spécifie le nom du serveur et de l'instance pour SQL Server)
   - `-E` (vous permet d'établir une connexion de confiance)
   - `-i` (spécifie le fichier de commande d'entrée)

9. Cliquez sur **Suivant** pour terminer la création de la tâche.

Si vous souhaitez tester la tâche, revenez au **planificateur de tâches**, faites un clic droit sur la tâche et sélectionnez **Exécuter**.

Le répertoire **C\Backup** doit exister sur la machine serveur, sinon la procédure échouera.

Stockage hors site

Nous vous recommandons d'effectuer des sauvegardes régulièrement et d'utiliser une installation de stockage hors site ou un fournisseur externe pour vous assurer qu'une copie se trouve dans un emplacement hors site sécurisé.

Décharge de responsabilité et garantie

Limitation de responsabilité: Bien que tous les efforts ont été faits pour s'assurer de l'exactitude dans la représentation de ce produit, ni Integrated Control Technology Lté, ni ses employés, sera en aucun cas responsable, envers aucun parti, à l'égard des décisions ou des actions qu'ils pourraient entreprendre suite à l'utilisation de cette information. Conformément à la politique de développement amélioré d'ICT, la conception et les caractéristiques sont sujettes à modification sans préavis.

Pour des informations sur la garantie, consultez notre Garantie standard du produit.

Concepteurs et fabricants de produits électroniques intégrés de contrôle d'accès, de sécurité et d'automatisation.
Conçus et fabriqués par Integrated Control Technology Lté.