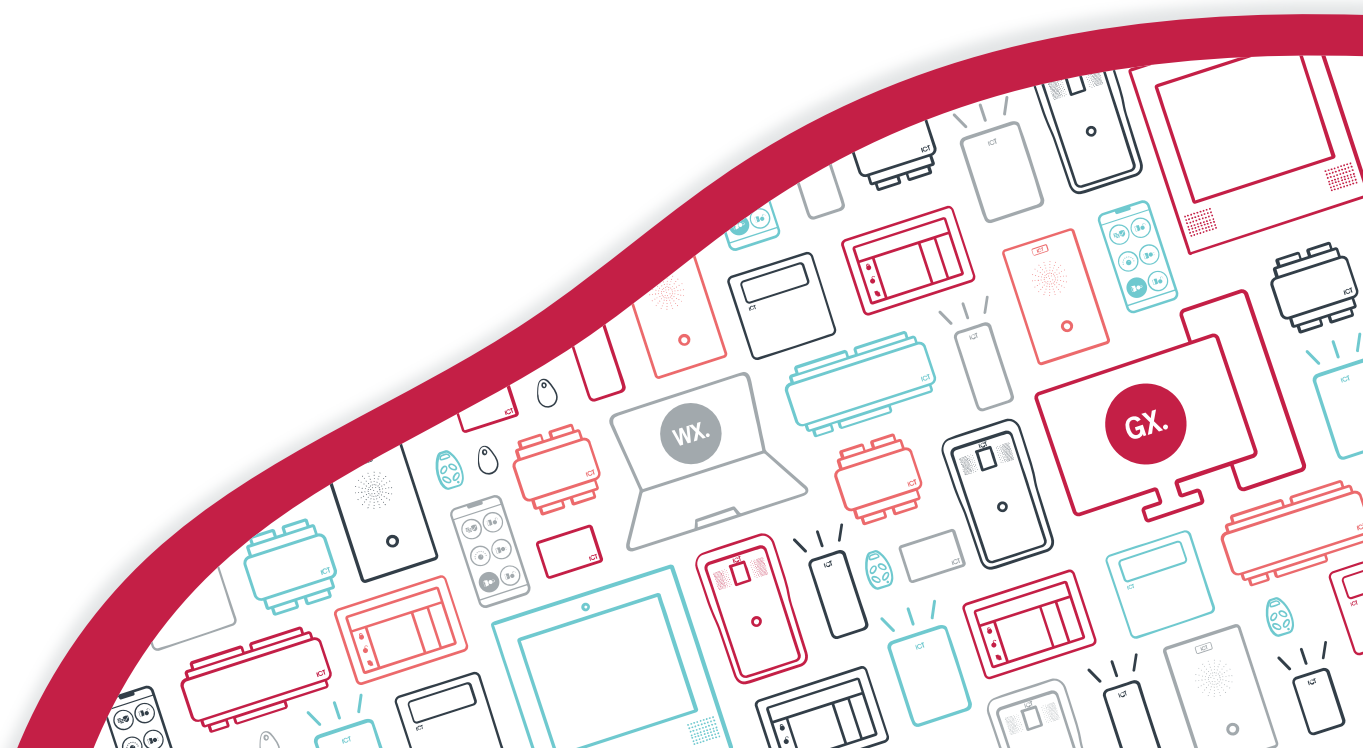
AN-210

Sécurisation de l’application mobile Protege

Note d'application



Dernière publication en 19-août-22 10:28.

Contenu

Introduction

Lorsque vous connectez l'application mobile Protege à un endroit Protege GX ou Protege WX, il est important de s'assurer que les communications sont sécurisées. Pour ce faire, il est fortement recommandé pour tous les sites en direct d'utiliser un certificat SSL signé par une autorité de certificat tiers de confiance. Ceci est utilisé pour crypter les communications entre l'application mobile et Protege GX ou Protege WX respectivement.

Si vous utilisez uniquement l'application mobile Protege pour accéder aux identifiants plutôt que de vous connecter à un endroit, cette configuration n'est pas nécessaire.

Sécurisation d'un lieu Protege GX

Par défaut, le client web Protege GX utilise un certificat SSL auto-signé qui est généré automatiquement lors de l'installation. Cependant, ce certificat n'est pas en soi considéré comme de confiance par les appareils mobiles. Si vous connectez l'application mobile à un emplacement Protege GX, il est fortement recommandé d'installer un certificat SSL tiers sur le site Protege GX dans IIS.

Avant de commencer, vous devez acquérir et valider un certificat d'une autorité de certification reconnue, comme :

- **GoDaddy**: https://www.godaddy.com/web-security/ssl-certificate
- **Network Solutions**: https://www.networksolutions.com/
- **RapidSSL**: https://www.rapidsslonline.com/
- **Let's Encrypt**: https://letsencrypt.org/

Pour plus d'informations, voir le Manuel d'installation du client web Protege GX.

Utilisation d'un certificat tiers pour le client web

Après avoir obtenu un certificat tiers auprès d'une autorité de certification de confiance, vous devez l'installer dans le site **ProtegeGXWeb** dans le gestionnaire Internet Information Services (IIS). Cela sécurise la connexion entre le client web et le navigateur web ou l'application mobile, et supprimera tout avertissement de sécurité.

Il s'agit de la méthode recommandée pour sécuriser le client web sur les sites en direct.

Remplir la demande de certificat

1. Ouvrez IIS Manager en appuyant sur les touches **Windows + R** pour ouvrir l'invite **Run**, puis entrez **inetmgr**.
2. Dans la section **IIS**, double-cliquez sur **Certificats de serveur**.
3. Dans le panneau **Actions** à droite, cliquez sur **Complete Certificate Request...**
4. Pour localiser votre fichier de certificat, cliquez sur le bouton **[...]**.
5. Sélectionnez ***. *** comme extension du nom de fichier.
6. Sélectionnez le certificat et cliquez sur **Ouvrir**.
7. Saisissez un **nom amical** pour le fichier de certificat, puis cliquez sur **OK**.

Lier le certificat au site ProtegeGXWeb.

1. Dans le panneau **Connexions** situé à gauche du gestionnaire IIS, développez le serveur sur lequel vous avez installé le certificat.
2. Cliquez sur la flèche déroulante à côté de **Sites** et sélectionnez le site **ProtegeGXWeb**.
3. Dans le panneau **Actions**, cliquez sur **Liaisons...**.
4. Sélectionnez la liaison https (port 8060) et cliquez sur **Modifier...**.

   Vous pouvez également ajouter une nouvelle liaison pour le port HTTPS par défaut de 443. Il n'est donc plus nécessaire de saisir le numéro de port dans l'URL lors de la connexion au client web.
5. Définissez le **Certificat SSL** sur le certificat que vous venez d'installer. Cliquez sur **OK**.
6. Vous verrez un avertissement concernant l'écrasement du certificat existant. Cliquez sur **Oui**.
7. Fermez la fenêtre des liaisons de sites et la fenêtre du gestionnaire IIS.

Lorsque le client web est mis à niveau, le certificat sera réinitialisé à la valeur par défaut. Répétez les étapes ci-dessus pour lier à nouveau le certificat personnalisé.

Configuration du lieu

Pour vous connecter au site Protege GX en HTTPS, vous devez mettre à jour l'adresse externe de l'application mobile vers le point d'extrémité HTTPS du client web.

1. Ouvrez une session dans l'application mobile Protege.
2. Accédez à **Mes lieux**.
3. Repérez l'endroit que vous voulez modifier et touchez l'icône **Modifier**.
4. Mettre à jour l'adresse **Adresse externe** et **Adresse interne** au point d'extrémité HTTPS du client web Protege GX. Cela devrait avoir la forme suivante :

   https://<nom de l'ordinateur>.<nom de domaine>:<numéro de port>/ProtegeGXWebClient/login.php

   Le numéro de port par défaut pour HTTPS est 8060.
5. Touchez **Enregistrer**.

Maintenant, l'application mobile devrait avoir une connexion cryptée au client web.

Sécurisation d'un lieu Protege WX

Protege WX contrôleurs sont pré-installés avec un certificat HTTPS auto-signé à l'usine. Bien que cela fournisse une connexion cryptée, elle n'est pas fiable pour les appareils mobiles et ne peut pas être utilisée pour fournir une connexion sécurisée entre le contrôleur et l'application mobile. Si vous connectez l'application mobile à un emplacement Protege WX, il est fortement recommandé d'installer un certificat SSL tiers sur le contrôleur Protege WX.

Installation d'un certificat tiers sur le contrôleur

Les étapes de base de l'installation d'un certificat tiers sur un contrôleur Protege WX sont décrites ci-dessous. Des instructions complètes sont incluses dans Note de l'application 280 : Configuration de la connexion HTTPS au Protege WX contrôleur.

1. Exposez le contrôleur à Internet via le transfert de port et assignez-lui un nom de domaine. Vous pouvez utiliser DDNS si l'adresse IP externe du contrôleur n'est pas stable.
2. Obtenir un certificat de tiers auprès d'une autorité de certification de confiance, comme :
   - **GoDaddy**: https://www.godaddy.com/web-security/ssl-certificate
   - **Network Solutions**: https://www.networksolutions.com/
   - **RapidSSL**: https://www.rapidsslonline.com/

   Assurez-vous de sélectionner **fichier ou validation HTTP** lorsqu'on vous demande de choisir une méthode d'authentification/validation. Vous aurez besoin d'un fichier . txt pour télécharger vers le contrôleur.
3. Téléchargez le fichier d'authentification fourni (extension.txt) dans le contrôleur. L'autorité de certification doit authentifier le domaine et envoyer le certificat signé.
4. Convertir le certificat en fichier . pfx. Assurez-vous d'inclure tous les certificats intermédiaires fournis par l'autorité de certification.

   Sans les certificats intermédiaires inclus, les appareils Android ne pourront pas se connecter.
5. Télécharger le certificat final signé au contrôleur.

Configuration du lieu

Pour vous connecter au contrôleur Protege WX via HTTPS, vous devez mettre à jour l'adresse externe de l'application mobile vers l'adresse HTTPS du contrôleur.

1. Ouvrez une session dans l'application mobile Protege.
2. Accédez à **Mes lieux**.
3. Localisez l'endroit que vous voulez modifier et touchez l'icône **Modifier**.
4. Mettre à jour l'adresse **External Address** et **Internal Address** à l'adresse HTTPS du contrôleur. Cette adresse doit être la même que l'adresse originale, mais en utilisant le préfixe https://.
5. Touchez **Enregistrer**.

Maintenant, l'application mobile devrait avoir une connexion cryptée au contrôleur Protege WX.

Utilisation de certificats auto-signés

Il est possible d'utiliser un certificat auto-signé personnalisé à la place d'un certificat tiers. Cela offre le même niveau de cryptage, mais n'est pas en soi considéré comme de confiance par les appareils mobiles. Par conséquent, une configuration supplémentaire est nécessaire pour installer le certificat sur chaque appareil mobile.

Les certificats auto-signés ne sont pas recommandés pour les sites en direct.

Obtention du certificat d'auto-signature

Avant de commencer, vous aurez besoin du fichier de certificat pour le certificat auto-signé qui est installé sur le Protege GX service SOAP ou Protege WX contrôleur respectivement.

- **Protege GX** : Vous pouvez créer et exporter un certificat personnalisé auto-signé pour le client web dans IIS. Pour obtenir des instructions, consultez le Manuel d'installation du client web Protege GX.
- **Protege WX** : Vous devez générer et installer un certificat personnalisé auto-signé sur le contrôleur Protege WX. Le certificat auto-signé installé en usine ne peut pas être utilisé. Pour des instructions, voir Note d'application 280 : Configuration de la connexion HTTPS au Protege WX contrôleur.

Assurez-vous d'avoir le mot de passe utilisé pour générer le certificat.

Installation du certificat sur un appareil Android

Les instructions suivantes peuvent varier en fonction de votre version d'Android et de l'appareil que vous utilisez.

1. Transférez le fichier de certificat sur votre appareil Android en utilisant l'une des méthodes suivantes :
   - Transférez le fichier de certificat au stockage local de l'appareil ou à la carte SD via USB.
   - Envoyez le certificat à l'appareil par courriel. Ceci n'est pas recommandé à moins d'utiliser un serveur de messagerie sécurisé.
2. Ouvrez **Paramètres** sur votre appareil.
3. Ouvrez le menu **Sécurité**.
4. Touchez la section **Avancé** pour l'agrandir et ouvrir **Chiffrement et identifiants**.
5. Sélectionnez **Installer à partir d'une ressource de stockage** (ou **Installer à partir d'une carte SD**). Localisez le certificat dans le gestionnaire de stockage.
6. Si nécessaire, saisissez les informations d'identification utilisées pour accéder à votre appareil.
7. Lorsque vous y êtes invité, saisissez le mot de passe du certificat.
8. Saisissez un nom pour le certificat.
9. Dans la liste déroulante **Utilisation de l'identifiant**, sélectionnez VPN et applications.
10. Touchez **OK**.

Comme il s'agit d'un certificat auto-signé, le système d'exploitation Android présentera occasionnellement un avertissement indiquant que votre réseau peut être surveillé par un tiers. Cela est normal et ne signifie pas que la connexion n'est pas cryptée.

Installation du certificat sur un appareil iOS

Les instructions suivantes peuvent différer en fonction de votre version d'iOS et de l'appareil que vous utilisez.

1. Transférez le fichier de certificat sur votre appareil iOS en utilisant l'une des méthodes suivantes :
   - Transférez le fichier du certificat sur le dispositif de stockage local de l'appareil via un port USB, iCloud Drive ou Airdrop.
   - Envoyez le certificat à l'appareil par courriel. Cela n'est pas recommandé, sauf si vous utilisez un serveur de messagerie sécurisé.
2. Sélectionnez le lien pour télécharger le certificat ou localiser et touchez le fichier de certificat pour ajouter le profil. Une fenêtre contextuelle s'affiche, indiquant que le profil a été téléchargé.
3. Ouvrez **Paramètres**.
4. Touchez la bannière **Profil téléchargé**.
5. Touchez **Installation**.
6. Si nécessaire, saisissez les informations d'identification utilisées pour accéder à votre appareil.
7. Touchez **Installer maintenant**.
8. Lorsque vous y êtes invité, saisissez le mot de passe du certificat.
9. Ouvrez **Paramètres**.
10. Naviguez vers **Général > À propos de > Paramètres de confiance du certificat**.
11. Cette page affiche les certificats de base installés sur l'appareil. Basculez à faire confiance **activé** pour le certificat que vous venez d'installer.
12. Touchez **Continuer** pour confirmer.

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