AN-210

Securing the Protege Mobile App

Application Note

Last Published: 11-Jul-23 08:39 AM

Contents

Introduction

When you are connecting the Protege Mobile App to a place in a Protege system it is important to ensure that the communications are secure. To achieve this, it is strongly recommended for all live sites to use an SSL certificate signed by a trusted third-party certificate authority. This is used to encrypt communications between the mobile app and the Protege system.

If you are only using the Protege Mobile App for credential access rather than connecting to a place, this configuration is not required.

Securing a Protege GX Place

By default, the Protege GX web client uses a self-signed SSL certificate which is automatically generated during installation. However, this certificate is not inherently trusted by mobile devices. If you are connecting the mobile app to a Protege GX place, it is strongly recommended that you install a third-party SSL certificate on the Protege GX site in IIS.

Before you begin, you must acquire and validate a certificate from a recognized certificate authority such as:

- **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/

For more information see the Protege GX Web Client Installation Manual.

Using a Third-Party Certificate for the Web Client

Once you have obtained a third-party certificate from a trusted certificate authority, you must install it in the **ProtegeGXWeb** site in Internet Information Services (IIS) Manager. This secures the connection between the web client and web browser or mobile app, and will remove any security warnings.

This is the recommended method for securing the web client on live sites.

Completing the Certificate Request

1. Open IIS Manager by pressing the **Windows + R** keys to open the **Run** prompt, then entering **inetmgr**.
2. In the **IIS** section, double-click **Server Certificates**.
3. From the **Actions** panel on the right, click **Complete Certificate Request...**
4. To locate your certificate file, click the ellipsis **[...]** button.
5. Select ***.*** as the file name extension.
6. Select the certificate and click **Open**.
7. Enter a **Friendly name** for the certificate file, then click **OK**.

Binding the Certificate to the ProtegeGXWeb Site

1. In the **Connections** panel on the left of IIS Manager, expand the server where you installed the certificate.
2. Click the drop-down arrow next to **Sites** and select the **ProtegeGXWeb** site.
3. In the **Actions** panel, click **Bindings...**.
4. Select the https binding (port 8060) and click **Edit...**.

   Alternatively, you can add a new binding for the default HTTPS port of 443. This removes the need to enter the port number in the URL when connecting to the web client.
5. Set the **SSL certificate** to the certificate you just installed. Click **OK**.
6. You will see a warning about overwriting the existing certificate. Click **Yes**.
7. Close the site bindings window and the IIS Manager window.

When the web client is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Configuring the Place

To connect to the Protege GX site over HTTPS, you must update the external address in the mobile app to the web client's HTTPS endpoint.

1. Log in to the Protege Mobile App.
2. Navigate to **My Places**.
3. Locate the place you want to edit and tap the **Edit** icon.
4. Update the **External Address** and **Internal Address** to the HTTPS endpoint of the Protege GX Web Client. This should have the form:
   https://<pcname>.<domainname>:<portnumber>/ProtegeGXWebClient/login.php

   The default port number for HTTPS is 8060.
5. Tap **Save**.

Now the mobile app should have an encrypted connection to the web client.

Securing a Protege WX Place

Protege WX controllers are pre-installed with a self-signed HTTPS certificate at the factory. While this provides an encrypted connection, it is not trusted by mobile devices and cannot be used to provide a secure connection between the controller and the mobile app. If you are connecting the mobile app to a Protege WX place, it is strongly recommended that you install a third-party SSL certificate on the Protege WX controller.

Installing a Third-Party Certificate on the Controller

The basic steps involved in installing a third-party certificate on a Protege WX controller are outlined below. Full instructions are included in Application Note 280: Configuring HTTPS Connection to the Protege WX Controller.

1. Expose the controller to the internet via port forwarding and assign it a domain name. You may use DDNS if the controller's external IP address is not stable.
2. Obtain a third-party certificate from a trusted certificate authority such as :
   - **GoDaddy**: https://www.godaddy.com/web-security/ssl-certificate
   - **Network Solutions**: https://www.networksolutions.com/
   - **RapidSSL**: https://www.rapidsslonline.com/

   Ensure that you select **file or HTTP-based validation** when asked to choose an authentication/validation method. You will require a .txt file to upload to the controller.
3. Upload the provided authentication file (.txt extension) to the controller. The certificate authority should authenticate the domain and send the signed certificate.
4. Convert the certificate to a .pfx file. Ensure that you include any intermediate certificates provided by the certificate authority.

   Without the intermediate certificates included, Android devices will fail to connect.
5. Upload the final signed certificate to the controller.

Configuring the Place

To connect to the Protege WX controller over HTTPS, you must update the external address in the mobile app to the controller's HTTPS address.

1. Log in to the Protege Mobile App.
2. Navigate to **My Places**.
3. Locate the place you want to edit and tap the **Edit** icon.
4. Update the **External Address** and **Internal Address** to the controller's HTTPS address. This should be the same as the original address, but using the https:// prefix.
5. Tap **Save**.

Now the mobile app should have an encrypted connection to the Protege WX controller.

Securing a Protege X Place

For connection to Protege X the place does not require any HTTPS configuration. The mobile app does not communicate directly with the controller, and communication between the mobile app and Protege X is automatically fully secured via HTTPS certificate.

However, it is still recommended that for maximum security the controller has a third-party certificate installed (see previous page) to secure access to the web interface.

Using Self-Signed Certificates

It is possible to use a custom self-signed certificate in place of a third-party certificate. This offers the same level of encryption, but is not inherently trusted by mobile devices. Therefore, additional configuration is required to install the certificate on each mobile device.

Self-signed certificates are not recommended for live sites.

Obtaining the Self-Signed Certificate

Before you begin, you will need the certificate file for the self-signed certificate which is installed on the Protege GX SOAP service or Protege WX controller respectively.

- **Protege GX**: You can create and export a custom self-signed certificate for the web client in IIS. For instructions, see the Protege GX Web Client Installation Manual.
- **Protege WX**: You must generate and install a custom self-signed certificate on the Protege WX controller. The self-signed certificate installed at the factory cannot be used. For instructions, see Application Note 280: Configuring HTTPS Connection to the Protege WX Controller.

Ensure that you have the password used to generate the certificate.

Installing the Certificate on an Android Device

The following instructions may differ depending on your version of Android and the device you are using.

1. Transfer the certificate file to your Android device using one of the following methods:
   - Transfer the certificate file to the device's local storage or SD card via USB.
   - Send the certificate to the device via email. This is not recommended unless using a secured email server.
2. Open the **Settings** on your device.
3. Open the **Security** menu.
4. Tap the **Advanced** section to expand it and open **Encryption & credentials**.
5. Select **Install from storage** (or **Install from SD card**). Locate the certificate in the storage manager.
6. If required, enter the credentials used to gain access to your device.
7. When prompted, enter the password for the certificate.
8. Enter a name for the certificate.
9. From the **Credential use** dropdown, select VPN and apps.
10. Tap **OK**.

As this is a self-signed certificate, the Android OS will occasionally present a warning stating that your network may be monitored by a third party. This is expected and does not mean that the connection is not encrypted.

Installing the Certificate on an iOS Device

The following instructions may differ depending on your version of iOS and the device you are using.

1. Transfer the certificate file to your iOS device using one of the following methods:
   - Transfer the certificate file to the device's local storage via USB, iCloud Drive or Airdrop.
   - Send the certificate to the device via email. This is not recommended unless using a secured email server.
2. Select the link to download the certificate or locate and tap the certificate file to add the profile. You will be presented with a popup stating that the profile has been downloaded.
3. Open **Settings**.

4. Tap the **Profile Downloaded** banner.
5. Tap **Install**.
6. If required, enter the credentials used to gain access to your device.
7. Tap **Install Now**.
8. When prompted, enter the password for the certificate.
9. Open **Settings**.
10. Navigate to **General > About > Certificate Trust Settings**.
11. This page displays the root certificates installed on the device. Toggle trust **on** for the certificate you just installed.
12. Tap **Continue** to confirm.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.