AN-366

Upgrading Protege GX to Version 4.3.402

Application Note

Last Published: 20-May-26 11:39 AM

Contents

Introduction

As part of ICT's commitment to secure software, the latest version of Protege GX includes cybersecurity enhancements that improve the protection of your systems.

The quarterly release version 4.3.402 introduces the following cybersecurity improvements:

- **Password policy**: All operator passwords must now meet the following requirements:
  - 8-32 characters long
  - Does not contain any part of your username or email address
  - Contains at least three out of four character types:
    - Uppercase letter
    - Lowercase letter
    - Number
    - Special character
- **One-time passwords**: It is not possible for anyone to set a permanent password for another operator, ensuring that only the operator knows their own password. When someone else sets an operator's password, the **Change password on next login** checkbox will be enabled. The operator will be required to set a new password the next time they log in.
- **Encrypted connections**: Protege GX no longer accepts unencrypted connections, preventing passwords and other sensitive data from being sent in the clear. It now requires:
  - Encrypted connections between server and clients (TLS 1.2)
  - Encrypted connection between server and SOAP service (TLS 1.2)
  - Encrypted connections between the SOAP service and integrated applications (HTTPS)
  - Encrypted connections between the web client and web browsers (HTTPS)
- **SOAP API changes**: Applications must log in to the SOAP service using LogonType 0. LogonType 1 has been deprecated.

Altogether, these enhancements ensure that all Protege GX operators have strong passwords, and those passwords are never sent over unencrypted connections.

There are also some additional changes that may affect your sites:

- **64-bit application**: The Protege GX Download Service is now a 64-bit service, improving download capacity. 32-bit operating systems are no longer supported.
- **Suprema integration**: The Suprema integration has been upgraded to support second-generation Suprema devices. Some first-generation devices are no longer supported.

Upgrading the Software

If your Protege GX software is currently using the previous public release (**4.3.352**), or any other version **prior to 4.3.370**, you will need to take additional actions when you upgrade to version 4.3.402.

If you do not complete these actions, parts of your system may not be able to connect after the upgrade. For example, clients and web clients might not be able to connect to the server.

When you upgrade to version 4.3.402, you must complete the following:

- If your server has a 32-bit operating system, you must migrate the server to a 64-bit operating system.
- If your site uses the Suprema integration, you need to upgrade or replace devices.
- You must upgrade all relevant software components at the same time.
- If you have custom third-party SOAP integrations, these may need to be updated by the developer before you upgrade.
- If your system uses unencrypted connections, you must implement encrypted connections.

- After the upgrade, all Protege GX operators must update their passwords. All new passwords must meet the password policy.

This application note provides detailed instructions for what you need to do when you upgrade Protege GX to version 4.3.402.

If your Protege GX version is already 4.3.370 or higher, most of these actions have already been completed and so are not required. Some operators may need to update their passwords to match the latest password policy.

Upgrade Checklist

This checklist provides a summary of the actions you need to complete when you upgrade Protege GX to version 4.3.402. You can print this page for easy reference as you work through the application note.

Before Upgrading

- ☐ Check operating system compatibility (see next page).
- ☐ Check SQL Server compatibility (see page 8)
- ☐ Check Suprema device compatibility and update DLL files (see page 8)
- ☐ Establish TLS 1.2 connections between server and clients (see page 9)
- ☐ Update SOAP service to use TLS 1.2 (see page 12)
- ☐ Update SOAP integrations from HTTP to HTTPS (see page 13)
- ☐ Update Data Sync Service from HTTP to HTTPS (see page 13)
- ☐ Upgrade third-party SOAP integrations (see page 14)
- ☐ Upgrade touchscreen entry station firmware and update to use HTTPS (see page 17)
- ☐ Validate web client HTTPS connection (see page 18)
- ☐ Update mobile app users from HTTP to HTTPS (see page 19)

Upgrading the System (see page 21)

- ☐ Back up your Protege GX database
- ☐ Make a copy of GXSV.exe.config (if customized)
- ☐ Upgrade Protege GX server
- ☐ Replace GXSV.exe.config (if customized)
- ☐ Upgrade Protege GX clients
- ☐ Upgrade Protege GX SOAP Service
- ☐ Rebind custom SOAP certificate (if used)
- ☐ Upgrade Protege GX Web Client
- ☐ Rebind custom web client certificate (if used)

After Upgrading (see page 22)

- ☐ Log in to Protege GX, update your own password if necessary
- ☐ Update passwords used by SOAP integrations
- ☐ Ask Protege GX operators to update their passwords
- ☐ Ask mobile app operators to update their passwords

Before Upgrading

Before you upgrade Protege GX, you must check the compatibility of some components to ensure that your server supports the latest versions.

In addition, we recommend that you set up all of the encrypted connections that you will need before upgrading. This ensures that your clients and other applications will not unexpectedly lose connection when you upgrade. It also allows you to easily roll back if you encounter issues or delays, which is much more difficult after you have upgraded the software. This section contains instructions for reviewing the system's current encryption status and completing any actions required.

If your systems already use encrypted communication, you will not need to make any changes.

Operating System Compatibility

The latest Protege GX software version is not compatible with 32-bit operating systems. If your server has a 32-bit operating system, you must migrate the system to a 64-bit operating system. Otherwise, the software installation will fail.

To check the server's current operating system:

1. Open a command prompt.
2. Type `systeminfo` and press **Enter**.
3. Check the **OS Name**. If the OS name includes **32-bit**, the server must be migrated to a supported 64-bit operating system.

   All Windows Server versions since 2008 R2 are 64-bit only, as are all Windows 11 versions. If your OS version is 64-bit, no action is required—proceed to the next section.

4. Check the **System Type**. If this is **x86-based**, you must also replace the server hardware with an x64-based processor.

If you need to upgrade the server, we recommend upgrading to Windows Server 2025 or Windows 11.

Upgrading the operating system from 32-bit to 64-bit requires reformatting the hard drives—even if you intend to use the same hardware, you must completely uninstall and reinstall Windows, SQL Server and Protege GX. In most cases, we would recommend upgrading the hardware at the same time to meet the latest specifications in the Protege GX Installation Manual.

For advice on server migration, see these knowledge base articles:

- Server Migration Preparation
- Protege GX Server Migration Process

Remember to contact ICT Technical Support to reset your server's hardware profile so you can license the new server.

Ensure that you also install the latest supported version of SQL server (see next page). As you reinstall the Protege GX software components, you can work through the instructions in this document to set up encrypted connections.

SQL Server Compatibility

Before you upgrade, you must check whether your SQL Server instance is compatible with the latest versions of Protege GX. Specifically, the database must support TLS 1.2 for encrypted communications.

To check your SQL Server version:

1. Open SQL Server Management Studio and log in.
2. In the **Object Explorer**, right click on the server name and select **Properties**.
3. You can find the **Version** on the **General** tab. The first number in the version tells you which year you have.
4. Depending on your version, follow the action in the table below:

First Number in Version	Year	Action
10	2008	This version is no longer supported by Microsoft or ICT. Upgrade to SQL Server 2022.
11	2012	This version is no longer supported by Microsoft or ICT. Upgrade to SQL Server 2022.
12	2014	This version is no longer supported by Microsoft or ICT. Upgrade to SQL Server 2022.
13	2016	This version is currently supported by ICT. However, Microsoft plans to drop support for this version after 14th July, 2026. This means that it will no longer receive bug fixes and security patches. We recommend that you upgrade to SQL Server 2022.
14	2017	No action required.
15	2019	No action required.
16	2022	No action required.
17	2025	No action required. This version has not yet been validated by ICT, but there is no need to change the installation unless you experience issues.

For assistance with the upgrade, see Upgrade SQL Server and Upgrade SQL Server Using the Installation Wizard (Setup) in the Microsoft Help.

Suprema Integration Support

This Protege GX version contains major changes to the Suprema integration. If your site uses the Suprema integration, be aware of the following before you upgrade Protege GX:

- Protege GX versions 4.3.393 and higher no longer support first-generation Suprema devices with V1 firmware. Some device models can be upgraded to V2 firmware, allowing you to keep using them with Protege GX. However, some models cannot be upgraded to a supported version and must be replaced with second-generation devices.

  If you purchased your Suprema devices from ICT, contact ICT Technical Support for assistance with upgrading them to V2 firmware. Otherwise, contact your Suprema dealer.

- When you upgrade Protege GX, you must also update the DLL files used by this integration. Download the latest DLL files from the ICT website and install them in the Protege GX directory.

For more details about supported device models and instructions for updating DLL files, see Application Note 264: Suprema Biometrics Integration with Protege GX.

Server-Client Connections (TLS 1.2)

The new Protege GX version requires an encrypted protocol for server-client communications. The available protocols are:

- **TLS 1.2**: TLS 1.2 is an industry-standard protocol that encrypts communications between the server and client. TLS uses an encryption certificate installed on the server to secure the connection.

  This protocol should be used for most Protege GX sites.
- **Windows Authentication**: Windows Authentication allows operators to log in to Protege GX with single sign-on using Active Directory. It is a licensed feature.

  This protocol should only be used on sites that use this integration. Windows Authentication can be combined with TLS 1.2, improving security for clients connecting from outside the firewall. For more information about setting up Windows Authentication, see Application Note 288: Using Active Directory in Protege GX.

By default, TLS 1.2 will be enabled when you install the new version. However, you may need to complete some additional steps to ensure that all components will connect. We recommend that you investigate the status of the system and, if needed, take action **before** you upgrade Protege GX.

Investigation

The following questions will help you determine whether any action is required to implement an encrypted connection.

A. What communication method does your system use currently?

If your system already uses TLS 1.2 or Windows Authentication and currently has no connection issues, no action is required.

If you do not know what connection type is in use, check the following:

1. If operators can log in to Protege GX with Windows Authentication, your system has Windows Authentication enabled. No action is required.
2. To check whether your system has TLS 1.2 enabled:
   - In a File Explorer, navigate to the installation directory: C:\Program Files (x86)\Integrated Control Technology\Protege GX
   - Open GXSV.exe.config.
   - Check whether the file includes the text `sslProtocols="Tls12"`.

     You can use **Ctrl+F** to search for this phrase.

   If this text is present, the system already has TLS 1.2 enabled. No action is required.
3. If the system has neither TLS 1.2 nor Windows Authentication, you should enable TLS 1.2 before you upgrade. Proceed to **B**.

B. How do the clients connect to the server?

TLS 1.2 uses certificates containing encryption keys to create a secure connection. When you enable TLS 1.2, the Protege GX server generates a default certificate. This certificate is sufficient for most client connections over the local network.

However, the default certificate only works when the client uses the internal IP address or hostname (i.e. computer name) of the server to connect. Any clients that connect from different networks always use an external IP address, external hostname or Fully Qualified Domain Name that is not listed on the default certificate. In these cases, you must generate and install a custom certificate to enable the connection.

In summary:

- Clients on the **same network** as the server can use the default certificate, as long as the operators use the **internal IP address or hostname** of the server.

- Clients on **different networks** (e.g. connecting over the internet) need a custom certificate that contains the server's **external IP address, external hostname or Fully Qualified Domain Name**.

Regardless of your answer, proceed to Enabling TLS 1.2.

Enabling TLS 1.2

If the system currently has an unencrypted connection (**A**), we strongly recommend that you enable TLS 1.2 **before** you upgrade Protege GX. Both the server and client must have TLS 1.2 enabled to allow the connection.

To enable TLS 1.2:

1. Uninstall Protege GX.
2. Run the installer for your current Protege GX version (e.g. 4.3.352).
3. On the **Customize WCF TCP/IP Port** page, select **TLS 1.2**.
4. Complete the installation.
5. Repeat the reinstallation process for at least one client machine on the same network.
6. Validate that you can log in to the server from this client. Make sure you use the local IP address or hostname of the server.

All clients on the **same network** as the server should be able to connect using its local IP address or hostname. You can uninstall, reinstall and validate them now, or do this when you upgrade the system (see page 21).

If your system has clients on **different networks**, you must install a custom certificate on the server. Proceed to Installing a Custom TLS 1.2 Certificate.

See the Protege GX Installation Manual for additional security recommendations for TLS 1.2 connections.

Installing a Custom TLS 1.2 Certificate

To allow remote connections, you must install a custom certificate that contains the server's external IP address, external hostname or Fully Qualified Domain Name.

This section gives instructions for a standard certificate. For a wildcard certificate, see the Protege GX Installation Manual. There is additional troubleshooting assistance in this Knowledge Base Article.

Acquiring a Custom Certificate

To harden your system, we recommend using a trusted certificate. There are two main methods for acquiring a trusted certificate:

- If the company has an internal PKI (Public Key Infrastructure), they can issue the server a certificate that is trusted internally.
- You can acquire a trusted certificate from a third-party certificate authority.

Alternatively, you can generate a self-signed custom certificate using a tool such as OpenSSL.

You will need a certificate in **.pfx** format, as well as the **password** used to create the certificate. The .pfx format includes the private key needed to secure the connection. If you receive a certificate format that does not include the private key (e.g. .cer, .crt, .pem), you must first combine it with the private key and export a .pfx file.

Make sure that the certificate contains the names and IP addresses that operators will use to log in to the server (e.g. the Fully Qualified Domain Name or external IP address).

Installing the Custom Certificate

To install the custom certificate on the server computer:

1. Copy the .pfx file to the Protege GX server.
2. Double click the certificate to initiate the **Certificate Import Wizard**.

3. Set the **Store Location** to Local Machine.
4. Do not change the **File to Import**.
5. Enter the password used to generate the .pfx file.
6. Set the place where you wish to store the certificate as the **Personal folder**.
7. Complete the import.

Configuring Protege GX to use the Custom Certificate

Once the custom certificate is installed you can configure Protege GX to use that certificate for its connections.

1. Press **Windows + R**. Type **certlm.msc** and press **Ctrl + Shift + Enter**. This opens the Certificate Manager.
2. Navigate to **Certificates (Local Computer) > Personal > Certificates**.
3. You should be able to see your installed certificate here. Double click on it.
4. In the **Details** tab, locate the field named **Thumbprint** and copy the data from it to a safe place.
5. In the File Explorer, navigate to the installation directory: C:\Program Files (x86)\Integrated Control Technology\Protege GX
6. Open **GXSV.exe.config**.

   Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

7. Locate the following section in the XML:
   /configuration/system.serviceMode1/behaviors/serviceBehaviors/behavior[@name="md"]/serviceCertificate

   If this section does not exist it is because you did not install Protege GX with TLS enabled.

8. In the `<serviceCertificate>` tag, change the `findValue` to the thumbprint of the new certificate you installed. The result will look similar to the following:

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

9. **Save** the config file.
10. Make a copy of the config file and save it to a safe location. The software will overwrite the config file when you upgrade it, so you must reapply the custom certificate thumbprint afterwards.
11. **Restart** the Protege GX Data Service for the changes to take effect.

Server-SOAP Service Connections (TLS 1.2)

The SOAP service must use the same protocol as the Protege GX server to allow communication. This is TLS 1.2 for most systems, or Windows Authentication for systems that use Active Directory integration.

If your system already uses TLS 1.2 or Windows Authentication, no action is required.

If your system is currently unencrypted, we recommend that you enable TLS 1.2 for the SOAP service before you upgrade the software. To enable TLS 1.2:

1. Open **Add or Remove Programs** on the Protege GX server. Find the **Protege GX SOAP Service** and click **Uninstall**.
2. Run the Protege GX SOAP Service installer.
3. On the **Customize WCF TCP/IP Port** page, select **Enable TLS 1.2 Authentication**.
4. Complete the installation.

SOAP Service-Integration Connections (HTTPS)

All applications connected to the SOAP service must use an HTTPS connection. There are a few key aspects that you need to consider:

- Applications must use the **HTTPS port** to connect to the SOAP service (8040 by default). They can no longer use the HTTP port (8030 by default).
- Any third-party applications used on your site must support HTTPS and the latest version of the SOAP service.
- The SOAP service must be accessible via HTTPS on the computers where the applications are installed.

This may affect the following first-party ICT integrations:

- ICT Data Sync Service
- Protege Tenancy Portal Sync Service
- KeyWatcher Integration Service

  Must also be upgraded to version 1.0.0.11.
- KeySecure Integration Service

This will also affect any third-party SOAP integrations that you have installed.

Updating ICT SOAP Integrations

All SOAP integrations that used HTTP must be updated to use the HTTPS port (8040 by default).

The instructions may differ slightly for different integration services. See the relevant documentation for more information. Not required for the Protege GX Web Client.

To update a service to use HTTPS:

1. First, check whether HTTPS is accessible on the computer where the service is installed. Open a web browser and enter the HTTPS URL:

   https://server.domain:8040/ProtegeGXSOAPService/service.svc

   Replace the placeholders with the details for your server.
2. If the SOAP service is accessible, you will see a default page with the following text. You may have to click through a security warning first.

   Service1 Service
   You have created a service.

   If you do not see this page, you may need to adjust the networking or certificates to allow the connection. See Resolving HTTPS Accessibility Issues for causes and resolution.
3. Open the configuration tool for the service.
4. Check the **SOAP Server Address**. If this is already an HTTPS address, there is no need to change it.
5. Click **Stop** to stop the service.
6. Set the **SOAP Server Address** to the HTTPS address:

   https://server.domain:8040/ProtegeGXSOAPService/service.svc
7. Click **Save**.
8. Click **Start**. Ensure that the service starts successfully and doesn't display any errors.
9. Validate that the integration still functions correctly.

Repeat for all integration services connected to the SOAP Service.

Updating Third-Party SOAP Integrations

If you use a SOAP integration that was created in-house or by a third-party developer, you must contact the developer to ensure that the integration supports the latest version of the SOAP service.

The integration must support the following:

- Connecting to the SOAP service via HTTPS.
- Logging in with LogonType 0. LogonType 1 has been deprecated.

Optionally, it may also support the following changes:

- New ChangePassword request, allowing operators to update their passwords as they log in.
- New error codes 220 (submitted password does not match policy) and 221 (login failed because password change required).

The developer should request the latest version of the Protege GX SOAP Service API Specification from ICT.

Before you update Protege GX, we recommend that you upgrade third-party integrations (if necessary) and update them to connect to SOAP via HTTPS.

Resolving HTTPS Accessibility Issues

There are two main reasons that the SOAP service may not be available over HTTPS on another computer:

- The firewall of the network or computer may be blocking the HTTPS port (e.g. if you have only opened the HTTP port in the past). Open the HTTPS port 8040 on all relevant firewalls. You can also close port 8030 when there are no further applications using HTTP.
- The default certificate used by the SOAP service is self-signed and may not have the correct Subject Alternative Names. Therefore, the other computer may reject this certificate. Follow the instructions below:
  - Using a Trusted Certificate for SOAP
  - Using a Self-Signed Certificate for SOAP

Using a Trusted Certificate for SOAP

The best method for securing the HTTPS connection is to install a certificate that is inherently trusted by the relevant computers. This can be a third-party certificate from a known certificate authority, or a certificate issued from an internal Public Key Infrastructure (PKI).

You will need a certificate in **.pfx** format, as well as the **password** used to create the certificate. The .pfx format includes the private key needed to secure the connection. If you receive a certificate format that does not include the private key (e.g. .cer, .crt, .pem), you must first combine it with the private key and export a .pfx file.

Once you have obtained a trusted certificate, you must install it in the **ProtegeGX** site in Internet Information Services (IIS) Manager. This secures the connection between the SOAP service and other applications.

This is the recommended method for securing the SOAP service 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 ProtegeGX 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 **ProtegeGX** site.
3. In the **Actions** panel, click **Bindings...**.
4. Select the https binding and click **Edit...**.
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 SOAP service is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Using a Self-Signed Certificate for SOAP

As an alternative to an external certificate, you may use a self-signed certificate for the SOAP service. As self-signed certificates are not inherently trusted by other computers and applications, it is necessary to import the certificate to the trusted root store of each other computer that will connect to the SOAP service directly.

The instructions below cover creating a custom self-signed certificate, binding it to a site, and importing it as a trusted certificate on other computers.

For live sites, it is recommended that you use a third-party certificate or a trusted certificate issued by your IT department.

Creating and Exporting a New Self-Signed Certificate

There are multiple methods to create a self-signed certificate. The steps below describe how to create a certificate using IIS Manager. Alternatively, you may create a certificate using a utility such as OpenSSL, or a certificate may be supplied by your IT department.

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 **Create Self-Signed Certificate...**
4. Enter a name for the certificate.
5. Set the certificate store to Personal.
6. Click **OK**. Your new certificate will be added to the list.
7. Double-click on the new certificate to view it.
8. Navigate to the **Details** tab and select **Copy to File...** The certificate export wizard will open.
9. Complete the instructions in the wizard, selecting these options:
   - Do **not** export the private key.
   - **Format**: DER encoded binary X.509 (.CER)
   - Specify the name and location where you want to export the certificate.
10. Click **Finish** to complete the export.

Binding the Certificate to the ProtegeGX 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 **ProtegeGX** site.
3. In the **Actions** panel, click **Bindings...**.
4. Select the https binding and click **Edit...**.

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 SOAP service is upgraded, the certificate will be reset to the default. Repeat the steps above to rebind the custom certificate.

Importing the Certificate to Another Computer

This section must be completed on each computer that will connect directly to the SOAP service.

1. Open the certificate manager by pressing **Windows + R**, then entering **certlm.msc**.
2. Browse to **Certificates - Local Computer > Trusted Root Certification Authorities > Certificates**.
3. Right click on the Certificates folder and select **All Tasks > Import...**. This will open the certificate import wizard.
4. Click **Next**.
5. Browse to and select the certificate file that you exported.
6. Select the option to **Place all certificates in the following store** and enter Trusted Root Certification Authorities as the certificate store.
7. Click **Finish** to complete the import.

SOAP Service-Entry Station Connection (HTTPS)

If your Protege Vandal Resistant Touchscreen Entry Station has a user directory synchronized with Protege GX, you must upgrade the firmware and update the settings to use HTTPS.

To update the entry station to use HTTPS:

1. Log in to the entry station.
2. On the **Home Page**, the device's current firmware version is displayed in the **Application** field.

   If the firmware version is **1.12.203 or higher**, you do not need to upgrade the firmware. If the firmware version is lower than 1.12.203, you must upgrade the entry station to the latest firmware version on the ICT website.
3. Navigate to **Device Settings | Directory Sync**.
4. Set the **SOAP Server Protocol** to https.
5. Set the **SOAP Server Port** to the SOAP HTTPS port (**8040** by default).
6. Click **Save**.

Web Client-Web Browser Connections (HTTPS)

In the latest version, the Protege GX Web Client only allows HTTPS connections from web browsers. This will have the following effects:

- You must open the HTTPS port (**8060** by default) on the computer with the web client installed and any other relevant firewalls. You can close the HTTP port (8050).
- Operators must enter the HTTPS URL to access the web client. This is:

  https://server.domain:8060/ProtegeGXWebClient/login.php

  > Replace the placeholders with the details for your server.

- Operators must update any bookmarks they use to access the web client.
- The web client uses a self-signed certificate for the HTTPS connection. These certificates are not inherently trusted by web browsers, so operators will see a security warning when they log in to the web client. Optionally, you can remove the security warning by installing a custom HTTPS certificate. See the Protege GX Web Client Installation Manual for instructions and further security recommendations.

We recommend that you validate the HTTPS connection on at least one computer outside of the server before you continue. To validate the connection, enter the HTTPS URL into a web browser:

https://server.domain:8060/ProtegeGXWebClient/login.php

If the web client login page appears, the connection was successful.

> Alternatively, you can replace the web client with the new **Protege GX Web App**. This new application is easy to install and provides improved performance and user experience.
>
> The web app does not yet have all of the features available in the web client, so we recommend that you review it on the test bench first to ensure that it has everything needed for this site. For more information and installation instructions, see the Protege GX Web App Installation Manual.

Mobile App Connections (HTTPS)

After the upgrade, Protege GX will only allow HTTPS connections from Protege Access+ or the Protege Mobile App. Any app used for site monitoring and control must be updated to use HTTPS if it doesn't already.

We recommend updating and validating at least one device before you upgrade Protege GX. It will be more convenient for most end users to update their settings after you upgrade Protege GX, at the same time that they update their passwords.

Only site control is affected. No change is required to keep using mobile credentials.

Protege Access+

Protege Access+ connects to the SOAP service over HTTPS (port 8040 by default). However, if any users are currently using HTTP (port 8030), they must update their apps to use HTTPS instead.

In addition, the SOAP service HTTPS port must be able to receive incoming connections from the Protege cloud service, if it isn't already. You can close any routes or rules that allow connection to the HTTP port.

To change the connection from HTTP to HTTPS in Protege Access+:

1. Log in to Protege Access+.
2. In the **Organizations** tab, open your organization.
3. Swipe from the bottom up to fullscreen the organization.
4. Tap the **Settings** icon ⚙ at the top left.
5. Select **Delete organization**.
6. Tap **+** to add a new organization.
7. Select **https** and enter the rest of the connection details.

See the Protege Access+ Setup Guide for more detailed instructions.

Protege Mobile App

The Protege Mobile App connects to the web client over an internal network or over the internet. The latest web client version only allows HTTPS connections from the app.

Instead of updating the settings for the Protege Mobile App, we recommend transitioning your end users to the Protege Access+. The new app is faster, cleaner and easier to use than the previous app.

See the Protege Access+ Setup Guide for more information about this app and instructions for connecting to organizations. Note that Protege Access+ connects to the SOAP service, not the web client. You will need to reconfigure the network to allow incoming connections from the Protege cloud service to the SOAP service.

If your end users want to continue using the Protege Mobile App, you must update them to use HTTPS connections. If the HTTPS connection is not currently available, you must:

- Make the HTTPS port of the web client (port 8060 by default) accessible on the internal network and/or internet. You can close the HTTP port (port 8050 by default).
- Install a third-party HTTPS certificate on the web client. This is required for mobile phones to allow the connection, as they do not inherently trust the self-signed certificate used by the web client.

For more information and instructions, see Application Note 210: Securing the Protege Mobile App.

To change the connection from HTTP to HTTPS in Protege Mobile:

1. Log in to the Protege Mobile App.
2. Navigate to **My Places**.

3. Update the **External Address** and **Internal Address** to the HTTPS endpoint for the web client. This should have the format:

   https://server.domain:8060/ProtegeGXWebClient/login.php

4. Tap **Save**.

Upgrading the System

We recommend upgrading the system in this order:

1. Download the latest software installers from the ICT website (unless newer installers have been provided to you by ICT Technical Support).
2. Before you upgrade the system, we recommend that you take a database backup. Navigate to **Global | Global settings | General** and click **Backup now**.
3. If you have edited **GXSV.exe.config** and have not already made a backup, navigate to the installation directory (C:\Program Files (x86)\Integrated Control Technology\Protege GX). Make a copy of the file and place it in a different folder.
4. Make copies of any other config files that you have customized for your installation.
5. Upgrade the **Protege GX server**.

   If you have customized GXSV.exe.config, replace this file with your saved copy. Restart the Protege GX Data Service.
6. Upgrade **all client workstations**.

   If you have a large number of workstations to upgrade, see Application Note 167: Protege GX Silent Client Installation for an automated method.
7. Upgrade the **Protege GX SOAP Service**.

   If you use a custom certificate for the SOAP service, you must bind the certificate to the IIS site again. Follow the instructions for binding a certificate in Using a Trusted Certificate for SOAP.
8. Upgrade the **Protege GX Web Client**.

   If you use a custom certificate for the web client, you must bind the certificate to the IIS site again. Follow the instructions for binding a certificate in Using a Trusted Certificate for SOAP, but use the ProtegeGXWeb site instead of the ProtegeGX site.
9. Validate that remote clients and web clients can connect to the server successfully.

After Upgrading

In the latest version of Protege GX, all passwords must meet the new password policy. The policy is as follows:

- 8-32 characters long
- Does not contain any part of your username or email address
- Contains at least three out of four character types:
    - Uppercase letter
    - Lowercase letter
    - Number
    - Special character

To ensure that passwords meet the policy, Protege GX requires every operator to update their password.

Workstation and Web Client operators

The first time an operator logs in to Protege GX, they will be prompted to set a new password.

SOAP operators

Any operator passwords used for SOAP connections must also be updated. The application will fail to connect until you update the password.

To update a SOAP operator password:

1. Log in to Protege GX using the username and password of the SOAP operator.
2. When prompted, set a new password.
3. Open the configuration tool for the service.
4. Click **Stop** to stop the service.
5. Set the **Password** to the new password.
6. Click **Save**.
7. Click **Start**. Ensure that the service starts successfully and doesn't display any errors.
8. Validate that the application can connect to the SOAP service.

Mobile App Operators

Any operator who is using Protege Access+ or Protege Mobile for site monitoring and control must also update their passwords. If required, they can also update the app to use HTTPS at the same time.

For Protege Access+:

1. Log in to Protege Access+.
2. In the **Organizations** tab, open your organization.
3. Swipe from the bottom up to fullscreen the organization.
4. Tap the **Settings** icon at the top left.
5. Select **Delete organization**.
6. Tap **+** to add a new organization.
7. Select **https** and enter the rest of the connection details.
8. Enter your **Username** and the new **Password**.
9. Tap **Next** and complete the connection process.

For more details, see the Protege Access+ Setup Guide.

For Protege Mobile:

1. Log in to the Protege Mobile App.
2. Navigate to **My Places**.
3. If required, update the **External Address** and **Internal Address** to the HTTPS endpoint for the web client. This should have the format:

   https://<pcname>.<domainname>:8060/ProtegeGXWebClient/login.php
4. Enter your new **Password**.
5. Tap **Save**.