Protege GX Web App

Installation Manual

Last Published: 05-May-26 4:02 PM

Contents

Introduction

The Protege GX Web App is a browser-based interface for Protege GX, allowing end users to manage access, control the site and review events from a clean, easy-to-use interface. Operators can access the web app from any device with a web browser—desktops, laptops, tablets and mobile phones.

When you install the web app, you must also install the Protege GX Extended Event Service to handle events and statuses from controllers. The extended event service is faster, more scalable and more reliable than the existing event service.

This document provides instructions for installing and configuring the Protege GX Web App and Extended Event Service.

If you don't need the web app, you can install the extended event service separately. See Application Note 363: Protege GX Extended Event Service.

Web App vs. Web Client Comparison

While the Protege GX Web App is still in development, ultimately it will become the replacement for the Protege GX Web Client. If you're upgrading an existing site or setting up a new one, we recommend you try the web app: it looks better, performs better and will gain more feature support over time.

Web App Features

The web app already supports most of the key features of the web client, including:

- User management
- Access level management
- Operator management
- Schedule and holiday management
- Event monitoring and export
- Device status monitoring
- Device control
- Multi-language support

In addition, the web app offers a number of enhancements over the existing web client, including:

- New, modern user interface
- Support for desktop, tablet and mobile screens
- Two-factor authentication for better security
- Improved filtering and sorting of tables with saved views
- Comprehensive help documentation aimed at end users
- Bundled with the extended event service, improving the reliability of event and status monitoring

Web App Limitations

The following features from the web client are currently not supported, but will be added in future releases:

- Sign on with Windows Authentication
- Viewing and editing groups (e.g. door groups, area groups)
- Viewing and editing calendar actions
- Viewing and editing daylight savings
- Viewing and editing roles and security levels
- Running Protege GX reports

In addition, the web app does not currently have full support for:

- ICT wireless locking systems
- Third-party wireless locking systems
- Biometric credentials

If a feature you need is not currently available in the web app, contact ICT to find out where it is on our roadmap.

Prerequisites

Protege GX Components

Component	Version	Notes
Protege GX Extended Services Installer	Latest version from ICT	This installer installs the **web app**, **extended event service** and **admin tool** on the Protege GX server. If you already have the extended event service on the server, uninstall it before running the combined extended services installer.
Protege GX Server	4.3.398.2 or higher	You must have a working Protege GX installation before installing the web app and extended event service. For more information, see Protege GX Server Setup (page 11).
Protege GX Controllers	2.08.1487 or higher	Ensure that all existing controllers are online with Protege GX before you begin.

Other Software Prerequisites

Component	Versions	Editions	Compatibility Level
SQL Server	2016 2017 2019 2022	Express Standard Enterprise	The Compatibility Level must be **SQL Server 2016 (130) or higher** for both the ProtegeGX and ProtegeGXEvents databases. See View or change the compatibility level of a database in the Microsoft Help to check the compatibility level. We recommend using the highest available compatibility level for both databases.

.NET version 8 will be installed by the Protege GX Extended Services Installer, if it is not already available.

Permissions

You must have administrator permissions on the computer where you are installing the web app and extended event service.

Licensing

You must have an active Protege GX SSN to install the new services. No additional licenses are required.

IT Requirements

This section covers the server, networking and cybersecurity requirements for the Protege GX extended services (web app and extended event service). We recommend you share this information with the site's IT team for assistance.

The following requirements are in addition to the requirements for a standard Protege GX installation. For the standard requirements, see the Protege GX Installation Manual and Protege GX Network Administrator Guide, available from the ICT website.

See the Maintenance section for related IT tasks such as backing up and restoring databases.

Server Specifications

Before you install the extended services, we recommend that the server meets the current requirements for a new Protege GX installation.

Component	Server: 1-29 Controllers	Server: 30+ Controllers	Recommendations
CPU	64-bit 4 cores 8 threads 3.3GHz	64-bit 6 cores 12 threads 2.5GHz	For new sites, select a CPU model that is no more than 5 years old at time of commissioning.
RAM	16GB	32GB	Install additional RAM whenever possible to improve performance.
Disk	500GB	500GB	Use an SSD, as this will give better performance than an HDD.
Ethernet	100Mb/1Gb	100Mb/1Gb	Use Cat5e or Cat6 ethernet cables for optimal transmission speeds.

If you have an existing system with lower server specifications, you are not required to upgrade before installing the web app. However, if the system experiences performance issues we strongly recommend that you upgrade your server to match the specifications above.

Extended Event Service Networking

The extended event service requires the following communication paths to be available. Open firewall ports as necessary.

From	To	Default Port	Transport Protocol	Description
Extended Event Service	SQL Server (ProtegeGX Instance)	1433 1434	TCP/IP	Save events and configuration changes to the databases.
Extended Event Service	Protege GX Event Service	22000*	TCP/IP	Send status updates.
Controllers	Extended Event Service	32005*	TCP/IP	Send events, status updates and configuration changes.

* These ports are configurable and may be changed by the integrator—see Connecting Controllers to the Extended Event Service.

Typically, most controllers are on the same network as the Protege GX services. However, some systems have remote controllers on separate Layer 3 networks. In this case, you must set up firewall routes and rules to allow the controllers to communicate with the extended event service.

Web App Accessibility

The Protege GX Web App must be accessible in the web browser to any Protege GX operator. It is designed to be used on a range of devices, including computers, tablets and mobile phones. Depending on your organization's policies, Protege GX operators may also need to access the web app from outside the local network. Some actions may be required to provide access to operators.

By default, you can access the web app on the computer where it is installed using either https://localhost:8083 or https://127.0.0.1:8083.

Web App Port

The web app port on the Protege GX server must be accessible to other computers on the network. Configure the firewall on the Protege GX server to allow incoming requests to this port.

The default port for the web app is **8083** (HTTPS).

You can modify this port as required—see Changing the HTTPS Port for instructions. We recommend setting the port to the standard HTTPS port of **443** if this is available. This allows users to connect to the web app without specifying a port.

HTTP access is not available.

URL

The web app can be accessed from a web browser using the Protege GX server's IP address or name, e.g. **https://servername.domainname:8083**

We recommend that you set up a static DNS entry mapping the IP address of the Protege GX server to a URL that is easy for users to remember.

HTTPS Certificate

The web app is secured with a self-signed HTTPS certificate. Self-signed certificates are not trusted by computers and web browsers by default, so operators may receive security warnings. Some web browsers may completely block access to the web app.

There are a few options for resolving this issue:

- For internal access, issue a certificate from an internal public key infrastructure.
- For internal and external access, acquire a certificate from a third-party certificate authority.
- (Not recommended) If you wish to use the self-signed certificate that was created by the server, you must install it on each device that will need access. On Windows domains, you can use a group policy to push this certificate to all computers in the domain.

Make sure you issue the certificate to the URL that operators will use to access the web app.

When the extended services have been installed, you can install the certificate—see Installing a Custom HTTPS Certificate.

External Access

Some organizations allow operators to access Protege GX from devices outside the network. The recommended methods for offsite access are:

- Use a VPN to allow authorized people to connect to your network externally.
- Set up a secure tunnel or reverse proxy to allow people to connect to the web app over the internet.

For example, Cloudflare Zero Trust enables you to create a tunnel. When setting up a Cloudflare tunnel, use the following settings:

- **Service Type**: HTTPS
- **URL**: IP address and HTTPS port used by the web app (e.g. 192.168.1.2:8040)
- **No TLS Verify**: Enabled

Email Server

We recommend that you connect Protege GX to an email server to enable it to send outgoing emails. This is used for several key features in the web app, including:

- Sending invitation emails to operators
- Resetting forgotten passwords
- Exporting large files such as event reports

The web app will function without an email server, but these features will not be available. For example, operators would only be able to generate small event reports that can be downloaded immediately.

You can use an existing email (SMTP) server owned by the organization or a free provider such as Gmail. The Protege GX server must be able to access the email server over the internal or external network.

If the existing Protege GX server is already connected to an email server, no change is required. If you wish to add an email server, the integrator will need the outgoing server address, port and login credentials. See Setting up an Email Server for setup instructions.

To use Gmail as an email server, you must generate an app password. See Sign in with app passwords in the Google help documentation.

Installation Checklist

Before You Begin

- ☐ Discuss the IT requirements with the site's IT administrator (see page 7).
- ☐ Ensure that you have all of the prerequisite software (see page 6).

Prepare Protege GX

- ☐ Install or upgrade the Protege GX server (see next page).
- ☐ **New sites**: Bring at least one controller online.
- ☐ **Existing sites**: Ensure that all controllers are online and operational.
- ☐ Set up an email server (see next page).
- ☐ Take backups of the Protege GX databases.

Install the Extended Services

- ☐ If the extended event service is separately installed on the server, uninstall it.
- ☐ Run the Protege GX Extended Services installer (see page 13).
- ☐ Connect the controllers to the extended event service (see page 14).

Set up the Protege GX Web App

- ☐ Log in to the web app and set up two-factor authentication (see page 16).
- ☐ Validate functionality in the web app (see page 17).
- ☐ Make the web app accessible across the network (see page 7).
- ☐ Prepare locations, views and dashboards (see page 18).
- ☐ Invite and onboard operators to the web app (see page 20).

Protege GX Server Setup

The Protege GX extended services must be installed alongside an existing Protege GX server and databases. Before you begin, ensure that your Protege GX system is up and running.

New Protege GX Systems

1. Download the Protege GX Extended Services installer provided by ICT.
2. Set up the prerequisite software outlined in the Protege GX Installation Manual.
3. Install the latest Protege GX server software (version 4.3.398.2 or higher). Complete all initial setup described in the Protege GX Installation Manual, including licensing and creating a controller.
4. Bring at least one controller online with Protege GX, following the steps in the Protege GX Setup Guide.
5. Optionally, set up an email server (see below).

Existing Protege GX Systems

1. Download the Protege GX Extended Services installer and Protege GX server version provided by ICT.
2. The latest server software version includes cybersecurity changes that may affect your system. You may need to take several additional actions when you upgrade to this version:
   - You must upgrade all software components at the same time.
   - Unencrypted client and SOAP connections are no longer permitted. If your Protege GX installation previously used unencrypted communications you may need to complete additional security configuration.
   - All operators will need to reset their passwords the first time they log in. If you have any SOAP integrations, you must reset the passwords of those operators as well.
   - Mobile app users must update their Protege GX places to use HTTPS and their new passwords.

   For more details and instructions, see Application Note 366: Upgrading Protege GX to Version 4.3.402.
3. Upgrade your Protege GX server and clients to the latest version.
4. Ensure that all Protege GX services are running.
5. Ensure that all controllers are online and receiving downloads.
6. Optionally, set up an email server (see below).
7. If the databases are not backed up regularly, back up both Protege GX databases now. See the Protege GX Installation Manual for instructions.

Setting up an Email Server

We recommend that you set up an email server to enable the web app to verify operator email addresses, reset forgotten passwords and send large reports (see page 9).

You can set up the email server in the global settings in the Protege GX client. You will need the network settings and login credentials for the email server.

If Protege GX already has an email server set up for scheduled reports or event notifications, you can keep the existing settings.

To set up an email server:

1. If you are using Gmail as the email server, you must generate an app password. See Sign in with app passwords in the Google help documentation.
2. In Protege GX, navigate to **Global | Global settings | Email settings**.

3. Enter the details of the email server:
   - **SMTP mail server**: The address of the outgoing email server.
   - **SMTP port**: The port used for outgoing mail connections.
   - **Use SSL**: Enable this setting to send emails using the encrypted TLS 1.2 protocol. The **SMTP port** must be set to a port that allows TLS (e.g. 587, 2525).

     When this option is disabled, no encryption will be used.
   - **SMTP login**: The username to log in to the email server. For Gmail accounts this is the email address that you used to generate the app password.
   - **SMTP password**: The password for the email server. For Gmail accounts this is your app password.
   - **SMTP timeout**: Defines how long (in seconds) before the connection to the email server times out.
4. Set the sender details for Protege GX. These will appear in the emails sent by the web app.
   - **Sender email address**: The email address used by Protege GX when sending outgoing mail.
   - **Sender display name**: The display name used when sending outgoing mail.
5. Enter a **Test email address** (e.g. your email address) and click **Test email settings**. You should receive an email from Protege GX.

Installing the Protege GX Extended Services

The Protege GX Extended Services installer includes both the web app and the extended event service, as well as an admin tool.

You must install the extended services on the same computer as the Protege GX Data Service. You will need administrator permissions on this computer.

To install the extended services:

1. If you have previously installed the Protege GX Extended Event Service as an individual service, uninstall it before you run the combined extended services installer.
2. Run the Protege GX Extended Services installer.
3. The default folder location is **C:\Program Files (x86)\Integrated Control Technology\Extended Services**.
   You can change this if the Protege GX server software is installed in a different folder.
   Click **Next** to continue.
4. Click **Install**.
5. The installer will show its progress as it installs the Protege GX extended services. When installation is complete, click **Finish**.

Protege GX Admin Tool

The Protege GX Admin Tool is installed alongside the extended services. It provides a number of useful functions for maintaining and monitoring your system, including:

- Stopping and starting services
- Backing up and restoring the Protege GX Extended Service databases
- Viewing logs

To run the admin tool, navigate to **C:\Program Files (x86)\Integrated Control Technology\Extended Services**. Right click on **ProtegeGXAdminTool.exe** and select **Run as Administrator**.

See Troubleshooting and Maintenance for admin tool functions.

Connecting Controllers to the Extended Event Service

To use the extended event service, you must switch the controllers over from the standard event service. The two services use different network ports for communication. To connect the controllers to the new service, you can simply redirect them to send events and statuses to the new service's port.

There are two methods for switching controllers to the new service:

- **Switch all controllers**: Swap the ports used by the two event services so that the extended event service receives events and statuses from all controllers. This method is faster with minimal site downtime.
- **Switch individual controllers**: Change the event port that each controller uses to send events and statuses, then restart the controller. This method is more controlled, but requires more work and downtime.

The existing Protege GX Event Service is still required for some functions. You must continue to run this service even after all controllers have been switched over to the extended event service.

Switching All Controllers

To switch all controllers at once, you can configure the extended event service to use the port currently used by the standard event service (22000 by default). You must also change the standard event service's port to prevent conflicts.

During this process, the Protege GX server will temporarily receive no events or statuses from controllers. Events will be stored on the controllers until the extended event service is available.

First, change the standard event service to a different port:

1. In Protege GX, navigate to **Global | Event server**.
2. Make a note of the **Port** (usually 22000), then change it to a different value. This can be any port that is available on the server (e.g. 22001).
3. Click **Save**.
4. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
5. Right click on the **Protege GX Event Service** and select **Restart**.

Then, change the extended event service's port to the original event port:

1. Open the File Explorer and navigate to the installation directory, by default:
   C:/Program Files (x86)/Integrated Control Technology/Extended Services
2. Open the **Events** directory.
3. Open **appsettings.json**.

   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.
4. In the `"ConnectionStrings"` section, locate `"EventIngestionPort"`.
5. Set the port to the one originally used by the standard event service. For example:
   ```
   "EventIngestionPort": "22000"
   ```

6. Save the file.
7. In the services manager, right click on the **Protege GX Extended Event Service** and click **Restart**. The extended event service will now receive events and statuses from all controllers.
8. Confirm that the controllers have come online with the new event service:
   - In **Sites | Controllers**, make sure that all controllers are Online.
   - Open a status page or floor plan. Make sure that events and statuses are coming through from the controllers.

If you need to revert to using the standard event service, simply swap the ports back.

Switching Individual Controllers

To switch individual controllers to the extended event service, simply redirect the **Event Port** to that of the new service and restart the controller.

The controller will be unable to perform its normal functions while it restarts.

To switch a single controller:

1. In a web browser, navigate to the controller's web interface and log in.
2. Open the **Settings** page.
3. Set the **Event Port** to 32005.
4. Click **Save**.
5. Click **Restart**. This controller will start reporting events and statuses to the Protege GX Extended Event Service.
6. Once the controller has restarted, confirm that the controller has come online with the new event service:
   - In **Sites | Controllers**, make sure that the controller's status is Online.
   - Open a status page or floor plan that displays events from this controller. Trigger an event and make sure it appears on the status page.

If you need to revert to using the standard event service, you can reset the event port of each controller or change the event service ports on the server as described above.

Setting Up the Protege GX Web App

You can now access the Protege GX Web App using the following URLs:

- https://localhost:8083 or https://127.0.0.1:8083 (on the computer where it is installed)
- https://servername.domainname:8083 (on other computers on the domain)

Some additional steps are required to make the web app accessible outside of the server computer—see Web App Accessibility. We recommend that you consult with the site's IT administrator for assistance.

Logging In to the Web App

You can log in to the Protege GX Web App using your **existing username and password** from Protege GX. As the Protege GX web app requires two-factor authentication, you will be required to set up an authenticator app account. You may also need to verify your email address.

If you do not have an authenticator app already, download one such as Microsoft Authenticator or Google Authenticator. If you already use an authenticator app for other work or personal accounts, you can use the same authenticator for your web app account.

Logging In—Video Demonstration

Setting Up Operator Access

Logging In—Instructions

To log in to the web app:

1. Open a web browser and browse to the web app. On the server computer, you can use the URL: https://localhost:8083
2. If you are logging in on a computer that is not the server, you will see a security warning. Your connection is still encrypted, but is not considered secure due to the self-signed certificate. To continue to the web app, click **Advanced**, then **Proceed to localhost** (or similar in your browser).
3. On the login screen, enter your **Username** and **Password**. These are the same credentials that you use to log in to Protege GX.
4. The web app will prompt you to set up your authenticator app. Open your authenticator app and add a new account. Scan the QR code to set up the Protege GX Web App account.
5. By default, the authenticator account is called Protege GX. Installers and technicians will need a different account for each customer site, so we recommend that you add the site address or organization name to the name of the account to differentiate them.
6. Once you've set up the account in your authenticator app, click **Next** in the web browser.
7. Enter the 6-digit code displayed in your authenticator app. Click **Verify**, then **Continue**.
8. If your system has an email server connected (see page 11), you must validate your email address.

- If there is already an email address associated with your Protege GX operator record (**Global | Operators**), the web app will send a verification email to that address.
- If there is no email address associated with the operator, enter your work email address and click **Continue**.

Enter the 6-digit verification code from the email, then click **Continue**.

> The default Admin account cannot set an email address.

9. Review the terms of use and privacy policy, then check **I accept the terms and privacy policy**. Click **Continue**.
10. You will now be logged in to the Protege GX web app. In future, you can log in with your username or email address, password and authenticator app.

Validating the Web App

Before you invite operators to log in to the web app, we recommend that you validate a few operations to make sure that everything is working correctly. This is also useful for familiarizing yourself with the web app if you have not used it before.

To validate that the web app is functioning correctly:

1. If your system has multiple sites, click the **Account** button in the top corner. Confirm that all of the sites are available in the **Site** selector.
2. Navigate to **Users**, **Manage**. Confirm that existing users appear in the web app.
3. Add a new user with credentials and access levels. Confirm that this user appears in the Protege GX client. Enter the user's card or PIN code at a card reader and confirm that they are granted or denied access correctly.
4. Navigate to **Controls**. Select a door and click **Unlock**. Check that the door's status updates correctly.
5. Navigate to **Events**. You should see the recent events from the door being unlocked and locking again.

For more information about using the web app generally, the online help provides a comprehensive resource. Click the **Help** button in the web app to access the documentation.

Changing the HTTPS Port

The default HTTPS port for accessing the Protege GX Web App is **8083**. If this port is not available on your server or you wish to use the standard HTTPS port (443), you can change this port.

1. On the server, open the File Explorer.
2. Navigate to: **C:\Program Files (x86)\Integrated Control Technology\Extended Services\UI**
3. Open **appsettings.json**.

> 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.

4. Update the `"Port"` to the required value. For example:

```
"Port": 443
```

5. Save the file.
6. Run the Protege GX Admin Tool from **C:/Program Files (x86)/Integrated Control Technology/Extended Services/AdminTool.exe**

> You must run the tool as an administrator.

7. Open the **Services** page, **Extended Services** tab.
8. Locate **Protege GX Extended Services Web UI** and click **Restart**.

You can now browse to the web app using the new port, e.g. https://servername.domainname:10025

If you set the port to 443, you do not need to specify the port in the URL, e.g. https://servername.domainname

Installing a Custom HTTPS Certificate

By default, the Protege GX Web App uses a self-signed HTTPS certificate. This certificate is not trusted by web browsers, so operators will see security warnings when they open the web app. In some cases, access to the web app may be blocked entirely. To avoid this, we recommend that you install a custom HTTPS certificate that is trusted on your network.

Certificate Files

Request an HTTPS certificate from the site's IT team—see Web App Accessibility for more information.

You will need two files with the following names:

- cert.pem (containing the public certificate)
- key.pem (containing the private key)

The certificate and key must be provided as separate files. Both files must be unencrypted.

Installing the Custom Certificate

1. On the server, open the File Explorer.
2. Navigate to: **C:\Program Files (x86)\Integrated Control Technology\Extended Services\UI**
3. Copy and paste the cert.pem and key.pem files into the folder.
4. Run the Protege GX Admin Tool from **C:/Program Files (x86)/Integrated Control Technology/Extended Services/AdminTool.exe**

   You must run the tool as an administrator.
5. Open the **Services** page, **Extended Services** tab.
6. Locate **Protege GX Extended Services Web UI** and click **Restart**.
7. To test the certificate, open a web browser on a different computer and browse to the web app's URL. Ensure that there is no security warning when you access the page. The URL bar of the browser should show that the connection is secure.

Preparing the Web App for Operators

This section covers some optional steps that prepare the web app for everyday use. It will also help you learn about the new features available in the web app.

Creating Locations

Standard Protege GX uses **record groups** to partition the system into regions, buildings, client companies and other segments.

In the web app, you can mark specific record groups as **locations**. Locations represent specific physical places where controllers and doors are installed. Operators can use locations for filtering events, doors, areas and other records, allowing them to focus on a specific physical place.

For example, filtering events by location restricts the list to only display events from controllers and other records that are physically in that location.

Rule of thumb: Every record group that is assigned to a controller, door or area should be a location (or the child of a parent location). Record groups that are not associated with physical infrastructure should not be locations.

To set up locations:

1. In the web app, navigate to **Record groups**.
2. Open a record group that represents a physical location.
3. Enable **Make this record group a location**.
4. Enter the **Address**.
5. If you want to view this location frequently, enable **Add to my favorite locations**.
6. Click **Save**.
7. Repeat for other locations.

Navigate to **Events**. Click the **location picker** at the top of the page (under the title **Events**) to select from your favorite locations. This will filter the event list to only include events from that location.

For more information, see Record Groups in the online help.

Setting Up Views

In the web app you can easily filter, sort and change the columns in record lists. After modifying what records and columns are displayed, you can save these rules as a **view**. Operators can open a view to apply those filters, helping them quickly and consistently find the records they need.

Before onboarding operators, we recommend you create and share some views that will be useful in day-to-day operations. For example, you could create:

- **Event views**:
  - Specific event types, such as alarm events or door forced events
  - Events for specific doors or areas

  Three default event views are created by the system: All errors, All alarms and All acknowledged alarms.
- **User views**:
  - Users with specific access levels
  - Users missing credentials, PIN codes or photos
  - Inactive users
  - Users with expiring PIN codes or credentials
  - List displaying the Reporting ID (to share with the offsite monitoring station)
- **Control views**:
  - Disarmed areas
  - Areas or doors in alarm
  - Bypassed inputs

You can create as many shared views as needed. For more information and examples, see Filters and Views in the online help.

Example: View of Users with Expiring PINs

To set up a view containing users with a PIN expiring in the next week:

1. Navigate to **Users**, **Manage**.
2. Click the **Filter** button.
3. Set the **PIN** dropdown to **User with PINs expiring in 7 days**.
4. Click **Save as new view**.
5. Enter a **Name** and **Description** for the view.

   Keep the name short so it does not take up too much space in the view bar.
6. Enable **Shared view**.

7. Only the owner of a view can edit and delete it. You can keep this view on your own account, or assign it to someone else by selecting a different **Owner**.
8. Click **Save**.

Now any other operator can use this view by selecting it from the view bar above the user list.

For more information and examples, see Filters and Views in the online help.

Setting Up Dashboards

Dashboards in the web app are similar to status pages in the client. They can display live events and device statuses, as well as alarms and other issues.

We advise setting up at least one dashboard for operators. Navigate to **Dashboard** and click one of the following buttons:

- **Start with default**: Creates a dashboard that displays all events, areas and doors.
- **Create new**: Creates a new custom dashboard. You can display all issues, events and devices, or select specific tiles and views to display.

You can create additional dashboards with the **Add Dashboard** button. Whenever you create a dashboard for use by other operators, make sure you turn **Shared dashboard** on.

If you have already created shared views, you can use them to filter dashboard tiles. For example, if you have a view that displays disarmed areas, you can create a dashboard for operators to check that every area is armed before they leave site.

For more detailed instructions, see Creating a Dashboard in the online help.

Views and Dashboards—Video Demonstration

Views and Dashboards

Onboarding Operators to the Web App

Before you start onboarding operators to the new user interface, make sure that the IT team has completed the networking steps for the web interface (see page 7). Without these steps, operators may not be able to access the web app from other computers.

There are two ways to invite existing operators to the web app:

- Send the operator an **invitation link** from the web app.
- Send the operator the **URL** for the web app and invite them to log in with their **existing username and password**. This is the same process as you followed in Logging In to the Web App above.

Each operator will need an **authenticator app**, such as Microsoft Authenticator or Google Authenticator. If the operator already uses an authenticator app for other work or personal accounts, they can use the same app for Protege GX.

Inviting an Operator through the Web App

To invite one operator:

1. In the main menu, select **Users**, then **Operators**.
2. Find the operator you want to invite to the web app and click the name to open the record.
3. If the **Email address** field is blank, enter the operator's email address.

   This is typically their business email address, not their personal one.

4. If your system has an email server, click **Send invitation link**. Protege GX will send the operator an invitation email.

   If the system does not have an email server, click **Copy invitation link**. You can then email or message the invitation link to the new operator.

The operators can click the invitation link to log in and set up two-factor authentication. .

Inviting Multiple Operators

If your system has an email server, you can also invite multiple operators at once. All of the operators must already has an **Email address** set. To invite multiple operators:

1. In the main menu, select **Users**, then **Operators**.
2. Use the checkboxes to select the operators who will receive invitations.
3. Click **Actions**, then select **Send invitation**.
4. The popup will indicate how many operators will receive this invitation. Some selected operators may not receive an invitation (e.g. if their account has already been activated).

   Click **Send** to confirm.

First Steps

When the operator has created their account, we recommend that you give them a tour of the web app, focusing on the features they need to use.

There are a few things operators may want to set up as they begin.

Select Favorite Locations

Operators with access to multiple locations can select one or more as favorites. They can easily switch between their favorite locations using the location picker at the top of the page.

To select a favorite location:

1. Navigate to **Record groups**.
2. Click the menu button next to a location.
3. Select **Show in my favorite locations**.

Select Favorite Controls

The operator may have a few key doors, areas or devices that they regularly need to monitor or control, such as the front door of the building. They can add these to their favorite controls for quick access.

To select favorite controls, navigate to each **Controls** page. Click the **Favorite** button next to commonly-used devices. These will now appear on the **Controls**, **Favorites** page.

Create Views and Dashboards

While the integrator or system administrator can set up key views and dashboards that are needed by the whole organization, other operators might have unique needs. You can help them set up new personal views and dashboards, or direct them towards the relevant pages in the online help:

- Filters, Columns and Views
- Creating a Dashboard

Troubleshooting

Installation Logs

You can find logs for the installer in the installation directory. By default this is: **C:\Program Files (x86)\Integrated Control Technology\Extended Services\Logs**

Service Logs

You can view logs for the extended services in the Protege GX Admin Tool:

1. Run the Protege GX Admin Tool as an administrator.
2. Open the **Logs** page.
3. Select the **Service** you want logs for. By default, the **Log File** is set to the most recent file, but you can select an older file to investigate a previous day.

   When you select All Services, you can select logs from any service in the **Log File** dropdown. You can still only display the logs from one service at a time.

The logs are displayed in chronological order, with the newest at the bottom. To share the logs, copy the lines you want to share and paste them into a text file.

You can filter the logs by typing in the **Filter** field. For example:

- Type **ERR** or **WRN** to view only errors or warnings respectively.
- To find events that occurred in a specific hour, type **T**, then the hour in 24-hour format. For example, enter **T14** to see events from the 2pm hour.

The event server diagnostic window (in **Sites | Controllers | General**) only applies to the standard Protege GX Event Service. It does not provide diagnostic information about the extended event service.

Web App

Device statuses are showing as 'Offline' or 'Unknown' in the web app, even though the client shows their current statuses correctly

The web app receives device statuses from the extended event service. If your controllers are still reporting to the existing Protege GX Event Service, the web app cannot display any device statuses.

To display statuses correctly in the web app, connect all controllers to the extended event service (see page 14).

Maintenance

This section contains information about software maintenance.

Backing Up Databases

The Protege GX extended services use Postgres databases, which are independent of the SQL Server databases used for the standard Protege GX server. You must back up and restore these databases separately.

We recommend that you back up all databases regularly.

To back up the extended service databases:

1. Run the Protege GX Admin Tool as an administrator.
2. Open the **Backup** page.
3. Select the databases to include in the backup (all databases are included by default).
4. Set the **Output Folder** where the backup will be saved.
5. Edit the **File Name** if desired.
6. You must enter and confirm an **Encryption Password**. This password is used to encrypt the data, so you will need to enter it when you restore the backup.

   If you lose the encryption password, it will not be possible to restore the backup. Store the password in a secure, accessible location such as a company password manager.
7. Click **Back Up Now**. The backup log will show progress as the tool creates the backup.

You can find the backup file in the **Output Folder** specified above. All selected databases will be included in the same backup file.

Restoring Databases

When you need to recover the system after an incident or move the server to a different computer, you can restore a recent backup.

To restore the extended service databases:

1. Run the Protege GX Admin Tool as an administrator.
2. Open the **Restore** page.
3. Under **Select Backup File**, enter the path to the .dbbak file or click **Browse** and select it.
4. Enter the **Encryption Password** that was set when taking this backup. Click **Unlock**.
5. Check the date and contents of the backup file.
6. Click **Restore**.
7. Read and acknowledge the warning that databases will be overwritten. Click **Restore**.
8. The restore log will show progress as the tool stops the services, restores the backup and starts the services again. Once the restoration is complete, log in to the Protege GX Web App and ensure that the data you expect is available.

Remember that you must restore the ProtegeGX and ProtegeGXEvents databases separately in SQL Server. See the Protege GX Installation Manual for instructions.

Uninstalling the Extended Services

The Protege GX extended services are installed as a separate program from the Protege GX server, so you must uninstall them separately.

To uninstall the extended services:

1. Open **Add or remove programs** on the Protege GX server.
2. Find **Protege GX Extended Services**.
3. Open the options dropdown, then click **Uninstall**.

Upgrading the Extended Services

To upgrade the extended services, simply run the new installer.

Currently the appsettings.json file is overwritten when you upgrade the extended services. If you have changed the HTTPS port, you will need to update this file again after you upgrade (see page 17).

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