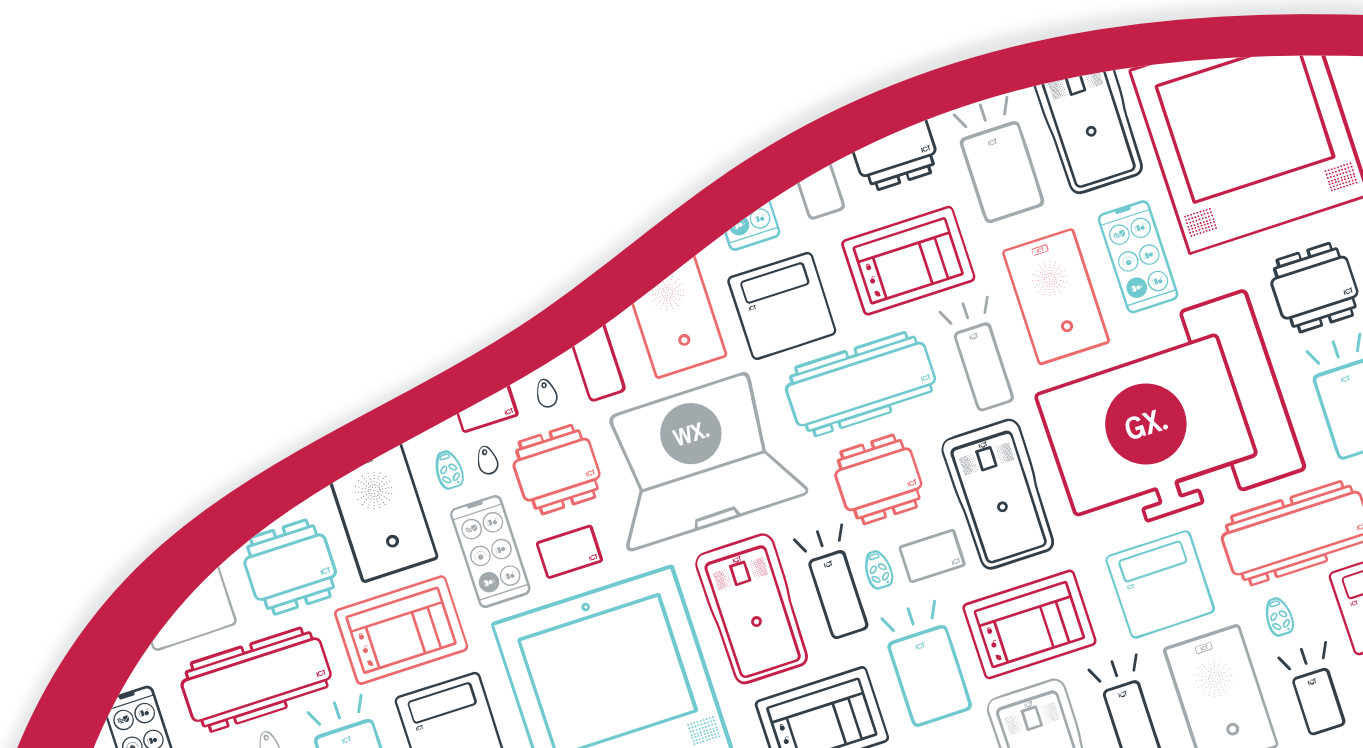
PRT-GX-SRVR

Protege GX

Installation Manual



Last Published: 10-Oct-22 11:15 AM

Contents

About this Manual 5
What This Manual Covers 5
Who Should Read This Manual 5
What You Should Already Know 5
Before You Begin 6
System Requirements 6
Standard Controller Installation 6
Multiple Controller Installation 6
Supported Operating Systems 7
Virtual Server Environments 7
SQL Server Compatible Versions 7
Database Installation on Remote SQL Server 7
Client Workstation Requirements 7
Additional Performance Requirements 8
DVR/NVR Integrations 8
Prerequisites 8
Administrative Permission Requirements 8
Minimum Service Permissions 8
Minimum Service Permissions for PIN Encryption 9
Licensing 9
Licensed Items and Features 9
Optional Features 10
Installation 14
Installation Overview 14
Installing the Prerequisites 14
Installing the Microsoft .NET Framework 14
Installing Microsoft SQL Server 14
Installing the Protege GX Server 15
Installing the Protege GX Client on Remote Workstations 16
Recommended Security Settings 17
Configuring Protege GX to use TLS 1.2 17
Disabling Insecure Cipher Suites and Protocols 20
Enabling Mandatory ASLR 21
Allowing Services Through The Windows Firewall 21
Initial Protege GX Site Configuration 23

Log In to Protege GX 23
Creating a Secure Password 23
Activating Your License 23
Adding a Site 24
Adding a Controller 24
System Backups 26
Backing Up Your Database 26
Scheduled Backups 26
Create a Backup Stored Procedure 26
Create a Backup Script 27
Create a Windows Scheduled Task 27
Offsite Storage 28
Disclaimer and Warranty 29

About this Manual

What This Manual Covers

This manual contains information and instructions on:

- System requirements
- Licensed features
- Installing Protege GX
- Connecting a controller in Protege GX
- Initial site configuration and license activation
- Performing system backups

Who Should Read This Manual

This manual is intended for those that will be installing and configuring Protege GX.

For instructions on using and programming Protege GX, refer to the Protege GX Operator Manual.

What You Should Already Know

This manual assumes that you have an intermediate working knowledge of the Microsoft Windows operating system. Details of basic Windows functionality are beyond the scope of this document.

For support, please contact ICT technical support by email or telephone. Refer to the ICT website (www.ict.co) for additional details.

Before You Begin

This manual provides instructions on installing and configuring Protege GX. It also includes information on system requirements and backup procedures.

Please take a moment to read the material in this section before installation.

System Requirements

The following hardware requirements are based on the size and communication requirements of the installation.

An installation with base Protege GX features can operate on the machine specified. A higher performance machine is recommended when using graphics, photo ID and automation features. Use performance specifications appropriate to your installation.

Standard Controller Installation

A standard Protege GX installation consists of up to 10 system controllers which communicate with up to 16 modules each. Controllers are connected over Ethernet.

Server Hardware Requirements – Standard Installation

- Intel® Dual Core Machine 2.8GHz
- 4 GB RAM
- 40 GB free disk space
- Mouse / Keyboard
- Ethernet 10/100MBs

Multiple Controller Installation

A multiple controller installation consists of over 10 controllers, which may operate as multiple sites running individual controllers, or a single site running multiple controllers. Each controller may have any number of modules connected. The connection to the controllers may utilize any variety of communication mediums and can communicate independently or on demand.

For best performance, connect using an Ethernet 10/100Mbs connection or similar over a local LAN or WAN network.

Server Hardware Requirements – Multiple Controller

- Intel® Quad Core, 2.8GHz or higher
- 8 GB RAM
- 100 GB free disk space
- Mouse / Keyboard
- Dual Ethernet 10/100MBs

Supported Operating Systems

Operating System	Edition	Architecture
Microsoft Windows Server 2022	Standard, Datacenter	64-bit
Microsoft Windows Server 2019	Standard, Datacenter	64-bit
Microsoft Windows Server 2016	Standard, Datacenter	64-bit
Microsoft Windows Server 2012	Standard, Datacenter	64-bit
Microsoft Windows 11	Pro, Business, Enterprise	64-bit
Microsoft Windows 10	Professional, Enterprise	32 / 64-bit
Microsoft Windows 8.1	Professional, Enterprise, Ultimate	64-bit

Virtual Server Environments

The Protege GX server is supported on virtual server environments. However, ICT reserves the right to request customer replication of any errors in a non-virtual environment.

When installing under virtual server environments special care must be taken to ensure that the system requirements (see previous page) are met by the virtualized hardware. The VM must be carefully reviewed with regard to resource and performance before completing any installation.

SQL Server Compatible Versions

The Protege GX application uses a non-proprietary open SQL database engine to store and share information. The software is compatible with SQL 2008, 2012, 2014, 2016, 2017 and 2019 in Standard, Express, and Enterprise editions.

The Express edition is a scaled down, free edition of SQL Server that includes the core database engine and functionality. The Express version of SQL supports up to 10 GB.

For your convenience, the setup files for SQL Server 2014 (SP2) and 2016 (SP2) are included as part of the full distribution package.

Database Installation on Remote SQL Server

The Protege GX platform supports remote SQL Server installations. Careful consideration must be given to the bandwidth requirements, which are vital to the correct operation of the system.

When Protege GX has been installed on a remote SQL Server environment, ICT Technical Support reserves the right to request customer replication of any errors in a local SQL Server environment.

Client Workstation Requirements

Recommended Hardware Requirements - Standard Client

- Intel® Dual Core Machine 3GHz
- 4 GB RAM
- 40 GB free disk space
- DirectX 10 Compatible Video Card
- Mouse / Keyboard
- Ethernet 10/100/1000MBs

Additional Performance Requirements

When communicating with remote sites, additional hardware may be required such as modems, fiber modems or routers. These are beyond the scope of this document.

Server and client machine requirements may differ depending on the intended usage. When performing graphics, photo ID and automation functions from the client workstation, a higher performance machine may be required to ensure that floor plans and photo identification tasks can operate correctly. When the server machine is not used for local login with the Protege GX user interface, a lower performance video card configuration may be selected.

The Protege GX user interface supports the following standard screen resolutions:

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

Selecting alternative screen resolutions may produce unexpected display results.

DVR/NVR Integrations

When integrating with a DVR/NVR system it will have its own minimum system requirements. It is important that you check with the manufacturer prior to installation to ensure that your machine meets these specifications.

Prerequisites

The following third-party components must be installed prior to installing Protege GX:

- The latest version of Microsoft .NET Framework 4.

  At the time of writing, the latest available version is Microsoft .NET Framework 4.8.1

- Microsoft SQL Server (required on server machine only): The software is compatible with SQL 2008, 2012, 2014, 2016, 2017 and 2019 in Standard, Express, and Enterprise editions.

  Note that Microsoft SQL Server has its own set of prerequisites, which are specific to the version of Microsoft SQL Server being installed. Please refer to the Microsoft website for the prerequisites, associated files and installation instructions for your particular version.

Administrative Permission Requirements

To successfully complete installation, you must have local administrative privileges on the workstation(s) you are performing the installation on. You do not need to have domain administrative permissions.

Administrator permissions are not required to open (run) a client that connects to the Protege GX server. You can run the client application as a limited user on any workstation.

Minimum Service Permissions

On some sites it is not preferable to grant full administrative permissions to the Protege GX services.

The Protege GX services may use a service account with the following minimum permissions granted for both the main Protege GX database and the events database:

- CONNECT
- EXEC
- db_datareader
- db_datawriter

Minimum Service Permissions for PIN Encryption

The Protege GX user PIN encryption option (available with version 4.3.291.6 or higher) uses the SQL Server Always Encrypted feature. Additional permissions beyond the minimums stated above are required to configure and use this feature.

For more information, see Application Note 306: Configuring User PIN Encryption in Protege GX.

- To **set up** user PIN encryption, the following permissions are required:
  - VIEW ANY COLUMN MASTER KEY DEFINITION
  - VIEW ANY COLUMN ENCRYPTION KEY DEFINITION
  - ALTER ANY COLUMN MASTER KEY
  - ALTER ANY COLUMN ENCRYPTION KEY
  - Read and write access to the Local machine > Personal certificate store
  - Read and write access to the Local machine > Trusted Root Certification Authorities certificate store
- To **use** user PIN encryption, the following permissions are required:
  - VIEW ANY COLUMN MASTER KEY DEFINITION
  - VIEW ANY COLUMN ENCRYPTION KEY DEFINITION
  - Read access to the Local machine > Personal certificate store

The permissions that are not required to use PIN encryption may be disabled after initial configuration.

Licensing

Protege GX uses a modular licensing model which is both flexible and scalable. This enables you to purchase only the features you need, yet easily extend your system by adding additional features as you need them.

During installation you will be prompted to enter your software serial number (SSN). All Protege GX software products also require registration. This is achieved by connecting to the web registration service from the server or obtaining and loading a license file (see page 23). If additional features are purchased at a later date, simply repeat the licensing process.

Licensed Items and Features

Protege GX offers two distinct license packs and a flexible licensing model that reduces barriers to entry and scales as sites expand.

The **Protege GX Starter License** is designed to make implementation more cost-effective. This option is ideal for smaller organizations who want to adopt an enterprise-level solution while maintaining the flexibility to expand their Protege GX system as their site grows. The starter license comes with 10 doors and is limited to 100 doors. To license more than 100 doors, you must upgrade to a Standard License.

The **Protege GX Standard License** is ideal for large organizations with greater system requirements. The standard license includes 50 doors, 1 camera and 1 concurrent operator connection, and also adds the calendar actions and email on event features.

Both license packs include powerful reporting capabilities, customizable status pages, graphical floor plans, and no restrictions on the number of users, events, schedules, areas, or hardware modules. The following table indicates the features and scope included in each license. For information on how to expand the functionality and size of your system, refer to the Optional Features section below.

Functionality	Starter License	Standard License
Concurrent Client Connections	1	1
Doors *	10	50
Sites	1	Unlimited

Functionality	Starter License	Standard License
Controllers	Unlimited	Unlimited
Users	Unlimited	Unlimited
Cameras	0	1
DVRs	N/A	Unlimited
Calendar Actions Feature	Not Enabled	Enabled
Email on Event Feature	Not Enabled	Enabled
SOAP Web Service Feature	Enabled	Enabled
Web Client Feature	Not Enabled	Enabled
Web Operators	0	3

* wireless locks are considered doors and are included in the doors total.

Additional client, door and camera licenses can be purchased to extend the original configuration. These are only required when exceeding the quantity included in the site's current license.

A starter license will support up to 100 doors (wired or wireless), the features listed as 'Enabled' in the comparison table, and all integrations not marked with * in the Optional Features section. For additional expansion, including camera integration, an upgrade to a standard license is required.

Top Out Limits

Doors have a 'top out' limit of 1000, and once this limit has been reached the number of doors allowed becomes unlimited. This means that the maximum number of additional door licenses ever required (in addition to a standard license) would be 950.

Cameras have a 'top out' limit of 500, and once this limit has been reached the number of cameras allowed becomes unlimited. This means the maximum number of additional camera licenses ever required (in addition to a standard license) would be 499.

Optional Features

Optional features and a flexible licensing model mean that you can add functionality as your needs change. Flexible license packs are available for doors, cameras, and many other features and integration packages, enabling you to easily extend your system as your business grows.

Product Code	Description
Protege GX Software Extensions	
PRT-GX-CLNT	**Protege GX Client License**: Provides an additional concurrent operator (thick client) connection.
PRT-GX-WEB-OPR	**Protege GX Operator License**: Provides an additional web operator connection.
PRT-GX-DB-SYNC	**ICT Data Sync Service License**: Enables synchronization of user data from third party systems used for visitor management, HR management, gyms and fitness centers, freight/delivery, and education.
PRT-GX-AD-OPR	**Protege GX Active Directory Operator Integration License**: Enables operators to log in to Protege GX automatically using their Windows credentials, providing centralized authentication and the convenience of single sign-on.

Product Code	Description
PRT-GX-AD-USR	**Protege GX Active Directory User Integration License**: Enables organizations to automatically create and maintain Protege GX users based on a defined Windows Active Directory security group.
PRT-GX-DOR-10	**Protege GX 10 Door License**: Increases the number of licensed doors on the Protege GX server by an additional 10 doors.
PRT-GX-DOR-50	**Protege GX 50 Door License**: Increases the number of licensed doors on the Protege GX server by an additional 50 doors.
PRT-GX-VOIP-10	**Protege GX 10 SIP Station License**: Licensing for 10 Protege GX VoIP intercom stations per PRT-GX-SRVR instance. Each licensed VoIP station is able to make calls to Protege GX client workstations, and operate as master intercom through the workstation user interface.
PRT-GX-VIM	**Protege GX Visitor Integration Module License**: Enables organizations to register and track visitors directly from the Protege GX interface, eliminating the need for a separate visitor management system.
PRT-GX-MUST	**Protege GX Muster Report License**: Allows organizations to create muster reports to quickly identify who is in a defined area by listing all users that have entered and/or exited via the readers associated with a door.
PRT-GX-TNA	**Protege GX Time and Attendance License**: Allows organizations to create time and attendance reports that utilize the access data from Protege GX to provide information on the in-and-out movements of staff, assisting with payroll and HR management.
PRT-GX-PHOTO	**Protege GX Photo ID License**: Allows operators to create and tailor custom photo ID templates and define the layout and information included on a user's card or label.
PRT-GX-SOAP-SDK	**Protege GX SOAP Web Service Software Development Kit**: Provides a simple way to access Protege GX via a web platform. Build your own application with a customized interface, or integrate with a physical device to unlock doors and disarm areas. Compatible across multiple platforms/operating systems. Use of the SOAP SDK requires signing a non-disclosure agreement.

Features marked with an asterisk * are not supported by the starter license. An upgrade to a standard license is required to implement these optional features.

Product Code	Description
Protege GX Integration Licenses	
* PRT-GX-CAM-10	**Protege GX 10 Camera License**: Additional 10 cameras, standalone or for use with supported DVR/NVR systems.
* PRT-GX-CAM-50	**Protege GX 50 Camera License**: Additional 50 cameras, standalone or for use with supported DVR/NVR systems.

Product Code	Description
PRT-GX-TPR-IF	**Protege GX Third-Party Reader Interface License**: Enables integration of third-party card readers and other identification devices over ethernet or the generic reader interface. A license is required for each smart reader configured.
-	**ICT RS-485 Smart Reader License**: Enables integration of third-party card readers over the RS-485 reader interface. A license is required for each smart reader configured.
PRT-GX-BIO-SP	**Protege GX Suprema Biometric Integration License**: Allows the use of Suprema BioEntry devices for access control directly within Protege GX. One license is required for each Suprema reader that is connected to the system.
PRT-GX-BIO-PR	**Protege GX Princeton Identity Biometric Integration License**: Allows integration with the Princeton Identity system for user identification and integrated access control. One license is required for each Princeton Identity reader that is connected to the system.
PRT-GX-DOR-ALEG	**Protege GX Allegion IP Wireless Door License**: Enables the connection of a supported Allegion wireless door to a system controller. A license is required for each connected wireless door. Requires a compatible RS-485 Allegion Hub.
PRT-GX-DOR-AP	**Protege GX Aperio Wireless Door License**: Enables the connection of a supported Aperio wireless door to a system controller. A license is required for each connected wireless door. Requires a compatible RS-485 Aperio Hub
PRT-GX-DSR-DOR	**Protege GX ASSA ABLOY DSR Door License**: Enables the connection of a supported ASSA ABLOY DSR system door to a system controller. A license is required for each connected IP-enabled door lock.
* PRT-GX-DOR-IP	**Protege GX Salto SHIP Door License**: Enables the connection of a supported Salto SHIP wireless door to a system controller. A license is required for each connected wireless door. Requires a compatible RS-485 Salto IP Hub.
* PRT-GX-DOR-SL	**Protege GX Salto SALLIS Door License**: Enables the connection of a supported Salto SALLIS wireless door to a system controller. A license is required for each connected wireless door. Requires a compatible RS-485 Salto Sallis Hub.
PRT-GX-INOV	**Protege GX Inovonics IP Gateway License**: Enables integration with Inovonics wireless detection devices.
PRT-GX-VING-HLI	**Protege GX ASSA ABLOY VingCard Integration License**: Enables integration with the VingCard VisiOnline system.
* PRT-GX-ELV-HLI-KN	**Protege GX KONE Elevator High Level Interface License**: Enables integration with new or existing HLI KONE elevator systems. One license is required per KONE destination server to be integrated with Protege GX.
* PRT-GX-ELV-HLI-MCE	**Protege GX MCE Elevator High Level Interface License**: Enables integration with new or existing HLI MCE elevator systems. One license is required per MCE destination server to be integrated with Protege GX.

Product Code	Description
* PRT-GX-ELV-MLI-OT	**Protege GX Otis Elevator Medium Level Interface License**: Enables integration with new or existing MLI Otis elevator systems. One license is required per Otis destination server to be integrated with Protege GX.
* PRT-GX-ELV-HLI-OT	**Protege GX Otis Elevator High Level Interface License**: Enables integration with new or existing HLI Otis elevator systems. One license is required per Otis destination server to be integrated with Protege GX.
* PRT-GX-ELV-EMS-OT	**Protege GX Otis Elevator Management System License**: Enables integration with new or existing EMS Otis elevator systems. One license is required per Otis destination server to be integrated with Protege GX.
* PRT-GX-ELV-HLI-SC	**Protege GX Schindler Elevator High Level Interface License**: Enables integration with new or existing HLI Schindler PORT Technology elevator systems. One license is required per Schindler PORT destination server to be integrated with Protege GX.
* PRT-GX-ELV-HLI-TK	**Protege GX ThyssenKrupp Elevator High Level Interface License**: Enables integration with new or existing HLI ThyssenKrupp elevator systems. One license is required per ThyssenKrupp destination server to be integrated with Protege GX.
PRT-GX-KWI	**Protege GX KeyWatcher TOUCH High Level Interface License**: Enables KeyWatcher TOUCH server integration with Protege GX, allowing management of users, operators, schedules and access levels in KeyWatcher cabinets from Protege GX.
PRT-GX-KSI	**Protege GX CIC Technology KeySecure High Level Interface License**: Enables KeySecure server integration with Protege GX, allowing management of users, schedules and access levels in C.Q.R.iT cabinets from Protege GX.
PRT-GX-RED	**Protege GX REDWALL IP Detector License**: Enables integration with Optex Redwall laser scan detectors.
PRT-GX-BAC-CORE	**Protege GX BACnet Core Service License**: Enables BACnet integration with Protege GX, allowing monitoring and control of industry-standard building automation devices. The core service license covers the basic integration and the first 32 connected objects.
PRT-GX-BAC-PL32	**Protege GX BACnet 32 Object License**: Each license allows connection of an additional 32 BACnet objects beyond those provided by the core license.

Installation

The following section outlines the steps required to install Protege GX so you can get up and running quickly.

1. Install the prerequisites (see below)
2. Install the Protege GX server (see next page)
3. Install the Protege GX client on any remote workstations (see page 16)
4. Configure TLS 1.2 (see page 17)
5. Connect the Protege GX controller (see page 24)
6. Perform the initial site configuration (see page 23)

You must have local administrative privileges on the server and workstation(s) you are performing the installation on.

Installation Overview

Protege GX uses a client/server architecture. Every installation includes a server which holds the main system database and the Protege GX services. In most cases it will also have the client software installed. The client application can then be installed on additional workstations, enabling multiple operators to access the system. These workstations connect to the database and services on the Protege GX server.

Installing the Prerequisites

Before Protege GX can be installed the prerequisite software must be installed.

- Microsoft .NET Framework
- Microsoft SQL Server

Installing the Microsoft .NET Framework

Each workstation running Protege GX client software requires the latest version of Microsoft .NET Framework 4.

At the time of writing, the latest available version is Microsoft .NET Framework 4.8.1

To Install the Microsoft .NET Framework

1. Download the latest .NET Framework 4 installer from the Microsoft website.
2. Run the .NET Framework installer file. This launches the Microsoft .NET Framework Setup.
3. Read and accept the License Agreement, then click **Install**.
4. Follow the onscreen instructions to complete installation.

It is recommended that the machine is rebooted once the .NET installation has completed. Although a reboot is not essential, additional components may be necessary to complete the installation, such as the Windows Image Control installation.

Installing Microsoft SQL Server

There are several editions of SQL Server (users can use either SQL Server or SQL Server Express), ranging from a database only installation to database, advanced services, and manageability tools installation.

Advanced settings within SQL Server or customizing the SQL installation to a particular environment are beyond the scope of this document. If you have specific enquiries, please contact your system administrator or the ICT support team.

The following instructions are for the Protege GX SQL installer (packaged as the supplied **SQLSetup.exe**). This contains SQL 2014 SP2 for 32 Bit operating systems, and SQL 2016 SP2 for 64 bit systems.

During the installation you will be presented with several choices that allow you to customize how SQL Server is installed. Default values will already be selected for all choices presented, and you should simply select **Next** to continue installation. It is strongly recommended that you do not change the default configuration details or SQL instance as these are required for Protege GX to run correctly.

To Install Microsoft SQL Server:

1. Run the supplied **SQLSetup.exe** file. This launches the Protege GX SQL Server Installation wizard.
2. Select **Install SQL Server**. The contents are extracted to a temporary location.
3. During setup, checks are performed to ensure that you have the necessary prerequisites required to successfully install SQL Server. If you are missing required components, you will be prompted to install these before continuing.

   Click **OK** to return to the Protege GX SQL Server installation wizard and install the required prerequisites, then repeat Step 2.
4. Accept the license terms and click **Next**.
5. Depending on your version, an **Install Rules** check will ensure there are no potential problems during the setup. Correct any failed prerequisites if necessary, then click **Next** to continue. Warnings can be ignored.
6. Ensure the following **Features** are selected, then click **Next**:
   - Database Engine Services
   - SQL Server Replication
7. Ensure the **Named instance** and **Instance ID** are set to PROTEGEGX, then click **Next** to continue.
8. The Server Configuration details are shown. Click **Next** to continue.
9. The Database Engine Configuration details are shown. Click **Next** to continue.
10. If required, enable the error reporting option to automatically send error reports to Microsoft. Click **Next** to continue.
11. The installation will progress until SQL Server setup is complete. Click **Close** to exit the setup wizard.
12. Click **Close** again to exit the Protege GX SQL Server setup wizard.

Installing the Protege GX Server

Before installing Protege GX, the database engine (Microsoft SQL Server) must be installed separately.

You do not need to install SQL Server on client workstations (computers that will connect remotely to the Protege GX server). To complete client installations, refer to the Protege GX Client Installation section (see next page).

Installing the Protege GX Server Components:

1. Run the supplied **setup.exe** file. This launches the Protege GX install wizard. Click **Next** to continue.
2. Read and accept the license agreement, then click **Next**.
3. Enter your registration information, including your name, company, and product serial number. Click **Next** to continue.
4. Click **Next** to install to the default folder, or click **Change** to choose another location.
5. Choose the **Setup Type**, then click **Next**.

- **Complete**: To install all program features
- **Custom**: To choose the program features and where they will be installed. Use this option if you don't want to install the client interface on the server. Click the icon next to a feature to disable it. Click **Next** to continue.

6. Click **Next** to start the services automatically before the installation completes. By default, services are installed using the local account. If performing a remote installation, you will need to customize the logon and passwords, so you should disable this option and configure the services manually after installation.
7. Enter the details of the database server where the Protege GX database will be created. If you selected the defaults when installing SQL Server, this will be the server name and Protege GX (where Protege GX is the SQL instance). Click **Next** to continue.
8. To customize the database names and/or paths, clear the setting to **Hide advanced database configuration options** and enter the relevant details. It is recommended that these settings only be modified by advanced users. Click **Next** to continue.
9. Click **Next** to use the default WCF TCP/IP port, or specify the ports used by entering the new details.

   This option should be changed where another application on the target machine uses the default port, as this will prevent the services from starting.

   - To enable logging in with Windows Authentication using Active Directory, the **Enable Windows Authentication on Data Service / Client Communications** option must be selected.
   - If it is not selected during installation, to enable this feature in the future Protege GX will need to be uninstalled, then reinstalled with this option selected.

10. Click **Install** to begin installation.
11. Click **Finish** to complete the installation and exit the install wizard.

Installing the Protege GX Client on Remote Workstations

The Protege GX client is automatically installed as part of the server installation and does not need to be installed if the server components have already been installed on the machine. The following steps need to be performed on additional operator workstations.

Installing the Protege GX Client Application:

1. Run the supplied **setup.exe** file. This launches the Protege GX install wizard. Click **Next** to continue.
2. Read and accept the license agreement, then click **Next**.
3. Enter your registration information, including your name, company, and product serial number. Click **Next** to continue.
4. Click **Next** to install to the default folder, or click **Change** to choose another location.
5. Choose the **Custom** setup type and click **Next**. This enables you to select the program features that will be installed.
6. Click the **Server** option and select **This feature will not be available**. The server component is removed from the list of features to be installed.
7. Click **Next** to enable or disable Windows Authentication for the Protege GX server/client communications and configure the WCF TCP/IP ports. You can use the default WCF TCP/IP port, or customize the port used by clearing the setting to use the default option and entering the new TCP/IP Port.

   This option should be changed where another application on the target machine uses the default port, as this will prevent the services from starting.

8. Click **Install** to begin installation.
9. Click **Finish** to complete the installation and exit the Install Wizard.

Recommended Security Settings

It is strongly recommended that Protege GX server installations use best-practice security settings to reduce the risk that the server is exposed to attack. This includes:

- Configuring Protege GX to use TLS 1.2 (see below).
- Disabling insecure cipher suites and protocols (see page 20).

Configuring Protege GX to use TLS 1.2

TLS (Transport Layer Security) is a set of security protocols which are implemented to protect communications and transferred data. However, several known vulnerabilities have been reported against earlier versions of TLS. We recommend that you upgrade to TLS 1.2 for secure communication.

TLS 1.2 Setup

TLS 1.2 is the default security option in the Protege GX installation process, and required items are automatically set up in the background unless a different option is selected. If TLS 1.2 is not currently enabled in your installation, you can enable it by reinstalling the application and ensuring that TLS 1.2 is selected.

To check whether TLS 1.2 was enabled during installation, navigate to the installation directory (C:\Program Files (x86)\Integrated Control Technology\Protege GX) and open GXSV.exe.config in a text editor. If the file contains the text `sslProtocols="Tls12"`, then TLS 1.2 was enabled.

As part of the Protege GX install process a number of items are installed or configured. These include:

- Installing Microsoft .NET Framework 4.6.2.
- Installing OLE DB Driver 18.
- Creating a self-signed certificate on the local PC.
- Adding configuration entries into the Windows Registry.
- Adding required configuration entries into the Protege GX config files.

In addition to the above the following manual steps are required to fully enable TLS 1.2 for Protege GX.

Different configuration is required to use TLS 1.2 with Windows Authentication. For instructions see Application Note 277: Configuring Protege GX to use TLS 1.2.

Enabling Force Encryption and TCP/IP

1. Open SQL Server Configuration Manager:
   - Press **Windows + R** to open the run dialogue.
   - Type sqlservermanager<version>.msc, replacing <version> with the version number of the application corresponding to your SQL Server installation (see this page).
   - Click **OK**.
2. Open the **SQL Server Network Configuration** section from the left-hand pane.
3. Right click on **Protocols for ProtegeGX** (or the SQL instance name that holds the Protege GX database), and select **Properties**.
4. In the Properties window set **Force Encryption** to Yes and click **OK**.
5. Open **Protocols for Protege GX**.
6. Double click **TCP/IP** and set **Enabled** to Yes. Click **OK** to close the window.
7. Open **SQL Server Services** from the left-hand pane.
8. Right click on **SQL Server (ProtegeGX)** in the right-hand pane and select **Restart** to restart the Protege GX SQL Server Service.
9. When complete, close the SQL Server Configuration Manager.

Enabling the IIS Management Console

1. Enable the IIS Management Console by navigating to: **Control Panel > Programs and Feature > Turn Windows Features On or Off**.
2. In the feature list, navigate to **Internet Information Services > Web Management Tools > IIS Management Console**. Check the box to enable this feature.
3. Click **OK**.
4. Restart all Protege GX services.

Using a Custom Certificate

In some systems, it is preferred to use a custom TLS/SSL certificate instead of the self-signed certificate generated by Protege GX during installation. Some additional configuration is needed to install the custom certificate.

This is required when there are Protege GX clients connecting to the server from outside the router/firewall and port forwarding is in place. The custom certificate must refer to the external hostname of the Protege GX server.

The exact process may vary depending on your operating system. Consult your IT provider for more detailed instructions.

Obtaining the Server Certificate

An SSL certificate in the form of a .pfx file must be obtained from your IT provider. This can be self-signed or provided by a trusted certificate authority. You will also require the password used to generate the file, in order to install the certificate.

Installing the Server Certificate

1. Copy the .pfx file to the Protege GX server you are installing the certificate on.
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. The person who generated the certificate should know this.
6. Set the place where you wish to store the certificate as the **Personal folder**.
7. Complete the import.

Configure Protege GX to use the Certificate

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

1. Open **Microsoft Management Console** by pressing **[WIN + r]**, typing mmc and pressing enter.
2. Once the console is open, open **Add or Remove Snap-ins** by pressing **[CTRL + m]**, or via the **File** menu.
3. Double click **Certificates**, select **Computer Account** and click **Next**.
4. Select **Local Computer** and click **Finish**.
5. Click **OK** to close the snap-ins window.
6. Navigate to **Certificates (Local Computer) > Personal > Certificates**.
7. You should be able to see your installed certificate here. Double click on it.
8. Find the field named **Thumbprint** and copy the data from it to a safe place.
9. Open **GXSV.exe.config**, located in the installation directory (C:\Program Files (x86)\Integrated Control Technology\Protege GX).

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.

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

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

11. 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" />
```

12. **Save** the config file and **restart** the Protege GX Data Service for the changes to take effect.

Enabling Certificate Validation on the Client

When a custom trusted certificate is in use, it is recommended to enable service certificate validation to harden the connection between the Protege GX server and client. This protects against man-in-the-middle attacks during the initial connection.

This is only available when a third-party certificate provided by a trusted authority is used, or a self-signed certificate that has been installed as a trusted certificate on client workstations. If the same client workstation is used to connect to multiple Protege GX servers, this setting requires all servers with TLS enabled to use a trusted certificate.

To enable service certificate validation, complete the following configuration on all client workstations:

1. Open **GXPI.exe.config**, located in the installation directory (C:\Program Files (x86)\Integrated Control Technology\Protege GX).

   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.

2. Directly after the **<configSections>** node, add the **<appSettings>** node as shown below:

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

3. Save the config file.

The customized config file may be overwritten when the software is upgraded. You may be required to add the **<appSettings>** node to each client again after the upgrade.

Configuring the Protege GX SOAP Service

This section describes the additional configuration required to deploy the Protege GX SOAP Service for TLS 1.2.

1. When installing the Protege GX SOAP Service, ensure that you install with **TLS enabled**.
   On the **Customize WCF TCP/IP Port** page, point the SOAP service to the Protege GX server:
   - **Protege GX Data Server installed PC name**: the DNS name or hostname of the Protege GX server
   - **Data Server Port**: 8000 (or as configured)
   - **Report Server Port**: 8010 (or as configured)

   For instructions on installing the SOAP Service, see the Protege GX SOAP Service Installation Manual.
2. Locate and edit the following file: **C:\inetpub\wwwrootProtegeGXSOAPService\Web.config**.
   - Under `/configuration/system.serviceModel/`, comment out or remove this line: `<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />`.
   - When using TLS security (recommended) on the data service:
     - Under `/configuration/system.serviceModel/client/endpoint@address`, set the endpoint hostname to the DNS name or hostname of the Protege GX server.
     - Under `/configuration/system.serviceModel/client/endpoint/identity/dns@value`, set the endpoint DNS-identity to one of the 'Subject Alternative Names' in the data service's TLS Certificate.
     - The following node should not exist when using a custom certificate. Remove if present: `/configuration/system.serviceModel/behaviors/endpointBehaviors/behavior[@name=md0]/clientCredentials/serviceCertificate/authentication`.

Renewing TLS Certificates

Sometimes it is necessary to renew or update the TLS certificate associated with a Protege GX installation. This can happen when:

- The existing certificate expires.
- The server's IP address or hostname changes so that the existing certificate is no longer valid.

If you are using the default self-signed certificate generated by your Protege GX installation, you must uninstall and reinstall Protege GX to generate a new self-signed certificate.

If you are replacing a custom certificate, you will need to install and configure the new certificate as described above (see page 18). To complete the process, restart the Protege GX Data Service.

Disabling Insecure Cipher Suites and Protocols

We recommend that you follow best practice by disabling old and insecure cipher suites and communication protocols on the Protege GX server and SOAP server. This requires editing the registry settings on the computer where the Protege GX server is installed, as well as the computer hosting the SOAP service if this is installed separately. For more information about the relevant settings, see the Microsoft documentation and contact your IT provider.

Always back up (export) the registry settings before editing the registry.

IIS Crypto by Nartac Software is a useful tool for managing security settings. It allows you to apply security settings to the server without needing to manually edit the registry.

A standard Protege GX installation has been validated with the **PCI 3.2** and **Best Practices** settings from IIS Crypto 3.2. PCI 3.2 provides stricter security and is the recommended setting.

To apply these settings:

1. Download IISCrypto.exe from the link above.
2. Run the program and click **Yes** to allow it to make changes to your computer.
3. Navigate to the **Templates** tab.

4. Select the PCI 3.2 template from the dropdown, then click **Apply**.
5. Restart the computer to implement the new settings.

Protege GX supports a wide range of integrations, which may not all be compatible with best-practice security settings. In addition, older hardware may not support more recent encryption protocols. In some situations, it may be necessary for you to enable less secure cipher suites and communication protocols. It is the responsibility of the installer to ensure that appropriate security settings are applied.

Enabling Mandatory ASLR

Address space layout randomization (ASLR) is a memory-protection process which randomizes the location where system executables are loaded into memory. This helps to guard against buffer-overflow attacks by making it more difficult for an attacker to predict target addresses and exploit memory corruption vulnerabilities.

The Mandatory ASLR option available in Windows Security can be used to ensure that all EXEs and DLLs on the operating system are forcibly randomized at runtime. For more information about Mandatory ASLR see the Microsoft documentation or contact your IT provider.

To maintain legacy compatibility this feature is disabled by default on all Windows operating systems. We recommend that you follow best practice by enabling Mandatory ASLR on your Protege GX server, SOAP server, and for maximum security all Protege GX client workstations.

You will require administrator permissions to enable this feature.

To enable Mandatory ASLR:

1. Open **Windows Security**.
2. Navigate to **App and browser control**.
3. Under the **Exploit protection** section, select **Exploit protection settings**.
4. Under **System Settings**, go to the **Force randomization for images (Mandatory ASLR)** option and change the setting to On by default.
5. Restart the computer to implement the new settings.

Allowing Services Through The Windows Firewall

It may be necessary to allow the Protege GX services through the Windows firewall to prevent system communication being blocked.

1. Open the Windows firewall settings at **Control Panel > System and Security > Windows Defender Firewall**.
2. Click the **Allow an app or feature through Windows Defender Firewall** link on the left of the screen.

   Third-party antivirus or firewall software may prevent modification of Windows Firewall rules. If this is the case, refer to the third-party manufacturer for details on allowing programs through the firewall.
3. Select **Allow another app...** to add a program as an exception.
4. Click **Browse...**, then navigate to the Protege GX installation directory.

   The default installation directory is C:\Program Files (x86)\Integrated Control Technology\Protege GX.
5. Select (double click or select and **Open**) the executable that you want to allow, then click **Add**.
   Add the following Protege GX executables, one by one:
   - GXSV.exe
   - GXSV2.exe
   - GXSV3.exe
   - GXPI.exe
   - GXEvtSvr.exe

- GXDVR1.exe
- GXDVR2.exe

This allows the necessary Protege GX services access through the Windows firewall.

The above process will only allow access through your primary network connection. If you have multiple networks connected you will need to manually allow access (tick the checkbox in the network column) for each additional network that the Protege GX executable requires access through.

Initial Protege GX Site Configuration

After installing Protege GX, the software must be configured to communicate with the controller.

For detailed instructions on programming a controller, see the Protege GX Integrated System Controller Configuration Guide, available from the ICT website.

Log In to Protege GX

1. Double-click the Protege GX icon on your desktop, or browse to the program from your Windows Start Menu:
   Start > All Programs > ICT > Protege GX > Protege GX
   The Logon window is displayed.
2. Log in as a user with full access to the system. For new installations, log in using the default administrator operator username of admin with a blank password.
3. If connecting to a Protege server on a different machine, enter the server details or IP address.
4. Click **Logon**.

It is **highly recommended** that you change the admin operator's password to a very secure password after first logon. To do this, click the **Change password** button at the bottom of the home page.

Creating a Secure Password

When creating or changing the admin operator password it is **highly recommended** that you create a very secure password.

As a guideline, a secure password should include these features:

- Minimum 8 characters in length
- Combination of upper and lower case letters
- Combination of numbers and letters
- Inclusion of special characters

Passwords must comply with password policy requirements.

Activating Your License

Before you can begin using Protege GX, you must register and activate your license.

Only operators with access to all sites in the system can activate the license. This procedure must be carried out from the server and not from a remote client workstation. You must also have local administrative privileges on the server in order to activate the license correctly.

1. On the server machine, open the Protege GX client.
2. From the main menu, select **About | License**.
3. Select the **License update** tab.
4. Select the **Automatic** or **Manual** option to download and activate your Protege GX license:
   - If the server machine has internet access, use the **Automatic** option.
   - If the server machine does not have internet access, you must use the **Manual** option.

   The steps of manually generating the license and uploading it to Protege GX must be carried out from the server rather than a remote client workstation, or the profile will not match and the license activation will fail.

To Automatically Activate Your License:

1. Click **Download license**, enter the required information and select **OK**.
2. The Protege application passes your details to the ICT web registration service, then activates your software automatically.
3. Close and restart the Protege GX client to implement the new license.

To Manually Activate Your License:

1. Click **Generate** to create a license request file. When prompted, save the **ICT_LicenceRequest.req** file to a folder on your network or a portable drive.
2. Click the link to **Select your licensing options**. This opens a webpage where you will be prompted to enter your site, installer and serial number (SSN) details.
3. Browse to the saved **ICT_LicenceRequest.req** file and click **Submit**.
4. Your details are then passed to the ICT web registration service. Once registration is complete you will be prompted to download your license (*.lic) file.
5. Click **Browse** to select the license file and activate your Protege GX license.
6. Close and restart the Protege GX client to implement the new license.

Note: Steps 2 to 4 can be performed on any workstation with internet access. Steps 1 and 5 **must be performed on the server**.

Adding a Site

1. When your first log in, you will be prompted to add a site.
2. Enter a name for your **New site** and click **OK**.

Adding a Controller

Once a site has been added, the **Add controller** window will appear.

1. Enter a **Name** for the controller and set the **Count** field to 1 to add a single controller.
   - Select the **Type** of controller you wish to add.
   - Keypad and expander records can then be added from the relevant sections.

     Hardware does not need to be connected before records are created.
   - In the **Options** section, select whether to **Create installer menu group**, **Create floor plan** and assign a **CID report map** type.
   - In the **Doors** section, specify how many door records are to be created. The following options can also be enabled or disabled:
     - **Assign to reader expanders**
     - **Assign door trouble inputs**
     - **Assign reader lock output to door configuration**
     - **Assign reader beeper to door alarm configuration**
   - Once complete, click **Add Now**.
2. Navigate to **Sites | Controllers**. The settings set below should match those in the controller's web interface.
   - **Serial number**: The serial number of the controller.
   - **IP address**: The system controller has a built in TCP/IP ethernet device and must be programmed with a valid TCP/IP Address to allow the software to connect. By default the IP address is set to 192.168.1.2.
   - **Download port**: The TCP/IP port used to send downloads to the controller. By default this is port 21000.

- **Download server**: From the drop-down menu, select the download server to be used by the controller.
- **Control and status request port**: The TCP/IP port used to send control commands to the controller. By default this is port 21001.

3. Click **Save**.

You may need to restart the services to bring the controller online. Select the **Services** option from the **Control Panel** and restart the **Protege GX services**.

System Backups

If you are upgrading an installation it is vital that you perform a system backup before completing the upgrade. Failure to do so may cause permanent loss of data.

The instructions below outline how to back up your databases from SQL Server Management Studio (SSMS). You can also take backups and set up scheduled backups in Protege GX under **Global | Global settings**.

Backing Up Your Database

The following procedure allows you to take a backup of either database in SQL Server Management Studio (SSMS). The instructions may differ slightly depending on the version of SSMS you are using.

1. Open SSMS and connect to the Protege GX server.
2. Expand the **Databases** node. Right click the ProtegeGX or ProtegeGXEvents database and select **Tasks > Back Up...**.
3. If a backup has been created previously, the file will be displayed in the **Destination** field. To use this file click the **Media Options** tab and select whether you will append the current backup to the existing file or overwrite the existing file.

   To back up to a different file click **Remove**. Then click **Add...** to enter the name and location of the new backup file. Click **OK**.

   The backup file must be in the .bak format. It is recommended that you add the database version number to the filename.
4. Click **OK** to perform the backup.

Scheduled Backups

Scheduled backups allow a regular backup to be taken automatically. The following steps outline a basic scheduled backup procedure. The scripts provided can be adapted as required to suit the IT environment and SQL version installed.

Create a Backup Stored Procedure

The following SQL stored procedure can generate a full, differential or transaction log backup, with a dynamic file name based on the backup type and date/time. You can create a stored procedure by running this script as a query in SQL.

This stored procedure should be modified as required for your installation.

```
USE MASTER
GO

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

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

```
SELECT @dateTime = REPLACE(CONVERT(VARCHAR, GETDATE(),111),'/','') +
REPLACE(CONVERT(VARCHAR, GETDATE(),108),':','')

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

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

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

EXECUTE sp_executesql @sqlCommand
END
```

You may need to refresh SSMS with Control + Shift + R before the stored procedure becomes available for use.

Create a Backup Script

Create an SQL script to run the stored procedure. Save the script as dbbackup.sql and store in the C:\Backup folder.

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

The first parameter defines the database name - either ProtegeGX or ProtegeGXEvents. The second parameter defines the type of backup: **F** for full, **D** for differential or **L** for transactional.

You can create multiple scripts to perform the required backups on each database.

Create a Windows Scheduled Task

These steps create a scheduled task to run the SQL script using the sqlcmd utility.

Some versions of SSMS do not include the sqlcmd utility in the installer. If it is not present, you must download the Microsoft Command Line Utilities for SQL Server. Ensure that the version downloaded matches the version of SQL Server in use.

The standard installation location for this utility is C:\Program Files (x86)\Microsoft SQL Server\Client SDK\ODBC\XXX\Tools\Binn, where XXX is a number based on the version number of the utility. However, note that the utility may be installed under an **earlier** version number than expected. You can confirm the actual version of the utility by typing `sqlcmd -?` into a command prompt.

1. Open the Windows Task Scheduler by navigating to **Start > Control Panel > System and Security > Administrative Tools** and selecting **Task Scheduler**.
2. Under the **Actions** pane, select **Create Basic Task...**.
3. Enter a **Name** for the task and an optional **Description**. Click **Next**.
4. Select the frequency and time of day the task should run. Click **Next**.
5. Select **Start a Program**, then click **Next**.
6. Click **Browse...** and browse to the installation location of sqlcmd as noted above.
7. Select sqlcmd.exe and click **OK**.

8. Enter the following command in the **Add arguments (optional)** field: `-S .\instancename -E -i C:\Backup\dbBackup.sql`.

   This command is broken down as follows:

   - `-S` (specifies the server and instance name for SQL Server)
   - `-E` (allows you to make a trusted connection)
   - `-i` (specifies the input command file)

9. Click **Next** to finish creating task.

If you want to test the task, return to the **Task Scheduler**, right-click on the task, and select **Run**.

The **C:\Backup** directory must exist on the server machine, or the procedure will fail.

Offsite Storage

We recommend that backups are performed on a regular basis and you use an offsite storage facility or external provider to ensure that a copy is located in a secure offsite location.

Disclaimer and Warranty

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.

For warranty information, see our Standard Product Warranty.

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