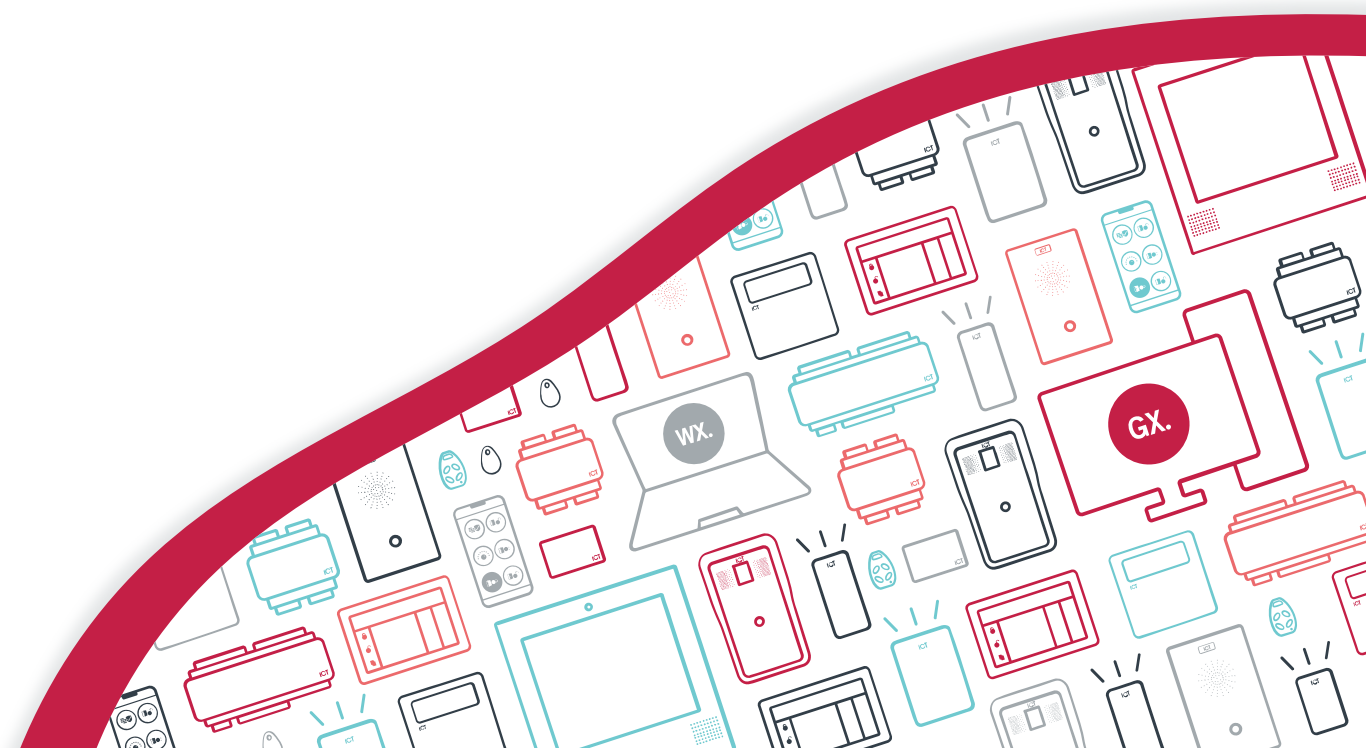
AN-220

KeyWatcher Touch Integration with Protege GX

Application Note



Last Published: 07-Mar-24 11:01 AM

Contents

Introduction

KeyWatcher Touch is an electronic key management system manufactured and distributed by Morse Watchmans Incorporated USA. KeyWatcher Touch cabinets are modular in design, allowing the system to be customized to suit the needs of each site. The user interface comprises a 7" color touchscreen which can be integrated with the extensive programming and reporting functionality available in Protege GX.

Keys available for use within the system are attached to a SmartKey, and each SmartKey contains an identification chip. This allows a Protege GX user to log on to the KeyWatcher Touch cabinet and have SmartKeys electronically released or returned to key slots within the cabinet, or any other cabinet on site.

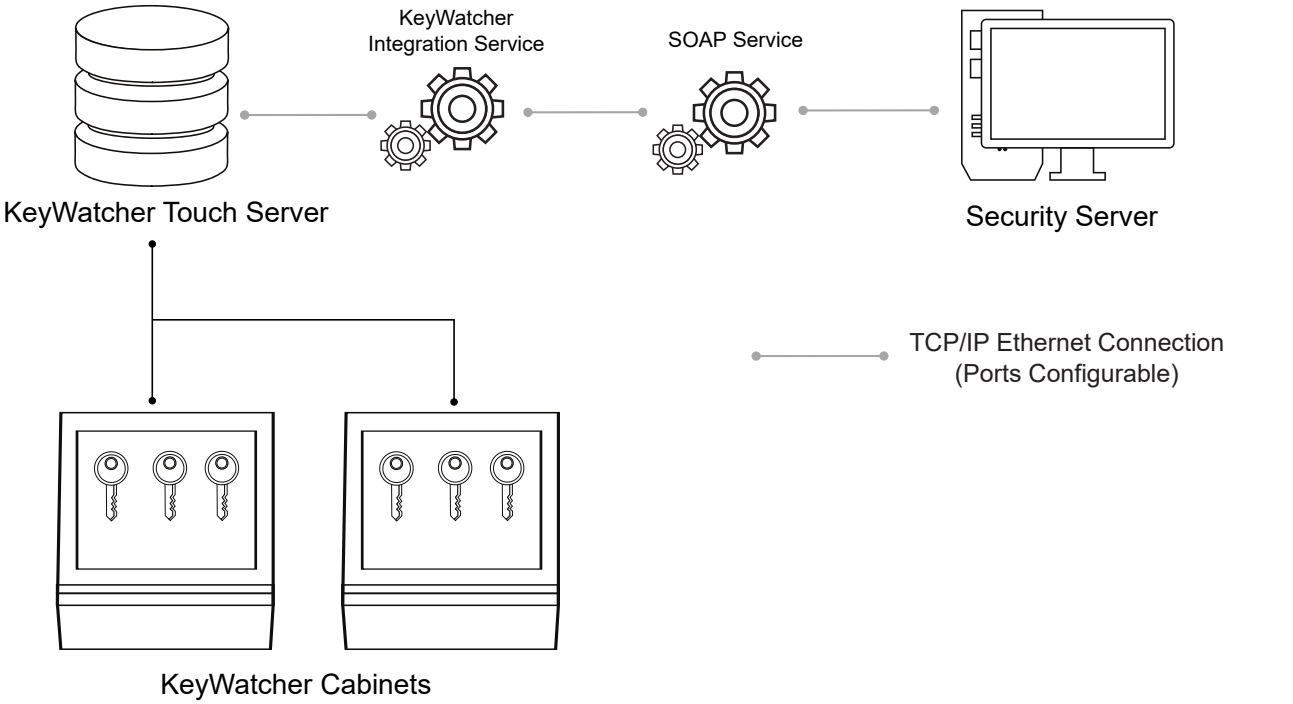
This integration allows KeyWatcher Touch system operation to be synchronized with Protege GX users, access levels and schedules. Integration between systems also allows the extensive reporting functionality available within Protege GX to be used with the events and alarms available with KeyWatcher Touch.

This integration is a licensed feature.

Integration Architecture

In this integration, all keys and key groups are programmed in KeyWatcher, while users and access requirements are programmed in Protege GX. These are synchronized between the two servers by the Protege GX KeyWatcher Integration Service and Protege GX SOAP Service, via a TCP/IP connection.

Access decisions are made by the KeyWatcher system, using the credentials and access level restrictions received from Protege GX.



Prerequisites

Software Requirements

The following software prerequisites must be installed and operational prior to beginning unless otherwise stated.

Software	Version	Notes
Protege GX	4.2.190 or higher	
Protege GX SOAP service	1.6.0.1 or higher	
Protege GX KeyWatcher Integration Service	1.0.0.0 or higher	Instructions for installing this service are included in this application note (see page 8). MSMQ (Microsoft Message Queue) must be activated on the machine the integration service is running on.
KeyWatcher Touch Server	2.0.29	This is the **only** tested and supported version for this integration.
KeyWatcher TrueTouch Client Software	2.0.0.33	This is the **only** tested and supported version for this integration.

Basic setup and programming of the KeyWatcher system is required. This includes installation of the server and client, setup of the site, and creation of the keys and key groups required within the system. For more information, see Programming Requirements in KeyWatcher (below).

IMPORTANT: It is recommended that installers back up both the Protege GX and KeyWatcher Touch databases before enabling the integration service.

It is the responsibility of the installation professional to verify the version of the proposed third-party system and supported components with the version listed in this document. ICT will not accept responsibility for the failure to verify integrated system versions and requirements.

Controller Requirements

Controller	Firmware Version	Notes
PRT-CTRL-DIN	2.08.741 or higher	
PRT-CTRL-DIN-1D		

Licensing Requirements

License	Order Code	Notes
Protege GX KeyWatcher Integration License	PRT-GX-KWI	1 per Protege GX server Adding this license to your SSN also adds the SOAP interface license (PRT-GX-SOAP).

Programming Requirements in KeyWatcher

In this integration, all users, access levels and schedules are managed in Protege GX and synchronized to the KeyWatcher server. Only the keys and groups should be programmed directly in the KeyWatcher system.

In particular, note the following:

- Protege GX can be integrated with a single KeyWatcher site only. It is recommended that you create a new KeyWatcher site for this integration and add the necessary keys and groups.
- The KeyWatcher site must have no users configured except for the default administrator user. The **User ID** of this administrator user must be 0.

  Users in the KeyWatcher server with any other User ID will cause an error to be logged every time a sync occurs, as Protege GX is unable to delete the extra users.

- The **User ID Digit Length** must be set in the KeyWatcher system. The same length value should be entered when the integration is set up in Protege GX (see next page). If this value must be edited, it should be edited in KeyWatcher first, then in Protege GX.
- The integration supports authentication with PIN, proximity card or biometrics at the KeyWatcher cabinet. The required authentication type(s) must be enabled in the KeyWatcher software's **Site Configuration** section:
  - For card authentication, under **Site Configuration** you must set the **Card Type** to Wiegand 128 Bit Compatibility.
  - The **Card Data Type** for each user is set by the integration service. Non-standard data types can be downloaded into the KeyWatcher Touch software and are available directly from Morse Watchmans. For data types other than 26 or 34 bit, a custom format file must also be obtained from ICT (see page 10).
  - Additional configuration of the integration service is required for biometric authentication (see page 10).
- All access levels (permissions) and schedules (time restrictions) must be created in Protege GX.

Configuring KeyWatcher Touch Integration

Enabling the Integration

The following instructions outline how to enable the KeyWatcher integration in Protege GX.

Enabling the KeyWatcher Touch Integration

1. Navigate to **Global | Sites**. Select the site that will use the KeyWatcher Touch integration.

   Take note of the **Database ID**. This will be required when installing the integration service (see next page).

2. In the **Key cabinets** tab, set the **Integration type** to KeyWatcher - Morse Watchmans.

   This tab will not be available until the KeyWatcher Integration license has been applied to the SSN.

3. Check the **Enable integration** option.
4. If desired, check the **Enable logging** option. When this option is enabled, all KeyWatcher integration activity is logged in the log file for the integration service (see page 9). When it is disabled, only errors are logged.

   This option should be disabled when the integration is live and only used for debugging the integration.

5. In the **Third party user ID length** field enter the **User ID Digit Length** value assigned in the KeyWatcher True Touch client software.

   To change the **User ID Digit Length**, the change must be made in the KeyWatcher True Touch Software (**Site Configuration > Site Settings > General Settings**), then manually updated in Protege GX to match. Changes made to this field in Protege GX will **not** be synchronized back to the KeyWatcher Touch software and could cause programming inconsistencies.

6. Click **Save**.

Configuring an Integration Operator

This integration requires the use of an administrator operator, which KeyWatcher will use to access Protege GX.

1. Navigate to **Global | Operators**.
2. Add a new operator and enter the following details:
   - The **Name** of the operator.
   - The **Username** for the operator. This will be used when configuring the integration service.
   - The **Password** for the operator. This will be used when configuring the integration service.
   - For the integration to function correctly the operator must be assigned a **Role** with the Administrator preset.
3. Enable the **Show PIN numbers for users** check box.
4. Protege GX will present you with a warning. Click **OK** to enable the check box. This setting must be enabled in order for the integration to work correctly.
5. Click **Save**.

Configuring the Integration Service

The following instructions outline the installation and service configuration of the KeyWatcher integration service in Protege GX.

Installing the KeyWatcher Integration Service Manager

1. Run the installer file to launch the KeyWatcher integration service install wizard.
2. Click **Next**, then **Next** again to begin the installation process.
3. Click **Next** to install the service to the default location, or click **Change** to select an alternative directory.
4. Configure the settings required to connect to the Protege GX server:
   - **Site ID**: The Database ID for the site in Protege GX. This can be found by navigating to **Global | Sites** in the Protege GX software.
   - **SOAP Address**: The Protege GX SOAP Service endpoint URL where the service can be accessed by a client application.
   - **Operator Username**: The **Username** of the KeyWatcher operator configured in Protege GX (see previous page).
   - **Operator Password**: The **Password** of the KeyWatcher operator configured in Protege GX.
5. Click **Next**.
6. Enter the following details for the KeyWatcher system:
   - **KeyWatcher Server IP Address**: The IP address of the KeyWatcher server.
   - **KeyWatcher Server Port**: The TCP port for the KeyWatcher server. It is best to leave this field at the default setting.
   - **KeyWatcher Version**: The database version of KeyWatcher.
   - **KeyWatcher Site ID**: The ID number for the KeyWatcher site that is being integrated with Protege GX. This field is assigned by the KeyWatcher client software.
7. Click **Next**.
8. Enter the following details:
   - **KeyWatcher Windows Username**: The name of the Windows user account for the KeyWatcher TrueTouch Server assigned during installation of the TrueTouch Server.
   - **KeyWatcher Windows User Password**: The password of the Windows user account for the KeyWatcher TrueTouch Server assigned during installation of the True Touch Server.
   - **KeyWatcher Admin Username**: The user name of the KeyWatcher admin user, which has a User ID of 0 in KeyWatcher (see page 5).
   - **KeyWatcher Admin User Password**: The password of the KeyWatcher admin user.
9. Click **Next**.
10. Enter the following details:
    - **Network Adapter**: The IP address of the computer that the integration service is installed on.
    - **Sync Interval (Mins)**: The length of time between synchronizations of KeyWatcher Touch and Protege GX, in minutes.
11. Click **Next** to begin the installation.
12. Click **Finish**.
13. Once the installation is complete, the **KeyWatcher Integration Service Manager** window will open. Click **Save** and close the window.

Configuring the Integration Service

By default, the Protege GX KeyWatcher Integration Service Manager is installed in the following directory: C:\Program Files (x86)\Integrated Control Technology\KeyWatcher Integration Service. This directory includes the KWIntgManager application.

This service manager allows you to update any of the settings that were configured during installation. You can also start and stop the service using the buttons at the top right. Ensure that the service is Running to enable integration with Protege GX.

IMPORTANT: If any changes are made to the settings within the KeyWatcher Integration Service Manager, the service must be stopped and restarted for correct operation.

Integration Service Log File

The installation directory (C:\Program Files (x86)\Integrated Control Technology\KeyWatcher Integration Service) also includes the log file for the integration service, which logs messages and errors when the service is running. This can be opened with any text editor, and is useful for troubleshooting the integration during initial setup.

To log all available messages, check **Enable logging** in Protege GX (**Global | Sites | KeyWatcher**). When this option is disabled, only errors are logged.

Message logging should be disabled during normal operation.

Granting User Access

Once the integration is enabled and Protege GX has started to synchronize with KeyWatcher, you can assign keys and key groups to user access levels and set credentials for use with the KeyWatcher cabinet.

IMPORTANT: Integrators should not manage users, profiles/permissions or time restrictions from within the KeyWatcher client software. They must be managed in Protege GX and then synchronized with KeyWatcher.

Adding Schedules

You can create schedules for use with KeyWatcher as normal under **Sites | Schedules**, however schedules to be synchronized with KeyWatcher can only be defined in **Period 1**.

There are no holiday settings available in the KeyWatcher software, so select Ignore holiday to ensure that the schedule operates every day.

In addition, schedules cannot be programmed to operate between days (e.g. 22:00 Monday to 02:00 Tuesday).

If both the **Start time** and **End time** are set to 00:00, a 24 hour time restriction will be created in KeyWatcher.

Adding Keys to an Access Level

1. Navigate to **Users | Access Levels**. Select existing access levels or create a new one to be used with KeyWatcher.
2. Click on the **Keys** or **Key groups** tab.

   These tabs will not be available until the KeyWatcher keys have been synchronized with Protege GX.
3. Click **Add** and select the required keys or key groups.
4. Click **OK**.
5. Click **Save**.
6. Assign the required schedule to each key or key group by selecting it from the drop down menu. This action is the equivalent of adding a time restriction to a permission within the KeyWatcher client software.
7. Click **Save**.

Configuring Users

When you have created or modified the access levels, navigate to **Users | Users** and assign them to the users who require KeyWatcher access. Users can have multiple access levels assigned, corresponding to multiple profiles assigned in KeyWatcher.

When an access level containing keys or key groups is assigned to a user, they are automatically assigned a unique **Third party user ID**. This is equivalent to the **User ID** that is used to identify each user in the KeyWatcher system. To view this ID, scroll down to the **Key cabinet integration** section on the **General** tab.

The **Third party user ID** can be edited manually in Protege GX, but must be unique to each user. If the ID has already been assigned to a user, Protege GX will present a warning and offer the next available ID. The **Third party user ID** cannot be zero.

All users who have access to any keys or key groups will be synchronized and copied to the KeyWatcher server.

Setting User Credentials

Protege GX can synchronize user PINs, cards and biometric credentials to KeyWatcher, allowing users to unlock the KeyWatcher cabinet with the same credentials that they use in the Protege GX system.

The KeyWatcher site must be configured to accept the required credentials (see page 5).

User PINs

Protege GX allows the use of PIN numbers up to 6 digits. However, KeyWatcher only accepts 4-digit PINs. The user PIN that is sent to KeyWatcher will be modified as necessary to meet this requirement.

The **Key cabinet PIN** is displayed to the right of the **PIN** field in the Protege GX user programming.

- Any PIN in Protege GX that is longer than 4 digits will be truncated to the first 4 digits only. For example, a PIN of 12345 will be modified for KeyWatcher to 1234.

  Care should be taken to ensure that this does not result in users having duplicate PINs in KeyWatcher.

- Any PIN in Protege GX that is shorter than 4 digits will have leading zeros added. For example, a PIN of 123 will be lengthened to 0123.

Card Credentials

It is possible to have a Wiegand format card reader connected to a KeyWatcher cabinet to allow access to the cabinet without the need to enter a user ID or PIN. The KeyWatcher Touch cabinet must have a card access interface board installed and connected to the KeyWatcher system.

By default, only the first **Facility/Card number** programmed for each user will be synchronized to KeyWatcher. If only a single card is required, it should be programmed into the first card number row.

Card Formats

The default card format is **HID 26 bit**. If your site uses a different format, some configuration is required.

This feature is available with KeyWatcher integration service version 1.0.0.10 or later.

1. If you are using a format that is **not** HID 26 bit or HID 34 bit, contact ICT Technical Support for assistance with creating a custom format file. Store this file on the Protege GX server or somewhere accessible on the network.
2. Open the Protege GX KeyWatcher Integration Service Manager and click **Stop** to stop the service.
3. Navigate to the installation directory:
   C:\Program Files (x86)\Integrated Control Technology\KeyWatcher Integration Service
4. Open the KeyWatcherIntegration.exe.config file with a text editor.

   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.

5. In the `<appSettings>` section, add the following line:

   ```
   <add key="CardFormat" value="X" />
   ```

   Where **X** represents the format that you will use:
   - **0** = HID 26 bit
   - **1** = HID 34 bit
   - **2** = Custom format
6. If you are using a custom format, add another line directly underneath with the path to the custom format file:

   ```
   <add
   key="CardFormatCustomDefinitionFile" value="C:\pathtofile\customformat.icf"
   />
   ```

7. Save the config file.
8. Open the Protege GX KeyWatcher Integration Service Manager and click **Start** to start the service.

Multiple Cards and Biometrics

The integration service requires special configuration to enable it to synchronize multiple cards or biometric credentials with KeyWatcher. This enables it to send one or more cards for each user, including the biometric credential enrolled in the second row.

This feature is available with KeyWatcher integration service version 1.0.0.8 or later.

1. Open the Protege GX KeyWatcher Integration Service Manager and click **Stop** to stop the service.
2. Navigate to the installation directory:
   C:\Program Files (x86)\Integrated Control Technology\KeyWatcher Integration Service
3. Open the KeyWatcherIntegration.exe.config file with a text editor.

   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 **<appSettings>** section, add the following line:

   ```
   <add key="FacilityCodes" value="X,Y" />
   ```

   Where the **value** represents the facility/site codes of the credentials that will be synchronized to KeyWatcher. Any number of facility codes can be entered as a comma-separated list, which may include:
   - The facility code for the biometric credentials. This is typically 100.
   - The facility codes for any card credentials that must be synchronized to KeyWatcher.

   When user records are synchronized to KeyWatcher, the first programmed credential which matches each of these facility codes is sent.
5. Save the config file.
6. Open the Protege GX KeyWatcher Integration Service Manager and click **Start** to start the service.

KeyWatcher Events in Protege GX

There are 30 KeyWatcher events and alarms that are synchronized with Protege GX when triggered in the KeyWatcher system.

These events and alarms can be added to standard Protege GX reporting functions and can be viewed in the **All Events** window of a status page.

Event Types

KeyWatcher event types can be viewed by navigating to **Global | Event types**.

You can sort the list in alphabetical order by clicking on the **Name** heading, or use the **Find** tool to find specific events.

The following table explains the meaning of each KeyWatcher event/alarm.

KeyWatcher Event	Notes
Box AC Power Loss	KeyWatcher Slave box has lost AC power
Box Controller Battery Fail	KeyWatcher Touch box battery fault/failure
Box Controller Battery Low	KeyWatcher Touch box battery low
Box Door Illegal Entry	KeyWatcher Touch box door has been opened by illegal entry
Box Door Latch Release	KeyWatcher Touch box door latch released by KW Admin user
Box Door Left Open	KeyWatcher Touch box door left open by user
Box Location Release	KeyWatcher Touch box location released by KW Admin user
Box Slot Release	KeyWatcher Touch box key slot released by KW Admin user
Key Overdue	Key removed from KeyWatcher Touch box by user is overdue The time limit for an overdue key is assigned in the KeyWatcher Touch software.
Key Remove	Key removed from KeyWatcher Touch box by user
Key Remove Emergency Release	Key removed from KeyWatcher Touch box using emergency release Emergency release is activated by PIN+9
Key Remove Invalid Key	Invalid Key removed from KeyWatcher Touch box by user
Key Return Not Taken	Key removed from KeyWatcher Touch box but not taken
Key Return Inconsistent	Key returned to KeyWatcher Touch box by different user
Key Return Invalid Key	Invalid Key returned to KeyWatcher Touch box by user
Key Return Not Returned	Key returned to KeyWatcher Touch by user, but not returned to box slot
Key Return Overdue	Overdue key returned to KeyWatcher Touch box
KWT AC Power Loss	KeyWatcher Touch box has lost AC power
KWT Restart	KeyWatcher Touch server restarting
KWT Server Not Available	KeyWatcher Touch server not available
Problem Key	SmartKey with problem removed from KeyWatcher Touch box

KeyWatcher Event	Notes
Server KWT Stopped Sending Status	KeyWatcher Touch box stopped sending status to server
Server Network Down	KeyWatcher Touch server network is down
Server Shut Down	KeyWatcher Touch server shutting down
Server Start Up	KeyWatcher Touch server starting up
User Log Off	User has logged off at KeyWatcher Touch box
User Logon	User has logged on at KeyWatcher Touch box
User Logon Duress	User logon at KeyWatcher Touch box under duress Duress is activated by PIN+7

Event Search

The event search function allows you to view what is happening within the KeyWatcher system. It generates a temporary report that can be printed (but not saved).

The following example demonstrates using an event search to view KeyWatcher events that have occurred within a selected time period.

1. Navigate to **Events | Event search**.
2. In the **Time period** section, define the period over which to generate the event report. Either:
   - Select a **Period** from the drop down box and set a **Start date**.

     The **End date** field will automatically be disabled.
   - Define a custom period by defining the **Start date** and **End date**.
3. Disable the **Include all event types** check box.
4. In the **Event types** section, click **Add**.
5. In the **Select event types** window, enter KeyWatcher or KWT into the **Keyword** field to locate KeyWatcher events.
6. Select the KeyWatcher events you wish to view in the report and click **OK**.
7. Click **Find**.

An event report displaying the selected events for the defined time period will be generated.

Troubleshooting

The KeyWatcher service has a retry mechanism to prevent it from timing out due to an idle connection. To set how many retries are permitted, edit the following line in KeyWatcherIntegration.exe.config, under **<appSettings>**:

```
<add key="KWRetryLimit" value="X" />
```

Where **X** is the number of retries made by the service before it times out.

This feature is available with KeyWatcher integration service version 1.0.0.10 or later.

Release History

Note: Before upgrading your installation, ensure that you uninstall any existing versions of the Protege GX KeyWatcher integration service.

Version 1.0.0.0

Initial release of the Protege GX KeyWatcher integration service.

Version 1.0.0.8

- Resolved an issue where the integration could not handle sites with a large number of access levels/users.
- Resolved an issue where every user was being updated on every sync with KeyWatcher.
- Added support for multiple user credentials and biometric credentials. For more information, see Setting User Credentials (page 10).

Version 1.0.0.10

- Added the ability to select a custom card format for use with this integration. For more information, see Setting User Credentials (page 10).
- Resolve an issue where the KeyWatcher service could time out and fail to sync on large sites.
- Resolved an issue where the service was failing to post notifications to KeyWatcher using MSMQ.

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