AN-358

XProtect Access Integration with Protege GX

Application Note

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

Last Published: 08-Jun-26 12:46 PM

Contents

Introduction ____ 5
Milestone XProtect Integration Comparison ... 5
Integration Architecture ... 5
Synchronized Records ... 6
Prerequisites ... 7
Preparation ____ 9
HTTPS Certificates ... 9
Service Accessibility ... 9
Installing on Different Domains ... 10
Configuring Protege GX ____ 11
Enabling the Integration ... 11
Creating the Operator ... 11
Syncing Events ... 11
Installing the Plugin ____ 12
Granting Folder Access ... 12
Configuring the XProtect Management Client ____ 13
Enabling the Access Control Plugin ... 13
Access Control Plugin Settings ... 14
General Settings ... 14
Doors and Associated Cameras ... 14
Access Control Events ... 14
Access Request Notifications ... 14
Cardholders ... 15
Access Control in the XProtect Smart Client ____ 16
Monitoring Events ... 16
Monitoring and Controlling Devices ... 16
Viewing Cardholders ... 17
Adding Doors and Devices to Maps ... 17
Alarms ____ 18
Configuring Alarms ... 18
Viewing and Acknowledging Alarms ... 18
Access Request Notifications ____ 20
Troubleshooting ____ 22
Known Issues ____ 23

Release History 24

Introduction

The Protege GX XProtect Access Integration synchronizes Protege GX records and events with the Milestone XProtect video management system (VMS), unlocking a wide range of functionality within the XProtect Smart Client. It enables you to:

- View the status of doors, controllers, areas and other devices in XProtect.
- Monitor live and archived footage from doors.
- Use manual commands to lock, unlock and lock down doors, arm and disarm areas and activate and deactivate outputs.
- Add Protege GX doors and other records to XProtect maps, creating a unified view of the whole building.
- Monitor and report on access control and intrusion events within XProtect and view archived camera footage for each event.
- Set up custom alarms in XProtect based on Protege GX events. Acknowledging alarms in either XProtect or Protege GX will also acknowledge them in the other software, preventing double-handling.
- Receive an access request notification with camera footage whenever a user is denied access at a door, enabling operators to assess the situation and unlock the door remotely.
- View Protege GX users and photos within the XProtect Smart Client.

The application note covers the installation and setup instructions for the Protege GX XProtect Access Integration plugin for Milestone XProtect. For more information about using XProtect, see the Milestone documentation.

Milestone XProtect Integration Comparison

ICT offers two different integrations between Milestone XProtect and Protege GX which have different architecture and capabilities.

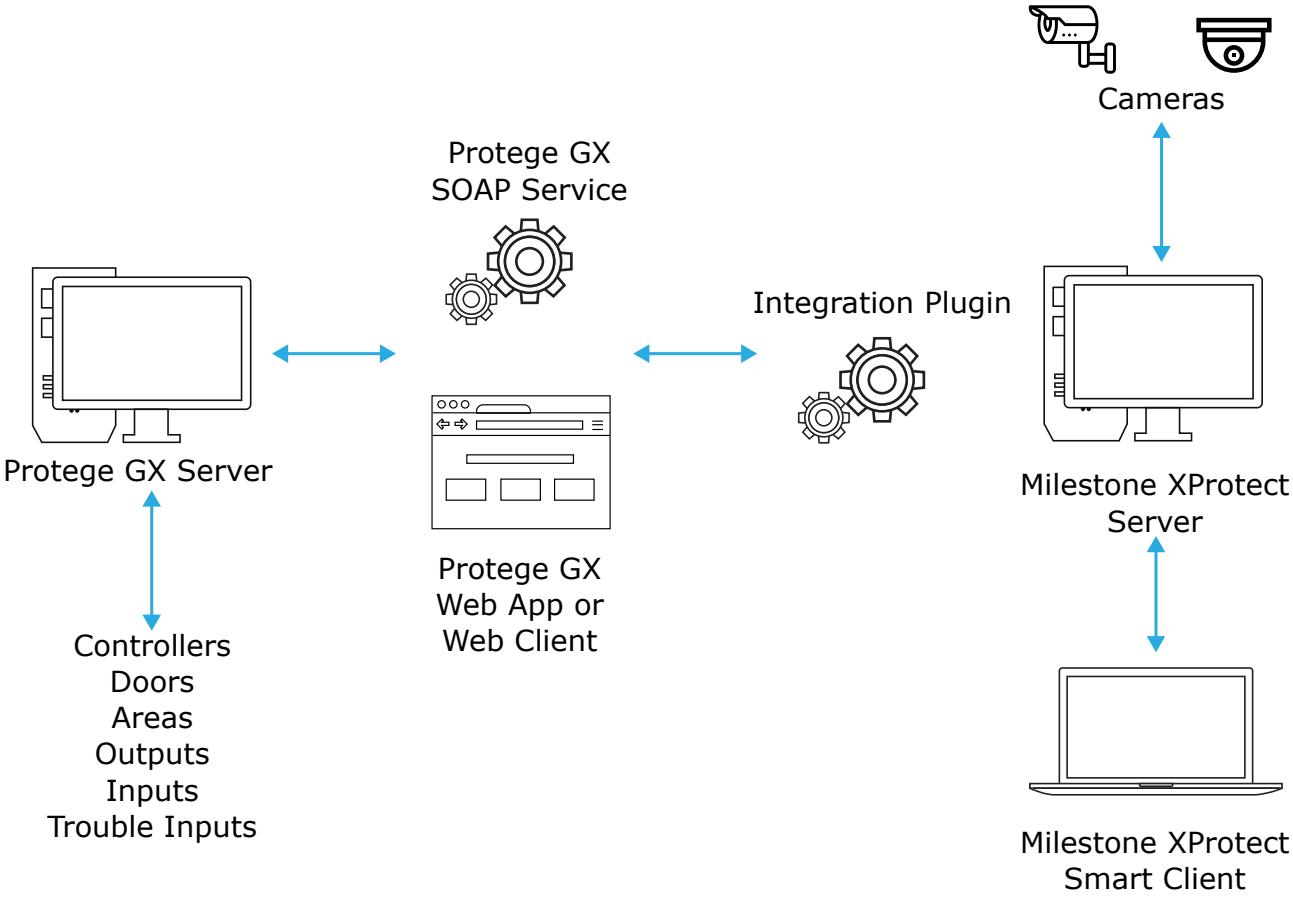
	Protege GX XProtect Video Integration	Protege GX XProtect Access Integration
Architecture	A middleware service connects the two systems	An MIP plugin installed on the XProtect server connects to the Protege GX SOAP Service
Main User Interface	Protege GX Client	XProtect Smart Client
Synchronization	Cameras and events are synchronized from XProtect to Protege GX	Access control devices, events and cardholders are synchronized from Protege GX to XProtect.
Commands	PTZ commands are sent from Protege GX to XProtect	Manual commands (e.g. lock, unlock) are sent from XProtect to Protege GX
Application Note	AN-242 Protege GX XProtect Video Integration	AN-358 XProtect Access Integration with Protege GX

The XProtect Access integration was formerly known as Milestone XProtect Bidirectional.

It is possible to run both integrations at the same time, enabling operators to use either Protege GX or XProtect as their user interface. These must be installed and configured separately following their respective application notes.

Integration Architecture

The Milestone XProtect Access Integration is based on a plugin that sits inside the XProtect Event Server. This plugin communicates with the Protege GX SOAP Service and Web Client to retrieve information from Protege GX and display it in the XProtect Smart Client. It also sends commands back to Protege GX based on operator actions such as locking/unlocking doors and acknowledging alarms.



Synchronized Records

The following records are synchronized from Protege GX to XProtect:

Protege GX Record	XProtect Record	Notes
Events	Events	
Users	Cardholders	User photos are synchronized if they are present in Protege GX.
Doors	Doors	Status and manual commands are available in XProtect. Only records that are associated with a host controller will be synchronized.
Salto doors	Doors	
Areas	Devices	
Inputs	Devices	
Outputs	Devices	
Trouble inputs	Devices	Status is available in XProtect, but not manual commands.
Controllers	Devices	

If multiple Protege GX sites have the integration enabled, all of them will be synchronized to XProtect.

Prerequisites

You must have administrator permissions on the machine where you are installing the plugin.

Software

This integration is only supported when all Protege GX components are installed on a different server from Milestone XProtect. For more information, see Preparation (page 9).

Component	Version	Notes
Protege GX	4.3.362.1 or higher	
Protege GX SOAP Service	1.6.0.12 or higher	
Protege GX Web App	Any version	Either the web app or web client can be used with this integration.
Protege GX Web Client	1.48.0.0 or higher	
Protege GX XProtect Access Integration Plugin	1.0.5.0 or higher	
Milestone XProtect	Professional+ 2026 R1, 2025 R3	These are the **only** tested and supported versions for this integration. If you are using version 2025 R3, you must apply the latest **Event Server Hotfix** to your XProtect installation. This resolves an issue where some alarms do not trigger correctly in XProtect. The hotfix is not required for the 2026 version. You can download the hotfix from the Milestone Support Portal.

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.

Licensing

License	Order Code	Notes
Protege GX XProtect Access Integration License	PRT-GX-VMS-MLSTN-30DR PRT-GX-VMS-MLSTN-99DR PRT-GX-VMS-MLSTN-100+DR	1 per Protege GX system. There are three license tiers based on the number of Protege GX doors that will be synchronized to XProtect: • 1-30 doors • 31-99 doors • 100+ doors
Protege GX XProtect Access Integration Annual Care Plan	PRT-GX-VMS-MLSTN-ACP-30DR PRT-GX-VMS-MLSTN-ACP-99DR PRT-GX-VMS-MLSTN-ACP-100+DR	The annual care plan must be purchased alongside the base integration license. It is charged annually for ongoing support and integration updates. Select the annual care plan license that corresponds to your base license tier.

License	Order Code	Notes
Protege GX Photo ID License	PRT-GX-PHOTO	1 per Protege GX system. Only required if you need to synchronize user photos from Protege GX to XProtect.
Milestone XProtect Base License		Contact Milestone for licensing information.
Milestone XProtect Access Control License		1 per integrated door. Contact Milestone for licensing information.

Time Settings

VMS integrations rely on the time being accurately configured for both the hardware and the operating systems used in a site.

To ensure the system is keeping precise time, all devices should be set to synchronize with the same NTP time server. NTP servers work by sending accurate time information periodically to the system. Many corporate organizations have an NTP server running on the internal network, allowing you to simply enter the relevant IP address. Alternatively, you could use any public NTP server. Finding an NTP server relevant to your region is usually as simple as a quick web search.

The same time server must be used for all workstations, servers and controllers within the site. You can configure the time server for each computer in the Windows **Date and Time** settings, and set a time server for the controller in the **Sites | Controllers | Time update** settings in Protege GX.

Preparation

All Protege GX and Milestone XProtect must be installed on separate servers.

Before you begin, install the following software on each server:

- **Protege GX Server**: Protege GX, SOAP service, and web app or web client
- **XProtect Server**: Milestone XProtect

Installing these software components on the same server will cause Milestone XProtect to become unusable. If this happens, contact ICT Technical Support.

You must also complete some additional preparation to ensure that the two servers can communicate with each other.

HTTPS Certificates

HTTPS certificates enable Protege GX and XProtect to communicate with each other using the encrypted HTTPS protocol. To allow communication, the Protege GX SOAP Service and Web Client must both use HTTPS certificates that are trusted by the XProtect server.

By default, the self-signed certificates used by the SOAP service and web client are not trusted by other computers, so XProtect will refuse the connection from Protege GX. There are two ways to solve this problem:

1. Acquire trusted certificates and bind them to the SOAP service and web app or web client. The certificates can be supplied by a third-party certificate authority or internal public key infrastructure (PKI).

   This is the recommended method for live sites.

2. Export the self-signed certificates for the SOAP service and web app or web client, then import them to the Trusted Certificates Store on the XProtect server.

For instructions covering these processes for both SOAP and the web client, see the Protege GX Web Client Installation Manual. For the web app, see the Protege GX Web App Installation Manual.

Service Accessibility

The Milestone XProtect server must be able to reach the endpoints for the SOAP service and web app or web client.

Ensure that networks and firewalls are configured so that the XProtect server can access the following ports from the Protege GX server:

- 8040 (default SOAP port)
- 8083 (default web app port); or,
- 8060 (default web client port)

To confirm that the services are accessible, open a web browser on the XProtect server. Enter the following URLs, replacing the placeholders with the details of the Protege GX server:

- **SOAP service**: https://<pcname>.<domainname>:8040/ProtegeGXSOAPService/service.svc
- **Web app**: https://<pcname>.<domainname>:8083
- **Web client**: https://<pcname>.<domainname>:8060/ProtegeGXWebClient/login.php

If the browser can load web pages for these URLs, the services are accessible.

Installing on Different Domains

If your XProtect server is **on a different domain** from the Protege GX server, you may also need to add an entry to the hosts file on the XProtect server so that it can recognize the Protege GX server's IP address.

1. On the Protege GX server open **Settings** and find the following details:
   - Find the Protege GX server's IP address in **Network & internet**.
   - Find the **Full device name** (fully qualified domain name) in **System > About**.
2. On the XProtect server, in the File Explorer, navigate to C:\Windows\System32\drivers\etc
3. Open the **hosts** file.

   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. On a new line, enter the IP address of the Protege GX server, followed by a space, then the fully qualified domain name of the Protege GX server. For example:

   ```
   10.10.32.410 pcname.domainname
   ```

5. Save the file.

Configuring Protege GX

Some configuration is required in Protege GX before installing the plugin.

Enabling the Integration

To enable the integration:

1. In Protege GX, navigate to **Global | Sites**.
2. In the **Site Defaults** tab, check **Enable Milestone bidirectional integration**.
3. Click **Save**.

Creating the Operator

An operator record will be needed for the plugin to connect to the SOAP service. Creating a unique operator record ensures that actions performed from the XProtect Smart Client can be distinguished from other actions by Protege GX operators.

1. Navigate to **Global | Operators**.
2. Add a new operator with a descriptive name, e.g. XProtect Access Integration.
3. Set a new **Username** and a temporary **Password**.
4. Set the **Role** to Administrator or Installer.
5. Click **Save**.
6. Open another instance of Protege GX and log in as the new operator. When prompted, set a new, secure password.

   You will need to enter this password regularly when you synchronize the integration. Store it in a secure but accessible location such as a password manager.

Syncing Events

When the integration was enabled, the system automatically created the Milestone Bidirectional event filter to determine which events would be synchronized to XProtect. You must apply this filter to an event report and enable synchronization to send events through to Milestone.

1. Navigate to **Reports | Setup | Events**.
2. Add a new event report with a descriptive name, e.g. XProtect Integration Events.
3. Under **Event filters**, add the Milestone Bidirectional event filter.
4. Under **Integrations**, select **Sync to Milestone**.
5. Click **Save**.

By default the event filter allows all events, but only events that are relevant to access and devices are received by XProtect. If you wish to further restrict the events sent to the integration, edit the Milestone Bidirectional event filter in **Events | Event filters**.

Installing the Plugin

You must run the plugin installer on the machine where the XProtect Event Server is installed.

1. Locate the Milestone XProtect Event Server icon in the notification area at the right of the taskbar.
2. Right click on the icon and click **Stop Event Server service**.
3. Run the XProtect Access integration installer provided by ICT.
4. Click **Next**.
5. Accept the license agreement, then click **Next**.
6. Make a note of the installation folder for the plugin. This is where the data synchronized from Protege GX will be stored.
7. Select **Everyone** to install the application for all users on this computer. Click **Next**.
8. Click **Next**.
9. Once the installation is complete, click **Close**.
10. Right click on Milestone XProtect Event Server and click **Start Event Server service**. This will load the plugin into the XProtect Event Server.

Granting Folder Access

The XProtect Event Server needs write access to the folder where the service data is stored to allow it to use the plugin.

1. In the File Explorer, navigate to C:\Program Files\Milestone\XProtect Event Server\MIP Plugins
2. Right click on the plugin folder and select **Properties**.
3. In the **Security** tab, select the account that the XProtect Event Server is using.
   - If the service is using a local system account (default), select **Users**.
   - If this is a specific service account, select that account from the list.
4. Click **Edit**.
5. Enable the **Full control** permission.
6. Click **OK**.
7. Click **OK**.

Configuring the XProtect Management Client

This section covers how to enable the access control plugin and configure the integration in the XProtect Management Client.

Enabling the Access Control Plugin

You must enable and configure the plugin in order to synchronize doors, devices, cardholders and events from Protege GX.

1. Log in to the XProtect Management Client.
2. Navigate to **Access Control**.
3. Right click on **Access Control** and select **Create new...**
4. Enter a descriptive name, e.g. Protege GX Access Integration.
5. Set the **Integration plug-in** to BiDirectional_Milestone.
6. Enter the connection details for Protege GX:
   - **Address**: Enter the HTTPS endpoint for the SOAP service. Typically this is:
     https://<pcname>.<domainname>:8040/ProtegeGXSOAPService/service.svc
   - **User**: The operator username created above.
   - **Password**: The operator password created above.
   - **Event polling period**: By default, event and status data will be updated from Protege GX every 1000ms (once per second).
   - **Event polling max count**: The maximum number of events and status updates returned per request (maximum of 200).
   - **Configuration polling period**: By default, user information will be updated from Protege GX every 60 minutes. You can also update the data manually by clicking the **Refresh Configuration...** button.

     Due to a limitation of XProtect, configuration for other records can only be refreshed manually using the **Refresh Configuration...** button.
   - **Web URL**: The HTTPS URL for the Protege GX Web App or Web Client. This allows operators to easily open the users page when they need to view or edit a user record.

     The default URL is:
     - **Web app**: https://<pcname>.<domainname>:8083/
     - **Web client (Users page)**: https://<pcname>.<domainname>:8060/ProtegeGXWebClient/user.php
   - **The xml folder**: The folder where the data retrieved from Protege GX is cached. The XProtect Event Server must have write permission for this folder. By default this is:

     C:\Program Files\Milestone\MIPPlugins\Bidirectional
7. Click **Next**.
8. The plugin will sync the event types, users, doors and other devices from Protege GX. Once this is complete, click **Next**.

   Records that do not have a host controller will not be synchronized.
9. In the next screen you can associate cameras with the doors and Salto doors synchronized from Protege GX. This can also be done later in the **Doors and Associated Cameras** tab.
   - All synchronized doors are enabled by default. If there are any Protege GX doors that should not be available in XProtect, disable the checkboxes.
   - To associate a camera with a door, click on the door record, then drag and drop the camera into the entry

or exit field.

10. Click **Next**, then **Close** to complete the setup.

Access Control Plugin Settings

Open the Protege GX plugin from the **Access Control** menu to configure the integration.

General Settings

This tab allows you to edit any of the synchronization settings configured during the initial setup (see previous page). In addition, the following settings are available:

- **Refresh Configuration...**: Click this button to resynchronize the records from Protege GX. This is required if there are any configuration changes to doors and other devices, and can also be used to update the user configuration before the **Configuration polling period** has expired.

  You may be asked to enter the Protege GX operator password to complete the operation.

- **Cardholder image override enabled**: With this option enabled, whenever a user image is updated in Protege GX the new image will be synchronized to XProtect. If an operator has changed the cardholder image in XProtect, it will be overwritten by the new image from Protege GX.

  With this option disabled, cardholder images will only synchronize from Protege GX the first time the image is added, and can be changed permanently in XProtect.

Doors and Associated Cameras

This tab enables you to assign entry and exit cameras to doors and Salto doors synchronized from Protege GX. When you view a door in the XProtect Smart Client you will also see the live camera footage for that door. In addition, events from that door will include recorded footage from the associated camera.

- All synchronized doors are enabled by default. If there are any Protege GX doors that should not be available in XProtect, disable the checkboxes.
- To associate a camera with a door, click on the door record, then drag and drop the camera into the entry or exit field.

Access Control Events

This tab enables you to view the event types that have been synchronized from Protege GX. Use the checkboxes to disable events that are not required in XProtect.

Each event type has a default **Event Category** based on its function (e.g. Door, User). You can also assign additional event categories to each event to activate specific features when that event occurs.

- **Alarm**: Select the Alarm category to log an alarm whenever the event occurs. Any events that were already configured as alarms in Protege GX will have this category applied automatically. For more information, see Alarms (page 18).
- **Access Request**: Select this category to generate an access request whenever specific events occur. For more information, see Access Request Notifications (page 20).
- **User-defined Categories**: Click this button at the bottom of the window to create custom categories that can be applied to events. You can use these categories to trigger alternative alarms and access requests.

Access Request Notifications

Access request notifications are camera popups that appear when specific events occur and allow you to activate a manual command. Typically they are used when a user is denied access at a door, enabling the operator to assess the access request and choose whether to unlock the door from the XProtect Smart Client.

For more information, see Access Request Notifications (page 20).

Cardholders

In this tab you can view the cardholders (Protege GX users), including their name, photo, access level, card number and expiry date.

It is also possible to update the cardholder photo, but note that this will not be synchronized back to Protege GX due to a limitation in the XProtect system. If **Cardholder image override enabled** is checked, the image will be overwritten the next time it is updated in Protege GX.

Access Control in the XProtect Smart Client

The **Access Control** tab in the XProtect Smart Client contains all of the events, cardholders, doors and other devices synchronized from Protege GX.

For more information about using XProtect's access control features, see the Milestone XProtect Smart Client documentation.

Monitoring Events

The XProtect Smart Client enables you to monitor live and archived events from Protege GX alongside camera footage from the Milestone system. You can also export access reports based on a filtered set of events.

- The event list shows the event type, source and cardholder. Select the event to read the full text, view the cardholder's details and review camera footage from the time of the event.
- Use the search bar and filters to narrow down the events list to those you are interested in.
- To view live events, set the **Time** filter to Live Update. The event list will be updated from Protege GX every second by default.
- To view archived events, select a pre-defined time period or define a custom period.

  If there was a disconnection between the XProtect and Protege GX systems during this period, you will see the warning 'Interruption registered in the specified interval'. Click the warning to see when the disconnection occurred.
- After filtering the event list, click the **Access Report** button to export the filtered events. Select **Include Snapshots** to incorporate camera images from the time of each event.

Monitoring and Controlling Devices

To view the devices synchronized from Protege GX, navigate to **Access Control > Doors**. This tab displays all of the doors, Salto doors, areas, outputs, inputs, trouble inputs and controllers synchronized from Protege GX, as well as the connection status with the Protege GX server.

- Each door and device displays its current status. Select the record to display the live feed from the camera associated with it.
- The manual commands for the device are displayed beneath the camera feed. Click the down arrow to display the commands that are not visible. This allows you to lock/unlock doors, arm/disarm areas, activate/deactivate outputs and bypass/unbypass inputs.
- By default the list displays the All doors list (including doors, Salto doors and controllers). To view other devices:
  - Open the third filter (All doors).
  - Select **Other...**
  - Select each device you wish to display and click **Add**.
  - Click **OK** to apply the new filter.
- To locate specific devices, use the search bar or filter the list by device type, current state (e.g. locked vs. unlocked) or record names.

Notes

- Each door record from Protege GX is represented by three objects in XProtect: the door itself, the entry location (outside the door) and the exit location (inside the door). The entry and exit locations can have different cameras assigned to them but do not have a status.
- No commands are available for controllers and trouble inputs.

- **Cancel Override** is equivalent to the **Cancel calendar action** command in Protege GX. **Restore Status** is equivalent to **Restore calendar action**. These commands are only relevant if calendar actions are in use.

Viewing Cardholders

View cardholders in the **Access Control > Cardholders** tab.

- If you need to view or edit the user record, click the **Manage Cardholder** button to open the users page. You will need to log in the first time you click the button.
- Click **View cardholder events** to open a filtered event log for that cardholder.

Adding Doors and Devices to Maps

The easiest method for monitoring and controlling specific Protege GX doors and other devices in XProtect is to add them to a map. To add objects to a map:

1. In the XProtect Smart Client, select the tab for the map you wish to edit.
2. Click **Setup** in the top right.
3. In the **Tools** window, select **Add access control**.
4. Locate a door or other device, then click and drag it into the appropriate location on the map.
5. When you are done editing the map, click **Setup** again.

When viewing the map:

- Doors, Salto doors and controllers have icons that show their current status graphically.
- For other device types (e.g. areas and inputs), to view the current status right click on the text label and select **Status details**. This opens the status in a small popup window.
- Right click on any object to select manual commands for that object.

Alarms

Protege GX events can be configured as alarms in Milestone XProtect, causing them to appear in the **Alarms** tab of the XProtect Smart Client. When you acknowledge an alarm in XProtect, it will also be acknowledged in Protege GX.

Configuring Alarms

To select the events that will raise alarms in XProtect, you must apply the Alarm event category or a custom user-defined event category. There are two different ways of achieving this.

If you want the same events to generate alarms in both Protege GX and XProtect, you can create the alarms in Protege GX:

1. In **Events | Event filters**, create an event filter containing the events which should raise the alarm.
2. In **Events | Alarms**, create an alarm record containing that event filter.
3. In the XProtect Management Client, under **Access Control > General**, click **Refresh Configuration...**. The Alarm category will automatically be applied to the selected event types.

If you want events to generate alarms in XProtect but not in Protege GX, configure the event categories in the XProtect Management Client:

1. In **Access Control**, select the **Access Control Events** tab.
2. If desired, click **User-defined categories** to create a new category. This allows you to differentiate multiple types of alarms.
3. Locate the events you wish to generate alarms and set the **Event Category** to either Alarm or your custom category.
4. Click **Save**.

You must then create an alarm definition for that event category:

1. In the Site Navigation, navigate to **Alarms > Alarm Definitions**.
2. Right click on the heading and select **Add New...**
3. Enter a **Name** for the alarm definition.
4. Enter any **Instructions** you wish to display with this alarm.
5. Set the **Triggering Event** to Access Control Event Categories.
6. From the second dropdown, select the Alarm category or your custom category created above.
7. By default, the alarm will occur for any door or device from Protege GX. Use the **Sources** dropdown to select specific devices that will trigger this alarm (e.g. only high-security doors).
8. Set any other options that are needed for this alarm (see the XProtect documentation for more information).
9. Click **Save**.

Viewing and Acknowledging Alarms

When an access control alarm occurs, it will appear in the **Alarms** tab of the XProtect Smart Client. Here you can view the event and any instructions and camera views associated with it.

Due to limitations of the XProtect system, only the event type and source are displayed, not the full event text. To view the event text, use the timestamp to locate the same event in **Access Control > Events**.

Right click and select **Acknowledge** to change the alarm's status from New to In Progress. When you acknowledge an alarm in XProtect it will also be acknowledged in Protege GX, adding the event to the All Acknowledged Alarms report. This also works in reverse: acknowledging alarms in Protege GX will also acknowledge them in XProtect.

Access Request Notifications

Access request notifications are camera popups that appear when specific events occur, allowing XProtect Smart Client operators to observe the situation and activate manual commands. For example, when a user is denied access at the door the operator can view who is trying to get through, communicate with them and choose whether to unlock the door.

This example shows how to create a popup notification for 'Access Denied' events at specific doors. If you create a custom event category in the **User-defined Categories** tab, you can configure popups for different scenarios such as area alarms.

First you must configure the notification:

1. In the XProtect Management Client, navigate to **Access Control** and open the **Access Request Notifications** tab.
2. Select the **Access denied** category.

   This category is automatically created when you install the plugin. It contains all access denied events from Protege GX. You can edit this category or create different ones in the **User-defined Categories** tab.
3. By default the **Camera** is set to Related camera so that the notification window shows the cameras assigned to the entry and exit of the door (in the **Doors and Associated Cameras** tab). Select a specific camera if required.
4. The **Speaker** and **Microphone** settings enable the person at the door to communicate with the operator. By default these use the camera's inbuilt speaker and microphone.
5. If required, select a **Sound alert** to play when the notification appears.
6. In the **Commands** field you can select the commands that will be available to the operator in the notification window. To add commands:
   - Click **Add Command**.
   - Expand the **Select command...** dropdown.
   - Select **Related access request commands** to list all of the commands available for the source of the event (e.g. lock/unlock/lockdown commands for a door).
   - Alternatively, select a specific **Access control command** to display. You can select a command for either the source of the event, or another record.
7. Click **Save**.

Then you can create the rule that triggers the notification when specific events occur:

1. Navigate to **Rules and Events**, **Rules**.
2. Add a new rule called Access Request Notifications.
3. **Step 1**: Under **Type of rule**, select the action: **Perform an action on <event>**
4. In the lower pane, set the description for this rule:
   - **Perform an action on event**: The events that will cause the notification to appear. Under **Access Control > Access Control**, select **Access Denied**.
   - **from devices/recording server/management server**: Select the doors that will generate the notification.

   Click **Next**.
5. **Step 2**: If required, set conditions on the notifications (e.g. a specific time period when notifications will occur). Click **Next**.
6. **Step 3**: Scroll to the bottom of the **Actions** list and select **Show <access request notification>**.
7. Set **Show access request notification** to the custom access request notification that you created above. Click **Next**.
8. **Step 4**: No configuration required. Click **Finish**.

When someone is denied access at one of these doors, any operator using the Smart Client should receive a popup with the camera view and manual commands you selected.

Troubleshooting

Events not populating in XProtect after Protege GX database change

If you restore a new Protege GX database, swap databases or change the instance name after installing the plugin, events may stop flowing through to XProtect. This occurs because the XProtect Access plugin caches the Protege GX database details. A standard configuration refresh is not sufficient to clear this cached data.

To resolve this issue:

1. In the XProtect Management Client, delete the existing Access Control plugin instance.
2. Stop the **Milestone XProtect Event Server** service.
3. Uninstall the XProtect Access plugin.
4. Delete all contents of the plugin cache folder. The default location is:
   C:\Program Files\Milestone\XProtect Event Server\MIPPlugins\BiDirectionalProtegeGXMilestone
5. Reinstall the XProtect Access plugin (see page 12).
6. Start the **Milestone XProtect Event Server** service.
7. Recreate the Access Control plugin instance with the original connection details (see page 13).
8. Verify that events are populating in the XProtect Smart Client under Access Control > Events.

Known Issues

ICT would like to make you aware of the following known issues with this integration:

- Cardholder expiry dates may display incorrectly within the XProtect client.
- If your system uses the web client, when you click **Manage Cardholder** it only opens the Users page, not the specific user you were viewing. This issue does not occur in the web app.
- If you disable and re-enable the integration in the **Access Control | Systems** page of the XProtect Management Client, it will not prompt for the password again. This will cause the integration to disconnect on the next configuration refresh with an Invalid credential error.

  To avoid this issue, disable and re-enable the integration on the **General settings** page for the plugin. If the password has been cleared, you can enter it again on this page.

Release History

Version 1.0.0.0

Initial release of the Protege GX XProtect Access Integration Plugin.

Version 1.0.1.0

- Resolved a synchronization issue that prevented Protege GX events and statuses from syncing to XProtect.

Version 1.0.5.0

- Added support for XProtect 2026 R1 and 2025 R3.

  If you are using version 2025 R3, you must apply the latest **Event Server Hotfix** to your XProtect installation. You can download the hotfix from the Milestone Support Portal.

- Updated the name of the integration from "Milestone Bidirectional" to "XProtect Access".
- Added support for the Protege GX Web App.

  If you want to transition your system from the web client to the web app, change the **Web URL** in the access control plugin settings in XProtect (see page 13). Then restart the XProtect Event Service.

- When you enable the plugin, it now automatically creates event categories for 'Access Denied' and 'Access Granted' events from Protege GX. See Access Request Notifications for more information about how to use event categories.
- Resolved an issue where the integration could stop functioning after a configuration change.
- Resolved an issue where some alarms would not trigger as expected within XProtect.
- Resolved an issue where operator events could incorrectly be associated with the user with the same Database ID.
- Resolved an issue where user images updated in Protege GX would not override the cardholder images in XProtect.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

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.