AN-341

Programming Area Loiter Functionality in Protege GX

Application Note

Last Published: 27-Jan-22 1:51 PM

Contents

Introduction

The area loiter feature in Protege GX enables facilities to limit the amount of time users spend in an area. This is commonly used in carparks, and can potentially be used to enforce payment for exceeding a free parking period. It can help restrict congregation in transition areas, and may be used in break rooms to ensure that staff are not exceeding break times.

When a user enters the area the loiter timer starts. If they stay in the area longer than the allotted time the system automatically moves the user into the loiter reset area (a virtual 'holding area'). When the user attempts to leave the physical area the system detects that they are in the wrong area and records an event due to the antipassback violation. The user may also be denied exit, and cannot leave until their antipassback status has been reset.

Antipassback

The area loiter function utilizes antipassback programming to enforce area loiter settings. Antipassback works by tracking which area each user is currently in, based on the doors they have entered or exited. Each door is assigned an 'inside area' and 'outside area', which represent the physical rooms on either side of the door.

When a user requests access at an antipassback-controlled door, the system checks whether the area they were last detected in matches the required inside/outside area for the door. If the current area recorded in the system matches the area the user is physically in, the system grants access and updates the current area to the one the user is entering. If the current area does not match the actual area, the user triggers an antipassback violation.

When an antipassback violation occurs there are two possible responses, based on the configuration of the door:

- **Hard antipassback**: When a user violates antipassback rules they are denied access to the door. They cannot gain access until they reset their current area in the system to the correct area. An event is logged to indicate the reason access was denied. This option actively prevents people from accessing doors illegitimately.
- **Soft antipassback**: When a user violates antipassback rules they are still allowed access to the door, however an event is recorded in the event log which allows operators to monitor and report on antipassback violations without interrupting the normal flow of traffic.

For more information on antipassback, see Application Note 337: Configuring Antipassback in Protege GX.

Prerequisites

Area loiter functionality is supported in all versions of Protege GX. No specific software or firmware versions are required but it is recommended that you use the latest versions to take advantage of any relevant improvements.

The following area loiter feature enhancement was introduced in the stated Protege GX software version.

Area Loiter Feature	Protege GX Software Version
Reset loiter area command from User Loiter Time Expired events	4.2.181 or higher

Antipassback Requirements

To track user areas correctly, every door which uses antipassback must have a card reader or other credential input (such as PIN pad or license plate camera) for both entry and exit.

If a door does not allow access in one direction, there is no need to have a reader on that side of the door.

Area Loiter Programming

Programming the area loiter feature requires the following configuration:

- Loiter mode must be enabled for each area in which a loiter limit will be enforced.
- The loiter time needs to be defined to specify how long users are permitted to stay in each area.
- A loiter reset area must be assigned as the virtual holding area for users who exceed the loiter time.
- Doors will require door types assigned which have antipassback rules configured for loiter operation.
- Doors must have the area inside and area outside defined to identify where users are moving out of and into.
- The loiter expiry count option needs to be enabled for users who will be subject to area loiter rules.

Area Programming

1. Navigate to **Programming | Areas**.
2. If you do not already have a loiter reset area, click **Add** and create one.

   > The loiter reset area does not require any additional programming like a normal intruder area, and doesn't need to be armed. However, you might want to arm the 24hr portion to prevent health status messages.

3. Now select the area that will have loiter restrictions applied.
4. In the **Options 1** tab, enable the **Area enabled in loiter mode** option.
5. In the **Configuration** tab, set the **Loiter time in minutes** to define how long users can remain in this area before they are 'moved' into the assigned **Loiter reset area**.
6. Set the **Loiter reset area** to the virtual holding area. This must be an area which users cannot physically access.
7. Click **Save**.

Antipassback Configuration

Antipassback configuration in door types allows you to define what will happen when a user attempts to enter or exit an area controlled by a door with that type assigned. You may need only one configuration (door type) for all loiter related doors, or you may want to apply different antipassback rules to different doors.

1. Navigate to **Programming | Door types** and click **Add** to create a new door type to use for area loiter control.
2. In the toolbar, click **Copy**. This allows you to use an existing door type which has the necessary access settings (such as Card, Card and PIN, or even a custom configuration) as a basis for your new door type.
3. In the **Copy from existing record** window, select the door type **Record** to copy, then click **OK**.
4. Edit the **Name** of the new door type.
5. Set the **Entry/Exit passback mode** as required for each direction.

   > None is **not** a valid selection. Each direction must have soft or hard passback enabled.

   - Soft passback: Antipassback is enabled in this direction. When there is a violation the door will generate an event, but allow access.
   - Hard passback: Antipassback is enabled in this direction. When there is a violation the door will deny access and generate an event.

   > Entry passback settings control access to the door's **Area inside door**. Exit passback settings control access to the door's **Area outside door**.

6. You may want to enable the **Entry/Exit passback is qualified with door opening** options to ensure that the user's area is only updated if the door is actually opened, not simply when they are granted access.
7. Click **Save**.

Door Programming

For the area loiter feature to work the system needs to know when a user is in the loiter area. For this to occur, as a minimum the area needs to be set as the area inside door for any entry doors which access the area, and as the area outside door for any exit doors which lead out to the loiter area.

A more comprehensive configuration is to assign the area inside/outside for every door in the system, with an 'offsite' area outside external doors, however this is not required for simply configuring the loiter operation.

1. Navigate to **Programming | Doors** and select the door which controls access to the loiter area.
2. Set the **Area inside door** to the loiter area.
3. Click **Save**.
4. Repeat for all doors which provide entry access to the loiter area.
5. If any doors exit from another area into the loiter area, set the **Area outside door** to the loiter area.

   Antipassback settings operate on the door direction, not the area. If the loiter area is accessed by exiting from another area the door will apply the antipassback **exit** setting, so you may require another door type to configure antipassback behavior accordingly.

User Loiter Expiry Count Enabled

For a user to be subject to area loiter control they need to have the loiter expiry count option enabled.

1. Navigate to **Users | Users | Options** and select the user(s) to enable area loiter control for.
2. Check the **User loiter expiry count enabled** option, then click **Save**.

When this option is enabled the user will be included in loiter processing and restricted by any antipassback programming that applies. When this option is disabled the user is not affected by area loiter programming.

Users with **User has super rights and can override antipassback** enabled are also excluded from loiter control.

Resetting Antipassback Status

When an antipassback violation is triggered it must be reset before users will again be able to access the area.

Reset User Antipassback

Resetting the user's antipassback status sets their current area back to 'Unknown', which allows them to access any door that they have valid permission for.

There are three methods for manually resetting the antipassback status of a single user.

- Right click on the hard or soft antipassback failure event in a status list and click **Reset user antipassback**.
- Right click on the loiter time expired event in a status list and click **Reset loiter area**.

  This option requires Protege GX version 4.2.181 or higher.
- Right click on the user record in **Users | Users** and click **Reset antipassback**.

Automatic Reset

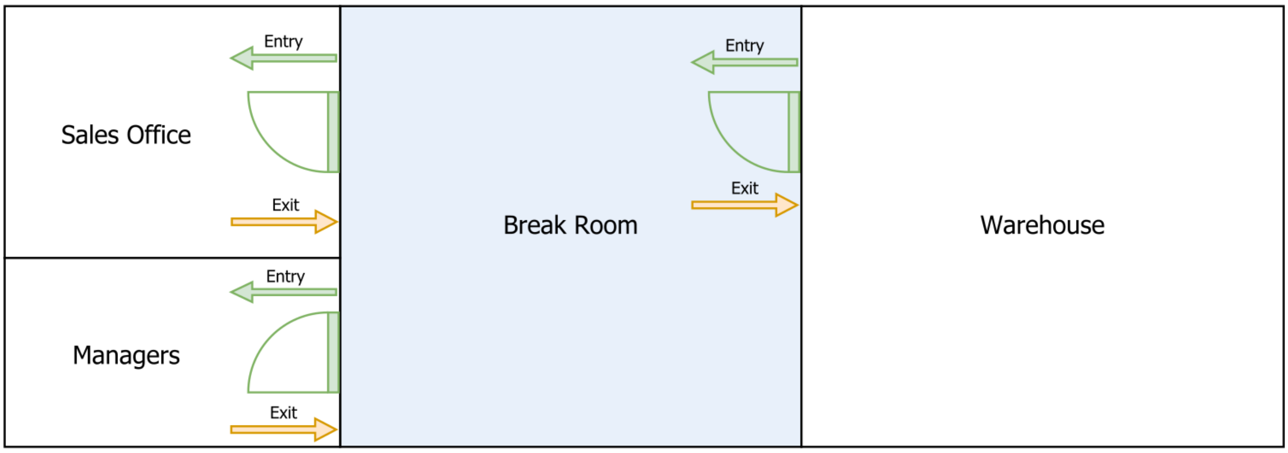
It is also possible to automatically reset the antipassback status for all users who have used a particular door, either on a fixed schedule or a timed periodic reset.

For more information see Application Note 337: Configuring Antipassback in Protege GX.

Programming Example

For this programming scenario we are going to apply area loiter control to the break room at B-Ear Brewing, who want to address an issue with staff taking excessive breaks. All staff are entitled to two 20 minute breaks per day, so we're going to use the area loiter function to help enforce this.

The break room can be accessed from the warehouse by **entering** through the break room door, or from the sales and managers offices by **exiting** through the sales office and managers doors respectively.



Because access to the break room is via 'entry' to the break room door and 'exit' from the office door, we will need two door types to configure the necessary antipassback settings. The managers door will not use any antipassback control. All doors in the building are accessed by card only.

If warehouse staff exceed the allocated break time we want to deny them exit from the break room so that they must go to the managers office and have their antipassback status reset by a manager before they can return to the warehouse. Sales staff regularly use the break room for meetings, so we don't want to deny them exit from the break room but we do want to record an antipassback violation event so that managers can review their violations and confirm that they are legitimate. The managers will not be subject to antipassback control.

Preparation

To complete this programming you will need the following records already created.

- A Break Room area
- A Warehouse area
- A Sales Office area
- A Managers area
- A User Loiter Area
- A Break Room Door
- A Sales Office Door
- A Managers Door
- At least 10 user records, including 3 'manager' users. Ensure that all users have access to all doors.
- A status page showing all events

You could extend this programming scenario by adding all external doors and set an 'offsite' area as their Area outside door for when staff leave the building.

Programming the Loiter Area

We first need to enable area loiter control for the break room.

1. Navigate to **Programming | Areas** and select the Break Room area.
2. In the **Options 1** tab, enable the **Area enabled in loiter mode** option.
3. In the **Configuration** tab, set the **Loiter time in minutes** to 22, to allow some lenience on the 20 minute limit.
4. Set the **Loiter reset area** to the User Loiter Area.
5. Click **Save**.

Adding the Antipassback Door Types

We will need to create two door types to configure the different entry/exit access direction and passback mode restriction settings.

1. Navigate to **Programming | Door types** and click **Add**.
2. In the toolbar, click **Copy**.
3. In the **Copy from existing record** window, set the door type **Record** to Card, then click **OK**.
4. Set the **Name** of the new door type to Antipass - Warehouse to Break Room.
5. Set the **Entry passback mode** to Soft passback.

   We do not want to deny entry to the break room, however the area loiter function does need to track user movement through this door, so that we know when users have entered the break room.

   > The system will record an antipassback violation event if the user attempts to enter the break room from the warehouse while the system believes they are in a different area.

6. Set the **Exit passback mode** to Hard passback.

   The system will record an antipassback violation event and deny exit access from this door if the user exceeds the 22 minute loiter time.

   > The same will apply if a user attempts to access the warehouse from the break room while the system believes they are in a different area.

7. Click **Save**.
8. Click **Add** and **Copy** the Card door type to create the second door type.
9. Set the **Name** of the new door type to Antipass - Break Room to Sales Office.
10. Set both the **Entry passback mode** and **Exit passback mode** to Soft passback.
11. Click **Save**.

Programming the Doors

1. Navigate to **Programming | Doors** and select the Break Room Door.
2. Set the **Door type** to Antipass - Warehouse to Break Room.
3. Set the **Area inside door** to the Break Room. Set the **Area outside door** to the Warehouse.
4. Click **Save**.
5. Select the Sales Office Door.
6. Set the **Door type** to Antipass - Break Room to Sales Office.
7. Set the **Area inside door** to the Sales Office. Set the **Area outside door** to the Break Room.
8. Click **Save**.
9. The **Managers** door should have its **Door type** set to Card.

Enabling the User Loiter Expiry Count

All staff other than the managers will be subject to area loiter control.

1. Navigate to **Users | Users | Options**.
2. Click on a user record, then press Ctrl + A on the keyboard to select all user records.
3. Check the **User loiter expiry count enabled** option, then click **Save**.
4. Now use Ctrl + C to select the 3 'manager' users and disable the **User loiter expiry count enabled** option.
5. Click **Save**.

This is the quickest way to apply a setting to a large number of records while omitting just a few.

Although the managers door does not enforce area loiter control or antipassback, the managers will still be moving through the other doors so this setting needs to be disabled so that they are not restricted.

Testing the Programming

To simplify our testing process, name one standard user Tom Tester and one manager Marcia Manager.

For testing purposes you will want to change the Break Room area's **Loiter time in minutes** setting to 1.

Events

Following are the access, loiter and antipassback events we expect to see during this testing.

Granted Entry

```
User <First name> <Last name> (<Facility>:<Card>) (UN<Database ID>)
Granted Entry To <Door name> (DR<Database ID>)
Access Level <Access level name> (AL<Database ID>)
Reading Mode <Reading mode description>
```

- **Example**: User Tom Tester (1:100) (UN10) Granted Entry To Break Room Door (DR15) Access Level Staff Access (AL3) Reading Mode Card Input

Granted Exit

```
User <First name> <Last name> (<Facility>:<Card>) (UN<Database ID>)
Granted Exit From <Door name> (DR<Database ID>)
Access Level <Access level name> (AL<Database ID>)
Reading Mode <Reading mode description>
```

- **Example**: User Tom Tester (1:100) (UN10) Granted Exit From Break Room Door (DR15) Access Level Staff Access (AL3) Reading Mode Card Input

Loiter Time Expired

```
User <First name> <Last name> (<Facility>:<Card>) (UN<Database ID>)
Loiter Time Expired In <Area name> (AR<Database ID>)
User Area Reset To <Loiter reset area name> (AR<Database ID>)
```

- **Example**: User Tom Tester (1:100) (UN10) Loiter Time Expired In Break Room (AR27) User Area Reset To User Loiter Area (AR29)

Soft Antipassback

```
User <First name> <Last name> (<Facility>:<Card>) (UN<Database ID>)
<Door Direction> Soft Antipassback Failure At <Door name> (DR<Database ID>)
Area <Area name> (AR<Database ID>)
User Area Reset To <Area name> (AR<Database ID>)
```

- **Example**: User Tom Tester (1:100) (UN10) Entry Soft Antipassback at Sales Office Door (DR16) Area Break Room (AR27) User Area Reset to Break Room (AR27)

Hard Antipassback

```
User <First name> <Last name> (<Facility>:<Card>) (UN<Database ID>)
<Door Direction> Antipassback Failure At Door <Door name> (DR<Database ID>)
Area <User Current Area name> (AR<Database ID>)
Required Area <Required User Area name> (AR<Database ID>)
```

- **Example**: User Tom Tester (1:100) (UN10) Exit Antipassback at Break Room Door (DR15) Area User Loiter Area (AR29) Required Area Break Room (AR27)

Baseline Testing

1. Navigate to **Monitoring | Status page view** and select a status page which displays all events.
2. Badge Tom Tester's card at the Break Room Door **entry** reader.
   - The system should record a Granted Entry To Break Room Door event.

     Depending on previous activity, an Entry Soft Antipassback Failure event may also be recorded.
3. Immediately badge Tom Tester's card at the Break Room Door **exit** reader.
   - The system should record a Granted Exit From Break Room Door event.

   If these basic entry and exit events are not working correctly you will need to review your programming. Denied access will likely be caused by incorrect area, door or acccess level configuration.

Area Loiter Hard Passback Testing

1. Badge Tom Tester's card at the Break Room Door **entry** reader.
   - The Granted Entry To Break Room Door event will be recorded.
2. Wait at least 1 minute for the loiter timer period to expire.
   - A Loiter Time Expired In Break Room, User Area Reset to User Loiter Area event will be recorded.
3. After the loiter time expired event is recorded, badge Tom Tester's card at the Break Room Door **exit** reader.
   - The system should record an Exit Antipassback Failure at Door Break Room Door event.
4. Right click on the Exit Antipassback Failure event and click **Reset user antipassback**.
5. Now badge Tom Tester's card at the Break Room Door **exit** reader again.
   - The Granted Exit From Break Room Door event should be recorded.

Area Loiter Soft Passback Testing

1. Badge Tom Tester's card at the Sales Office Door **exit** reader.
   - The Granted Exit From Sales Office Door event will be recorded.
2. Wait at least 1 minute for the loiter timer period to expire.
   - A Loiter Time Expired In Break Room, User Area Reset to User Loiter Area event will be recorded.
3. After the loiter time expired event is recorded, badge Tom Tester's card at the Sales Office Door **entry** reader.
   - The system should record an Entry Soft Antipassback Failure at Sales Office Door event.
   - The Granted Entry To Sales Office Door event should be recorded.

User Loiter Expiry Count Disabled Testing

1. Now badge Marcia Manager's card at the Break Room Door **entry** reader.
   - The system should record a Granted Entry To Break Room Door event.

     Depending on previous activity, an Entry Soft Antipassback Failure event may also be recorded.
2. Wait at least 2 minutes. You should **not** see a Loiter Time Expired event.
3. Badge Marcia Manager's card at the Break Room Door **exit** reader.
   - The Granted Exit From Break Room Door event should be recorded.

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

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.