AN-337

# Configuring Antipassback in Protege GX

Application Note

Last Published: 10-Dec-21 8:54 AM

# Contents

# Introduction

It is often considered polite to hold open a door for a colleague, or lend your access card to someone who has forgotten their own. Unfortunately, these social practices can undermine the security of your facility and create opportunities for dishonest employees or social engineers.

Antipassback configuration in Protege GX enables you to discourage or prevent users from passing back their access cards or PIN codes to someone else, or tailgating other employees through doors without entering credentials. Along with appropriate user education, antipassback can enhance the security and safety of the site, and improve the accuracy of user counting features such as automatic arming, attendance reports and muster reports.

Antipassback in Protege GX is ideal for:

- High-security areas such as server rooms, counting rooms and vaults
- Hazardous facilities where it is vital to have an accurate record of who is in the area
- Car parks
- Any facility using area counting, attendance reporting or muster reporting

## How Antipassback Works in Protege GX

Antipassback in Protege GX works by tracking which area each user is currently in, based on the doors they have accessed. 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 (the 'current area' or 'user area') matches the required inside/outside area for the door. For example, if a user is trying to enter a door, they must physically be within the outside area.

If the current area recorded in the system matches the area the user is physically present in, the system grants access to the door and updates the current area to the one that the user is now 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 that 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.

Antipassback may be enabled on specific high-security doors only, or across the entire site. It is not limited to specific controllers: when a user enters a door, the controller which hosts that door will send the user's new area to the other controllers in the system.

User education is very important for systems which use antipassback. Users must be aware that they are expected to enter their credentials every time they enter or exit an antipassback-controlled door. If they are not aware of this, legitimate users are likely to violate antipassback rules by accident, potentially preventing them from entering or exiting certain areas.

## Benefits of Using Antipassback

Antipassback settings are primarily designed to prevent or discourage users from 'passing back' their access cards, mobile credentials, PIN codes or other credentials to unauthorized people. This feature is commonly used in carparks, building entry doors and high security rooms.

For example, consider an employee carpark with card access. Without antipassback an employee can enter the carpark, then pass their card back to a friend to allow them to park there. In contrast, if antipassback is enabled, when the employee enters the the gate the system will record that they are in the carpark area. If another person then tries to enter using the same card, they will trigger an antipassback violation because the employee should already be in the carpark. Depending on the configuration, the system will either deny access or grant access and record an event so that the security team can investigate the issue.

Along with preventing unauthorized access, antipassback can be used to encourage legitimate users to enter their credentials every time they enter or exit a door. This improves the operation of a number of other features in the Protege GX system:

- Area counting
- Attendance reports
- Muster reports

For example, sometimes people follow other users through doors without entering their own credentials ('tailgating'). This makes it difficult to keep an accurate count of the users in an area or report on attendance statistics. A combination of antipassback and user education can mitigate these issues.

Antipassback also allows you to use the area loiter function, which discourages users from staying too long in an area such as a carpark or transitional zone.

# Requirements

- All Protege GX controllers and reader expanders support antipassback operation. 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.
- 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.

  For example, if a door has an entry reader but only a REX button for exit, it cannot identify which users are exiting the door. Therefore the system will not update the user's current area, which may lead that user to unknowingly cause antipassback violations later.

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

# Basic Antipassback Programming

The following steps provide an overview for programming antipassback for a single door with entry and exit card readers.

1. Navigate to **Programming | Doors** and select the door which requires antipassback settings.
2. Ensure that the door has an **Area inside door** and **Area outside door** set. These are both required for antipassback programming to operate correctly, as they tell the system which areas are physically adjacent to the door.

   > It is recommended that you create an 'Offsite' area to set as the outside area for external doors. This is not used as an intruder area, but instead keeps track of which users are not in the facility. If there is no outside area set, the user's current area will be set to 'Unknown' when they leave.

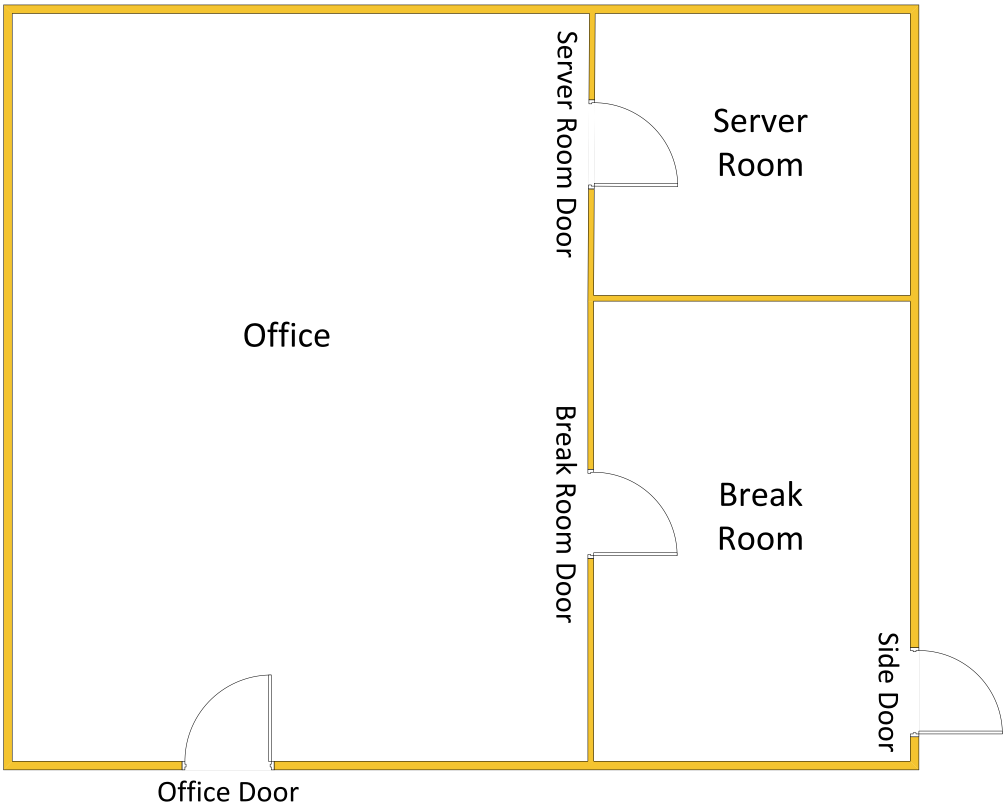
3. Navigate to **Programming | Door types** and add a new door type. This door type can be used for multiple doors, or you can create a new door type for each door.
4. Antipassback is set separately for the door's entry and exit directions. Enable entry antipassback to control access to the area inside the door, and enable exit antipassback to control access to the area outside the door.

   To enable antipassback, set the **Entry/Exit passback mode** as required for each direction:

   - None: Antipassback is not enabled in this direction. When the user passes through the door in this direction the system will not update the user's current area.
   - 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.
5. Set the **Entry/Exit reading mode** as required (e.g. card only, card and PIN).
6. Click **Save**.
7. Return to **Programming | Doors** and select the door which requires antipassback.
8. Set the **Door type** to the one created above.
9. Click **Save**.

# Scenario Outline

We will use a programming scenario to demonstrate the various antipassback features available in Protege GX. In this scenario, a company called Silph has experienced some security incidents caused by employees sharing or misplacing access cards. They also want to improve the quality of their attendance and muster reporting by ensuring that employees badge in and out of the office.



To fully program and test this scenario you will need a controller and reader expander, and an entry and exit reader for each door. All of the hardware must be online with Protege GX.

It is possible to test the programming with only a controller and 4 card readers by changing the address of the onboard reader expander.

Before you begin, program the following area records:

- Office
- Server Room
- Break Room
- Offsite

  This area is used for keeping track of users when they leave the building (not for intruder detection).

Configure the following door records, including the inside and outside areas required for antipassback operation:

| Reader Port | Door | Area inside door | Area outside door |
|---|---|---|---|
| RD1 Port 1 | Office Door | Office | Offsite |
| RD1 Port 2 | Server Room Door | Server Room | Office |
| RD2 Port 1 | Break Room Door | Break Room | Office |
| RD2 Port 2 | Side Door<br>(exit only) | Break Room | Offsite |

Finally, create an All Silph Doors access level and assign it to a user. We will create the Silph IT administrator, Gio Stone.

# Scenario: Hard and Soft Antipassback

Silph has two main antipassback requirements:

- Hard antipassback on the server room door to prevent users from passing their access cards to unauthorized people and allowing them into the server room.
- Soft antipassback on the office door to improve attendance and muster reporting for the building. The managers want to see which employees are forgetting to badge in and out.

## Programming the Server Room Door

1. Navigate to **Programming | Door types**.
2. Add a new door type with the name Server Room (Hard APB).
3. Set the **Entry passback mode** to Hard passback.
4. Set the **Exit passback mode** to Hard passback.
5. We will leave the **Entry/Exit reading mode** set to Card only.
6. Click **Save**.
7. Navigate to **Programming | Doors** and select the Server Room Door.
8. Set the **Door type** to Server Room (Hard APB).
9. Click **Save**.
10. We will test the programming using Gio Stone's access card.

    Badge at the entry reader of the Server Room Door. Access is granted, and the system records Gio entering the Server Room area.
11. Badge the same card at the entry reader again, as if Gio has passed his card back to another user. Access should be denied, and you will see the following event:

    ```
    User Gio Stone (1:6) (UN8) Entry Antipassback Failure At Door Server Room
    Door (DR16) Area Server Room (AR17) Required Area Office (AR16)
    ```

    This indicates that the system expects anyone entering the server room to be in the Office area, but Gio was last detected in the Server Room area. Therefore, there is an antipassback violation and access is denied.
12. Badge Gio's card at the exit reader for the Server Room Door to exit the room.
13. Badge at the entry reader again. Access is now granted, because Gio has correctly exited into the Office area before attempting to enter the Server Room.

## Programming the Office Door

1. Navigate to **Programming | Door types**.
2. Add a new door type with the name Office Door (Soft APB).

3. Set the **Entry passback mode** to Soft passback.
4. Set the **Exit passback mode** to Soft passback.
5. We will leave the **Entry/Exit reading mode** set to Card only.
6. Navigate to **Programming | Doors** and select the Office Door.
7. Set the **Door type** to Office Door (Soft APB).
8. Click **Save**.
9. To test the programming, we will simulate Gio leaving the office for the day. Badge at the exit reader for the Server Room Door.

   When he leaves the office, Gio tailgates another user and does not correctly badge out. Do not badge his card at the exit reader for the Office Door.
10. Gio arrives the next day and badges in. Badge the card at the entry reader for the Office Door. Access will be granted, but you will see the following event:

    ```
    User Gio Stone (1:6) (UN8) Entry Soft Antipassback Failure At Office Door
    (DR15) Area Office (AR16) User Area Reset To Office (AR16)
    ```

    This indicates that the system has recognized that Gio is not in the correct area (Offsite) to access this door. It resets his current user area to reflect the area he is actually entering now (the Office area).
11. Badge at the exit reader to leave the office. Gio passes his access card back to another employee who has forgotten their own. Badge at the exit reader again to trigger another soft antipassback violation:

    ```
    User Gio Stone (1:6) (UN8) Exit Soft Antipassback Failure At Office Door
    (DR15) Area Offsite (AR19) User Area Reset To Offsite (AR19)
    ```

## Combined Testing

Because the system tracks which area the user is currently in, the user's antipassback status can be kept consistent across multiple doors.

1. Badge at the entry reader for the Server Room Door.
2. This time, Gio tailgates another employee to exit the server room and leave work. Badge at the exit reader for the Office Door.

   This triggers another soft passback violation, because the system is expecting Gio to still be in the server room:

   ```
   User Gio Stone (1:6) (UN8) Exit Soft Antipassback Failure At Office Door
   (DR15) Area Offsite (AR19) User Area Reset To Offsite (AR19)
   ```
3. The next day, Gio forgets to badge in at the Office Door when he enters the building and attempts to enter the Server Room. Badge at the Server Room Door entry reader.

   This triggers a hard antipassback violation, because Gio is still expected to be in the Offsite area.

   ```
   User Gio Stone (1:6) (UN8) Entry Antipassback Failure At Door Server Room
   Door (DR16) Area Offsite (AR19) Required Area Office (AR16)
   ```
4. In this situation, Gio cannot enter the Server Room at all because he has not followed the correct sequence for entry. There are two options to correct his current area:
   - Gio can badge out of the Office area, then badge in again. Now he has correctly entered the Office area and will be allowed into the Server Room.
   - Gio can ask a manager or security guard to reset his antipassback status. In Protege GX, right click on the antipassback failure event and select **Reset user antipassback**. This sets Gio's current area to 'Unknown', allowing him to enter the Server Room.

# Additional Programming

There are a number of optional antipassback settings available in Protege GX to customize each door for the customer's requirements.

## Resetting Antipassback Status

As we saw in the example above, it is convenient to have a method of resetting the antipassback status of a particular user, or for all users who have used a certain door. Resetting the antipassback status sets the user's current area back to 'Unknown', which allows them to access any door.

There are two methods for manually resetting the antipassback status of a single user. These are useful for remotely freeing a user when they have been 'trapped' by an antipassback violation.

- Right click on the hard or soft antipassback failure event on a status page or floor plan and click **Reset user antipassback**.
- Right click on the user record and click **Reset antipassback**.

It is also possible to automatically reset the antipassback status for all users who have used a particular door. The following options are available in **Programming | Doors | Advanced options**:

- **Reset antipassback status on schedule**: To reset antipassback on a schedule, enable this option and set the **Antipassback reset schedule** below.

  Whenever the reset schedule becomes valid, the system resets the antipassback status of all users who have accessed that door since the last reset.

  For example, you could configure the schedule to become valid for 1 minute every night at midnight or once a week. Alternatively, you could validate the schedule using an output, so that all users' antipassback status can be reset by turning the output on.
- **Enable timed user antipassback reset**: To reset antipassback status on a timer, enable this option and set the **Antipassback entry/exit user reset time** above.

  When this option is enabled, after each reset period the system automatically resets the antipassback status of all users who have passed through the door. For example, if the **Antipassback entry user reset time** is set to 20 minutes, every 20 minutes the system resets the status of all users who have entered the door during that time.

  This option can be useful in situations where the door does not have card readers on both sides (for example, in a carpark with a REX sensor). After a user enters the carpark, their antipassback status will be reset within the next 2 hours. This discourages users from passing their cards back to unauthorized people, but allows them to leave the carpark using REX and re-enter the next day.

### Scenario: Resetting Status by Schedule

The management at Silph have decided to reset the antipassback status for all users around midnight on Sunday. We can use a reset schedule to achieve this.

1. Navigate to **Sites | Schedules** and add a new schedule with the name APB Reset (Sunday Midnight).
2. In **Period 1**, enable **Sun**.
3. Set the **Start time** to 11:59 pm and the **End time** to 12:00 am.
4. Click **Save**.
5. Navigate to **Programming | Doors**.
6. Use **Ctrl + Click** to multi-select the Office Door and Server Room Door.
7. In the **Advanced options** tab, enable **Reset antipassback status on schedule**.
8. Set the **Antipassback reset schedule** to APB Reset (Sunday Midnight).

9. Click **Save**.
10. Wait for the change to be downloaded to the controller, then badge Gio Stone's card at the entry reader for the Server Room Door.
11. Badge at the entry reader again. Access should be denied by hard antipassback.
12. Navigate to **Sites | Controllers**.
13. Right click on the relevant controller and enter a date of 11:58:55 pm, next Sunday. Click **Set controller date time**.
14. After 5 seconds you will see the APB Reset (Sunday Midnight) schedule become valid.
15. Badge Gio's card at the entry reader again. He will be allowed access because his antipassback status has been reset.

# Overriding Antipassback for Specific Users

Some users, such as managers and security personnel, should not be prevented from moving around the building. There are a few ways to disable antipassback restrictions for these users:

- **Super user rights**: The simplest method to disable antipassback for an individual user is to enable the **User has super rights and can override antipassback** option in **Users | Users | Options**. When this option is enabled the user will never be affected by antipassback violations.

  **Note**: Enabling this option will also allow the user to override door lockdowns and dual authentication requirements for doors and areas.

- **Access level door type**: If you have multiple users who need antipassback disabled at specific doors, it may be useful to set up access level door types. This has two requirements:
  - The **Use access level door type** setting must be enabled in the access level (**Users | Access levels | General**).
  - Every programmed door type must have an **Access level door type** programmed (**Programming | Door types | General**).

  You could enable **Use access level door type** for the Security Guard access level. Then for each door type you would set an **Access level door type** with lower restrictions, such as replacing a Card (Hard Passback) door type with Card Only. This would make it easier for the security guards to move around the building, without being blocked by antipassback settings.

## Scenario: Manager and Technicians

In our Silph office scenario, the manager wants super user rights so that she can move around the office freely and open locked down doors. In addition, the security system technicians need to bypass antipassback restrictions when they are installing and servicing the system, but should not have super user rights.

### Programming the Manager

We will program a manager user record with super user rights.

1. Navigate to **Users | Users**.
2. Add a new user record with the name Maxine Blaise.
3. Assign the user an access card.
4. In the **Access levels** tab, assign the All Silph Doors access level.
5. In the **Options** tab, enable **User has super rights and can override antipassback**.
6. Click **Save**.

7. To test the programming, badge Maxine's card at the Server Room Door entry reader. Wait for the door to relock, then badge again. Access should be granted both times, indicating that Maxine can bypass hard antipassback.
8. Repeat this test at the Office Door. There should be no event to indicate that Maxine has committed a soft antipassback violation.

### Programming the Technicians

The technicians will use access level door types to bypass antipassback restrictions.

1. To use access level door types, it is important that every door type used on site has a corresponding access level door type. Navigate to **Programming | Door types**.
2. Use Shift + Click to select both Server Room (Hard APB) and Office Door (Soft APB).
3. Set **Access level door type** to Card.
4. Click **Save**.
5. The other two doors in this facility are currently using the basic Card door type with no antipassback settings. However, it is still necessary to assign an access level door type.

   Select the Card door type and set the **Access level door type** to Card (the same record). Click **Save**.
6. Now we can create an access level that uses these alternative door types. Navigate to **Users | Access levels**.
7. Add a new access level. Click the **Copy** icon in the toolbar, select All Silph Doors and click **Ok**.
8. Change the name to All Silph Doors (APB Disabled).
9. Enable **Use access level door type**.
10. Click **Save**.
11. Navigate to **Users | Users**.
12. Add a new user record with the name Archie Drake.
13. Assign the user an access card.
14. In the **Access levels** tab, assign All Silph Doors (APB Disabled).
15. Click **Save**.
16. To test the programming, badge Archie's card at the Server Room Door entry reader. Wait for the door to relock, then badge again. Access should be granted both times, because the door is not using hard antipassback settings for Archie.
17. Repeat this test at the Office Door. There should be no event to indicate that Archie has committed a soft antipassback violation.

# Qualifying Antipassback

Sometimes a user may badge their card at a door, but not open the door and move through it. This can cause antipassback violations the next time the user badges their card, even though they are not acting maliciously.

To alleviate this problem, you can enable the **Entry/Exit passback is qualified with door opening** settings in the door type. With this option enabled, when a user gains access to the door but does not open it, the system does not update their current area.

## Scenario: Qualifying Antipassback

To prevent employees from being denied access unnecessarily, Silph has asked for antipassback on the Server Room Door to only activate when the door is opened.

1. Navigate to **Programming | Door types** and select Server Room (Hard APB).
2. Enable **Entry passback is qualified with door opening**.

3. Enable **Exit passback is qualified with door opening**.
4. Click **Save**.
5. To test the programming, badge Gio Stone's card at the entry reader for the Server Room Door. Do not open the door sense input.
6. Wait for the door to relock, then badge the card again. Access is granted again. The system has not updated Gio's current area since he did not enter the Server Room.
7. This time, open and close the door sense input to simulate Gio opening the door.
8. Badge at the entry reader a third time. This time, access is denied due to hard antipassback violation. Because Gio opened the door, the system updated his current area to the Server Room.

# Updating User Areas without Antipassback

By default, only doors which have antipassback enabled will update the user's current area in the system. This typically does not matter if the area the user is entering is not adjacent to any antipassback-controlled doors. However, in some cases this can lead to the user's current area becoming desynchronized from the area they are physically present in.

To alleviate this issue, enable **Update user area when passback disabled** (**Programming | Doors | Advanced options**) on any doors which are not using antipassback. This can also be used when a door has antipassback enabled in one direction but not the other. With this option enabled, the door will update the user's current area when they gain access, even when antipassback is disabled.

## Scenario: Updating User Area at the Side Door

In the Silph building there is an additional side door in the break room which only allows exit from the building (see page 7). It is not the normal exit but occasionally employees do leave through that door. Silph would like this door to update users' antipassback status so that they are not penalized when they exit this way.

The building also has a break room door which does not track users' antipassback status. However, this door does not need to update the user's area, because the Break Room area is not connected directly to any antipassback-controlled doors. When users enter the Break Room, it is acceptable to consider them still in the Office area.

1. Before implementing the programming, we will observe the default operation. Badge Gio Stone's card at the exit reader for the Side Door to simulate him leaving the facility.
2. Badge Gio's card at the entry reader for the Office Door as he enters the building again. The event log will indicate that there is a soft antipassback failure even though Gio exited the building correctly.
3. Navigate to **Programming | Doors** and select the Side Door.
4. In the **Advanced options** tab, enable **Update user area when passback disabled**.
5. Click **Save**.
6. To test the programming, badge Gio Stone's card at the Side Door exit reader.
7. Badge Gio's card again at the Office Door entry reader. This time there is no antipassback violation, because the Side Door updated his current area to Offsite.

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.