AN-272

Allegion Integration with Protege WX

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 2003-2025. All rights reserved.

Last Published: 27-May-25 2:13 PM

Contents

Introduction ____ 4
Prerequisites 4
Supported Functionality ____ 5
Supported Hardware Components 5
Supported Capacity 5
Door Functionality 5
Supported Allegion Functionality 6
Allegion Hardware Installation ____ 10
Wiring an Allegion AD300/301 Lock 10
Wiring an Allegion PIM 10
Wiring an Allegion GWE 12
Protege WX Setup ____ 14
Configuring the Controller's Onboard Reader Expander 14
Programming Allegion PIMs and GWEs 14
Programming Allegion AD300/301 Locks 14
Adding an Allegion Wireless Lock as a Smart Reader 15
Adding an Allegion AD300/301 Lock as a Smart Reader 15
Trouble Inputs 16
Adding Trouble Inputs 16
Configuring Privacy Mode 18
Configuring Toggle Mode 18
Configuring Apartment Mode 18
Door Commands 19
Allegion Configuration ____ 20
Manual Door Commands on PIMs 20
Locks with Keypads 20
ENGAGE Series Lock Functions 20
Known Limitations ____ 21

Introduction

Allegion integration is a licensed feature that allows you to utilize Allegion locks within Protege WX.

Users and access control are configured within Protege WX, while the Allegion locks act as credential readers as well as locking devices. Lock control is programmed through the Protege WX door control functionality.

The Allegion integration enables Protege WX to communicate with the locks, either directly through the controller reader ports or via Allegion interface devices connected to the controller.

- Allegion AD300 Series locks are hardwired directly to the controller reader ports
- Allegion AD400 Series wireless locks interface with the controller via Panel Interface Modules (PIMs)
- Allegion ENGAGE Series wireless locks interface with the controller via ENGAGE Gateways (GWEs)

The following instructions outline essential Allegion lock integration configuration. This includes the wiring of an Allegion lock, PIM or GWE to a Protege WX controller, the setup of an Allegion PIM or GWE within Protege WX, and the programming of Allegion locks within Protege WX.

For information on Allegion lock configuration we recommend you consult the relevant Allegion documentation.

Prerequisites

Controller Requirements

Controller	Firmware Version for AD Series	Firmware Version for ENGAGE Series
Protege WX Controller	4.0.255 or higher	4.00.782 or higher

Only controllers with RS-485 functionality on the reader ports support this integration.

Important:

Connection via RS-485 is only supported with hardware revisions of controllers that are equipped with the added RS-485 reader functionality on the reader ports. This is easily determined by checking the reader ports on the front panel of the controller. Hardware revisions that are equipped with RS-485 reader functionality have the NA and NB labels beneath the D0 and D1 labels, as shown below.

Earlier revisions of the controller hardware that do not have the NA and NB labels (as in the example below) do not have the added RS-485 reader functionality.

All one door controllers come equipped with RS-485 reader functionality.

Protege WX Licensing Requirements

License	Order Code	Notes
Allegion Door License	PRT-WX-LIC-ALEG-1	1 license per Allegion lock connected to the Protege system.

Supported Functionality

This section outlines the supported hardware, capacity and features in this integration.

Supported Hardware Components

ICT has only validated this integration with the Allegion hardware and versions listed below. It may be possible to use other Allegion models and firmware, but ICT cannot directly support them without a sample being supplied for testing.

Allegion AD Series Locks

Device	Model	Firmware Version
Hardwired lock	AD300/301	N/A
Wireless lock	AD400/401	N/A
Panel Interface Module	PIM400-485	N/A
Handheld Device with Schlage Utility Software	BM170 R2	6.6.3

Allegion ENGAGE Series Wireless Locks

Device	Model	Firmware Version
Wireless lock	LE Networked Wireless Lock	3.8.6
	NDE Networked Wireless Lock	3.8.6
Gateway	ENGAGE Gateway	1.60.8

Supported Capacity

AD300 Series Hardwired Locks

- Maximum number of AD300 locks supported: 64
- Maximum number of AD300 locks supported per reader port: 32

AD400 Series Wireless Locks

- Maximum number of AD400 locks supported: 128
- Maximum number of AD400 locks supported per PIM400-485: 16
- Maximum number of PIM400-485 panel interface modules supported: 64
- Maximum number of PIM400-485 panel interface modules supported per reader port: 32

ENGAGE Series Wireless Locks

- Maximum number of LE/NDE locks supported: 128
- Maximum number of LE/NDE locks supported per ENGAGE gateway: 10
- Maximum number of ENGAGE gateways supported: 64
- Maximum number of ENGAGE gateways supported per reader port: 32

Door Functionality

The Allegion locks perform the reading and locking part of the integration, while Protege programming defines access control. The following Protege functionality is supported:

- Users, access levels and credential matching (card and/or PIN, custom credential types, custom formats)
- Granting or denying access based on doors, door groups and schedules
- Unlock on schedule, by area and by calendar action
- Holiday groups for schedules
- Pre-alarm, left open, forced open alerts
- Manual door commands (lock, unlock and lockdown commands)

Any programming features not explicitly listed here may not be supported by this integration. It is the installer's responsibility to validate that features work as expected before implementation.

Supported Allegion Functionality

The following Allegion features and functionality are supported by this integration.

Remote Lock / Unlock and Remote Lockdown

This functionality is supported via Protege manual door commands.

Because the REX function is mechanical, Allegion locks always allow exit even when the door is locked down. Super users can access locked down doors as normal.

Deadbolt

Users can manually actuate the deadbolt on Allegion locks. In most operating modes, when someone unlocks the door with a credential and presses down on the handle, the deadbolt will retract. The deadbolt can also be retracted using a key.

If the lock is using apartment mode or has privacy mode active, when the deadbolt is extended the lock will deny access requests from outside the door.

Inside Handle REX

Because REX is controlled mechanically rather than electronically it is always allowed for Allegion locks, including when in lockdown.

When the inside handle of an Allegion lock is turned, an **Unlocked by REX** event will be generated for that door.

Lock Schedules and Holidays

When a door unlock schedule becomes valid:

- The lock allows free access without a credential
- A **Door Unlocked By Schedule** event will be generated
- The door status will change to **Unlocked by Schedule - Closed**

When the door unlock schedule becomes invalid:

- The lock requires a credential for access
- A **Door Locked By Schedule** event will be generated
- The door status will change to **Locked - Closed**

Apartment Mode

When the lock is in apartment mode, the door can be toggled between locked and unlocked states by pressing the inside push button, actuating the deadbolt, or badging a card while the door is closed. Using the inside handle and opening the door will cause it to latch unlock. Extending the deadbolt will cause the lock to deny entry until the deadbolt is unlocked with a key.

Office Mode

The office mode lock function is **not** supported by this integration. Please ensure that this function is not selected during lock commissioning as it will result in unexpected behavior.

Privacy Mode

When this feature is enabled, a user can press the interior push button (IPB) to activate privacy mode. In this mode the door will deny all access from the outside except for users with super rights. Privacy mode is deactivated by pressing the IPB again or opening the door with the inside handle.

Privacy mode is enabled by default, but can be disabled when programming the locks in Protege.

Storeroom Mode

In storeroom mode, the door can be locked or latch unlocked by presenting a valid credential.

- When a user is granted access the door status will change to **Unlocked by User Latched - Closed**. The door can now be opened without a credential.
- When a user is next granted access the door status will change to **Locked - Closed**

Door Left Open

When a door with an Allegion lock is left open:

- A **Door Pre-Alarm** event will be generated after the configured pre-alarm delay time
- The door status will change to **Not Locked - Open Alert**
- A **Door Left Open** event will be generated after the configured left open alarm time expires
- The **Door Left Open** trouble input status will change to open

When the door is closed the corresponding events will be generated and statuses updated accordingly.

Door Forced Open

When a door with an Allegion lock is forced open:

- There is a delay of 4 seconds. This ensures that the forced door is not a false alarm.
- A **Door Forced Open** event will be generated
- The door status will change to **Not Locked - Forced Open**
- The **Door Forced Open** trouble input status will change to open

When the door is closed the corresponding events will be generated and statuses updated accordingly.

Interior Cover Tamper - Lock Enclosure

When an Allegion lock enclosure is opened:

- A **Reader Unit Tamper Alarm** event will be generated
- The associated door's **Reader Tamper** trouble input status will change to open

When the enclosure is closed the events and status will be updated accordingly.

Interior Cover Tamper - PIM/GWE Enclosure

When an Allegion PIM or GWE enclosure is opened:

- A **Reader Unit Tamper Alarm** event will be generated
- The **Reader Tamper** trouble input of the **first lock** associated with the PIM/GWE will change to open. This is the lock with the lowest **Configured Address**.

When the enclosure is closed the events and status will be updated accordingly.

Gateway BLE Tamper

When somebody connects to an Allegion GWE Gateway using the ENGAGE app:

- A **Reader Unit Tamper Alarm** event will be generated
- The **Reader Tamper** trouble input of the **first lock** associated with the PIM/GWE will change to open. This is the lock with the lowest **Configured Address**.

Upon disconnection, the events and status will be updated accordingly.

Communication Loss

When an Allegion ENGAGE Series lock loses communication with the GWE:

- A **Reader Unit RF Loss Alarm** event will be generated
- The **RF Loss** trouble input status will change to open

When the lock regains communication with the GWE the events and status will be updated accordingly.

When an Allegion PIM, GWE or AD Series hardwired lock loses RS-485 connection with the reader port:

- The **Reader 1/2 Tamper / Missing** trouble input status will change to open
- An **Allegion 485 Reader Offline** event will be generated

When the device regains communication with the reader port:

- The **Reader 1/2 Tamper / Missing** trouble input status will change to closed
- An **Allegion 485 Reader Online** event will be generated

Power Loss

When an Allegion PIM or GWE loses power:

- An **Allegion 485 Reader Offline** event will be generated
- No door events will be generated (or cached) while the Allegion interface module is offline

When power is restored to the Allegion PIM or GWE:

- An **Allegion 485 Reader Online** event will be generated
- Door events will resume as normal

When the Protege controller loses power:

- No events will be generated (or cached) while the controller is offline

When power is restored to the Protege controller:

- An **Allegion 485 Reader Online** event will be generated
- Door events will resume as normal

Battery Status

The Allegion lock monitors its battery status and alerts the controller when it drops below a prescribed range.

When an Allegion lock's battery drops to 4.5V:

- A **Reader Unit Battery Low Alarm** event will be generated
- The **Battery Low** trouble input status will change to open

When an Allegion lock's battery drops to 4V:

- A **Reader Unit Battery Critical Alarm** event will be generated
- The **Battery Critical** trouble input status will change to open

When an Allegion lock's battery restores to 4.5V:

- A **Reader Unit Battery Critical Restore** event will be generated
- The **Battery Critical** trouble input status will change to closed

When an Allegion lock's battery restores to 6V:

- A **Reader Unit Battery Low Restore** event will be generated
- The **Battery Low** trouble input status will change to closed

Notes on Battery Status

For AD Series locks, the default heartbeat is 10 minutes and the Allegion algorithm requires 6 reads before confirmation of battery status. As a result, it may take up to 1 hour before low/critical battery events are generated and trouble input statuses are updated.

For ENGAGE Series locks, the default heartbeat is 2 hours and the Allegion algorithm requires 6 reads before confirmation of battery status. As a result, it may take up to 12 hours before low/critical battery events are generated and trouble input statuses are updated.

This behavior is by Allegion design, to preserve battery life and maintain lock access functionality.

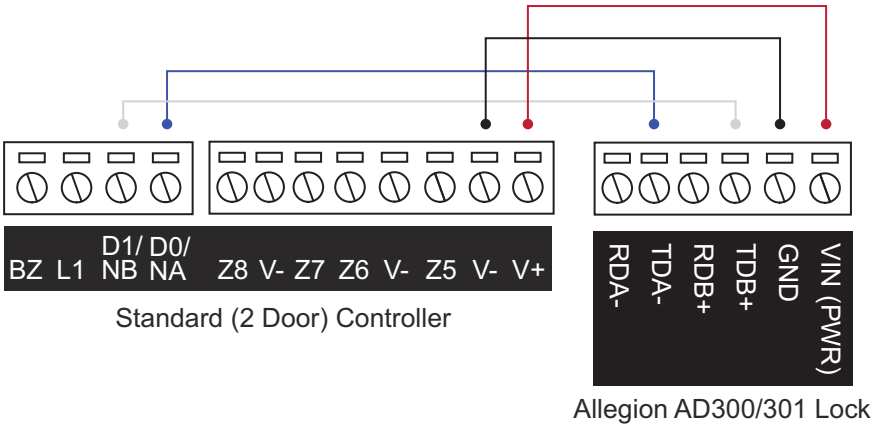
Allegion Hardware Installation

Allegion locks, PIMs and GWEs are wired to the controller's RS-485 reader ports.

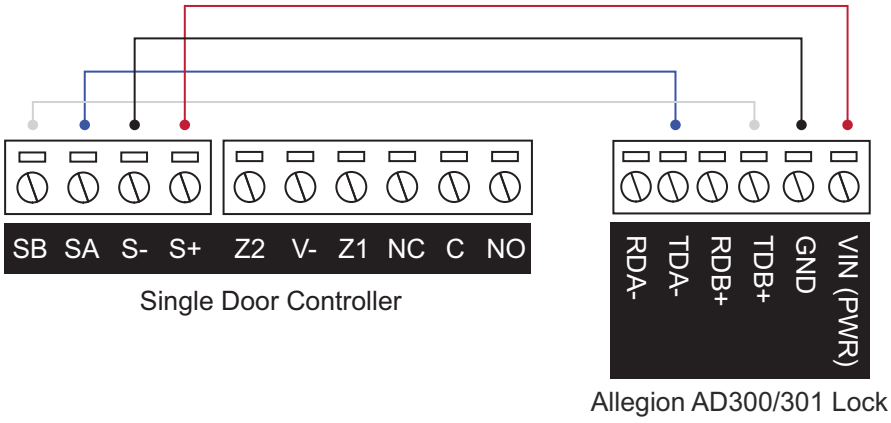
Wiring an Allegion AD300/301 Lock

Allegion AD300 Series locks are hardwired directly to the controller reader ports.

Standard (2 Door) Controller to AD300/301 Lock



Single Door Controller to AD300/301 Lock



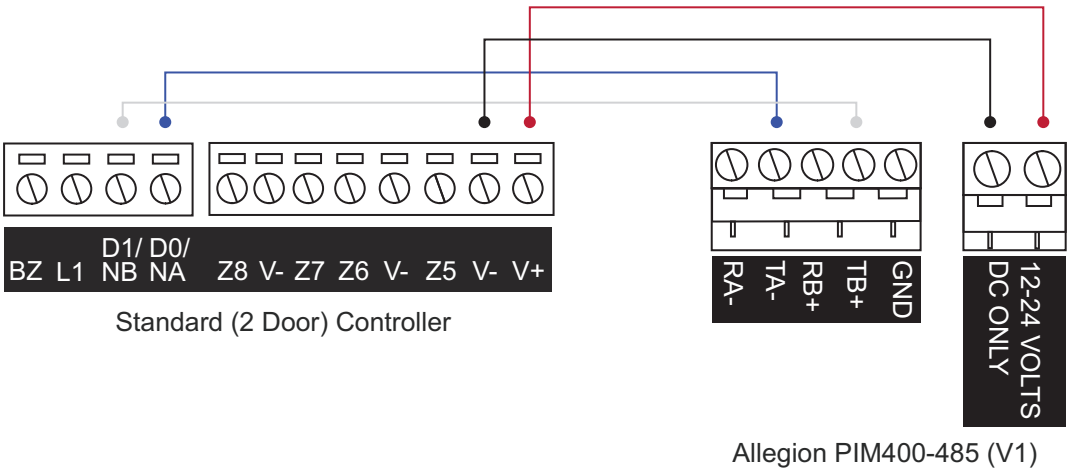
Wiring an Allegion PIM

For the Protege system to communicate with the wireless AD400 Series locks, you need to wire a PIM to the Protege controller. This integration uses an Allegion PIM400-485, which enables the configuration of up to 16 wireless locks.

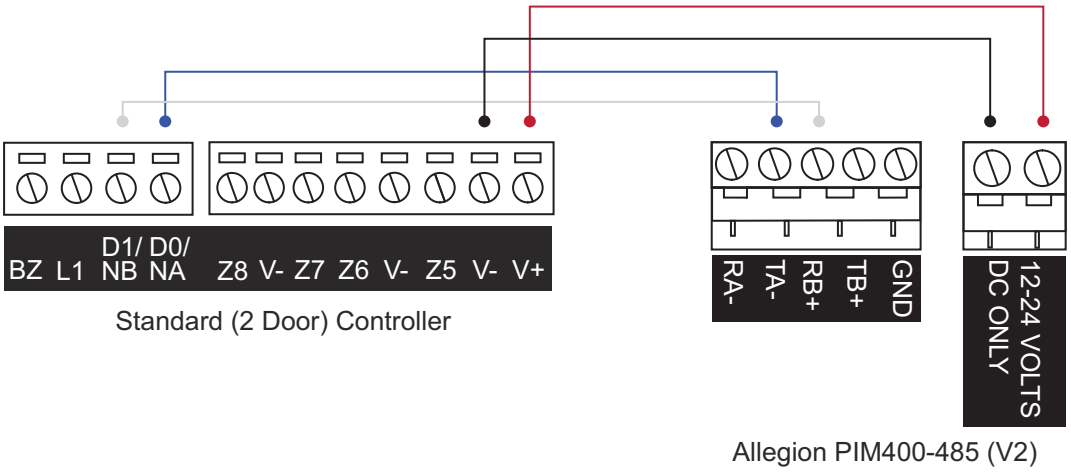
The Allegion PIM400-485 is compatible with both standard and single door Protege controllers equipped with onboard RS-485 reader ports. The controller provides the PIM with a network connection and power supply.

Wiring varies slightly depending on the version of Allegion PIM400-485 you are using:

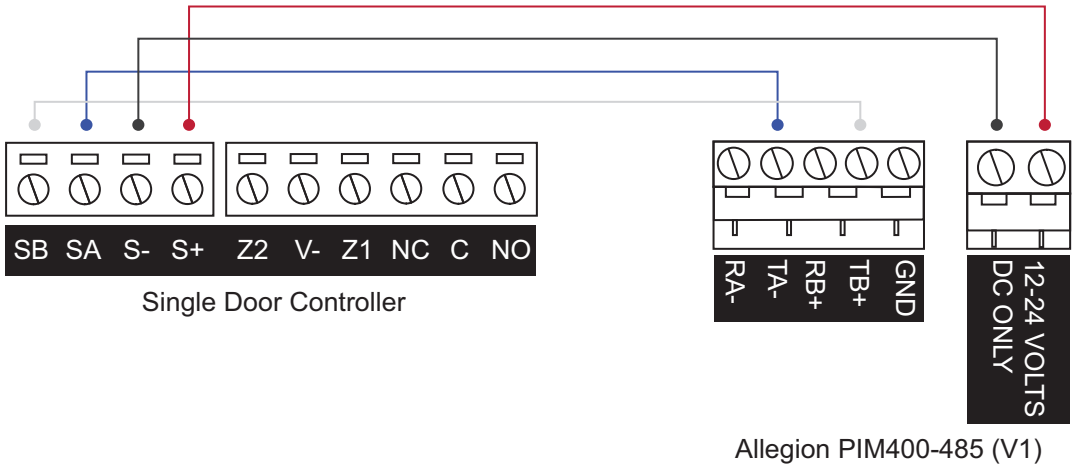
Standard (2 Door) Controller to PIM 400-485 V1: D1/NB connected to TB+



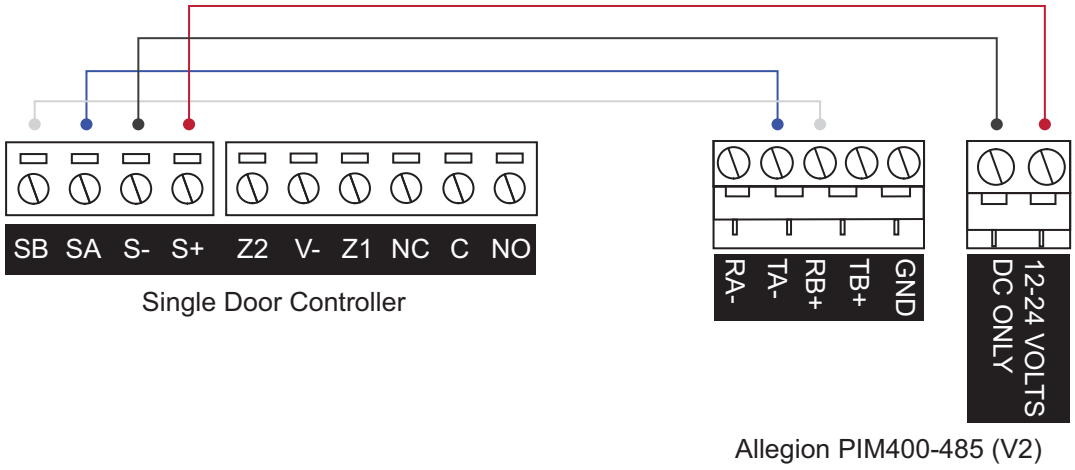
Standard (2 Door) Controller to PIM 400-485 V2: D1/NB connected to RB+



Single Door Controller to PIM 400-485 V1: SB connected to TB+



Single Door Controller to PIM 400-485 V2: SB connected to RB+

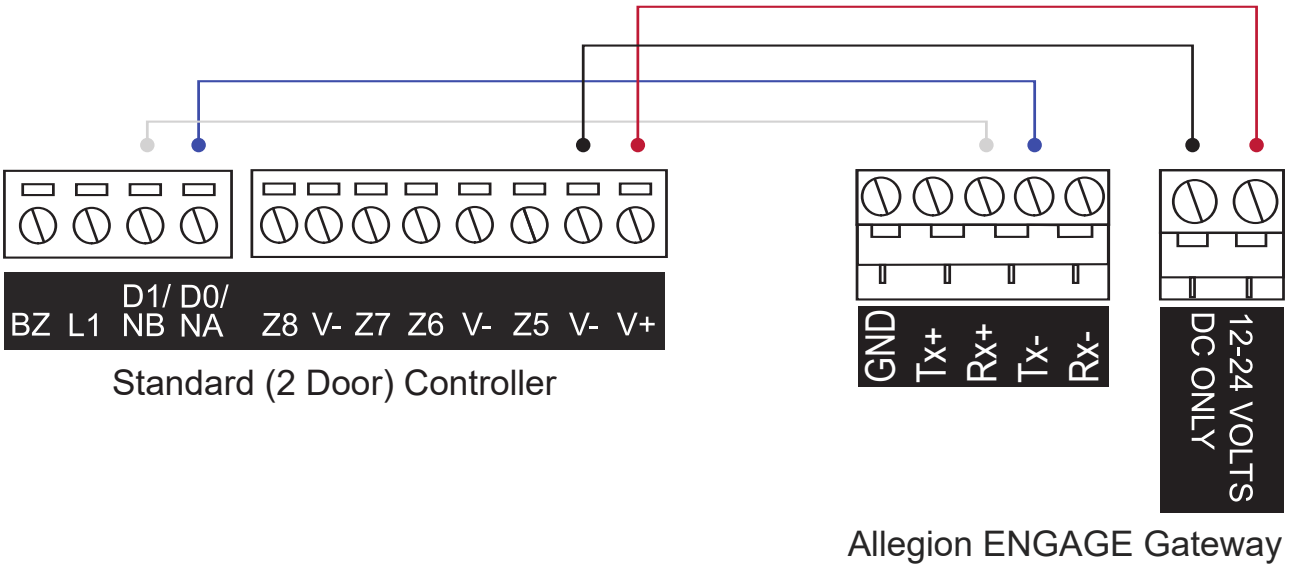


Wiring an Allegion GWE

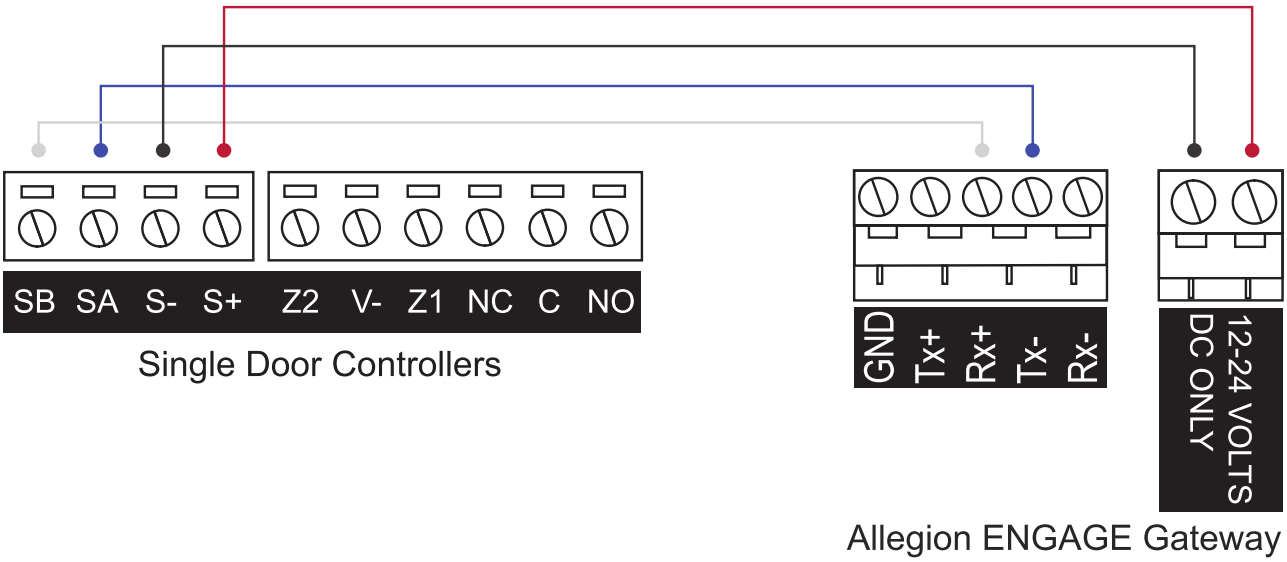
For the Protege system to communicate with the wireless LE and NDE locks, you need to wire a GWE to the Protege controller. This integration uses an Allegion ENGAGE Gateway, which enables the configuration of up to 10 wireless locks.

The Allegion ENGAGE Gateway is compatible with both standard and single door Protege controllers equipped with onboard RS-485 reader ports. The controller provides the gateway with a network connection and power supply.

Standard (2 Door) Controller to ENGAGE Gateway: D1/NB connected to Rx+



Single Door Controller to ENGAGE Gateway: SB connected to Rx+



Protege WX Setup

In order to control the locks from within Protege WX, you need to configure the controller's onboard reader expander and add the locks as smart readers.

Configuring the Controller's Onboard Reader Expander

The Allegion integration must first be enabled on the controller's onboard reader expander.

1. Navigate to **Expanders | Reader Expanders** and select the onboard reader (reader expander at address 1).
2. On the **General** tab, set the **Port 1 Network Type** and/or the **Port 2 Network Type** to Allegion.

   This needs to be configured for whichever port(s) an Allegion lock/PIM/GWE is wired to.
3. Click **Save**.

The required Allegion configuration options will not be available until this is done.

Programming Allegion PIMs and GWEs

For wireless locks, PIMs or GWEs must be configured as the communication interface between the wireless locks and the Protege WX controller.

1. Select the **Reader 1/2 PIM Config** tab.
2. Click **Add** to add a new Allegion interface module.
3. Set the **PIM Address** for the PIM/GWE connected to the reader port.
4. Set the **APM Start Address**. This defines the value set for the Low APM Range of the PIM/GWE connected to the reader port, which determines the address of the first wireless lock assigned to the device.

   Note: There cannot be any duplicate APM (lock) addresses on a single RS-485 communications bus, even across multiple PIMs/GWEs. For example, if there are two PIMs/GWEs connected, each with 16 APMs allocated, PIM 1 should have an APM Start Address of **1**, and PIM 2 should have an APM Start Address of **17**. This ensures there will be no duplication of APM addresses.
5. Set the **Number Of APMs** (wireless locks) connected to the PIM/GWE.

   A maximum of 16 locks can be connected to a PIM. A maximum of 10 locks can be connected to a GWE.
6. Click **Save.**

Protege does not allow PIMs/GWEs (RSDs) and locks (APMs) to be addressed as 0. As a result the PIM Address and APM Start Address of the Allegion PIM in Protege will both start at 1.

Programming Allegion AD300/301 Locks

Allegion AD300 Series locks are connected directly to the reader ports and are not associated with a PIM/GWE. Each hardwired lock must be represented by an individual PIM record in the **Reader 1/2 PIM Config** tab to configure the connection between the lock and the controller.

1. In the **Reader 1/2 PIM Config** tab, click **Add** to add a new PIM record to represent the lock.
2. Set the **PIM Address** for the AD300/301 lock connected to the reader port.
3. Set the **APM Start Address** to 1.
4. Set the **Number Of APMs** to 1.
5. Click **Save**.

Adding an Allegion Wireless Lock as a Smart Reader

Each Allegion lock must be configured as a Protege smart reader, to enable communication with the controller.

1. Navigate to **Expanders | Smart Readers** and click **Add**.
2. Set the **Expander Address** to that of that of the controller's onboard reader expander.
3. Select the **Expander Port** that the PIM/GWE is wired to.
4. Select the **Configured Address** of the lock.
5. Select the **Linked RSD Address**. This is the **PIM Address** of the PIM record that the lock is linked to.
6. The privacy mode feature is enabled by default. To disable it, add the following in the **Commands** field:
   `DisablePrivacyMode = true`
7. Select the **Reader** tab.
8. Set the **Reader One Format** to the required credential format:
   - If an appropriate preset format is available, select it from the dropdown.
   - If you are using a credential type (recommended method), select Custom Credential. For more information and instructions, see Application Note 218: Configuring Custom Credential Types in Protege WX.
   - If you are using a custom reader format (programmed in the controller record), select Custom Format.
9. Set the **Reader 1 Location** to Entry or Exit.
10. Set the **Reader 1 Door** to the door this Allegion lock will control.
11. Click **Save**.

Protege does not allow PIMs/GWEs (RSDs) and locks (APMs) to be addressed as 0. As a result the Linked RSD Address and Configured Address of the Allegion smart reader in Protege will both start at 1.

Adding an Allegion AD300/301 Lock as a Smart Reader

1. To configure a smart reader as an AD300 Series lock, navigate to **Expanders | Smart Readers** and click **Add**.
2. Set the **Expander Address** to that of that of the controller's onboard reader expander.
3. Select the **Expander Port** that the AD300/301 lock is wired to.
4. Select the **Configured Address** of the connected lock.
5. Set the **Linked RSD Address** to Not Set.

   As AD300 Series locks are connected directly to the reader ports, they do not have any link to a PIM.
6. The privacy mode feature is enabled by default. To disable it, add the following in the **Commands** field:
   `DisablePrivacyMode = true`
7. Select the **Reader** tab.
8. Set the **Reader One Format** to the required credential format.
   - If an appropriate preset format is available, select it from the dropdown.
   - If you are using a credential type (recommended method), select Custom Credential. For more information and instructions, see Application Note 218: Configuring Custom Credential Types in Protege WX.
   - If you are using a custom reader format (programmed in the controller record), select Custom Format.
9. Set the **Reader 1 Location** to Entry or Exit.
10. Set the **Reader 1 Door** to the door this Allegion lock will control.
11. Click **Save**.

Trouble Inputs

A number of trouble inputs are available for reporting troubles in locks and hubs. Note that some trouble conditions are grouped so that one trouble input reports on multiple conditions.

The following table details the mapping used for the integration:

Trouble Input Name	Module Input Number	Type	Lock Condition
Door Forced Open	1	Door	Lock has been forced open
Door Left Open	2	Door	Lock has been left open
Reader Tamper*	3	Door	Lock tamper PIM tamper GWE BLE tamper
Battery Low	4	Door	Lock has low battery
RF Loss	5	Door	Lock has RF loss
Battery Critical	9	Door	Lock has critical battery
Reader 1 Tamper / Missing**	12	Reader Expander	PIM/GWE/AD300 lock offline on reader port 1
Reader 2 Tamper / Missing**	13	Reader Expander	PIM/GWE/AD300 lock offline on reader port 2

*When a PIM or GWE tamper is triggered, the Reader Tamper trouble input of the first door associated with that hub will open. This is the door corresponding to the lock with the lowest **Configured Address**.

**If any wired lock or hub goes offline, the Reader 1/2 Tamper / Missing trouble input will open.

Adding Trouble Inputs

The trouble input records must be added for each door that is integrated with an Allegion lock, and for each reader port that has a PIM/GWE or AD300 lock physically connected to it.

1. Navigate to **Programming | Trouble inputs** and create six trouble inputs for each door that is integrated with an Allegion lock, with the following configuration.

Door Forced Open

- **Module type**: Door (DR)
- **Module address**: Select the relevant door record.
- **Module input**: 1
- **Trouble group**: 3 - Access
- **Trouble group options**: AC failure / Module tamper / Forced door

Door Left Open

- **Module type**: Door (DR)
- **Module address**: Select the relevant door record.
- **Module input**: 2
- **Trouble group**: 3 - Access
- **Trouble group options**: Battery / Module lost / Door left open

Reader Tamper

- **Module type**: Door (DR)
- **Module address**: Select the relevant door record.
- **Module input**: 3
- **Trouble group**: 2 - System
- **Trouble group options**: AC failure / Module tamper / Forced door

RF Loss

- **Module type**: Door (DR)
- **Module address**: Select the relevant door record.
- **Module input**: 5
- **Trouble group**: 2 - System
- **Trouble group options**: Battery / Module lost / Door left open

Battery Low

- **Module type**: Door (DR)
- **Module address**: Select the relevant door record.
- **Module input**: 4
- **Trouble group**: 3 - Access
- **Trouble group options**: Battery / Module lost / Door left open

Battery Critical

- **Module type**: Door (DR)
- **Module address**: Select the relevant door record.
- **Module input**: 9
- **Trouble group**: 3 - Access
- **Trouble group options**: Battery / Module lost / Door left open

2. Create a trouble input for each reader port that has a PIM/GWE or AD300 lock physically connected to it, with the following configurations.

Reader 1 Tamper / Missing

- **Module type**: Reader (RD)
- **Module address**: Select the **Physical address** of the reader expander that has an Allegion PIM/GWE or AD300 lock physically connected to port 1.
- **Module input**: 12
- **Trouble group**: 2 - System
- **Trouble group options**: Battery / Module lost / Door left open

Reader 2 Tamper / Missing

- **Module type**: Reader (RD)
- **Module address**: Select the **Physical address** of the reader expander that has an Allegion PIM/GWE or AD300 lock physically connected to port 2.
- **Module input**: 13
- **Trouble group**: 2 - System
- **Trouble group options**: Battery / Module lost / Door left open

Configuring Privacy Mode

When this feature is enabled, a user can press the interior push button (IPB) to activate privacy mode. In this mode the door will deny all access from the outside except for users with super rights. Privacy mode is deactivated by pressing the IPB again or opening the door with the inside handle.

When a user is denied access by privacy mode, the system will generate a 'Schedule Not Valid' event.

Privacy mode is enabled by default, but can be disabled when programming the locks in Protege. To disable privacy mode, add the following command in the smart reader programming (**Expanders | Smart readers | General**):

```
DisablePrivacyMode = true
```

Super users can access doors in privacy mode and locked down doors. To enable super user rights:

1. Navigate to **Users | Users** and select the relevant user record.
2. In the **Options** tab, enable the **User has super rights and can override antipassback** option.
3. Click **Save**.

Configuring Toggle Mode

Toggle mode allows an Allegion lock to be toggled between locked and latch unlocked by simply badging at the reader. Storeroom mode must be enabled during lock commissioning.

Toggle mode needs to be enabled in the door programming, and access must be granted for the toggle to occur, so the user's access level must provide them access to the relevant door(s). This ensures that unauthorized access attempts cannot lock or unlock a door, and locks cannot be toggled outside valid schedules.

1. To program toggle mode, navigate to **Programming | Doors** and select the relevant door record(s).
2. In the **Outputs** tab, under the **Lock output** section, set the **Lock activation time** to 0.
3. Click **Save**.
4. Ensure that access to these doors is only available to select users at the required times.

While the door is latch unlocked, you can enable or disable door open/closed events using the **Enable open/close events on schedule** setting in **Programming | Doors | Options**.

Configuring Apartment Mode

Apartment mode is available in Protege WX version 4.00.1646 or higher.

When the lock is in apartment mode, users can toggle the door between locked and unlocked states by pressing the interior push button, actuating the deadbolt, or badging a card while the door is closed. Using the inside handle and opening the door will cause it to latch unlock. Extending the deadbolt will cause the lock to deny entry until the deadbolt is unlocked with a key.

To enable apartment mode:

1. To enable apartment mode, you must first enable toggle mode. In **Programming | Doors | Outputs**, set the **Lock Activation Time** to 0 for each Allegion lock.
2. Enter one of the commands from the table below, depending on how many locks you need to enable apartment mode for.

Locks Affected	Location	Command
One lock	**Expanders | Smart Readers | General | Commands**	`ApartmentMode = true`
All locks on a reader port	**Expanders | Reader Expanders | General | Commands**	`Port1ApartmentMode = true` `Port2ApartmentMode = true`
All locks in the system	**System | Settings | General | Commands**	`ApartmentMode = true`

An event will be generated whenever the door is unlocked or locked in apartment mode. While the door is latch unlocked, you can enable or disable door open/closed events using the **Enable Open/Close Events On Schedule** setting in **Programming | Doors | Options**.

Door Commands

The integration supports sending Protege WX manual door commands to Allegion locks to provide remote control of Allegion lock functions.

In **Monitoring | Doors**, click on the **Controls** button beside the door record and select the required command.

Door Control

These commands allow you to remotely control basic lock functionality. The available commands are:

- **Lock**
- **Unlock** (momentarily activate the lock)
- **Unlock Latched** (activate the lock and keep the door unlocked)

Door Lockdown

These commands allow you to remotely lock down individual doors. Any lockdown command will lock the door regardless of any other function causing it to be unlocked.

The available commands are:

- **Allow Entry**
- **Allow Exit**
- **Allow Entry and Exit**
- **Deny Entry and Exit**
- **Clear** (remove the lockdown from the door)

Because the REX function is mechanical, Allegion locks always allow exit even when the door is locked down. Super users can access locked down doors as normal.

Allegion Configuration

Some features require specific configuration when commissioning Allegion locks and hubs.

Manual Door Commands on PIMs

For manual door commands (including door lockdown commands) within Protege to work with the Allegion AD400 Series wireless locks, the Allegion PIMs must have a programmed **Wake Time** of 10 seconds.

This is set via the PIM's **Device Properties** using the Schlage Utility software on the provided handheld device.

The Allegion ENGAGE Gateways have this functionality enabled by default, and no additional programming is required for manual door commands within Protege to work with the Allegion LE/NDE wireless locks.

Locks with Keypads

For Allegion AD Series locks with keypads to work correctly within Protege, the locks must be programmed with specific keypad settings. These are set via the lock's **Device Properties** in the Schlage Utility software on the provided handheld device.

The settings required are different depending on the firmware version of your controller.

Controller Firmware Version	Required Settings
Protege GX: 2.08.1319 and higher Protege WX: 4.00.1269 and higher	• **Output Type**: Wiegand • **Keys Buffered**: 1 • **Output Format**: 1
Protege GX: Prior to 2.08.1319 Protege WX: Prior to 4.00.1269	• **Output Type**: Wiegand • **Keys Buffered**: 8 • **Output Format**: 9

Ensure that you update the lock settings when you upgrade the controller's firmware so that keypads continue to function.

ENGAGE Series Lock Functions

The operating mode of LE/NDE locks is defined via the ENGAGE app during lock commissioning, by selecting the desired **lock function**:

- Apartment
- Office (this function is **not** supported)
- Privacy
- Storeroom

A mode cannot be activated at the lock unless the corresponding lock function has been selected in the lock configuration. For more information, refer to the Allegion ENGAGE Series documentation.

The **Office** lock function is not supported by this integration. Please ensure that this function is not selected during lock commissioning as it will result in unexpected behavior.

Known Limitations

The following functional limitations are known to exist in the Allegion integration.

Reader 1/2 Tamper / Missing Trouble Input Recovery

Prior to Protege WX version 4.00.1646, when an Allegion PIM, GWE or AD Series hardwired lock loses RS-485 communication, and the connected reader expander's Reader 1/2 Tamper / Missing trouble input activates, after communication is restored the trouble input remains open and does not recover as expected.

To manually reset the trouble input, power cycle the associated controller.

REX Event during Door Lockdown

Because REX is controlled mechanically rather than electronically it is always allowed for Allegion locks, including when in lockdown. When a door with an Allegion lock is put into a lockdown mode which denies exit and you pull the inside handle, a 'REX Denied By Door Lockdown' event will be generated, even though REX is allowed.

Access Denied by Access Level Schedule Event

In versions prior to 4.00.1111, when a user is denied access due to an invalid schedule the event that is generated does not include the word 'Denied'. This is corrected in version 4.00.1111 and above.

Door Forced Delay

Allegion locks may register unexpected door forced alarms when they are opened by REX. This is because the controller often receives the "door opened" message from the lock before it receives the "request to exit" message. To resolve this issue, in Protege WX version 4.00.1520 a door forced delay of 4 seconds has been added to every Allegion door. This allows time for the controller to receive a REX message before activating the door forced alarm.

If you need to override this delay, enter the following command in the door programming:

```
DoorForcedStateDelay = #
```

Where **#** is the delay time in seconds.

Privacy Mode

Prior to Protege WX version 4.00.1646, whenever the controller is powered on privacy mode is automatically deactivated for all Allegion locks. Upgrading the controller firmware will resolve this issue for controllers with USB ports. However, due to hardware limitations this issue will still occur on older controllers without USB ports.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2025. 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.