Schneider Electric

Allegion Integration with Security Expert

Application Note

AN-182
June 2021

Legal Information

Contents

Introduction

Allegion integration is a licensed feature that enables you to utilize the Allegion AD-Series of wireless locks within Security Expert.

The Allegion integration uses wireless technology that enables Security Expert to communicate with the locks, either directly through the controller or via panel interface modules (PIMs) connected to the controller.

A Security Expert smart reader is configured to represent each Allegion lock and provide the programming required for the lock to communicate with the controller.

The following instructions outline basic Allegion wireless lock integration configuration. This includes the wiring of an Allegion PIM to a Security Expert controller, the setup of an Allegion PIM within Security Expert, and the programming of Allegion locks within Security Expert.

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

Prerequisites

Security Expert Allegion integration has been tested and verified with the following versions:

- An operational Security Expert system with software version 4.0.128 or higher.
- Security Expert controller firmware version 2.08.582 or higher.
- One Security Expert Allegion Door license (Ordering code: SX-DOR-ALG) is required for each Allegion wired or wireless lock connected in this integration.

Supported Capacity

- Maximum number of PIM400-485 supported: 64
- Maximum number of PIM400-485 supported per reader port: 32
- Maximum number of AD400 locks supported: 128
- Maximum number of AD400 locks supported per PIM400-485: 16
- Maximum number of AD300 locks supported: 64
- Maximum number of AD300 locks supported per reader port: 32

Allegion Hardware Installation

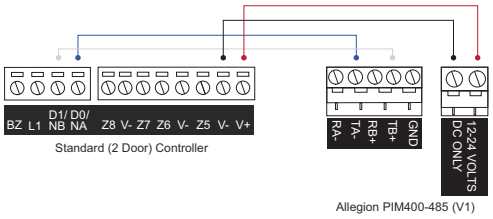
Wiring an Allegion PIM to a Security Expert Controller

In order for the Security Expert system to be able to communicate with the wireless locks, you need to wire a PIM to the Security Expert controller. This integration uses an Allegion PIM400-485 which enables the configuration of up to 16 wireless locks.

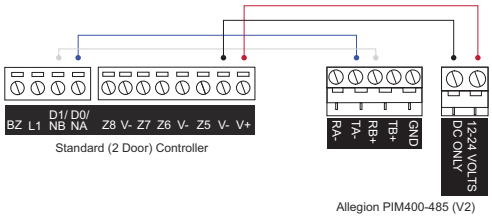
The Allegion PIM400-485 is compatible with both the standard and single door Security Expert controller as they are both equipped with onboard RS-485 enabled reader ports. The onboard reader ports of these controllers are capable of providing a PIM with a network connection and a power supply.

Wiring varies slightly according to the type of controller and the version of Allegion PIM400-485 you are using:

Standard (2 Door) Controller:

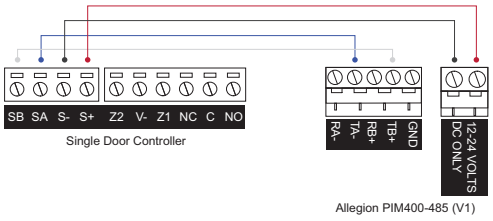


If using a PIM400-485 V1, D1/NB should be connected to TB+

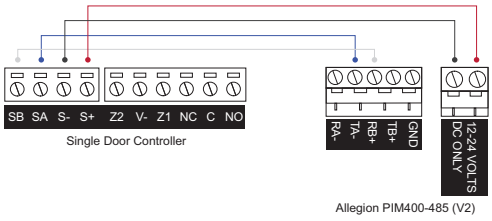


If using a PIM400-485 V2, D1/NB should be connected to RB+

Single Door Controller:



If using a PIM400-485 V1, SB should be connected to TB+

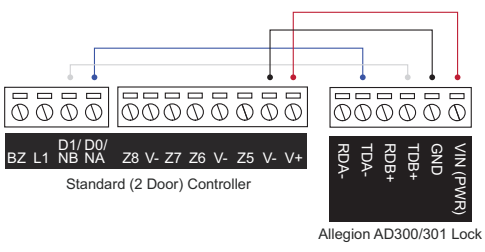


If using a PIM400-485 V2, SB should be connected to RB+

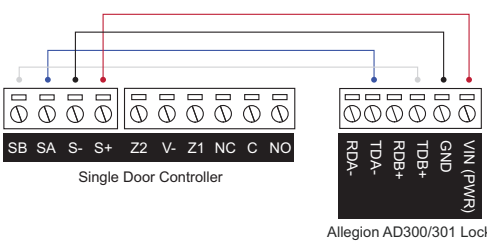
Wiring an Allegion AD300/301 Lock to a Security Expert Controller

Wiring varies slightly according to the type of controller you are using:

Standard (2 Door) Controller:



Single Door Controller:



Security Expert Setup

In order to control the locks from within Security Expert, you need to configure the controller's onboard reader expander to communicate with a PIM, and add the locks as smart readers.

Configuring the Controller's Onboard Reader Port

1. If the controller is not currently registered as a reader expander:
   - Create a new reader expander record for that controller, with a unique **Module Address**, in **Expanders | Reader Expanders**.
   - Then navigate to **Sites | Controllers | Configuration** and set the **Register as Reader Expander** field to the **Module Address** of the reader expander you created above.
2. Navigate to **Expanders | Reader Expanders** and select the reader expander registered by the controller.
3. On the **General** tab, set either the **Port 1 Network Type** or the **Port 2 Network Type** (depending on which port the PIM is wired to) to Allegion AD Series.
4. Click **Save**.

Programming the Allegion PIM

1. Select the **Reader 1/2 Pims** tab. Click **Add** to add a new PIM to the field.
2. Set the **PIM Address** for the PIM connected to the reader port.
3. Set the **APM Start Address**. This defines the value set for the *Low APM Range* of the PIM connected to the reader port.

   Note: There cannot be any duplicate APM addresses on a single RS-485 communications bus, even across multiple PIMs. For example, if there are two PIMs connected, each with 16 APMs allocated to it, 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. .
4. Set the **Number Of APMs** (wireless locks) connected to the PIM.

   A maximum of 16 locks can be connected to a PIM.
5. Click **Save.**

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

Programming Allegion AD300/301 Locks

The Allegion AD300/301 locks are connected directly to the reader ports. As result, they do not have any direct association with a PIM, and therefore need to be configured with an equivalent entry in the Reader PIM tab.

1. In the **Reader 1/2 Pims** tab, click **Add** to add a new PIM 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 Security Expert smart reader, to enable communication with the controller.

1. To configure a smart reader as a wireless 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 PIM is wired to.
4. Select the **Configured Address** of the lock connected to the PIM.
5. Select the **Linked PIM Address**. This defines the address of the PIM that the lock is linked to.
6. Select the **Reader** tab.
7. Set the **Reader One Format** to the required credential format.
8. Set the **Reader One Location** to **Entry** or **Exit**.
9. Set the **Reader One Door** to the door this Allegion lock will control.
10. Click **Save**.

Security Expert does not allow PIMs (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 Security Expert will both start at 1.

Adding an Allegion AD300/301 Lock as a Smart Reader

1. To configure a smart reader as an AD300/301 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. Select the **Linked PIM Address** to *Not Set*.

   The Allegion AD300/301 locks are connected directly to the reader ports. As result, they do not have any association/link to any PIM.
6. Select the **Reader** tab.
7. Set the **Reader Location** to **Entry** or **Exit**.
8. Set the **Reader One Door** to the door this Allegion lock will control.
9. Click **Save**.

Trouble Inputs

As there are currently no individual trouble inputs provided for this integration, some trouble conditions are grouped and mapped to trouble inputs already assigned to the controller's onboard reader expander.

The following table details the mapping used for the integration:

Trouble Input Name	Module Input Number	Type	Allegion Specific Triggers
Door Forced Open	1	Door	Lock has been Forced Open
Door Left Open	2	Door	Lock has been Left Open
Reader Tamper	3	Door	Reader Tamper or PIM 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/AD300 Lock Offline
Reader 2 Tamper / Missing	13	Reader Expander	PIM/AD300 Lock Offline

For example, if any PIM or AD300 lock connected to Reader Port 1 of the onboard reader expander is detected to have gone offline, the ‘Reader 1 Tamper / Missing’ trouble input will be reported.

When the PIM tamper has been triggered, all locks linked to the PIM will have their ‘Reader Tamper’ trouble inputs reported.

Privacy Mode Operation

Pressing and releasing the Inside Push Button on an Allegion lock toggles Privacy Mode operation for the lock. By default, whenever the controller is powered on, Privacy Mode is automatically turned off for all Allegion locks.

In order for a user to access an Allegion lock operating in Privacy Mode the user must be a super user.

1. To set up a user as a super user, 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**.

If the user does not have super user rights and attempts to gain access while Privacy Mode is active, a '*Schedule Not Valid*' event will be recorded.

Additional Allegion Configuration

PIM Configuration for Manual Door Commands

In order for manual door commands within Security Expert to work with the Allegion integration, 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.

Configuration for Locks with Keypads

In order for Allegion locks with keypads to work correctly within Security Expert, the locks must be programmed with the following keypad settings:

- **Output Type**: Wiegand
- **Facility Code**: 1
- **Keys Buffered**: 8
- **Output Format**: 9

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

Schneider Electric

www.schneider-electric.com

June 2021