ARITECH

Aritech Reliance XR Series Door Access Programming Guide

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: recyclethis.info.

Contact information   https://www.firesecurityproducts.com.au/contact

Content

Important Information

This document includes an overview of the detailed instructions explaining how to use the Aritech Reliance XR Series system access control functionality. To use this documentation effectively, you should have a basic knowledge of alarm systems.

Read these instructions and all ancillary documentation entirely before operating this product.

Typographical Conventions

This manual uses certain notational and typographical conventions to make it easier for you to identify important information.

Table 1: Notational and typographical conventions

Item	Description
Keys	Capitalised, for example "press Enter".
Note	Notes alert you to information that can save you time and effort.
Caution	Cautions identify conditions or practices that may result in damage to the equipment or other property.
❑	Check boxes let you indicate whether a particular option is available or not. The manager can provide details on the available options.

Door Programming Guide

Prerequisites

Perform the full system configuration as for intrusion detection. Note that the Door Access features require some system resources to cover door control and monitoring, so these resources need to remain available prior to setting up Access-related features:

- Every Door which requires open/forced/door left open states reporting, needs to have a zone allocated to monitor the Door Contact state.

    Note: Can be shared with intrusion detection, for example, Entry Door zone.

- Every Door which requires unlocking by Request to Exit (RTE) signal, needs to have a zone allocated to monitor this signal.

- It is recommended to connect the Door Relay signal to the NXG-1832/33-EUR internal output. This open collector output can used for this purpose without consuming any additional system resources.

    Alternatively, it is possible to wire the Door Relay signal to any generic system output. Such a setup requires a single system Output and a single Action set up and allocated in the system for each Door or a group of Doors.

Programming Steps

Set basic door parameters

As an Installer, enter "Settings/Doors" menu in panel's web page (alternatively: "Doors" menu in DLX900 software).

Configure the following parameters:

- Door Name (up to 32 characters)

    The name is used to identify the door to users, to show the door state, or control the door.

- Door Type

    The parameter sets the level of door state monitoring. A combination of the following features can be selected:

    - Detection of the Door Left Open (DLO) state: Door kept open for the time longer than configured.

    - Detection of the Door Forced state: Door forcibly opened.

    - Door shunt: Prevents from generation of intrusion alarm if the door was opened legitimately.

- If a magnetic lock is used, then the Mag Lock option should be checked: The lock remains released as long as the door is opened.

- If any type of door monitoring is configured (Door forced / DLO / Shunt), then the Door Zone parameter must be set. The door contact signal should be wired to the selected zone.

- If Request to Exit signal is required (for example, door unlocking by a manual switch), then the RTE Zone parameter must be set. RTE signal should be wired to the selected zone.

- Timing parameters for DLO and Shunt features can be adjusted, if needed.

See also *Aritech Reliance XR Series Installation and Programming Guide*, "Programming Doors".

Note: Both door contact and RTE signals can be wired to input connector of NXG-1832/33-EUR keypads. In such a case, the relevant zone parameters should be set in the panel, *and* input-related parameters should be set in the keypad.

See also *NXG-183x Installation Sheet* (explanation on the required wiring), and "Advanced Keypad Configuration" on page 8.

Configure user permissions to Doors

User permissions to view/control the doors are based on Door Groups which are organised similarly to Partition Groups. Refer to "Door Groups" on page 16 for more information.

As an Installer, enter Advanced > Door Groups menu in the panel web page (alternatively: Door Groups menu in the DLX900 software).

Group the doors as desired by setting the door group names and selecting the doors belonging to particular group.

Note: One door may belong to multiple groups if needed. By default, the door group 17 contains all doors.

There are two alternative ways to set the user permissions to Doors:

Simplified: Standard/Arm Only/Duress/Master users have the Door Group parameter, which defines the group of doors the user has access to.

1. As a Master, enter Users menu in the panel web page (alternatively: Users menu in the DLX900 software).

2. Set the desired Door Groups to users.

   Note: By default, users have access to all doors (17 door group set).

Advanced: Custom user type may have up to four Schedule/Permission pairs defined. Permissions have a Door Group parameter, which defines the group of accessible doors.

1. As an Installer, enter the Advanced > Permissions > Control Groups menu in panel's web page (alternatively: Permissions menu in the DLX900 software).

2. Select the desired Door Groups, per Permission.

3. As a Master, enter Users menu in the panel web page (alternatively: Users menu in the DLX900 software).

4. Select the desired Schedules and Permissions to Custom users.

See also *Aritech Reliance XR Series Installation and Programming Guide*, "Programming Doors".

Configure keypad's permissions to Doors

If the door is accessed via NXG-1832/33-EUR keypads, then both User and Keypad access rights are considered together, similarly to the Partition access permissions.

Keypad access rights to doors are defined by means of Schedules/Permissions assigned to the keypad.

Note: By default, the keypad has All Partitions Permission set, which also gives access to all doors (door group 17 set).

Optional Door Customisation

Configure Door security features

The following features can be configured for doors:

*   Door access may be prevented if the door partition is armed
*   Door unlocking may cause automated disarming of armed partition
*   Door may be automatically unlocked in case of fire alarm
*   Door access may be prevented in case of alarm if the user has no right to disarm.

All door security features are related to the Partition Group the door belongs to. By default, this is defined by the partition group of the Door Zone but can also be set explicitly by modifying the Partition Group parameter.

See also: "Advanced System Configuration > Door Options" on page 15.

Configure reporting

Doors may generate several events to system log (Access and/or Main event category). By default, only the Door Forced and Door Accessed events are being reported. More event types can be enabled by relevant options in the door configuration.

Note: Monitoring station can receive Door Forced and Door Left Open (DLO) events, only. Other event types are stored to internal log.

See also: "Advanced System Configuration > Door Options" on page 15.

Configure scheduling and automation

Door can be automatically unlocked, either by Schedule or by Action. By default, door does not depend on any Schedules/Actions.

If unlocking schedule is defined, the actual unlocking may occur once the schedule trips (default setting), or may be deferred to the first valid user entry.

See also: "Auto Door Unlock" on page 14, "Door Options > Auto Door Unlock at 1st Entry on page 15.

Operation of RTE signal may be limited either by Schedule, or by Action. By default, RTE signal works anytime it is tripped.

See also "Advanced System Configuration > Auto Enable RTE" on page 14.

Card Programming Guide

Prerequisites

• All Users requiring a user card or tag must first be created and configured.

• At least one NXG-1832-EUR/NXG-1833-EUR Mifare keypad must be enrolled in the panel and be operational.

• Door Access functionality is supported with the Aritech Reliance XR Series panel series.

Programming Steps

Set card security mode (optional)

This step is needed only if the same cards are to be used by users on multiple systems. Otherwise, default settings may be left unchanged.

1. As an Installer, enter Advanced > System > Card Security Options menu in the panel web page or via keypad Program menu (alternatively: System menu, System and Siren Options tab in the DLX900 software).

2. By default, the Secure Key Mode parameter is set to Panel-specific key, which means that the cards configured can only be used in this specific site and this single panel only.

   Set Secure Key Mode to Manual to allow user cards to be used in multiple sites and multiple panels.

3. Define your password in the Secure Key parameter. The password must be at least 8 characters long. The same password must be set on all sites/panels that are supposed to support the same cards.

See also: *Aritech Reliance XR Series Installation and Programming Guide*, "Programming Card Security".

Add Cards to Users from the keypad

The most convenient and efficient way to assign Cards to Users is to perform this operation from the NXG-1832/33-EUR keypad menus. This method allows adding multiple cards sequentially, and it combines the two required operations in one step: securing cards (copying the security key from the panel to the card or tag) and assign the card to the user.

1. As a Master user, enter User Cards > Add Multiple Cards menu in the NXG-1832/33-EUR keypad. List of Users with no cards assigned will be shown.

2. Present a card or tag which is to be assigned to the user being displayed. The card or tag will automatically be secured and added to the user. The next user with no card assigned will appear.

   To select a specific user, press Up and Down keys.

See also: *NXG-183x User Manual*, "Add Multiple Cards".

Add Cards to Users from the panel web pages

Cards may be assigned to Users from the panel web pages. This mode requires the card numbers to be entered manually and this for every user.

1. As a Master user, enter User Cards menu in the panel web page, and select the user to add the Card.

2. Type the card number into relevant field. Check the Card Enabled option and press the Save button.

3. If the card was not secured before (typically in case of new cards out of factory), then press the Secure button to secure the card. The card or tag can be presented to any NXG-1832/33-EUR Mifare keypad in the system.

   If the card has been secured before, this step is not needed.

See also: *Aritech Reliance XR Series Installation and Programming Guide*, "Adding Cards to Users".

Add Cards to Users from DLX900

Cards may be assigned to Users by using the DLX900 software. This mode requires the card numbers to be entered manually and this for every user. This mode *does not support* securing of cards, so the cards to be assigned must be secured prior to assignment, using keypad's menu.

1. Connect to the system via DLX900 software

2. Enter User menu. Select user to add the Card.

3. Type the card number into relevant field. Check that the Card Enabled option is on. Send the changes to the panel.

Configure Card functions

Presenting a card or tag to the NXG-1832/33-EUR keypad can trigger up to 3 functions, depending the keypad settings. When a card or tag is presented, the keypad will respond with a beep sound to confirm it has read the card and will execute the first function. Presenting the card to the keypad and keeping the card in front of the keypad for another second will make the keypad to sound beep, double beeps, and execute the 2nd function. Presenting the card but keeping the card in front of the keypad for another second longer will make the keypad to sound beep, double beeps, triple beeps, and execute the 3rd function. This method allows the user to distinguish and select which function to trigger.

See also *NXG-183x User Manual*, "Using Cards".

Card functions can be configured in the keypad device menu: Single/Double/Triple Beep, available in Card Reader submenu. See "Card Reader Menu" on page 8 for details.

Secure Spare Cards and Tags (optional)

It is recommended but not mandatory, to secure all spare cards and tags, which are left unassigned on a system after initial system configuration. This allows that spare cards or tags can be assigned to users in the future without the need of presenting the card or tag in front of the Mifare keypad and, for example, allow just to enter the card number for the user, even remotely via DLX900 or the panel web page. Securing cards can be done from the NXG-1832/33-EUR keypad menu:
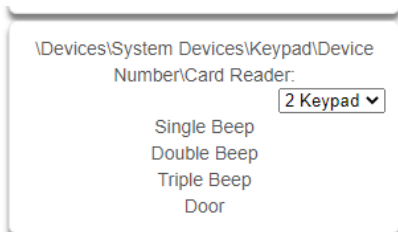
1. As a Master, enter User Cards > Secure Cards menu in NXG-1832/33 keypad.

2. Swipe all cards to be secured, one by one. Keypad will show the information on the successful securing operation.

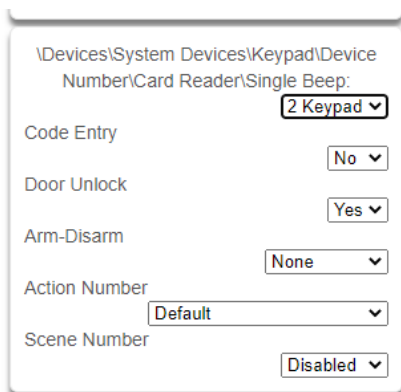See also: *NXG-183x User Manual*, "Secure Cards".

Advanced Keypad Configuration

Card Reader Menu

The Card Reader menu contains 4 submenus and keypad selector drop-down.

```
\Devices\System Devices\Keypad\Device
         Number\Card Reader:
                              [ 2 Keypad ∨ ]
                  Single Beep
                  Double Beep
                  Triple Beep
                     Door
```

Single/Double/Triple Beep

Select one of these submenus to configure functions to be executed when a card or tag is being presented to the Mifare keypad NXG-1832/NXG-1833-EUR. Up to 3 functions can be configured: single, double, triple beep respectively. The menu structure is identical for these submenus:

```
\Devices\System Devices\Keypad\Device
      Number\Card Reader\Single Beep:
                              [ 2 Keypad ∨ ]
 Code Entry
                                   [ No ∨ ]
 Door Unlock
                                   [ Yes ∨ ]
 Arm-Disarm
                              [ None        ∨ ]
 Action Number
                              [ Default        ∨ ]
 Scene Number
                              [ Disabled ∨ ]
```

- **Code Entry:** Presenting a card or tag is causing the keypad to either deactivate the screensaver (if the screensaver is currently visible) or enter the user menu (if the keypad shows its main screen).

- **Door Unlock:** Presenting a card or tag unlocks the door defined by Door parameter (see "Door" on page 9).

- **Arm-Disarm:** Presenting a card or tag triggers the arming or disarming operation selected on drop-down list. The following options are available:

  - Disarm: Disarm partitions.

  - Arm Away, Arm Stay, Arm Instant, Arm Night: Arm partitions in the relevant arming mode (if the system configuration supports it).

  - Clr Screensaver-Disarm: If the screensaver is active, presenting a card will deactivate the screensaver. If the screensaver is not active, presenting a card will disarm the partitions.

  - Arm Away – Disarm, Arm Stay – Disarm, Arm Instant – Disarm, Arm Instant – Disarm: If all partitions are disarmed, presenting a card will arm the

partitions in the relevant arming mode. If any partition is armed in any mode, or is in alarm, presenting a card will disarm the partitions and/or silence the alarm.

Note: To select the operation to be performed, the keypad considers the state of the partitions that the card user is permitted to disarm.

- **Action Number:** Presenting a card or tag executes an Action, as selected on drop-down list

- **Scene Number:** Presenting a card or tag executes a Scene, as selected on drop-down list.

Notes

- Multiple actions can be selected for a particular beep count level (for example: unlocking the door and triggering a scene to switch on the lights).

- Actions will only be executed if the User of the card or tag has sufficient permissions to execute particular action.

Door

Select this option to configure the Door in the system which should be unlocked by presenting a card to this keypad, if the card functions are configured to do so (see "Single/Double/Triple Beep" on page 8). This option will also define the door which will be controlled by this keypad output.
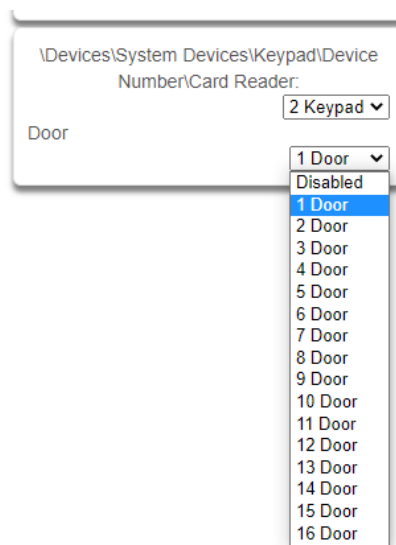
Input Menu

The Input menu contains two parameters to configure the keypad input.
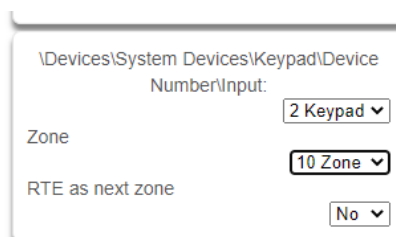
- **Zone:** Logical zone number assigned to the keypad input.

- **RTE as next zone:** Available on NXG-1832/33-EUR Mifare keypad only. Enable this option if the door contact and the Request-To-Exit (RTE) button are both wired to the keypad input (see the Keypad Installation Sheet for wiring diagrams).
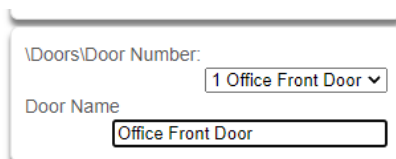
Advanced System Configuration

Doors

The Doors menu contains a few submenus and a door selection drop down. Select the door to program and then select the desired submenus.
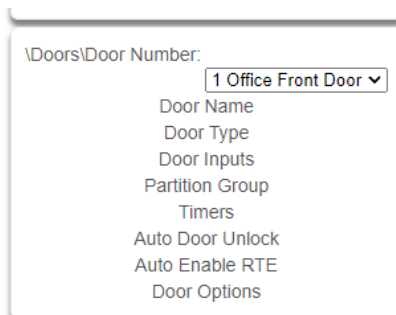
Door Name

Select this submenu to program an up to a 32-character custom name for the selected door. This name will appear in any lists in the system including keypad GUIs controlling doors:

Door Type

Select this submenu to enable the door with the desired combination of Door Zone Shunting (Shunt), Forced Door Monitoring (Forced), Door Left Open (DLO) monitoring.
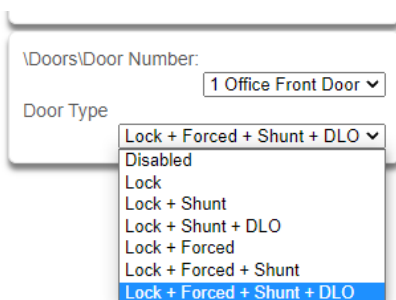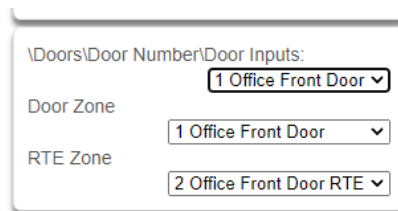

Lock: At the start of the door unlock time, the door is unlocked and is locked at the end of the door unlock time. There are no zone inputs assigned. At the end of the door unlock time, the door is deemed to be closed and secure. There is no shunting, forced door or DLO support.

If anything, other than Lock is selected, The Door Zone Input must be programmed in the Door Inputs submenu. Shunting will cause the alarm system to ignore the Door Zone input for time programmed in the door Timers submenu. If the Forced Option is selected, the system will log a Forced Door Event if the door is opened while it is still locked. If the DLO feature is enabled, an event will be logged when the shunt timer expires. The Forced and DLO events can optionally be reported off premises by selecting the corresponding option in the Options submenu.
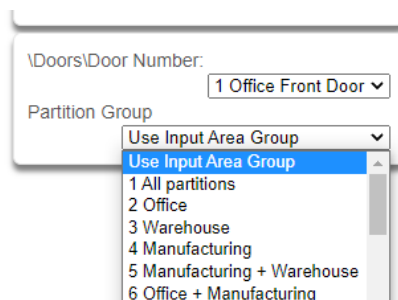
Door Inputs

Choose the desired system zone inputs for the Door Zone and the Request to Exit Zone (RTE). The Door zone is to indicate if the door is open or closed. This is usually a magnetic contact and can be part of the alarm system and have any appropriate zone type. The RTE zone should not be used by the alarm system except for requesting Exits.
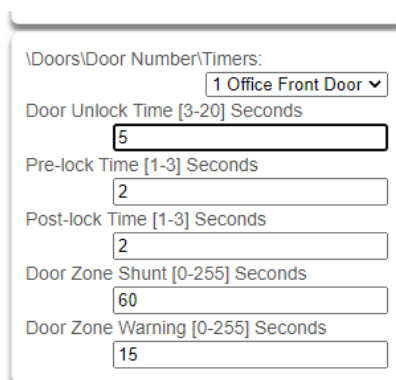

Partition Group

This optional feature can be used to select which partition armed states are checked when an attempt is made to unlock a door. If a partition or partitions in the group are armed, the system will either disarm the partitions or deny access depending on the options selected in the Options submenu. If a partition is armed and the User accessing the door does not have permission to disarm that partition, access will be denied. If a partition is armed and the No Access if Armed option is set in the door options, access will also be denied. Leaving at the default of Use Input Partition Group will use the partition group of the zone selected for the Door Zone.

Timers

This submenu contains all the timers associated with a door. Access this menu to adjust times if the application needs times other than the default time.
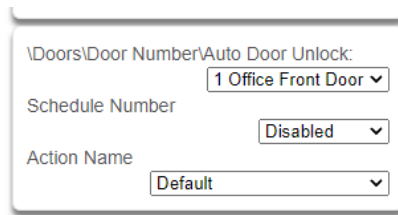

- **Door Unlock Time:** This is the number of seconds the door will remain unlocked when a user presents a credential to access a door. This allows time for a user to pass through the door and shut it again.

- **Pre-lock Time:** When the shunt cancel feature is enabled, the system monitors the Door Zone to determine when the door has been closed. Once the door is closed it starts the pre-lock timer. If the Door Zone remains closed for the entire pre-lock time, the system will lock the door and start the post lock timer. If the Door Zone opens before the pre-lock timer expires, the pre-lock timer is cancelled, and the door is considered open. The shunt continues during the pre-lock timer.

- **Post-lock Time:** The post-lock time allows time for a lock to fully engage. If the Door Zone remains closed for the entire post-lock time, the door is considered secure and the shunt is removed. If the Door Zone opens before the post-lock timer expires, the post-lock timer is canceled, and the door is considered open. The shunt continues during the post-lock timer.

- **Door Zone Shunt:** The amount of time (0 to 255sec) the Door Zone can remain open before the zone will create an alarm. If the Door Zone Shunt timer expires while the Door Zone is open, or expires during the pre-lock or post-lock time, then a normal alarm or DLO occurs.

- **Door Zone Warning:** The time (0 to 255sec) remaining in the Door Zone Shunt timer before a door warning condition becomes active. The panel will activate the keypad buzzers which will sound with a different audible pattern compared to an intrusion alarm. Also relay outputs can be programmed to sound a sounder to notify the user of a pending shunt expiration.

Auto Door Unlock

A schedule or a system condition that causes a door to stay unlocked thus allowing access without a User credential. It can be accomplished with a schedule OR an Action.
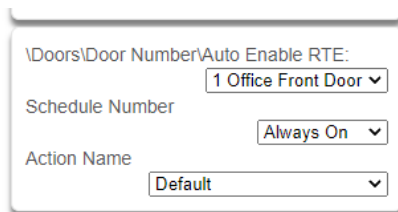
\Doors\Door Number\Auto Door Unlock:
1 Office Front Door
Schedule Number
Disabled
Action Name
Default

- **Schedule:** Select disabled to not use a schedule to automatically unlock a door. Select a programmed schedule that will unlock the door when the schedule is true.

- **Action:** Select default to not use an Action to automatically unlock a door. Select a programmed Action that will automatically unlock the door when the Action is true.

Note: If both an Action and a Schedule are selected, the door will automatically unlock when either the schedule OR the Action is true. If the Schedule is disabled and the Action is set to default the automatic unlock is never active.

Auto Enable RTE

Per default settings, the RTE will work anytime it is tripped. This submenu can be used to limit the RTE with a schedule or an Action.

\Doors\Door Number\Auto Enable RTE:
1 Office Front Door
Schedule Number
Always On
Action Name
Default

- **Schedule:** Select Always on to not use a schedule to limit the RTE. Select a programmed schedule that will allow the RTE to work when the schedule is true.

- **Action:** Select default to not use an Action to limit the RTE. Select a programmed Action that will allow the RTE to work when the Action is true.

Note: If both an Action and a Schedule are selected, the RTE will work when either the schedule OR the Action is true. If schedule is set to Always On and Action is set to default, the RTE will work all the time.

Door Options

Use this to select the desired behavior of the door.

- **Door Forced Reporting:** When the Door Type selected supports the Forced Door feature, ticking this box will cause the Forced Door Alarm to be reported off premises.

- **Door Left Open Reporting:** When the Door Type selected supports the DLO feature, ticking this box will cause the DLO Alarm to be reported off premises.

- **Log Door Access:** Ticking this box will cause a logging event when the door is unlocked. This event identifies the Door and the user that opened it.

- **Log Door Secure:** Ticking this box will cause a logging event when the door is secure (Locked, Closed and not Shunted). This event identifies the Door and the user that unlocked it.

- **Door Zone Shunt Cancel:** Ticking this box will enable the shunt cancel feature. This feature will disable the shunt after the expiration of the Post Lock Timer (See pre-lock ad post-lock times in the Timers section above).

- **No Access if Armed:** Ticking this box will prevent the door from opening if any partition in the Door Partition Group is armed.

- **Disarm if Armed:** Ticking this box will disarm any partitions in the Door Partition Group that are armed. If the user has no authority to disarm it will deny access.

- **Auto Door Unlock at 1st Entry:** Ticking this box will (when the Auto Door Unlock is active) only automatically unlock the door when the door is unlocked by a User for the first time.

- **RTE when Fire Alarm:** Ticking this box will force the RTE to be enabled anytime a fire alarm is active.

- **No Access if Alarm:** Ticking this box will cause access to be denied unless the User permissions allow to disarm from alarm.

- **Mag Lock:** Choose this option to prevent the lock from engaging until the door has been closed for the Pre-Lock time. If the door remains open past the shunt time the shunt will be removed and if enabled, the DLO event will be triggered. The door will remain unlocked until it is closed.

- **Log Door Open and Close:** Ticking this box will cause a logging event the first time the door is opened following an unlock state and a door closed event when the door is closed, locked, and not shunted. This event identifies the Door and the user that unlocked it.

- **Access Denied Event:** Access Denied events are always reported to the log. This is not a programmable option.

Door Groups

The **Door Groups menu** contains submenus and a door group selection drop down. Select the door group to program and then select the desired submenus. There are 64 Door Groups available for configuration.

Note: Door Groups are preconfigured as follows:

- Groups 1 to 16 are configured with a single Door 1 to 16 respectively
- Group 17 is configured with all doors 1 to 16, and named All Doors
- Groups 18 to 64 are undefined

Door groups can be customised by setting the following parameters:

Door Group Name

Select this submenu to program an up to a 32-character custom name for the selected door group. This name will appear in any lists in the system:

\Door Groups\Door Group Number:
```
                    [ 1 Internal doors ⌄ ]
Door Group Name
    [ Internal doors                    ]
```

Door List

Select this submenu to program the list of doors to be assigned to particular Door Group:

\Door Groups\Door Group Number:
```
                    [ 1 Internal doors ⌄ ]
1 Door                              ☑
2 Door                              ☑
3 Door                              ☑
4 Door                              ☑
5 Door                              ☐
6 Door                              ☐
7 Door                              ☐
8 Door                              ☐
9 Door                              ☐
10 Door                             ☐
11 Door                             ☐
12 Door                             ☐
13 Door                             ☐
14 Door                             ☐
15 Door                             ☐
16 Door                             ☐
```