



TS1067E Network Access Controller Programming Manual

Copyright	©2025 Aritech, All rights reserved.	
Trademarks and patents	The Challenger name and logo are trademarks of KGS Fire and Security Australia Pty Ltd. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.	
Manufacturer	Made in China by KGS Safety Systems No. 80, Changjiang East Road, QETDZ, Qinhuangdao, Hebei, P. R. China 066004 Imported by KGS Fire and Security Australia Pty Ltd Suite 4.01, 2 Ferntree Place Notting Hill, Victoria, 3168, Australia	
ACMA compliance	Notice! This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.	
WEEE compliance	For proper recycling, dispose all the batteries and the packaging as required by local ordinances or regulations.	
Contact information	For contact information, see https://www.aritech.com.au/	

Content

Important information	3
Limitation of liability	3
Agency compliance	3
 Product overview	 4
About this manual	4
Related documentation.....	4
Introduction	4
Operating modes.....	7
Doors	11
Lock types.....	12
Interlocking doors.....	14
Alarm control.....	15
Bus formats.....	16
Flexible device locations	20
Input and relay mapping.....	22
Configuring the Auxiliary SW output	25
Overriding door state.....	26
Random lockout time.....	29
LED area mapping for door readers	29
Overriding lift state	29
 Recommended programming sequence	 31
DIP switches	32
Defaulting the NAC.....	32
CTPlus connection	32
Uploading default configuration.....	37
Upgrading firmware	38
Licensing Functionality	40
Programming IP communications	43
Programming the NAC	46
Programming holidays.....	64
Programming time zones	65
Programming regions	66
Programming doors.....	67
Programming lifts	91
Programming input and relay mapping options.....	95
Programming macro logic	103
Programming user information	106
 Management via CTPlus	 109
Status and control	109
Configuring door/lift schedules.....	115
 Appendix A: Reference materials.....	 117
Using time and attendance readers.....	117
Macro events	118

NAC Door Defaults.....	123
APPENDIX B: Enclosure Access Restrictions.....	125

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will KGS Fire and Security Australia Pty. Ltd. be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of KGS Fire and Security Australia Pty. Ltd. shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether KGS Fire and Security Australia Pty. Ltd. has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with these manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

The customer is responsible for testing and determining the suitability of this product for specific applications. The customer is responsible for testing the product at least once every three months.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, KGS Fire and Security Australia Pty. Ltd. assumes no responsibility for errors or omissions.

Agency compliance

This product conforms to the standards set by Standards Australia on behalf of the Australian Communications and Media Authority (ACMA). KGS Fire and Security Australia Pty. Ltd. recommend enclosure covers remain fitted to maintain ACMA compliance.

Notice! This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Product overview

About this manual

This manual is intended for use only by trained Challenger installation and configuration technicians. The manual introduces the TS1067E Network Access Controller (NAC) and covers all aspects of programming the NAC.

This manual applies to the following models:

- **TS1067E** Network Access Controller w/ onboard Wiegand

For the purposes of this manual, unless otherwise specified 'TS1067E' shall refer to all models generically.

Related documentation

The *TS1067E Network Access Controller Installation Manual* provides instructions on installing the Network Access Controller.

The *ChallengerPlus Programming Manual* provides detailed information about Challenger system configuration and programming.

The Challenger system is modular. Refer also to the documentation that is shipped with each module that you intend to use.

The CTPlus online help describe the CTPlus user interface and all available programming options for Challenger*Plus* and the NAC.

Introduction

The **TS1067E Network Access Controller** is a complete access control solution which allows you to manage not only your door and lift access requirements but also supports intrusion applications.

The flexible connection options mean you can connect the NAC directly to your management software without the need for other panel hardware, or you can connect to the Challenger*Plus* panel for an easy upgrade on your existing site.

Powerful processing and on-board storage means the NAC suits a range of applications from small standalone systems, to distributed systems covering hundreds of thousands of users.

Features

The Network Access Controller has the following features:

- Compatible with Challenger*Plus* panels
- Direct Ethernet and USB connections to supported management software via up to ten communications paths

- Supports up to eight doors (depending on operating mode and license issued):
- Large memory capacity (depending on operating mode):
 - Up to 250,000 users
 - 10,000 door groups
 - 1,000 floor groups
 - 50,000 access history events
 - 2,000 time zones ('hard' time zones)
 - 8 sub-time zones per time zone
 - 100 holidays
 - Up to 128 bit card data
- Two local RS-485 buses supporting the following protocols:
 - Tecom
 - OSDP v2
 - SALLIS by SALTO Systems
 - Aperio
- Remote flash firmware upgradeable
- Configurable end-of-line (EOL) resistor values
- Up to 100 door schedules can be programmed to lock or unlock doors at set times
- Supports operator-defined door overrides for use from management software
- Each person can have a 4 to 10 digit PIN
- Map up to 32 inputs and 16 relays for use with a Challenger*Plus* panel
- 16 onboard inputs that can be further expanded to 32 with the use of the input expander
- A variety of lock types reduces the need for complex lock programming
- Easy configuration of interlocking doors on the same NAC
- Battery management using intelligent charging process.
- Flexibility in device locations for devices (inputs/relays/readers) attached to the NAC
- Two sets of plug-in connectors (providing communications), which require no wiring, for ease of connection to additional boards
- Each door can have up to six readers in any combination of IN or OUT readers
- Doors can be programmed to lock out a certain percentage of the times that a valid card or PIN is presented to a reader

- Supports mapping of Challenger*Plus* areas to door reader LEDs (in supported modes)
- Detailed door diagnostics from the NAC can be requested from management software
- Up to 48 macros can be programmed

Note: Configuration via keypad is not available for the Network Access Controller. Configuration must be done via software (CTPlus).

Note: For access restrictions to the interior of the enclosure, refer to APPENDIX B: Enclosure Access Restrictions.

The major features are described in the following sections.

Operating modes

The Network Access Controller can operate in three different ways depending on your current system and access requirements:

- **IP Direct mode** – in this mode, management software has a direct IP connection to the NAC, without needing a Challenger panel. The NAC provides access control functionality but does not provide alarm control functionality.
- **IP Extended mode** – in this mode, management software has a direct IP connection to the NAC. In addition to access control, the NAC provides alarm control and reporting functionality in conjunction with a Challenger*Plus* panel.
- **Classic mode** – this mode is for direct upgrade of a V8 Four-Door Controller with minimal programming changes. In addition to access control, the NAC provides alarm control and reporting functionality in conjunction with a Challenger*Plus* panel.

The limits for users and other entities vary according to the operating mode, as shown in Table 1 below.

Table 1: NAC limits per mode

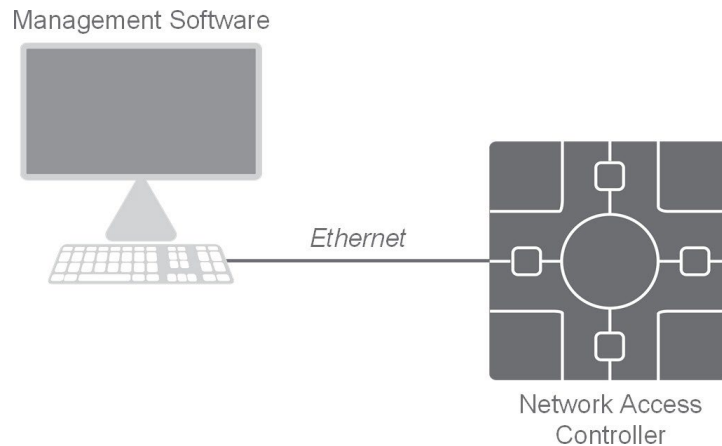
	IP Direct	IP Extended	Classic
Doors	8	8	8
Lifts	8	8	8
Floors (per lift)	100	100	64
Users	250,000	250,000	65,535 (2000)
Door groups	10,000	10,000	255
Floor groups	1,000	1,000	128
Time zones	2,000	2,000	64
Sub time zones	8	8	8
Holidays	100	100	24
Holiday types	8	8	8
Card bit length	128	128	48
History event buffer	50,000	50,000	50,000

The modes are described in more detail in the following sections.

IP Direct mode

IP Direct mode allows software to communicate with the NAC directly via IP rather than through a Challenger panel. The IP connection allows for high-speed download of users and other configuration data to the NAC. The NAC provides access control functionality but does not provide alarm control functionality. In this mode, a Challenger panel is optional.

Figure 1: IP Direct mode



In this mode, management software downloads users, door groups, etc. directly to the NAC, allowing the NAC to utilise its maximum capacities, as shown in Table 1 on page 7.

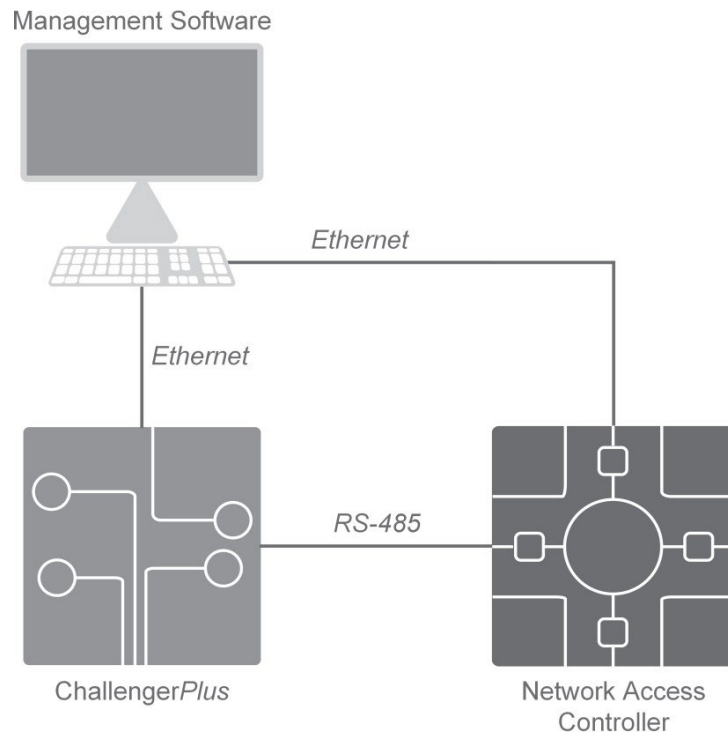
History events, alarms, and NAC status are reported via IP to management software.

Note: The NAC will still be fully functional if it is disconnected from management software.

IP Extended mode

IP Extended mode allows software to communicate with the NAC directly via IP rather than through a Challenger*Plus* panel (like IP Direct mode), while retaining the alarm control and reporting functionality of a NAC in Classic mode.

Figure 2: IP Extended mode



In this mode, management software downloads users, door groups, etc. directly to the NAC, allowing the NAC to utilise its maximum capacities, as shown in Table 1 on page 7. The NAC retains its own database of users, door groups etc. from the Challenger*Plus* panel.

The number of users that can exercise alarm control from the NAC is limited by the user capacity of the Challenger*Plus* panel (2,000 users or 65,535 users if the Challenger*Plus* panel has a TS1084 Memory Expansion Module). See the “Alarm control” section on page 15 for more information.

History events are sent directly via IP to management software, while alarms and NAC status are sent to the Challenger*Plus* panel. [eg. DGP tamper reports to c10 to be dialled out to monitoring station, but can also report to management software via IP.]

Note: The NAC will still be fully functional if it is disconnected from management software.

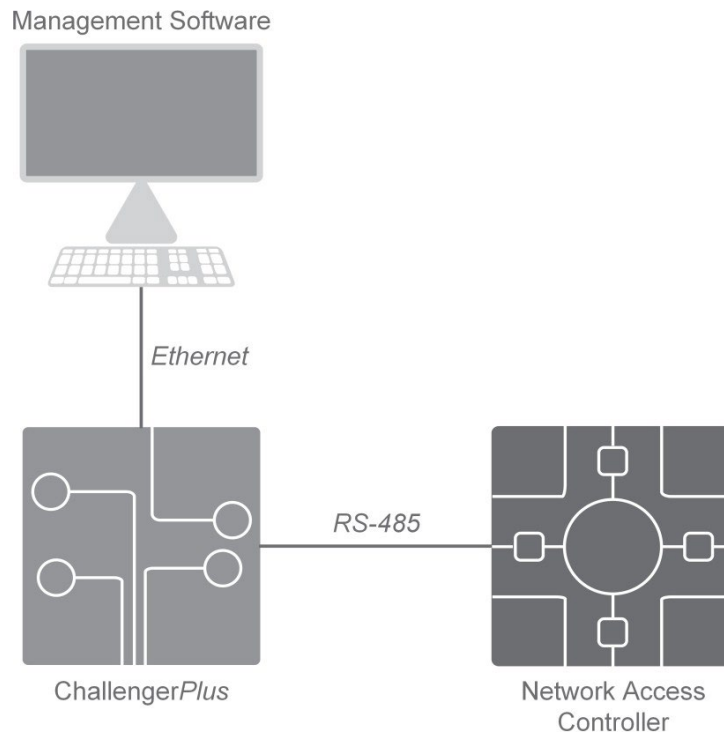
Note: Inputs will only register alarms in the Challenger*Plus* panel if they are mapped to Challenger*Plus* inputs. See the “Input and relay mapping” section on page 22 for information on Challenger*Plus* input mapping.

Classic mode

Classic mode can be used for direct upgrade of a V8 Four-Door Controller with minimal programming changes. In addition to access control, the NAC provides alarm control functionality in conjunction with a Challenger*Plus* panel.

The NAC is polled as a DGP on one of the Challenger*Plus* system LANs.

Figure 3: Classic mode



In this mode, management software downloads configuration (users, door groups, etc.) to the Challenger*Plus* panel. The Challenger*Plus* panel distributes the configuration to the NAC via the RS-485 LAN.

Since the Challenger*Plus* is responsible for the distribution of users, door groups etc. to the NAC, the numbers allowed are limited, as shown in Table 1 on page 7.

History events, alarms, and NAC status are sent from the NAC to the Challenger*Plus* panel.

Note: Inputs will only register alarms in the Challenger*Plus* panel if they are mapped to Challenger*Plus* inputs. See the “Input and relay mapping” section on page 22 for information on Challenger*Plus* input mapping.

Multiple modes

Warning: It is possible to configure a NAC to operate in one mode and still connect to it via one of the other modes. Programming commands will always be accepted and processed by the NAC. This may cause conflicted or incorrect programming in the NAC.

For example, it is possible to connect a NAC in IP Direct mode to a Challenger*Plus* panel and attempt to program it in IP Extended or Classic mode. Programming commands issued via the LAN will be accepted and processed by the NAC.

Doors

The Network Access Controller supports up to eight doors (depending on operating mode and license issued).

If the NAC is connected to a Challenger*Plus* panel (i.e. in IP Extended or Classic mode), then the NAC can support either four or eight doors, depending on model and configuration of the DGP. The licensing of the device can also determine how many doors are available on the NAC. The doors are numbered from 17 to 64 or from 81 to 128, depending on which Challenger*Plus* system LAN the NAC is connected to.

NACs may use the first 12 addresses on each Challenger*Plus* system LAN. Table 2 below lists the LAN number, the address of the NAC (set via the NAC's DIP switches), the DGP number that the NAC is polled as, the ranges of door numbers for 4 Doors and 8 Doors Modes.

If 8 Doors Mode is selected, no door-type DGPs (E.g. NAC, DWI, 4DC, 4LC) can be polled in the next DGP address. (E.g. NAC with 8 doors mode addressed as DGP 1, next NAC can only be addressed from DGP 3 onwards)

Standard type DGPs such as TS1020, TS0820, TS1025 and 4 inputs DGP can still be polled in the next DGP address even if the NAC is configured for 8 Doors Mode.

Table 2: Door numbers per DGP address

Challenger <i>Plus</i> LAN	Address	Polled as	4 Doors Mode	8 Doors Mode
LAN 1	1	DGP 1	17 to 20	17-24
LAN 1	2	DGP 2	21 to 24	21-28
LAN 1	3	DGP 3	25 to 28	25-32
LAN 1	4	DGP 4	29 to 32	29-36
LAN 1	5	DGP 5	33 to 36	33-40
LAN 1	6	DGP 6	37 to 40	37-44
LAN 1	7	DGP 7	41 to 44	41-48
LAN 1	8	DGP 8	45 to 48	45-52
LAN 1	9	DGP 9	49 to 52	49-56

ChallengerPlus LAN	Address	Polled as	4 Doors Mode	8 Doors Mode
LAN 1	10	DGP 10	53 to 56	53-60
LAN 1	11	DGP 11	57 to 60	57-64
LAN 1	12	DGP 12	61 to 64	-
LAN 2	1	DGP 17	81 to 84	81-88
LAN 2	2	DGP 18	85 to 88	85-92
LAN 2	3	DGP 19	89 to 92	89-96
LAN 2	4	DGP 20	93 to 96	93-100
LAN 2	5	DGP 21	97 to 100	97-104
LAN 2	6	DGP 22	101 to 104	101-108
LAN 2	7	DGP 23	105 to 108	105-112
LAN 2	8	DGP 24	109 to 112	109-116
LAN 2	9	DGP 25	113 to 116	113-120
LAN 2	10	DGP 26	117 to 120	117-124
LAN 2	11	DGP 27	121 to 124	121-128
LAN 2	12	DGP 28	125 to 128	-

When an operator connects CTPlus to a NAC, upon performing an upload the doors are automatically created.

Each door controlled by the NAC can have two door inputs, an egress input, two lock relays, a DOTL (Door Open Too Long) relay, a forced door relay, a warning relay, and six assigned readers in any combination of IN and OUT readers.

Each door has various options for access, shunting, egress, and anti-passback. There are also options for alarm control if the NAC is connected to a ChallengerPlus panel.

Doors are programmed on the **Doors/Lifts** form in CTPlus. See the “Programming doors” section on page 67.

Lock types

To support more complex door operation than the V8 Four-Door Controller, the Network Access Controller introduces new lock types, with associated inputs, relays and timers.

The new lock types are:

- **Strike**
- **Maglock**

There are two inputs for each door, and two lock relays for each door:

- **Door input 1** – Connected to the door to indicate if the door is open or closed. This is usually the reed switch.

- **Door input 2** – Connected to the lock monitor on Strike and Maglock locks.
- **Lock relay 1** – Unlocks the door.
- **Lock relay 2** – Reserved for future use.

The door's lock type, and inputs and relays are programmed in CTPlus on the *Hardware* tab for the door. See the "Programming hardware options" section on page 69 for instructions.

The following timers can be defined:

- **Pre-Lock time** – Once the door open input (**Door input 1**) has been sealed, the NAC waits for the pre-lock time to expire before locking the door. If the door open input unseals during the pre-lock time, the door is deemed open and the pre-lock timer is cancelled. The shunt continues during the pre-lock time.
- **Post-lock time** – The post-lock time allows time for a lock to fully engage. After the post-lock time has expired, the door is deemed secure, and the shunt is cancelled. If the door open input unseals during the post-lock time, the door is deemed open and the post-lock timer is cancelled. The shunt continues during the post-lock time.

Note: There are also two roller door specific timers that are reserved for future use.

The timers are programmed in CTPlus on the *Access* tab for the door. See the "Programming access options" section on page 74 for instructions.

Example door operation scenarios

Simple door unlock with no inputs

At the start of the access time, the door is unlocked (via **Lock relay 1**) and is locked at the end of the access time. There are no inputs assigned. At the end of the access time, the door is deemed to be closed and secure.

There is no shunting, forced door or DOTL support.

Door unlock with one input for open door

At the start of the access time, the door is unlocked (via **Lock relay 1**). If the door is opened within the access time (i.e., **Door input 1** is unsealed), then the shunt timer starts. When the door is subsequently closed, the pre-lock timer starts. After the pre-lock time, the door is deemed closed. At that time, maglocks can be locked. After the post-lock time, the shunt is cancelled, and the door is deemed secure.

If the shunt timer expires while the door is open, or expires during the pre-lock or post-lock time, then a normal alarm or DOTL occurs.

Interlocking doors

Interlocking is a method that stops two or more doors from being opened at the same time. Interlocking may be used in a vault, for example.

When programming a door on the NAC, there are two ways to specify an interlock door: either another door on the same NAC, or a door on a separate controller.

The NAC has simplified configuration of interlocking doors on the same controller.

Interlock door on same controller

When programming the door, navigate to the door's *Hardware* tab and tick the required interlock doors in the **Interlock doors** field.

When an attempt to open/unlock the programmed door occurs (either from user action or from management software), the NAC will check all other locally linked doors to ensure that no other door is unsecured, before allowing the door to open.

When internal interlocking option is enabled on NAC, a special interlocking timer (300ms if only internal interlocking is enabled) is started when a user credential is presented. Any repeated attempt to gain access by providing a user credential while the timer is running and the remaining time is greater than 100ms will cause *Access Denied Void* and 7 error beeps. If access is granted and the door becomes in access, this waiting time is bypassed and all the consequent credential requests are processed without that delay.

A proposed sequence of user action on the interlocked doors is below:

- Present a credential (hear a single beep if it's a card or press enter if it's a pin);
- Wait for the NAC to confirm. NAC confirms with either 2 beeps if the credential has a right to access or 7 beeps in case of a wrong credential. The waiting time may be less than a second if no external interlocking is enabled or about 3 seconds if external interlocking is enabled;
- Proceed to the next step.

Interlock door on external controller

There are three external input fields provided for the NAC to check for interlocking on external controllers.

To interlock with a door on an external controller, a contact from the external door must be wired to a spare input connected to the NAC, and vice versa.

When programming the door on the NAC, navigate to the door's *Hardware* tab and define the locations of the inputs connected to external door contacts in the **External input** fields.

When an attempt is made to open/unlock the programmed door (either by user action or from management software), then the NAC will check the state of these external inputs. If any of the external inputs is unsealed, access will be denied immediately.

If all external inputs are sealed, the NAC will activate the “Door unlocked” event. A macro should be created which takes the “Door unlocked” event and activates a relay linked to the other controller(s).

When external interlocking option is enabled on NAC, a special interlocking timer (3sec if only external interlocking is enabled) is started when a user credential is presented. Any repeated attempt to gain access by providing a user credential while the timer is running and the remaining time is greater than 100ms will cause *Access Denied Void* and 7 error beeps. If access is granted and the door becomes in access, this waiting time is bypassed and all the consequent credential requests are processed without that delay.

A proposed sequence of user action on the interlocked doors is below:

- Present a credential (hear a single beep if it's a card or press enter if it's a pin);
- Wait for the NAC to confirm. NAC confirms with either 2 beeps if the credential has a right to access or 7 beeps in case of a wrong credential. The waiting time may be less than a second if no external interlocking is enabled or about 3 seconds if external interlocking is enabled;
- Proceed to the next step.

Interlocking is programmed on the *Hardware* tab of the **Doors/Lifts** form. See the “Interlock options” section on page 71.

Alarm control

Note: Alarm control does not apply to the NAC in IP Direct mode.

The Network Access Controller can perform alarm control functions, such as arming areas, if it is connected to a Challenger*Plus* panel. Alarm control for each NAC door is determined through **alarm control levels**, which are analogous to alarm groups in Challenger.

Each alarm control level can be assigned a time zone:

- In IP Extended mode, a NAC time zone can be assigned to an alarm control level
- In Classic mode, a Challenger*Plus* time zone (either a “hard” panel time zone or a soft time zone) can be assigned to an alarm control level

Each alarm control level can be allocated a list of up to ten areas for arming, disarming, timed disarming, and resetting alarms. Other alarm control attributes such as the ability to reset system alarms can be programmed for each alarm control level.

A NAC door can have up to six alarm control levels, which are then assigned to a door side (either IN or OUT) in any combination. Up to six alarm control levels can be assigned to a door side.

If a user initiates some alarm control functionality at a reader (e.g. they badge their card three times to arm areas), the NAC checks the alarm control levels for

the door that apply to the reader (depending on whether the reader is an IN or OUT reader).

If any of the assigned alarm controls levels has a time zone that is valid, then the user's credential information is sent to the Challenger*Plus* panel, along with information about any applicable alarm control levels. The Challenger*Plus* panel checks the user's credentials in its user database and checks the corresponding Challenger*Plus* user's alarm group.

If the corresponding Challenger*Plus* user's alarm group and the reader's alarm control level allow an alarm function, then the alarm function proceeds.

Note: In IP Extended mode, the number of users that can exercise alarm control from the NAC is limited by the user capacity of the Challenger*Plus* panel (2,000 users or 65,535 users if the Challenger*Plus* panel has a TS1084 Memory Expansion Module).

Alarm control levels are set up in CTPlus on the *Alarm control levels* tab for the door. Alarm control levels must also be assigned to the door's readers, which can be done on the *Alarm* tab for the door. The alarm control functionality is programmed in CTPlus on the *Alarm* tab for the door. See the "Programming alarm control options" section on page 85 for instructions.

Bus formats

There are two RS-485 buses on the Network Access Controller. Each bus can have up to 16 RAS devices. Each bus can support readers other than Tecom readers.

Each bus supports the following protocols:

- Tecom
- OSDP (Open Supervised Device Protocol) version 2
- SALLIS by SALTO Systems
- Aperio

Each bus can use one protocol at a time, but the two buses can use different protocols.

The bus format for each bus is defined on the *NAC options* tab of the DGPs form for the NAC. See the "

Bus options" section on page 50. If the bus format is OSDP, then the baud rate of the bus can be configured, and encryption can be enabled by entering the OSDP encryption key. OSDP encryption uses the AES 128-bit encryption algorithm.

When assigning a RAS to the NAC via the *Assigned RAS* tab of the DGPs form, specify the bus format that the reader will use (which depends on the RAS's number). See the "Assigning RASs" section on page 53.

Note: The two 4-pin RS-485 cable sockets provide data and power from Bus 1. For more information about the cable sockets, see the *TS1067E Network Access Controller Installation Manual*.

Non-Tecom devices must meet certain requirements to work with the NAC, as described in the following sections.

OSDP

The Network Access Controller supports OSDP version 2.

Note: OSDP has a fixed baud rate of 9600 baud.

OSDP reader addresses

If the OSDP reader has DIP switches, refer to the manual for the reader to configure the reader's address using the DIP switches. If the reader does not have DIP switches, then the reader's address must be configured using a configuration card. Assign the reader the desired address by badging the appropriate configuration card at the reader.

OSDP encryption

Without an encryption key configured for the NAC bus, the NAC communicates with the OSDP devices using a default encryption key as specified in the OSDP standard. To use a non-default encryption key with OSDP readers, set the 128-bit AES encryption key for the bus in CTPlus. See the "Bus encryption key" section on page 51. The encryption key will be set on each OSDP reader attached to the bus once the encryption key is defined.

Once set, the encryption key on an OSDP reader cannot be changed by changing the encryption key for the bus. To reset the encryption key used by an OSDP reader, the reader must be changed to Install Mode.

HID ordering codes

For legacy readers configuration cards may be required to configure OSDP readers. The ordering codes for HID configuration cards for HID OSDP version 2 readers are shown in Table 3 below.

Table 3: HID configuration card ordering codes

Address	Ordering code
0	SEC9X-CRD-B-00
1	SEC9X-CRD-B-01
2	SEC9X-CRD-B-02
3	SEC9X-CRD-B-03
4	SEC9X-CRD-B-04
5	SEC9X-CRD-B-05

Address	Ordering code
6	SEC9X-CRD-B-06
7	SEC9X-CRD-B-07
8	SEC9X-CRD-B-08
9	SEC9X-CRD-B-09
10	SEC9X-CRD-B-10
11	SEC9X-CRD-B-11
12	SEC9X-CRD-B-12
13	SEC9X-CRD-B-13
14	SEC9X-CRD-B-14
15	SEC9X-CRD-B-15

Aperio

The Aperio® protocol is a short distance wireless communication protocol designed to link an access control system with an Aperio enabled mechanical lock.

A single Aperio hub can be connected to each local bus on the NAC. Refer to the *TS1067E Network Access Controller Installation Manual* for instructions.

Note: Aperio has a fixed baud rate of 19200 baud.

Aperio device addresses

An Aperio lock is addressed in the NAC via its EAC (Electronic Access Control) number, which can be found in the Aperio Programming Application. In CTPlus there is a field for the EAC number in the Assign RAS form when assigning the RAS to the NAC.

Aperio locks can contain all or a subset of the following items that can be referred to directly by the NAC.

- card reader
- keypad
- mechanical lock output
- door input
- egress input (via the handle)
- “activator” button, sometimes referred to as a privacy button.

When referring to these items in CTPlus, please follow the guidelines in the “SALLIS” section on page 19.

The Aperio reader, input and output, will be referred to by the RAS number of the lock.

Aperio lock events

The following Aperio lock events can be reported by the NAC.

- Battery flat
- Battery low
- Battery OK
- Reader offline
- Reader online
- Lock jammed

SALLIS

The SALLIS protocol enables you to link wirelessly to a SALLIS enabled mechanical lock.

A single SALLIS RS485 router can be connected to each local bus on the NAC.

Refer to the *SALLIS Installation & Maintenance Guide* for information on configuring the router and the rest of the SALLIS system.

Note: SALLIS has a fixed baud rate of 38400 baud.

SALLIS device addresses

Each SALLIS lock address can be configured using the SALLIS Application via the Portable Programmer Device. The configured address will be used by the NAC to address the SALLIS lock.

SALLIS locks can contain a reader, a lock and a keypad (if supported). When referring to these items in CTPlus, please follow the guidelines below. The SALLIS reader, input and output, will be referred to by the RAS number of the lock.

SALLIS lock events

The following SALLIS lock events can be reported by the NAC.

- Battery low
- Battery OK
- Reader offline
- Reader online
- Forced door; the lock uses its own hardware and internal logic to determine if the door is open.
- Forced door end
- DOTL (Door Open Too Long); at the time of writing, the DOTL time is a fixed value set in the SALLIS lock.

Flexible device locations

With the Network Access Controller, there is flexibility in how devices such as inputs, relays and readers can be physically wired up to the NAC and how they are addressed.

Devices can be connected directly to the NAC or can be connected to DGPs or RASs on one of the NAC's buses. Thus, when programming the NAC, devices are not addressed by their number alone, but must be defined according to how they have been physically wired up to the NAC.

When specifying a device attached to the NAC in CTPlus, the operator must enter information in location fields that look like the following:

Location	Address	Device number
None		

The fields are defined as follows:

1. **Location** – select the device's location from the following options:
 - *Onboard* – The device is connected directly to the NAC's onboard terminals (or a relay on an attached relay controller). Enter the device's number in the **Device number** field.
 - *DGP* – The device is connected to a DGP that is connected to one of the NAC's buses. Enter the address of the DGP in the **Address** field, and the device's number on the DGP in the **Device number** field. The DGP must be assigned to the NAC and polled on the bus.
 - *RAS* – The device is a RAS, or is an input or relay connected to a RAS, which is connected to one of the NAC's buses. Enter the address of the RAS in the **Address** field. The RAS must be assigned to the NAC and polled on the bus.
2. **Address** – if the device is connected to a DGP or RAS that is connected to one of the NAC's local buses, then the address of the DGP or RAS must be specified.

DGP addresses from 1 to 15 are defined to be on Bus 1, and DGP addresses from 17 to 32 are defined to be on Bus 2. (The DGP with address 16 is the NAC itself.)

Similarly, RAS addresses from 1 to 16 are defined to be on Bus 1, and RAS addresses from 17 to 32 are defined to be on Bus 2.

There can be 31 DGPs and 32 RASs attached to the NAC.

3. **Device number** – the device number (address) of the device attached to the RAS, DGP, or NAC.

Note: The four onboard lock relays are treated as the first four relay numbers assigned to the NAC. If a relay is connected to the NAC via an attached relay controller board, then the relays are numbered from 5 onward. The number of relay controller boards must be configured on the *NAC options* tab of the **DGPs** form. See the “Relay controllers” option on page 49.

Note: If the **Location** is set to *RAS* or *DGP*, then the RAS or DGP must be assigned to the NAC using the *Assigned RAS* or *Assigned DGP* tab of the **DGPs** form, respectively, and must be polled. See the “Assigning RASs” section on page 53, and the “Assigning DGPs” section on page 55 for more information.

Device locations example

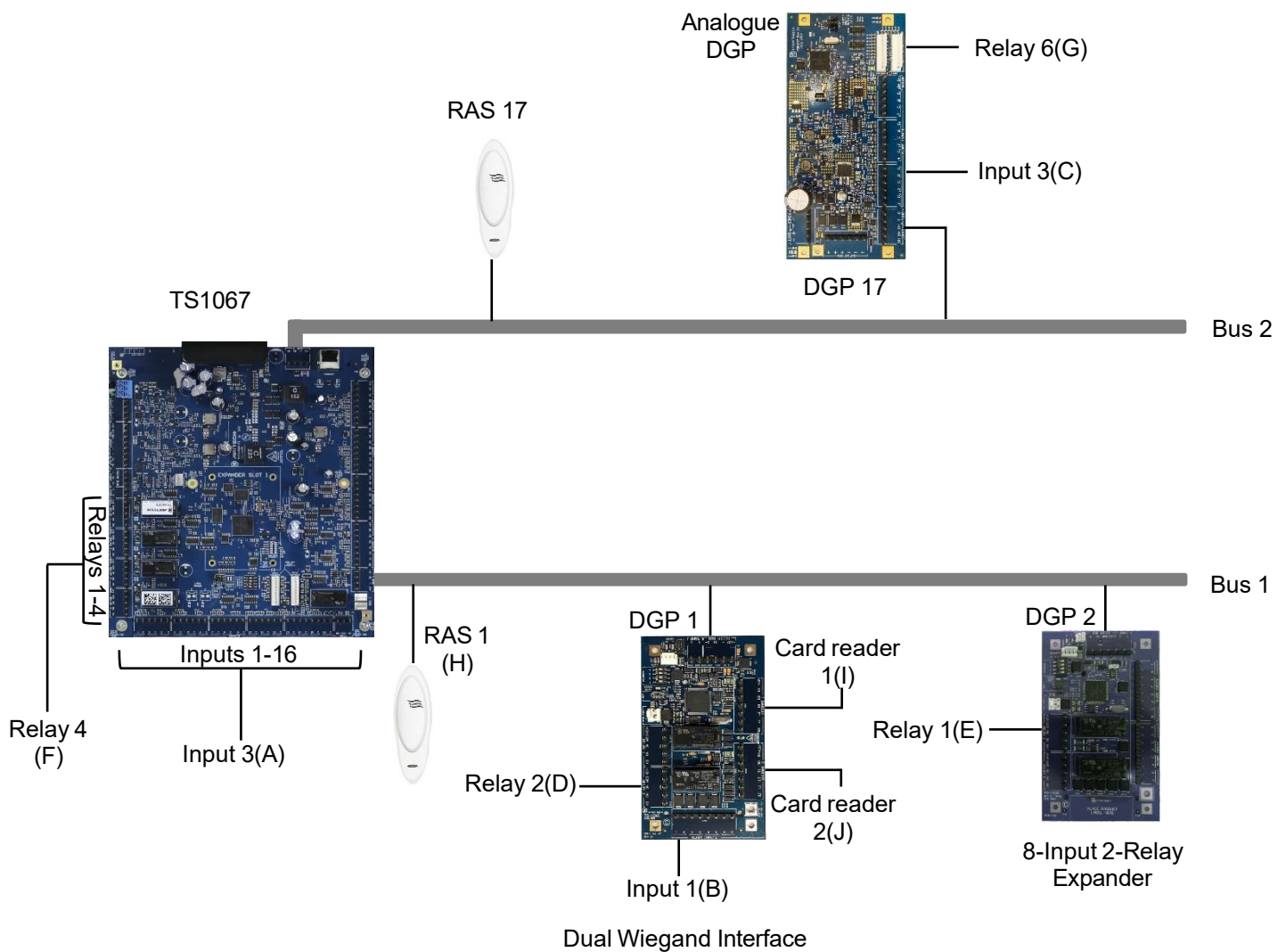
The following example demonstrates the flexibility of specifying devices on the NAC and on RASs or DGPs attached to its local buses, using a single door’s attributes (inputs, relays, and readers). In this example, both local buses use the Tecom protocol.

A single door can have two door inputs, an egress input, two lock relays, a DOTL relay, a forced door relay, a warning relay, and up to six assigned readers. The diagram in Figure 4 on page 22 shows devices attached to the NAC and RASs/DGPs attached to its local buses that must be configured for use with the door. Table 4 below shows how an operator would specify the device locations when configuring the door.

Table 4: Door example

Door 1 device	Location	Address	Device	Figure reference
Door input 1	Onboard	-	3	(A)
Door input 2	DGP	1	1	(B)
Egress input	DGP	17	3	(C)
Lock relay 1	DGP	1	2	(D)
Lock relay 2	DGP	2	1	(E)
DOTL relay	Onboard	-	4	(F)
Warning relay	DGP	17	6	(G)
Assigned reader 1	RAS	1	1	(H)
Assigned reader 2	DGP	1	1	(I)
Assigned reader 3	DGP	1	2	(J)

Figure 4: Device locations example



Input and relay mapping

Note: Input and relay mapping does not apply to the NAC in IP Direct mode.

If the Network Access Controller is attached to a Challenger*Plus* panel, then the NAC can present up to 32 inputs for the Challenger*Plus* to respond to and up to 16 relays for the Challenger*Plus* to activate, without complex use of macros or other programming.

While the controller is being used in conjunction with the Challenger*Plus* panel, the user will have access to the onboard inputs 1-16. This can be further expanded to onboard inputs 17-32 by connecting up to two input expanders to the NAC, input expander address 2 allows the use of inputs 17-24 and input expander 3 will provide access to inputs 25-32.

Note: Addressing any input expanders with address 1 will cause a conflict with inputs 9-16.

These inputs and relays must be configured in the NAC via input and relay mappings. The Challenger*Plus* must also be programmed with additional inputs and relays, with their numbering depending on the NAC's address (set via its DIP switches) and which Challenger*Plus* system LAN the NAC is attached to.

Input mapping

Each input presented to the Challenger*Plus* can reflect the sealed or unsealed state of an input attached to the NAC (either directly onboard, or attached to a DGP or RAS on one of its buses), or can reflect the state of a NAC door (e.g. a Forced door condition).

An **input mapping** must be set up in the NAC to map the state of the input or door to an input number in the range 1 to 32.

Each mapped input has a type, which may be one of the following:

- **Not used** – the input always reports as sealed. This type of input cannot be assigned to a door.
- **Forced** – the input is a logical input associated with a door and is unsealed when the door has a Forced Door alarm (from the door's **Door input 1** being unsealed) or there is a tamper condition.
- **Egress** – the input is a logical input associated with a door and is unsealed when the door is in egress condition (i.e. the door's **Egress input** is unsealed) or there is a tamper condition.
- **DOTL** – the input is a logical input associated with a door and is unsealed when the door has a Door Open Too Long (DOTL) alarm (from the door's **Door input 1** being unsealed).
- **Shunted pass through** – the input is a physical input which is passed through to the Challenger*Plus* panel if the associated door is not shunting.
- **Direct pass through** – the input is a physical input which is passed directly through to the Challenger*Plus* panel. This type of input cannot be assigned to a door.

Note: NAC inputs are masked from the Challenger*Plus* if they are not mapped.

Input mapping is programmed in CTPlus on the *Input/Relay mapping* tab of the **DGPs** form for the NAC. See the “Programming input and relay mapping” section on page 99 for instructions.

Since the NAC can have flexible device locations, any physical input must be programmed using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Shunted pass through operation

When the door is shunting, and the input goes unsealed, the input will not pass through, i.e. the Challenger*Plus* will see the input as remaining sealed.

If the door shunt expires for any reason (Forced or DOTL), and the input is unsealed, the NAC will pass through the input state to the Challenger*Plus* panel.

If the input unseals when the door is not shunted, or the door is in alarm, the input will pass through and report the unsealed state to the Challenger*Plus* panel.

If the input is unsealed when the door shunt starts, the Challenger*Plus* panel will not see a change in the input state.

A tamper on these inputs will be passed through to the Challenger*Plus* panel immediately regardless of the shunt state.

Relay mapping

Each relay presented to the Challenger*Plus* is a direct map of a relay attached to the NAC (either directly onboard, or attached to a DGP or RAS on one of its buses).

A **relay mapping** must be set up in the NAC to map the relay to a relay number in the range 1 to 16. Activating the Challenger*Plus* relay number will activate the specified relay attached to the NAC.

Note: The controller has a bell relay that is defined as onboard relay 512. This relay can be treated as an additional output.

Each mapped relay has a type, which may be one of the following:

- **Disabled** – the relay is not mapped to a physical relay. The relay may be used as an input to a macro.
- **Direct map** – the relay is directly mapped to a physical relay attached to the NAC.

Relay mapping is programmed in CTPlus on the *Input/Relay mapping* tab of the **DGP**s form for the NAC. See the “Programming input and relay mapping” section on page 99 for instructions.

Since the NAC can have flexible device locations, any physical input must be programmed using the scheme described in the “Flexible device locations” section on page 20.

Challenger*Plus* input and relay numbering

Challenger*Plus* allocates 32 inputs and 16 relays per DGP address. To allow Challenger*Plus* to utilise the maximum possible number of inputs and relays on a NAC, up to 32 mapped inputs and up to 16 mapped relays can be configured on the NAC.

Note: The input and relay mappings are specific to each NAC. Additional NACs require additional mappings of inputs and relays.

The mapped input and relay numbers are indexes into the Challenger*Plus* panel’s device numbering scheme, which depends on the NAC’s address (set via its DIP switches) and which Challenger*Plus* system LAN it is attached to.

NACs may use the first 12 addresses on each Challenger*Plus* system LAN. Table 5 on page 25 lists the LAN number, the address of the NAC (set via the

NAC's DIP switches), the DGP number that the NAC is polled as, and the ranges of Challenger*Plus* input and relay numbers.

Table 5: Challenger*Plus* inputs and relays per DGP address

Challenger <i>Plus</i> LAN	Address	Polled as	Challenger <i>Plus</i> inputs	Challenger <i>Plus</i> relays
LAN 1	1	DGP 1	17 to 48	17 to 32
LAN 1	2	DGP 2	49 to 80	33 to 48
LAN 1	3	DGP 3	81 to 112	49 to 64
LAN 1	4	DGP 4	113 to 144	65 to 80
LAN 1	5	DGP 5	145 to 176	81 to 96
LAN 1	6	DGP 6	177 to 208	97 to 112
LAN 1	7	DGP 7	209 to 240	113 to 128
LAN 1	8	DGP 8	241 to 272	129 to 144
LAN 1	9	DGP 9	273 to 304	145 to 160
LAN 1	10	DGP 10	305 to 336	161 to 176
LAN 1	11	DGP 11	337 to 368	177 to 192
LAN 1	12	DGP 12	369 to 496	193 to 208
LAN 2	1	DGP 17	497 to 528	257 to 272
LAN 2	2	DGP 18	529 to 560	273 to 288
LAN 2	3	DGP 19	561 to 592	289 to 304
LAN 2	4	DGP 20	593 to 624	305 to 320
LAN 2	5	DGP 21	625 to 656	321 to 336
LAN 2	6	DGP 22	657 to 688	337 to 352
LAN 2	7	DGP 23	689 to 720	353 to 368
LAN 2	8	DGP 24	721 to 754	369 to 384
LAN 2	9	DGP 25	753 to 784	385 to 400
LAN 2	10	DGP 26	785 to 816	401 to 416
LAN 2	11	DGP 27	817 to 848	417 to 432
LAN 2	12	DGP 28	849 to 880	433 to 448

In order for Challenger*Plus* to utilise the mapped inputs and relays, you must also program the Challenger*Plus* input and relays. See the “

Programming mapped inputs and relays” section on page 102 for instructions.

Configuring the Auxiliary SW output

By default the AUX SW output is ON, however it can be controlled by the onboard output 511. If nothing has been configured to the output then AUX SW will stay ON, but if it has been configured the AUX SW will follow the state of output 511.

Overriding door state

In addition to being able to define an override time zone for a door, there are additional methods for overriding a door's default state. These methods are:

- **Door schedules** (see the "Door schedules" section below).
- **User defined time zones** (see the "User defined time zones" section on page 28).

Door state priorities

The priorities for controlling the state of a door are as follows, from highest to lowest priority:

1. Direct control from management software, e.g. an operator sends a door open/unlock command.
2. User access, e.g. a user badges their card at a door's card reader.
3. The door's schedule, set using management software.
4. The door's programmed override time zone (which uses an installer-defined panel time zone), set using configuration software such as CTPlus, or the door's override (set using management software).

Door schedules

Up to 100 **door schedules** can be programmed in the NAC, allowing for very flexible door locking and unlocking schedules.

Door schedules have an **active period** (set via a **start date** and an optional **end date**). If no end date is set, then the active period is for the start date only. You can also specify if the door schedule is active on particular days of the week (and/or holidays) during the active period.

Door schedules must be configured with a **start time** for when the **start action** (e.g. door unlock) will be executed.

Start actions can be either **timed** or **immediate**:

- Timed actions have an **action duration** that can be configured from 1 second to 366 days. The door will remain in the state defined by the start action for the action duration.

If the door's state is overridden (e.g. by management software or a user badging a card), then at the conclusion of the overriding state, the door will revert to the state defined by the start action. At the end of the active duration, the **end action**, if defined, will be executed.

If no end action is defined, then the door will revert to its default state.

- If no action duration is configured, then the start action is immediate. The door will remain in the state defined by the start action.

If the door's state is overridden (e.g. by management software or a user badging a card), then at the conclusion of the overriding state, the door

will revert to its default state. The start action will no longer have any bearing on the state of the door.

The possible door actions, which can be configured to execute at the start time or the end time, are:

- **Unlock**
- **Lock**
- **Disable**
- **Enable**

Door and lift schedules are programmed in CTPlus on the **Door/lift schedule action** form. See the “Configuring door/lift schedules” section on page 115 for instructions.

Note: With reference to the priorities for overriding a door’s state (see the “Door state priorities” section on page 26), a door schedule’s end action has a lower priority than any override time zone in effect, unless the end action is to disable the door.

Note: A door schedule will not override the operation of a door schedule that has already started.

Note: Door schedules that have reached the end of their active period can be deleted via management software.

Door Unlock action

If the start action is Unlock, then the door will unlock at the start time and remain unlocked for the specified action duration (or indefinitely if there is no action duration configured).

During this time if an existing override time zone ends (either the door’s programmed override time zone, or the operator-defined door override), then the door will remain unlocked.

When the action duration has completed, the end action will occur. However, if the start action ends and an existing override time zone is active (either the door’s programmed override time zone, or the operator-defined door override), then the door will remain unlocked.

A manual lock command sent from management software will lock the door and cancel the start action.

If the door has “Override after entry” enabled (see the “Override after entry” section on page 79), the door will not unlock until a valid user PIN or card is presented at the door.

Door Lock action

If the start action is Lock, then the door will lock at the start time and remain locked for the specified action duration (or indefinitely if there is no action duration configured).

During this time if an existing override time zone becomes active (either the door's programmed override time zone, or the operator-defined door override), then the door will remain locked.

Authorised PIN/card users can open the door as normal.

An unlock command issued from management software will unlock the door and cancel the start action.

An open door or timed open door command issued from management software will perform the function but will not cancel the start action.

Cancelling a start action

A start action that is running can be cancelled by overriding its operation from management software. For example:

- Where a start action is holding the door unlocked, the action can be cancelled by locking the door via management software. The cancellation is only for the current iteration of the door schedule and future iterations will still operate.
- In the case where the door is being unlocked by the start action and an unlock command is sent from management software, the action will continue to operate and is not affected.

When a start action is cancelled, the end action is not performed. The door will return to its default state (locked) if no other override or macro is active.

If a start action that enables the door is cancelled then the door will remain enabled. Similarly, if a start action that disables the door is cancelled then the door will remain disabled.

Deleting a door schedule

When deleting an active door schedule, the start action is immediately cancelled and the cancellation rules described in the "Cancelling a start action" section above apply. Once the running action has been terminated, the door schedule record is removed from the NAC so that no future iterations of the door schedule can occur.

When deleting a door schedule that is not active, the door schedule is immediately deleted and no future iterations of the start action can occur.

User defined time zones

An operator using management software such as TecomC4 can configure an automatic lock/unlock schedule for each door, called a **door override**. The operator can define the override schedule per door without using any of the installer-defined panel time zones. Programming for a door override is similar to the programming for a "hard" panel time zone for a NAC or Challenger*Plus* panel.

Note: If either the door override or an existing door override time zone is active, then the door will be unlocked.

Door overrides are programmed in CTPlus on the **Door/lift** form under the **User defined time zones** tab. See the “Programming user defined time zones” section on page 89 for instructions.

Random lockout time

When the “Door random bit” event triggers on a Network Access Controller door (which can occur if the door’s **Random event %** setting is non-zero), then there is a new setting which locks out the door for a specified amount of time, called **Random % lockout time**. The lockout time can also be specified as indefinite. During this time, the door can only be opened by users with the “Privileged” flag; the door cannot be opened by any other users.

Any LCD RAS attached to the door will display “Locked Out”.

Note: Users with the “Privileged” flag cannot cause a door lockout.

A door’s random lockout time can be programmed in CTPlus on the **Access** tab of the **Doors/Lifts** form. See the “Random % lockout time” section on page 77.

LED area mapping for door readers

Note: LED area mapping does not apply in IP Direct mode.

It is possible to map the LEDs on door readers to specific areas, in the same way as can be done for a Challenger*Plus* RAS.

The LED area mapping is programmed in the **Door reader** dialog, accessed from the **Readers** tab of the **Doors/Lifts** form. See the “Door reader dialog – LED mapping tab” section on page 74.

Overriding lift state

Just like how a door’s default state can be overridden, a lift’s default state can be overridden with these two additional methods:

- **Lift control levels** (see the “Lift Control Levels” section on page 62).
- **Lift override/security group** (see the “Programming lift options” section on page 91).

Lift state priorities

The priorities for controlling the state of a door are as follows, from highest to lowest priority:

1. Direct control from management software, e.g. a command is issued to secure the floor.
2. User access, e.g. a user badges their card at a door’s card reader.
3. Door/lift scheduled action, set using management software.

4. The lift's programmed override and security override time zone, set using configuration software such as CTPlus.

Lift override using Lift control level

Lifts can be assigned up to 10 control levels for each lift, a control level consists of several floors linked to a time schedule, allowing multiple time schedules to be applied to the same set of floors or different time schedules for different floors.

When the time schedule for any assigned lift control becomes active, the floors associated with it become automatically accessed. A "Floor auto accessed" event is reported for each floor that has become "accessed".

When the time schedule for any assigned lift control ends, the floors linked to it will automatically secure and a "Floor auto secure" event is reported for each floor that is secured.

See the "Programming control level options" section on page 98 for instructions.

Lift override using Floor group

The lift is programmed with a floor group in the Lift override group field or the Lift Security group. A floor group consist of several different floors with their own unique time zone. When the time zone on any of the floors becomes active, that floor's state will automatically become accessed and the event "Floor auto accessed" is reported.

When the time zone ends, the floor will automatically become secure and the event "Floor auto secured" is reported.

See the "Programming floor groups" section on page 106 for instructions.

Recommended programming sequence

The following is a suggested programming sequence for a Network Access Controller:

Note: For access restrictions to the interior of the enclosure, refer to APPENDIX B: Enclosure Access Restrictions

1. Set the NAC's DIP switches if the NAC will be connected to a Challenger*Plus* panel.
2. Default the NAC.
3. Connect NAC to Challenger*Plus* (if required).
4. Connect CTPlus to NAC via USB or to the Challenger*Plus* panel, depending on the intended operating mode.
5. Add the NAC as a panel in CTPlus (for IP Direct or IP Extended mode) or add the NAC as a DGP in CTPlus (for Classic mode).
6. Upload the default configuration from the NAC to CTPlus.
7. Upgrade the NAC's firmware to the latest version.
8. Program the NAC's IP communications if the NAC will operate in IP Direct or IP Extended mode. Reconnect to the NAC via IP if desired.
9. Program the NAC:
 - a. Program the NAC's general controller options.
 - b. Assign RASs to the NAC and ensure they are polled.
 - c. Assign DGPs to the NAC and ensure they are polled.
10. Program holidays if required.
11. Program time zones if required.
12. Program regions if required.
13. Program the NAC's doors/lifts:
 - a. Program hardware options for each door.
 - b. Assign readers to each door.
 - c. Program access options for each door.
 - d. Program shunt, passback and egress options for each door.
 - e. Program alarm control for each door, if applicable.
14. Program input and relay mappings for Challenger*Plus*, if applicable.
15. Program the NAC's macro logic, if required.
16. Program user information:
 - a. Program door groups.
 - b. Program floor groups

c. Program users.

The following sections describe each step of the recommended programming sequence above. In the descriptions, CTPlus is used for programming the NAC.

Note: If TecomC4 will be used for management of the NAC, then some aspects of programming should not be done in CTPlus, since TecomC4 will be responsible for those aspects. TecomC4 can be used to configure and manage:

- Holidays
 - Time zones
 - Door and Floor groups
 - Users
-

In addition to the initial setup and programming of the NAC, ongoing management can be performed via management software.

For information on management via TecomC4, refer to the *TecomC4 Operators Manual*.

For information on management via CTPlus, see the “Management via CTPlus” section on page 109.

DIP switches

If the Network Access Controller will be connected to a Challenger*Plus* (i.e. the NAC will operate in IP Extended or Classic mode), then set the NAC’s address using the DIP switches on the NAC. Refer to the *TS1067E Network Access Controller Installation Manual* for instructions.

Note: On a Challenger*Plus* system LAN 2, DIP switch addresses 1 to 12 are used for NACs that are polled as 17 to 28.

Defaulting the NAC

Refer to the *TS1067E Network Access Controller Installation Manual* for instructions on defaulting the Network Access Controller.

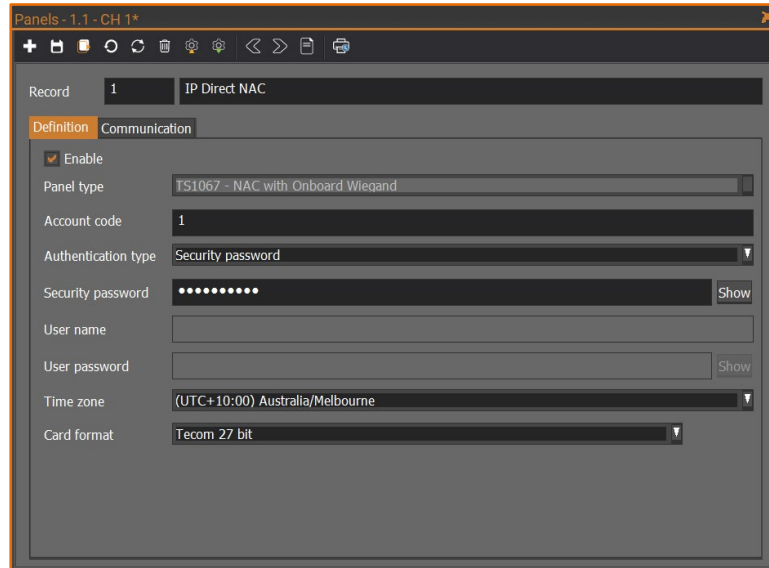
CTPlus connection

The following sections describe how to connect to the NAC.

Connecting NAC in IP Direct mode

Firstly, connect CTPlus to the NAC using USB by following these steps:

1. Connect the NAC to the CTPlus computer using a USB cable.
2. In CTPlus, click the **Panels**  button on the *Panel programming* ribbon tab to open the Panels form.
3. On the Panels form, click the **New**  button in the toolbar to add a new panel record.



The screenshot shows the 'Panels - 1.1 - CH 1*' window. The 'Record' field is set to '1' and 'IP Direct NAC'. The 'Definition' tab is selected, showing the 'Communication' section. The 'Enable' checkbox is checked. The 'Panel type' is set to 'TS1067 - NAC with Onboard Wiegand'. The 'Account code' is '1'. The 'Authentication type' is 'Security password'. The 'Security password' field is masked with dots and has a 'Show' button. The 'User name' and 'User password' fields are empty, with a 'Show' button for the password. The 'Time zone' is set to '(UTC+10:00) Australia/Melbourne'. The 'Card format' is set to 'Tecom 27 bit'.

1. Enter a description for the NAC connection in the **Record** description field.
2. On the *Definition* tab, enable the panel connection by ticking the **Enable** check box.
3. Set the **Panel type** to be *TS1067 – NAC with Onboard Wiegand*.
4. Set the **Time zone** and **Card format** fields as required.
5. Click the **Save**  button in the toolbar to save the NAC panel record.

CTPlus will connect to the NAC via USB.

CTPlus automatically creates a new DGP record associated with the NAC (DGP number 16), allowing you to configure the options for the NAC. See Status and control section for more details depending on the operating mode of NAC.

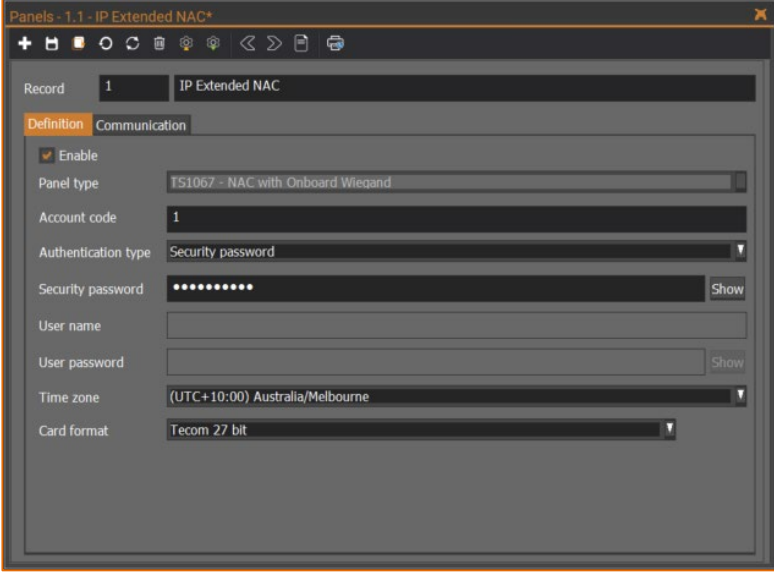
If desired, you can set up IP communications on the NAC and reconnect CTPlus to the NAC using IP instead of USB. See the Programming IP communications section on page 43.

Connecting NAC in IP Extended mode

Firstly, connect the NAC to the Challenger*Plus* panel's LAN 1 or LAN 2, as required.

Secondly, connect CTPlus to the NAC using USB by following these steps:

1. Connect the NAC to the CTPlus computer using a USB cable.
2. In CTPlus, click the **Panels**  button on the *Panel programming* ribbon tab to open the Panels form.
3. On the Panels form, click the **New**  button in the toolbar to add a new panel record.



The screenshot shows the 'Panels - 1:1 - IP Extended NAC*' window. The 'Record' field is set to '1' and the description is 'IP Extended NAC'. The 'Definition' tab is active, showing the following fields: 'Enable' (checked), 'Panel type' (TS1067 - NAC with Onboard Wiegand), 'Account code' (1), 'Authentication type' (Security password), 'Security password' (masked with dots and a 'Show' button), 'User name' (empty), 'User password' (empty with a 'Show' button), 'Time zone' ((UTC+10:00) Australia/Melbourne), and 'Card format' (Tecom 27 bit).

4. Enter a description for the NAC in the **Record** description field.
5. On the *Definition* tab, enable the panel connection by ticking the **Enable** check box.
6. Set the **Panel type** to be *TS1067 – NAC with Onboard Wiegand*.
7. Set the **Time zone** and **Card format** fields as required.
8. Click the **Save**  button in the toolbar to save the NAC panel record.
9. CTPlus will connect to the NAC via USB.

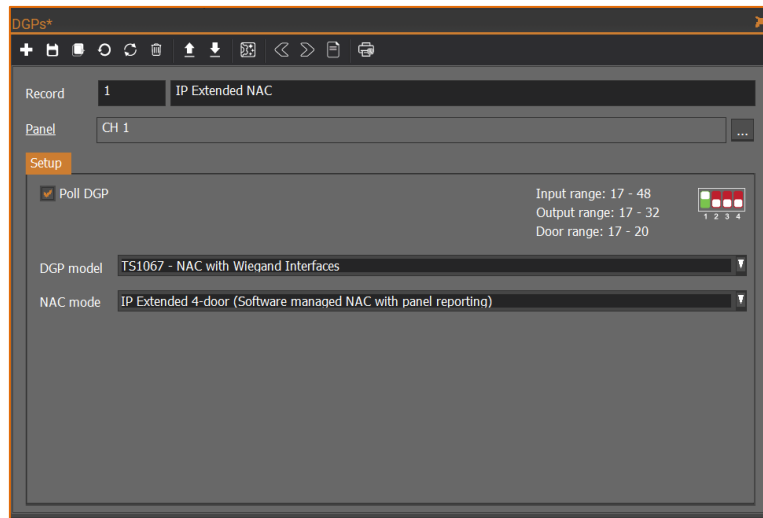
CTPlus automatically creates a new DGP record associated with the NAC (DGP number 16), allowing you to configure the options for the NAC.

CTPlus automatically creates four doors for the NAC. Four additional doors can be added for the NAC on the Doors/Lifts form.

Finally, add a DGP representing the NAC to an existing Challenger*Plus* panel so that alarms can be communicated to the Challenger*Plus* panel. Using CTPlus, follow these steps:

1. Connect CTPlus to the Challenger*Plus* panel. See the *CTPlus Operators Manual* or CTPlus online help for more information.

2. Click the **DGPs**  button on the *Panel programming* ribbon tab to open the DGPs form. Note that there is an existing DGP record for the NAC itself (DGP 16 on the NAC).
3. On the DGPs form, click the **New**  button in the toolbar to add a new DGP record.



The screenshot shows the 'DGPs+' window with the following configuration:

- Record:** 1, IP Extended NAC
- Panel:** CH 1
- Setup:**
 - ☒ Poll DGP
 - Input range: 17 - 48
 - Output range: 17 - 32
 - Door range: 17 - 20
 - DGP model: TS1067 - NAC with Wiegand Interfaces
 - NAC mode: IP Extended 4-door (Software managed NAC with panel reporting)

4. Enter the number the NAC will be polled as in the **Record** number field (1 to 12 if the NAC is connected to the Challenger*Plus* system LAN 1, or 17 to 28 if the NAC is connected to LAN 2).
5. Enter a description for the NAC in the **Record** description field.
6. Ensure the **Panel** field is set to the Challenger*Plus* panel that the NAC is connected to via its system LAN. If necessary, click the **Browse**  button next to the **Panel** field to select the Challenger*Plus* panel.
7. On the *Setup* tab, tick the **Poll DGP** check box.
8. Set the **DGP model** to be *TS1067 – NAC with Wiegand Interfaces*.
9. Set the **NAC mode** to be *IP Extended 4-door*.
10. Click the **Save**  button in the toolbar to save the DGP record.

The NAC is now connected to the Challenger*Plus* panel as well as CTPlus.

See Status and control section for more details depending on the operating mode of NAC.

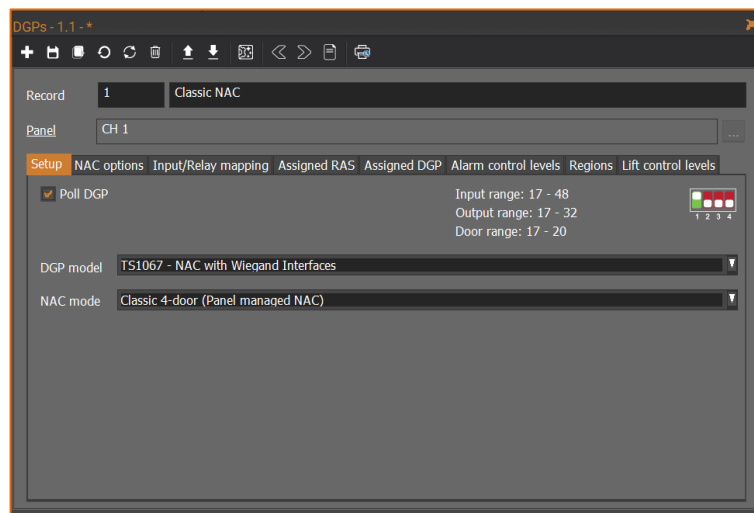
If desired, you can set up IP communications on the NAC and reconnect CTPlus to the NAC using IP instead of USB. See the Programming IP communications section on page 43.

Connecting NAC in Classic mode

Connect the NAC to the Challenger*Plus* panel's LAN 1 or LAN 2, as required.

Add the NAC as a new DGP to an existing Challenger*Plus* panel. Using CTPlus, follow these steps:

1. Connect CTPlus to the Challenger*Plus* panel. See the *CTPlus Operators Manual* or CTPlus online help for more information.
2. Click the **DGPs**  button on the *Panel programming* ribbon tab to open the DGPs form.
3. On the DGPs form, click the **New**  button in the toolbar to add a new DGP record.



4. Enter the number the NAC will be polled as in the **Record** number field (1 to 12 if the NAC is connected to the Challenger*Plus* system LAN 1, or 17 to 28 if the NAC is connected to LAN 2).
5. Enter a description for the NAC in the **Record** description field.
6. Ensure the **Panel** field is set to the Challenger*Plus* panel that the NAC is connected to via its system LAN. If necessary, click the **Browse**  button next to the **Panel** field to select the Challenger*Plus* panel.
7. On the *Setup* tab, tick the **Poll DGP** check box.
8. Set the **DGP model** to be *TS1067 – NAC with Wiegand Interfaces*.
9. Set the **NAC mode** to be *Classic 4-door*.
10. Click the **Save**  button in the toolbar to save the DGP record.

The NAC is now connected to the Challenger*Plus* panel.

New tabs will appear on the DGPs form to allow the operator to program the NAC.

CTPlus automatically creates four doors for the NAC.

See Status and control section for more details depending on the operating mode of NAC.

Uploading default configuration

It is important to upload the default values from the Network Access Controller into the CTPlus database.

The method for uploading depends on the operating mode of the NAC.

Uploading in IP Direct or IP Extended mode

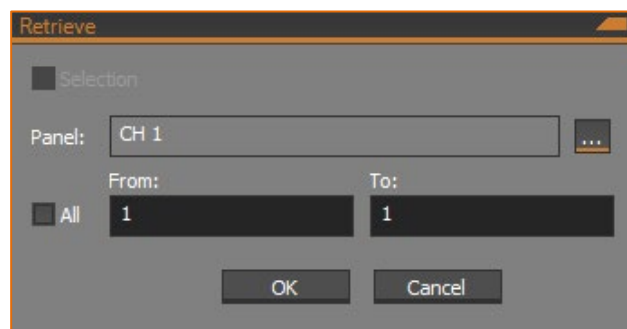
Use one of the following methods to upload the default configuration into CTPlus in IP Direct or IP Extended mode:

- Click the **Panels**  button on the *Panel programming* ribbon tab to open the Panels form. Ensure the currently selected panel record is the NAC. Click the **Upload**  button in the toolbar to upload the configuration from the NAC to CTPlus.
- Click the **Connections**  button on the *Operation* ribbon tab to open the Connections window. Select the NAC from the list of panel connections. Click the **Upload**  button in the toolbar to upload the configuration from the NAC to CTPlus.

Uploading in Classic mode

In Classic mode, you must upload the NAC programming and its door programming separately.

Click the **DGPs**  button to open the DGPs form. Ensure the currently selected DGP record is the NAC. Click the **Retrieve**  button in the toolbar to open the Retrieve dialog:

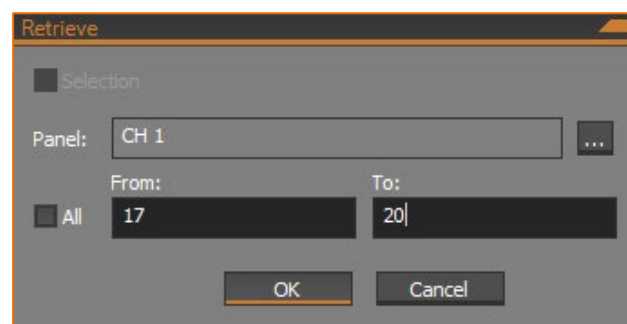


The Retrieve dialog box is shown with the following fields and controls:

- Selection** (checkbox): Unchecked.
- Panel:** CH 1 (text field).
- From:** 1 (text field).
- To:** 1 (text field).
- All** (checkbox): Checked.
- OK** and **Cancel** buttons.

Click the **OK** button to start the upload.

Click the **Doors/Lifts**  button to open the Doors/Lifts form. Click the **Retrieve** button in the toolbar to open the Upload dialog:



The Retrieve dialog box is shown with the following fields and controls:

- Selection** (checkbox): Unchecked.
- Panel:** CH 1 (text field).
- From:** 17 (text field).
- To:** 20 (text field).
- All** (checkbox): Checked.
- OK** and **Cancel** buttons.

Enter the required door numbers in the **From** and **To** fields, and click the **OK** button to start the upload.

Upgrading firmware

Firmware on the Network Access Controller is upgradeable in all operating modes. It is highly recommended that the installer upgrade to the most recent firmware version upon installation.

Note: It is recommended that firmware upgrade be performed via IP or USB where possible, since it is faster than upgrading via a Challenger*Plus* panel.

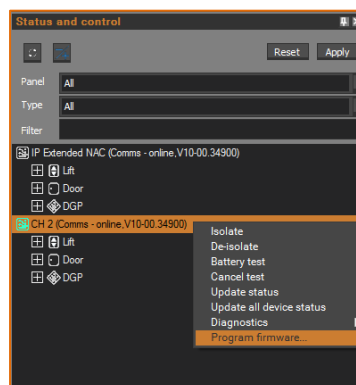
Upgrading firmware

The method for upgrading firmware depends on the operating mode of the NAC.

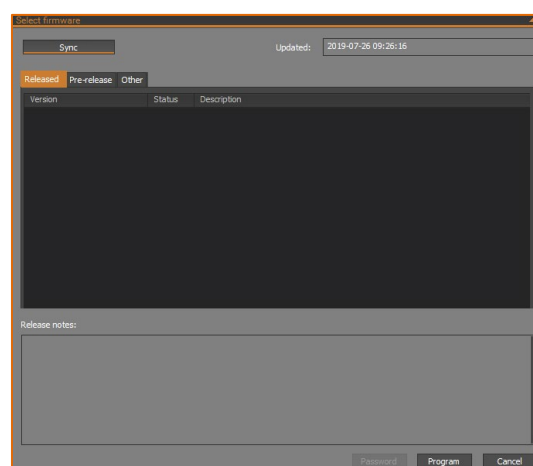
Upgrading firmware in all modes

Follow these steps to upgrade NAC firmware:

1. Click the **Status and Control**  button in the *Operation* ribbon tab to open the Status and Control window.
2. If the NAC is connected in Classic Mode, expand the DGP category under the relevant Challenger*Plus* panel so that the NAC is visible; otherwise, expand the DGP category directly under your NAC connection.
3. Right-click the NAC to open its context menu and select **Program firmware > Panel** from the menu.



4. Click **Sync** button to display the available firmware versions on the server.



5. Select the required firmware file from the list under the Released tab.
6. Check the release notes section related to this version before upgrading.
7. Click **Program** button to upgrade NAC to your desired version.

If you are unable to upgrade the firmware using the above method in case the panel is non-responsive please follow the instructions below as an alternative.

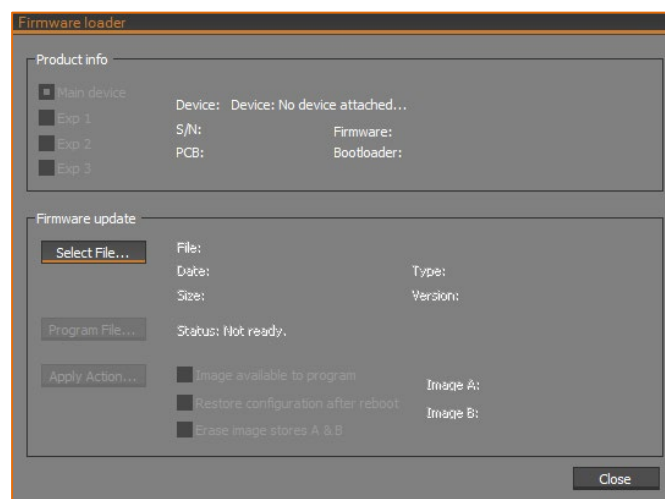
Using the Firmware Loader

This method requires USB connection directly to NAC.

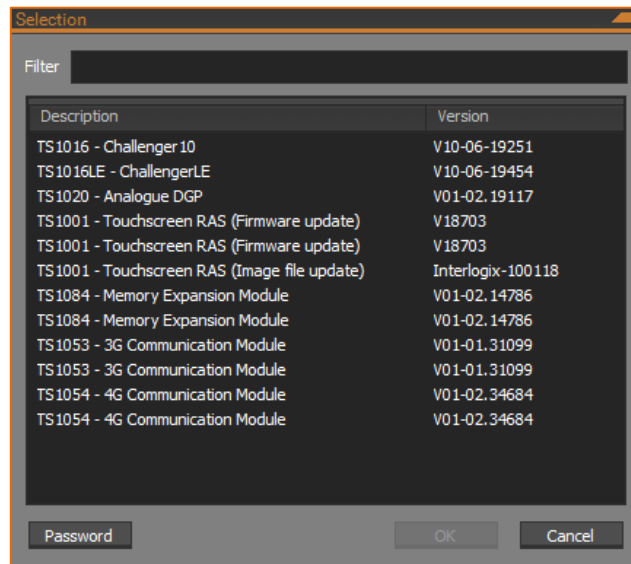
Method

To upgrade the NAC panel firmware:

1. Remove power to the NAC panel and wait for all LEDs to turn off.
2. Fit test links 1 and 2.
3. Reconnect power to the panel.
4. Use the USB cable to connect the computer to the NAC panel's USB port.



5. In CTPlus, select Administration -> Firmware loader from Navigation bar to open the Firmware Loader form.
6. When running, it will tell you if the device is ready otherwise you can't program a file.
7. Ensure that the Product Info section displays the information of the Device, S/N, Firmware, PCB and Bootloader.
8. Under the Firmware update section, click on **Select File** button.



8. Selection form pops up. And then choose the firmware file to be programmed. If no file is available for selection, ensure you are online and click on Administrator ->Sync firmware from the Navigation bar in CTPlus. Once the Sync is complete, try this step again.
9. Ensure that the Firmware update section displays the information of the File, Date, Type, Size and Version.
10. Click **Program File** button to send the firmware file to the panel. The process will take several minutes. The percentage completion displays in the Status text. When finished, a "Programming is complete" message displays.
11. Remove the USB cable from the NAC panel.
12. Remove power to the NAC panel and wait for all LEDs to turn off.
13. Remove test links 1 and 2.
14. Reconnect power to the panel.

Licensing Functionality

The Network Access Controller allows for adjustments to the supported numbers of users and doors through the use of a license system.

License Capacity

The license will be able to set the following capacities:

Expand from 4 doors (default) to 8 doors

Expand from 2,000 users (default) to:

- 65,535 users or
- 250,000 users

User and operating limits will be applied to existing operating modes of the device.

Once the product has received an upgrade to any capacities it will not be possible to reduce or downgrade its expansions, even if a different license of a lower setting is issued.

For example, a TS1067E board that has a licensed capacity for 8 doors has a new license issued that enables 65,535 users and 4 doors, the result will be a controller that has 65,535 users and 8 doors. The 4 door limit that comes with the second license is ignored in this case.

Note: If a TS1067E board is already licensed for 8 door operation and is being added to the Challenger Plus panel for the first time, it will have to be configured to 4-Door NAC mode the first time the DGP record is created. When the TS1067E DGP goes online, 8-Door mode will be automatically enabled. The user will then have to change the NAC mode to 8-Door and save the changes made.

User Limits

If the maximum user limit has been reached, any additional users downloaded will not be stored in the device. Existing users can be modified or deleted while the maximum limit is in use.

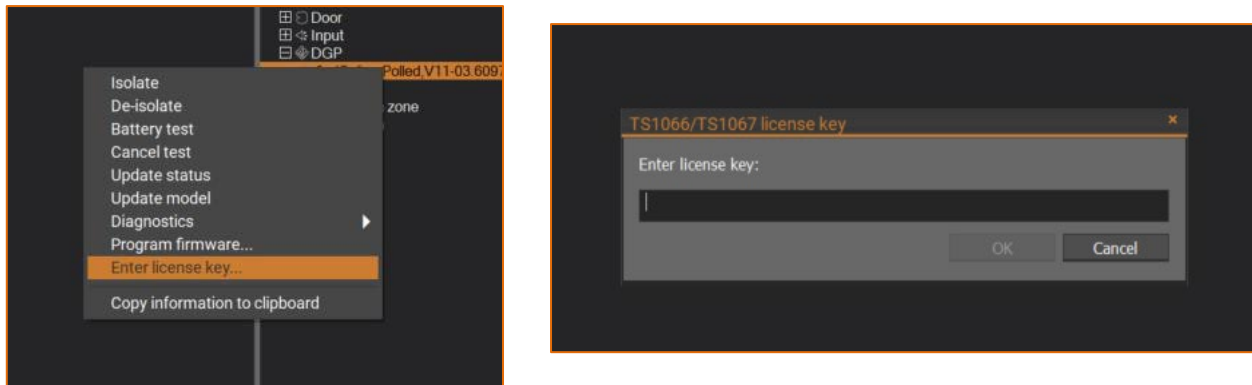
Factory Default's impact on licenses

The TS1067E has the default factory settings of 2,000 users and 4 doors. Once a license has been applied, performing a factory default procedure will not modify the licensed capacity of the product. For example, if the controller is licensed for 65,535 users, this limit will be retained after a full factory default.

Applying the License

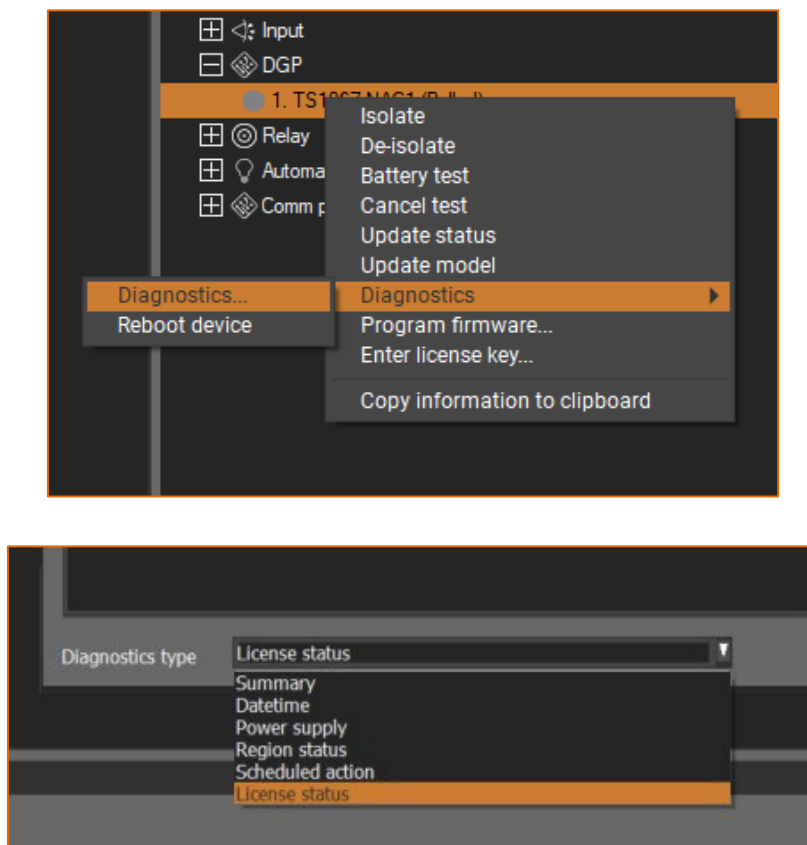
To get a license for the NAC, you will need to fill in the online license form found at <https://www.aritech.com.au>, the TS1067E's serial number will be required for this form. Once processed, a license key will be provided to you from your Tecom distributor. Open up CTPlus and access the system that has the T1067E NAC connected, go to the **Status and control** panel, right click on the NAC and select "Enter license key".

A new pop up window will then appear where the license key can be entered.



Checking License status

To look into the status of the TS1067's license, right click on the NAC in the **Status and control** panel and select "Diagnostics", a new window will appear and at the bottom of the window select License status from the drop down menu.



Programming IP communications

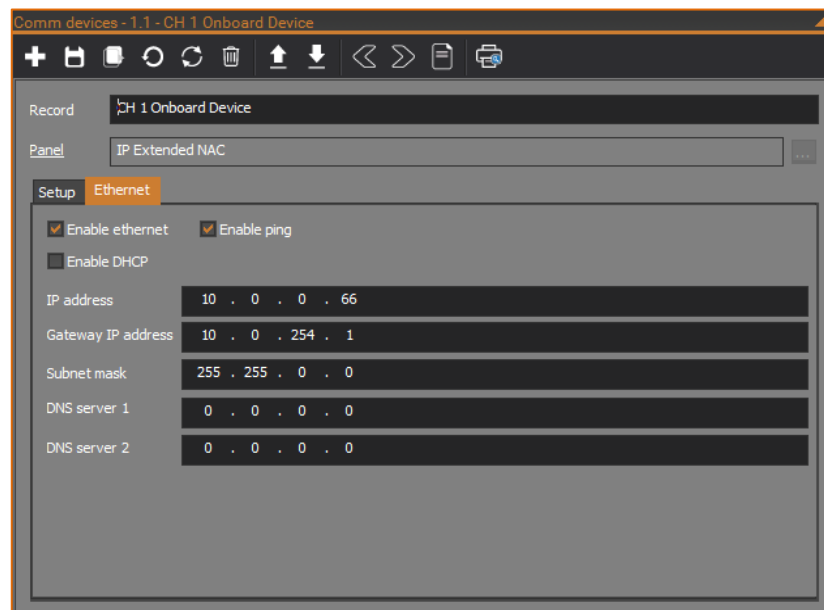
If the Network Access Controller is operating in IP Direct or IP Extended mode, then set up IP communications on the NAC.

Once IP communications have been configured on the NAC, you can reconnect CTPlus to the NAC using IP instead of USB, if desired.

Configuring Ethernet

Configure Ethernet communications on the NAC. Using CTPlus, follow these steps:

1. Click the **Communications**  button on the *Panel programming* ribbon tab and select **Comm devices** to open the Comm devices form.
2. Select the NAC's onboard communications device record (ensure the record's associated **Panel** field matches the NAC panel).
3. On the *Ethernet* tab, set up the Ethernet settings for the NAC (i.e. **IP address** and **Subnet mask**). Ensure that the **Enable Ethernet** check box is ticked.



Field	Value
Record	CH 1 Onboard Device
Panel	IP Extended NAC
Enable ethernet	☒
Enable ping	☒
Enable DHCP	☐
IP address	10 . 0 . 0 . 66
Gateway IP address	10 . 0 . 254 . 1
Subnet mask	255 . 255 . 0 . 0
DNS server 1	0 . 0 . 0 . 0
DNS server 2	0 . 0 . 0 . 0

4. Click the **Save**  button in the toolbar to save the Comm device record.

Configuring communications path

Configure an IP communications path on the NAC for management software. Using CTPlus, follow these steps:

1. Click the **Communications**  button on the *Panel programming* ribbon tab and select **Comm paths** to open the Comm paths form.

2. Select one of the NAC's communications paths, e.g. communications path 3 (ensure the record's associated **Panel** field matches the NAC panel).

Comm paths - 1.3 - MANAGEMENT SOFT

Record: 3 | MANAGEMENT SOFT

Panel: IP Extended NAC

Main | Connection control | Filter | Test calls | Dial settings | IP/Encryption settings | Advanced settings | Authentication

Interface location: On Board | Interface port: Ethernet

Format: Computer Event Driven | Sub-format:

Backup for path: | Account code: 1

Security password: | Show | Path priority: 0

☒ Enable

3. On the *Main* tab, tick the **Enable** check box to enable the path.
4. Configure any other settings required, such as **Account code** and **Computer password**.
5. On the Comm Paths form, click the **Config Wizard** button in the toolbar to set the IP address and Send/Receive port of the management software computer.

Comm paths - 1.3 - MANAGEMENT SOFT

Record: 3 | MANAGEMENT SOFT

Panel: IP Extended NAC

Main | Connection control | Filter | Test calls | Dial settings | IP/Encryption settings | Advanced settings | Authentication

Interface location: On Board | Interface port: Ethernet

Format: Computer Event Driven | Sub-format:

Backup for path: | Account code: 1

Security password: | Show | Path priority: 0

☒ Enable

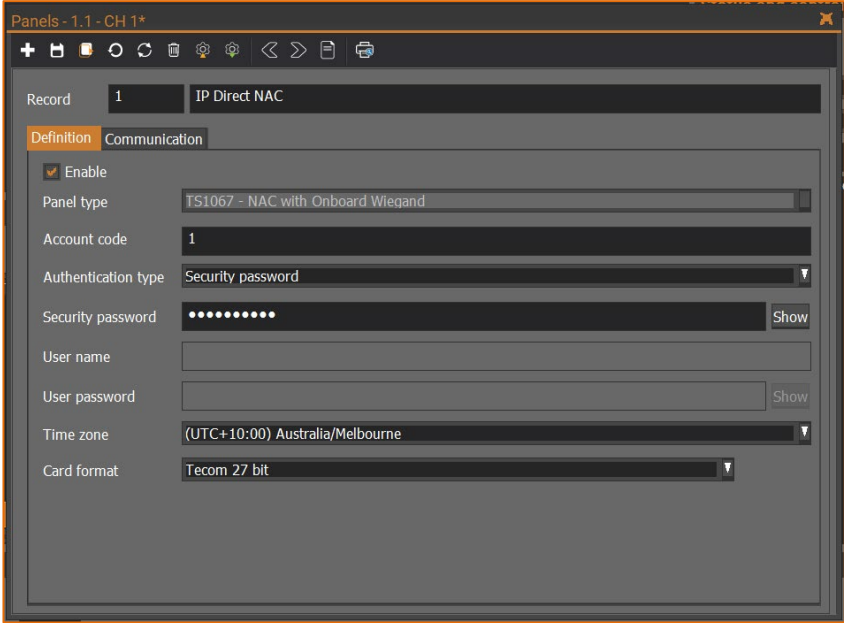
6. Click the **Save** button in the toolbar to save the Comm path record.

The configured communications path can be used by CTPlus for further configuration and management, or by TecomC4 for management. If required, set up additional communications paths by repeating the steps in this section with a different communications path.

Connecting CTPlus to NAC via IP

If desired, reconfigure the NAC panel record to use Ethernet communications instead of USB. Using CTPlus, follow these steps:

1. Connect the NAC to the CTPlus computer using an Ethernet cable.
2. Click the **Panels**  button on the *Panel programming* ribbon tab to open the Panels form.
3. On the Panels form, select the NAC panel.
4. On the *Definition* tab, ensure the **Account code** is set to the communication path's **Account code**, the **Authentication type** is set to *Security password*, and the **Security password** is set to the communication path's **Computer password**.



Panels - 1.1 - CH 1*

Record: 1 IP Direct NAC

Definition Communication

☒ Enable

Panel type: TS1067 - NAC with Onboard Wiegand

Account code: 1

Authentication type: Security password

Security password: Show

User name:

User password: Show

Time zone: (UTC+10:00) Australia/Melbourne

Card format: Tecom 27 bit

5. On the *Communication* tab, configure the Ethernet communications settings as required. Set the **Type** to *UDP/IP*. Set the **IP address** to the **IP address** configured for the NAC's onboard communications device. Set the **Port** to the **Send port/Receive port** configured for the communications path. Configure encryption if required.

The screenshot shows the 'Panels - 1.1 - CH 1*' window with the 'Communication' tab selected. The configuration fields are as follows:

Field	Value
Type	UDP/IP
COM port	COM1
IP address	10 . 0 . 0 . 66
Port	3001
Serial number	257153380061
Passcode	[Empty]
Encryption type	None
Encryption key	[Empty]
Command timeout	5
Heartbeat (sec)	60
Init string	[Empty]
Phone	[Empty]
Connection timeout (s)	60
Maximum redial attempts	5
Number of calls	1
Number of rings	3
Call option	Dial out

6. Click the **Save**  button in the toolbar to save the NAC panel record.
7. CTPlus will connect to the NAC via Ethernet instead of USB. The USB cable can now be removed.

Programming the NAC

The Network Access Controller is programmed via the DGPs form. Click the **DGPs**  button on the *Panel programming* ribbon tab to open the DGPs form.

The screenshot shows the 'DGPs - 1.1 -' window with the 'Setup' tab selected. The configuration fields are as follows:

Field	Value
Record	1
Panel	CH 1
Setup	☒ Poll DGP
DGP model	TS1067 - NAC with Wiegand Interfaces
NAC mode	Classic 4-door (Panel managed NAC)
Input range	17 - 48
Output range	17 - 32
Door range	17 - 20

A NAC in IP Direct mode will have an automatically generated DGP record. It will have DGP number 16. The DGP form's **Panel** field will be the NAC. See the Connecting NAC in IP Direct mode section on page 33 for more information.

A NAC in IP Extended mode will have two DGP records:

- An automatically generated record with DGP number 16. The DGP form's **Panel** field will be the NAC.
- A record with a DGP number configured when the NAC was initially added. The DGP form's **Panel** field will be the Challenger*Plus* panel that the NAC is connected to.

See the Connecting NAC in IP Extended mode section on page 34 for more information.

A NAC in Classic mode will have the DGP number configured when the NAC was initially added. The DGP form's **Panel** field will be the Challenger*Plus* panel that the NAC is connected to. See the Connecting NAC in Classic mode section on page 36 for more information.

The following tabs can appear on the DGPs form when a NAC record is selected:

- *Setup* tab – shows information about the NAC's operating mode, and allows the NAC to be polled or depolled if the NAC is connected to a Challenger*Plus* panel.
- *NAC options* tab – allows you to program general controller options. See the "Programming general controller options" section on page 49.
- *Input/Relay mapping* tab – allows you to program input and relay mapping on the NAC. See the "Programming input and relay mapping" section on page 99.

Note: The *Input/Relay mapping* tab does not appear if the NAC is in IP Direct mode, since input and relay mapping does not apply in that IP Direct mode.

- *Assigned RAS* tab – allows you to assign RASs on the NAC or one of its buses to the NAC. RASs must be assigned to the NAC and polled before they can be used. See the "Assigning RASs" section on page 53.
- *Assigned DGP* tab – allows you to assign DGPs on the NAC or one of its buses to the NAC. DGPs must be assigned to the NAC and polled before they can be used. See the "Assigning DGPs" section on page 55.
- *Alarm Control Levels* – allows you to control a group of areas when assigned to a door in Classic Mode. See Alarm Control Levels section on page 56
- *Regions* – allow you to control regions when assigned to a door in Classic Mode. See Regions section on page 60.
- *Lift Control Levels* – allows you to create a group of floors with a time schedule to be assigned to either a Lift override or a Lift security key override on any of the controller's lifts. See Lift Control Levels on page 62.

Setup tab

Each field of the *Setup* tab is explained in the following sections.

Poll DGP

If the NAC is connected to a *ChallengerPlus* panel, and the current DGP record is for the NAC as a *ChallengerPlus* DGP, then the **Poll DGP** check box can be used to poll the DGP from the *ChallengerPlus* panel.

DGP model

This field shows the DGP model. For a NAC, the field will always show *TS1067 – NAC with Wiegand Interfaces*.

NAC mode

This field shows the operating mode of the NAC. The field can be one of the following:

- *IP Extended 4-doors: In this mode, management software has a direct IP connection to the NAC. In addition to access control, the NAC provides alarm control and reporting functionality in conjunction with a ChallengerPlus panel. It allows to control up to 4 doors.*
- *IP Extended 8-doors: In this mode, management software has a direct IP connection to the NAC. In addition to access control, the NAC provides alarm control and reporting functionality in conjunction with a ChallengerPlus panel. It allows the user to control up to 8 doors. This mode will only be available with the activation of the relevant licensed capacity (refer to Licensing Functionality on page 40).*
- *Classic 4-door: In this mode, in addition to access control, the NAC provides alarm control functionality in conjunction with a ChallengerPlus panel and it allows up to 4 doors.*
- *Classic 8-doors: In this mode, in addition to access control, the NAC provides alarm control functionality in conjunction with a ChallengerPlus panel and it allows up to 8 doors. This mode will only be available with the activation of the relevant licensed capacity (refer to Licensing Functionality on page 40).*

Programming general controller options

The NAC's general controller options can be programmed on the *NAC options* tab of the DGPs form.

Each field is explained in the following sections.

Relay controllers

Enter a value in the range 1 to 8 in order to use TS0841 or TS0842 clocked relay expansion cards. Alternatively, enter 0 (disabled) to use a TS0840 4-Way Relay Card, or for no relay expansion.

Use a value that represents groups of eight clocked relays or open collectors. For example:

- Enter a value of 1 if one 8-way relay card is used (TS0841).
- Enter a value of 2 if one 16-way open collector card is used (TS0842).
- Enter a value of 4 if four 8-way relay cards are used (TS0841).

EOL resistor

The EOL (End-Of-Line) resistor is used to detect the electrical states of input circuits. This field defines the actual resistor value.

Challenger*Plus* panels normally have the default 10 k Ω EOL resistor value to detect the electrical states of the 16 input circuits connected directly to the Challenger*Plus* panel. For systems that use a different EOL resistor, select the required value from the list.

Input tamper monitoring

If the Challenger*Plus* panel monitors input circuits for tamper conditions, then the NAC must do the same.

When enabled, the system can detect sealed, unsealed, and fault (open and short circuit) states. When disabled, the system can detect sealed and unsealed states only. Open and short circuit states are detected as unsealed.

Siren monitor

The use of a siren on a controller is optional and siren monitoring is disabled by default. The siren circuit is not monitored for fault conditions unless siren monitoring is enabled.

Tamper relay

Program the relay to be activated when a “Cabinet Tamper” or a “Siren Fault” condition exists on the NAC. Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Mains fail relay

Program the relay to be activated when a “Mains Fail” condition exists on the NAC. Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Low battery relay

Program the relay to be activated when a “Low Battery” condition exists on the Intelligent Controller. Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Bus options

There are two RS-485 buses on the NAC. Each bus can have up to 16 RAS devices. Bus 1 can have up to 15 DGP devices and Bus 2 can have up to 16 DGP devices.

Note: DGP number 16 on Bus 1 is the NAC itself.

Each bus can have devices other than Tecom devices. Each bus supports the OSDP (Open Supervised Device Protocol), SALLIS (by SALTO Systems), and Aperio protocols. Each bus can use one protocol at a time, but the two buses can use different protocols.

See “Bus formats” on page 16 for more information.

Bus format

Each bus format may be one of:

- *Tecom* – Tecom protocol for adding devices from the Tecom family of products
- *Aperio* – Aperio protocol
- *SALLIS (SALTO)* – SALLIS protocol by SALTO systems
- *OSDP* – Open Supervised Device Protocol version 2

Bus baud rate

If the **Bus format** is not set to *Tecom*, the baud rate on the bus can be configured to be one of the following:

- *4800 baud*
- *9600 baud*
- *19200 baud*
- *38400 baud*
- *57600 baud*
- *115200 baud*

If the **Bus format** is set to *OSDP*, then set the baud rate to *9600 baud*.

If the **Bus format** is set to *Aperio*, then set the baud rate to *19200 baud*.

If the **Bus format** is set to *SALLIS (SALTO)*, then set the baud rate to *38400 baud*.

Note: If the **Bus format** is set to *Tecom*, then the baud rate is fixed at 4800 baud.

Bus encryption key

To use encryption with OSDP readers, set the 128-bit AES encryption key for the bus. There is a 16-character limit on the key length.

The encryption key will be set on each OSDP reader attached to the bus once the encryption key is defined.

Note: Once set, the encryption key on an OSDP reader cannot be changed by changing the encryption key for the bus. To reset the encryption key used by an OSDP reader, the reader must be reconfigured with the appropriate OSDP configuration card.

Note: A single OSDP configuration card cannot be used twice in succession to configure an OSDP reader. Different configuration card must be used in between.

Siren mode

The onboard siren output can be configured for use with a standard siren, or for use with an integrated siren/strobe unit that requires a 12 V DC supply. Alternatively, the 12 V DC output can be used for a device that requires 12 Volt DC power when the NAC's siren relay is active.

Duress mode

Duress mode allows a user to signal a duress condition (for example, a holdup) by entering a special duress code on a keypad RAS instead of their usual door code.

The system will behave as if the user's PIN was entered (for example, to open a door), and it will initiate a duress alarm. The duress alarm can be reset (cancelled) by entering the normal PIN.

Select the duress mode from the following options:

- *No duress* – Duress codes are not supported by the NAC.
- *Increment last digit* – The duress code is the user's PIN with the last digit incremented by 1. For example, if the user's PIN is 1234, then the duress code is 1235. If the user's PIN is 1239, then the duress code is 1230.
- *Add last digit* – The duress code is the user's PIN with an extra 5 appended. For example, if the user's PIN is 1239, then the duress code is 12395.

Note: This option is not compatible with 10 digit PINs.

- *Add first digit* – The duress code is the user's PIN with an extra 5 prepended. For example, if the user's PIN is 1239, then the duress code is 51239.

Note: This option is not compatible with 10 digit PINs.

In IP Direct mode, the duress alarm is sent directly to management software.

In IP Extended and Classic modes, the duress alarm is sent to the Challenger*Plus* panel.

Advanced options

Transformer size

Specify the size of the transformer being used by the NAC. This is required to handle correct power output when using either the supplied NAC transformer, or an alternative.

Battery size

The size of the batteries being used by the Network Access Controller can be set as either Small (7AH) or Large (12AH). This will ensure the NAC is best optimised to use the type of batteries connected to it.

Interlock timer (msec)

Program the timer to be activated to stop two or more door from being opened at the same time.

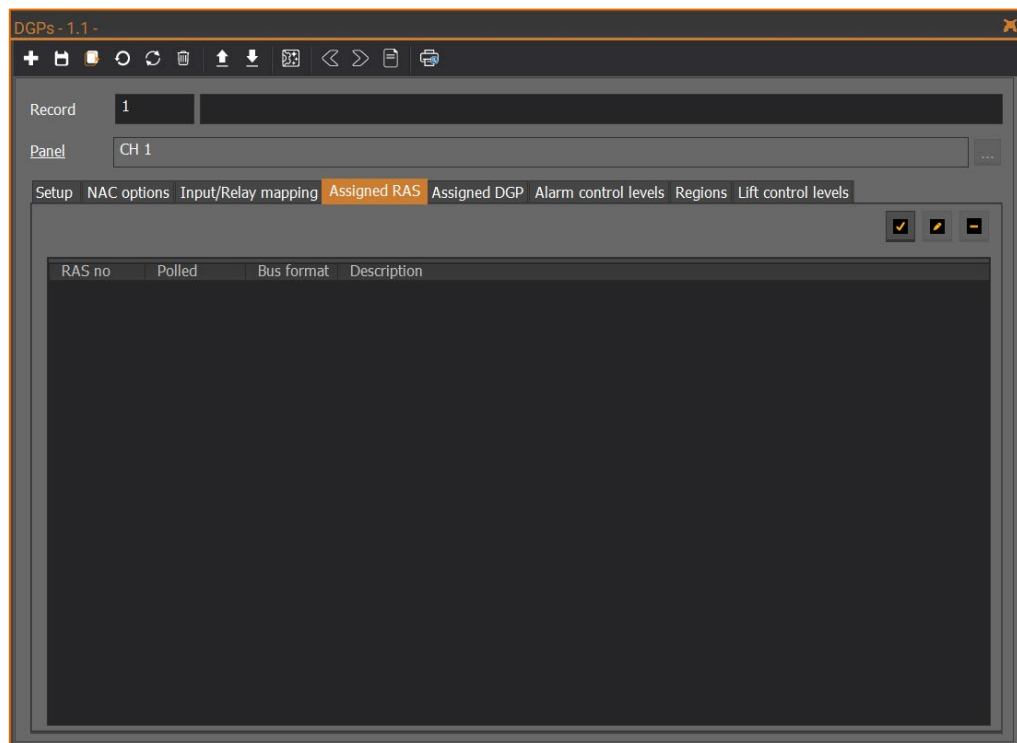
Press "Enter" 3 times after PIN to arm

Tick this option if you want to arm a related area by entering your PIN code and pressing the "Enter" key 3 times in quick succession. This option will only function when the NAC is connected to a Challenger*Plus* panel.

Assigning RASs

RASs attached to one of the Network Access Controller's buses must be assigned to the NAC. RASs can be assigned on the *Assigned RAS* tab of the DGPs form. Click the **DGPs**  button on the *Panel programming* ribbon tab to open the DGPs form.

The *Assigned RAS* tab shows a list of assigned RASs.

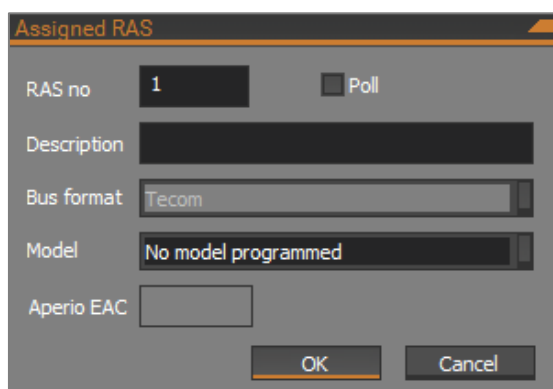


Click the **Assign**  button to open the Assigned RAS dialog to assign a RAS to the NAC.

Click the **Edit**  button to open the Assigned RAS dialog to edit the settings of the selected assigned RAS in the RAS list.

Click the **Remove**  button to remove the selected RAS from the RAS list.

The following figure shows the Assigned RAS dialog:



RAS no

Enter the RAS number from 1 to 32. RAS numbers from 1 to 16 are defined to be on Bus 1, and RAS numbers from 17 to 32 are defined to be on Bus 2.

Poll

Tick the check box to poll the RAS.

Description

Enter an optional description for the RAS.

Bus format

This read-only field shows the bus format used by the bus for the defined **RAS no.** See the “

Bus options” section on page 50.

Model

If the **Bus format** field is set to *Tecom*, then the RAS model can be selected from the following:

- *CA1110 – 2 line no reader*
- *CA1111 – 4 line no reader*
- *CA1115 – 2 line with reader*
- *CA1116 – 4 line with reader*
- *TS0003 – 3/4 LED keypad*
- *TS0004 – 4 LED arming station*
- *TS0006 – Heavy duty keypad*
- *TS0007 – Mag swipe reader with keypad*
- *TS0008 – Mag swipe reader*
- *TS0801 - 8 Area RAS*
- *TS0804 - 16 Area RAS*
- *TS0862 – Single Door Controller*
- *TS0870 – Smart card reader range*
- *TS0870D – Smart card reader range*
- *TS0870H – Smart card reader range*
- *TS1001 – Touch Screen RAS*
- *TS1162 – 3 LED arming station*
- *No model programmed- Default setting. Choose the model if it is in the list above provided otherwise the system cant auto detect.*

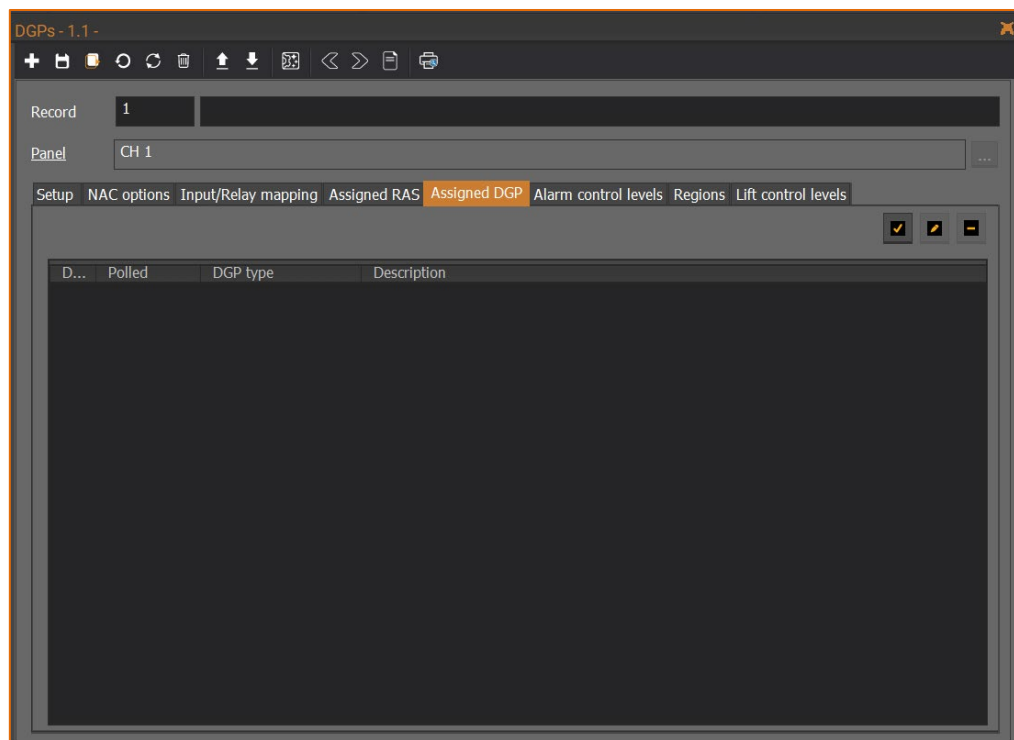
Aperio EAC

If the **Bus format** for the bus is set to *Aperio*, then enter the Aperio EAC (Electronic Access Control) number in this field. Values can range from 1 to 255.

Assigning DGPs

DGPs attached to one of the Network Access Controller's buses must be assigned to the NAC. DGPs can be assigned on the *Assigned DGP* tab of the DGPs form. Click the **DGPs**  button on the *Panel programming* ribbon tab to open the DGPs form.

The *Assigned DGP* tab shows a list of assigned DGPs.

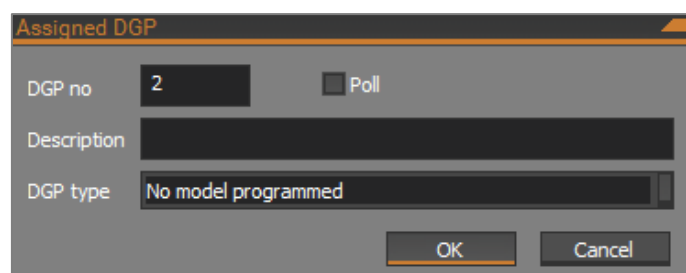


Click the **Assign**  button to open the Assigned DGP dialog to assign a DGP to the NAC.

Click the **Edit**  button to open the Assigned DGP dialog to edit the settings of the selected assigned DGP in the DGP list.

Click the **Remove**  button to remove the selected DGP from the DGP list.

The following figure shows the Assigned DGP dialog:



DGP no

Enter the DGP number from 1 to 15, or 17 to 32. DGP numbers from 1 to 15 are defined to be on Bus 1, and DGP numbers from 17 to 32 are defined to be on Bus 2.

Note: DGP number 16 is the NAC itself.

Poll

Tick the check box to poll the DGP.

Description

Enter an optional description for the DGP.

DGP type

Select the type of DGP:

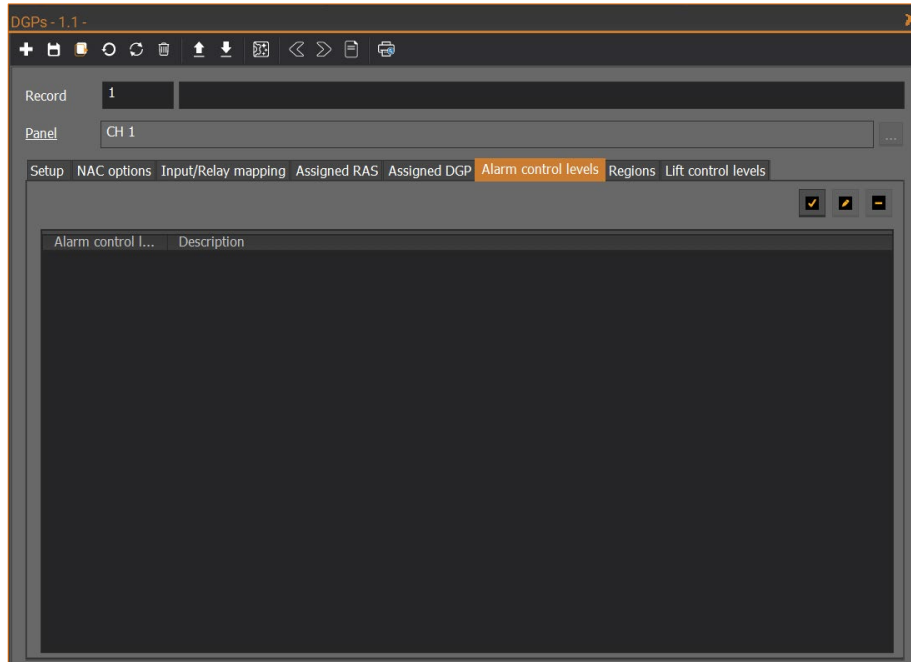
- *TS0820 - Challenger V8 DGP*
- *TS1020 - Challenger10 DGP*
- *TS1061 - Dual Wiegand interface*
- *Default setting. Choose the model if it is in the list above provided otherwise the system cant auto detect.*

Alarm Control Levels

Note: Alarm control does not apply to the NAC in IP Direct mode.

If the NAC is connected to a Challenger*Plus* panel, it can support alarm control functionality, such as arming areas via badging a card. Alarm control functionality can be configured separately for IN and OUT readers.

The following figure shows the *Alarm control levels* tab of the DGPs form:



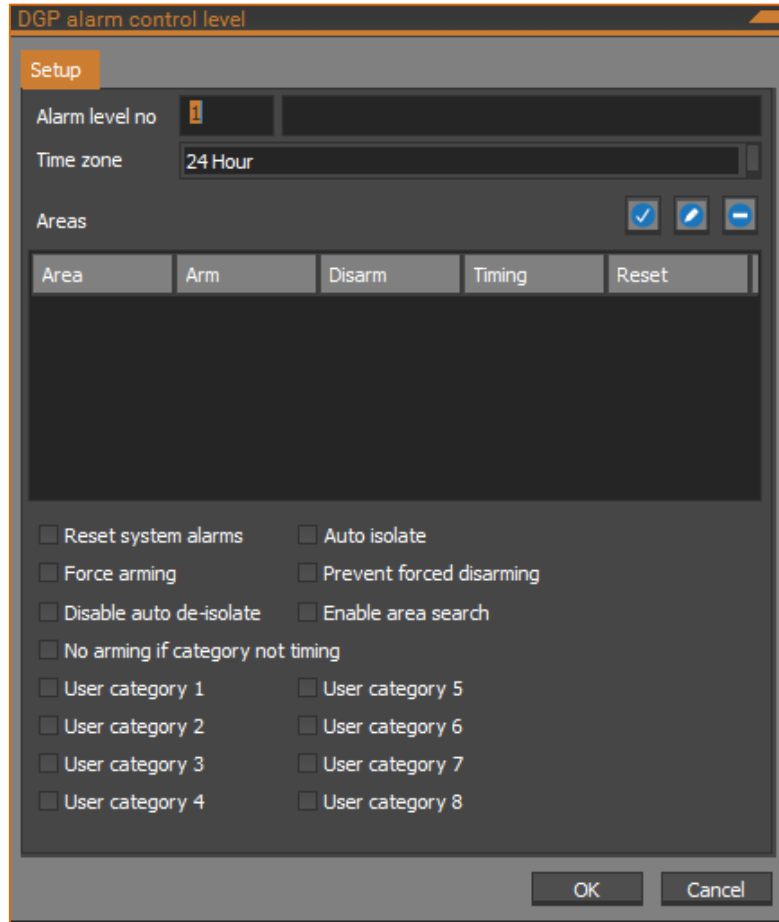
The *Alarm control levels* tab shows a list of alarm control levels.

Click the **Assign**  button to open the DGP alarm control level dialog to set an alarm control level.

Click the **Edit**  button to open the DGP alarm control level dialog to edit the settings of the selected alarm control level in the list.

Click the **Remove**  button to remove the selected alarm control level from the list.

The following figure shows the DGP alarm control level dialog:



The image shows a software dialog box titled "DGP alarm control level". It has a "Setup" tab. The "Alarm level no" field contains the number "1" and has a warning icon. The "Time zone" dropdown menu is set to "24 Hour". Below these is an "Areas" section with a table that has columns for "Area", "Arm", "Disarm", "Timing", and "Reset". The table is currently empty. To the right of the table are three icons: a checkmark, a pencil, and a minus sign. Below the table is a list of checkboxes for various settings: "Reset system alarms", "Auto isolate", "Force arming", "Prevent forced disarming", "Disable auto de-isolate", "Enable area search", "No arming if category not timing", and eight "User category" options (1 through 8). At the bottom right are "OK" and "Cancel" buttons.

Alarm control level no

Each door can have up to six alarm control levels. Alarm control levels can be assigned to the door's IN and OUT readers separately.

Enter a number for the alarm control level, and, optionally, a name to identify the alarm control level.

Time zone

Specify a time zone to apply to this alarm control level. The alarm control level is only available if the time zone is valid.

Reset system alarms

A user with the appropriate alarm group can reset latching system alarms at the door. The user's alarm group and the door's alarm control level must allow arming, disarming, and resetting. The "Latching system alarms" system option must also be enabled on the *ChallengerPlus* panel. Refer to the *ChallengerPlus Programming Manual* for details of latching system alarms.

Auto isolate

When a user with the appropriate alarm group arms an area, all unsealed inputs will be automatically isolated. The system is armed without causing an alarm.

Force arming

When a user with the appropriate alarm group arms an area, the check for unsealed inputs is ignored. If there are unsealed inputs when the arming procedure is started, the system still arms (the unsealed inputs might cause an alarm).

Prevent forced arming

This setting controls the treatment of unsealed inputs during the disarming procedure and may be used if there are access alarm input types such as type 1 or type 11 in the system. If enabled, the area cannot be disarmed if there are unsealed inputs.

No arming if category not timing

This option prevents the area from being automatically rearmed without a user category. For example, a guard might have a user category that automatically re-arms an area when the user category timer expires. But if someone else disarmed the area (the user category timer isn't running), then the guard's user category will not automatically re-arm the area. If enabled, automatic re-arming is prevented when an area is occupied by non-user category staff.

Disable auto deisolate

Select this option to prevent certain users (for example, cleaners) from being able to automatically deisolate inputs in the area they disarm. If enabled, a user in the appropriate alarm group can disarm areas with isolated inputs remaining isolated even if the system is programmed (via the *ChallengerPlus* panel's "Automatic deisolate" system option) to automatically deisolate (sealed) isolated inputs. Refer to the *ChallengerPlus Programming Manual* for details of automatic deisolate.

Enable area search

When enabled, a user with the appropriate alarm group must perform an area search as part of the disarming process during the time zone specified in the *ChallengerPlus* panel's "Area search time zone" system option. Refer to the *ChallengerPlus Programming Manual* for details of area search.

User category 1 to 8

User categories assigned to an alarm control level provide timing functionality via a corresponding user category time. Refer to the *ChallengerPlus Programming Manual* for more information on user categories.

If multiple user categories are assigned to an alarm control level, then the lowest user category number applies. System functionality can depend on the alarm

group assigned to a user, and the alarm control levels assigned to a door. In these cases, the lowest common user category number applies.

For example, if a user has an alarm group containing user categories 3 and 4, and a door has an alarm control level containing user categories 1, 2, 3, and 4, then only user category 3 would apply to that user at that door.

When ticked, the user category activates when a user with the appropriate alarm group enters their PIN or badges their card.

Areas

An alarm control level can only control the functions of areas that are assigned to it. An alarm control level can be linked to multiple areas. For each area, the alarm control level can control the area's permissions for arming, disarming, alarm reset, and for timing.

Click the **Assign**  button to open a dialog to assign areas to the alarm control level. In the dialog, move the required areas from the **Available areas** list to the **Assigned areas** list using the  button. Areas can be removed from the **Assigned areas** list using the  button. Click the **OK** button when finished.

Note: In IP Extended mode, the NAC is programmed via the USB/IP connection. Thus CTPlus does not have information about which areas are programmed on the Challenger*Plus* panel that the NAC is connected to. Therefore, the **Available areas** list will contain all 99 theoretically available areas on a Challenger*Plus* panel, and will not show the names of the areas. You must match the area numbers to assign to the alarm control level with the area numbers required for alarm control on the Challenger*Plus* panel.

The following permissions for each area can be changed:

- **Arm** – A user with the appropriate alarm group can arm the area.
- **Disarm** – A user with the appropriate alarm group can disarm the area.
- **Timing** – A user with the appropriate alarm group can reset alarms for the area.
- **Reset** – Depending on the application, a user with the appropriate alarm group can disarm the area for the user category time (in which case disarming must be permitted), or automatically arm another area via vault programming (in which case arming must be permitted).

Area permissions for arming, disarming, timing, and for alarm reset can be modified in two ways:

- On a per-area basis from the **Areas** list. Tick the check box that you want to toggle.
- In bulk, by selecting multiple areas, and then clicking the **Edit**  button. The Area flags dialog displays. Set the permissions for arming, disarming, alarm reset, and for timing that you want to apply to all selected areas, and then click the **OK** button.

Click the **Remove**  button to remove the selected area from the **Areas** list.

Regions

Note: Regions does not apply to the NAC in IP Direct mode.

If the NAC is connected to a Challenger*Plus* panel, it can support Regions functionality, such as high security user verification.

The following figure shows the *Regions* tab of the DGPs form:

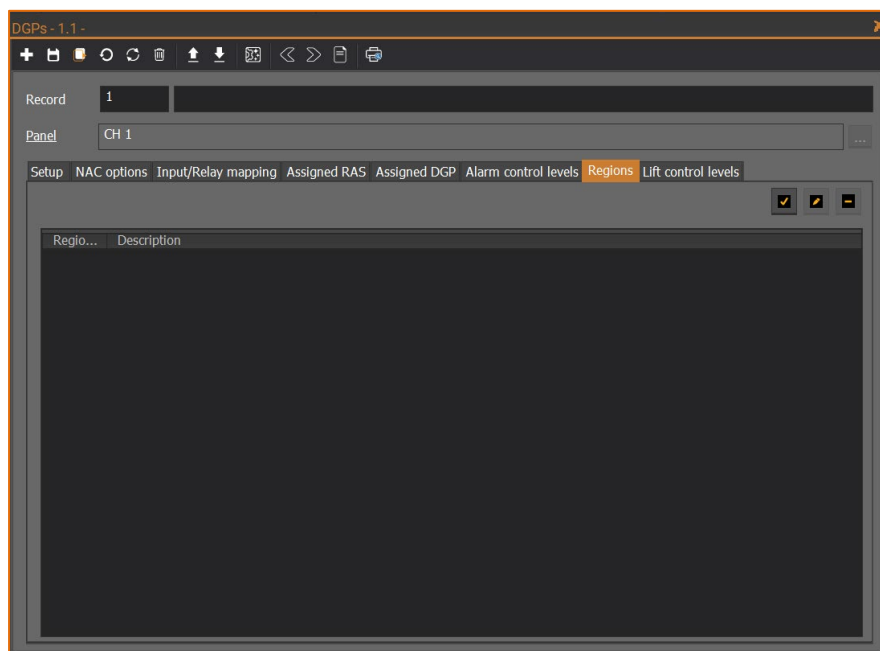


Figure 5 DGP Regions

Figure 6 DGP NAC regions Setup

Region number: Select the region by clicking the **Browse**  button, or type the region number directly into the field.

Low limit: Minimum number of the people that represent the region.

High limit: Maximum number of people that represent the region.

Low user limit relay: Physical address of the relay when the number of people in the region is less than the low limit.

High user limit relay: Physical address of the relay when the number of people in the region is more than the high limit.

Deny access when high limit reached: Access is denied when the number of people trying to access the region and in the region is more than the high limit.

Release users from region when time zone starts: Users are released from the region when the configured TZ starts, forcing them to badge their cards again to enter the region.

Release users from region when time zone ends: Users are released from the region when the configured TZ ends, forcing them to badge their cards again to enter the region.

Time Zone: Specify a time zone to apply to the region. Releasing users is only available when the time zone starts or ends.

Enable high security users: Users with high security profile are enabled in the region.

HSU warning time: Specify the maximum time allowed in minute or seconds, after no HSU is in the region or the number of the HSU is below or above the defined range for HSU warning timer to expire.

Minimum HSU in region: Minimum number of HSUs allowed in the region.

Maximum HSU in region: Maximum number of HSUs allowed in the region.

Low HSU limit relay: Physical address of the relay when the number of HSUs in the region is less than minimum limit.

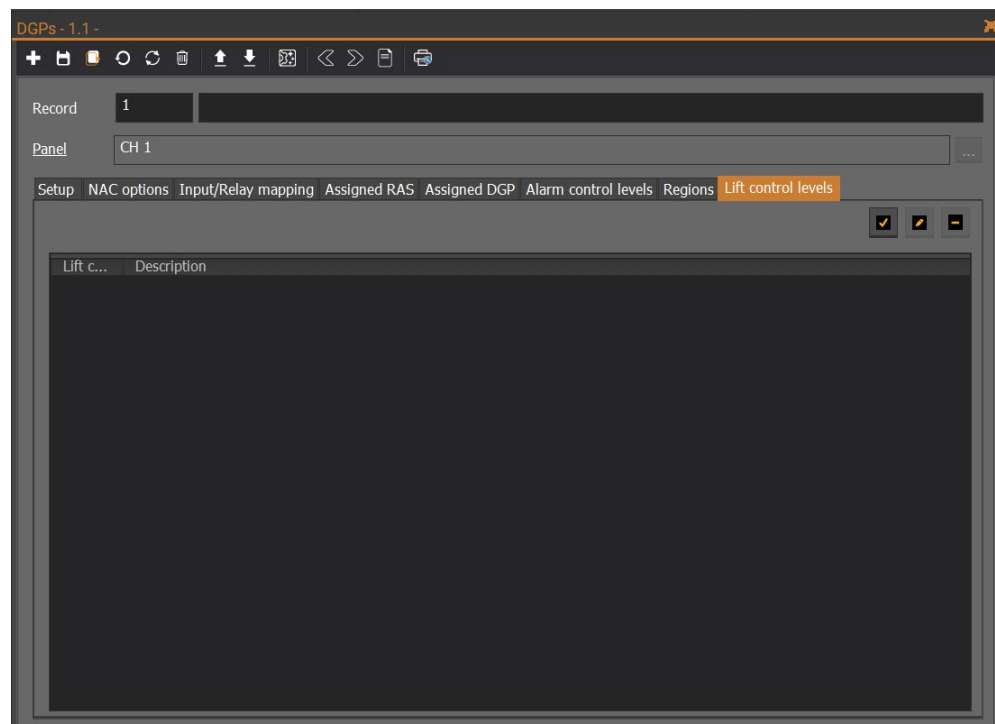
High HSU limit relay: Physical address of the relay when the number of HSUs in the region is more than maximum limit.

HSU warning relay: Physical address of the warning relay that will be triggered when the HSU warning timer expires.

HSU alarm relay: Physical address of the alarm relay that will be triggered when the HSU warning timer expires.

Lift Control Levels

Up to 100 Lift control levels can be configured for the entire NAC, each NAC lift can have up to 10 Lift control levels. These lift control levels can be assigned as a 'Lift override control level' or 'Security key override control level', see "Programming control level options" on page 98 for more information.



Control level 1 Lift Control L1

Floors

Num...	Description
1	CH 1 Floor 1
2	CH 1 Floor 2
3	CH 1 Floor 3
4	CH 1 Floor 4

Time zone

Start time	End time	Days	Holiday types
09:00	17:00	Mon, Tue, Wed, Thu, Fri	

OK Cancel

Control level no: Enter a number for the Lift control level, and, optionally, a name to identify the lift control level.

Floors: A Lift control level can control the functions of floors that are assigned to it. A lift control level can be linked to multiple floors. For each floor, the lift control level can control the floor permissions for secure or access mode based on the time zone.

Click the Assign  button to open a dialog to assign Floors to the lift control level. In the dialog, move the required Floors from the Available Floors list to the Assigned floors list using the  button. Floors can be removed from the Assigned Floors list using the  button. Click the OK button when finished.

When the selected time zone is active, the floors selected will be in Auto Access mode.

When the time zone is not active, the floors selected will be in Auto Secure mode.

Click the Remove  button to remove the selected Floor from the Floors list.

Time zone: Specify a time zone to apply to this Lift control level. The Lift control level is only active if the time zone is valid. The time zone to be applied can be created from dialog below which is similar to the panel time zone

	Start time	End time	S	M	T	W	T	F	S	All	H1	H2	H3	H4	H5	H6	H7	H8	All	
1.	09:00 AM	05:00 PM	☒	☒	☒	☒	☒	☒	☒	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All
2.	10:10 AM	10:10 AM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All
3.	10:10 AM	10:10 AM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All
4.	10:10 AM	10:10 AM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All
5.	10:10 AM	10:10 AM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All
6.	10:10 AM	10:10 AM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All
7.	10:10 AM	10:10 AM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All
8.	10:10 AM	10:10 AM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	All

Holiday type description

H1 Holiday type H5 Holiday type
H2 Holiday type H6 Holiday type
H3 Holiday type H7 Holiday type
H4 Holiday type H8 Holiday type

OK Cancel

Programming holidays

Note: Typically, holidays will be configured using TecomC4. The following information is for using CTPlus to program holidays if required.

Holidays can be used for:

- Programming time zones
- Programming door/lift overrides
- Programming door/lift schedules

If required, program holiday types for the Network Access Controller on the Holiday types form. Click the **Holiday types**  button on the *User access* ribbon tab. Refer to the *ChallengerPlus Programming Manual* for more information on holiday types. Refer to the *CTPlus Operators Manual* or CTPlus online help for more information on the Holiday types form.

In Classic mode, the NAC uses the same holidays as the *ChallengerPlus* panel it is connected to.

In the other operating modes, the NAC supports up to 100 holidays.

To add a holiday to a NAC, follow these steps:

1. Click the **Holidays**  button on the *User access* ribbon tab to open the Holidays form.

2. On the Holidays form, click the **New**  button in the toolbar to add a new holiday record.
3. Enter a description for the holiday in the **Record** description field.
4. Ensure the **Panel** field is set to the NAC. If necessary, click the **Browse**  button next to the **Panel** field to select the NAC.
5. On the *Setup* tab, program the **Start date**, **End date**, **Recurring**, and **Holiday types** fields as required for the holiday.

Note: A holiday must have be assigned at least one holiday type.

6. Click the **Save**  button in the toolbar to save the holiday record.

Refer to the *ChallengerPlus Programming Manual* for more information on holidays. Refer to the *CTPlus Operators Manual* or CTPlus online help for more information on the Holidays form.

Programming time zones

Time zones can be used in the Network Access Controller for the following:

- Door and floor groups
- Override time zone and low security time zone (in door access options)
- Egress time zone (in door egress options)

In Classic mode, the NAC uses the same time zones as the *ChallengerPlus* panel it is connected to.

In the other operating modes, the NAC supports time zones numbered 1 to 2,000.

Note: Time zone 0 is a 24-hour time zone (always valid) and cannot be edited or deleted. In CTPlus it is called “24 Hour”.

To add a panel time zone to a NAC, follow these steps in CTPlus:

1. Click the **Panel time zones**  button on the *User access* ribbon tab to open the Panel time zones form.
2. On the Panel time zones form, click the **New**  button in the toolbar to add a new panel time zone record.
3. Enter a description for the panel time zone in the **Record** description field.
4. Ensure the **Panel** field is set to the NAC. If necessary, click the **Browse**  button next to the **Panel** field to select the NAC.
5. On the *Setup* tab, program the **Start time**, **End time**, **Days**, and **Holiday types** fields as required for the panel time zone.
6. Click the **Save**  button in the toolbar to save the panel time zone record.

Refer to the *ChallengerPlus Programming Manual* for more information on panel time zones. Refer to the *CTPlus Operators Manual* or CTPlus online help for more information on the Panel time zones form.

Note: Soft time zones are not applicable to a NAC.

Programming regions

A region is a defined access control area having doors acting as boundaries. Regions are used by the anti-passback functions to keep track of users. The system can deny access to a card or PIN belonging to a user when the user is already assigned to the region.

Depending on the anti-passback settings (see the “Anti-passback options” section on page 82), the system may:

- Deny access and report an anti-passback violation.
- Allow access and report an anti-passback violation.

Separate programming fields are provided for each door’s IN reader and OUT readers. See the “Region IN” section on page 83 and the “Region OUT” section on page 83.

When a valid card or PIN is entered at the door reader, the number of the region that the user is entering into is recorded against the user code. The range is from region 0 to region 254. Region 0 acts as off-site. Region 255 is used for 'Region disabled'.

Users in region 0 (i.e. off-site) can be prevented from unlocking doors at IN readers and/or OUT readers. See the “Inhibit off-site users” section on page 78 (the inhibit off-site users option can be configured separately for IN readers and OUT readers).

To add a region to a NAC, follow these steps in CTPlus:

1. Click the **Regions**  button on the *Panel programming* ribbon tab to open the Regions form.
2. On the Regions form, click the **New**  button in the toolbar to add a new region record.
3. Enter a description for the region in the **Record** description field.
4. Ensure the **Panel** field is set to the required NAC or ChallengerPlus panel. If necessary, click the **Browse**  button next to the **Panel** field to select the NAC or ChallengerPlus panel.
5. Click the **Save**  button in the toolbar to save the region record.

Programming doors

The following is a suggested programming sequence for Network Access Controller doors:

1. Program hardware options for each door.
2. Assign readers to each door.
3. Program access options for each door.
4. Program shunt, passback and egress options for each door.
5. Program alarm control for each door.

Click the **Doors/Lifts**  button on the *Panel programming* ribbon tab to open the Doors/Lifts form.

By clicking New button in the toolbar of the Door/Lifts form, the door/lifts creation wizard pops up. The wizard allows the operator to create doors or lifts and any associated entities.

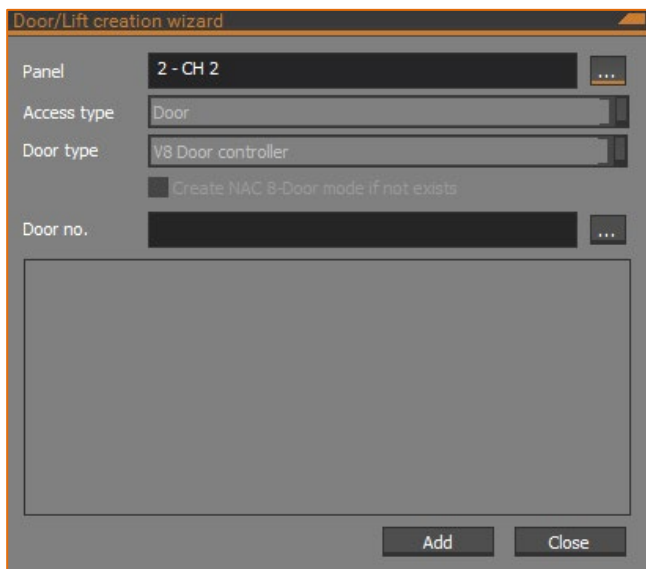
The image shows a 'Door/Lift creation wizard' dialog box. It has a title bar with the text 'Door/Lift creation wizard'. Inside, there are four labeled fields: 'Panel' with the value '2 - CH 2' and a browse button (three dots); 'Access type' with the value 'Door'; 'Door type' with the value 'V8 Door controller' and a sub-label 'Create NAC 8-Door mode if not exists'; and 'Door no.' with an empty field and a browse button. At the bottom, there are two buttons: 'Add' and 'Close'.

Figure 7 Door / Lift creation wizard

The wizard has the following fields:

Panel Click the Browse button on the right of the field to select the panel to add a door or lift to.

Access type

The user can choose to add a Door or Lift to the panel.

Door/lift type

Select the type of the controller that the door or lift will be added as part of:

- **Panel** – The door or lift will be added directly to the Challenger Panel as a standard door or a standard lift. A RAS will be created if necessary.

- Dual Wiegand Interface – The door or lift will be added to the Challenger Panel as a standard door or a standard lift. A DGP of type Dual Wiegand Interface will be created if necessary.
- V8 Door/Lift Controller – The door or lift will be added to as a part of a Four-Door controller as a V8 door or a Four-lift Controller as a V8 lift. A DGP of the appropriate type will be created if necessary.
- Network Access Controller – The door or lift will be added as part of NAC as a NAC door or a NAC lift. A DGP of type Network Access Controller will be created if necessary.

Device no

The first device number for the door or lift will be added. Standard doors are numbered in the range 1 to 2. Standard lifts are numbered in the range 1 to 16. NAC doors for a NAC in Classic mode or IP Extended mode, V8 doors, and V8 lifts are numbered in the range 17 to 64, or 81 to 128. NAC door for a NAC in IP Direct mode are numbered in the range 1 to 18. If the Controller type is V8 Door/Lift Controller, then four doors or lifts will be added starting from the number in this field.

Result

The field shows the results of adding the door or lift controller and its doors or lifts.

Programming hardware options

Hardware options for a door are configured on the *Hardware* tab of the Doors/Lifts form.

The following figure shows the *Hardware* tab of the Doors/Lifts form:

The screenshot shows the 'Hardware' tab of the 'Doors/Lifts - 1.1 - CH 1 Door 1' form. The 'Record' field is set to '1' and the 'Panel' is 'IP Extended NAC'. The 'Access' tab is selected, showing various hardware configuration options. The 'Lock type' is set to 'Strike'. Below this, there are several rows of configuration options, each with a 'Location' dropdown, a 'Polled address' field, and a 'Device number' field. The 'Interlock options' section includes a row of checkboxes for interlock doors 1 through 8. The 'External input' section has three rows for 'External input 1', 'External input 2', and 'External input 3', each with a 'None' dropdown and a 'Polled address' field.

Location	Polled address	Device number
Lock relay 1: Onboard		1
Lock relay 2: None		
Door input 1: Onboard		1
Door input 2: Onboard		8
Forced relay: Onboard		5
Warning relay: Onboard		6
DOTL relay: Onboard		7
Egress input: None		

Interlock options

Interlock doors: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8

External input	Polled address
External input 1: None	
External input 2: None	
External input 3: None	

Lock type

To support simple programming of complex door operation, the NAC has various lock types, with associated inputs, relays and timers. The lock type determines which inputs and relays are used and how they are used.

The lock types are:

- *Strike*
- *Maglock*

Lock relay 1

Specify the relay to be activated to unlock the door.

Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Lock relay 2

This relay is reserved for future use.

Door input 1

Specify the input used to indicate if the door is open or closed. This is usually the reed switch.

Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Door input 2

Specify the input connected to the lock monitor on *Strike*, *Maglock*, and *Drop bolt* lock types.

Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Forced relay

Specify the relay to be activated when an input is in a “Forced Door” condition, e.g. the door has been opened without a valid command.

Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Warning relay

Specify the relay to be activated during the “Warning time” when the shunt timer is about to expire, e.g. may be used to activate a buzzer above a door to indicate the door needs to be closed.

Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

DOTL relay

Specify the relay to be activated when an input is in a DOTL condition, e.g. the door left open after the shunt timer has expired.

Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Egress input

Specify the input that activates the egress function for the door being programmed.

Program the relay using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Egress functionality is programmed on the door's *Shunt/Egress/Passback* tab. See the "Egress options" on page 83.

Interlock options

For more information on door interlocking, see the "Interlocking doors" on page 14.

Interlock doors

Tick the door numbers on the same NAC that will be prevented from being accessed at the same time as the door being programmed.

External input 1, 2, 3

The NAC can check up to three external inputs for interlocking. If an input is wired up to an external controller's door contact, then specify the input in one of the external input fields. Program each input location using the scheme described in the "SALLIS" section on page 19 or the "Flexible device locations" section on page 20.

Assigning readers to doors

Each door can have up to six door readers associated with it in any combination of IN and OUT readers.

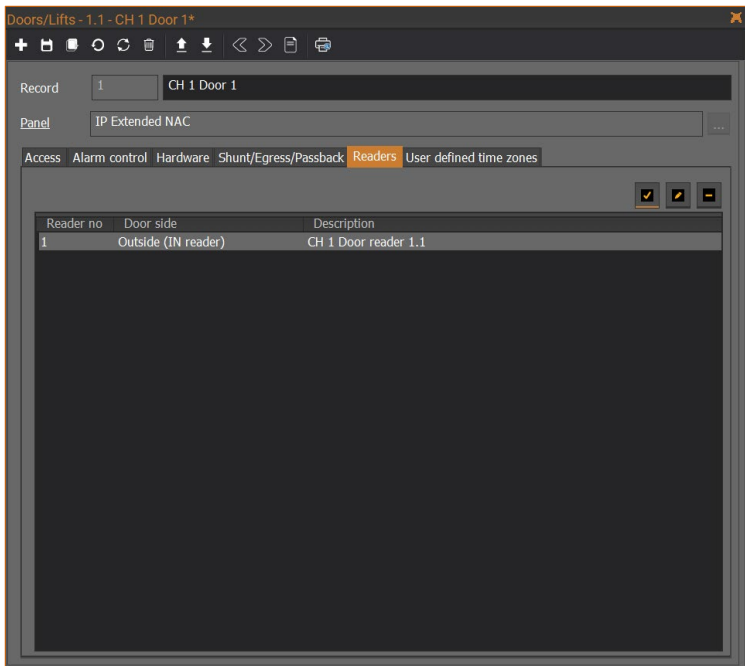
Readers can be assigned to doors on the *Readers* tab of the Doors/Lifts form.

Note: If the reader is attached to one of the NAC's buses, then the reader must be assigned to the NAC on the *Assigned RAS* tab of the NAC, and polled. See the "Assigning RASs" section on page 53.

Similarly, if the reader is attached to a DGP that is attached to one of the NAC's buses, then the DGP must be assigned to the NAC on the *Assigned DGP* tab of the NAC, and polled. See the "Assigning DGPs" section on page 55.

For readers attached to the Wiegand ports, the user will have to select "Onboard" for the reader location as well as the relevant device number that corresponds to the Wiegand port used, this will allow the reader to be polled.

The following figure shows the *Readers* tab of the Doors/Lifts form:



The *Readers* tab shows a list of assigned readers for the door.

Click the **Assign**  button to open the Door reader dialog to assign a reader to the door.

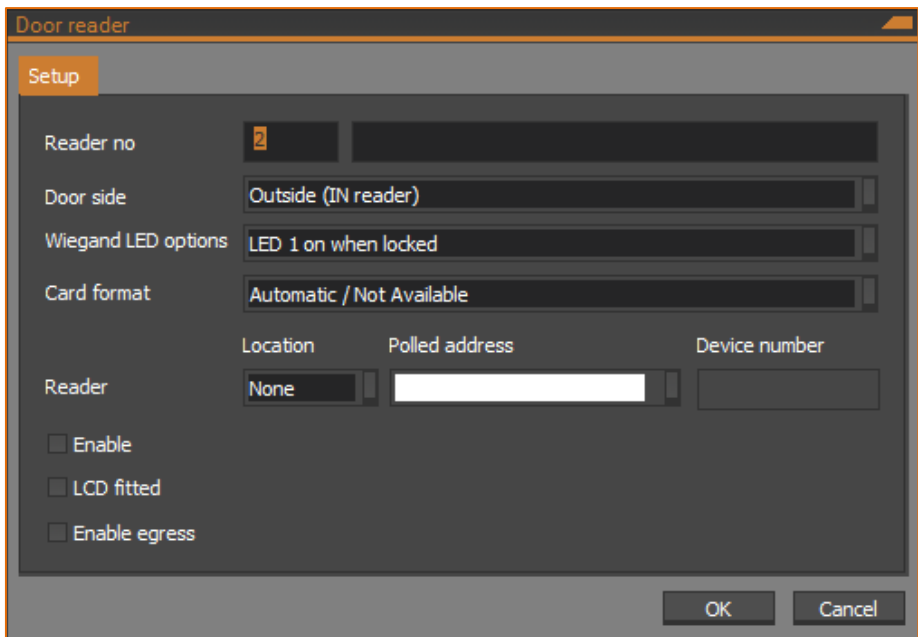
Click the **Edit**  button to open the Door reader dialog to edit the settings of the selected assigned reader in the reader list.

Click the **Remove**  button to remove the selected reader from the reader list.

The Door reader dialog has two tabs: *Setup* and *LED mapping*, described in the following sections.

Door reader dialog – Setup tab

The following figure shows the *Setup* tab of the Door reader dialog:



Reader no

Specify a reader number from 1 to 6. Enter an optional description next to the reader number.

Door side

Select the door side, which may be one of the following:

- *Outside (IN reader)* – IN reader placed on the outside of the door.
- *Inside (OUT reader)* – OUT reader placed on the inside of the door.

Wiegand option

Select the reader LED behaviour from the following options:

- *LED 1 on when locked* – LED 1 is on when the door is locked.
- *LED 1 on when unlocked* – LED 1 is on when the door is unlocked.
- *LED 1 on when area is armed* – LED 1 indicates if the area assigned to the door is armed (if more than one area is assigned, all areas assigned to the door must be armed before LED changes state).
- *LED 1 off when area is armed* – LED 1 indicates if the area assigned to the door is disarmed (if more than one area is assigned, all areas assigned to the door must be disarmed before LED changes state.)
- *Two LED access/secure* – Readers with dual LED control lines connected indicate the area disarmed and armed with different LED colours.
- *Two LED valid/void* – Readers with dual LED control lines connected indicate User Valid or Void using different LED colours.
- *LEDs disabled* – No LED control.

Note: On readers with dual LED control lines, LED 2 may also be programmed to indicate other conditions via the NAC's macro logic programming.

Format

Select the card format for the reader from the following options:

- *Tecom 27 bit* – For range of Tecom proximity readers supplied by KGS Fire and Security Australia Pty. Ltd.
- *Wiegand 26 bit* – For standard 26-bit Wiegand format readers. Has a 16-bit card number (0-65534) and an 8-bit site code (0-255).

Reader

Program the reader's location using the scheme described in the "SALLIS" section on page 19 or the "Flexible device locations" section on page 20.

Enabled

Tick the check box to enable the reader.

LCD fitted

Tick the check box if the reader has LCD (liquid crystal display).

Enable egress

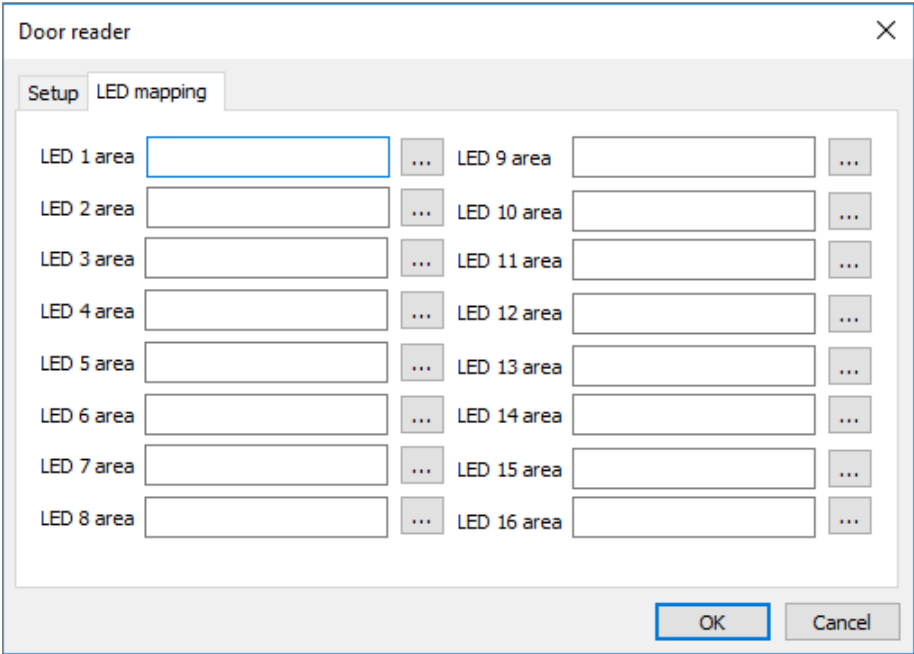
Tick the check box if the reader has an egress button connected to the reader's IN or EGRESS terminal.

Door reader dialog – LED mapping tab

The *LED mapping* tab allows the operator to program which area number is assigned to the reader's area LEDs, if applicable.

Note: LED mapping does not apply to the NAC in IP Direct mode.

The following figure shows the *LED mapping* tab of the Door reader dialog:



The screenshot shows a window titled "Door reader" with a close button (X) in the top right corner. Inside the window, there are two tabs: "Setup" and "LED mapping". The "LED mapping" tab is selected. It contains 16 rows, each with a label (LED 1 area to LED 16 area) and a corresponding text input field. To the right of each input field is a "Browse" button (three dots). The "LED 1 area" input field is highlighted with a blue border. At the bottom right of the window are "OK" and "Cancel" buttons.

In each **LED area** field, enter an area number or click the **Browse**  button next to the field to select an area.

Note: In IP Extended mode, the NAC is programmed via the USB/IP connection. Thus CTPlus does not have information about which areas are programmed on the Challenger*Plus* panel that the NAC is connected to.

Instead of clicking the **Browse**  button to select an area, enter an area number. You must match the area number to assign to an LED with the required area number on the Challenger*Plus* panel.

Programming access options

Access options for a door are configured on the *Access* tab of the Doors/Lifts form.

The following figure shows the **Access** tab of the Doors/Lifts form:

Doors/Lifts - 1.1 - CH 1 Door 1

Record: 1 CH 1 Door 1

Panel: IP Extended NAC

Access Alarm control Hardware Shunt/Egress/Passback Readers User defined time zones

Door type: Door Multi badge time: 5 Sec

Access time: 5 Sec Long access time: 15 Sec

Dual custody time: 8 Sec Card to PIN time: 8 Sec

Pre lock time: 2 Sec Post lock time: 2 Sec

Random event %: 0 Random % lockout time: Sec

Override TZ: Low security TZ

IN reader options:

- ☐ Card and PIN
- ☐ Inhibit PIN
- ☐ Dual custody
- ☐ Inhibit off-site users

OUT reader options:

- ☐ Card and PIN
- ☐ Inhibit PIN
- ☐ Dual custody
- ☐ Inhibit off-site users

☐ Dual custody both users enter region

☐ Hold door unlocked until door opens

☐ Disable duress

☒ Report DOTL

☒ Report door open/close

☐ Allow OUT reader access when TZ invalid

☐ 2 badge unlock, 1 badge re-lock

☐ Override after entry

☐ Time & attendance reader

☒ Report forced door

☒ Report secured/unsecured

Door type

The **Door type** field is for future use. Currently, the door type is set as *Door* and cannot be changed.

Multi badge time

Note: Multi badge time can be set per door on the NAC (it was set via the **Mode time** field for V8 Four-Door Controllers).

If two badge unlock is enabled for the door, then this field defines the amount of time permitted between the first and second badges. If the time expires, then the user will need to repeat the three badges in order to arm or disarm the area. See the “2 badge unlock, 1 badge re-lock” section on page 79.

Additionally, if a reader’s alarm control options specify three-badge alarm control for users who are authorised to arm and disarm areas, this field defines the amount of time permitted between the first and third badges. If the time expires, then the user will need to repeat the three badges in order to arm or disarm the area.

Note: Three-badge alarm control does not apply to the NAC in IP Direct mode.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Access time

Program the amount of time for the door to unlock when a user enters a valid card or PIN at the door reader. The user is then able to open the unlocked door during the access time.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Long access time

Program the amount of time for the door to unlock when a user, with the “Long Access” flag enabled, presents a valid card or PIN at the door reader. The user is then able to open the unlocked door during the extended access time.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Dual custody time

Note: In contrast to the V8 Four-Door Controller, dual custody time can be set per door on the NAC.

Note: By default, if dual custody functionality is enabled, only the second user is reported as having accessed a door. Thus, if a visitor and an accompanying guard badge their cards to open a door, only the guard is considered as having accessed the door.

If dual custody functionality is used, you can define the amount of time permitted between a visitor and an accompanying guard badging their cards to open a door, or between the first and second instances of badging when two badge unlock is used.

If the time expires before the second badging, then the door is not unlocked and the operation must be recommenced.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

See the “Dual custody” section on page 78 (the dual custody option can be configured separately for IN readers and OUT readers). Also see the “2 badge unlock, 1 badge re-lock” section on page 79.

Card to PIN time

Note: Card to PIN time can be set per door on the NAC.

If card and PIN functionality is used, you can define the amount of time permitted between a user badging their card and entering their entire PIN.

If the PIN is not completely entered before the time expires, then the user will need to repeat the door opening function.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

See the “Card and PIN” section on page 78 (the card and PIN option can be configured separately for IN readers and OUT readers).

Pre lock time

Once the door open input (**Door input 1**) has been sealed, the NAC waits for the pre-lock time to expire before locking the door. If the door open input unseals during the pre-lock time, the door is deemed open and the pre-lock timer is cancelled. The shunt continues during the pre-lock time.

Door input 1 is programmed on the *Hardware* tab for the door.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Post lock time

The post-lock time allows time for a lock to fully engage. After the post lock time has expired, the door is deemed secure, and the shunt is cancelled. If the door open input (**Door input 1**) unseals during the post-lock time, the door is deemed open and the post lock timer is cancelled. The shunt continues during the post-lock time.

Door input 1 is programmed on the *Hardware* tab for the door.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Random event %

The value defines the average percentage of the number of times that a valid card or PIN is presented to open the door that the door's "Door random bit" event will be activated.

The "Door random bit" event may then be used in the controller's macro logic programming to activate a relay or another event. For example, if the percentage value was set to 20, the "Door random bit" event would be activated an average of once every five times a card or PIN is successfully used at the reader.

Alternatively, if the **Random % lockout time** field (below) has a value, then the "Door random bit" event locks out the door for the specified time. During this time, the door cannot be opened by any user.

Enter a number in the range 0 to 100.

Random % lockout time

When the "Door random bit" event triggers (as described in **Random event %**, above), the door can be locked out for the amount of time specified in this field. During this time, the door can only be opened by a user with the "Privileged" flag. Any LCD RAS attached to the door will display "Locked Out".

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Override TZ

The override time zone controls the times when the door can be opened without the need to use a valid card or PIN. Free access is allowed when the time zone is valid.

Enter a time zone number or click the **Browse**  button to select a time zone.

Low security TZ

The low security time zone controls the times when the door can be opened with either a card or a PIN if the door is configured to require card *and* PIN. Only a valid card or PIN code is needed to open the door when the time zone is valid.

Enter a time zone number or click the **Browse**  button to select a time zone.

See the "Card and PIN" section on page 78 (the card and PIN option can be configured separately for IN readers and OUT readers).

IN reader options

Each door can have up to six readers in any combination of IN readers and OUT readers.

A reader is defined as an IN reader if its **Door side** field is set to *IN reader* when it is added using the Door reader dialog (accessed from the *Readers* tab for the door). Similarly, a reader is defined as an OUT reader if its **Door side** field is set to *OUT reader* when it is added using the Door reader dialog.

Card and PIN

Select this option to require that both a card *and* a PIN must be used to unlock the door via any of the IN readers. If not selected, then either a card *or* a PIN will unlock the door via any of the IN readers.

Inhibit PIN

Select this option to require that only a card must be used to unlock the door via any of the IN readers during the low security time zone (see the “Low security TZ” section on page 77). If not selected, then both a card and a PIN must be used to unlock the door via any of the IN readers during the low security time zone.

Dual custody

When selected, two different users must present their card and/or PINs in succession in order to unlock the door via any of the IN readers.

The presentation of card and/or PIN must occur within the dual custody time (see the “Dual custody time” on page 76).

Once the two valid card and/or PINs have been presented to the reader, a 60 second timer starts, which allows the second user to perform functions such as locking the door, or alarm control (if the NAC is not in IP Direct mode).

For example, if the **IN alarm control** for the door is set to *Alarm control on 1st badge*, then the second user can present their card to disarm areas. See the “IN alarm control” section on page 85.

Similarly, if **2 badge unlock, 1 badge re-lock** is configured for the door, then the second user can present their card to lock the door. See the “2 badge unlock, 1 badge re-lock” section on page 79.

Inhibit off-site users

Select this option to prevent users who are currently recorded as being off-site (i.e. in region 0) from unlocking this door via any of the IN readers.

See the “Programming regions” section on page 66 for more information about regions.

OUT reader options

The options for IN readers (see the “IN reader options” section above) can also be applied to OUT readers.

Dual custody both users enter region

If dual custody functionality is used, then enabling this option means that both users are reported as having accessed a door. In addition, anti-passback rules and region rules (including region count) will be applied to both users. If either user fails for any reason, e.g. passback, then the door will remain locked and access will be denied when the failed user presents their card or PIN.

Disabling this option means that only the second user is reported as having accessed a door. Thus if a visitor and an accompanying guard badge their cards to open a door, only the guard is considered as having accessed the door.

2 badge unlock, 1 badge re-lock

As an alternative to dual custody, two badge unlock avoids unintended unlocking of a door if a user accidentally presents their card to a reader, for example, by brushing past the reader with the card in a pocket. When two badge unlock is enabled (and the low security time zone is not valid), the user may unlock the door by presenting the same card twice within the dual custody time (see “Dual custody time” on page 76). If the low security time zone is valid, then the two badge unlock setting is ignored (see the “Low security TZ” section on page 77).

The door will remain unlocked until a user badges a card at the reader.

Note: When two badge unlock is enabled and two different cards are presented within the dual custody time (regardless of whether dual custody is used), then the door is not unlocked and a door access denied message is generated.

Hold door unlocked until door opens

For security reasons, it is possible for the door to re-lock at the moment it opens. The door relay will be de-activated after the door is opened. This option will override the unlock time. The door will stay unlocked until opened.

When selected, after a door is unlocked by a card or PIN, the door lock relay will remain activated until the door input is unsealed.

Override after entry

This field determines whether the override time zone (see the “Override TZ” section on page 77) takes effect immediately the time zone commences or after a user enters.

When selected, the override time zone takes cannot unlock the door for the programmed times unless a user has entered.

Disable duress

When selected, the system’s keypad duress functionality cannot be used at this door.

Time & attendance reader

When selected, the reader can be used as a time and attendance reader. See the “Using time and attendance readers” section on page 117 for more information.

Note: Some management software applications do not support time and attendance functionality.

Report DOTL

When selected, a report is sent to management software when the door’s **Door input 1** is in the door open too long (DOTL) state. For example, the door is still open after the shunt timer expires.

This is only a reporting function.

Report forced door

When selected, a report is sent to management software when the door’s **Door input 1** is unsealed without valid access (card, PIN, or egress request).

This is only a reporting function.

Report door open/close

When selected, a report is sent to management software when the door’s **Door input 1** is unsealed (opened) or resealed (closed).

This is only a reporting function.

Report secured/accessed

When selected, an “unsecured” (i.e. accessed) message is sent to management software if the door is unsecured, which occurs in any of the following situations:

- Access to the door is granted to a user
- The door’s shunt timer is running
- The door is forced
- The door is opened from management software
- The door is unlocked from management software

A “secured” message is sent to management software when the door is secured.

This is only a reporting function.

Note: The behaviour contrasts with a door on a V8 Four-Door Controller, which only reports unsecured when the door’s relay is active.

Allow OUT reader access when TZ invalid

If selected, OUT readers will allow access even if a user’s door group has an invalid time zone.

Programming shunt, egress and passback options

Options for shunting, egress and anti-passback for a door are configured on the *Shunt/Egress/Passback* tab of the Doors/Lifts form.

The following figure shows the *Shunt/Egress/Passback* tab of the Doors/Lifts form:

The screenshot shows the 'Doors/Lifts - 1.1 - CH 1 Door 1' window. The 'Shunt/Egress/Passback' tab is selected. The form includes the following fields and options:

- Record:** 1
- Panel:** IP Extended NAC
- Access:** Alarm control, Hardware, **Shunt/Egress/Passback**, Readers, User defined time zones
- Shunt options:**
 - Shunt type:** Input shunting & DOTL (dropdown)
 - Shunt time:** 1 (dropdown), Min (dropdown)
 - Long shunt:** 90 (dropdown), Sec (dropdown)
 - Warning time:** 15 (dropdown), Sec (dropdown)
 - ☐ Shunt until door closes
 - ☐ Cancel shunt when door secures
- Anti-passback options:**
 - Anti-passback:** Disabled (dropdown)
 - Anti-passback time:** (dropdown), Sec (dropdown)
 - Region IN:** (dropdown)
 - Region OUT:** (dropdown)
- Egress options:**
 - Egress:** Egress timed (dropdown)
 - Egress time zone:** 0 - 24 Hour (dropdown)
 - ☐ Egress IN disabled when secure
 - ☒ Egress reporting

Shunt options

Shunting is a procedure that stops an open door causing an alarm for a set time.

Shunt type

This field defines shunt conditions. The options are:

- *No shunting* – The door will not be shunted.
- *Input shunting* – The door will be shunted and will generate a forced door alarm if it is left open (i.e. **Door input 1** is unsealed) longer than the programmed **Shunt time** (or **Ext. shunt time**, if applicable).
- *Input shunting & DOTL* – The door will be shunted and will generate a DOTL (Door Open Too Long) alarm if it is left open (i.e. **Door input 1** is unsealed) longer than the programmed **Shunt time** (or **Ext. shunt time**, if applicable).
- *Auto shunting & DOTL* – If the areas assigned to the door are in access (disarmed), shunting of the door will commence when the **Door input 1** is unsealed. No card or PIN is required. A DOTL alarm is generated if it is left open longer than the programmed **Shunt time**.

Note: If the NAC is in IP Direct mode, then this option functions the same as *Input shunting & DOTL* above.

Shunt time

Program the amount of time that the door may be opened for without causing an alarm (shunted). This allows time for a user to pass through the door and shut it again.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Long shunt

Program the amount of time for the door to be shunted when a user, with the “Long access” flag enabled, presents a valid card or PIN at the door reader.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Warning time

Program the amount of time for a relay to activate, to sound a warning device, before the **Shunt time** (or **Ext. shunt time**, if applicable) expires.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Shunt until door closes

Select this option to ignore the programmed **Shunt time** (or **Ext. shunt time**), and to shunt **Door input 1** until the door closes (i.e. the door input is resealed).

Cancel shunt when door closes

For security reasons, it may be required to limit the shunt period as much as possible in order to detect the door being opened again during the shunt time (after the debounce time of approximately 2 seconds).

Select this option to use the programmed **Shunt time** (or **Ext. shunt time**) to shunt **Door input 1** and then to cancel the shunt when the door closes (i.e. the door input is resealed).

Anti-passback options

The anti-passback options control the operation of the reader if a card or PIN is used to enter the same region that the user is currently in.

This is valid only when a region is programmed for the door. See the “Region IN” section on page 83 and the “Region OUT” section on page 83.

Anti-passback violation is reported to management software.

Note: To clear an anti-passback violation, the card must be used at another appropriate reader to change the region number that the user is recorded against.

Alternatively, anti-passback can be cleared for specific user(s) using the **Reset anti-passback**  button on the toolbar of the Users form. See the *CTPlus Operators Manual* or CTPlus online help for more information.

Note: The door must be opened after the reader is used before anti-passback will take effect.

Note: Anti-passback settings do not apply to users with the “Privileged” flag in regions 0 to 199.

Anti-passback

Select the type of anti-passback desired:

- *Disabled* – The anti-passback functionality is not active. The card will open the door without generating an alarm.
- *Soft* – The card will open the door when used the second time but an alarm will be generated.
- *Hard* – The card will not open the door when used a second time and the attempt will generate an alarm.
- *Timed Hard* – The card will not open the door when used a second time in succession at the same door within the programmed time and the attempt will generate a report.

Anti-passback time

Enter the time delay that forces the user to wait until the delay timer expires.

Enter a number and specify *Sec* for seconds or *Min* for minutes.

Region IN

Specifies a region which represents the IN readers for each door.

When a valid card or PIN is entered at the door reader, the region that the user is entering into is recorded against the user code. The system is then able to report an anti-passback violation.

Select the region by clicking the **Browse**  button, or type the region number directly into the field.

Note: The door must be opened for this to be effective.

Region OUT

Specifies a region which represents the OUT readers for each door.

When a valid card or PIN is entered at the door reader, the region that the user is entering into is recorded against the user code. The system is then able to report an anti-passback violation.

Select the region by clicking the **Browse**  button, or type the region number directly into the field.

Note: The door must be opened for this to be effective.

Egress options

The egress options define the operation of the egress button (exit button).

There are two options for setting up an egress button:

- The egress button is wired to the **Egress input** defined on the *Hardware* tab for the door. See the “Egress input” section on page 70.
- A reader assigned to the door is defined as having an egress input. See the “Enable egress” section on page 74.

Note: There must be an egress time zone defined for egress functionality to work.

Egress

Defines the operation of the egress button:

- *Egress timed* – When the egress button is pressed, the door will unlock for the **Access time** programmed on the *Access* tab for the door. See the “Access time” section on page 75.
- *Egress held* – Allows the door to be held unlocked for as long as the egress button is pressed and for the access time after the egress input is released.
- *Egress shunts only* – When the egress button is pressed, the shunt timer is started for the door input. Holding the Egress button for longer than the shunt timer, will not extend the shunt time. Pressing the egress button again during the shunt timer, will restart the shunt timer.

Egress time zone

The egress time zone controls the times when an egress button will unlock a door to allow exit. When the time zone is valid, a user can press the egress button and the door will unlock.

Select the time zone by clicking the **Browse**  button, or type the time zone number directly into the field.

Egress IN disabled when secure

Note: This option does not apply to the NAC in IP Direct mode.

This check box controls the ability to use the egress button on any IN reader to open the door if any of the areas assigned to the door (via an access control level) are secure, i.e. armed. If any of the areas assigned to the door are secure then the egress button will not unlock the door.

Egress OUT disabled when secure

Note: This option does not apply to the NAC in IP Direct mode.

This check box controls the ability to use the egress button on any OUT reader to open the door if any of the areas assigned to the door (via an access control level) are secure, i.e. armed. If any of the areas assigned to the door are secure then the egress button will not unlock the door.

Egress reporting

When selected, a report is sent to management software when the egress function is used.

This is only a reporting function.

Programming alarm control options

Note: Alarm control does not apply to the NAC in IP Direct mode.

If the NAC is connected to a Challenger*Plus* panel, it can support alarm control functionality, such as arming areas via badging a card. Alarm control functionality can be configured separately for IN and OUT readers.

Alarm control tab is described in the following sections.

Alarm control tab

The following figure shows the *Alarm control* tab of the Doors/Lifts form:

IN alarm control

This field determines whether the door's IN readers can be used to control the alarm system (arm/disarm) and if so, the way in which it can be controlled:

- *No Alarm control* – It is not possible to arm/disarm via the reader.
- *Alarm control on 1st badge* – Presentation of a valid card at the reader will disarm the system on the first badge. (Three badges are still required to arm system).

- *Alarm control on 3rd badge* – Presentation of a valid card three times at the reader will arm/disarm system.
- *Alarm control always (off = IN, on = OUT)* – Presentation of a valid card at the IN reader will disarm the system and presentation of a valid card at the OUT reader will arm the system.
- *Alarm control via region* – Alarm control is enabled by the region which is set in DGP form, Regions tab.

OUT alarm control

This field determines whether the door's OUT readers can be used to control the alarm system (arm/disarm) and if so, the way in which it can be controlled. The options are the same as for the **IN alarm control** field. See the "IN alarm control" section on page 85.

IN reader denied if area secured

Stop a user opening a door using the IN reader when any of the areas assigned to the door are armed. When selected, a valid card or PIN will not open a door if any of the areas assigned to the door are armed.

OUT reader denied if area secured

Stop a user opening a door using the OUT reader when any of the areas assigned to the door are armed. When selected, a valid card or PIN will not open a door if any of the areas assigned to the door are armed.

Auth. RAS

Note: This option only applies to the NAC in Classic mode.

This field is used to select a RAS on the Challenger*Plus* system LAN (numbered from 1 to 16 or from 65 to 80).

The selected system RAS is authorised to arm/disarm and select areas when a valid badge is presented at one of the NAC door's readers. The selected system RAS must have a keypad for area selection.

The NAC door's readers can no longer be used to open the door: they are dedicated to arming and disarming areas controlled by the nominated system RAS.

The RAS on the system LAN that is selected for arm control must also have the "Toggle keyboard control" option enabled. See the *ChallengerPlus Programming Manual* for information on the "Toggle keyboard control" option.

Enter a RAS number or click the **Browse**  button to select a RAS.

Door unlock controls IN areas

When flag is set and the door is UNLOCKED, NAC should disarm all the IN areas and arm when the door is LOCKED.

The unlock/lock operation on the door can be from any of the following:

1. Door scheduled action
2. Override Time zone
3. Manual unlock command from management software
- 4.2-badge unlock

When the door has 'Override after entry' also set in Access options, the door remains locked when Override time zone becomes active and the areas will still remain armed, until a valid user card/PIN is presented. When this occurs, the door will unlock and disarm the IN areas.

NAC will request the Disarm and Arm on the door's IN areas as SYSTEM USER.

Lock door when IN areas armed

When flag is set and all the IN areas associated with the door IN alarm control are ARMED, NAC will automatically LOCK the door.

Low security when IN areas disarmed

When flag is set and all the IN areas associated with the door IN alarm control are DISARMED, NAC will automatically enable Low security on the door (similar to the Low security TZ setting in door access options).

This is only valid if 'Card and PIN' option set on the door IN Reader.

Unlock door when IN areas disarmed

If flag is set, the door is automatically UNLOCKED when all areas assigned to the door IN alarm control are DISARMED.

If a door override time zone (TZ) or user defined door override TZ is assigned, it postpones until all areas are DISARMED as well as TZ being valid.

If door 'Override after entry' is also set, this is also taken into account for the 1st unlock.

IN alarm control levels

This field shows a list of alarm control levels for the door's IN readers, as configured on the *Readers* tab for the door. Alarm control levels are defined on the DGP form's Alarm Control Levels.

Click the **Assign**  button to open a dialog to assign alarm control levels to the door's IN readers. In the dialog, move the required alarm control levels from the **Available alarm control levels** list to the **Assigned alarm control levels** list using the  button. Alarm control levels can be removed from the **Assigned alarm control levels** list using the  button. Click the **OK** button when finished.

Click the **Remove**  button to remove the selected alarm control level from the **IN alarm levels** list.

OUT alarm control levels

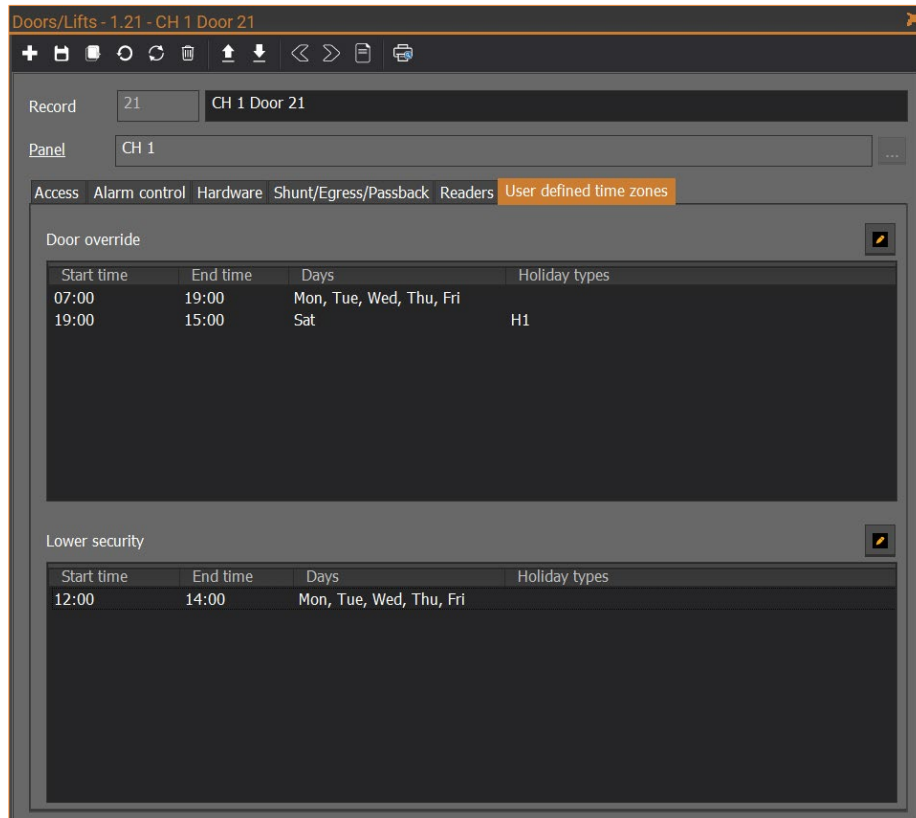
This field shows a list of alarm control levels for the door's OUT readers, as configured on the *Readers* tab for the door. Alarm control levels are defined on the DGP form's Alarm Control Levels.

Click the **Assign**  button to open a dialog to assign alarm control levels to the door's OUT readers. In the dialog, move the required alarm control levels from the **Available alarm control levels** list to the **Assigned alarm control levels** list using the  button. Alarm control levels can be removed from the **Assigned alarm control levels** list using the  button. Click the **OK** button when finished.

Click the **Remove**  button to remove the selected alarm control level from the **OUT alarm levels** list.

Programming user defined time zones

The User defined time zones tab allows the user to assign up to 8 time zone segments each for Door override of Lower security configuration for a NAC door. The settings are independent of the Panel time zones and provide more granular control at NAC door level. Also, the user defined time zones cannot be overwritten by management software when they delete/reprogram the panel time zones.



Door override

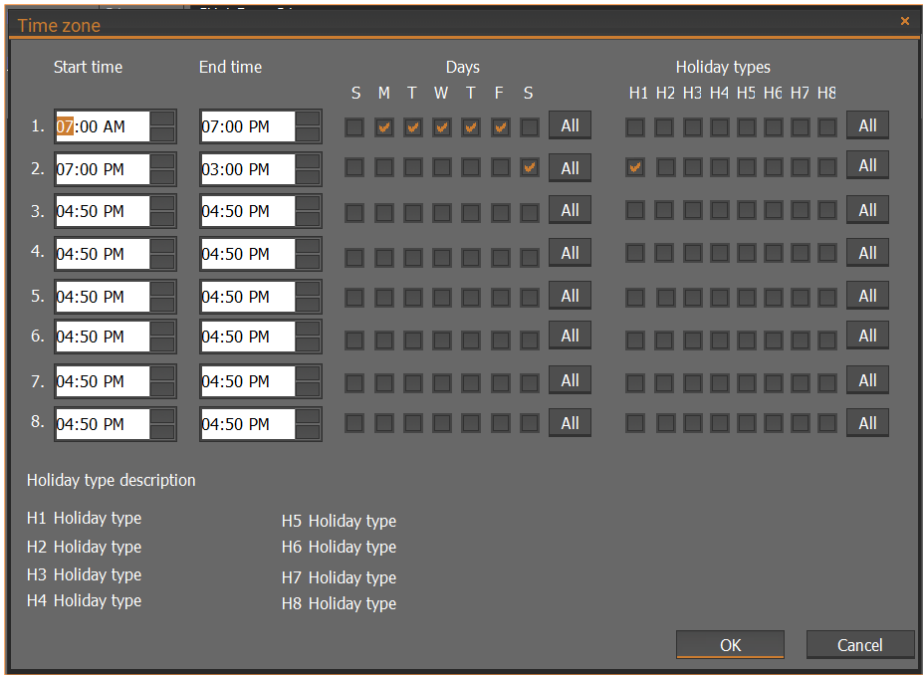
This field shows a list of configured Door override time zones. The Door override is similar to the legacy 'Override TZ' setting under the Access tab. It allows user to control the times when the door can be opened without need to use a valid card or PIN. Free access is allowed when the time zone segments are valid.

Click the Edit  button to open the Door time zone dialog to edit the 8 time zone segments for the NAC door. By default, all the time zone segments are disabled and not active.

Lower security

This field shows a list of Lower security time zones for the door. Lower security is similar to the legacy 'Low security TZ' setting under the Access tab. It allows user to control the times when the door can be opened with either a card or a PIN if the NAC door is configured to require 'card and PIN'. Only a valid card or PIN is enough to open the NAC door when the Lower security time zone is valid.

Click the Edit  button to open the Door time zone dialog to edit the 8 time zone segments for the NAC door. By default, all the time zone segments are disabled and not active.



	Start time	End time	S	M	T	W	T	F	S	All	H1	H2	H3	H4	H5	H6	H7	H8	All
1.	07:00 AM	07:00 PM	☒	☒	☒	☒	☒	☒	☒	All	☐	☐	☐	☐	☐	☐	☐	☐	All
2.	07:00 PM	03:00 PM	☐	☐	☐	☐	☐	☐	☒	All	☒	☐	☐	☐	☐	☐	☐	☐	All
3.	04:50 PM	04:50 PM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	All
4.	04:50 PM	04:50 PM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	All
5.	04:50 PM	04:50 PM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	All
6.	04:50 PM	04:50 PM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	All
7.	04:50 PM	04:50 PM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	All
8.	04:50 PM	04:50 PM	☐	☐	☐	☐	☐	☐	☐	All	☐	☐	☐	☐	☐	☐	☐	☐	All

Holiday type description

H1 Holiday type	H5 Holiday type
H2 Holiday type	H6 Holiday type
H3 Holiday type	H7 Holiday type
H4 Holiday type	H8 Holiday type

OK Cancel

Door time zone dialog

The NAC door time zone dialog is similar to the Panel time zone form. The settings include 8 time zone segments consisting of Start/End time, Days and Holiday types for which this time zone will be active.

Times

Each door override record contains one to eight sub-time zones. A start time and end time must be programmed for at least the first sub-time zone:

- **Start time:** The start time requires an hour, minute, and AM or PM to indicate when the sub-time zone begins.
- **End time:** The end time is programmed in the same way as the start time to indicate when the sub-time zone ends.

Days

Tick the check boxes to indicate the days of the week (SMTWTFS) that the sub-time zone is valid.

Holiday types

Tick the check boxes to indicate that the sub-time zone is valid on holidays of particular types. Holidays may have up to eight defined holiday types.

Note: A sub-time zone is invalid on any defined holiday unless the holiday’s type is included in the sub-time zone.

Holiday type description

For information purposes, each holiday type is listed with its name in these read-only fields.

Programming lifts

A lift consist of two components, a lift car and the number of floors.

In the door/lift creation wizard as seen on page 67, by selecting lift in the access type the user will be able to utilise the lift programming functionality.

Programming lift options

The following figure shows the Lift tab of the Doors/Lift form:

The screenshot shows a software interface for configuring a lift. The title bar reads "Doors/Lifts - 1.17 - CH 1 Lift 17". Below the title bar is a toolbar with icons for adding, deleting, saving, undo, redo, and printing. The main form has two tabs: "Lift" (selected) and "Readers". The "Lift" tab contains the following fields and controls:

- Record:** 17
- Panel:** CH 1
- Door type:** Lift car (dropdown menu)
- Access time:** 5 (text input) with a unit dropdown set to "Sec".
- Long access time:** 15 (text input) with a unit dropdown set to "Sec".
- Lift override group:** (text input) with a dropdown arrow.
- Lift security group:** (text input) with a dropdown arrow.
- Security key:** None (dropdown menu).
- Location:** (text input).
- Polled address:** (text input).
- Device number:** (text input).
- Wait for floor selection:** (checkbox, currently unchecked).

Door type

The door type is set as Lift car and cannot be changed.

Access time

Program the amount of time that the lift buttons will be enabled when a user enters a valid card or PIN at the door reader. The user is then able to press the floor button they wish to travel to during the access time.

Enter a number and specify Sec for seconds or Min for minutes.

Long Access time

Program the amount of time that the lift buttons will be enabled when a user with the Long Access flag enabled (the Long access field can be found on the Cards tab of the Users form), presents a valid card or PIN at the lift reader. The user is then able to press the floor button they wish to travel to during the extended access time.

Enter a number and specify Sec for seconds or Min for minutes.

User Lift Access Notes:

1. When the user credential is valid, and the door/floor group has lift/floors that are in time zone. The floors in the user floor group that are within the time zone will be accessed for the period of either the Lift access time, or the lift Long Access timer if the user credential has the Long Access Flag set. Any floors already overridden (in accessed state) by other means will not be changed. After the access time has expired, the "Access Granted" event will be generated with the Lift and User number.
2. When the user credential is valid and the door/floor group has lift/floors that are in time zone, in addition the floor input mapping is configured. The floors in the user's floor group that are within the time zone will be accessed for the period of either the Lift access time, or the lift Long Access time (if the user credential has the Long Access Flag set). Any floors already overridden (in accessed state) by other means will not be changed. If a floor button is pressed and the floor input is mapped, the "Access Granted Floor" event will be generated with the Lift, Floor and user number. If a floor button is pressed, the access timer will be terminated. If no button presses are detected when the access time has expired, the "Access Granted" event will be generated with the lift and user number.
3. If a user is configured as Dual Custody type, then a second user will need to present a card prior to the lift giving access. In the same way as a door, the second user is the authorizing user only, and the floors accessible will be determined from the first users floor group. The dual custody time for the lift is fixed at the default 8 seconds. If a dual custody user presents a credential and no other credential is presented after 8 seconds, the event "Access denied: Dual custody timeout" is reported.
4. If a user is configured as a Visitor type then a guard user must authorize the visitor before the floors become available. The visitor must present the credential to the reader first, followed by the guard. Both the guard and visitor must have access to the lift (Door Group). The dual custody time for the lift is fixed at the default 8 seconds. If a Visitor presents a card but no guard presents a credential within 8 seconds, the event "Access denied: Dual custody timeout" is reported.

Lift override group

Enter the designated floor group that determines the floors that may be freely accessed in the lift controls, and the times during which they can be in access, without using a valid card or PIN at the lift reader.

Select the floor group by clicking the Browse  button, or type the floor group number directly into the field. See “Programming floor groups” on page 106 for more information.

Lift security group

Enter the floor group that determines the floors that may be freely accessed in the lift controls, and the times during which they can be in access, without using a valid card or PIN at the lift reader, provided that the security key input is activated (see Security key below).

Select the floor group by clicking the Browse  button, or type the floor group number directly into the field. See “Programming floor groups” on page 106 for more information.

Security key

Enter the NAC security key Input address. If the security key input is activated, then the lift security floor group (see Lift security group above) is activated.

Program the input using the scheme described in the Flexible device locations section on page 19.

Lift cars often have a key slot on the lift car control panel. Keys are provided to security or fire personnel. A pre-defined set of floors can be accessed (by assigning a Lift security group) when a key is used in a lift car. The NAC uses an input to determine the state of the key.

Wait for floor selection

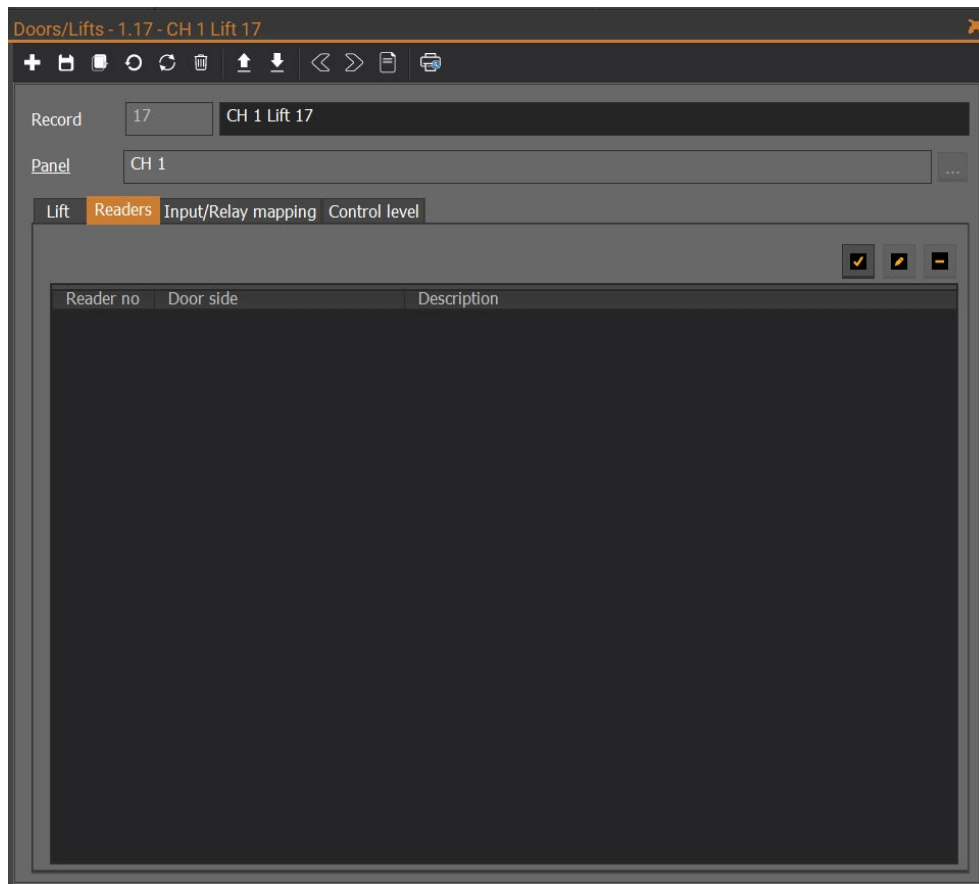
Wait for floor selection before going on. This flag is valid only when the Floor Input mappings are configured for Floors to detect which Floor has been selected by the user.

Tickd – The lift will wait for only one floor to be selected before going on.

Unticked – When the user is allowed access to multiple floors, multiple floors may be selected.

Programming reader options

The following figure shows the Readers tab of the Doors/Lift form:



Each lift can have up to six readers associated with it in any combination of IN and OUT readers.

This tab shows a list of assigned readers for the lift.

Note: If the reader is attached to one of the NAC's buses, then the reader must be assigned to the NAC on the Assigned RAS tab of the NAC, and polled. Similarly, if the reader is attached to a DGP which is attached to one of the NAC's buses, then the DGP must be assigned to the NAC on the Assigned DGP tab of the NAC, and polled.

Click the Assign  button to open the Door reader dialog to assign a reader to the lift.

Click the Edit  button to open the Door reader dialog to edit the settings of the selected assigned reader in the reader list.

Click the Remove  button to remove the selected reader from the reader list.

The process of assigning readers is similar to the method described in "Assigning readers to doors" on page 71.

Programming input and relay mapping options

The following figure shows the Input/Relay mapping tab of the Doors/Lift form:

The screenshot shows a software interface for configuring lift settings. The title bar reads "Doors/Lifts - 1.17 - CH 1 Lift 17". Below the title bar is a toolbar with icons for adding, deleting, and saving. The main area has a "Record" field with the value "17" and a "Panel" dropdown set to "CH 1". There are four tabs: "Lift", "Readers", "Input/Relay mapping" (which is selected and highlighted in orange), and "Control level". The "Input mapping" section contains a table with columns "Floor ...", "Description", "Location", "Address", and "Device no". The "Relay mapping" section also contains a table with the same columns. Both tables are currently empty.

Floor Input mapping

A lift may have button pressed outputs for each floor of the lift car. Each output can be wired to an input on the NAC to register which floor has been selected.

When a valid card is badged, the floor relays will be toggled to their active state for the defined access time and one of the two events may occur:

Without input mapping

- When the defined access time expires, the floor relays will be toggled back to their normal state, and an event will be generated and reported stating which **user** badged and which **lift** they badged at

With input mapping

- When a monitored floor button is pressed within the defined access time, the floor relays will immediately be toggled back to their normal state (without waiting for the remaining access time to expire), and an event will be generated with a report stating which **user** badged, which **lift** they badged at, and which **floor** was selected

The Floor Input mapping field shows a list of Floor input mappings for the NAC Lift.

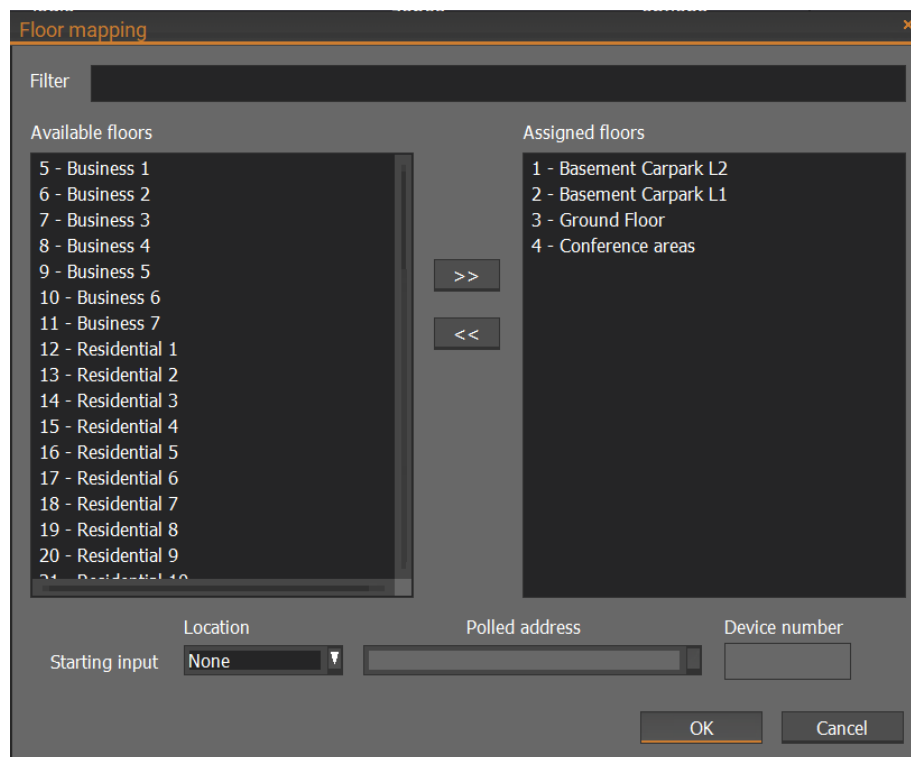
Click the Assign  button to open the Floor Input mapping dialog to add new floor input mappings for the lift.

Click the Edit  button to open the Floor Input mapping dialog to edit the selected floor input mapping in the floor Input mapping list.

Click the Remove  button to remove the selected floor input mapping from the Floor Input mapping list.

Floor input mapping dialog

The following figure shows an example of the dialog:



Available floors

Select which floors will be assigned to this lift for the purpose of monitoring floor inputs

Starting input

Choose the starting input number on the NAC (or a device connected to the NAC) to be programmed for the selected floor range. This will assign the selected input to the first assigned floor, and will increment the input number by 1 for each assigned floor. In the event that there are more floors selected than available inputs in the starting range, all floors outside of that range will be configured as 'Location: None' so that the operator may manually modify these later.

Note: You can add multiple batches starting at different input ranges by simply performing these steps multiple times.

Program the input using the scheme described in the Flexible device locations section seen on page 19.

Floor Relay mapping

The Floor Relay mapping field shows a list of Floor relay mappings for the NAC Lift.

The relay output controlled by the NAC is wired to the physical lift system. Each configured relay mapping controls the floor button availability for a specific floor of the NAC lift. When a person presents their credentials to the lift, the NAC checks their floor group and determines which floors they have access to. The NAC will toggle the authorised floor button(s) and allow the user to press it. This ensures that when a person presses their desired floor button, the signal is received by the lift and the lift may travel to that floor.

The relays operate in an inverted fail-safe mode. Therefore, if the NAC loses power or fails, all floors controlled by it become free access.

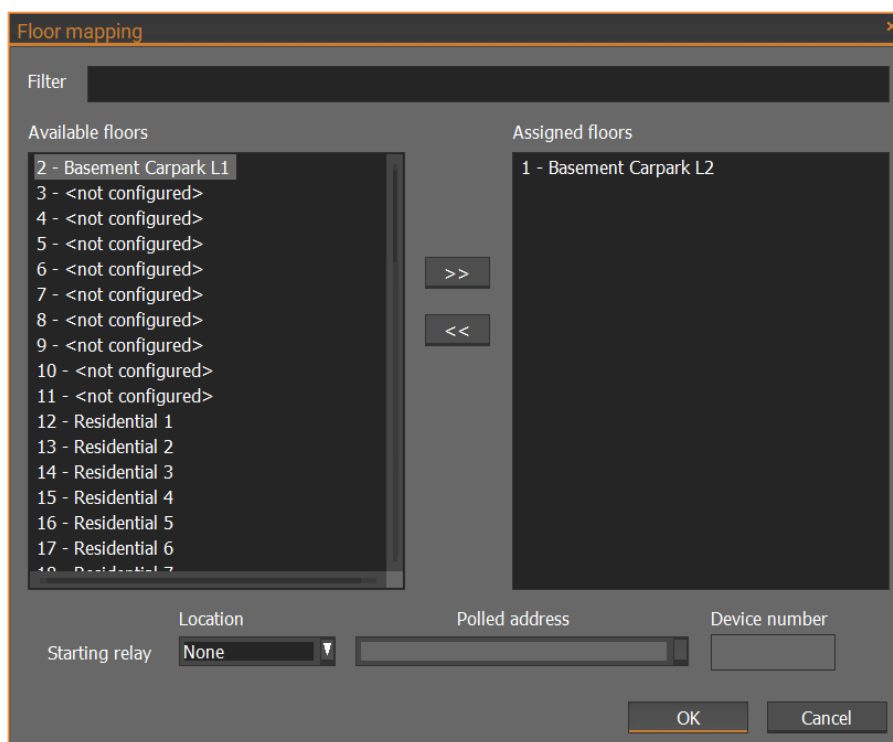
Click the Assign  button to open the Floor Relay mapping dialog to add new Floor Relay mappings for the lift.

Click the Edit  button to open the Floor Relay mapping dialog to edit the selected floor relay mapping in the floor Relay mapping list.

Click the Remove  button to remove the selected floor relay mapping from the Floor Relay mapping list.

Floor relay mapping dialog

The following figure shows an example of the dialog:



Available floors

Select which floors will be assigned to this lift.

Starting relay

Choose the starting relay number on the NAC (or a device connected to the NAC) to be programmed for the selected floor range. This will assign the selected relay to the first assigned floor, and will increment the relay number by 1 for each assigned floor. In the event that there are more floors selected than available relays in the starting range, all floors outside of that range will be configured as 'Location: None' so that the operator may manually modify these later. The relay will be activated once assigned to a floor to indicate Floor Secure mode.

Note: You can add multiple batches starting at different relay ranges by simply performing these steps multiple times.

Program the input using the scheme described in the Flexible device locations section seen on page 19.

Programming control level options

Lift override control levels

This field shows a list of Lift override control levels for the lift. Lift control levels are defined on the NAC DGP Lift control levels tab.

Click the Assign  button to open a dialog to assign lift control levels to the lift. In the dialog, move the required lift control levels from the Available lift control levels list to the Assigned lift control levels list using the  button. Lift control levels can be removed from the Assigned lift control levels list using the  button. Click the OK button when finished.

Click the Remove  button to remove the selected lift control level from the lift control levels list.

The lift override control level feature allows one or more floors to automatically access during a specified time zone and secured outside of that time zone.

When the time schedule for any assigned lift control level becomes active, the floors associated with the level will automatically access. A “Floor auto accessed” event is reported for each floor that becomes accessed.

When the time schedule for any assigned lift control level ends, the floors associated with the level will automatically secure if no other overrides are present and the “Floor auto secured” event is reported for each floor that is secured.

A Lift override will not function if the lift is disabled.

Security key override control levels

This field shows a list of Lift security key override control levels for the lift. Lift control levels are defined on the NAC DGP Lift control levels tab.

Click the Assign  button to open a dialog to assign lift security key override control levels to the lift. In the dialog, move the required lift control levels from the Available lift control levels list to the Assigned lift control levels list using the  button. Lift security key override control levels can be removed from the Assigned lift control levels list using the  button. Click the OK button when finished.

Click the Remove  button to remove the selected lift control level from the lift control levels list.

When the Security key input (configured under the Lift tab) is activated, the time schedules for the lift control levels assigned will be evaluated and the appropriate floors will be accessed.

A “Floor auto accessed” event is reported for each floor that changes state to access.

If while the key is active, time schedules for any lift control level become active, floors associated with the level will be accessed.

If while the key is active, time schedules for any lift control level become inactive, floors associated with the level will be secured.

When the security key is deactivated, floors that were activated by the key will be returned to Secure state if no other overrides are present.

A “Floor auto secured” event is reported for any floor that changes state to secure.

While the lift is disabled, if the security key is changed, the security key override will be performed. (Access and secure depending on Security key position).

Programming input and relay mapping

See the “Input and relay mapping” section on page 22 for information on input and relay mapping.

Note: Input and relay mapping does not apply to the NAC in IP Direct mode.

The Network Access Controller's input and relay mappings can be programmed on the *Input/Relay mapping* tab of the DGPs form. Click the **DGPs** button on the *Panel programming* ribbon tab to open the DGPs form.

The screenshot shows the 'DGPs - 1.1 -' window. At the top, there's a toolbar with various icons. Below it, the 'Record' field is set to '1' and the 'Panel' field is set to 'CH 1'. The main area has several tabs: 'Setup', 'NAC options', 'Input/Relay mapping' (which is selected), 'Assigned RAS', 'Assigned DGP', 'Alarm control levels', 'Regions', and 'Lift control levels'. Under the 'Input/Relay mapping' tab, there are two sections: 'Input mapping' and 'Relay mapping'. Each section has a table with columns for 'Input no', 'Input type', 'Door', 'Location', 'Address', and 'Device no'. To the right of each table are three buttons: a checkmark, a pencil, and a minus sign.

Programming input mapping

The **Input mapping** shows a list of input mappings.

Click the **Add** button to open the Input mapping dialog to add a new input mapping.

Click the **Edit** button to open the Input mapping dialog to edit the selected input mapping in the **Input mapping** list.

Click the **Remove** button to remove the selected input mapping from the **Input mapping** list.

Note: NAC inputs are masked if they are not mapped to Challenger*Plus* input numbers.

The following figure shows the Input mapping dialog:

The screenshot shows the 'Input mapping' dialog box. It has a title bar 'Input mapping'. Inside, there are several fields: 'Input no' with a dropdown menu, 'Input type' with a dropdown menu showing 'Not Used (reports sealed)', 'Door' with a text field and a dropdown arrow, 'Location' with a text field, 'Polled address' with a text field, and 'Device number' with a text field. At the bottom, there are 'OK' and 'Cancel' buttons.

Input no

Enter a number in the range 1 to 32. The mapped input number is an index into the Challenger*Plus* input numbering scheme. Thus, for the NAC with address 1 on the Challenger*Plus* panel's LAN1, mapped input numbers 1 to 32 correspond to Challenger*Plus* input numbers 17 to 48. See the "Input and relay mapping" section on page 22 for information on Challenger*Plus* input mapping.

Input type

Specify the input type for the input mapping. The input types are:

- *Not used (reports sealed)* – the input always reports as sealed. This type of input cannot be assigned to a door.
- *Forced* – the input is a logical input associated with a door and is unsealed when the door has a Forced Door alarm (from the door's **Door input 1** being unsealed) or there is a tamper condition. Specify the door in the **Door** field.
- *Egress* – the input is a logical input associated with a door and is unsealed when the door is in egress condition (i.e. the door's **Egress input** is unsealed) or there is a tamper condition. Specify the door in the **Door** field.
- *DOTL* – the input is a logical input associated with a door and is unsealed when the door has a Door Open Too Long (DOTL) alarm (from the door's **Door input 1** being unsealed). Specify the door in the **Door** field.
- *Shunted Pass through* – the input is a physical input which is passed through to the Challenger*Plus* panel if the associated door is not shunting. Specify the door in the **Door** field. The input location must be specified in the **Input** field.
- *Direct Pass through* – the input is a physical input which is passed directly through to the Challenger*Plus* panel. This type of input cannot be assigned to a door. The input location must be specified in the **Input** field.

Door

If the **Input type** field is one of *Forced*, *Egress*, *DOTL*, or *Shunted pass through*, then you must specify a door to be associated with the input mapping.

Enter the door number or click the **Browse**  button next to the **Door** field to associate the door with the input mapping.

Input

If the **Input type** field is one of *Shunted pass through* or *Direct pass through*, then an input device must be specified in the **Input** field, using the scheme described in the "SALLIS" section on page 19 or the "Flexible device locations" section on page 20.

Programming relay mapping

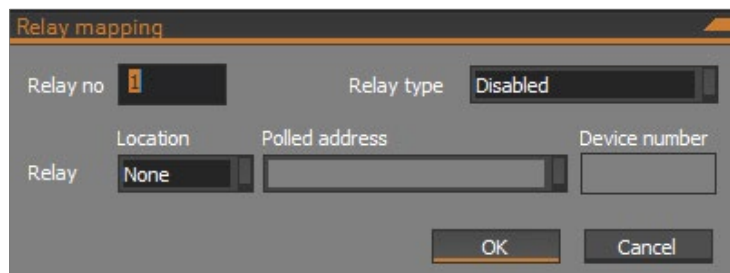
The **Relay mapping** shows a list of relay mappings.

Click the **Add**  button to open the Relay mapping dialog to add a new relay mapping.

Click the **Edit**  button to open the Relay mapping dialog to edit the selected relay mapping in the **Relay mapping** list.

Click the **Remove**  button to remove the selected relay mapping from the **Relay mapping** list.

The following figure shows the Relay mapping dialog:

The image shows a 'Relay mapping' dialog box. It has a title bar with the text 'Relay mapping'. Inside, there are several fields: 'Relay no' with a numeric input field showing '1'; 'Relay type' with a dropdown menu showing 'Disabled'; 'Location' with a dropdown menu showing 'None'; 'Polled address' with a text input field; and 'Device number' with a text input field. At the bottom right, there are 'OK' and 'Cancel' buttons.

Relay no

Enter a number in the range 1 to 16. The mapped relay number is an index into the Challenger*Plus* relay numbering scheme. Thus, for the NAC with address 1 on the Challenger*Plus* panel's LAN1, mapped relay numbers 1 to 16 correspond to Challenger*Plus* relay numbers 17 to 32. See the “Input and relay mapping” section on page 22 for information on relay mapping.

Activating the Challenger*Plus* relay will activate the specified relay device attached to the NAC.

Note: Relays that are not mapped to a device may be used as an input to a macro.

Relay type

Specify the relay type for the relay mapping. The relay types are:

- **Disabled** – The relay is disabled.
- **Direct map** – The relay is directly mapped from the Challenger*Plus* to the relay specified in the **Relay** field.

Relay

The relay location must be specified using the scheme described in the “SALLIS” section on page 19 or the “Flexible device locations” section on page 20.

Programming mapped inputs and relays

On the attached Challenger*Plus*, program the mapped inputs and relays as required.

Programming mapped inputs

To program a mapped Challenger*Plus* input, do the following in CTPlus:

1. Click the **Inputs**  button on the *Panel programming* ribbon tab to open the Inputs form.
2. On the Inputs form, click the **New**  button in the toolbar to add a new input record.
3. Enter the appropriate input number in the **Record** number field. Refer to Table 5 on page 25 for information on the possible input numbers, depending on the address of the NAC and the Challenger*Plus* system LAN the NAC is connected to.
4. Enter a description for the input in the **Record** description field.
5. Ensure the **Panel** field is set to the Challenger*Plus* panel that the NAC is connected to via its system LAN. If necessary, click the **Browse**  button next to the **Panel** field to select the Challenger*Plus* panel.
6. Configure the input as required on the *Setup* and *Events* tabs. Refer to the *ChallengerPlus Programming Manual* for information on input configuration.
7. Click the **Save**  button in the toolbar to save the input record.

Programming mapped relays

To program a mapped Challenger*Plus* relay, do the following in CTPlus:

1. Click the **Relays**  button on the *Panel programming* ribbon tab to open the Relays form.
2. On the Relays form, click the **New**  button in the toolbar to add a new relay record.
3. Enter the appropriate relay number in the **Record** number field. Refer to Table 5 on page 25 for information on the possible relay numbers, depending on the address of the NAC and the Challenger*Plus* system LAN the NAC is connected to.
4. Enter a description for the relay in the **Record** description field.
5. Ensure the **Panel** field is set to the Challenger*Plus* panel that the NAC is connected to via its system LAN. If necessary, click the **Browse**  button next to the **Panel** field to select the Challenger*Plus* panel.
6. Configure the relay as required on the *Setup* tab. Refer to the *ChallengerPlus Programming Manual* for information on relay configuration.
7. Click the **Save**  button in the toolbar to save the relay record.

Programming macro logic

Macro logic provides a powerful tool for activating (or deactivating) events controlled by programmed conditions. The programmed conditions are logic

equations combining the macro inputs (macro events) and timed or latched output conditions.

Up to 48 macros can be defined for the Network Access Controller.

Macro events are used as the macro logic program's inputs. Up to four macro inputs may be included in the logic equation. Each macro input in the logic equation can be programmed as an AND or an OR function and may be inverted to formulate NAND and NOR equations.

Options are provided so that the macro's result will trigger a macro output (event), which may be a pulse, timed, on delay, off delay or latched when activated. The output event can be inverted.

For more information on macro logic programming, refer to the *ChallengerPlus Programming Manual*.

To program a DGP macro for the NAC, do the following in CTPlus:

1. Click the **Macro logic**  button on the *Panel programming* ribbon tab and select **DGP macros** from the drop-down list to open the DGP macros form.
2. On the DGP macros form, click the **New**  button in the toolbar to add a new macro record.
3. Enter a description for the macro in the **Record** description field.
4. Ensure the **DGP** field is set to the NAC. If necessary, click the **Browse**  button next to the **DGP** field to select the NAC.
5. Configure the macro as required on the *Setup* tab. Refer to the "Macro options" section below.
6. Click the **Save**  button in the toolbar to save the macro record.

Macro options

Function

The result of the macro's logic and the macro's output function will trigger an event flag. The macro's output may have timing functions.

- *Disabled* – This macro logic program is disabled.
- *Non-timed* – Follows the result of the logic equation only. If a macro input for this macro changes, the logic equation will be calculated again.
- *On pulse (1-255) seconds* – Activates for the programmed time or the active period of the logic result, whichever is the shortest.
- *On pulse (1-255) minutes* – Activates for the programmed time or the active period of the logic result, whichever is the shortest.
- *On timed (1-255) seconds* – Activates for the programmed time regardless of the macro inputs changing.
- *On timed (1-255) minutes* – Activates for the programmed time regardless of the macro inputs changing.

- *On delay (1-255) seconds* – Activates after the programmed time period unless the result of the logic equation is no longer valid.
- *On delay (1-255) minutes* – Activates after the programmed time period unless the result of the logic equation is no longer valid.
- *Off delay (1-255) seconds* – Follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active.
- *Off delay (1-255) minutes* – Follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active.
- *Latched* – Activates on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input (any programmed AND / OR function is not used).

Duration

Enter the time period (1 to 255 seconds or minutes) that is used when any of the timed macro output functions are selected (*On pulse*, *On timed*, *On delay*, or *Off delay*).

When

Enables programming of up to four logic inputs, which can be a wide variety of conditions such as *Door open too long*, each corresponding to a specific DGP event. For each logic input, select the logic input type, then either select the specific device the condition relates to (e.g. door) by clicking the  button, or by entering the number of the device (e.g. input) directly into the field.

The events used as macro conditions are pre-defined as listed in “Macro events” on page 118. Some can only be used for macro inputs, some for macro outputs, and others may be used for either inputs or outputs.

The input can be set to *Disabled* to disable the condition.

The DGP event number corresponding to the condition is calculated and displayed to the right of the  button.

The logic connecting the four logic inputs can be programmed for AND or OR functions. A NAND or NOR function can be achieved by inverting the logic of the particular input with the **Not** check box.

Activate

This programmed DGP event will be activated when the result of the logic equation is true and any timing conditions are met. Select the type of entity to activate (e.g. *Door lock*), then either select the specific device the DGP event relates to (e.g. door) by clicking the  button, or by entering the number of the device (e.g. input) directly into the field.

The output can be set to *Disabled* to disable to activation.

The DGP event number corresponding to the programmed DGP event is calculated and displayed to the right of the  button.

Programming user information

Programming door groups

Note: Typically, door groups will be configured using TecomC4. The following information is for using CTPlus to program door groups if required.

A NAC in Classic mode inherits the door groups of the ChallengerPlus it is connected to, so is limited to 255 door groups. You can add NAC doors to existing door groups or create new ChallengerPlus door groups for the NAC doors.

A NAC in IP Direct or IP Extended mode uses NAC door groups, of which there can be up to 10,000.

To add a door group to a NAC or ChallengerPlus panel, follow these steps:

1. Click the **Door groups**  button on the *User access* ribbon tab to open the Door groups form.
2. On the Door groups form, click the **New**  button in the toolbar to add a new door group record.
3. Enter a description for the door group in the **Record** description field.
4. Ensure the **Panel** field is set to the correct NAC or ChallengerPlus panel. If necessary, click the **Browse**  button next to the **Panel** field to select the NAC or ChallengerPlus panel.
5. On the *Door group* tab, click the **Assign**  button to open a dialog to assign doors to a door group. In the dialog, select the **Time zone** for the door group. Move the required doors from the **Available doors** list to the **Assigned doors** list using the  button. Areas can be removed from the **Assigned doors** list using the  button. Click the **OK** button when finished.
6. Click the **Save**  button in the toolbar to save the door group record.

Refer to the *ChallengerPlus Programming Manual* for more information on door groups. Refer to the *CTPlus Operators Manual* or CTPlus online help for more information on the Door groups form.

Programming floor groups

Note: Typically, floor groups will be configured using TecomC4. The following information is for using CTPlus to program floor groups if required.

A NAC in Classic mode inherits the floor groups of the ChallengerPlus it is connected to, so it is limited to 128 floor groups. You can add NAC floors to existing floor groups or create new ChallengerPlus floor groups for the NAC floors. Access to floors for NAC lifts is configured within the ChallengerPlus floor group and NAC lift access is configured in the ChallengerPlus door groups.

A NAC in IP Direct or IP Extended mode uses NAC floor groups, of which there can be up to 1,000.

To add a floor group to a NAC or Challenger*Plus* panel, follow these steps:

1. Click the **Floor groups**  button on the *User access* ribbon tab to open the Floor groups form.
2. On the Floor groups form, click the **New**  button in the toolbar to add a new floor group record.
3. Enter a description for the door group in the **Record** description field.
4. Ensure the **Panel** field is set to the correct NAC or Challenger*Plus* panel. If necessary, click the **Browse**  button next to the **Panel** field to select the NAC or Challenger*Plus* panel.
5. On the *Floor group* tab, click the **Assign**  button to open a dialog to assign floors to a floor group. In the dialog, select the **Time zone** for the floor group. Move the required floors from the **Available floors** list to the **Assigned floors** list using the  button. Areas can be removed from the **Assigned floors** list using the  button. Click the **OK** button when finished.
6. Click the **Save**  button in the toolbar to save the floor group record.

Refer to the *ChallengerPlus Programming Manual* for more information on floor groups. Refer to the *CTPlus Operators Manual* or CTPlus online help for more information on the Floor groups form.

Programming users

Note: Typically, users will be configured using TecomC4. The following information is for using CTPlus to program users if required.

A NAC in Classic mode inherits the users of the Challenger*Plus* panel it is connected to, so is limited to 2,000 users (or 65,535 users if the Challenger*Plus* panel has a TS1084 Memory Expansion Module).

A NAC in IP Direct or IP Extended mode has its own user database of up to 250,000 users. You can add new users for the NAC, or configure NAC access and credentials for existing users in the CTPlus database.

To add a new user to a NAC, follow these steps:

1. Click the **Users**  button on the *User access* ribbon tab to open the Users form.
2. On the Users form, click the **New**  button in the toolbar to add a new user record.
3. Enter the required information on the *User* tab.
4. On the *Access* tab, ensure that the Door groups field has a door group entry that has NAC doors. Click the **Assign**  button to open a door group selection dialog. Select a door group and click the **OK** button.
5. Click the **Save**  button in the toolbar to save the user record.

6. On the *Cards* tab, click the **New**  button to add a new card. In the Cards dialog, ensure the **Panel** field is set to the relevant NAC or *ChallengerPlus* panel, and enter the card data and PIN as required. Click the **OK** button when finished.
7. Click the **Save**  button in the toolbar to save the user record.

Refer to the *ChallengerPlus Programming Manual* for more information on users. Refer to the *CTPlus Operators Manual* or CTPlus online help for more information on the Users form.

Note: A NAC in Classic mode is limited to 48 bits of card data. A NAC in IP Direct or IP Extended mode supports up to 128 bits of card data. However, in IP Extended mode, cards with more than 48 bits of card data cannot be used for alarm control functionality.

Management via CTPlus

Note: Typically, management of a NAC will be done using TecomC4. The following information is for using CTPlus to manage a NAC if required.

CTPlus can be used to manage the Network Access Controller:

- The status of the NAC can be viewed in the device tree in the Status and control window. See the “Status and control” section below.
- Devices can be controlled from the device tree by sending commands in the Status and control window. See the “Status and control” section below.
- Up to 100 door schedules can be configured via the Door schedule form, as described in the “Configuring door/lift schedules” section on page 115. For more information on door schedules, see the “Overriding door state” section on page 26.
- A door override can be configured for each door via the Door override form, as described in the “Programming user defined time zones” section on page 89. For more information on door overrides, see the “Overriding door state” section on page 26.

Status and control

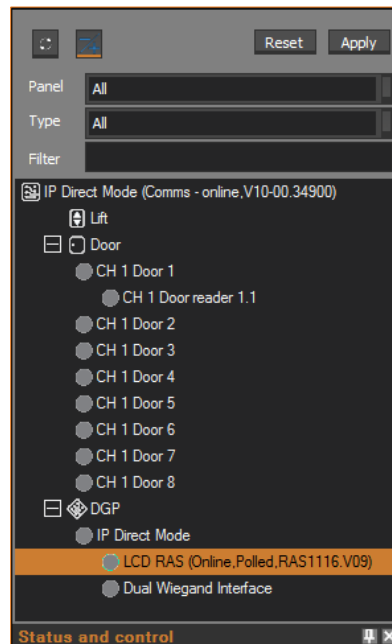
The Network Access Controller can be monitored for its status (including the status of polled devices on its buses) and controlled via CTPlus’s **Status and Control** window.

To open the Status and Control window, click the **Status and Control**  button on the *Operation* ribbon tab.

The NAC devices that appear in the device tree of the Status and control window depend on the operating mode of the NAC.

Direct mode

In IP Direct mode, the NAC appears as a distinct NAC panel  connection. For example:

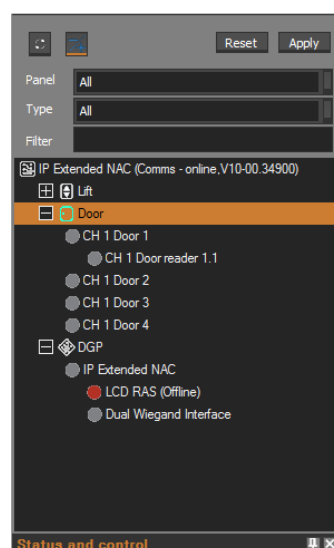


The NAC also appears as a DGP  category (DGP number 16) of the NAC panel connection. The NAC's assigned RASs and DGPs appear as sub-devices under the NAC's DGP node.

The NAC's doors appear as doors under the Door  category of the NAC panel connection.

IP Extended mode

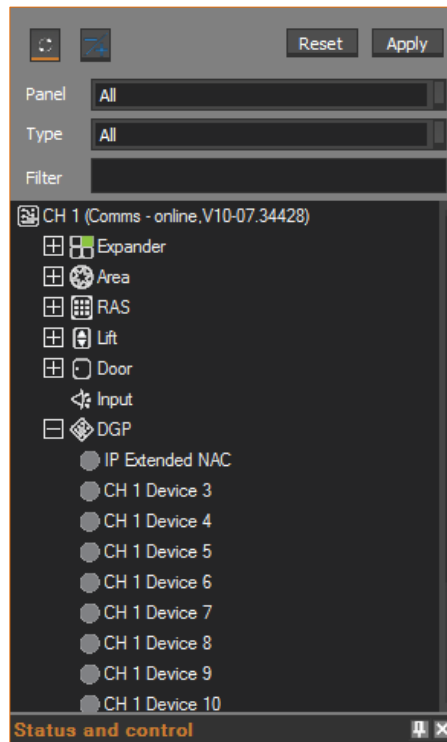
In IP Extended mode, the NAC appears as a distinct NAC panel  connection. For example:



The NAC also appears as a DGP  category (DGP number 16) of the NAC panel connection. The NAC's assigned RASs and DGPs appear as sub-devices under the NAC's DGP node.

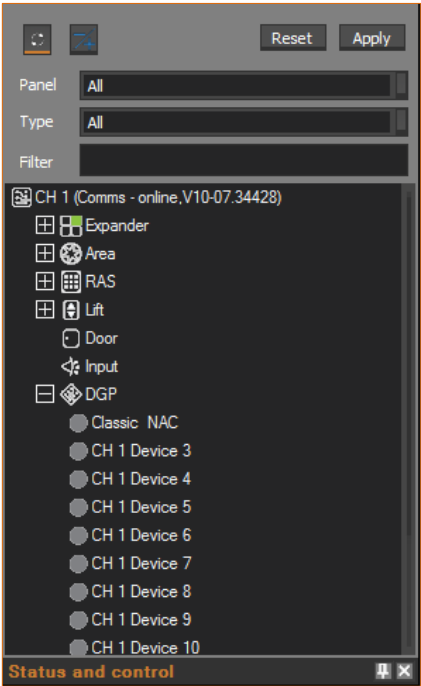
The NAC's doors appear as doors under the Door  category of the NAC panel connection.

The NAC also appears under the DGP  category under the Challenger*Plus* panel  that it is connected to. For example:



Classic mode

In Classic mode, the NAC appears under the DGP  category under the Challenger*Plus* panel  that it is connected to. For example:



The NAC’s assigned RASs and DGPs appear as sub-devices under the NAC.
The NAC’s doors appear as doors under the Door  category of the Challenger*Plus* panel.
Mapped inputs and relays appear under the Input  and Relay  categories.

Status

Coloured icons indicate the status of NAC doors (see Table 6 below and attached RASs and DGPs (see Table 7 below).

Table 6: Door status

Door status	Icon	Colour
Locked		Grey
Disabled		Orange
Unsecured/Open/Unlocked		Green
DOTL		Red
Forced/Fault		Flashing grey/red

Table 7: DGP/RAS status

DGP/RAS status	Icon	Colour
Online		Grey
Isolated		Yellow
Offline		Red

DGP/RAS status	Icon	Colour
Tamper/fuse fail	 	Flashing grey/red

Commands

The Status and Control window allows the operator to execute remote commands on the NAC and its devices via context menus.

If you right-click on the NAC, the following options appear in the context menu:

- **Isolate** – isolates the NAC.
- **De-isolate** – de-isolates the NAC.
- **Battery test** – starts a timed battery test.
- **Cancel test** – cancels an undergoing battery test.
- **Update status** – updates the icon and description of the NAC to its current status.
- **Update all device status** – updates the icons and descriptions of the NAC and all of its attached DGPs and RASs to their current status.

Note: This option only appears for a NAC panel connection (in IP Direct and IP Extended modes).

- **Reboot device** – reboots the NAC. CTPlus prompts you for your operator password
- **Diagnostics** – opens a window showing detailed diagnostics for the NAC, including its power supply voltage and current, battery status, and state of inputs.
- **Upgrade firmware** – allows the operator to upgrade the firmware on the NAC. See the “Upgrading firmware” section on page 38.

If you right-click on a door, the following options appear in the context menu:

- **Open** – opens the door.
- **Timed open** – opens the door for a set period of time.
- **Unlock** – unlocks the door.
- **Lock** – locks the door.
- **Enable** – enables the door.
- **Disable** – disables the door.
- **Reader status** – opens a window showing the status of all readers assigned to the door.
- **Update status** – updates the icon and description of the door to its current status.
- **Diagnostics** – opens a window showing detailed diagnostics for the door, including the state of inputs, relays, and configuration options.

If you right-click on a DGP (including the NAC's own DGP node), the following options appear in the context menu:

- **Isolate** – isolates the DGP.
- **De-isolate** – de-isolates the DGP.
- **Battery test** – starts a timed battery test.
- **Cancel test** – cancels an undergoing battery test.
- **Update status** – updates the icon and description to the current status of the DGP.
- **Diagnostics** – opens a window showing detailed diagnostics for the NAC, including its power supply voltage and current, battery status, and state of inputs.

Note: This option only appears if the DGP node represents the NAC itself.

- **Upgrade firmware** – allows the operator to upgrade the firmware on the DGP. Refer to the relevant manual.

Note: This option only appears if the DGP node represents a DGP assigned to the NAC and not the NAC itself.

If you right-click on a RAS, the following options appear in the context menu:

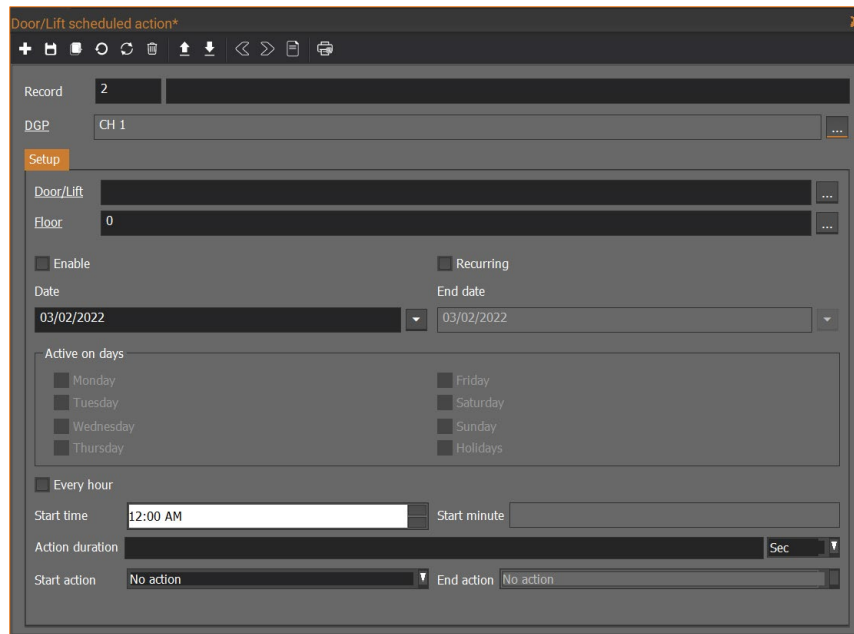
- **Isolate** – isolates the RAS.
- **De-isolate** – de-isolates the RAS.
- **Update status** – updates the icon and description of the RAS to its current status.

Configuring door/lift schedules

Up to 100 **door/lift schedules** can be programmed in the NAC, allowing for very flexible door locking and unlocking schedules.

For more information on door schedules, see the “Overriding door state” section on page 26.

-  To configure a door/lift schedule in CTPlus, click the **Door/Lift scheduled action** button on the *Operation* ribbon tab to open the Door schedule form:



On the Door/Lift schedule form, click the **New**  button in the toolbar to add a new door schedule record.

Enter a description for the door schedule in the **Record** description field.

When finished configuring the door schedule, click the **Save**  button in the toolbar to save the record.

DGP

Click the **Browse**  button to select the NAC.

Setup tab

Door/Lift

Enter the door/lift number on the NAC or click the **Browse**  button to select the door/lift.

Floor

Enter the Floor number on the NAC or click the **Browse**  button to select the floor.

Enabled

Tick the check box to enable the door schedule.

Start date

Enter the start date for the active period.

Use end date

Tick the check box to enable the use of an end date for the active period.

End date

Enter the end date for the active period, if required.

Active on days

Tick the days of the week (and/or holidays) that the door schedule will be active on during the active period.

Every hour

Tick the **Every hour** check box if the **Start action** is to repeat every hour.

Start time

Enter the start time for the start action.

Start minute

This option is only available if Every hour is selected. Enter a minute value to specify at what time in each hour the action should be performed..

Action duration

The action duration is the period of time that the **Start action** should remain in effect. When the action duration expires, the **End action** will be triggered.

Enter a number and specify *Sec* for seconds, *Min* for minutes, *Hour* for hours, or *Day* for days.

Start action

Select the start action from the following options:

- *No action* – take no action
- *Unlock* – unlock the door
- *Lock* – lock the door
- *Disable* – disable the door
- *Enable* – enable the door

End action

If Action **duration** is defined, select the end action from the options. The options are the same as for the **Start action** field. See the “Start action” section above.

Appendix A: Reference materials

Using time and attendance readers

There are two types of readers that may be used for time and attendance functionality (clocking on and off):

- There can be up to 32 RASs (readers or keypads) on the NAC's buses designated as time and attendance readers (see the "Time & attendance reader" section on page 80).
- There can be up to 31 DGPs on the NAC's buses that can have Wiegand interfaces (e.g. the TS1061 Dual Wiegand Interface).

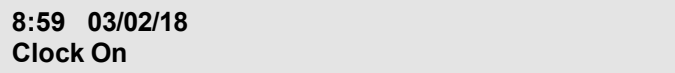
Using RASs for time and attendance

If using card readers on the NAC's buses, the functionality is determined by whether the reader is an IN reader or an OUT reader. IN readers are Clock On readers and OUT readers are Clock Off readers.

Badging a card on a Clock On card reader automatically clocks you on. Badging a card on a Clock Off card reader automatically clocks you off.

Using an LCD RAS

When used as a time and attendance reader, the LCD RAS will display the time and date similar to the following:

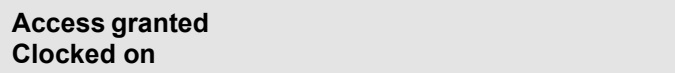


8:59 03/02/18
Clock On

Users can clock on and off using two methods, described as follows.

Method 1: Clock On

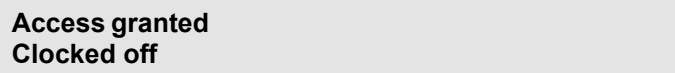
To clock on, key in the user PIN and press On. The current time and date will appear for about a second before this screen appears:



Access granted
Clocked on

Method 1: Clock Off

To clock off, key in the user PIN and press Off. The current time and date will appear for about a second before this screen appears:



Access granted
Clocked off

Method 2 (LCD keypad only): Clock On

To clock on, first press * to toggle the state so that Clock On is displayed, then key in the user PIN and press Enter.



8:59 03/02/18
Clock On

Method 2 (LCD keypad only): Clock Off

To clock off, first press * to toggle the state so that Clock Off is displayed, then key in the user PIN and press Enter.

8:59 03/02/18
Clock Off

Using Wiegand readers for time and attendance

Wiegand readers attached to DGPs on the NAC's buses, the functionality is determined by whether the reader is an IN reader or an OUT reader. IN readers are Clock On readers and OUT readers are Clock Off readers.

Badging a card on a Clock On card reader automatically clocks you on. Badging a card on a Clock Off card reader automatically clocks you off.

Macro events

Refer to the following tables:

- Table 8: Door macro event descriptions below
- Table 9: Other macro event descriptions on page 120

Table 8: Door macro event descriptions

Name	Description	Input	Output
Door access denied	Door access has not been allowed	Yes	No
Door access granted	Door access has been allowed	Yes	No
Door access granted 1st badge	Door access has been granted when badged once	Yes	No
Door access granted 2nd badge	Door access has been granted when badged twice	Yes	No
Door access granted 3rd badge	Door access has been granted when badged three times	Yes	No
Door access granted in button	Door access has been granted and IN button pressed	Yes	No
Door access granted out button	Door access has been granted and OUT button pressed	Yes	No
Door access granted traced	Door access has been granted to a user with trace On	Yes	No
** Door anti-passback	Anti-passback is active	Yes	No
Door area secure	Area assigned to door is secure	Yes	Yes
*** Door buzzer	Buzzer output is active	Yes	Yes
Door disabled	Door is disabled completely (from keypad or computer)	Yes	Yes
** Door dual custody inside	Dual Custody access is required at the "IN" reader	Yes	Yes

Name	Description	Input	Output
** Door dual custody outside	Dual Custody access is required at the "OUT" reader	Yes	Yes
Door enabled	Door is enabled	No	Yes
Door fire override	Secondary override is active	Yes	Yes
Door forced	Door Contact is unsealed with no valid door command	Yes	No
Door interlock	Interlock input(s) are unsealed	Yes	Yes
* Door interlock override	If the interlock has been overridden	Yes	Yes
*** Door keypad duress	Duress PIN code entered at door keypad	Yes	No
*** Door LED1	LED 1 output is active	Yes	Yes
*** Door LED2	LED 2 output is active	Yes	Yes
Door lock	Lock output is de-activated to lock the door	No	Yes
** Door low security inside	Card and PIN required to access at the "IN" reader	Yes	Yes
** Door low security outside	Card and PIN required to access at the "OUT" reader	Yes	Yes
Door open	Door Open command is active (to unlock / start shunt)	Yes	Yes
Door open too long	Door Contact is unsealed after shunt timer has expired	Yes	No
Door override	The override time zone assigned to the door is valid	Yes	Yes
* Door override inhibit	The override time zone is inhibited	Yes	Yes
Door random bit	An event is generated at random when the door is accessed	Yes	No
# Door reader disabled	Reader is disabled	Yes	Yes
Door reader enabled	Reader is enabled	No	Yes
Door secure	When the door is LOCKED and the door is CLOSED.	Yes	No
Door shunt warning	Shunt warning timer is running	Yes	No
Door shunting	Shunt timer is running	Yes	Yes
Door unlock	Lock output is active to unlock the door	Yes	Yes
*** DOOR READER FAULT	Fault detected on reader (Comms / tamper / etc)	Yes	No
*** DOOR LOCK FAULT	Cable tamper / fault detected on lock relay wiring	Yes	No

* Denotes rule can only be activated as a result of another door macro.

** Denotes rule can only be activated as a result of another door macro and the function of the door (the macro input is always true if the function is set in the programming)

*** Denotes the event is currently not enabled.

User with the 'Privilege' attribute set can override the 'Reader disabled' function.

Table 9: Other macro event descriptions

Name	Description	Input	Output	Operating Modes
** Area access	Area in access (99 events, 1 per area)	Yes	No	Classic & IP Extended Mode
** Area alarm	Input(s) in alarm in area (99 events, 1 per area)	Yes	No	Classic & IP Extended Mode
Controller DGP offline	DGP on Intelligent Controller sub-LAN is offline.	Yes	No	ALL Modes
* Controller battery test active	The battery test on this Controller is running (1 event)	Yes	No	ALL Modes
* Controller battery test fail	The battery test failed on this Controller (1 event)	Yes	No	ALL Modes
* Controller battery low	Low battery condition exists on the Controller (1 event)	Yes	No	ALL Modes
* Controller fuse fail	Fuse Fail condition exists on the Controller (1 event)	Yes	No	ALL Modes
* Controller mains fail	Mains fail condition exists on the Controller (1 event)	Yes	No	ALL Modes
* Controller offline	Controller is not communicating with the Challenger (1 event)	Yes	No	ALL Modes
* Controller siren active	The siren output (16th relay) is active (1 event)	Yes	No	ALL Modes
* Controller siren fail	Siren fail (siren tamper) condition exists on this Controller (1 event)	Yes	No	ALL Modes
* Controller tamper	Cabinet tamper condition exists on this Controller (1 event)	Yes	No	ALL Modes
** DGP relay	System relay assigned to this DGP is active (16 events, 1 per relay). The first 16 relays on DGP can also be activated by physical relay function.	Yes	Yes	ALL Modes
Input	Input on this DGP is unsealed (16 events, 1 per input)	Yes	Yes	ALL Modes
Physical relay	Relay connected to this DGP is active (255 events, 1 per relay). If the physical relay is numbered higher than the first 16 in the DGP, then it can only be activated by door macro.	Yes	Yes	ALL Modes
RAS Offline	RAS on Intelligent Controller sub-LAN is offline (16 events, 1 per RAS address)	Yes	No	ALL Modes
* Region limit	When the number of people in any region reaches the present limit (255 events, 1 per region)	Yes	No	N/A

* Denotes the event is currently not enabled.

** Not available in IP Direct mode

Table 9: Door macro event flag programming

Name	Input- I Output -O Both – I/O	D1	D2	D3	D4	D5	D6	D7	D8
DOOR OPEN	I/O	1	2	3	4	5	6	7	8
DOOR UNLOCKED	I/O	9	10	11	12	13	14	15	16
DOOR LOCK	O	17	18	19	20	21	22	23	24
DOOR OVERRIDE	I/O	25	26	27	28	29	30	31	32
DOOR OVERRIDE INHIBIT	I/O	33	34	35	36	37	38	39	40
DOOR DISABLED	I/O	41	42	43	44	45	46	47	48
DOOR ENABLED	O	49	50	51	52	53	54	55	56
# DOOR READER DISABLED	I/O	57	58	59	60	61	62	63	64
DOOR READER ENABLED	O	65	66	67	68	69	70	71	72
DOOR DUAL CUSTODY INSIDE	I/O	73	74	75	76	77	78	79	80
DOOR DUAL CUSTODY OUTSIDE	I/O	81	82	83	84	85	86	87	88
DOOR LOW SECURITY INSIDE	I/O	89	90	91	92	93	94	95	96
DOOR LOW SECURITY OUTSIDE	I/O	97	98	99	100	101	102	103	104
DOOR ANTI PASSBACK	I/O	105	106	107	108	109	110	111	112
DOOR SHUNTING	I/O	113	114	115	116	117	118	119	120
DOOR SHUNT WARNING	I	121	122	123	124	125	126	127	128
DOOR AREA SECURE	I/O	129	130	131	132	133	134	135	136
DOOR INTERLOCK	I/O	137	138	139	140	141	142	143	144
DOOR INTERLOCK OVERRIDE	I/O	145	146	147	148	149	150	151	152
* DOOR KEYPAD DURESS	I	153	154	155	156	157	158	159	160
* DOOR READER FAULT	I	161	162	163	164	165	166	167	168
DOOR LOCK FAULT	I	169	170	171	172	173	174	175	176
DOOR DOTL	I	177	178	179	180	181	182	183	184
DOOR FORCED	I	185	186	187	188	189	190	191	192
* DOOR LED 1	I/O	193	194	195	196	197	198	199	200
* DOOR LED 2	I/O	201	202	203	204	205	206	207	208
* DOOR BUZZER	I/O	209	210	211	212	213	214	215	216
* DOOR RANDOM BIT	I	217	218	219	220	221	222	223	224
DOOR ACCESS DENIED	I	225	226	227	228	229	230	231	232
DOOR ACCESS GRANTED	I	233	234	235	236	237	238	239	240
DOOR ACCESS GRANTED TRACED	I	241	242	243	244	245	246	247	248

Name	Input- I Output -O Both – I/O	D1	D2	D3	D4	D5	D6	D7	D8
DOOR ACCESS GRANTED 1ST BADGED	I	249	250	251	252	253	254	255	256
DOOR ACCESS GRANTED 2ND BADGED	I	257	258	259	260	261	262	263	264
DOOR ACCESS GRANTED 3RD BADGED	I	265	266	267	268	269	270	271	272
DOOR FIRE OVERRIDE	I/O	289	290	291	292	293	294	295	296
DOOR SECURE	I	297	298	299	300	301	302	303	304

Table 10 Macro Event Range

AREA NUMBER										
EVENTs	1	2	3	~	~	~	~	97	98	99
<i>These events can only be used as input conditions to a door macro not as an output activation of an door macro</i>										
*Area Accessed	4091	4092	4093	~	~	~	~	4187	4188	4189
*Area Alarm	4190	4191	4192	~	~	~	~	4186	4287	4288
DGP Relays	577	578	579	~	~	~	~	590	591	592

*These events are not currently enabled.

Table 11 Macro Event Range for BUS1 and BUS2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
RAS Off-line	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640
BUS1	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656
BUS2 DGP Off-line	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	
BUS1																
BUS2	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688

NAC Door Defaults

Table 12 Access, Shunt/Egress/Passback and Lift Defaults

	FUNCTION	DEFAULTS
Access TAB	Door Type	Door
	Access Time	5 sec
	Dual custody time	8 sec
	Pre lock time	2 sec
	Random event %	0
	Override TZ	
	Multi badge time	5 sec
	Long access time	15 sec
	Card to PIN time	8 sec
	Post lock time	2 sec
	Random % lockout time	
	Low security TZ	
Shunt/Egress/Passback TAB	Report DOTL	Enabled
	Report forced door	Enabled
	Shunt options	
	Shunt type	Input shunting& DOTL
	Ext.shunt time	90 sec
	Shunt time	1 min
	Warning time	15 sec
	Anti-passback options	
	Anti-passback	Disabled
	Egress options	
Lift TAB	Egress	Egress timed
	Egress time zone	0-(24 Hours)
	Egress reporting	Enabled
	Door type	Lift car
	Access time	5 sec
	Long access time	15 sec
	Lift override group	
	Lift security group	
	Security key	None

Table 13 Hardware Options: Default Input/Relay number assignments

	Door Number	Location	Device Number
Lock relay 1	1 st Door	Onboard	1
	2 nd Door	Onboard	2
	3 rd Door	Onboard	3
	4 th Door	Onboard	4
	5 th Door	NONE	NONE
	6 th Door	NONE	NONE
	7 th Door	NONE	NONE
	8 th Door	NONE	NONE
Door input 1	1 st Door	Onboard	1
	2 nd Door	Onboard	4
	3 rd Door	Onboard	7
	4 th Door	Onboard	10
	5 th Door	NONE	NONE
	6 th Door	NONE	NONE
	7 th Door	NONE	NONE
	8 th Door	NONE	NONE
Egress	1 st Door	Onboard	3

input	2 nd Door	Onboard	6
	3 rd Door	Onboard	9
	4 th Door	Onboard	12
	5 th Door	NONE	NONE
	6 th Door	NONE	NONE
	7 th Door	NONE	NONE
	8 th Door	NONE	NONE

Table 14: CTPlus programming sequence

Step	Classic	IP Direct	IP Extended
DIP switches	✓		✓
Default the NAC	✓	✓	✓
Connect to Challenger <i>Plus</i>	✓		✓
Connect to CTPlus		✓	✓
Set up IP communications		✓	✓
Upload defaults	✓	✓	✓
Upgrade firmware	✓	✓	✓
Program NAC:			
• NAC options	✓	✓	✓
• Assign RASs	✓	✓	✓
• Assign DGPs	✓	✓	✓
Program holidays*		✓	✓
Program time zones*		✓	✓
Program regions	✓	✓	✓
Program doors:			
• Hardware	✓	✓	✓
• Readers	✓	✓	✓
• Access	✓	✓	✓
• Shunt/egress/passback	✓	✓	✓
• Alarm control	✓		✓
Program input and relay mapping:			
• Program input mapping	✓		✓
• Program relay mapping	✓		✓
• Program mapped inputs	✓		✓
• Program mapped relays	✓		✓
Program macro logic	✓	✓	✓
Program user information			
• Program door/floor groups*		✓	✓
• Program users*		✓	✓

* If TecomC4 will be used for management, then do not use CTPlus for this step.

APPENDIX B: Enclosure Access Restrictions

According to the requirements of AS/NZS 60950-1, the interior of the enclosure presents hazards to general users and thus physical access restrictions **MUST** be instituted ensure safety. To comply with the restrictions:

- Access to the interior of the Enclosure should be limited to suitably trained and qualified installation and maintenance technicians.
- Access to the interior of the enclosure should require the use of a tool.

These restrictions can be met by suitably securing the enclosure door. To comply with the restrictions:

Fit a lock to the enclosure. Ensure it is always locked when not under the immediate control of suitably qualified technicians.

- Seal the enclosure door using standard head (non-knurled) screws, firmly tightened.
- When using finger operable screws (knurled head, etc) to seal the enclosure door, tighten to 2Nm (typically >1/4 turn beyond the finger tight point).