Configuring Command Centre for EN 50131

User Guide

Version: 10.00
Date: May 2026

Copyright © Gallagher Group Limited

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2026. All rights reserved.

Contents

1 Hardware 4
1.1 Compliant Gallagher Products 4
1.2 Compliant Power Supply 5
1.3 Compliant Configuration 5

2 Server Properties 6
2.1 Standards Tab 6
2.2 User Codes 7
2.3 Alarm Flooding 7
2.4 Default Action Plans 8

3 Levels of Access 9
3.1 Divisions 9
3.2 Level 2 Users 10
3.3 Level 3 Users 12

4 Alarm Zone Configuration 14

5 Terminal Settings 15

6 Action Plans 17
6.1 Confirmed Alarms 19

7 Detectors 21

8 Configuring Compliance with Specific Clauses - EN 50131 23
8.1 8.1.4 23
8.2 8.3.5 23
8.3 8.3.6 23
8.4 8.3.7 24
8.5 8.3.8 25
8.6 8.3.9 25
8.7 8.3.12 25
8.8 8.4 26
8.9 8.6.2 26
8.10 8.6.3 28
8.11 8.8.4 29
8.12 8.8.6 30
8.13 EN 50131-3 Optional Features Supported 30

9 Configuration of Specific Clauses - BS 8243 31
9.1 6.3 31
9.2 6.4 31

Appendix 1: Mandatory Events 40

Copyright © Gallagher Group Limited

1 Hardware

1.1 Compliant Gallagher Products

Orange = compliant to Grade 3
Green = compliant to Grades 3 and 4

All controller 6000 variants

Datasheet:
https://media.gallagher.com/m/35c93b8376a7d155/original/Controller-6000-datasheet.pdf

C305101 Controller 6000 HS PIV

C300100 Controller 6000

C300101 Controller 6000 HS

C300111 Controller 6000 2 Door Variant

Controller 7000 variants

Datasheet: https://media.gallagher.com/m/329b1702077f217a/original/Controller-7000-Product-Range-Datasheet.pdf

C400100 Controller 7000 Standard

C400111 Controller 7000 2 Door Standard

C400110 Controller 7000 Starter Kit Standard

Controller Modules

Datasheet:
https://media.gallagher.com/m/3329562e5b4946f4/original/HBUS_Modules_Datasheet.pdf

C300142 4H Module

C300182 8H Module

ELM

Datasheet:
https://media.gallagher.com/m/5eac883d03e9ab7/original/HSEC_End_of_Line_Module_Datasheet.pdf

C300636 HBUS End of Line Module

IO

Datasheet:
https://media.gallagher.com/m/6d3b1e30d4051cce/original/HBUS_IO_Devices_Datasheet.pdf

C300660 HBUS 8 In 2 Out Door Module

C300665 HBUS 4 In 2 Out Door Module - Wiegand

C300680 HBUS 8 In Board

C300684 HBUS 8 In 4 Out Board

C300688 HBUS 16 In 16 Out Board

T20s

Datasheet:
https://media.gallagher.com/m/57cf7b1450f74927/original/T-Series-Readers-Datasheet.pdf

C300450 T20 Mifare Terminal Black

C300451 T20 Mifare Terminal White

C300460 T20 Multi Tech Terminal Black

C300461 T20 Multi Tech Terminal White

C300463 T20 Alarms Terminal, Black

C300464 T20 Alarms Terminal, White

Copyright © Gallagher Group Limited

Hardware compliance certificates can be found here (via Security Support site):
Product Compliances - Resources | Security Hub

1.2 Compliant Power Supply

Power supply must comply with the relevant requirements of BS EN 50131-1, BS EN 50131-6 and PD6662; noting that the *Alternative Power Supply* capacity may be reduced under certain conditions.

1.3 Compliant Configuration

The rest of this document outlines how various Command Centre settings should be set in an installation compliant with BS EN 50131-1:2006+A2:2017, BS EN 50131-3:2009 and BS 8243:2010+A1:2014. In many cases there will be other ways to configure that may be compliant. Also described is compliance with the Swedish standard SSF1014 which requires some deviations from EN 50131-1.

Compliance can be achieved up to grade 4. Some settings must be configured differently according to the grade required.

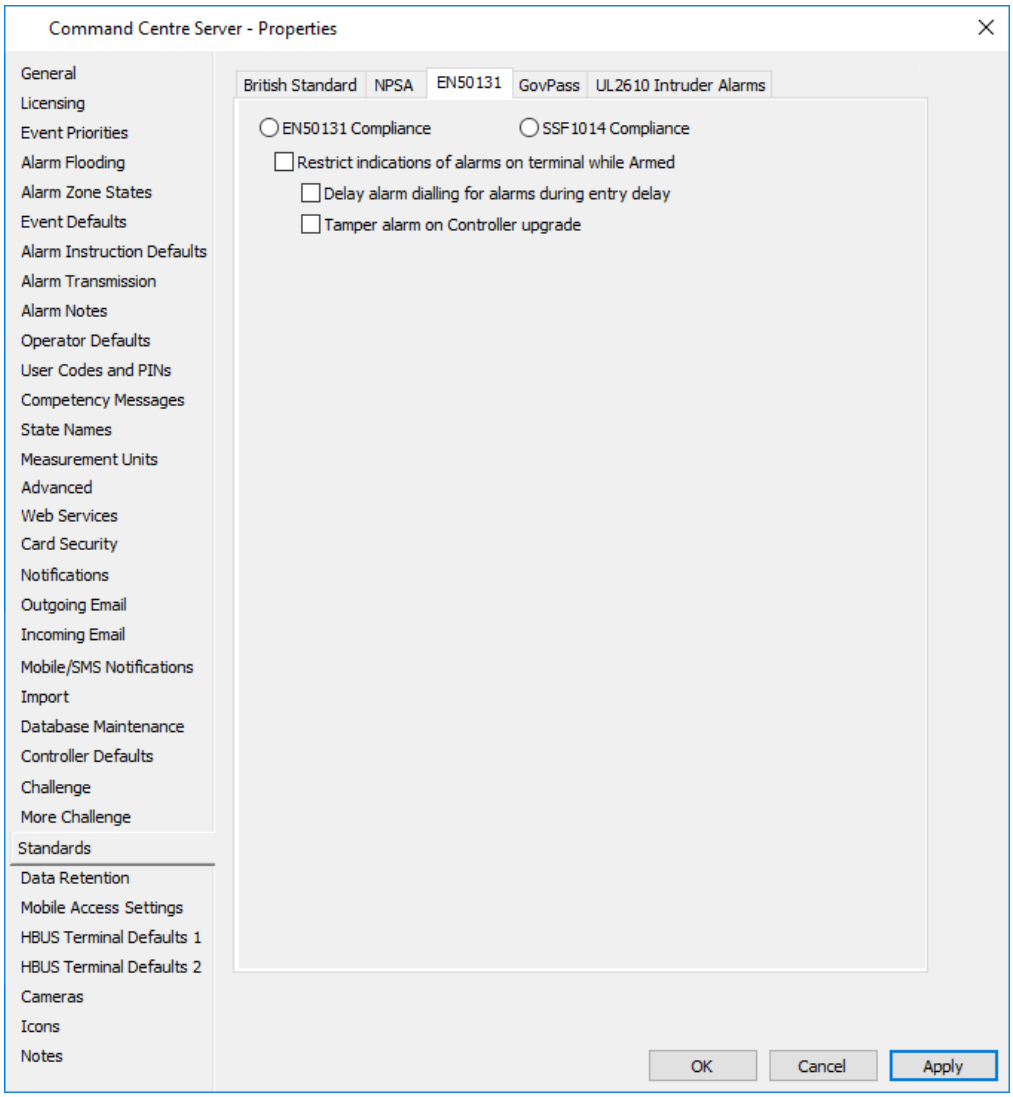
In general, unless otherwise stated, properties are set using the Gallagher Command Centre Configuration Client.

Copyright © Gallagher Group Limited

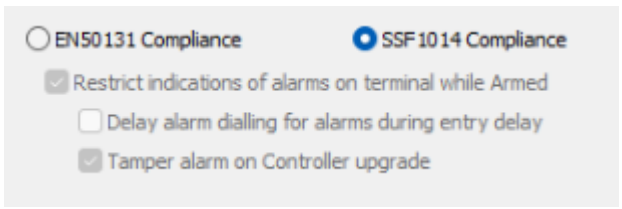
2 Server Properties

2.1 Standards Tab

Check the following settings:



In order to comply with SSF1014, select this option instead, as follows:

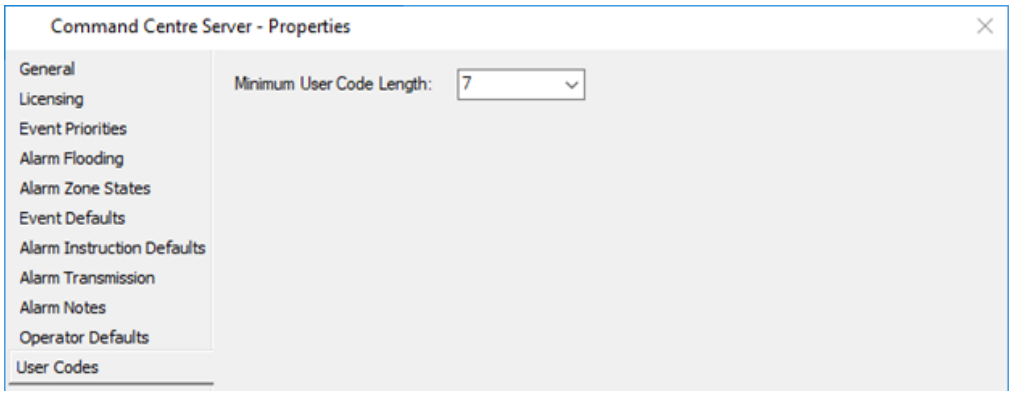


This has the effect of disabling delaying alarm dialling for alarms during entry delay. All other effects selecting this option are the same as for the EN50131 Compliance option.

Copyright © Gallagher Group Limited

2.2 User Codes

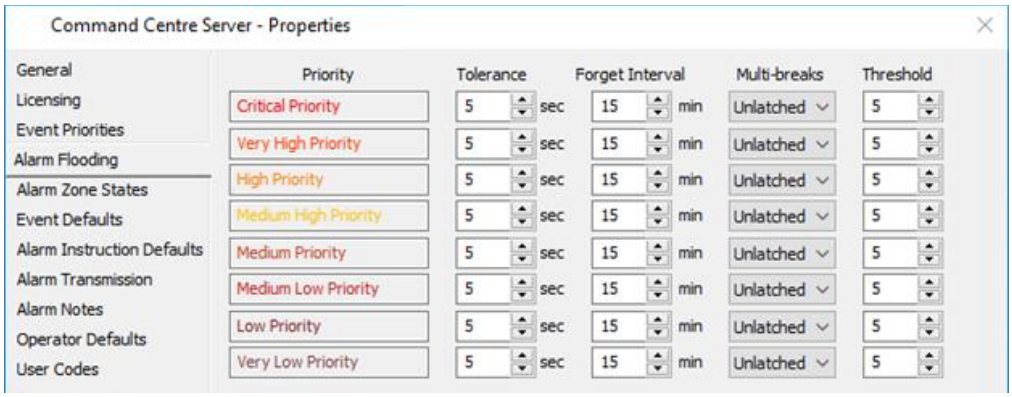
If using user codes for login to the Terminal, (e.g. T20) set the minimum user code length according to the grade. For grade 4, at least 7 digits is required (because some codes are not available). For grade 3, 6 digits and for grade 2, 5 digits. Grade 1 systems may use 4-digit user codes:



The reason that some codes are not available is that any user may indicate a duress situation by entering their code with the last digit incremented by 1 or 0 if the last digit is 9. This means that with 7 digit codes, there are 10,000,000 / 2 = 5,000,000 available codes, more than the 1,000,000 required at grade 4. When cards are used for login, the system allows card numbers from 1 to 16,777,215 for Gallagher cards, with all numbers available. This is more than the requirement for grade 4.

2.3 Alarm Flooding

For all priorities Multi-breaks should be set to Unlatched with a Threshold value between 3 and 10:



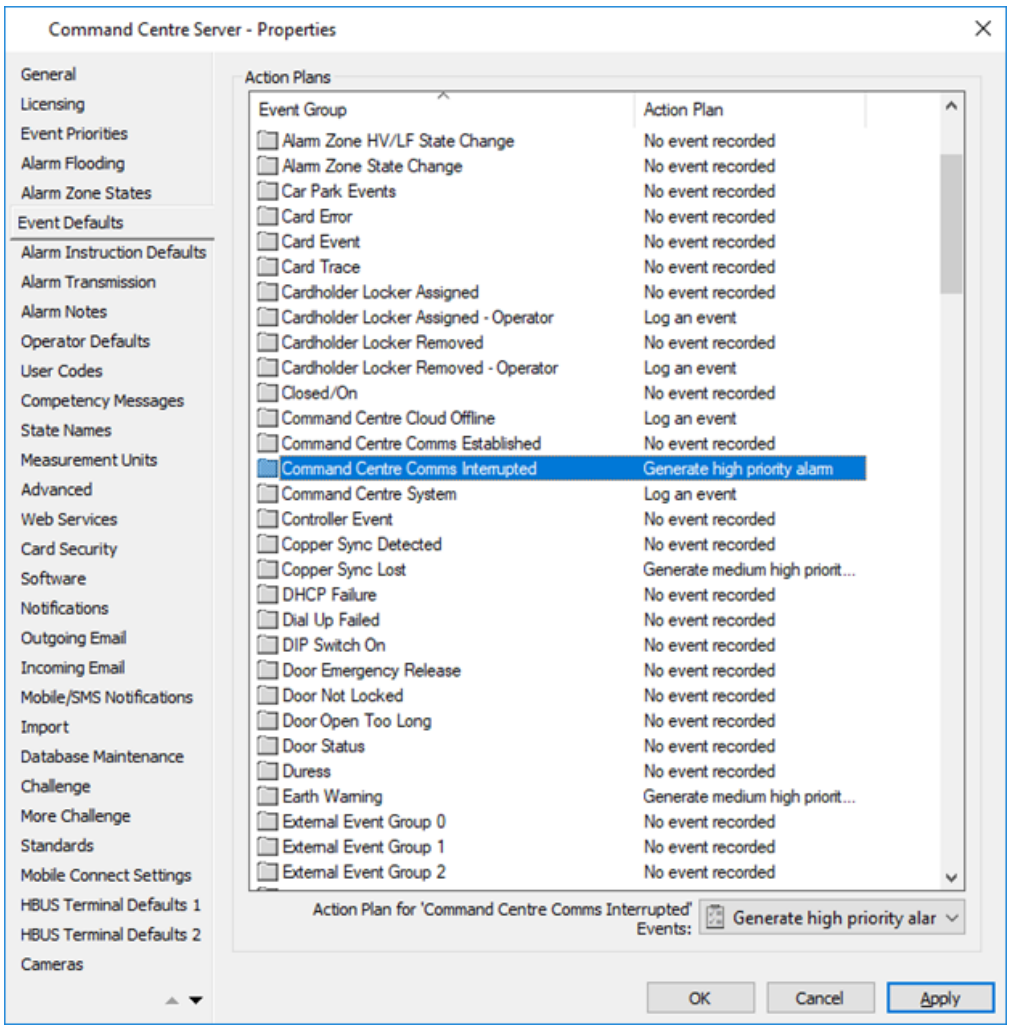
Copyright © Gallagher Group Limited

2.4 Default Action Plans

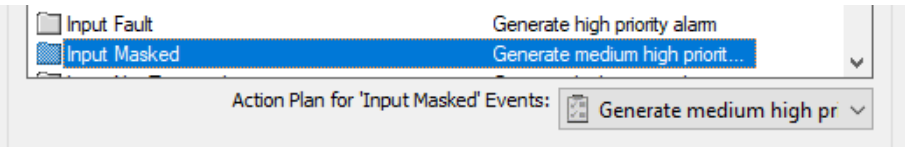
The Controller 6000 supports buffering up to approximately 120,000 events while offline from Command Centre. This will normally be more than enough to ensure that no events marked as mandatory in EN 50131-1, EN 50131-3 and BS 8243 are lost. However, to ensure compliance with this requirement in all eventualities non-mandatory events should be configured to "No event recorded" or the controller should only be used for intruder and hold-up alarms monitoring. The event groups listed in Appendix 1 correspond to the mandatory events that should be logged.

Additionally, the following default event group action plans should be changed.

The Command Centre Comms Interrupted, Primary ethernet link and Secondary ethernet link event groups must be changed to an action plan with High priority in all alarm zone states:



The Input Masked event group must be changed to an action plan with Medium priority (in order to allow level 2 users to override prevention of arm and acknowledge masked alarms), while Input Fault should be High priority:



Copyright © Gallagher Group Limited

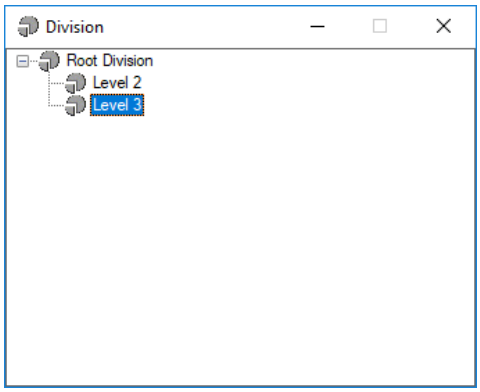
3 Levels of Access

EN 50131 defines 4 levels of access. Levels 2 and 3 correspond to users of Command Centre, with level 2 generally having operational responsibilities and level 3 having supervisor, installer or alarm company responsibility. Level 2 is generally more limited than level 3.

In this section we describe how to configure users with level 2 access versus level 3. In practice each user may have a subset of privileges allowed at each level and there are many other Command Centre privileges not covered by the standard which could be given or withheld from these groups.

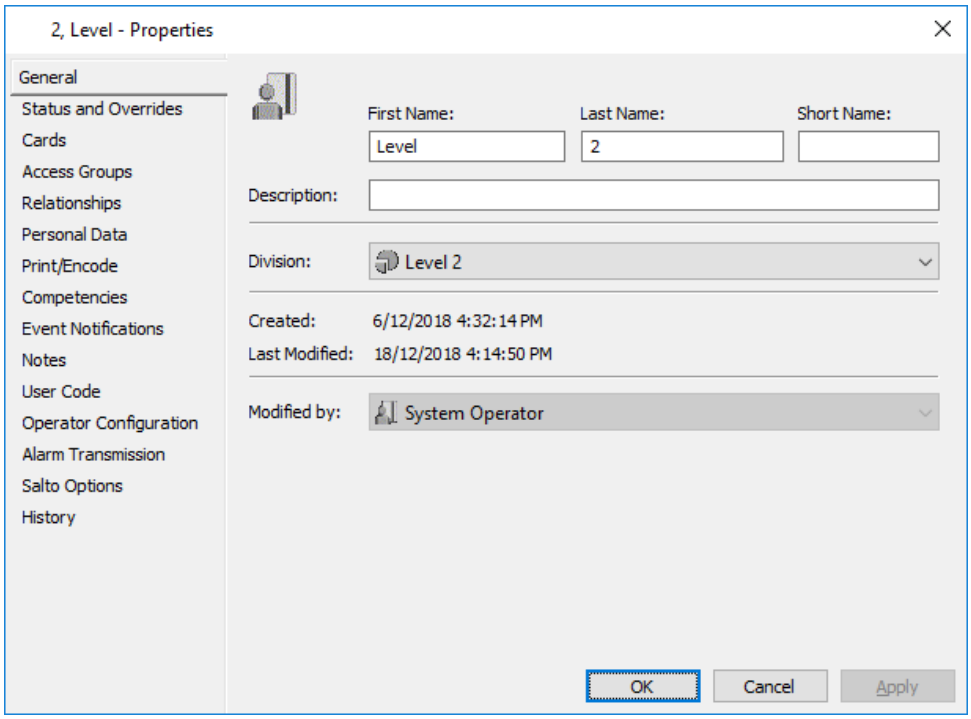
3.1 Divisions

Level 2 and 3 divisions are created below root division. Note: Level 3 division is not strictly necessary, root division could also be used for level 3.



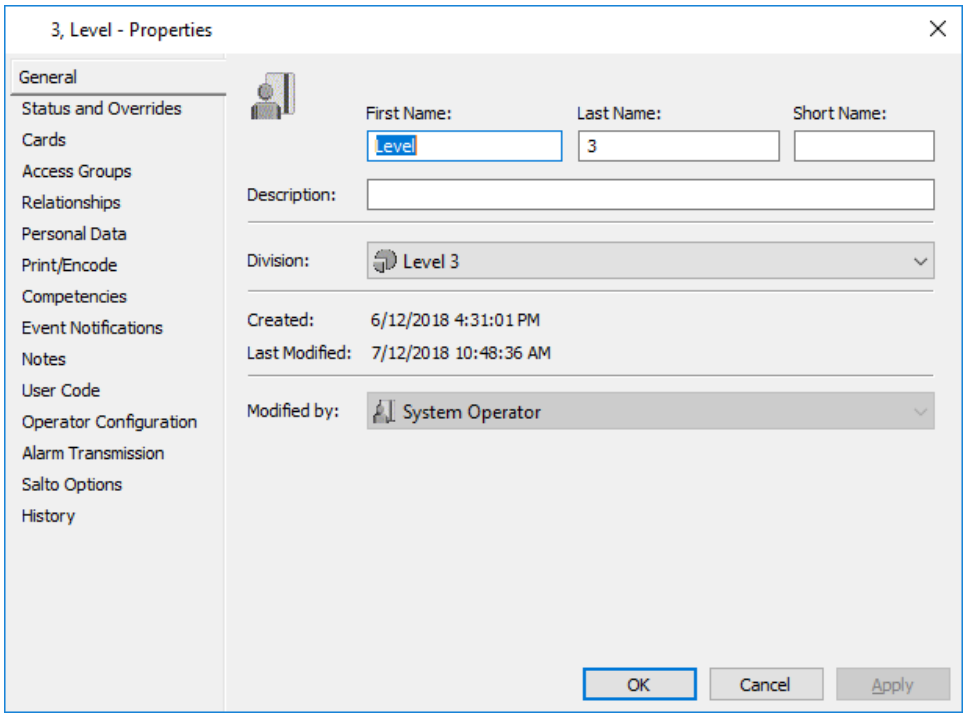
All items other than operator groups and operators can be created within the root division, or a lower division if required.

Level 2 users should have the level 2 division:



Copyright © Gallagher Group Limited

Level 3 users should have the Level 3 division:



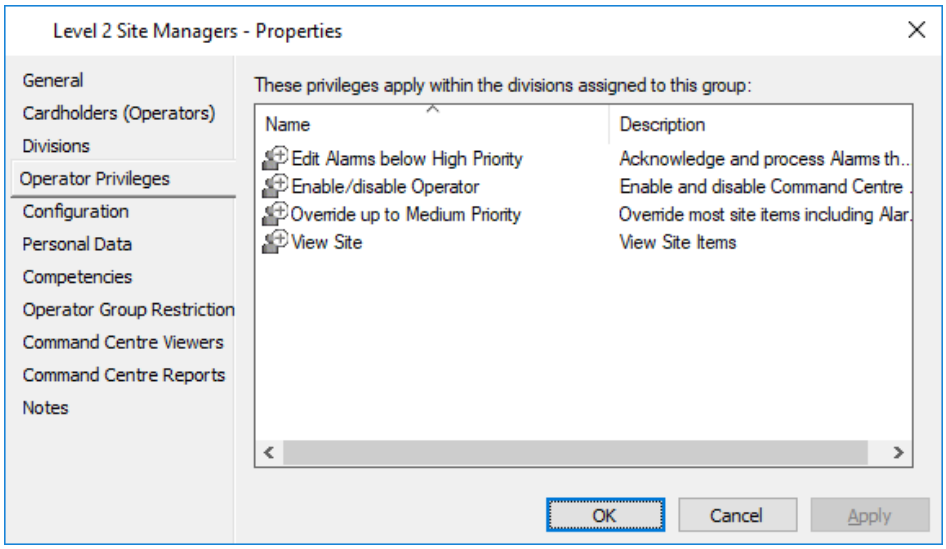
3.2 Level 2 Users

3.2.1 Level 2 Operators

In order to have all the capabilities of Level 2 users described in EN 50131 from Command Centre, two operator groups are required, both belonging to the Level 2 division.

3.2.1.1 Level 2 Site Managers

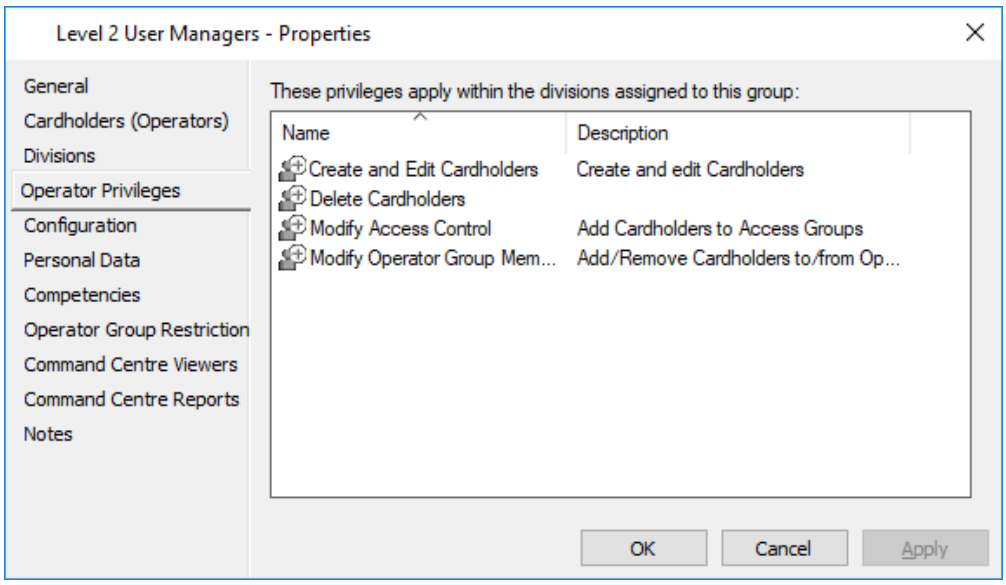
This group provides access to root division (or other lower divisions but should include Level 3) and provides all the site management/operational capabilities allowed for a level 2 user including the ability to enable a level 3 operator to login to Command Centre. This is achieved with the following set of privileges:



Copyright © Gallagher Group Limited

3.2.1.2 Level 2 User Managers

This group provides access to the Level 2 division and allows operators to create and manage other level 2 users (including controller users). This is achieved with the following set of privileges:



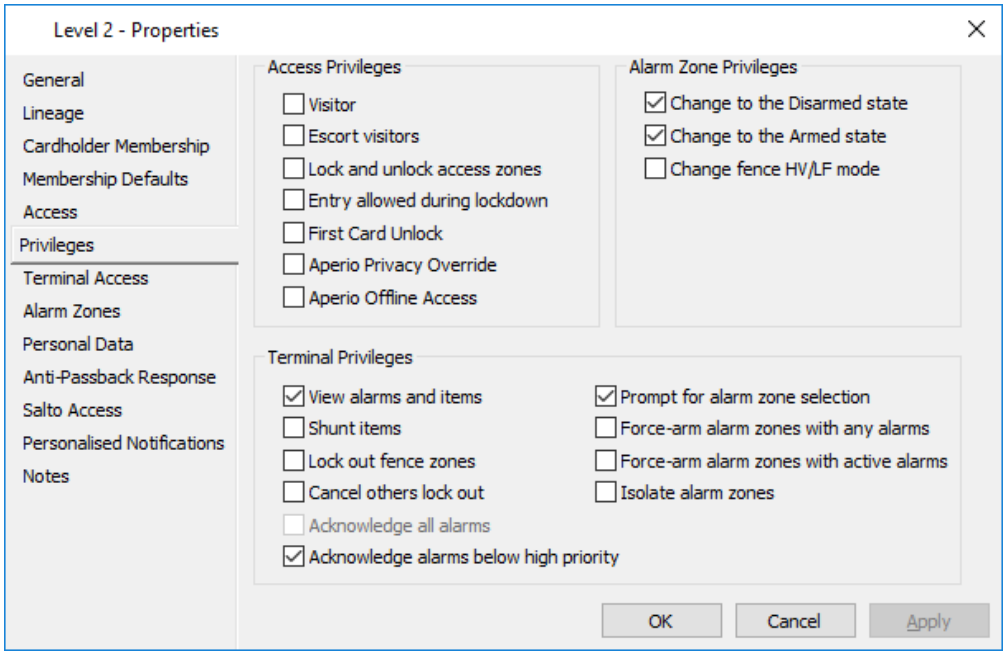
3.2.2 Level 2 Viewer Configuration

In order to be able to manage level 2 operators or enable/disable level 3 operators, at least one of the Level 2 operator groups requires the Cardholder Viewer (and normally the Alarm Viewer and Monitor Site Viewer). These are added in the Command Centre client. The Cardholder Viewer should also be configured to add the Operator Groups tile.

3.2.3 Level 2 Access Groups

For a controller (Terminal) user to have level 2 access, a Level 2 access group is required, belonging to the Level 2 division and with access to the required alarm zones. This group has the following privileges:

Copyright © Gallagher Group Limited



Note: Other privileges except for "Force-arm…", "Isolate alarm zones", and "Shunt items", could be given as they cover functions not covered by the standard.

Force Arm Behaviour for Level 2 Users

Level 2 users are permitted to perform a **Force Arm** action under specific conditions:

- Any alarm (active or inactive) must be **acknowledged**.
- The alarm's **priority must be medium or lower**.

Important: If all alarms are inactive, acknowledging them will **clear** the alarms. In such cases, force arming becomes unnecessary, as the system can be armed normally.

This behaviour ensures users are aware of existing alarm conditions and that high-priority alarms are appropriately restricted.

How to modify the priority of an event on any input or any Command Centre item

To adjust the priority of an event, navigate to the item's **Event Response** configuration. Replace the existing event response with a custom **Action Plan** designed to generate a **Medium Priority Alarm** (or lower), depending on the desired alarm zone state, (i.e. **Armed** or **Disarmed**). This allows for more granular control over alarm handling and ensures the event triggers only the intended level of response.

For more detailed guidance on configuring **Event Responses** and **Action Plans**, refer to the official *Gallagher Configuration Client User Guide*.

3.3 Level 3 Users

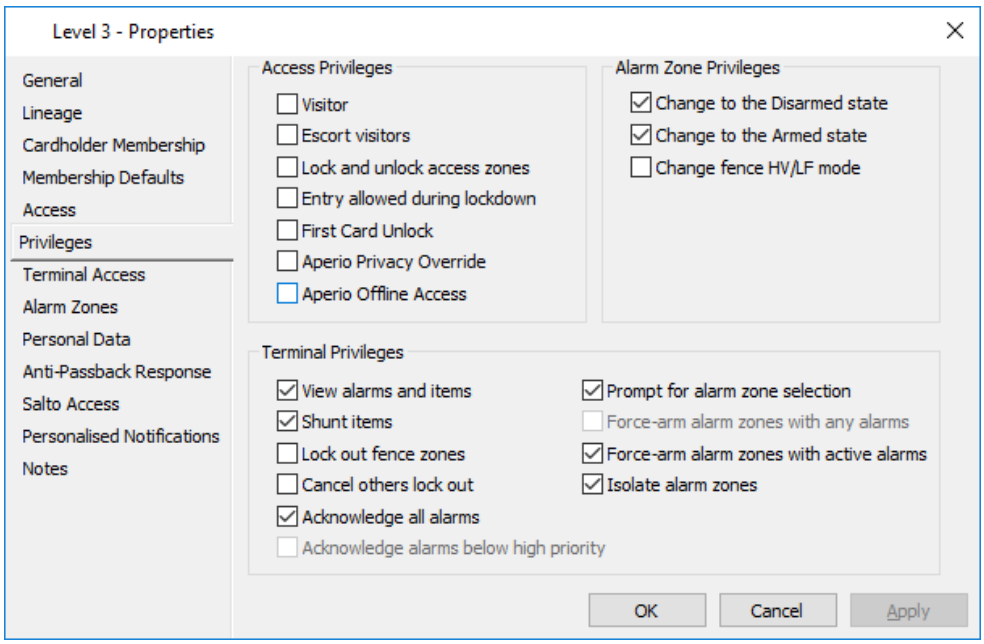
3.3.1 Level 3 Operators Group

This operator group belongs to root division (or some division inaccessible to level 2 operators) and provides access to root division (or lower divisions if a more restricted level 3 operator). This group may have the Advanced User privilege. Alternatively, specific Configure, Edit, Manage, etc privileges could be assigned.

Copyright © Gallagher Group Limited

3.3.2 Level 3 Access Group

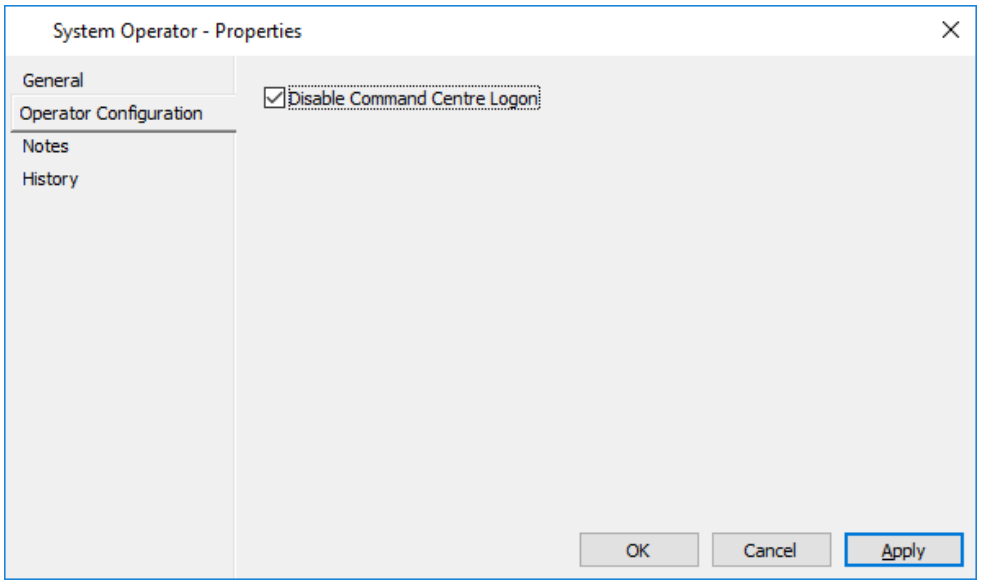
For a controller (Terminal) user to have level 3 access, a Level 3 access group is required, belonging to the Level 3 division and with access to the required alarm zones. This group has the following privileges:



Note: The Force-arm alarm zones with any alarms privilege should not be selected for EN 50131 compliance since it is not permissible to allow arming when this would result in alarms. Any of the other unchecked privileges could be given to this group as they control actions not covered by the standard.

3.3.3 System Operator

The System Operator is implicitly a level 3 user. For this reason, during installation, the system operator's ability to login should be removed by another operator unless this level 3 user is authorised (by a level 2 user):

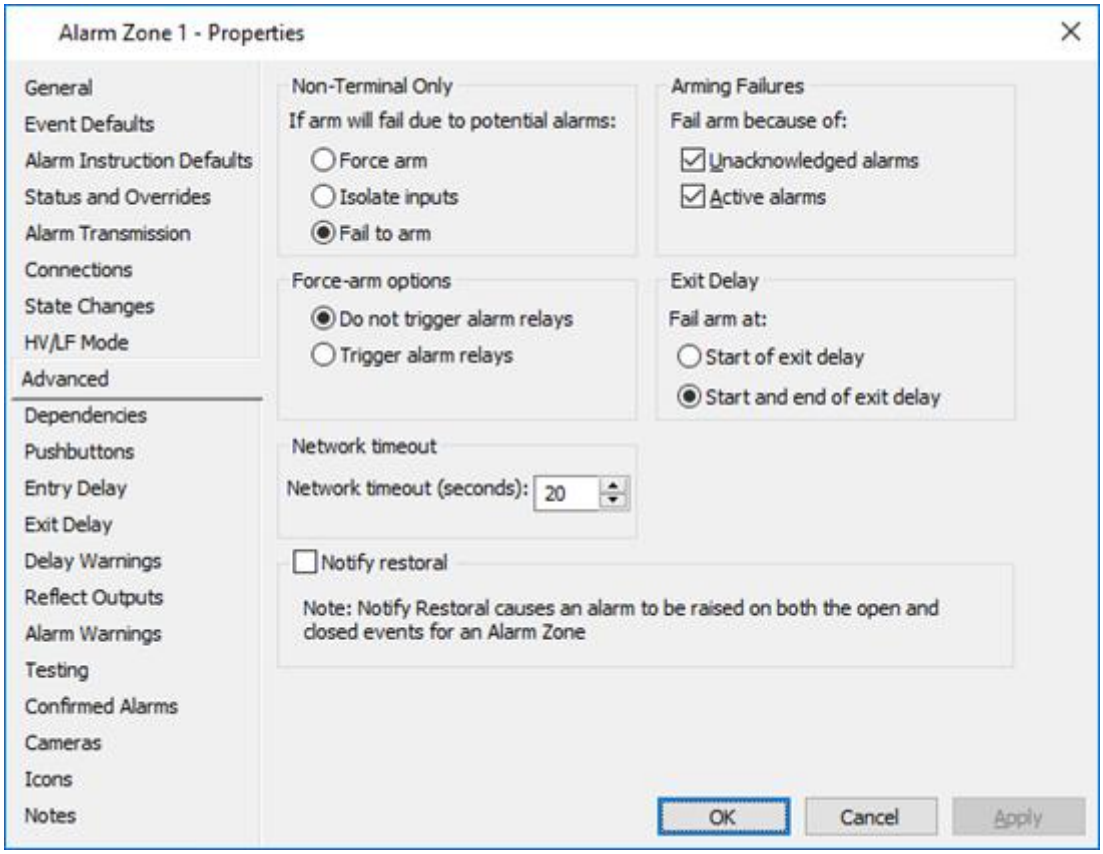


Note: If using a level 3 division, then the System Operator's division may also be changed to level 3.

Copyright © Gallagher Group Limited

4 Alarm Zone Configuration

Alarm Zones should be configured with the "Fail to arm", "Active alarms" and "Fail arm at start and end of exit" options selected on the Advanced tab:

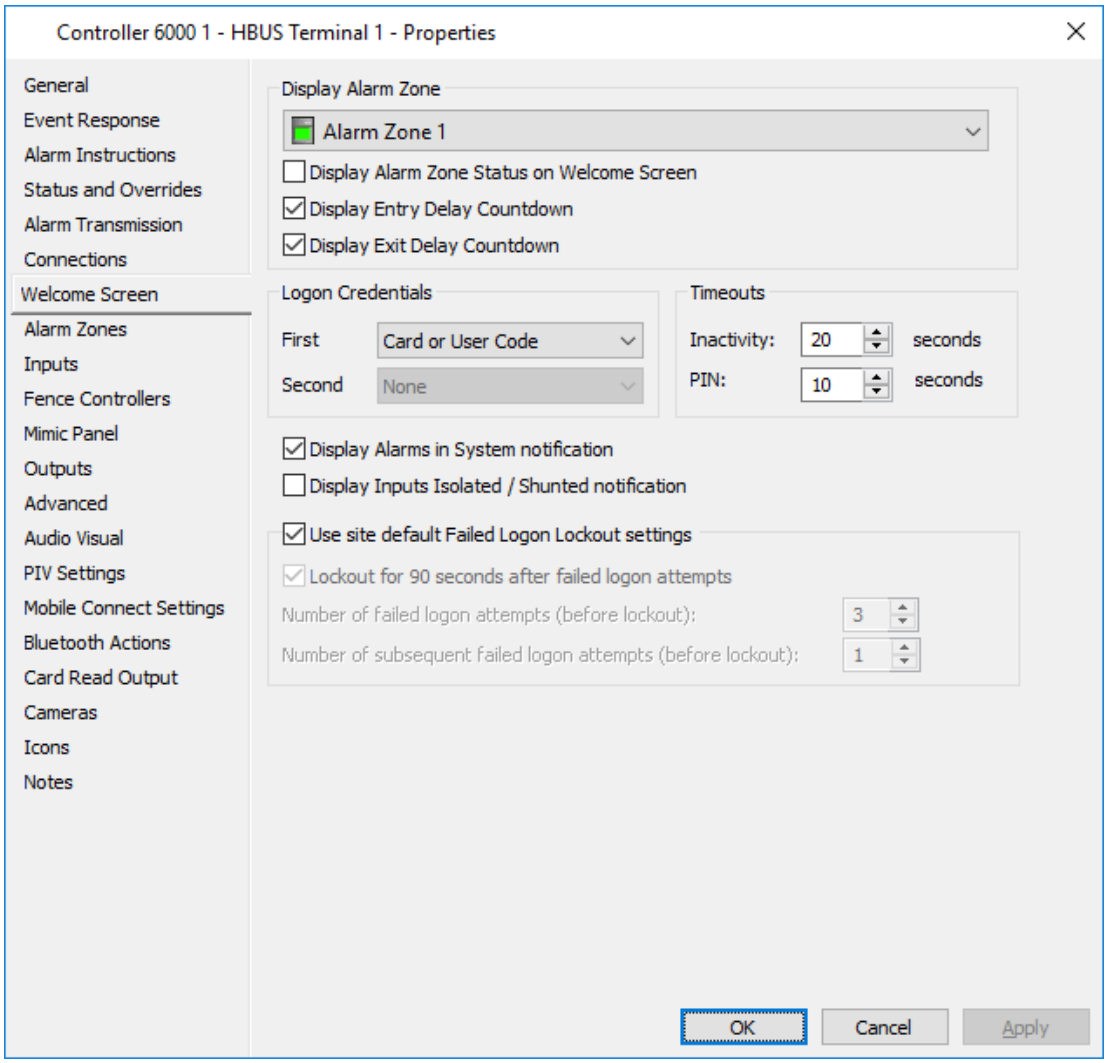


Copyright © Gallagher Group Limited

5 Terminal Settings

The Terminal Welcome screen should be configured with the following selected:

- Display Alarm Zone Status on Welcome Screen unselected (for compliance at Grades 3 & 4)
- Display Entry Delay Countdown
- Display Alarms in System notification

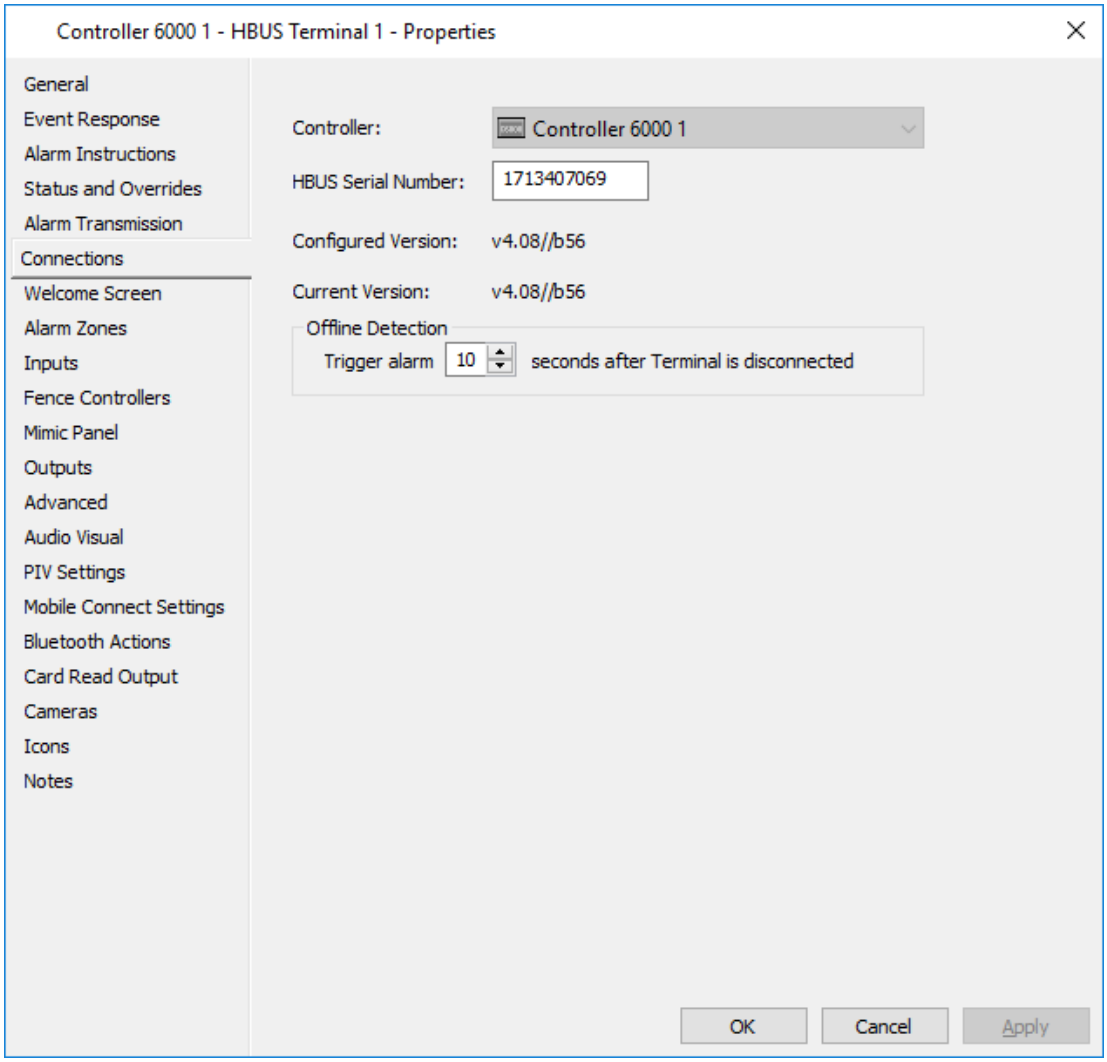


Display Inputs Isolated / Shunted notification should not be selected.

Display Exit Delay Countdown is optional.

For compliance at Grade 4, the offline detection timeout should be set to 10 seconds on the Connections tab:

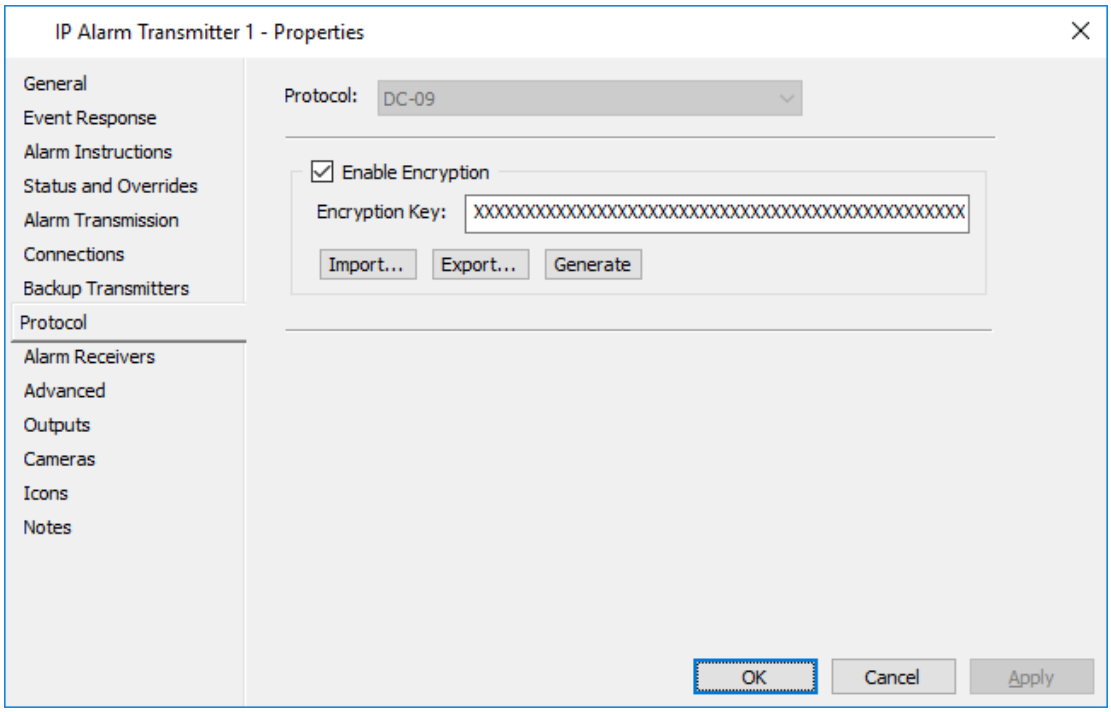
Copyright © Gallagher Group Limited



Copyright © Gallagher Group Limited

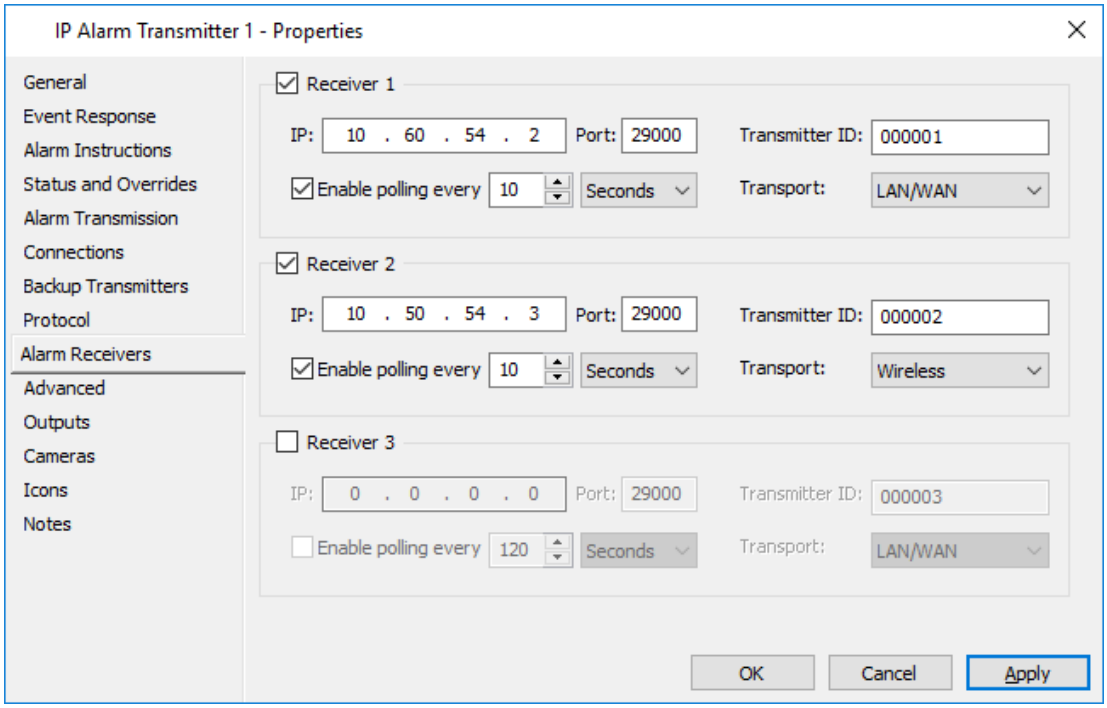
6 Action Plans

For 24-hour type alarms (generally all except Intruder) the default action plans may be used, or other specific action plans created. Action plans for Intruder alarms should have Medium Priority or below in the Armed state and Not an Event in other states. If off-site monitoring is required, then an Alarm Dialler or Alarm Transmitter should be configured on at least one controller and assigned to the action plans' Armed (and for 24-hour alarms Disarmed) tab. For Grade 4 compliance or Grade 3, where no Self-powered audible WD is used, either a third party encrypting SPT or an Alarm Transmitter is required which must be configured to use encryption:

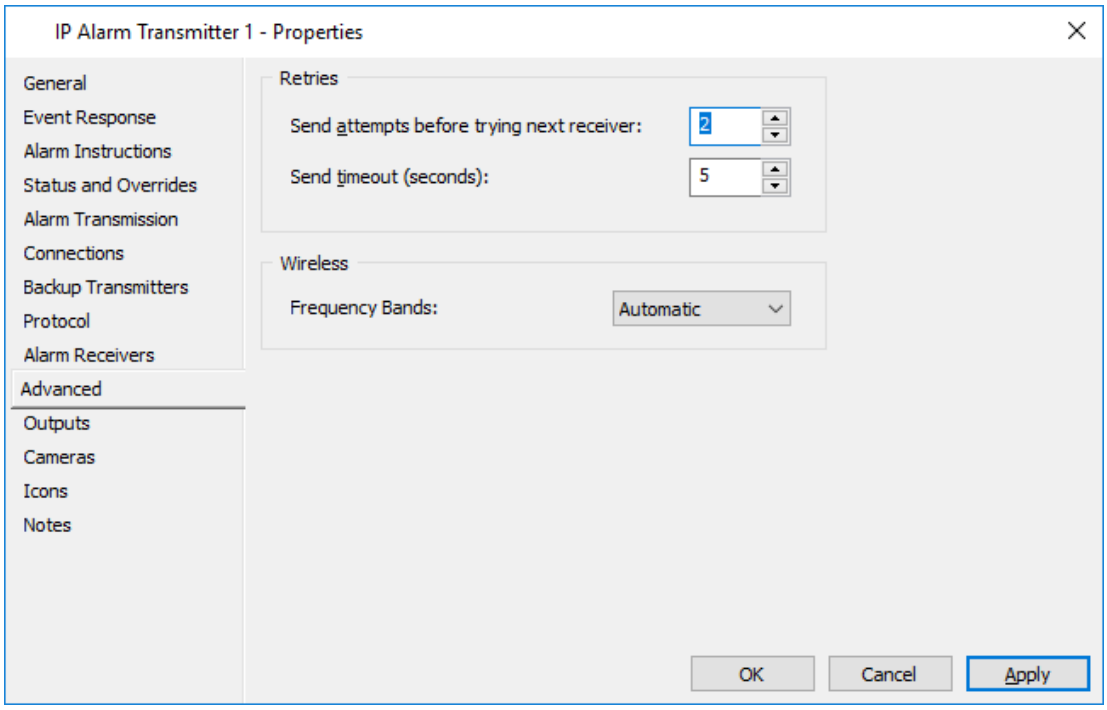


Whenever a Dual Path option has been selected (normally allowed as an alternative to having audible Warning Devices), these should use different technologies (i.e. LAN and Wireless) or have no components in common. Polling should be enabled, and for Grade 4 if options SP5, SP6 or DP4 are chosen, the poll time needs to be reduced for the primary and secondary receivers. For SP5 and DP4, this should be 30s. SP6 is not recommended, but if used, this needs to be 10 seconds.

Copyright © Gallagher Group Limited



The number of send attempts and send timeout should also be reduced to support SP6:

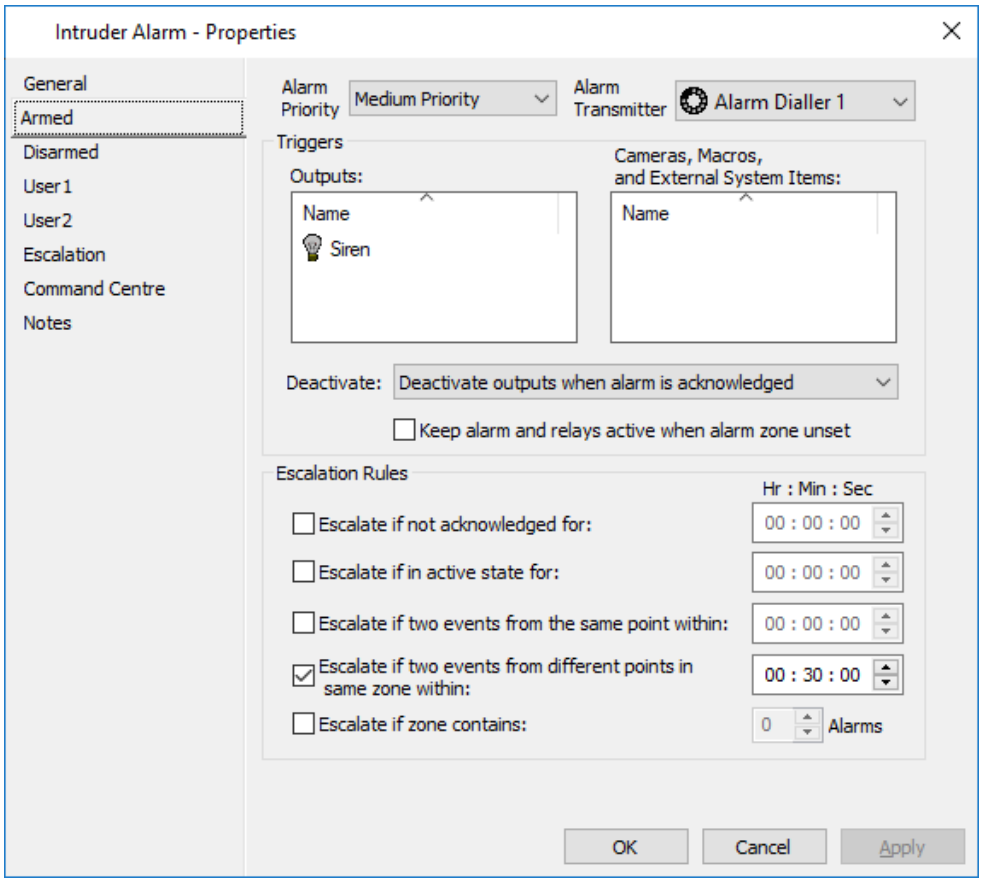


Note: Depending on the receiver used, the Transmitter ID may need to be set to match the Contact ID Account Code in Server Properties or Alarm Zone, Alarm Transmission or if the Account prefix is used, then this value is not sent. Refer to Command Centre Configuration Client online help or user guide.

Copyright © Gallagher Group Limited

6.1 Confirmed Alarms

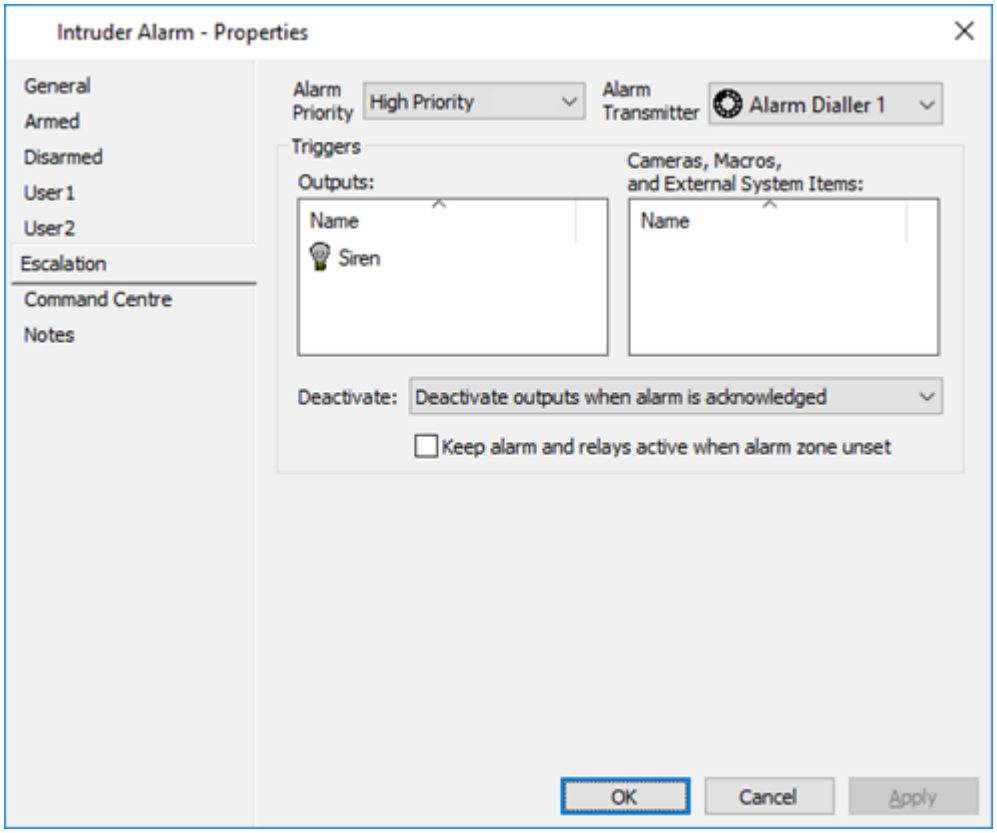
Alarm confirmation (BS 8243) is configured using escalation of the Intruder Alarm action plan. The Action Plan should be configured to escalate in the armed state according to the "Escalate if two events from different points in the same zone within x" rule. The time period assigned to this escalation rule will be the confirmation time for the zone. To comply with DD243 the confirmation time should be no less than 30 minutes and no more than 60 minutes. For a hold-up device, the confirmation time should be between 8 and 20 hours.



Note: For alarm confirmation to work correctly, all alarm points for an intruder alarm zone must be connected to the same controller.

The Action Plan should be configured with an escalation response on the Escalation page of the Action Plan. The behaviours configured into the escalated response will be the behaviours of confirmed alarms in the zone. An alarm dialler/transmitter should be assigned on the Escalation page. Escalated alarms will be transmitted to the alarm receiving centre using the Contact ID code for confirmed intrusion, which is code 139.

Copyright © Gallagher Group Limited



6.1.1 Tamper alarms contributing to confirmed alarms

According to BS 8243, tamper alarms are required to contribute to confirmed intruder alarms. To achieve this an action plan needs to be configured similar to Intruder Alarm above but assigned to the Tamper event group on detectors and other devices that can have tamper. For a small system this could be the default action plan for the Tamper event group. The difference from the above is that the alarm priority for tamper alarms must be High Priority or above, therefore the escalated action plan should be above this, (e.g. Very High Priority).

6.1.2 Siren output configuration

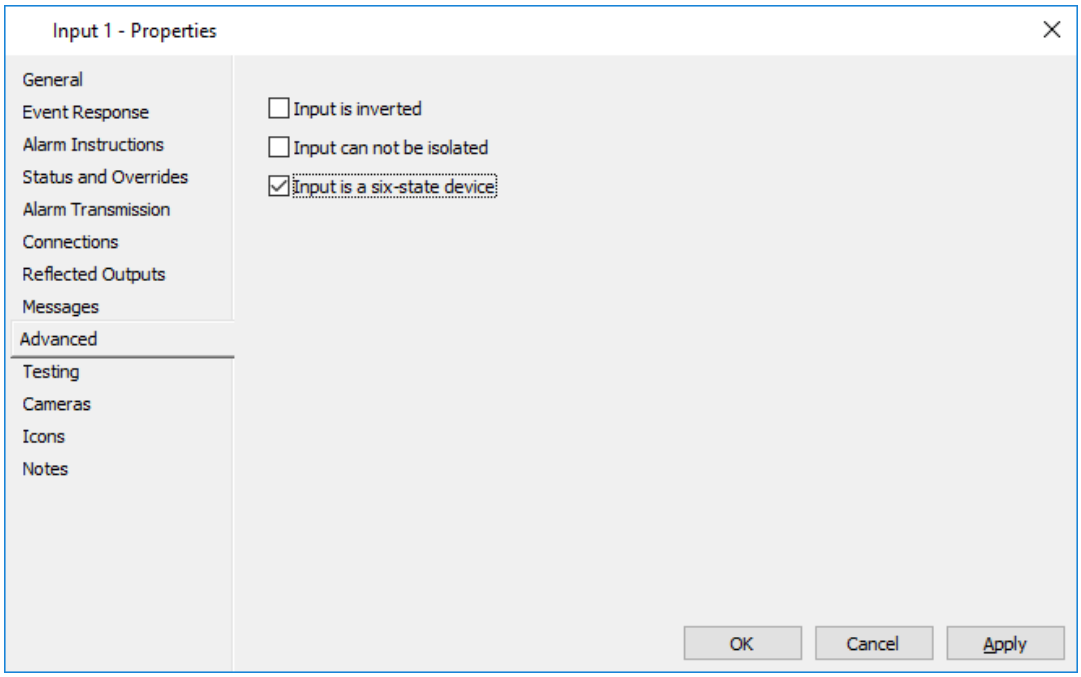
For correct operating of confirmed alarms, outputs assigned to action plans should have either no alarm zone assigned on the Event Response tab, or a different alarm zone not requiring alarm confirmation. Otherwise de-activation of the output is considered as contributing to alarm confirmation.

Copyright © Gallagher Group Limited

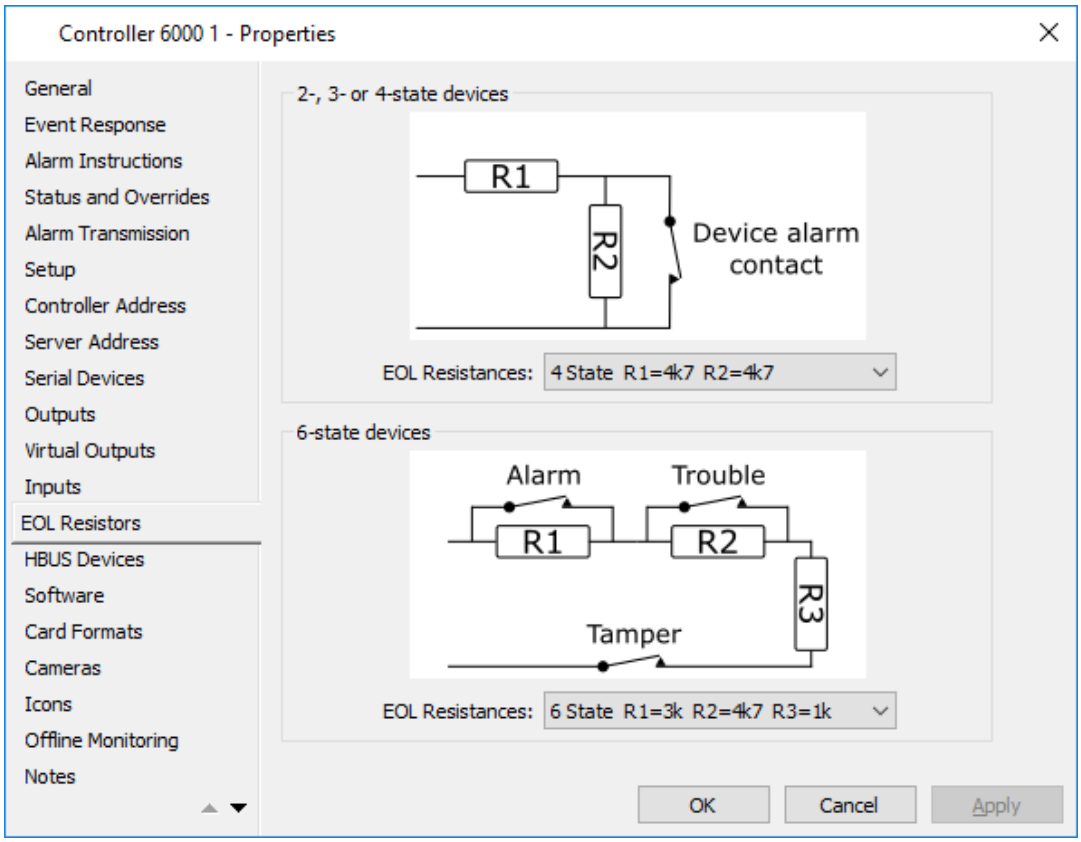
7 Detectors

For Grade 4 compliance, intrusion and hold-up detectors should be configured as Class 5 End-of-Line Modules.

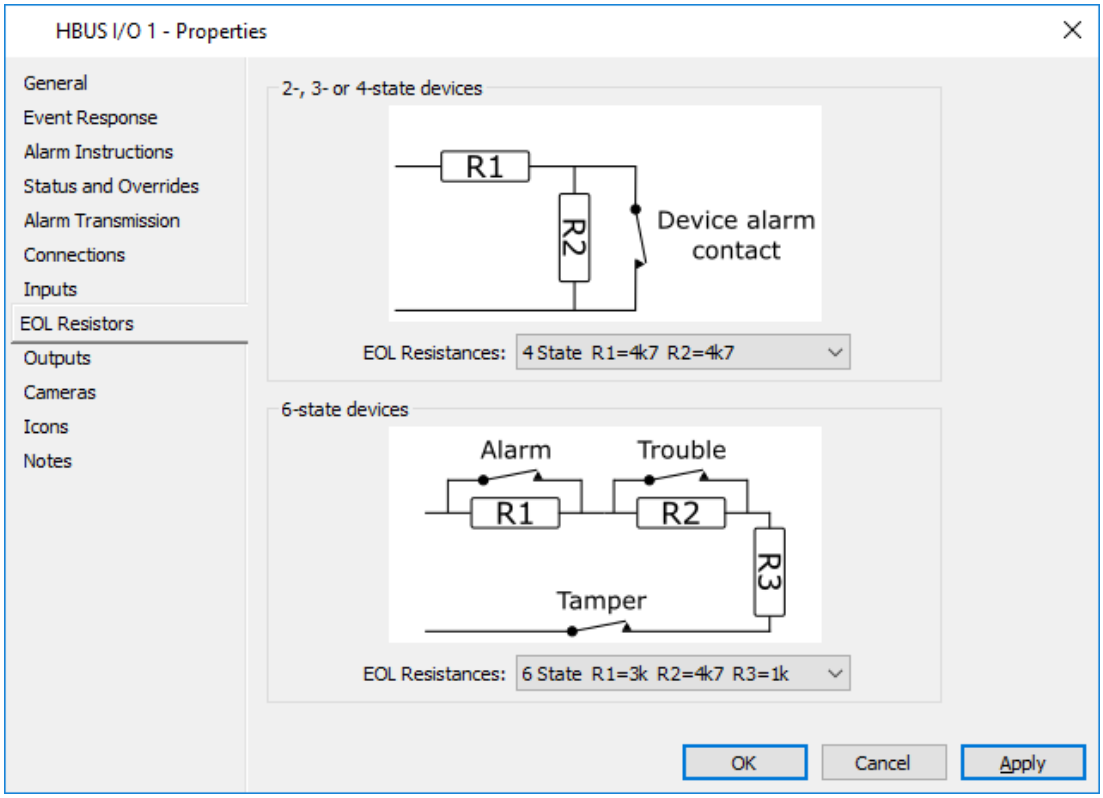
For lower grades, standard inputs can be used. If the detector supports the fault state and/or masked states, then the input needs to be configured to support these states using end-of-line resistances.



The specific end of line resistance values can be configured for each Controller or HBus I/O device.



Copyright © Gallagher Group Limited

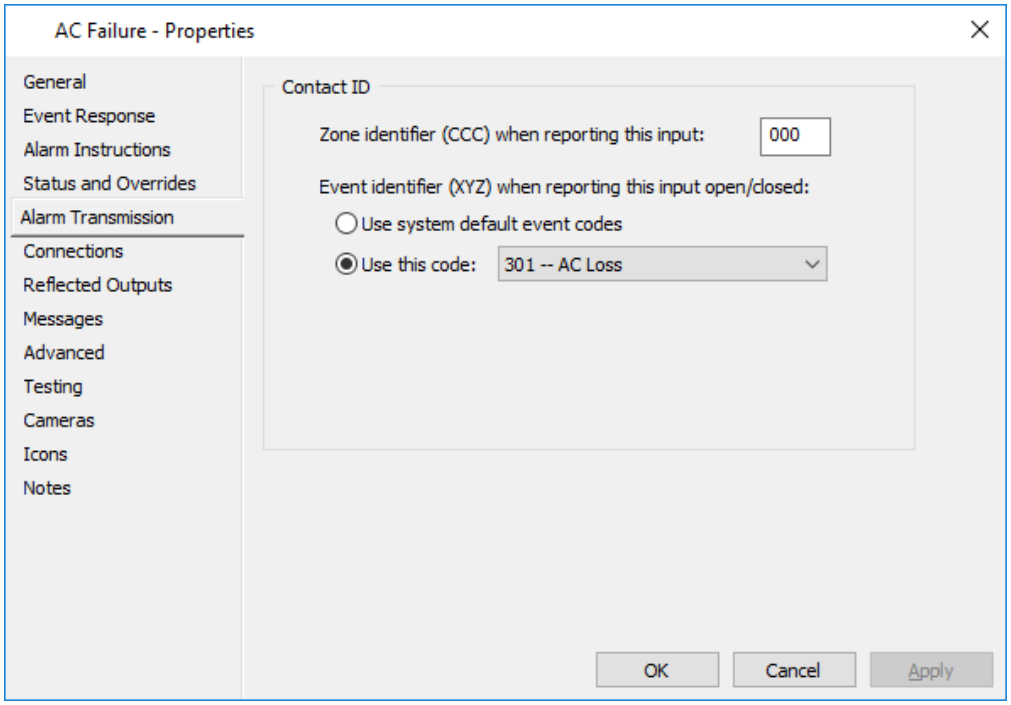


Copyright © Gallagher Group Limited

8 Configuring Compliance with Specific Clauses - EN 50131

8.1 8.1.4

Inputs should be wired from the power supply fault detection outputs to inputs on the controller. These inputs should be configured with an action plan with Medium priority or below, including an alarm transmitter or dialler. The inputs should have an appropriate alarm transmission code:



8.2 8.3.5

Setting is required to be prevented with various active alarm conditions present. As long as the alarm zone is configured as described above, this will work, however if there are multiple zones then it is possible that there are hardware items with faults or tamper conditions in a different zone from the one being armed. For the zone to be prevented from arming, hardware items such as I/O expansion boards should be configured with the same alarm zone as is assigned on the Controller's "Event Response" tab. If the "Conform to Standard EN50131" box has been checked on the Server Properties, Standards tab, active alarms in this zone will also prevent other zones from arming as required.

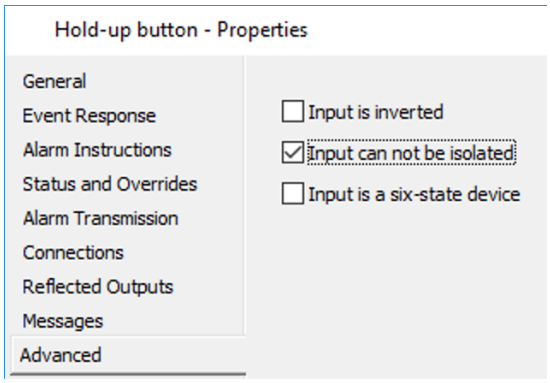
8.3 8.3.6

For compliance at Grades 3 & 4, the event groups corresponding to tamper (Tamper), Interconnection faults (Unit Stopped Responding, Command Centre Comms Interrupted, Inter-Controller Offline Monitoring), Alarm transmission system faults (Alarm Transmission Warning), Warning device fault (Open/Off for the appropriate input), and ATS and WD faults (Alarm Transmission Failure) should be assigned action plans with priority at least Medium High Priority.

Copyright © Gallagher Group Limited

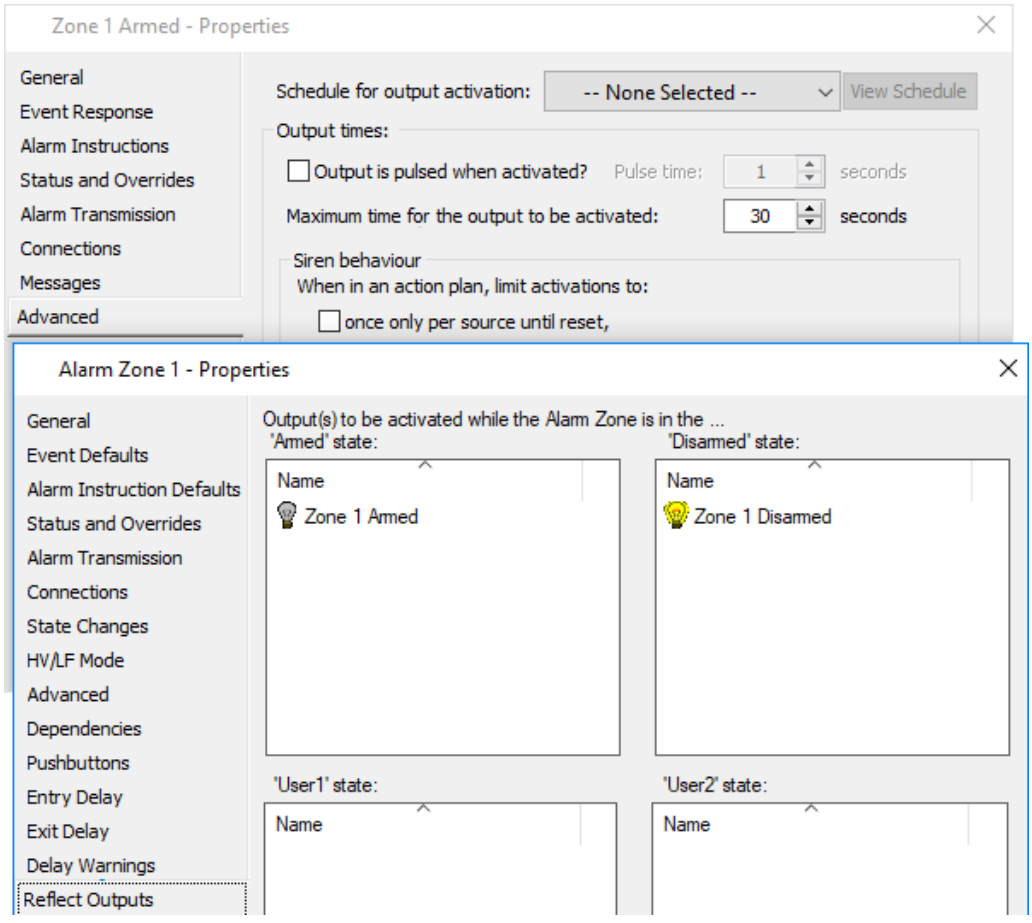
8.3.1 8.3.6.1

Auto-isolation is not allowed for hold-up inputs according to the standard. To ensure this, select “Input cannot be isolated” on the input’s Advanced tab:



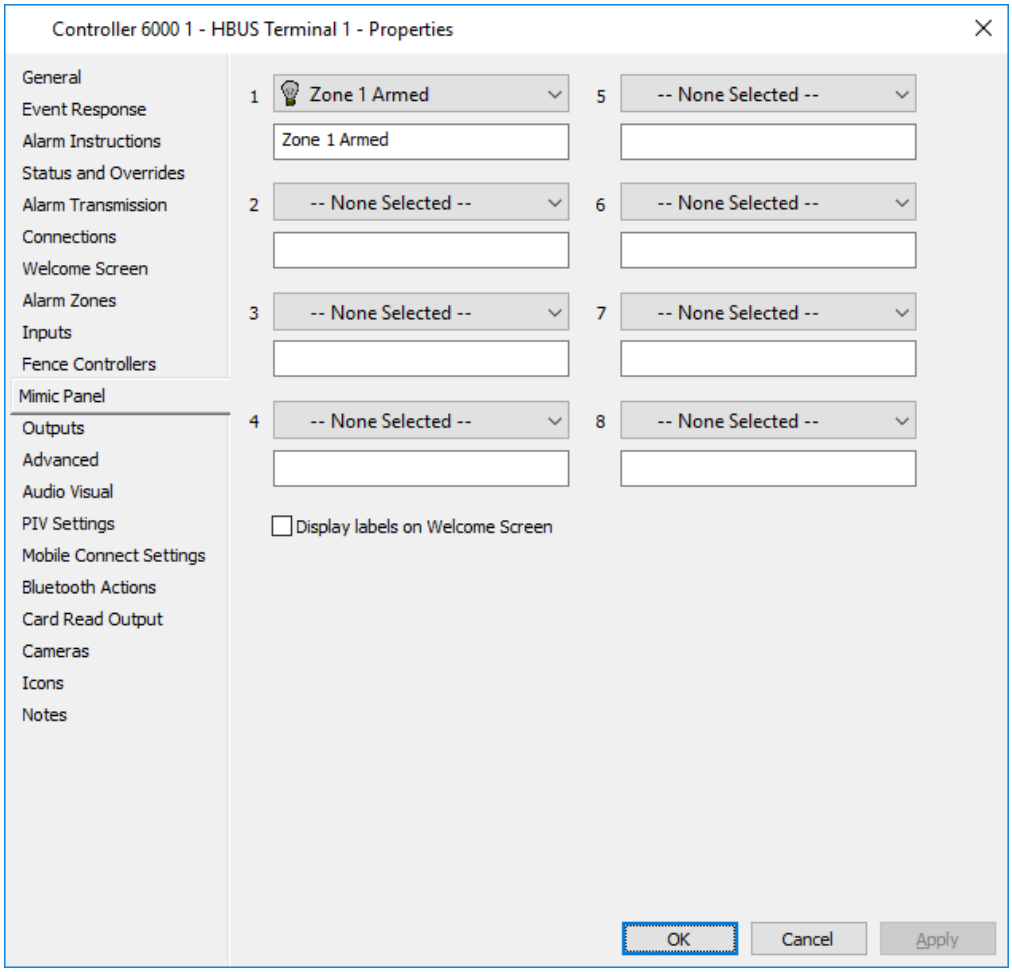
8.4 8.3.7

A time-limited completion of setting indication is required. This can be achieved by assigning an output to the Armed state of the alarm zone and configuring with a maximum on time:



Alternatively, or in addition, a real or virtual output configured as above can be assigned to the terminal’s LED mimic panel:

Copyright © Gallagher Group Limited



8.5 8.3.8

When an entry delay and route is configured for an alarm zone, the entry delay must be configured to no more than 45 seconds in order to comply.

8.6 8.3.9

For compliance at Grades 3 & 4, in order to enforce that restoring (acknowledging alarms) must be performed by a level 3 user for tamper and fault conditions (except for prime power source and alarm transmission/dialling failures), the event groups corresponding to these should have action plan assignments with alarm priority high or above.

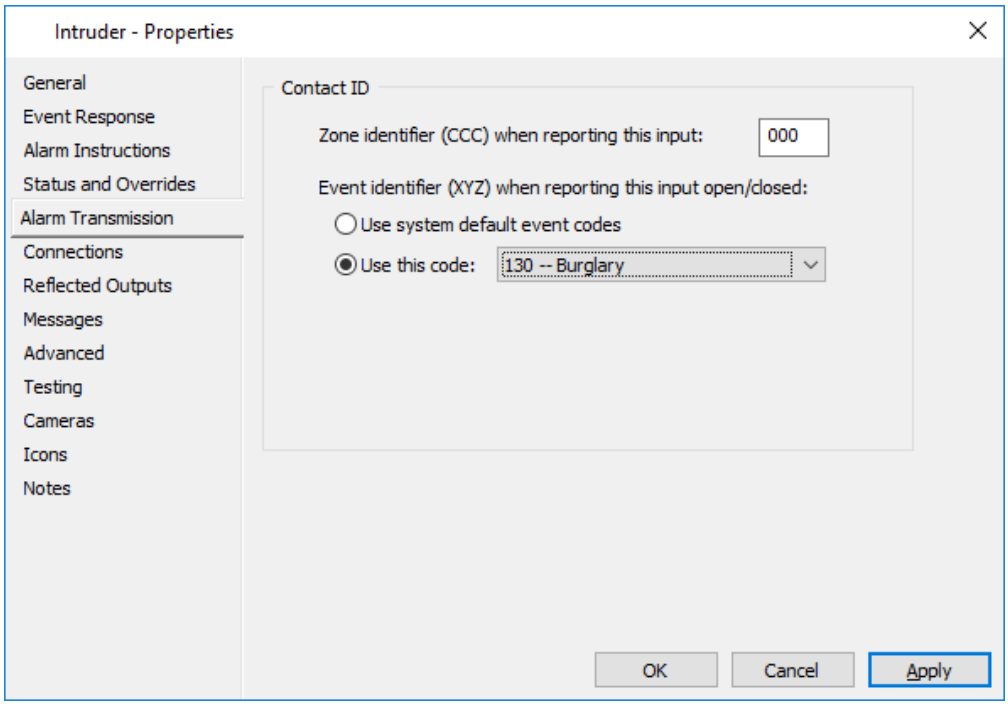
8.7 8.3.12

For compliance at Grades 3 & 4, Enabled should remain unchecked on the Testing tab for Class 5 End-of-line devices.

Copyright © Gallagher Group Limited

8.8 8.4

According to the grade and conditions, action plans should be configured with outputs for an External audible alarm, Internal audible alarm and alarm transmitter/dialler as required by table 7 of EN 50131-1. The ATS Message Type defaults are on the Server Properties, Alarm Transmission tab. For detectors these should be overridden according to the type of detector:

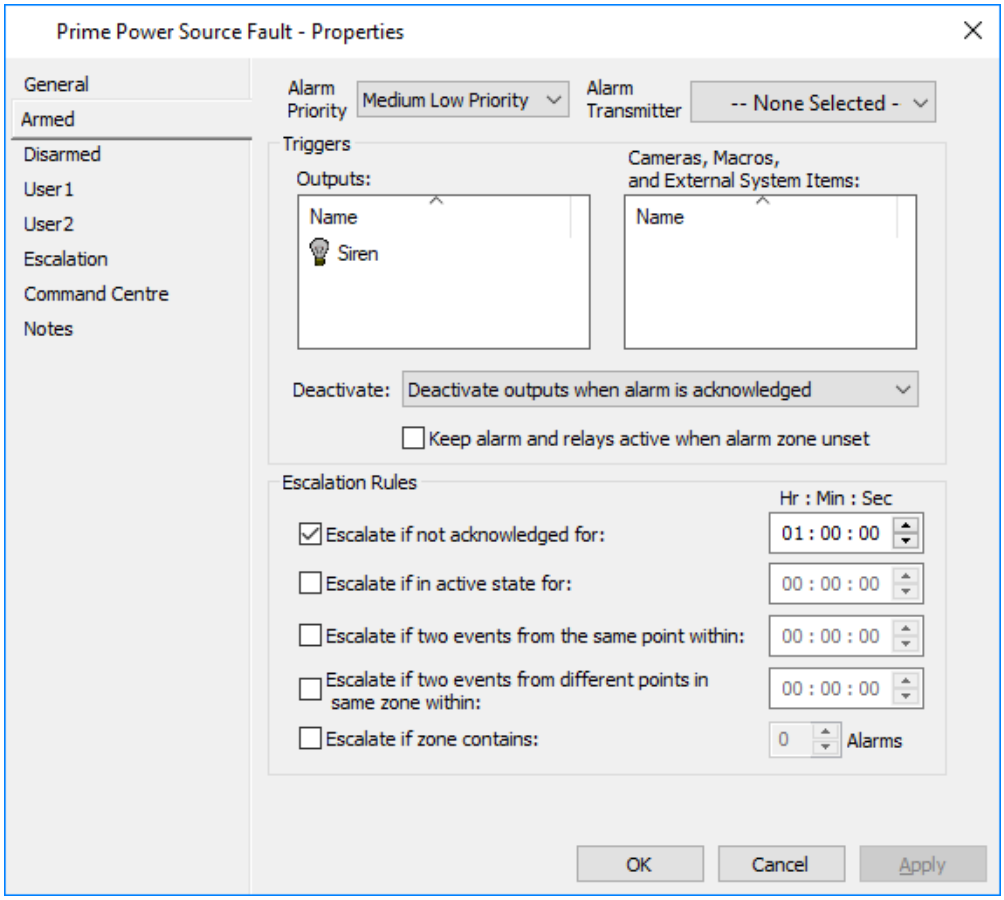


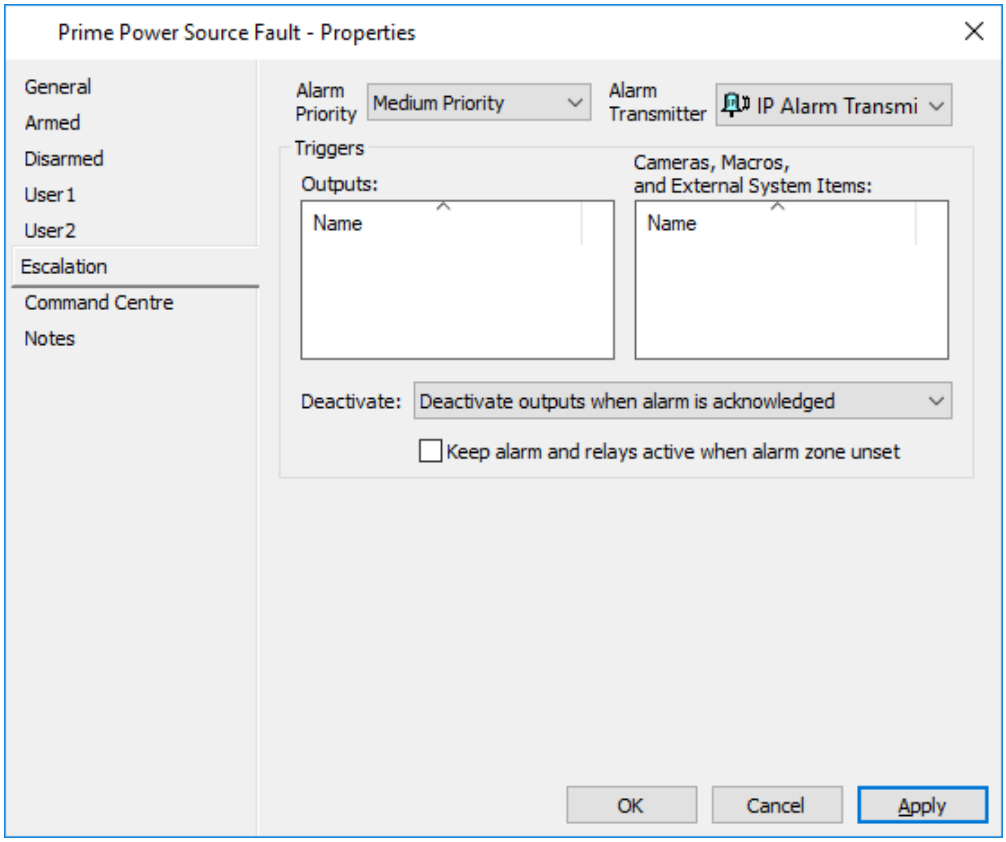
8.9 8.6.2

Action plans should be configured to comply with one of the options in table 10 according to the grade required. Warning devices are triggered by relays on action plans. Alarm transmission can be using an Alarm Dialler or Alarm Transmitter. For SP4, SP5, SP6, DP3 and DP4, an Alarm Transmitter with encryption enabled is required as described in section 6.

Notification of prime power source faults is allowed to be delayed by up to 1 hour (as long as the warning device activation is not delayed as in 8.6.3 next). This can be configured by using escalation on the action plan:

Copyright © Gallagher Group Limited

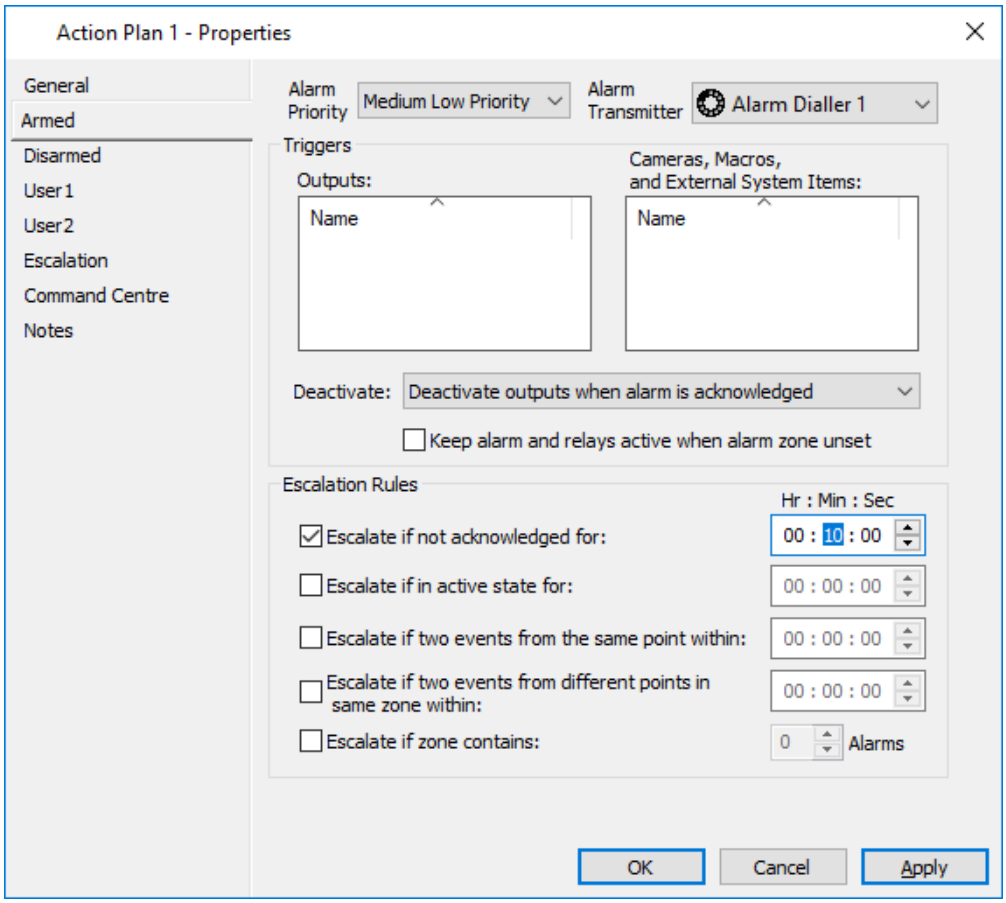




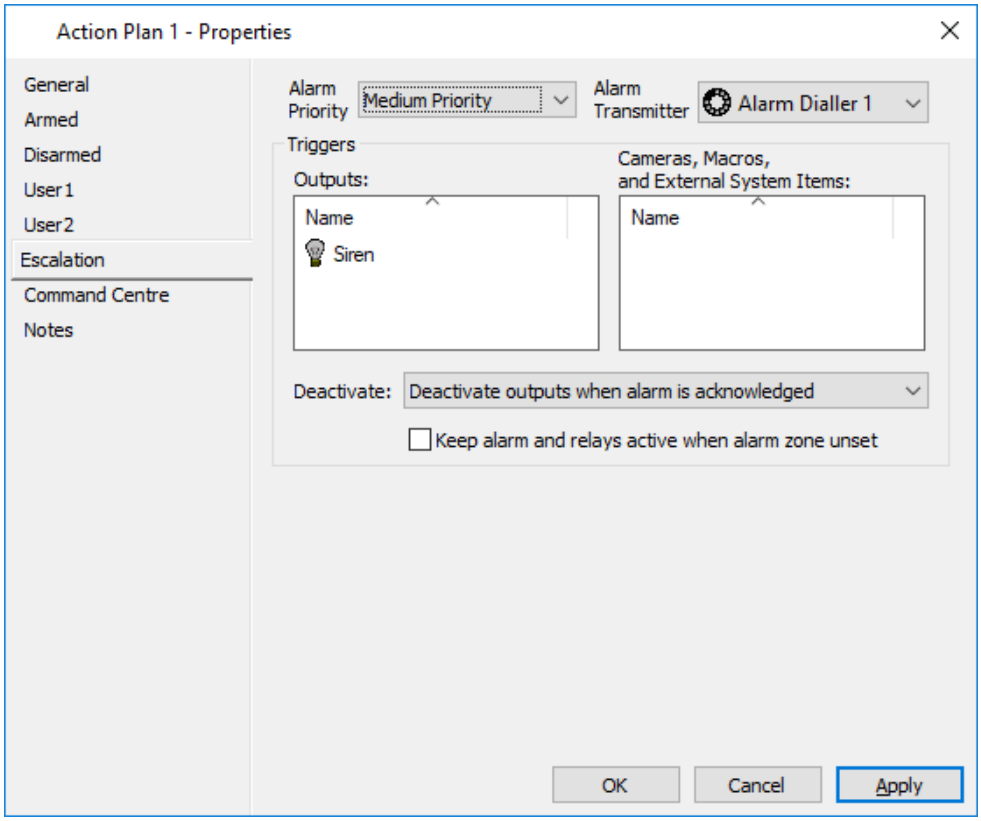
Copyright © Gallagher Group Limited

8.10 8.6.3

Warning device activation can be delayed by up to 10 minutes, provided alarm transmission happens immediately. This can be configured by using escalation on the action plan:

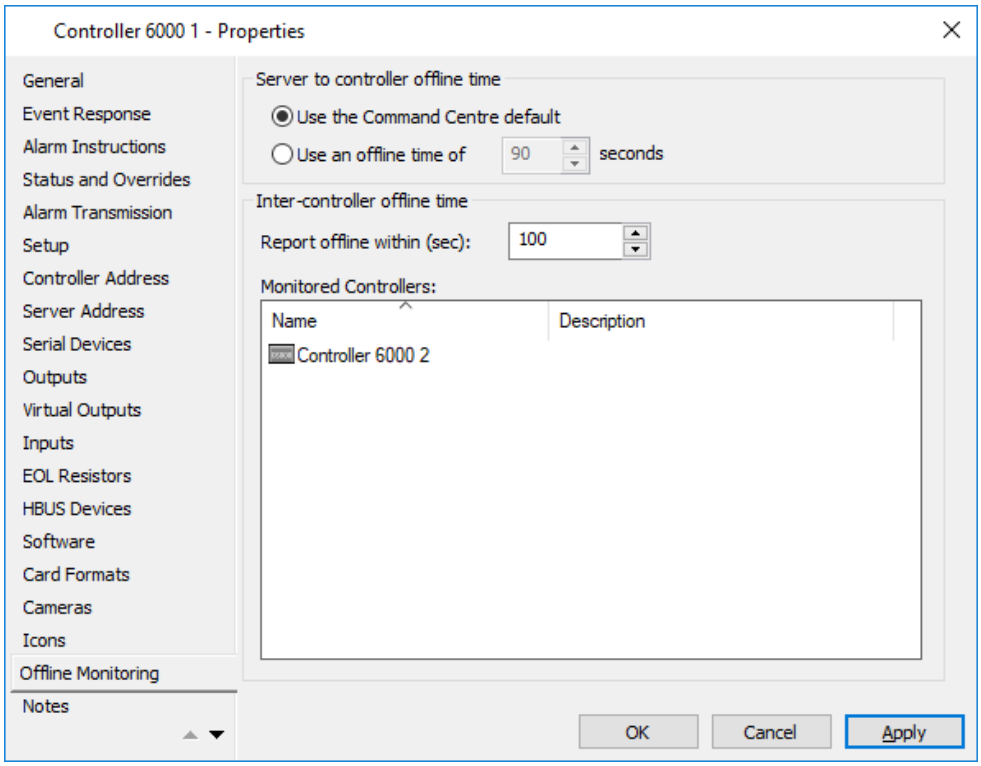


Copyright © Gallagher Group Limited



8.11 8.8.4

If alarms detection functionality is distributed across multiple controllers, (e.g. detectors within a single alarm zone), then inter-controller monitoring should be configured:

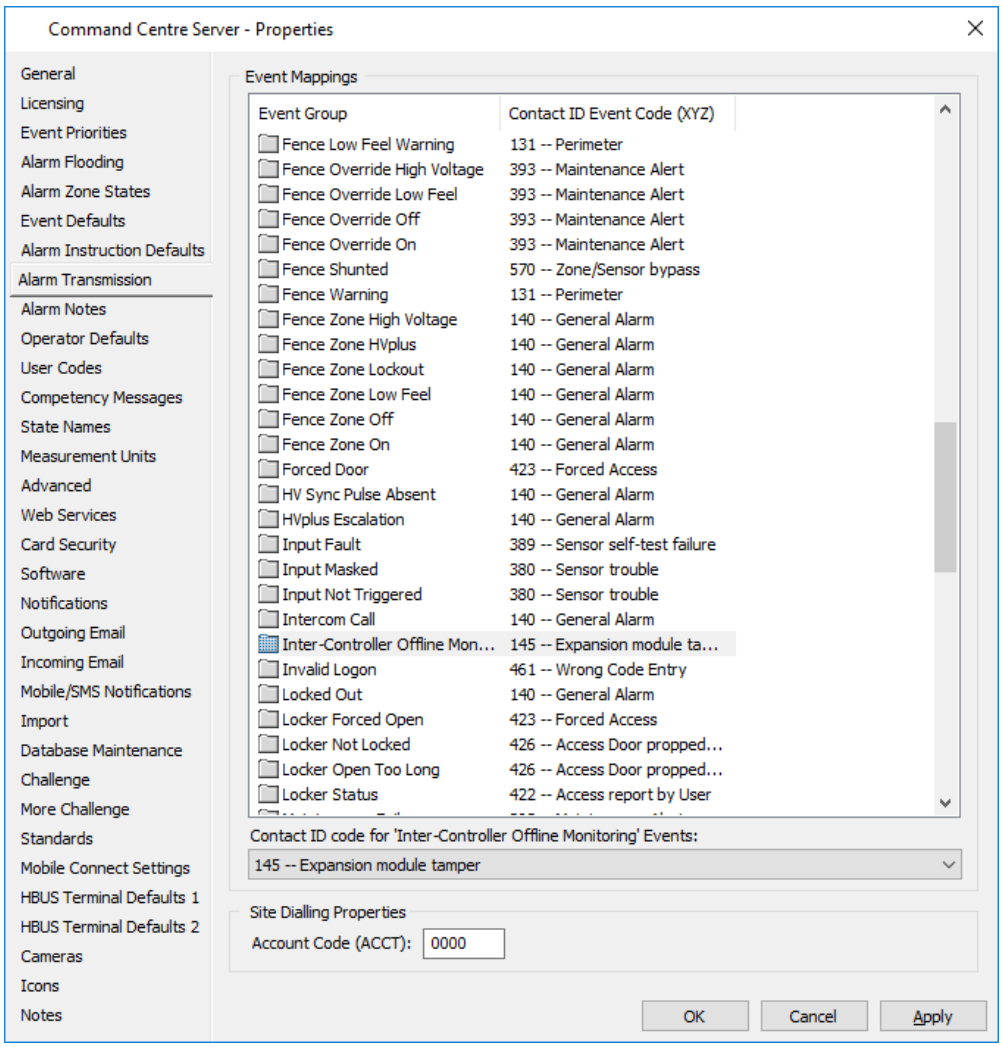


For compliance at Grade 4, functionality should not be distributed across controllers.

Copyright © Gallagher Group Limited

8.12 8.8.6

For compliance at Grades 3 & 4, the Command Centre Comms Interrupted, Primary ethernet link, Unit Stopped Responding and Inter-Controller Offline Monitoring event groups should be mapped to "145 - Expansion module tamper":



8.13 EN 50131-3 Optional Features Supported

The following features identified as optional for this standard at grade 4 supported by Command Centre are:

- Masking when unset (8.1.6)
- Exit routes (8.3.3.2)
- Entry routes (8.3.4)

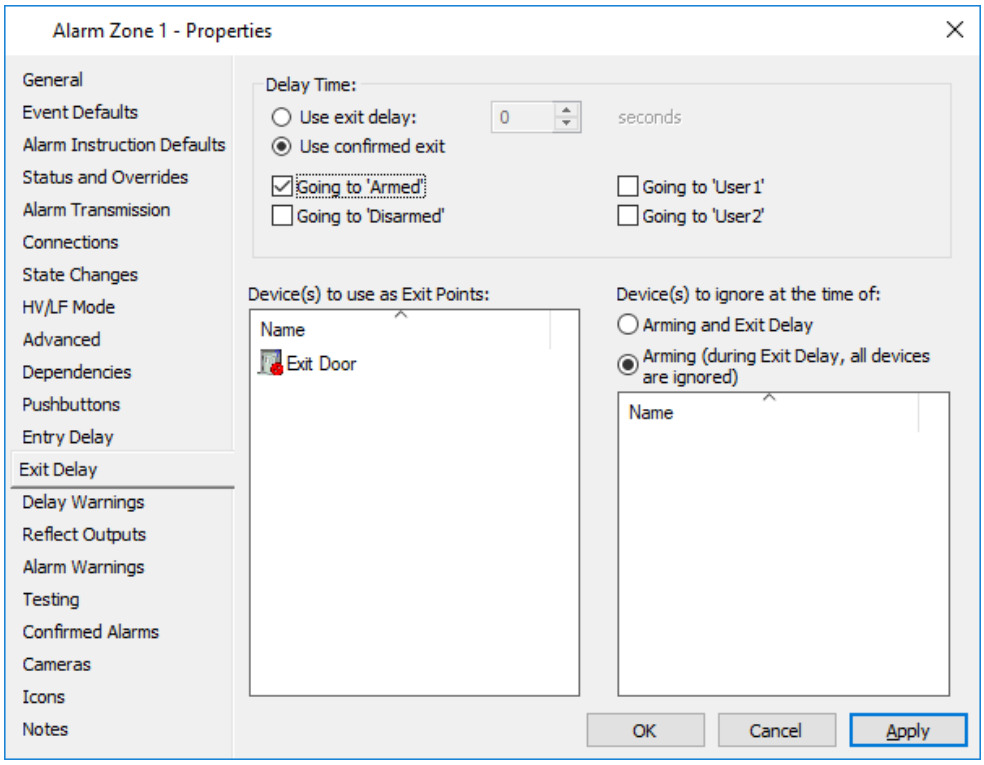
Copyright © Gallagher Group Limited

9 Configuration of Specific Clauses - BS 8243

9.1 6.3

BS 8243 requires that completion of setting is achieved solely by the range of signals listed in section 6.3 of the standard.

In order to comply with section 6.3 for zones with an exit path where arming is initiated from a keypad, select the “Use confirmed exit” option for the alarm zone’s exit procedure. This is found on the Alarm Zone | Exit Delay property page. This setting will cause the alarm zone to have an exit delay that doesn’t time out, but only completes when one of the exit points activates:



If the exit point is an Input – The exit delay will finish and the zone will arm when the input activates.

If the exit point is a Command Centre Door – The exit delay will finish and the zone will arm when the door transitions to a secure state.

Note that "confirmed exit" mode has potential dangers in that the zone will never set if one of the exit points does not activate. For this reason, confirmed exit mode should never be used for zones that have an arming schedule defined – because there is no guarantee that someone will be present at the time of auto-arming (to terminate the exit delay) and therefore the zone may not set.

9.2 6.4

BS 8243 approves five options for unsetting a site. These are specified in sections 6.4.2 to 6.4.6 of BS 8243. All five options are designed to minimise the risk of generating false confirmed alarms during unsetting.

Command Centre can be configured to support any of the five unsetting options. This section describes the configuration procedures for each option and then details the alarm behaviour

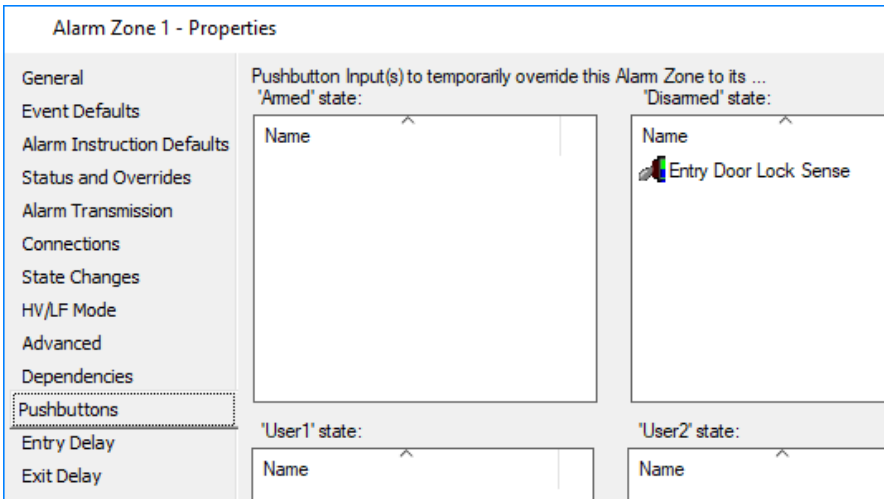
Copyright © Gallagher Group Limited

during an unsetting operation. For all options ensure that the system setting "Enable confirmed alarms" is enabled on the System | Standards property page.

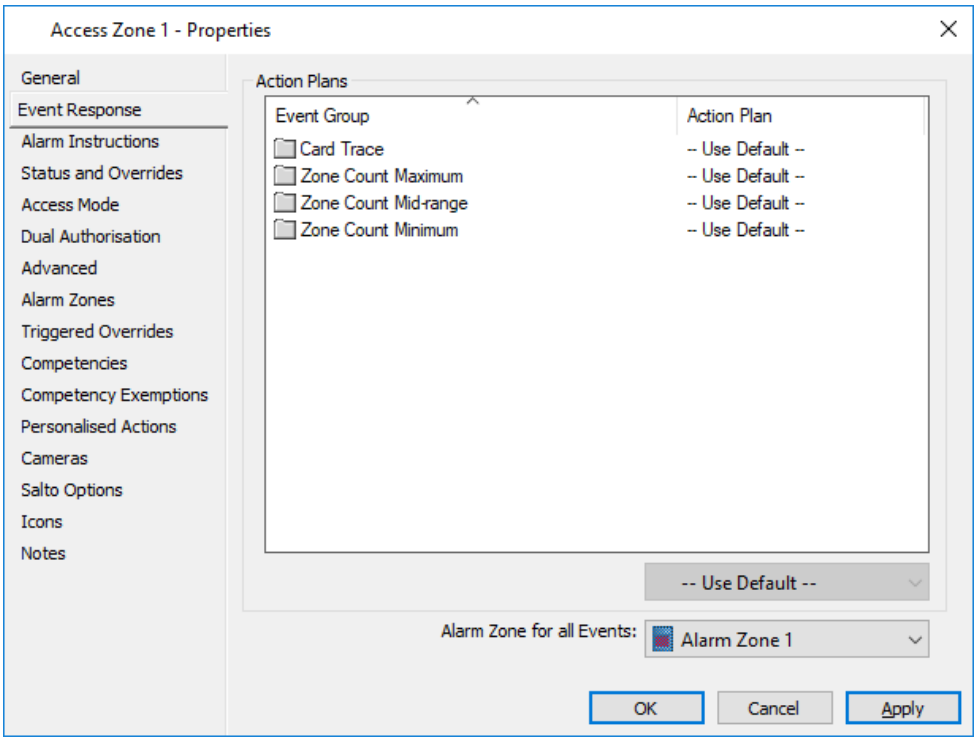
9.2.1 Option 1 – Prevention of entry before the system is unset – BS 8243 section 6.4.2

Either (a) unlocking the entry door unsets the system, or (b) unsetting the system before entering causes the entry door to be unlocked.

1. **To configure option (a)** – Configure the door's lock sensor input to override the alarm zone to its disarmed state, using the Alarm Zone | Pushbuttons property page.



2. **To configure option (b)** – Configure a Command Centre Door with an entry reader and entry access zone. Assign the alarm zone (whose state is to be controlled) to the entry access zone, using the Access Zone | Event Response property page. When access is granted to the entry door the system will automatically unset the alarm zone before unlocking the door.

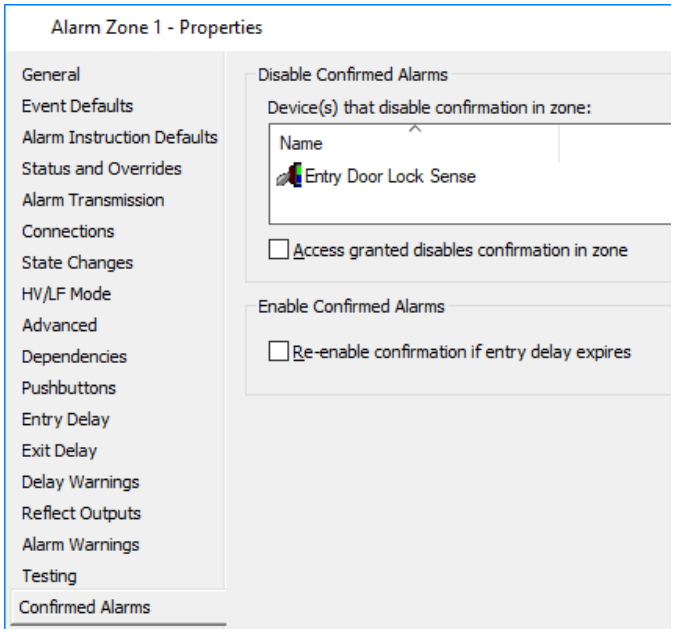


Copyright © Gallagher Group Limited

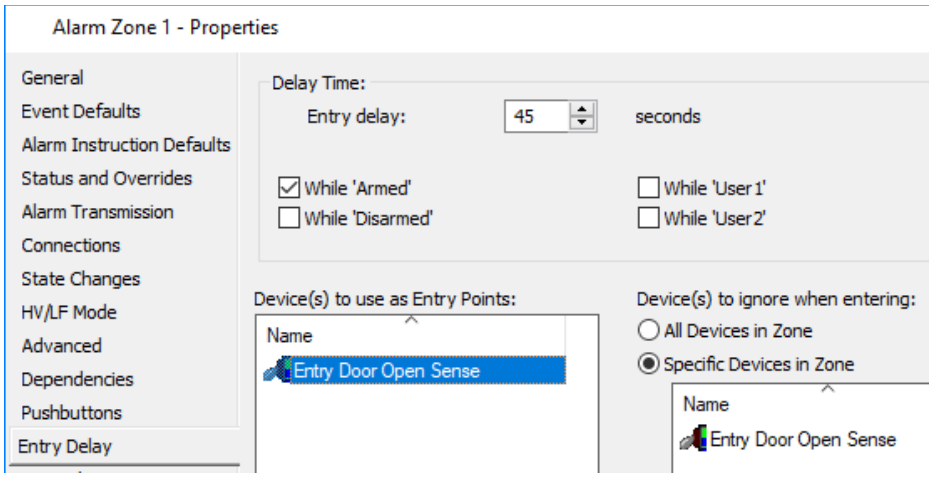
9.2.2 Option 2 – Prevention of entry before all means of confirmation have been disabled – BS 8243 section 6.4.3

Either (a) unlocking the entry door causes all means of alarm confirmation to be disabled, or (b) disabling means of confirmation before entering causes the entry door to be unlocked.

To configure option (a) – Configure the door's lock sensor to disable confirmed alarms in the zone, using the Alarm Zone | Confirmed Alarms page:

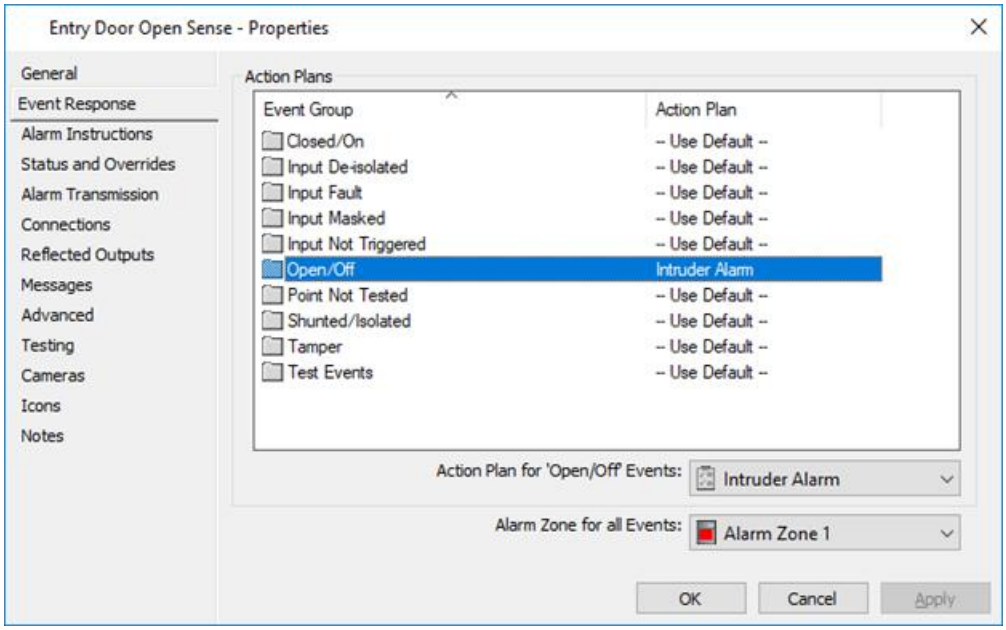


Configure the door's open sensor to be an entry point for the alarm zone and add it to the zone's entry path:



Assign the confirmed alarm Action Plan to the open sensor's active state.

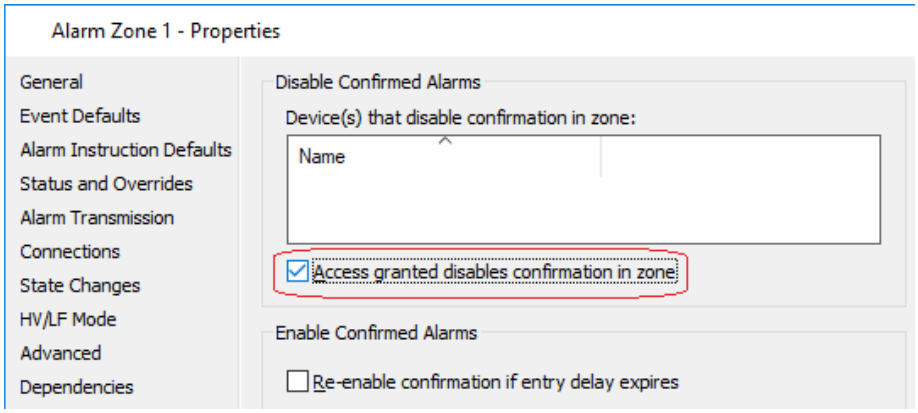
Copyright © Gallagher Group Limited



During a normal entry – The entry door will be unlocked and this will cause alarm confirmation to be inhibited in the alarm zone. The entry door will open and this will cause the entry delay procedure to start. And because the open sensor has been added to the entry path ignore list it will not cause an alarm to be generated on opening.

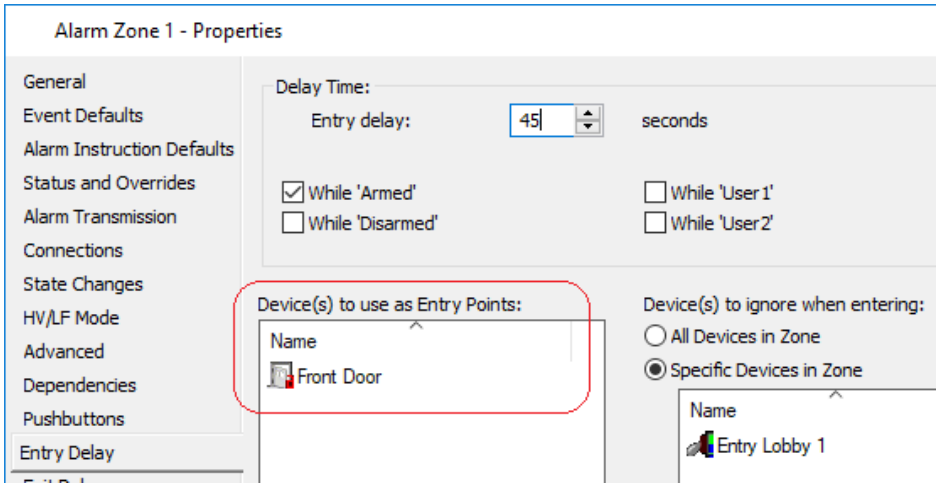
During a forced entry – The entry door will not be unlocked, the lock sensor will not activate, and therefore confirmed alarms will not be disabled in the zone. Because confirmed alarms have not been inhibited in the zone, the zone will not begin an entry delay procedure when the door opens. Because the zone is not in entry delay, the open sensor will cause an immediate unconfirmed alarm, (i.e. forced door) which will count towards a confirmed alarm if a second sensor activates within the confirmation time.

To configure option (b) – Use a full Command Centre access controlled door, configured as described in the instructions for 6.4.2, above – i.e. the entry access zone should be linked to the alarm zone that is to be controlled. Select the following option on the Alarm Zone | Confirmed Alarms property page:



Add the door to the entry point list for the alarm zone, on the Alarm Zone | Entry Delay page.

Copyright © Gallagher Group Limited



During normal entry – An access granted at the entry door will cause confirmed alarms to be inhibited in the alarm zone. Because the door is an entry point for the zone, when the door signals access taken, (i.e. access granted + door opened) the entry delay procedure will start.

During forced entry – Because there is no access granted at the entry door, confirmed alarms will not be inhibited for the zone. The Command Centre Door item will also raise a forced door alarm if the door's open sensor activates when there hasn't been an access granted. Entry delay will not start because the Command Centre door does not signal a valid access taken.

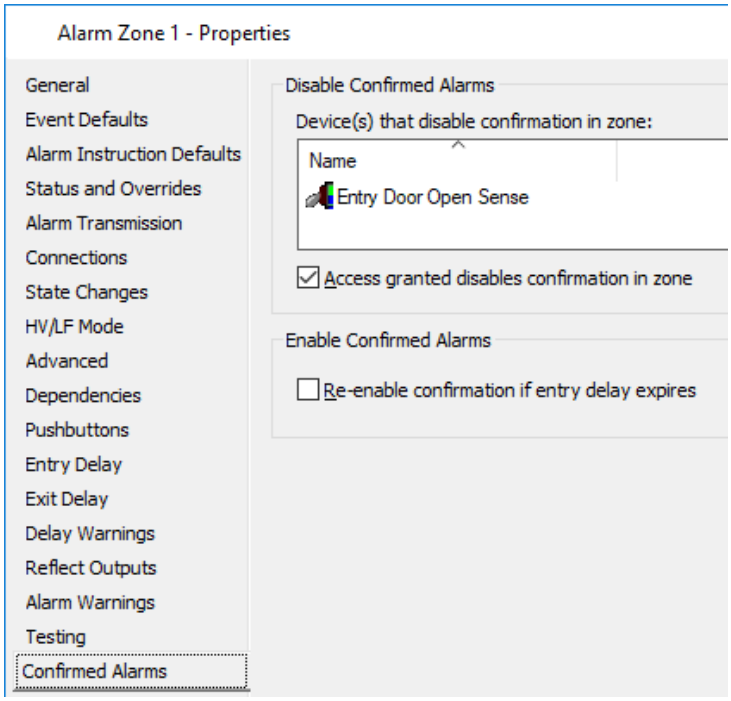
9.2.3 Option 3 – Opening the entry door disables all means of confirmation – BS 8243 section 6.4.4

Under this option the entry door has an open sensor but no lock sensor; therefore a forced entry door cannot be detected. On activation of the open sensor confirmed alarms are inhibited in the zone. The design proposal to the end user, and the as fitted document should contain the following warning:

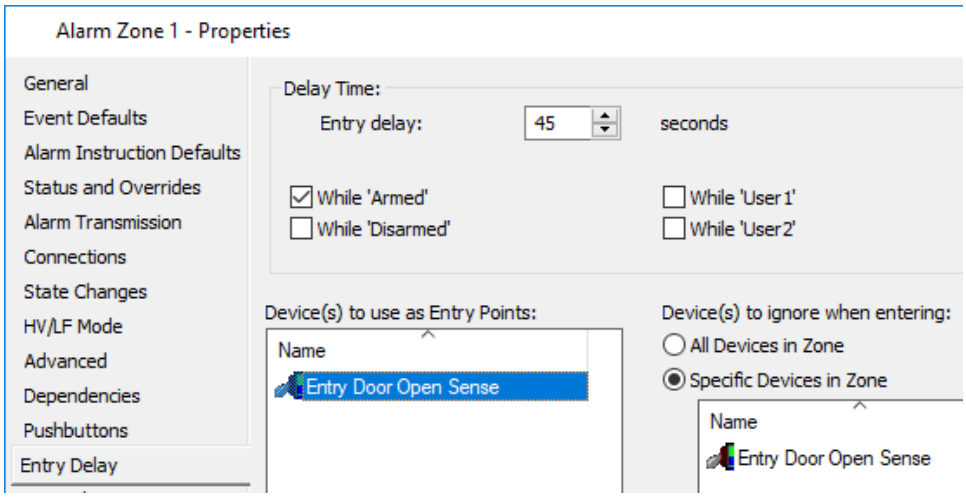
> **"IMPORTANT**
>
> **Your attention is drawn to the fact that by allowing this method of unsetting, if an intruder succeeds in forcing the initial entry door, the police will not be called, regardless of the intruder's further progress through the supervised premises.**
>
> **This method of unsetting the intruder alarm system might be unacceptable to your insurers."**

To configure this option – Configure the door's open sensor to disable confirmation in the alarm zone, using the Alarm Zone | Confirmed Alarms property page:

Copyright © Gallagher Group Limited



Configure the door's open sensor to be an entry point for the alarm zone and add it to the zone's entry path:



During any entry – When the entry door opens, confirmed alarms will be inhibited in the alarm zone. Because the open sensor is configured as an entry point, and because confirmed alarms have been inhibited in the zone, the zone will begin entry delay.

9.2.4 Option 4 – Completion of unsetting using a digital key – BS 8243 section 6.4.5

With this option, disarming is completed using a digital key, (i.e. a card). There are two options, either the reader is located outside the zone allowing the disarm to happen before entry or inside the zone, with an entry path to the reader. In the latter case if a T20 terminal is used, then it should be configured to only require a card for logon as using a code during entry delay is not permitted:

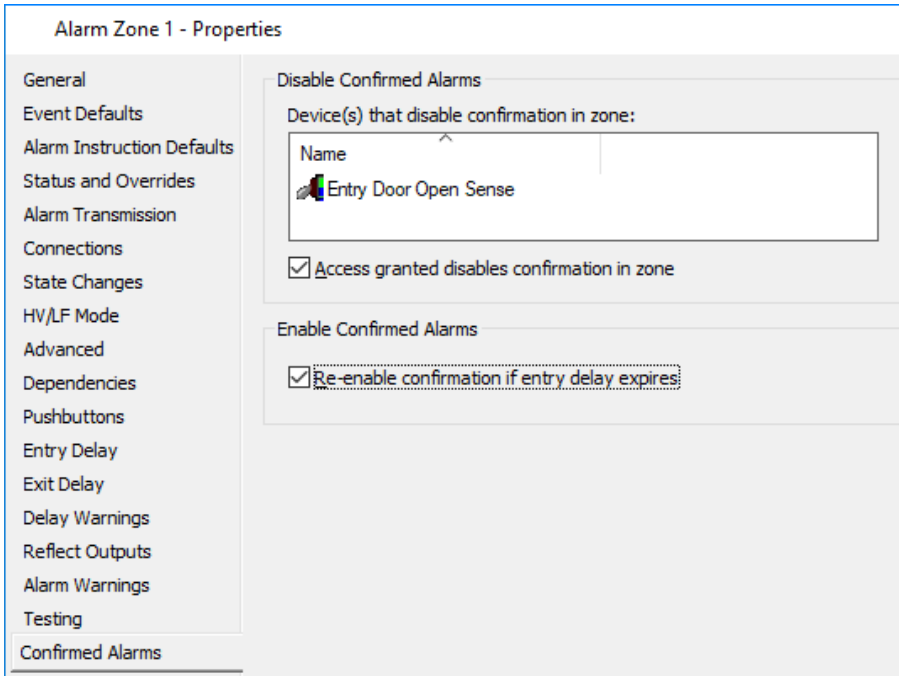


Copyright © Gallagher Group Limited

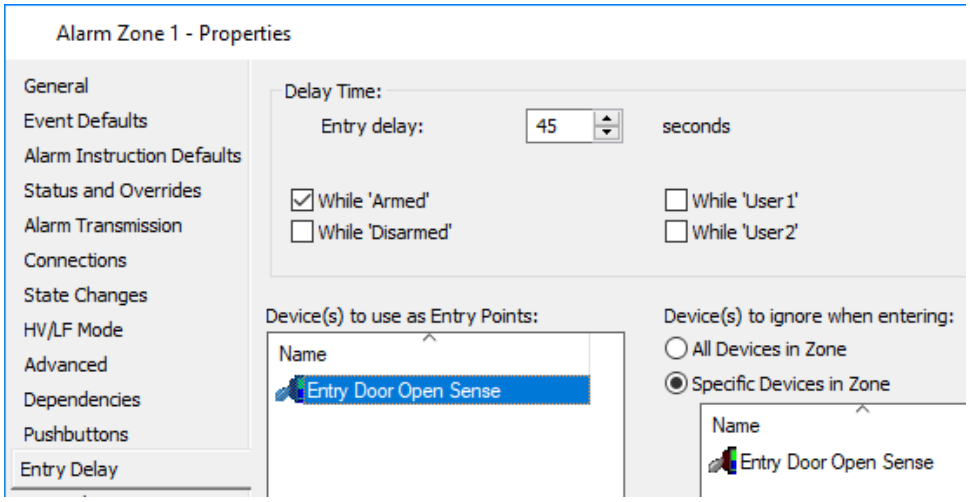
Under this option the entry door opening will inhibit confirmed alarms only during the entry delay period. If the entry delay expires then confirmed alarms are re-enabled and activations from detectors off the entry path can cause confirmed alarms.

In Command Centre, this mode may be configured either with a simple entry door having only an open sensor, or it may be configured with a full access controlled door.

To configure for a simple entry door – Configure the door's open sensor to disable confirmed alarms in the zone, using the Alarm Zone | Confirmed Alarms page. On the same page configure confirmed alarms to be re-enabled if entry delay expires:

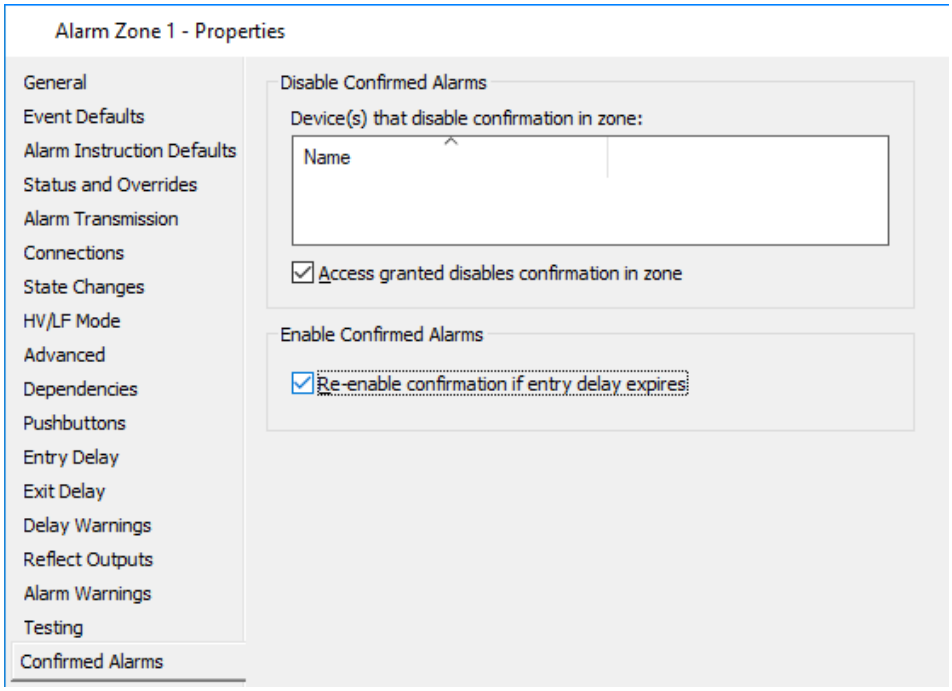


Configure the door's open sensor to be an entry point for the alarm zone and add it to the zone's entry path:

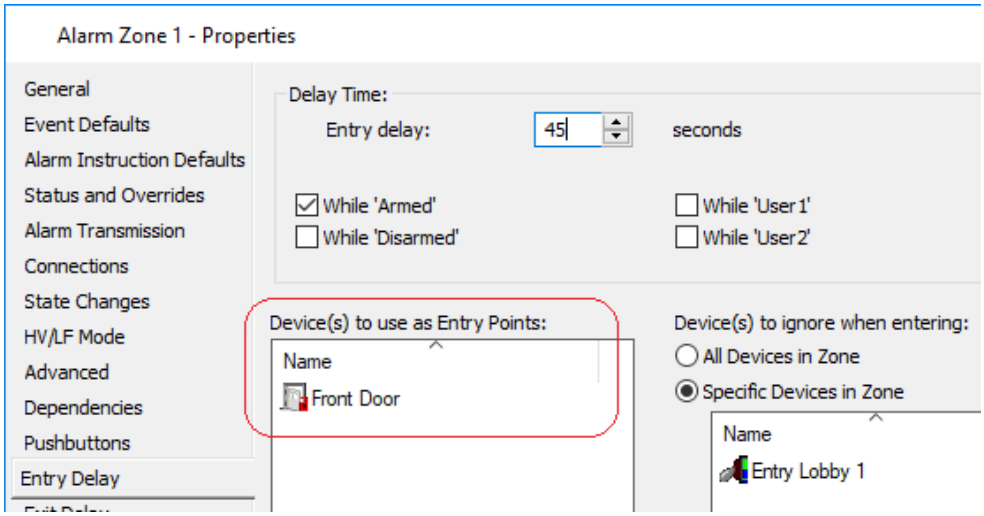


To configure for a Command Centre access controlled door – Configure access granted to disable confirmed alarms in the zone, using the Alarm Zone | Confirmed Alarms page. On the same page configure confirmed alarms to be re-enabled if entry delay expires:

Copyright © Gallagher Group Limited



Add the door to the entry point list for the alarm zone, on the Alarm Zone | Entry Delay page:



9.2.5 Option 5 - Unsetting in conjunction with ARC - BS 8243 section 6.4.6

This mode involves the alarm receiving centre unsetting the alarm zone, in conjunction with the user present at the site. One way of achieving this mode would be for the alarm receiving centre to have a Command Centre workstation that they use to unset the zone manually. Another way of achieving it would be to wire a relay output from a third party system as an input on the Command Centre system.

The input would then be configured as a pushbutton override for the alarm zone (via the Alarm Zone | Pushbuttons property page). The alarm company could then use the third party system to connect in and disarm the alarm zone.

Copyright © Gallagher Group Limited

Unsetting Option	Alarm Behaviour During Unsetting Red = Confirmation enabled. Green = Confirmation inhibited. Zone Armed	Entry Delay	Entry Delay Expired	Notes
6.4.2 Prevention of entry before IAS is unset	* Zone input: Unconfirmed alarm. Counts towards confirmed alarm. * Normal entry: Disarms zone. * Forced entry: Unconfirmed alarm. Zone remains armed.	N/A	N/A	* Requires lock sensor on entry door.
6.4.3 Prevention of entry before all means of confirmation have been disabled	* Points on entry path: Unconfirmed alarm, counts towards confirmed alarm. * Points off entry path: Unconfirmed alarm. Counts towards confirmed alarm. * Normal entry: Starts entry delay, no alarm. * Forced entry: Unconfirmed alarm. Counts towards confirmed alarm. No entry delay.	* Points on entry path: Ignored * Points off entry path: Unconfirmed alarm (delayed notification)	* On expiry of entry delay: Unconfirmed alarm. * Points on entry path: Ignored * Points off entry path: Unconfirmed alarm. Does not cause confirmed alarm.	* Requires lock & open sensors on entry door * Requires reset of zone (disarm then rearm) to re-enable confirmation.
6.4.4 Opening the initial entry door disables all means of confirmation	* Points on entry path: Unconfirmed alarm. Counts towards confirmed alarm. * Points off entry path: Unconfirmed alarm. Counts towards confirmed alarm. * Normal entry: Starts entry delay, no alarm. * Forced entry: **Starts entry delay, no alarm**.	* Points on entry path: Ignored * Points off entry path: Unconfirmed alarm (delayed notification)	* On expiry of entry delay: Unconfirmed alarm. * Points on entry path: Ignored * Points off entry path: Unconfirmed alarm. Does not cause confirmed alarm.	* Entry door has open sensor, but no lock sensor. * Requires reset of zone (disarm then rearm) to re-enable confirmation.
6.4.5 Completion of unsetting using a digital key	* Points on entry path: Unconfirmed alarm. Counts towards confirmed alarm. * Points off entry path: Unconfirmed alarm. Counts towards confirmed alarm. * Entry: Starts entry delay, no alarm	* Points on entry path: Ignored * Points off entry path: Unconfirmed alarm (delayed notification	* On expiry of entry delay: Unconfirmed alarm. Does not count towards confirmed alarm. * Points on entry path: Ignored * Points off entry path: Unconfirmed alarm. **Counts towards confirmed alarm**.	* Only allowed digital key for unsetting when an entry delay used. * Requires reset of zone (disarm then rearm) to re-enable CA for entry path inputs.

Copyright © Gallagher Group Limited

Appendix 1: Mandatory Events

Event Group	Standard	Events in Standard	Grades
Alarm Transmission Failure	50131-1	ATS fault	2-4
Alarm Transmission Warning	50131-1	ATS fault and ATP fault	2-4
Alarm Zone Change Problem	50131-3	Failure to set	2-4
Alarm Zone State Change	50131-1	Set/Unset	2-4
Command Centre Comms Interrupted	50131-1	Interconnections fault	3-4
Input Fault	50131-1	Detector fault/Holdup device fault	3-4
Input Masked	50131-3	Masking/Reduction of range	3-4
Inter-Controller Offline Monitoring	50131-1	Interconnections fault	3-4
Network Attack	50131-1	Interconnections fault	3-4
Power Failure	50131-3	Failure of CIE processing	3-4
Primary ethernet link	50131-1	Interconnections fault	3-4
Repeated Log On Failure	50131-3	Input device disabled for detection of repeated invalid authorisation codes	2-4
Secondary ethernet link	50131-1	Interconnections fault	3-4
Security Breach	50131-1	Detection of substitution	4
Shunted/Isolated	50131-1	Zone/Intrusion detector/Hold-up device Isolated/inhibited	2-4
Tamper	50131-1	Tamper condition	2-4
Tamper on Repeated Logon	50131-3	Tamper condition	2-4
Unit Stopped Responding	50131-1	Interconnections fault	3-4

Note: Perimeter security devices can be considered as intrusion detectors, so the following event groups should also be configured if these are being used:

Event Group	Standard	Events in Standard	Grades
Fence Alarm	50131-1	Intruder alarm condition	2-4
Fence Low Feel Alarm	50131-1	Intruder alarm condition	2-4
Fence Shunted	50131-1	Intrusion detector Isolated	2-4
Perimeter Attack	50131-1	Intruder alarm condition	2-4
Sensor Alert	50131-1	Intruder alarm condition	2-4

Copyright © Gallagher Group Limited